BrainDumps.SY0-401_830.questions&answers

Number: SY0-401
Passing Score: 800
Time Limit: 120 min
File Version: 23.01

BrainDumps
CompTIA SY0-401
CompTIA Security+ Certification

- 100% valid, I didn't fail any question, all of them are in this VCE.
- I have solved " Stream read error " problem in VCE player .
- All questions ok, many answers are well explained.

Exam A

QUESTION 1
Several employees submit the same phishing email to the administrator. The administrator finds that the links in the email are not being blocked by the company's security device. Which of the following might the administrator do in the short term to prevent the emails from being received?

A. Configure an ACL
B. Implement a URL filter
C. Add the domain to a block list
D. Enable TLS on the mail server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
A company has several conference rooms with wired network jacks that are used by both employees and guests. Employees need access to internal resources and guests only need access to the Internet. Which of the following combinations is BEST to meet the requirements?

A. NAT and DMZ
B. VPN and IPSec
C. Switches and a firewall
D. 802.1x and VLANs

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
LDAP and Kerberos are commonly used for which of the following?

A. To perform queries on a directory service
B. To store usernames and passwords for Federated Identity

C. To sign SSL wildcard certificates for subdomains
D. To utilize single sign-on capabilities

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
answer is valid.

QUESTION 4
An administrator needs to renew a certificate for a web server. Which of the following should be submitted to a CA?

A. CSR
B. Recovery agent
C. Private key
D. CRL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
An administrator needs to submit a new CSR to a CA. Which of the following is a valid FIRST step?

A. Generate a new private key based on AES.
B. Generate a new public key based on RSA.
C. Generate a new public key based on AES.

D. Generate a new private key based on RSA.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
The security team would like to gather intelligence about the types of attacks being launched against the organization. Which of the following would provide them with the MOST information?

A. Implement a honeynet
B. Perform a penetration test
C. Examine firewall logs
D. Deploy an IDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
After recovering from a data breach in which customer data was lost, the legal team meets with the Chief Security Officer (CSO) to discuss ways to better protect the privacy of customer data.

Which of the following controls support this goal?

A. Contingency planning
B. Encryption and stronger access control
C. Hashing and non-repudiation
D. Redundancy and fault tolerance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
A security engineer, Joe, has been asked to create a secure connection between his mail server and the mail server of a business partner. Which of the following protocol would be MOST appropriate?

A. HTTPS
B. SSH
C. FTP
D. TLS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
A new network administrator is setting up a new file server for the company. Which of the following would be the BEST way to manage folder security?

A. Assign users manually and perform regular user access reviews
B. Allow read only access to all folders and require users to request permission
C. Assign data owners to each folder and allow them to add individual users to each folder
D. Create security groups for each folder and assign appropriate users to each group

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
A recent vulnerability scan found that Telnet is enabled on all network devices. Which of the following protocols should be used instead of Telnet?

A. SCP

B. SSH
C. SFTP
D. SSL

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
A network engineer is setting up a network for a company. There is a BYOD policy for the employees so that they can connect their laptops and mobile devices.

Which of the following technologies should be employed to separate the administrative network from the network in which all of the employees' devices are connected?

A. VPN

B. VLAN
C. WPA2
D. MAC filtering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
A network administrator is asked to send a large file containing PII to a business associate.

Which of the following protocols is the BEST choice to use?

A. SSH
B. SFTP
C. SMTP

D. FTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
When performing the daily review of the system vulnerability scans of the network Joe, the administrator, noticed several security related vulnerabilities with an assigned vulnerability identification number. Joe researches the assigned vulnerability identification number from the vendor website. Joe proceeds with applying the recommended solution for identified vulnerability.

Which of the following is the type of vulnerability described?

A. Network based
B. IDS
C. Signature based
D. Host based

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
A malicious individual is attempting to write too much data to an application's memory. Which of the following describes this type of attack?

A. Zero-day
B. SQL injection
C. Buffer overflow
D. XSRF

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
Ann, a security administrator, wishes to replace their RADIUS authentication with a more secure protocol, which can utilize EAP. Which of the following would BEST fit her objective?

A. CHAP
B. SAML
C. Kerberos
D. Diameter

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
Ann, a security administrator, has concerns regarding her company's wireless network. The network is open and available for visiting prospective clients in the conference room, but she notices that many more devices are connecting to the network than should be.

Which of the following would BEST alleviate Ann's concerns with minimum disturbance of current functionality for clients?

A. Enable MAC filtering on the wireless access point.
B. Configure WPA2 encryption on the wireless access point.
C. Lower the antenna's broadcasting power.
D. Disable SSID broadcasting.
Real 63
CompTIA SY0-401 Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
A distributed denial of service attack can BEST be described as:

A. Invalid characters being entered into a field in a database application.
B. Users attempting to input random or invalid data into fields within a web browser application.
C. Multiple computers attacking a single target in an organized attempt to deplete its resources.
D. Multiple attackers attempting to gain elevated privileges on a target system.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
Joe analyzed the following log and determined the security team should implement which of the following as a mitigation method against further attempts?

```
Host 192.168.1.123

[00: 00: 01]Successful Login: 015 192.168.1.123 : local

[00: 00: 03]Unsuccessful Login: 022 214.34.56.006 : RDP 192.168.1.124

[00: 00: 04]UnSuccessful Login: 010 214.34.56.006 : RDP 192.168.1.124

[00: 00: 07]UnSuccessful Login: 007 214.34.56.006 : RDP 192.168.1.124

[00: 00: 08]UnSuccessful Login: 003 214.34.56.006 : RDP 192.168.1.124
```

A. Reporting
B. IDS
C. Monitor system logs
D. Hardening

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

answer is modified.

QUESTION 19
A computer supply company is located in a building with three wireless networks. The system security team implemented a quarterly security scan and saw the following.

SSID State Channel Level

Computer AreUs1 connected 1 70dbm

Computer AreUs2 connected 5 80dbm

Computer AreUs3 connected 3 75dbm

Computer AreUs4 connected 6 95dbm

Which of the following is this an example of?

A. Rogue access point
B. Near field communication
C. Jamming
D. Packet sniffing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
A systems administrator has implemented PKI on a classified government network. In the event that a disconnect occurs from the primary CA, which of the following should be accessible locally from every site to ensure users with bad certificates cannot gain access to the network?

A. A CRL
B. Make the RA available
C. A verification authority
D. A redundant CA

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
Real 65
CompTIA SY0-401 Exam
While configuring a new access layer switch, the administrator, Joe, was advised that he needed to make sure that only devices authorized to access the network would be permitted to login and utilize resources. Which of the following should the administrator implement to ensure this happens?

A. Log Analysis
B. VLAN Management
C. Network separation
D. 802.1x

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
A vulnerability assessment indicates that a router can be accessed from default port 80 and default port 22. Which of the following should be executed on the router to prevent access via these ports? (Select TWO).

A. FTP service should be disabled
B. HTTPS service should be disabled
C. SSH service should be disabled
D. HTTP service should disabled
E. Telnet service should be disabled

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 23
Results from a vulnerability analysis indicate that all enabled virtual terminals on a router can be accessed using the same password. The company's network device security policy mandates that at least one virtual terminal have a different password than the other virtual terminals. Which of the following sets of commands would meet this requirement?

A. line vty 0 6 P@s5W0Rd password line vty 7 Qwer++!Y password
B. line console 0 password password line vty 0 4 password P@s5W0Rd
C. line vty 0 3 password Qwer++!Y line vty 4 password P@s5W0Rd
D. line vty 0 3 password Qwer++!Y line console 0 password P@s5W0Rd Real 66
CompTIA SY0-401 Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
Joe, an employee, was escorted from the company premises due to suspicion of revealing trade secrets to a competitor. Joe had already been working for two hours before leaving the premises.

A security technician was asked to prepare a report of files that had changed since last night's integrity scan.

Which of the following could the technician use to prepare the report? (Select TWO).

A. PGP
B. MD5
C. ECC
D. AES
E. Blowfish
F. HMAC

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
Ann has read and write access to an employee database, while Joe has only read access. Ann is leaving for a conference.

Which of the following types of authorization could be utilized to trigger write access for Joe when Ann is absent?

A. Mandatory access control
B. Role-based access control
C. Discretionary access control
D. Rule-based access control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Human Resources suspects an employee is accessing the employee salary database. The administrator is asked to find out who it is. In order to complete this task, which of the following is a security control that should be in place?

A. Shared accounts should be prohibited.
B. Account lockout should be enabled
C. Privileges should be assigned to groups rather than individuals
D. Time of day restrictions should be in use

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
An administrator finds that non-production servers are being frequently compromised, production servers are rebooting at unplanned times and kernel versions are several releases behind the version with all current security fixes.

Which of the following should the administrator implement?

A. Snapshots
B. Sandboxing
C. Patch management
D. Intrusion detection system

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
An auditor's report discovered several accounts with no activity for over 60 days. The accounts were later identified as contractors' accounts who would be returning in three months and would need to resume the activities. Which of the following would mitigate and secure the auditors finding?

A. Disable unnecessary contractor accounts and inform the auditor of the update.

B. Reset contractor accounts and inform the auditor of the update.
C. Inform the auditor that the accounts belong to the contractors.
D. Delete contractor accounts and inform the auditor of the update.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
Ann, the security administrator, wishes to implement multifactor security. Which of the following should be implemented in order to compliment password usage and smart cards?

A. Hard tokens
B. Fingerprint readers
C. Swipe badge readers

D. Passphrases

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Customers' credit card information was stolen from a popular video streaming company. A security consultant determined that the information was stolen, while in transit, from the gaming consoles of a particular vendor. Which of the following methods should the company consider to secure this data in the future?

A. Application firewalls
B. Manual updates
C. Firmware version control
D. Encrypted TCP wrappers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
A new intern was assigned to the system engineering department, which consists of the system architect and system software developer's teams. These two teams have separate privileges. The intern requires privileges to view the system architectural drawings and comment on some software development projects. Which of the following methods should the system administrator implement?

A. Group based privileges
B. Generic account prohibition
C. User access review
D. Credential management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
One of the system administrators at a company is assigned to maintain a secure computer lab. The administrator has rights to configure machines, install software, and perform user account maintenance. However, the administrator cannot add new computers to the domain, because that requires authorization from the Information Assurance Officer. This is an example of which of the following?

A. Mandatory access
B. Rule-based access control
C. Least privilege
D. Job rotation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 33
A small business needs to incorporate fault tolerance into their infrastructure to increase data availability. Which of the following options would be the BEST solution at a minimal cost?

A. Clustering
B. Mirrored server
C. RAID
D. Tape backup

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
A new application needs to be deployed on a virtual server. The virtual server hosts a SQL server that is used by several employees.

Which of the following is the BEST approach for implementation of the new application on the virtual server?

A. Take a snapshot of the virtual server after installing the new application and store the snapshot in a secure location.
B. Generate a baseline report detailing all installed applications on the virtualized server after installing the new application.
C. Take a snapshot of the virtual server before installing the new application and store the snapshot in a secure location.
D. Create an exact copy of the virtual server and store the copy on an external hard drive after installing the new application.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
Ann wants to send a file to Joe using PKI. Which of the following should Ann use in order to sign the file?

A. Joe's public key
B. Joe's private key
C. Ann's public key
D. Ann's private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 36
Which of the following protocols is used to validate whether trust is in place and accurate by returning responses of either "good", "unknown", or "revoked"?

Real 71
CompTIA SY0-401 Exam

A. CRL
B. PKI
C. OCSP
D. RA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
During a recent investigation, an auditor discovered that an engineer's compromised workstation was being used to connect to SCADA systems while the engineer was not logged in. The engineer is responsible for administering the SCADA systems and cannot be blocked from connecting to them. The SCADA systems cannot be modified without vendor approval which requires months of testing.

Which of the following is MOST likely to protect the SCADA systems from misuse?

A. Update anti-virus definitions on SCADA systems
B. Audit accounts on the SCADA systems
C. Install a firewall on the SCADA network
D. Deploy NIPS at the edge of the SCADA network

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 38
A security administrator must implement a network authentication solution which will ensure encryption of user credentials when users enter their username and password to authenticate to the network.

Which of the following should the administrator implement?

A. WPA2 over EAP-TTLS
B. WPA-PSK
C. WPA2 with WPS
D. WEP over EAP-PEAP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Several employees have been printing files that include personally identifiable information of customers. Auditors have raised concerns about the destruction of these hard copies after they are created, and management has decided the best way to address this concern is by preventing these files from being printed.

Which of the following would be the BEST control to implement?

A. File encryption
B. Printer hardening
C. Clean desk policies
D. Data loss prevention

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
The company's sales team plans to work late to provide the Chief Executive Officer (CEO) with a special report of sales before the quarter ends. After working for several hours, the team finds they cannot save or print the reports.

Which of the following controls is preventing them from completing their work?

A. Discretionary access control
B. Role-based access control
C. Time of Day access control
D. Mandatory access control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 41
Real 73
CompTIA SY0-401 Exam
A security engineer is asked by the company's development team to recommend the most secure method for password storage.

Which of the following provide the BEST protection against brute forcing stored passwords? (Select TWO).

A. PBKDF2
B. MD5
C. SHA2
D. Bcrypt
E. AES
F. CHAP

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 42
After entering the following information into a SOHO wireless router, a mobile device's user reports being unable to connect to the network:

PERMIT 0A: D1: FA. B1: 03: 37

DENY 01: 33: 7F: AB: 10: AB

Which of the following is preventing the device from connecting?

A. WPA2-PSK requires a supplicant on the mobile device.
B. Hardware address filtering is blocking the device.
C. TCP/IP Port filtering has been implemented on the SOHO router.
D. IP address filtering has disabled the device from connecting.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
The call center supervisor has reported that many employees have been playing preinstalled games on company computers and this is reducing productivity.

Which of the following would be MOST effective for preventing this behavior?

A. Acceptable use policies
B. Host-based firewalls
C. Content inspection
D. Application whitelisting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 44
When creating a public / private key pair, for which of the following ciphers would a user need to specify the key strength?

A. SHA
B. AES

C. DES
D. RSA

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 45
A company has decided to move large data sets to a cloud provider in order to limit the costs of new infrastructure. Some of the data is sensitive and the Chief Information Officer wants to make sure both parties have a clear understanding of the controls needed to protect the data.

Which of the following types of interoperability agreement is this?

A. ISA
B. MOU
C. SLA
D. BPA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following solutions provides the most flexibility when testing new security controls prior to implementation?

A. Trusted OS
B. Host software baselining
C. OS hardening
D. Virtualization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following authentication services requires the use of a ticket-granting ticket (TGT) server in order to complete the authentication process?

A. TACACS+
B. Secure LDAP
C. RADIUS
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 48
Which of the following BEST describes a protective countermeasure for SQL injection?

A. Eliminating cross-site scripting vulnerabilities
B. Installing an IDS to monitor network traffic
C. Validating user input in web applications
D. Placing a firewall between the Internet and database servers

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
Which of the following MOST interferes with network-based detection techniques?

A. Mime-encoding
B. SSL

C. FTP
D. Anonymous email accounts

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 50
A certificate authority takes which of the following actions in PKI?

A. Signs and verifies all infrastructure messages
B. Issues and signs all private keys
C. Publishes key escrow lists to CRLs
D. Issues and signs all root certificates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 51
Real 103
CompTIA SY0-401 Exam
Use of a smart card to authenticate remote servers remains MOST susceptible to which of the following attacks?

A. Malicious code on the local system
B. Shoulder surfing
C. Brute force certificate cracking
D. Distributed dictionary attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52
Separation of duties is often implemented between developers and administrators in order to separate which of the following?

A. More experienced employees from less experienced employees
B. Changes to program code and the ability to deploy to production
C. Upper level management users from standard development employees
D. The network access layer from the application access layer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 53
A security administrator needs to update the OS on all the switches in the company. Which of the following MUST be done before any actual switch configuration is performed?

A. The request needs to be sent to the incident management team.
B. The request needs to be approved through the incident management process.
C. The request needs to be approved through the change management process.
D. The request needs to be sent to the change management team.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
Real 104
CompTIA SY0-401 Exam
Jane, an individual, has recently been calling various financial offices pretending to be another person to gain financial information. Which of the following attacks is being described?

A. Phishing
B. Tailgating
C. Pharming
D. Vishing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
A user in the company is in charge of various financial roles but needs to prepare for an upcoming audit. They use the same account to access each financial system. Which of the following security controls will MOST likely be implemented within the company?

A. Account lockout policy
B. Account password enforcement
C. Password complexity enabled
D. Separation of duties

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
A CRL is comprised of.

A. Malicious IP addresses.
B. Trusted CA's.
C. Untrusted private keys.
D. Public keys.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 57
Real 105
CompTIA SY0-401 Exam
Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?

A. Logic bomb
B. Worm
C. Trojan
D. Adware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
Which of the following may significantly reduce data loss if multiple drives fail at the same time?

A. Virtualization
B. RAID
C. Load balancing
D. Server clustering

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 59
Which of the following should be considered to mitigate data theft when using CAT5 wiring?

A. CCTV
B. Environmental monitoring
C. Multimode fiber
D. EMI shielding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 60
Real 106
CompTIA SY0-401 Exam
To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

A. Management
B. Administrative
C. Technical
D. Operational

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 61
Pete, a network administrator, is capturing packets on the network and notices that a large amount of the traffic on the LAN is SIP and RTP protocols. Which of the following should he do to segment that traffic from the other traffic?

A. Connect the WAP to a different switch.
B. Create a voice VLAN.
C. Create a DMZ.
D. Set the switch ports to 802.1q mode.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 62
Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO).

A. 10.4.4.125
B. 10.4.4.158
C. 10.4.4.165
D. 10.4.4.189
E. 10.4.4.199

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following algorithms has well documented collisions? (Select TWO).

A. AES
B. MD5
C. SHA

D. SHA-256
E. RSA

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 64
Which of the following is BEST used as a secure replacement for TELNET?

A. HTTPS
B. HMAC
C. GPG
D. SSH

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 65
An email client says a digital signature is invalid and the sender cannot be verified. The recipient is concerned with which of the following concepts?

A. Integrity
B. Availability
C. Confidentiality
D. Remediation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following is an effective way to ensure the BEST temperature for all equipment within a datacenter?

A. Fire suppression
B. Raised floor implementation
C. EMI shielding
D. Hot or cool aisle containment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 67
Which of the following transportation encryption protocols should be used to ensure maximum security between a web browser and a web server?

A. SSLv2
B. SSHv1
C. RSA
D. TLS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 68
Developers currently have access to update production servers without going through an approval process. Which of the following strategies would BEST mitigate this risk?

A. Incident management
B. Clean desk policy
C. Routine audits
D. Change management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
Which of the following is a difference between TFTP and FTP?

A. TFTP is slower than FTP.
B. TFTP is more secure than FTP.
C. TFTP utilizes TCP and FTP uses UDP.
D. TFTP utilizes UDP and FTP uses TCP.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
Matt, an administrator, notices a flood fragmented packet and retransmits from an email server.

After disabling the TCP offload setting on the NIC, Matt sees normal traffic with packets flowing in sequence again. Which of the following utilities was he MOST likely using to view this issue?

A. Spam filter
B. Protocol analyzer
C. Web application firewall
D. Load balancer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 71
Which of the following is characterized by an attacker attempting to map out an organization's staff hierarchy in order to send targeted emails?

A. Whaling
B. Impersonation
C. Privilege escalation
D. Spear phishing
Real 110
CompTIA SY0-401 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
corrected and modified.

QUESTION 72
Which of the following would a security administrator implement in order to discover comprehensive security threats on a network?

A. Design reviews
B. Baseline reporting
C. Vulnerability scan
D. Code review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 73
Which of the following is an example of a false positive?

A. Anti-virus identifies a benign application as malware.
B. A biometric iris scanner rejects an authorized user wearing a new contact lens.

C. A user account is locked out after the user mistypes the password too many times.
D. The IDS does not identify a buffer overflow.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 74
Data execution prevention is a feature in most operating systems intended to protect against which type of attack?

A. Cross-site scripting
B. Buffer overflow
C. Header manipulation
D. SQL injection
Real 111
CompTIA SY0-401 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 75
Use of group accounts should be minimized to ensure which of the following?

A. Password security
B. Regular auditing
C. Baseline management
D. Individual accountability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 76
Privilege creep among long-term employees can be mitigated by which of the following procedures?

A. User permission reviews
B. Mandatory vacations
C. Separation of duties
D. Job function rotation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 77
In which of the following scenarios is PKI LEAST hardened?

A. The CRL is posted to a publicly accessible location.
B. The recorded time offsets are developed with symmetric keys.
C. A malicious CA certificate is loaded on all the clients.
D. All public keys are accessed by an unauthorized user.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Configuring the mode, encryption methods, and security associations are part of which of the following?

A. IPSec
B. Full disk encryption
C. 802.1x

D. PKI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 79
Which of the following assessments would Pete, the security administrator, use to actively test that an application's security controls are in place?

A. Code review
B. Penetration test
C. Protocol analyzer
D. Vulnerability scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 80
A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

A. Confidentiality
B. Availability
C. Succession planning
D. Integrity
Real 113
CompTIA SY0-401 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 81

In the initial stages of an incident response, Matt, the security administrator, was provided the hard drives in QUESTION NO: from the incident manager. Which of the following incident response procedures would he need to perform in order to begin the analysis? (Select TWO).

A. Take hashes
B. Begin the chain of custody paperwork
C. Take screen shots
D. Capture the system image
E. Decompile suspicious files

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 82

Which of the following is used to certify intermediate authorities in a large PKI deployment?

A. Root CA
B. Recovery agent
C. Root user
D. Key escrow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 83

Which of the following components MUST be trusted by all parties in PKI?

A. Key escrow
B. CA
C. Private key
D. Recovery key

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 84
Which of the following should Matt, a security administrator, include when encrypting

smartphones? (Select TWO).

A. Steganography images
B. Internal memory
C. Master boot records
D. Removable memory cards
E. Public keys

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 85
Which of the following is the below pseudo-code an example of?

```
IF VARIABLE (CONTAINS NUMBERS = TRUE) THEN EXIT
```

A. Buffer overflow prevention
B. Input validation
C. CSRF prevention
D. Cross-site scripting prevention

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 86
A system administrator is using a packet sniffer to troubleshoot remote authentication. The administrator detects a device trying to communicate to TCP port 49. Which of the following authentication methods is MOST likely being attempted?

A. RADIUS
B. TACACS+
C. Kerberos
D. LDAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 87
Which of the following can use RC4 for encryption? (Select TWO).

A. CHAP
B. SSL
C. WEP
D. AES
E. 3DES

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 88
Which of the following defines a business goal for system restoration and acceptable data loss?

A. MTTR
B. MTBF
C. RPO
D. Warm site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 89
If Organization A trusts Organization B and Organization B trusts Organization C, then

Organization A trusts Organization C. Which of the following PKI concepts is this describing?

Real 116
CompTIA SY0-401 Exam

A. Transitive trust
B. Public key trust

C. Certificate authority trust
D. Domain level trust

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 90
Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency?

A. Business continuity planning
B. Continuity of operations
C. Business impact analysis
D. Succession planning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 91
Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

A. Recovery agent
B. Certificate authority
C. Trust model
D. Key escrow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 92
Which of the following devices will help prevent a laptop from being removed from a certain location?

Real 117
CompTIA SY0-401 Exam

A. Device encryption
B. Cable locks
C. GPS tracking
D. Remote data wipes

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 93
Which of the following is the MOST secure protocol to transfer files?

A. FTP
B. FTPS
C. SSH
D. TELNET

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 94
Suspicious traffic without a specific signature was detected. Under further investigation, it was determined that these were false indicators. Which of the following security devices needs to be configured to disable future false alarms?

A. Signature based IPS

B. Signature based IDS
C. Application based IPS
D. Anomaly based IDS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 95
A company storing data on a secure server wants to ensure it is legally able to dismiss and prosecute staff who intentionally access the server via Telnet and illegally tamper with customer data. Which of the following administrative controls should be implemented to BEST achieve this?

Real 118
CompTIA SY0-401 Exam

A. Command shell restrictions
B. Restricted interface
C. Warning banners
D. Session output pipe to /dev/null

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 96
Which of the following protocols is used to authenticate the client and server's digital certificate?

A. PEAP
B. DNS
C. TLS
D. ICMP

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 97
Which of the following can be used to mitigate risk if a mobile device is lost?

A. Cable lock
B. Transport encryption
C. Voice encryption
D. Strong passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 98
Which of the following security concepts would Sara, the security administrator, use to mitigate the risk of data loss?

A. Record time offset
Real 119
CompTIA SY0-401 Exam
B. Clean desk policy
C. Cloud computing
D. Routine log review

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 99

Which of the following is an example of multifactor authentication?

A. Credit card and PIN
B. Username and password
C. Password and PIN
D. Fingerprint and retina scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 100
After Matt, a user, enters his username and password at the login screen of a web enabled portal, the following appears on his screen:

`Please only use letters and numbers on these fields'

Which of the following is this an example of?

A. Proper error handling
B. Proper input validation
C. Improper input validation
D. Improper error handling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 101
Real 120
CompTIA SY0-401 Exam
Which of the following should the security administrator implement to limit web traffic based on country of origin? (Select THREE).

A. Spam filter

B. Load balancer
C. Antivirus
D. Proxies
E. Firewall
F. NIDS
G. URL filtering

Correct Answer: DEG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 102
Several bins are located throughout a building for secure disposal of sensitive information.

Which of the following does this prevent?

A. Dumpster diving
B. War driving
C. Tailgating
D. War chalking

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Matt, a developer, recently attended a workshop on a new application. The developer installs the new application on a production system to test the functionality. Which of the following is MOST likely affected?

A. Application design
B. Application security
C. Initial baseline configuration

D. Management of interfaces

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following?

A. Acceptable Use Policy
B. Physical security controls
C. Technical controls
D. Security awareness training

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 105
Mike, a network administrator, has been asked to passively monitor network traffic to the company's sales websites. Which of the following would be BEST suited for this task?

A. HIDS
B. Firewall
C. NIPS
D. Spam filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 106
Mike, a security professional, is tasked with actively verifying the strength of the security controls on a company's live modem pool. Which of the following activities is MOST appropriate?

A. War dialing
B. War chalking
C. War driving
D. Bluesnarfing
Real 122
CompTIA SY0-401 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 107
Users at a company report that a popular news website keeps taking them to a web page with derogatory content. This is an example of which of the following?

A. Evil twin
B. DNS poisoning
C. Vishing
D. Session hijacking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 108
An encrypted message is sent using PKI from Sara, a client, to a customer. Sara claims she never sent the message. Which of the following aspects of PKI BEST ensures the identity of the sender?

A. CRL
B. Non-repudiation
C. Trust models
D. Recovery agents

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 109
Jane, a security administrator, has observed repeated attempts to break into a server. Which of the following is designed to stop an intrusion on a specific server?

A. HIPS
B. NIDS
C. HIDS
D. NIPS
Real 123
CompTIA SY0-401 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 110
Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

A. Create a VLAN without a default gateway.
B. Remove the network from the routing table.
C. Create a virtual switch.
D. Commission a stand-alone switch.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 111
A security administrator implements access controls based on the security classification of the data and need-to-know information. Which of the following BEST describes this level of access control?

A. Implicit deny
B. Role-based Access Control
C. Mandatory Access Controls
D. Least privilege

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 112
A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

A. 20
B. 21

C. 22
D. 23

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 113
Which of the following could cause a browser to display the message below?

"The security certificate presented by this website was issued for a different website's address."

A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAs.
B. The website is using a wildcard certificate issued for the company's domain.
C. HTTPS://127.0.01 was used instead of HTTPS://localhost.
D. The website is using an expired self signed certificate.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 114
A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

A. Availability
B. Integrity
C. Confidentiality
D. Fire suppression

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 115
Which of the following pseudocodes can be used to handle program exceptions?

A. If program detects another instance of itself, then kill program instance.

B. If user enters invalid input, then restart program.
C. If program module crashes, then restart program module.
D. If user's input exceeds buffer length, then truncate the input.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 116
Which of the following technologies uses multiple devices to share work?

A. Switching
B. Load balancing
C. RAID
D. VPN concentrator

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 117
Which of the following protocols uses an asymmetric key to open a session and then establishes a symmetric key for the remainder of the session?

A. SFTP
B. HTTPS
C. TFTP
D. TLS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 118
Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device?

Real 126
CompTIA SY0-401 Exam

A. Man-in-the-middle
B. Bluejacking
C. Bluesnarfing
D. Packet sniffing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 119
Pete, an employee, is terminated from the company and the legal department needs documents from his encrypted hard drive. Which of the following should be used to accomplish this task?

(Select TWO).

A. Private hash
B. Recovery agent
C. Public key
D. Key escrow
E. CRL

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 120
Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems?

A. Incident management
B. Server clustering
C. Change management
D. Forensic analysis

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 121
Which of the following can Pete, a security administrator, use to distribute the processing effort

Real 127
CompTIA SY0-401 Exam
when generating hashes for a password cracking program?

A. RAID
B. Clustering
C. Redundancy
D. Virtualization

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 122
Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?

A. Identify user habits
B. Disconnect system from network
C. Capture system image
D. Interview witnesses

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 123
Jane, an administrator, needs to make sure the wireless network is not accessible from the parking area of their office. Which of the following would BEST help Jane when deploying a new access point?

A. Placement of antenna
B. Disabling the SSID
C. Implementing WPA2
D. Enabling the MAC filtering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 124
Real 128
CompTIA SY0-401 Exam
Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

A. Implement WPA

B. Disable SSID
C. Adjust antenna placement
D. Implement WEP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 125
Which of the following is a management control?

A. Logon banners
B. Written security policy
C. SYN attack prevention
D. Access Control List (ACL)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 126
Which of the following security strategies allows a company to limit damage to internal systems and provides loss control?

A. Restoration and recovery strategies
B. Deterrent strategies
C. Containment strategies
D. Detection strategies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 127
Real 129
CompTIA SY0-401 Exam
In order for Sara, a client, to logon to her desktop computer, she must provide her username, password, and a four digit PIN. Which of the following authentication methods is Sara using?

A. Three factor
B. Single factor
C. Two factor
D. Four factor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 128
Using proximity card readers instead of the traditional key punch doors would help to mitigate:

A. Impersonation
B. Tailgating
C. Dumpster diving
D. Shoulder surfing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
answer is verified.

QUESTION 129
Which of the following application attacks is used to gain access to SEH?

A. Cookie stealing

B. Buffer overflow
C. Directory traversal
D. XML injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 130
Which of the following is an authentication service that uses UDP as a transport medium?

A. TACACS+
B. LDAP
C. Kerberos
D. RADIUS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 131
Which of the following can be used on a smartphone to BEST protect against sensitive data loss if the device is stolen? (Select TWO).

A. Tethering
B. Screen lock PIN
C. Remote wipe
D. Email password
E. GPS tracking
F. Device encryption

Correct Answer: CF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 132
Jane, a security analyst, is reviewing logs from hosts across the Internet which her company uses to gather data on new malware. Which of the following is being implemented by Jane's company?

A. Vulnerability scanner
B. Honeynet
C. Protocol analyzer
D. Port scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 133
Which of the following should Pete, a security manager, implement to reduce the risk of

Real 131
CompTIA SY0-401 Exam
employees working in collusion to embezzle funds from their company?

A. Privacy Policy
B. Least Privilege
C. Acceptable Use
D. Mandatory Vacations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
Which of the following will allow Pete, a security analyst, to trigger a security alert because of a tracking cookie?

A. Network based firewall
B. Anti-spam software
C. Host based firewall
D. Anti-spyware software

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
Which of the following protocols allows for secure transfer of files? (Select TWO).

A. ICMP
B. SNMP
C. SFTP
D. SCP
E. TFTP

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 136
Real 132
CompTIA SY0-401 Exam
Which of the following passwords is the LEAST complex?

A. MyTrain!45
B. Mytr@in!!
C. MyTr@in12
D. MyTr@in#8

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 137
During a penetration test from the Internet, Jane, the system administrator, was able to establish a connection to an internal router, but not successfully log in to it. Which ports and protocols are MOST likely to be open on the firewall? (Select FOUR).

A. 21
B. 22
C. 23
D. 69
E. 3389
F. SSH
G. Terminal services
H. Rlogin
I. Rsync
J. Telnet

Correct Answer: BCFJ
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 138
Which of the following is an application security coding problem?

A. Error and exception handling
B. Patch management
C. Application hardening
D. Application fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
An IT security technician needs to establish host based security for company workstations. Which of the following will BEST meet this requirement?

A. Implement IIS hardening by restricting service accounts.
B. Implement database hardening by applying vendor guidelines.
C. Implement perimeter firewall rules to restrict access.
D. Implement OS hardening by applying GPOs.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 140
Which of the following is the MOST specific plan for various problems that can arise within a system?

A. Business Continuity Plan
B. Continuity of Operation Plan
C. Disaster Recovery Plan
D. IT Contingency Plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 141
Which of the following BEST describes the weakness in WEP encryption?

A. The initialization vector of WEP uses a crack-able RC4 encryption algorithm.
Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived.

B. The WEP key is stored in plain text and split in portions across 224 packets of random data.
Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key.
Real 134
CompTIA SY0-401 Exam

C. The WEP key has a weak MD4 hashing algorithm used.
A simple rainbow table can be used to generate key possibilities due to MD4 collisions.

D. The WEP key is stored with a very small pool of random numbers to make the cipher text.
As the random numbers are often reused it becomes easy to derive the remaining WEP key.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 142
Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years.

Each breach has cost the company $3,000. A third party vendor has offered to repair the security hole in the system for $25,000. The breached system is scheduled to be replaced in five years.

Which of the following should Sara do to address the risk?

A. Accept the risk saving $10,000.
B. Ignore the risk saving $5,000.
C. Mitigate the risk saving $10,000.
D. Transfer the risk saving $5,000.

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
up-to-date.

QUESTION 143
Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches?

A. DIAMETER
B. RADIUS
C. TACACS+
D. Kerberos

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

A. Input validation
B. Network intrusion detection system
C. Anomaly-based HIDS
D. Peer review

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 145
Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection?

A. Sign in and sign out logs

B. Mantrap
C. Video surveillance
D. HVAC

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 146
Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

A. Water base sprinkler system
B. Electrical
C. HVAC
D. Video surveillance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
well explained.

QUESTION 147
Matt, a security consultant, has been tasked with increasing server fault tolerance and has been given no budget to accomplish his task. Which of the following can Matt implement to ensure servers will withstand hardware failure?

A. Hardware load balancing
B. RAID
C. A cold site
D. A host standby

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 148
Which of the following fire suppression systems is MOST likely used in a datacenter?

A. FM-200
B. Dry-pipe
C. Wet-pipe
D. Vacuum

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 149
A security administrator has installed a new KDC for the corporate environment. Which of the following authentication protocols is the security administrator planning to implement across the organization?

A. LDAP
B. RADIUS
C. Kerberos
D. XTACACS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks?

A. Cross-site scripting

B. Buffer overflow

C. Header manipulation

D. Directory traversal

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 151
Jane has recently implemented a new network design at her organization and wishes to passively identify security issues with the new network. Which of the following should Jane perform?

A. Vulnerability assessment

B. Black box testing

C. White box testing

D. Penetration testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 152
A security technician is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks the security technician to explain the access control type found in a firewall. With which of the following should the security technician respond?

A. Rule based access control

B. Role based access control

C. Discretionary access control

D. Mandatory access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 153
Jane, a security administrator, has been tasked with explaining authentication services to the company's management team. The company runs an active directory infrastructure. Which of the following solutions BEST relates to the host authentication protocol within the company's environment?

A. Kerberos
B. Least privilege
C. TACACS+
D. LDAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 154
Pete, the compliance manager, wants to meet regulations. Pete would like certain ports blocked only on all computers that do credit card transactions. Which of the following should Pete implement to BEST achieve this goal?

A. A host-based intrusion prevention system
B. A host-based firewall
C. Antivirus update system
D. A network-based intrusion detection system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 155
Pete, the system administrator, wants to restrict access to advertisements, games, and gambling web sites. Which of the following devices would BEST achieve this goal?

A. Firewall

B. Switch
C. URL content filter
D. Spam filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 156
Pete, the system administrator, wishes to monitor and limit users' access to external websites.

Which of the following would BEST address this?

A. Block all traffic on port 80.
B. Implement NIDS.
C. Use server load balancers.
D. Install a proxy server.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 157
Which of the following provides additional encryption strength by repeating the encryption process with additional keys?

A. AES
B. 3DES
C. TwoFish
D. Blowfish

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 158
Real 180
CompTIA SY0-401 Exam
Which of the following BEST describes part of the PKI process?

A. User1 decrypts data with User2's private key
B. User1 hashes data with User2's public key
C. User1 hashes data with User2's private key
D. User1 encrypts data with User2's public key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 159
Two members of the finance department have access to sensitive information. The company is concerned they may work together to steal information. Which of the following controls could be implemented to discover if they are working together?

A. Least privilege access
B. Separation of duties
C. Mandatory access control
D. Mandatory vacations

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 160
A system administrator attempts to ping a hostname and the response is 2001:4860:0:2001::68.

Which of the following replies has the administrator received?

A. The loopback address
B. The local MAC address
C. IPv4 address
D. IPv6 address

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
Which of the following allows a network administrator to implement an access control policy based on individual user characteristics and NOT on job function?

A. Attributes based
B. Implicit deny
C. Role based
D. Rule based

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 162
Which of the following is a best practice when a mistake is made during a forensics examination?

A. The examiner should verify the tools before, during, and after an examination.
B. The examiner should attempt to hide the mistake during cross-examination.
C. The examiner should document the mistake and workaround the problem.
D. The examiner should disclose the mistake and assess another area of the disc.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 163
Which of the following allows lower level domains to access resources in a separate Public Key Infrastructure?

A. Trust Model
B. Recovery Agent
C. Public Key
D. Private Key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
Which of the following offers the LEAST secure encryption capabilities?

A. TwoFish
B. PAP
C. NTLM
D. CHAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 165
Which of the following network architecture concepts is used to securely isolate at the boundary between networks?

A. VLAN
B. Subnetting
C. DMZ
D. NAT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 166
Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter. The access records are used to identify which staff members accessed the data center in the event of equipment theft. Which of the following MUST be prevented in order for this policy to be effective?

A. Password reuse
B. Phishing
C. Social engineering
D. Tailgating

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 167
Elastic cloud computing environments often reuse the same physical hardware for multiple customers over time as virtual machines are instantiated and deleted. This has important implications for which of the following data security concerns?

A. Hardware integrity
B. Data confidentiality
C. Availability of servers
D. Integrity of data

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 168
When implementing fire suppression controls in a datacenter it is important to:

A. Select a fire suppression system which protects equipment but may harm technicians.
B. Ensure proper placement of sprinkler lines to avoid accidental leakage onto servers.
C. Integrate maintenance procedures to include regularly discharging the system.
D. Use a system with audible alarms to ensure technicians have 20 minutes to evacuate.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 169
Vendors typically ship software applications with security settings disabled by default to ensure a wide range of interoperability with other applications and devices. A security administrator should perform which of the following before deploying new software?

A. Application white listing
B. Network penetration testing
C. Application hardening
D. Input fuzzing testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
A technician is deploying virtual machines for multiple customers on a single physical host to reduce power consumption in a data center. Which of the following should be recommended to isolate the VMs from one another?

A. Implement a virtual firewall
B. Install HIPS on each VM
C. Virtual switches with VLANs
D. Develop a patch management guide

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 171
Mandatory vacations are a security control which can be used to uncover which of the following?

A. Fraud committed by a system administrator
B. Poor password security among users
C. The need for additional security staff
D. Software vulnerabilities in vendor code

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 172
Each server on a subnet is configured to only allow SSH access from the administrator's workstation. Which of the following BEST describes this implementation?

A. Host-based firewalls
B. Network firewalls
C. Network proxy
D. Host intrusion prevention

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 173
During a security assessment, an administrator wishes to see which services are running on a remote server. Which of the following should the administrator use?

A. Port scanner
B. Network sniffer
C. Protocol analyzer
D. Process list

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 174

In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified?

A. Security control frameworks
B. Best practice
C. Access control methodologies
D. Compliance activity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 175
Disabling unnecessary services, restricting administrative access, and enabling auditing controls on a server are forms of which of the following?

A. Application patch management
B. Cross-site scripting prevention
C. Creating a security baseline
D. System hardening
Real 186
CompTIA SY0-401 Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 176
A system administrator has noticed vulnerability on a high impact production server. A recent update was made available by the vendor that addresses the vulnerability but requires a reboot of the system afterwards. Which of the following steps should the system administrator implement to address the vulnerability?

A. Test the update in a lab environment, schedule downtime to install the patch, install the patch and reboot the server and monitor for any changes
B. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the patch, and monitor for any changes
C. Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the update, reboot the server, and monitor for any changes

D. Backup the server, schedule downtime to install the patch, installs the patch and monitor for any changes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 177
Which of the following services are used to support authentication services for several local devices from a central location without the use of tokens?

A. TACACS+
B. Smartcards
C. Biometrics
D. Kerberos

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 178
A network administrator has recently updated their network devices to ensure redundancy is in

place so that:

A. switches can redistribute routes across the network.
B. environmental monitoring can be performed.
C. single points of failure are removed.
D. hot and cold aisles are functioning.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 179
A network administrator recently updated various network devices to ensure redundancy throughout the network. If an interface on any of the Layer 3 devices were to go down, traffic will still pass through another interface and the production environment would be unaffected. This type of configuration represents which of the following concepts?

A. High availability
B. Load balancing
C. Backout contingency plan
D. Clustering

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 180
A system administrator needs to ensure that certain departments have more restrictive controls to their shared folders than other departments. Which of the following security controls would be implemented to restrict those departments?

A. User assigned privileges
B. Password disablement
C. Multiple account creation
D. Group based privileges

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
A network analyst received a number of reports that impersonation was taking place on the network. Session tokens were deployed to mitigate this issue and defend against which of the following attacks?

A. Replay
B. DDoS
C. Smurf
D. Ping of Death

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 182
Which of the following controls would prevent an employee from emailing unencrypted information to their personal email account over the corporate network?

A. DLP
B. CRL
C. TPM
D. HSM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
Which of the following is a measure of biometrics performance which rates the ability of a system to correctly authenticate an authorized user?

A. Failure to capture
B. Type II
C. Mean time to register
D. Template capacity

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 184
A company with a US-based sales force has requested that the VPN system be configured to authenticate the sales team based on their username, password and a client side certificate.

Additionally, the security administrator has restricted the VPN to only allow authentication from the US territory. How many authentication factors are in use by the VPN system?

A. 1
B. 2
C. 3
D. 4

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 185
A software development company wants to implement a digital rights management solution to protect its intellectual property. Which of the following should the company implement to enforce software digital rights?

A. Transport encryption
B. IPsec
C. Non-repudiation
D. Public key infrastructure

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 186
Users are unable to connect to the web server at IP 192.168.0.20. Which of the following can be inferred of a firewall that is configured ONLY with the following ACL?

PERMIT TCP ANY HOST 192.168.0.10 EQ 80

PERMIT TCP ANY HOST 192.168.0.10 EQ 443

Real 190
CompTIA SY0-401 Exam

A. It implements stateful packet filtering.
B. It implements bottom-up processing.
C. It failed closed.
D. It implements an implicit deny.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 187
Which of the following security awareness training is BEST suited for data owners who are concerned with protecting the confidentiality of their data?

A. Social networking use training
B. Personally owned device policy training
C. Tailgating awareness policy training
D. Information classification training

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 188
A security administrator is concerned about the strength of user's passwords. The company does not want to implement a password complexity policy. Which of the

following can the security Administrator implement to mitigate the risk of an online password attack against users with weak passwords?

A. Increase the password length requirements
B. Increase the password history
C. Shorten the password expiration period
D. Decrease the account lockout time

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
answer is well modified.

QUESTION 189
A company has purchased an application that integrates into their enterprise user directory for

account authentication. Users are still prompted to type in their usernames and passwords. Which of the following types of authentication is being utilized here?

A. Separation of duties
B. Least privilege
C. Same sign-on
D. Single sign-on

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 190
Which of the following are Data Loss Prevention (DLP) strategies that address data in transit issues? (Select TWO).

A. Scanning printing of documents.
B. Scanning of outbound IM (Instance Messaging).
C. Scanning copying of documents to USB.

D. Scanning of SharePoint document library.
E. Scanning of shared drives.
F. Scanning of HTTP user traffic.

Correct Answer: BF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 191
A user casually browsing the Internet is redirected to a warez site where a number of pop-ups appear. After clicking on a pop-up to complete a survey, a drive-by download occurs. Which of the following is MOST likely to be contained in the download?

A. Backdoor
B. Spyware
C. Logic bomb
D. DDoS
E. Smurf

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 192
A security administrator plans on replacing a critical business application in five years. Recently, there was a security flaw discovered in the application that will cause the IT department to manually re-enable user accounts each month at a cost of $2,000. Patching the application today would cost $140,000 and take two months to implement. Which of the following should the security administrator do in regards to the application?

A. Avoid the risk to the user base allowing them to re-enable their own accounts
B. Mitigate the risk by patching the application to increase security and saving money
C. Transfer the risk replacing the application now instead of in five years
D. Accept the risk and continue to enable the accounts each month saving money

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 193
The IT department has setup a share point site to be used on the intranet. Security has established the groups and permissions on the site. No one may modify the permissions and all requests for access are centrally managed by the security team. This is an example of which of the following control types?

A. Rule based access control
B. Mandatory access control
C. User assigned privilege
D. Discretionary access control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 194
Purchasing receives a phone call from a vendor asking for a payment over the phone. The phone number displayed on the caller ID matches the vendor's number. When the purchasing agent asks to call the vendor back, they are given a different phone number with a different area code.

Which of the following attack types is this?

A. Hoax
B. Impersonation
C. Spear phishing
D. Whaling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 195
Purchasing receives an automated phone call from a bank asking to input and verify credit card information. The phone number displayed on the caller ID matches the bank. Which of the following attack types is this?

A. Hoax
B. Phishing
C. Vishing
D. Whaling

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 196
The IT department has setup a website with a series of questions to allow end users to reset their own accounts. Which of the following account management practices does this help?

A. Account Disablements
B. Password Expiration
C. Password Complexity
D. Password Recovery

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 197
Real 194
CompTIA SY0-401 Exam
An information bank has been established to store contacts, phone numbers and other records. A UNIX application needs to connect to the index server using port 389. Which of the following authentication services should be used on this port by default?

A. RADIUS
B. Kerberos
C. TACACS+
D. LDAP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 198
An internal auditor is concerned with privilege creep that is associated with transfers inside the company. Which mitigation measure would detect and correct this?

A. User rights reviews
B. Least privilege and job rotation
C. Change management
D. Change Control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 199
Which of the following is the default port for TFTP?

A. 20
B. 69
C. 21
D. 68

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 200
Real 195
CompTIA SY0-401 Exam
Which of the following concepts are included on the three sides of the "security triangle"? (Select THREE).

A. Confidentiality
B. Availability
C. Integrity
D. Authorization
E. Authentication
F. Continuity

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 201
Which of the following concepts allows an organization to group large numbers of servers together in order to deliver a common service?

A. Clustering
B. RAID
C. Backup Redundancy
D. Cold site

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 202

Which of the following security concepts identifies input variables which are then used to perform boundary testing?

A. Application baseline
B. Application hardening
C. Secure coding
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
Users need to exchange a shared secret to begin communicating securely. Which of the following is another name for this symmetric key?

A. Session Key
B. Public Key
C. Private Key
D. Digital Signature

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 204
Which of the following cryptographic related browser settings allows an organization to communicate securely?

A. SSL 3.0/TLS 1.0
B. 3DES
C. Trusted Sites
D. HMAC

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 205
Which of the following is the BEST reason to provide user awareness and training programs for organizational staff?

A. To ensure proper use of social media
B. To reduce organizational IT risk
C. To detail business impact analyses
D. To train staff on zero-days

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
A firewall technician has been instructed to disable all non-secure ports on a corporate firewall. The technician has blocked traffic on port 21, 69, 80, and 137-139. The technician has allowed traffic on ports 22 and 443. Which of the following correctly lists the protocols blocked and allowed?

A. Blocked: TFTP, HTTP, NetBIOS; Allowed: HTTPS, FTP
B. Blocked: FTP, TFTP, HTTP, NetBIOS; Allowed: SFTP, SSH, SCP, HTTPS
C. Blocked: SFTP, TFTP, HTTP, NetBIOS; Allowed: SSH, SCP, HTTPS
D. Blocked: FTP, HTTP, HTTPS; Allowed: SFTP, SSH, SCP, NetBIOS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 207

A security administrator is responsible for performing periodic reviews of user permission settings due to high turnover and internal transfers at a corporation. Which of the following BEST describes the procedure and security rationale for performing such reviews?

A. Review all user permissions and group memberships to ensure only the minimum set of permissions required to perform a job is assigned.
B. Review the permissions of all transferred users to ensure new permissions are granted so the employee can work effectively.
C. Ensure all users have adequate permissions and appropriate group memberships, so the volume of help desk calls is reduced.
D. Ensure former employee accounts have no permissions so that they cannot access any network file stores and resources.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 208
A system administrator is responding to a legal order to turn over all logs from all company servers. The system administrator records the system time of all servers to ensure that:

A. HDD hashes are accurate.
B. the NTP server works properly.
C. chain of custody is preserved.
Real 198
CompTIA SY0-401 Exam
D. time offset can be calculated.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 209
While rarely enforced, mandatory vacation policies are effective at uncovering:

A. Help desk technicians with oversight by multiple supervisors and detailed quality control systems.
B. Collusion between two employees who perform the same business function.
C. Acts of incompetence by a systems engineer designing complex architectures as a member of a team.

D. Acts of gross negligence on the part of system administrators with unfettered access to system and no oversight.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 210
A company hires outside security experts to evaluate the security status of the corporate network. All of the company's IT resources are outdated and prone to crashing. The company requests that all testing be performed in a way which minimizes the risk of system failures. Which of the following types of testing does the company want performed?

A. Penetration testing
B. WAF testing
C. Vulnerability scanning
D. White box testing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 211
A security administrator notices that a specific network administrator is making unauthorized changes to the firewall every Saturday morning. Which of the following would be used to mitigate

this issue so that only security administrators can make changes to the firewall?

A. Mandatory vacations
B. Job rotation
C. Least privilege
D. Time of day restrictions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 212
A security administrator notices large amounts of traffic within the network heading out to an external website. The website seems to be a fake bank site with a phone number that when called, asks for sensitive information. After further investigation, the security administrator notices that a fake link was sent to several users. This is an example of which of the following attacks?

A. Vishing
B. Phishing
C. Whaling
D. SPAM
E. SPIM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 213
After a user performed a war driving attack, the network administrator noticed several similar markings where WiFi was available throughout the enterprise. Which of the following is the term used to describe these markings?

A. IV attack
B. War dialing

C. Rogue access points

D. War chalking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 214
The system administrator notices that their application is no longer able to keep up with the large amounts of traffic their server is receiving daily. Several packets are dropped and sometimes the server is taken offline. Which of the following would be a possible solution to look into to ensure their application remains secure and available?

A. Cloud computing

B. Full disk encryption

C. Data Loss Prevention

D. HSM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 215
After a recent internal audit, the security administrator was tasked to ensure that all credentials must be changed within 90 days, cannot be repeated, and cannot contain any dictionary words or patterns. All credentials will remain enabled regardless of the number of attempts made. Which of the following types of user account options were enforced? (Select TWO).

A. Recovery

B. User assigned privileges

C. Lockout

D. Disablement

E. Group based privileges

F. Password expiration

G. Password complexity

Correct Answer: FG
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 216
A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive's laptop they notice several pictures of the employee's pets are on the hard drive and on a cloud storage network. When the analyst hashes the images on the hard drive against the hashes on the cloud network they do not match.

Real 201
CompTIA SY0-401 Exam
Which of the following describes how the employee is leaking these secrets?

A. Social engineering
B. Steganography
C. Hashing
D. Digital signatures

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 217
During a routine audit a web server is flagged for allowing the use of weak ciphers. Which of the following should be disabled to mitigate this risk? (Select TWO).

A. SSL 1.0
B. RC4
C. SSL 3.0
D. AES
E. DES
F. TLS 1.0

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 218
Review the following diagram depicting communication between PC1 and PC2 on each side of a router. Analyze the network traffic logs which show communication between the two computers as captured by the computer with IP 10.2.2.10.

DIAGRAM

PC1 PC2

[192.168.1.30]--------[INSIDE 192.168.1.1 router OUTSIDE 10.2.2.1]-----

----[10.2.2.10] LOGS

10:30:22, SRC 10.2.2.1:3030, DST 10.2.2.10:80, SYN

10:30:23, SRC 10.2.2.10:80, DST 10.2.2.1:3030, SYN/ACK

10:30:24, SRC 10.2.2.1:3030, DST 10.2.2.10:80, ACK

Given the above information, which of the following can be inferred about the above environment?

A. 192.168.1.30 is a web server.
B. The web server listens on a non-standard port.
C. The router filters port 80 traffic.
D. The router implements NAT.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 219

The Chief Information Officer (CIO) wants to implement a redundant server location to which the production server images can be moved within 48 hours and services can be quickly restored, in case of a catastrophic failure of the primary datacenter's HVAC. Which of the following can be implemented?

A. Cold site
B. Load balancing
C. Warm site
D. Hot site

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 220
The security administrator is observing unusual network behavior from a workstation. The workstation is communicating with a known malicious destination over an encrypted tunnel. A full antivirus scan, with an updated antivirus definition file, does not show any signs of infection.

Which of the following has happened on the workstation?

A. Zero-day attack
B. Known malware infection
C. Session hijacking
D. Cookie stealing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 221
Which of the following controls can be used to prevent the disclosure of sensitive information stored on a mobile device's removable media in the event that the device is lost or stolen?

A. Hashing
B. Screen locks

C. Device password
D. Encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 222
Which of the following should be performed to increase the availability of IP telephony by prioritizing traffic?

A. Subnetting
B. NAT
C. Quality of service
D. NAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 223
A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

A. ICMP
B. BGP
C. NetBIOS
D. DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
A victim is logged onto a popular home router forum site in order to troubleshoot some router configuration issues. The router is a fairly standard configuration and has an IP address of

192.168.1.1. The victim is logged into their router administrative interface in one tab and clicks a forum link in another tab. Due to clicking the forum link, the home router reboots. Which of the following attacks MOST likely occurred?

A. Brute force password attack
B. Cross-site request forgery
C. Cross-site scripting
D. Fuzzing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 225
Which of the following assets is MOST likely considered for DLP?

A. Application server content
B. USB mass storage devices
C. Reverse proxy
D. Print server

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 226
In order to securely communicate using PGP, the sender of an email must do which of the following when sending an email to a recipient for the first time?

A. Import the recipient's public key
B. Import the recipient's private key
C. Export the sender's private key
D. Export the sender's public key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 227
A hacker has discovered a simple way to disrupt business for the day in a small company which relies on staff working remotely. In a matter of minutes the hacker was able to deny remotely working staff access to company systems with a script. Which of the following security controls is the hacker exploiting?

A. DoS
B. Account lockout
C. Password recovery
D. Password complexity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228
A security specialist has been asked to evaluate a corporate network by performing a vulnerability assessment. Which of the following will MOST likely be performed?

A. Identify vulnerabilities, check applicability of vulnerabilities by passively testing security controls.
B. Verify vulnerabilities exist, bypass security controls and exploit the vulnerabilities.
C. Exploit security controls to determine vulnerabilities and mis-configurations.
D. Bypass security controls and identify applicability of vulnerabilities by passively testing security controls.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
answer is verified.

QUESTION 229
A security technician is attempting to access a wireless network protected with WEP. The technician does not know any information about the network. Which of the following should the technician do to gather information about the configuration of the wireless network?

A. Spoof the MAC address of an observed wireless network client
B. Ping the access point to discover the SSID of the network
C. Perform a dictionary attack on the access point to enumerate the WEP key
D. Capture client to access point disassociation packets to replay on the local PC's loopback

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 230
After an assessment, auditors recommended that an application hosting company should contract with additional data providers for redundant high speed Internet connections. Which of the following is MOST likely the reason for this recommendation? (Select TWO).

A. To allow load balancing for cloud support
B. To allow for business continuity if one provider goes out of business
C. To eliminate a single point of failure
D. To allow for a hot site in case of disaster
E. To improve intranet communication speeds

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 231
A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks.

Which of the following is MOST likely the reason for the sub-interfaces?

A. The network uses the subnet of 255.255.255.128.
B. The switch has several VLANs configured on it.
C. The sub-interfaces are configured for VoIP traffic.
D. The sub-interfaces each implement quality of service.
Real 207
CompTIA SY0-401 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 232
Which of the following should be enabled in a laptop's BIOS prior to full disk encryption?

A. USB
B. HSM
C. RAID
D. TPM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 233
Company employees are required to have workstation client certificates to access a bank website. These certificates were backed up as a precautionary step before the new computer upgrade. After the upgrade and restoration, users state they can access the bank's website, but not login.
Which is the following is MOST likely the issue?

A. The IP addresses of the clients have change

B. The client certificate passwords have expired on the server

C. The certificates have not been installed on the workstations

D. The certificates have been installed on the CA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 234
Digital Signatures provide which of the following?

A. Confidentiality

B. Authorization

C. Integrity

D. Authentication

E. Availability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 235
A user ID and password together provide which of the following?

A. Authorization

B. Auditing

C. Authentication

D. Identification

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 236
RADIUS provides which of the following?

A. Authentication, Authorization, Availability
B. Authentication, Authorization, Auditing
C. Authentication, Accounting, Auditing
D. Authentication, Authorization, Accounting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 237
A recent intrusion has resulted in the need to perform incident response procedures. The incident response team has identified audit logs throughout the network and organizational systems which hold details of the security breach. Prior to this incident, a security consultant informed the company that they needed to implement an NTP server on the network. Which of the following is a problem that the incident response team will likely encounter during their assessment?

A. Chain of custody

B. Tracking man hours
C. Record time offset
D. Capture video traffic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 238
In order for network monitoring to work properly, you need a PC and a network card running in what mode?

A. Launch
B. Exposed
C. Promiscuous
D. Sweep

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 239
Which of the following utilities can be used in Linux to view a list of users' failed authentication attempts?

A. badlog
B. faillog
C. wronglog
D. killlog

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 240
A periodic update that corrects problems in one version of a product is called a

A. Hotfix

B. Overhaul

C. Service pack

D. Security update

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 241
A user has received an email from an external source which asks for details on the company's new product line set for release in one month. The user has a detailed spec sheet but it is marked "Internal Proprietary Information". Which of the following should the user do NEXT?

A. Contact their manager and request guidance on how to best move forward

B. Contact the help desk and/or incident response team to determine next steps

C. Provide the requestor with the email information since it will be released soon anyway

D. Reply back to the requestor to gain their contact information and call them

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 242
Which of the following techniques enables a highly secured organization to assess security weaknesses in real time?

A. Access control lists

B. Continuous monitoring

C. Video surveillance

D. Baseline reporting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 243
Which of the following techniques can be used to prevent the disclosure of system information resulting from arbitrary inputs when implemented properly?

A. Fuzzing
B. Patch management
C. Error handling
D. Strong passwords

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 244
Encryption of data at rest is important for sensitive information because of which of the following?

A. Facilitates tier 2 support, by preventing users from changing the OS
B. Renders the recovery of data harder in the event of user password loss
C. Allows the remote removal of data following eDiscovery requests
D. Prevents data from being accessed following theft of physical equipment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 245
Which of the following is synonymous with a server's certificate?

A. Public key

B. CRL
C. Private key
D. Recovery agent

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 246
A network administrator noticed various chain messages have been received by the company.

Which of the following security controls would need to be implemented to mitigate this issue?

A. Anti-spam
B. Antivirus
C. Host-based firewalls
D. Anti-spyware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 247
Which of the following types of application attacks would be used to specifically gain unauthorized information from databases that did not have any input validation implemented?

A. SQL injection
B. Session hijacking and XML injection
C. Cookies and attachments
D. Buffer overflow and XSS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 248
Which of the following should be deployed to prevent the transmission of malicious traffic between virtual machines hosted on a singular physical device on a network?

A. HIPS on each virtual machine
B. NIPS on the network
C. NIDS on the network
D. HIDS on each virtual machine

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 249
A security administrator wants to get a real time look at what attackers are doing in the wild, hoping to lower the risk of zero-day attacks. Which of the following should be used to accomplish this goal?

Real 213
CompTIA SY0-401 Exam

A. Penetration testing
B. Honeynets
C. Vulnerability scanning
D. Baseline reporting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 250
Which of the following protocols is the security administrator observing in this packet capture?

12:33:43, SRC 192.168.4.3:3389, DST 10.67.33.20:8080, SYN/ACK

A. HTTPS
B. RDP
C. HTTP
D. SFTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 251
Which of the following is true about asymmetric encryption?

A. A message encrypted with the private key can be decrypted by the same key
B. A message encrypted with the public key can be decrypted with a shared key.
C. A message encrypted with a shared key, can be decrypted by the same key.
D. A message encrypted with the public key can be decrypted with the private key.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 252
Which of the following is true about an email that was signed by User A and sent to User B?

Real 214

A. User A signed with User B's private key and User B verified with their own public key.
B. User A signed with their own private key and User B verified with User A's public key.
C. User A signed with User B's public key and User B verified with their own private key.
D. User A signed with their own public key and User B verified with User A's private key.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 253
The Chief Information Officer (CIO) is concerned with moving an application to a SaaS cloud provider. Which of the following can be implemented to provide for data confidentiality assurance during and after the migration to the cloud?

A. HPM technology
B. Full disk encryption
C. DLP policy
D. TPM technology

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 254
Which of the following protocols encapsulates an IP packet with an additional IP header?

A. SFTP
B. IPSec
C. HTTPS
D. SSL

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 255
A program has been discovered that infects a critical Windows system executable and stays dormant in memory. When a Windows mobile phone is connected to the host, the program infects the phone's boot loader and continues to target additional Windows PCs or phones. Which of the

following malware categories BEST describes this program?

A. Zero-day
B. Trojan
C. Virus
D. Rootkit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 256
A user has unknowingly gone to a fraudulent site. The security analyst notices the following system change on the user's host:

Old `hosts' file:

127.0.0.1 localhost

New `hosts' file:

127.0.0.1 localhost

5.5.5.5 www.comptia.com

Which of the following attacks has taken place?

A. Spear phishing
B. Pharming
C. Phishing
D. Vishing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 257
An investigator recently discovered that an attacker placed a remotely accessible CCTV camera in a public area overlooking several Automatic Teller Machines (ATMs). It is also believed that user accounts belonging to ATM operators may have been compromised. Which of the following attacks has MOST likely taken place?

Real 216
CompTIA SY0-401 Exam

A. Shoulder surfing
B. Dumpster diving
C. Whaling attack
D. Vishing attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 258
A user commuting to work via public transport received an offensive image on their smart phone from another commuter. Which of the following attacks MOST likely took place?

A. War chalking
B. Bluejacking
C. War driving

D. Bluesnarfing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 259
An attacker attempted to compromise a web form by inserting the following input into the username field: admin)(|(password=*))

Which of the following types of attacks was attempted?

A. SQL injection
B. Cross-site scripting
C. Command injection
D. LDAP injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

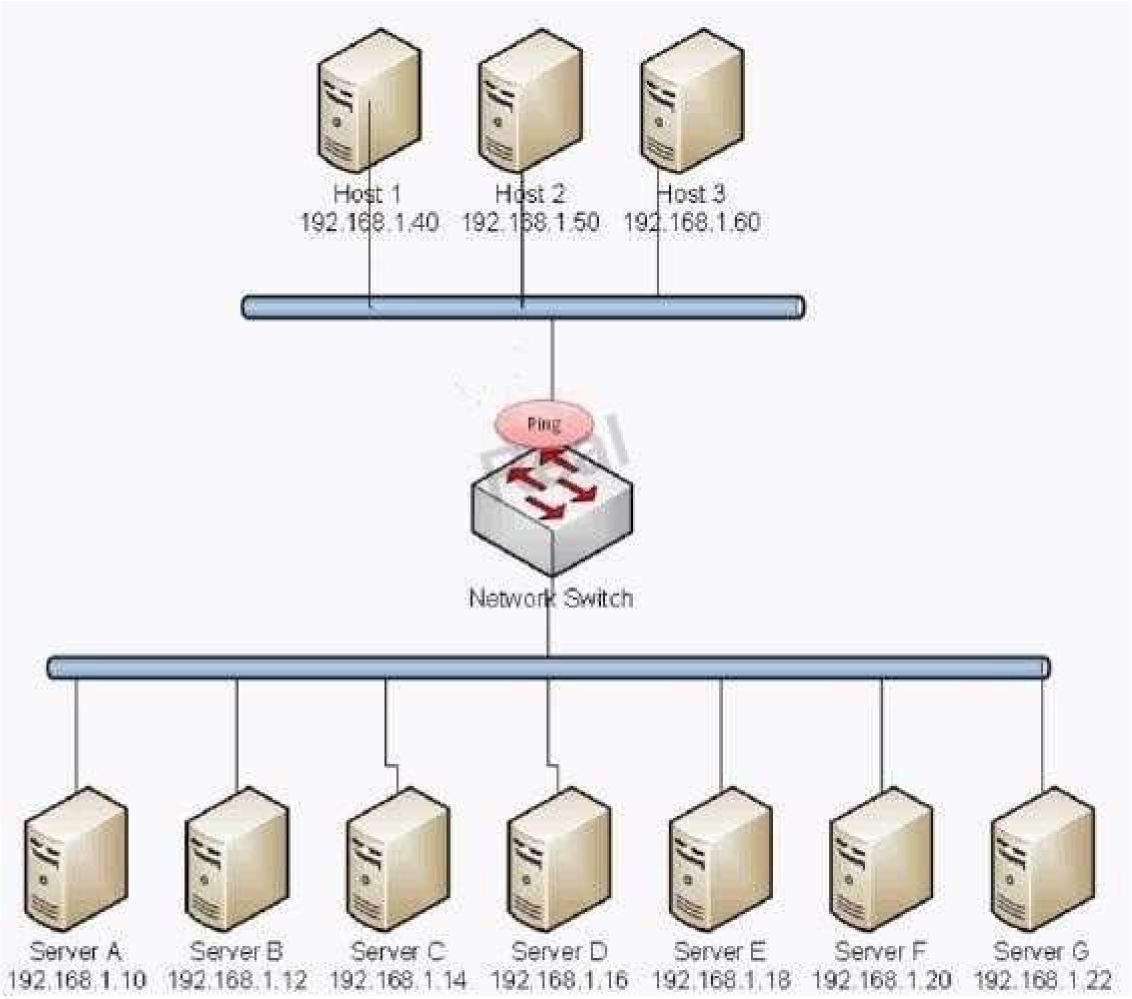
QUESTION 260
Real 217
CompTIA SY0-401 Exam
Which of the following is BEST carried out immediately after a security breach is discovered?

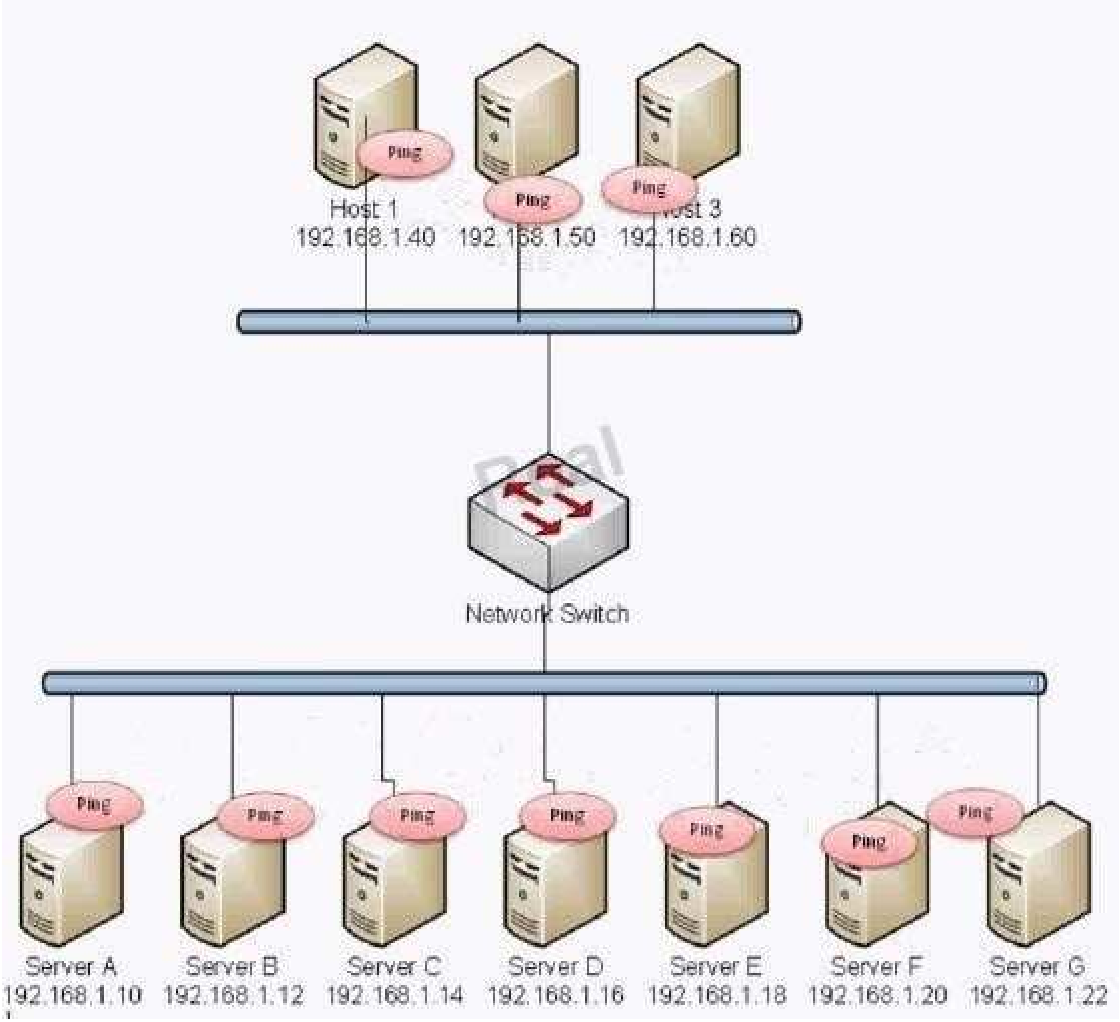
A. Risk transference
B. Access control revalidation
C. Change management
D. Incident management

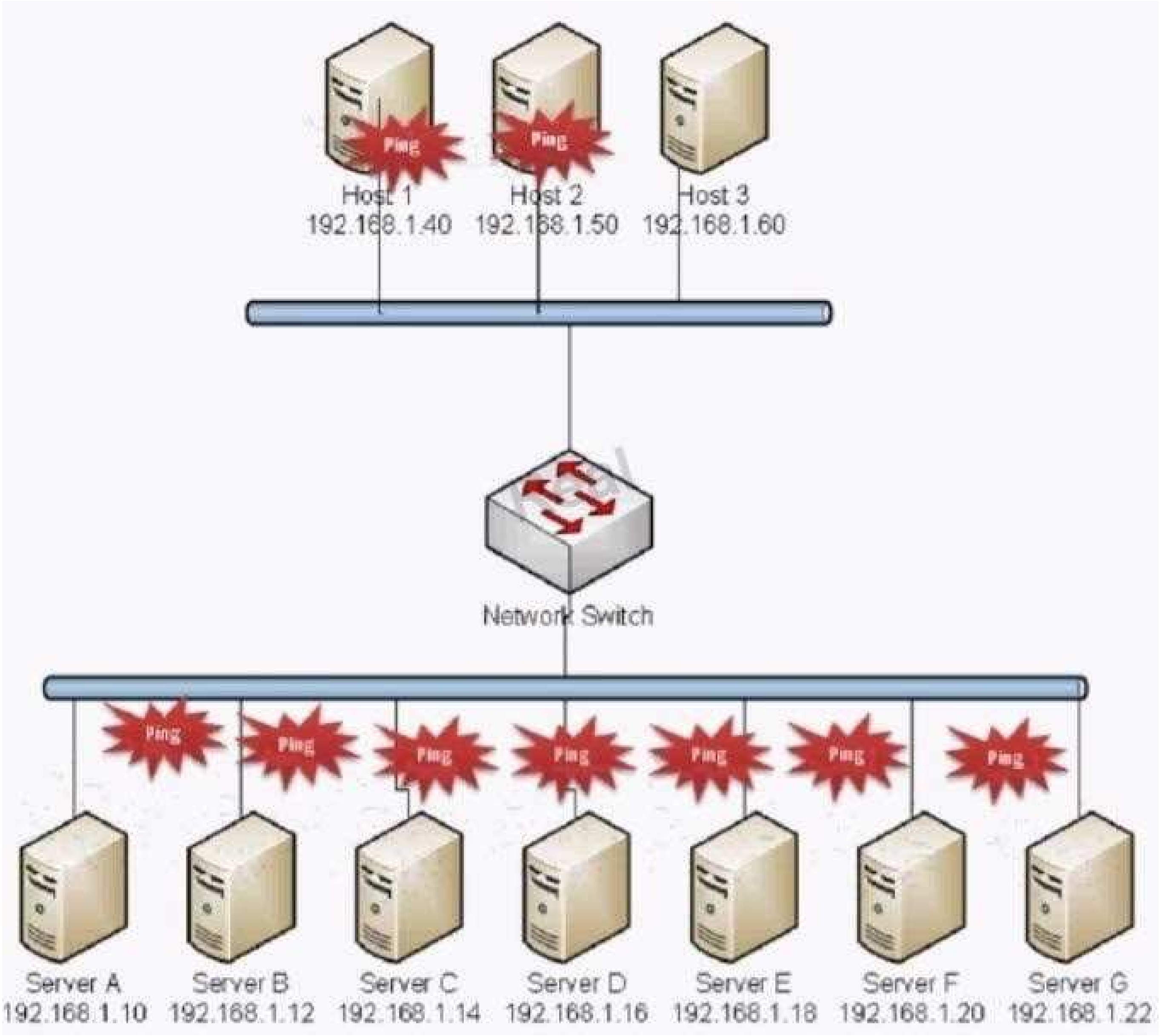
Correct Answer: D
Section: (none)
Explanation

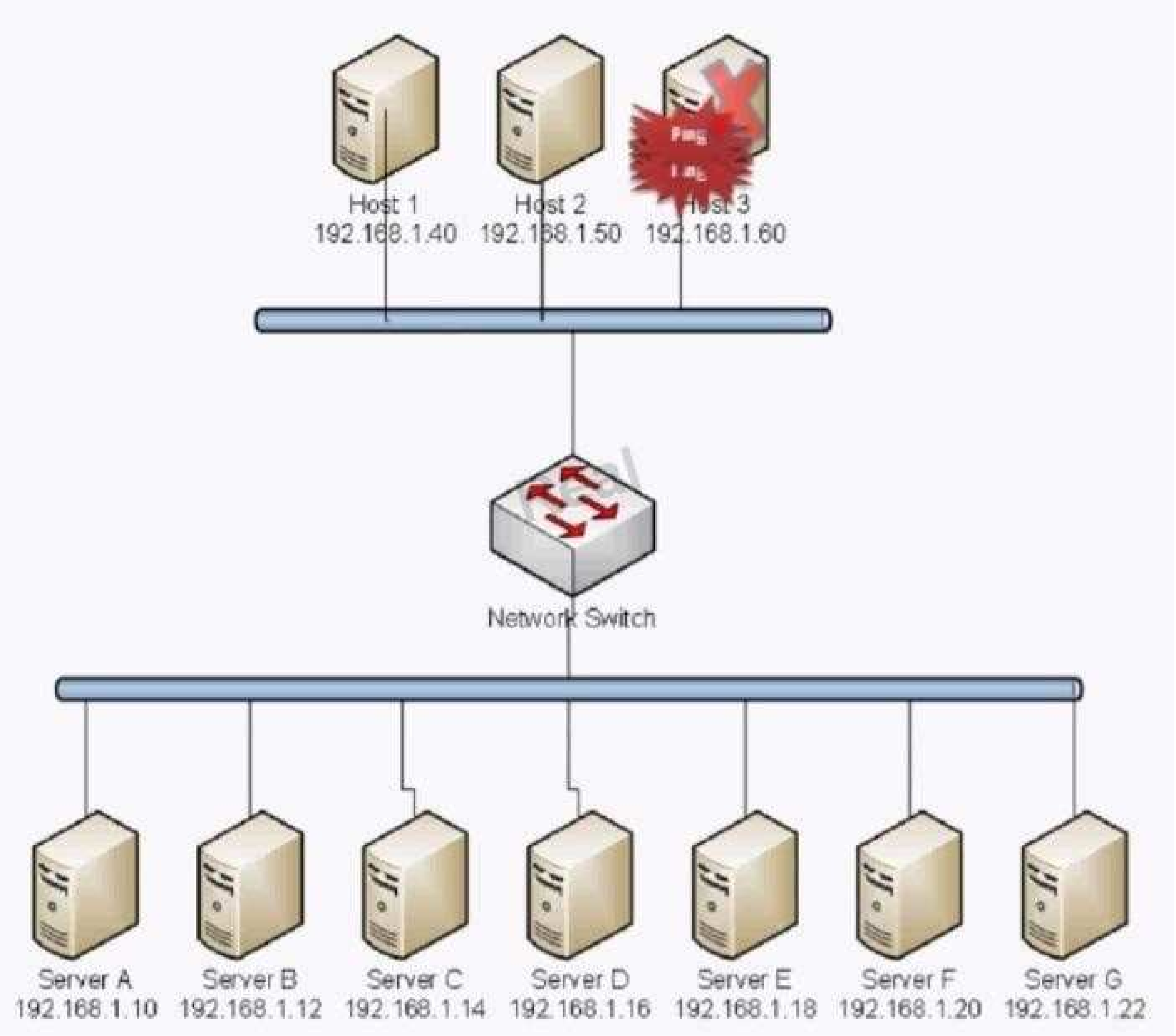
Explanation/Reference:
Explanation:

QUESTION 261
Which of the following BEST describes the type of attack that is occurring?




Ping
Ping
Ping
Host 1
192.168.1.40
192.168.1.50
Host 3
192.168.1.60
Network Switch
Ping
Ping
Ping
Ping
Ping
Ping
Ping
Server A
192.168.1.10
Server B
192.168.1.12
Server C
192.168.1.14
Server D
192.168.1.16
Server E
192.168.1.18
Server F
192.168.1.20
Server G
192.168.1.22


Ping
Ping
Host 1
192.168.1.40
Host 2
192.168.1.50
Host 3
192.168.1.60
Network Switch
Ping
Ping
Ping
Ping
Ping
Ping
Ping
Server A
192.168.1.10
Server B
192.168.1.12
Server C
192.168.1.14
Server D
192.168.1.16
Server E
192.168.1.18
Server F
192.168.1.20
Server G
192.168.1.22


Host 1
192.168.1.40
Host 2
192.168.1.50
Host 3
192.168.1.60
Network Switch
Server A
192.168.1.10
Server B
192.168.1.12
Server C
192.168.1.14
Server D
192.168.1.16
Server E
192.168.1.18
Server F
192.168.1.20
Server G
192.168.1.22

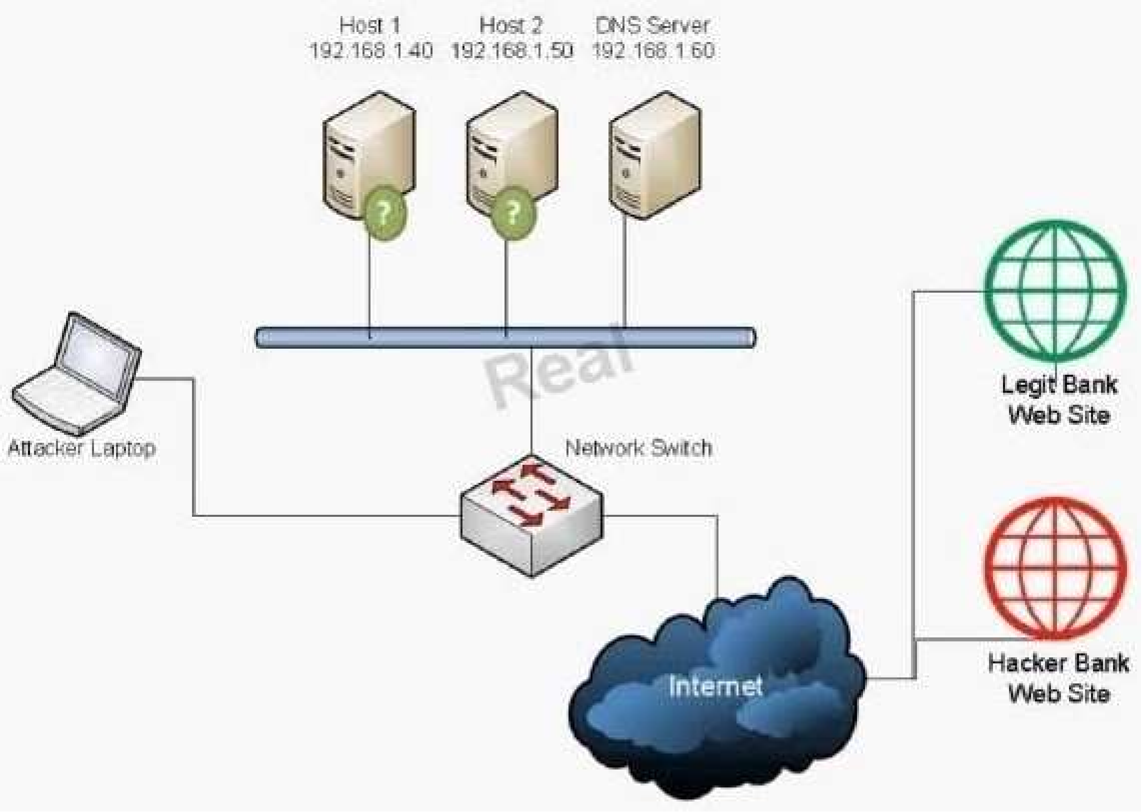
A. Smurf Attack
B. Man in the middle
C. Backdoor
D. Replay
E. Spear Phishing
F. Xmas Attack
G. Blue Jacking
H. Ping of Death

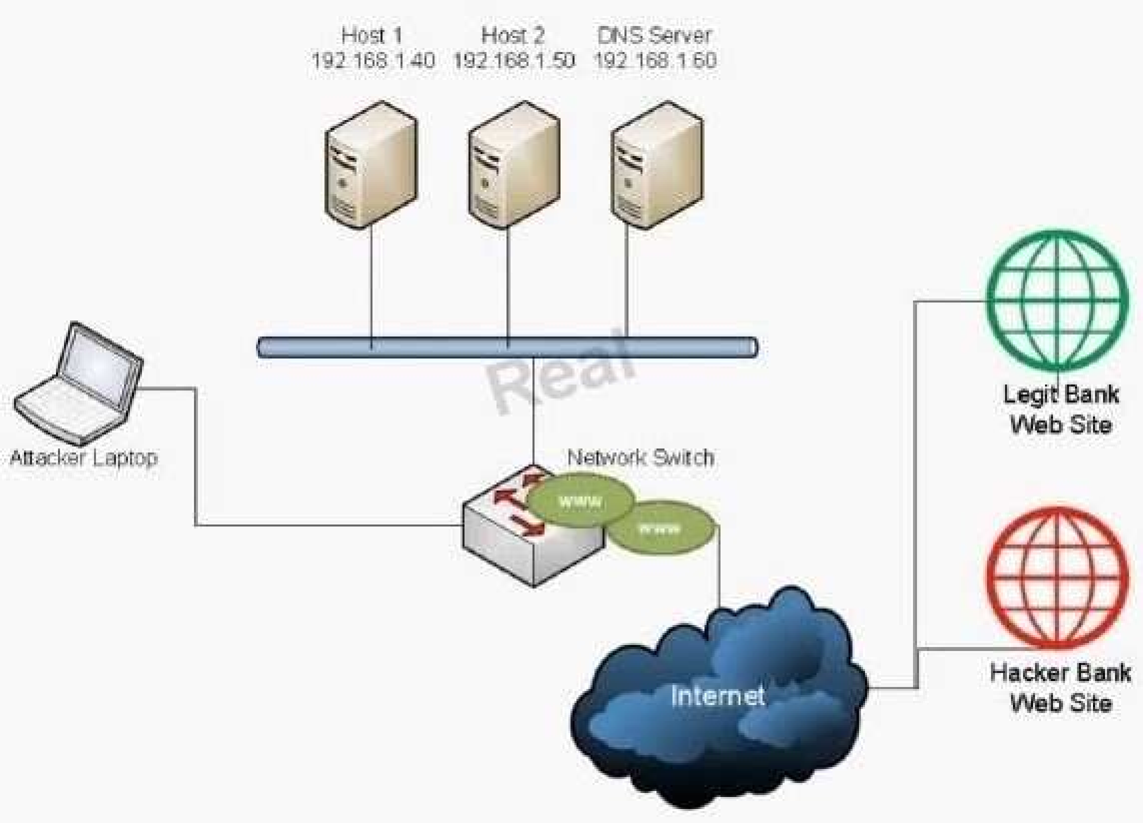
Correct Answer: A
Section: (none)
Explanation

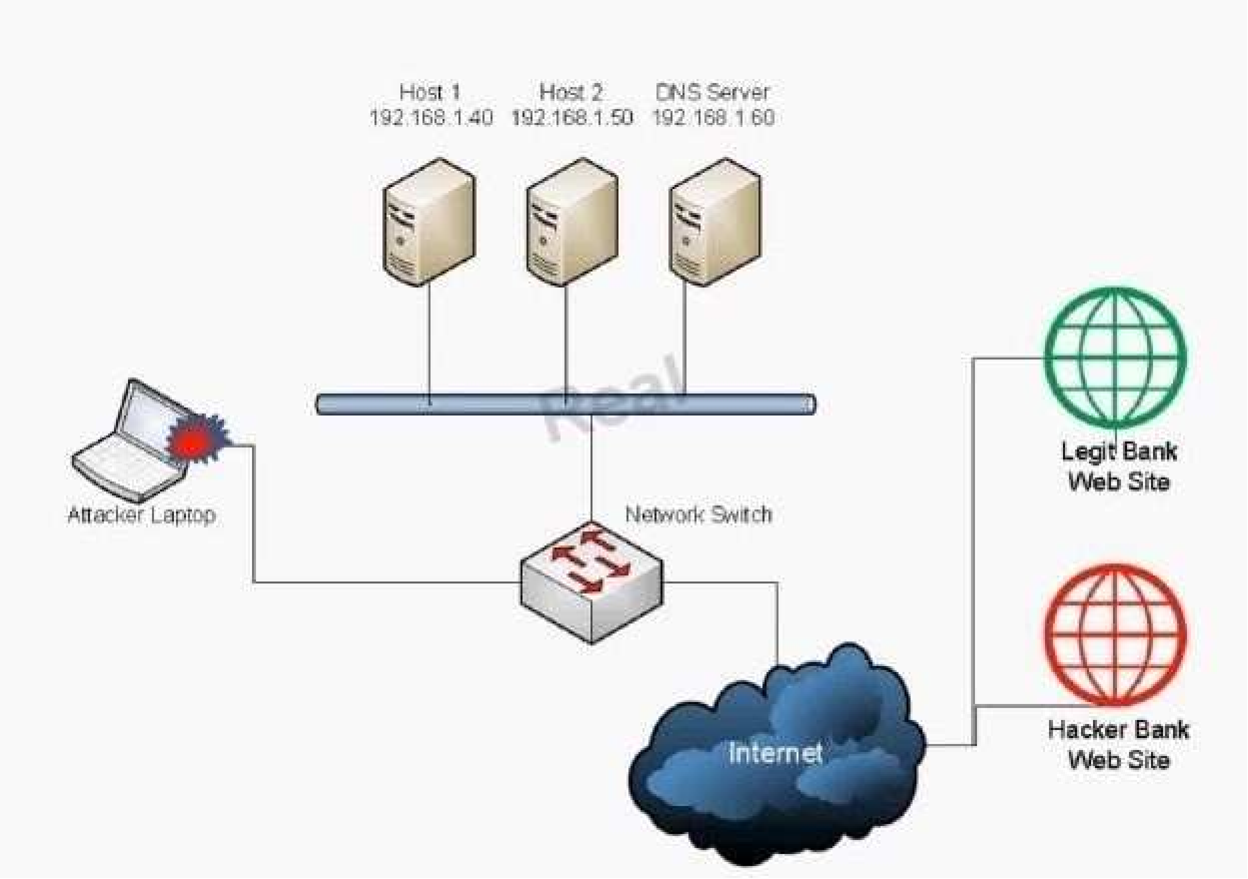
Explanation/Reference:
Explanation:

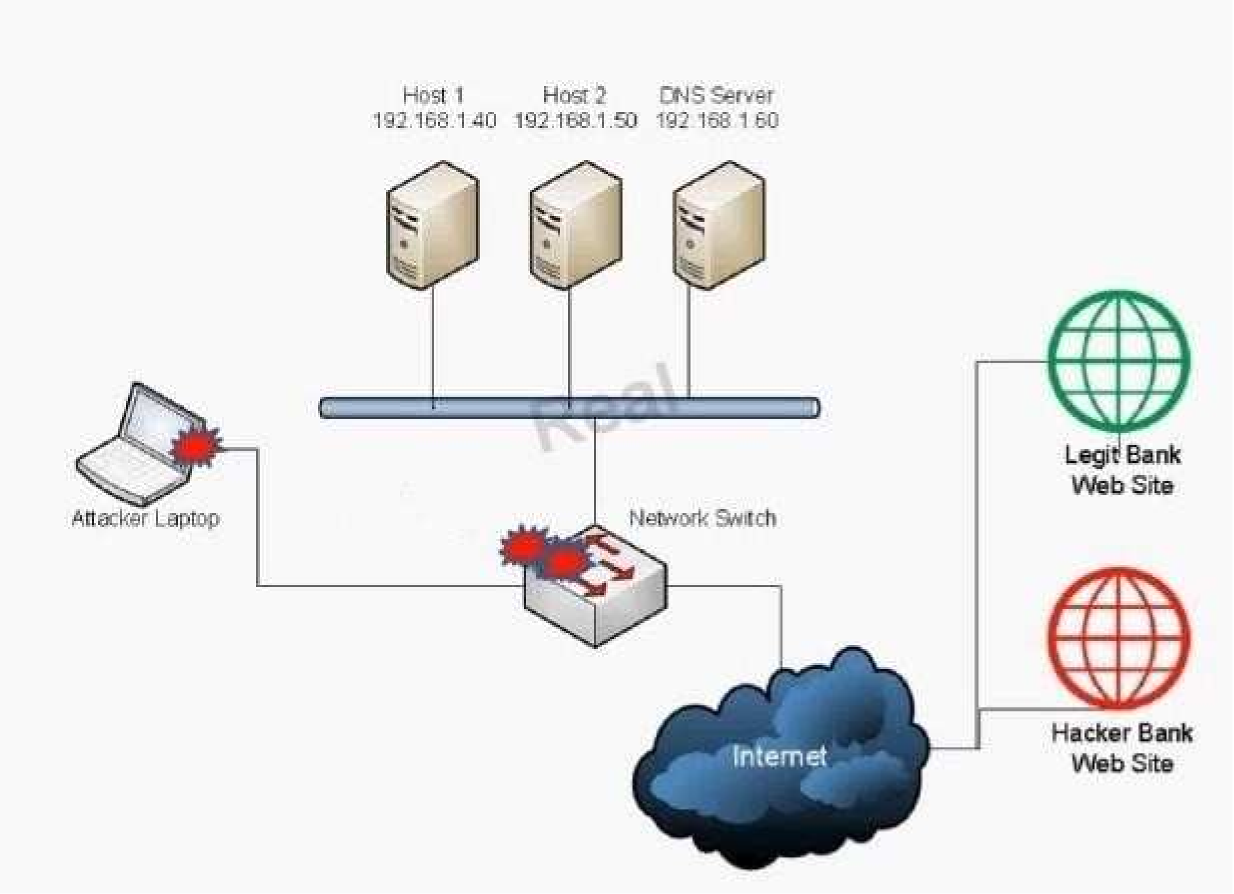
QUESTION 262
Which of the following BEST describes the type of attack that is occurring? (Select TWO).

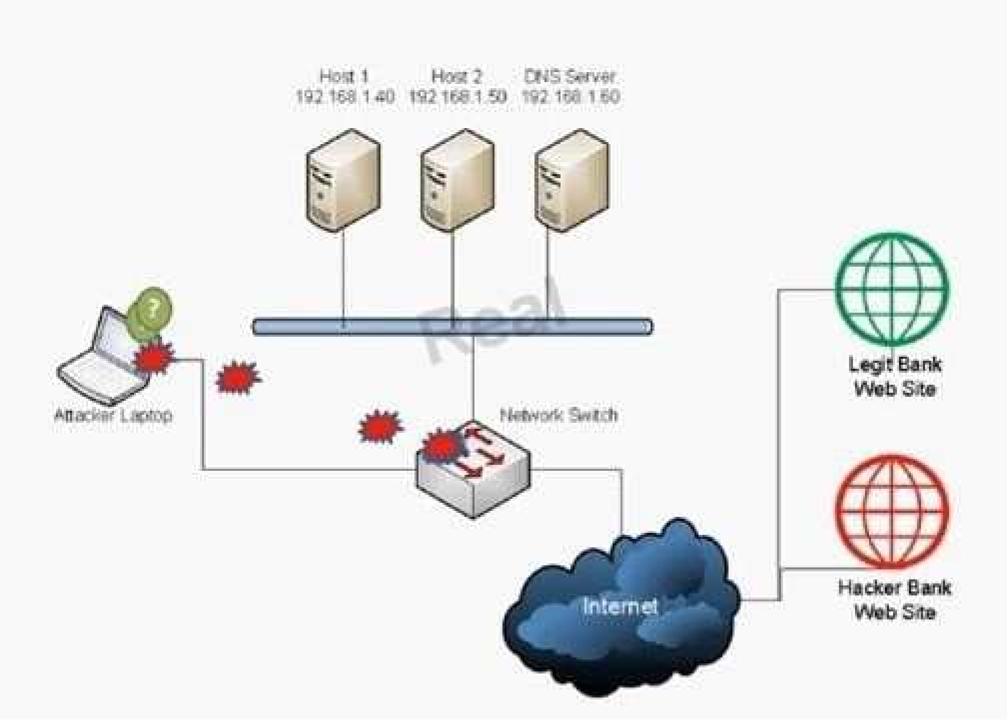
Real 220
CompTIA SY0-401 Exam

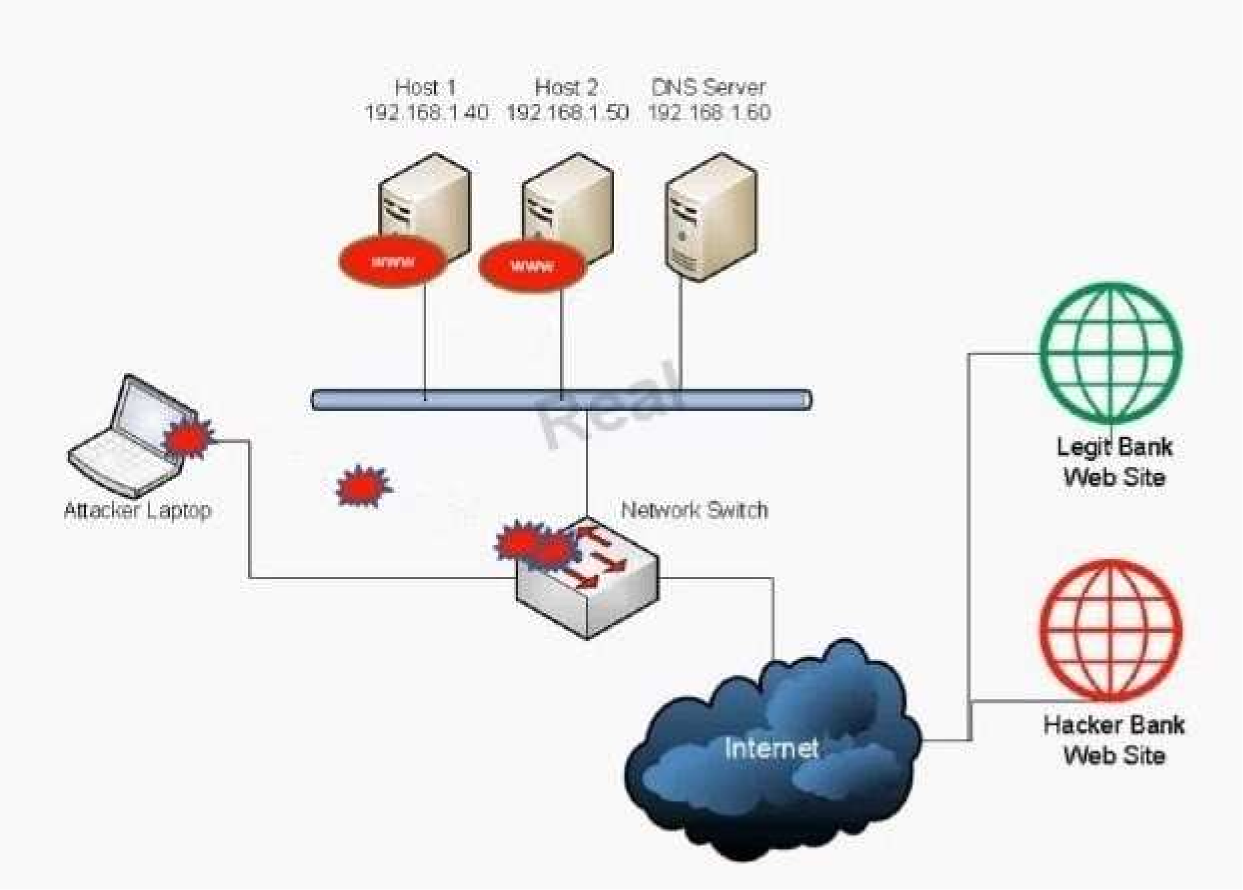

Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
Attacker Laptop
Network Switch
Internet
Legit Bank
Web Site
Hacker Bank
Web Site

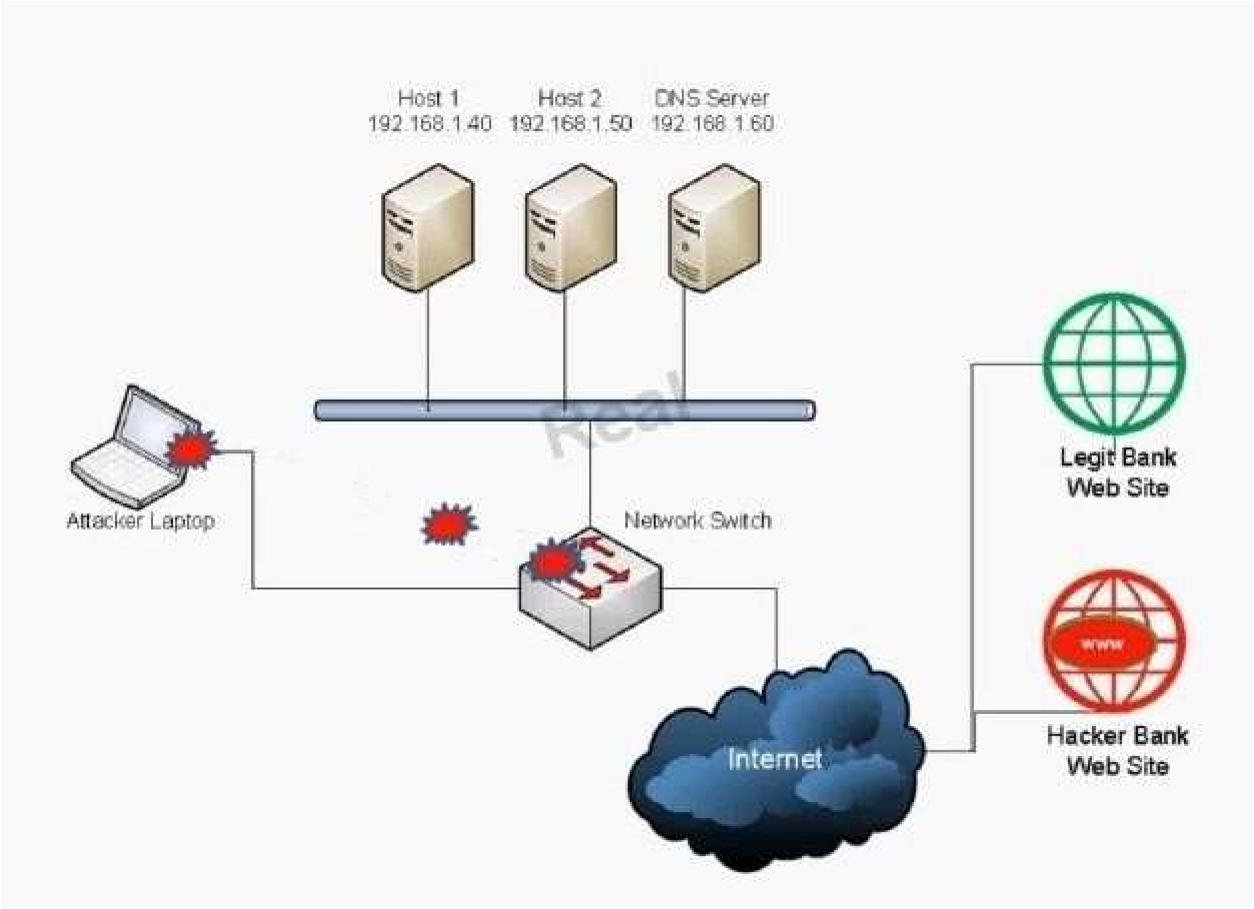

Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
Real
Attacker Laptop
Network Switch
www
www
Internet
Legit Bank
Web Site
Hacker Bank
Web Site


Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
Real
Attacker Laptop
Network Switch
Internet
Legit Bank
Web Site
Hacker Bank
Web Site


Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
Attacker Laptop
Network Switch
Legit Bank
Web Site
Hacker Bank
Web Site
Internet


Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
Real
Attacker Laptop
Network Switch
Internet
Legit Bank
Web Site
Hacker Bank
Web Site


Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
www
www
Attacker Laptop
Network Switch
Legit Bank
Web Site
Internet
Hacker Bank
Web Site



A. DNS spoofing
B. Man-in-the-middle
C. Backdoor
D. Replay
E. ARP attack
F. Spear phishing
G. Xmas attack

Correct Answer: AE

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 263
Which of the following is a hardware-based security technology included in a computer?

A. Symmetric key
B. Asymmetric key
C. Whole disk encryption
D. Trusted platform module

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264
Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site?

A. Internet content filter
B. Firewall
C. Proxy server
D. Protocol analyzer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 265
How often, at a MINIMUM, should Sara, an administrator, review the accesses and right of the users on her system?

A. Annually
B. Immediately after an employee is terminated
C. Every five years
D. Every time they patch the server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 266
An administrator is concerned that a company's web server has not been patched. Which of the following would be the BEST assessment for the administrator to perform?

A. Vulnerability scan
B. Risk assessment
C. Virus scan
D. Network sniffer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 267
An administrator notices that former temporary employees' accounts are still active on a domain.

Which of the following can be implemented to increase security and prevent this from happening?

A. Implement a password expiration policy.
B. Implement an account expiration date for permanent employees.
C. Implement time of day restrictions for all temporary employees.
D. Run a last logon script to look for inactive accounts.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 268
A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:

A. Logic bomb.
B. Backdoor.
C. Adware application.
D. Rootkit.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 269
Which of the following protocols uses TCP instead of UDP and is incompatible with all previous versions?

A. TACACS
B. XTACACS
C. RADIUS

D. TACACS+

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 270
Which of the following symmetric key algorithms are examples of block ciphers? (Select THREE).

A. RC4
B. 3DES
C. AES
D. MD5
E. PGP
F. Blowfish

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 271
Which of the following must be kept secret for a public key infrastructure to remain secure?

A. Certificate Authority
B. Certificate revocation list
C. Public key ring
D. Private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 272
Which of the following devices is BEST suited to protect an HTTP-based application that is susceptible to injection attacks?

A. Protocol filter
B. Load balancer

C. NIDS
D. Layer 7 firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 273
Which of the following is best practice to put at the end of an ACL?

A. Implicit deny
B. Time of day restrictions
C. Implicit allow
D. SNMP string

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 274
Which of the following security concepts can prevent a user from logging on from home during the weekends?

A. Time of day restrictions
B. Multifactor authentication

C. Implicit deny

D. Common access card

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 275
Which of the following would provide the STRONGEST encryption?

A. Random one-time pad

B. DES with a 56-bit key

C. AES with a 256-bit key

D. RSA with a 1024-bit key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 276
During a server audit, a security administrator does not notice abnormal activity. However, a network security analyst notices connections to unauthorized ports from outside the corporate network. Using specialized tools, the network security analyst also notices hidden processes running. Which of the following has MOST likely been installed on the server?

A. SPIM

B. Backdoor

C. Logic bomb

D. Rootkit

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 277
A security administrator wants to ensure that the message the administrator sends out to their Chief Financial Officer (CFO) does not get changed in route. Which of the following is the administrator MOST concerned with?

A. Data confidentiality
B. High availability
C. Data integrity
D. Business continuity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 278
Which of the following can be performed when an element of the company policy cannot be enforced by technical means?

Real 229
CompTIA SY0-401 Exam

A. Develop a set of standards
B. Separation of duties
C. Develop a privacy policy
D. User training

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 279

Timestamps and sequence numbers act as countermeasures against which of the following types of attacks?

A. Smurf
B. DoS
C. Vishing
D. Replay

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 280
Which of the following would be used as a secure substitute for Telnet?

A. SSH
B. SFTP
C. SSL
D. HTTPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 281
Which of the following is described as an attack against an application using a malicious file?

A. Client side attack

B. Spam
C. Impersonation attack
D. Phishing attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 282
Which of the following assessment techniques would a security administrator implement to ensure that systems and software are developed properly?

A. Baseline reporting
B. Input validation
C. Determine attack surface
D. Design reviews

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 283
Which of the following would a security administrator implement in order to identify a problem between two applications that are not communicating properly?

A. Protocol analyzer
B. Baseline report
C. Risk assessment
D. Vulnerability scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 284
Which of the following would a security administrator implement in order to identify change from the standard configuration on a server?

A. Penetration test

B. Code review
C. Baseline review
D. Design review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 285
Which of the following tools would a security administrator use in order to identify all running services throughout an organization?

A. Architectural review
B. Penetration test
C. Port scanner
D. Design review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 286
Which of the following protocols provides transport security for virtual terminal emulation?

A. TLS
B. SSH
C. SCP
D. S/MIME

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 287
Based on information leaked to industry websites, business management is concerned that unauthorized employees are accessing critical project information for a major, well-known new product. To identify any such users, the security administrator could:

Real 232
CompTIA SY0-401 Exam

A. Set up a honeypot and place false project documentation on an unsecure share.
B. Block access to the project documentation using a firewall.
C. Increase antivirus coverage of the project servers.
D. Apply security updates and harden the OS on all project servers.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 288
Which of the following is an indication of an ongoing current problem?

A. Alert
B. Trend
C. Alarm
D. Trap

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 289
Which of the following a programming interface that allows a remote computer to run programs on a local machine?

A. RPC
B. RSH
C. SSH
D. SSL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 290
Which of the following is the term for a fix for a known software problem?

A. Skiff
Real 233
CompTIA SY0-401 Exam
B. Patch
C. Slipstream
D. Upgrade

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 291
Connections using point-to-point protocol authenticate using which of the following? (Select TWO).

A. RIPEMD
B. PAP
C. CHAP
D. RC4

E. Kerberos

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 292
Which of the following will help prevent smurf attacks?

A. Allowing necessary UDP packets in and out of the network
B. Disabling directed broadcast on border routers
C. Disabling unused services on the gateway firewall
D. Flash the BIOS with the latest firmware

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 293
An advantage of virtualizing servers, databases, and office applications is:

A. Centralized management.
B. Providing greater resources to users.

C. Stronger access control.
D. Decentralized management.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 294
A major security risk with co-mingling of hosts with different security requirements is:

A. Security policy violations.
B. Zombie attacks.
C. Password compromises.
D. Privilege creep.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 295
Which of the following attacks targets high level executives to gain company information?

A. Phishing
B. Whaling
C. Vishing
D. Spoofing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 296
Which of the following can be used as an equipment theft deterrent?

A. Screen locks
B. GPS tracking
C. Cable locks
D. Whole disk encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 297
At the outside break area, an employee, Ann, asked another employee to let her into the building because her badge is missing. Which of the following does this describe?

A. Shoulder surfing
B. Tailgating
C. Whaling
D. Impersonation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
answer is verified.

QUESTION 298
A company that has a mandatory vacation policy has implemented which of the following controls?

A. Risk control
B. Privacy control
C. Technical control
D. Physical control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 299
Which of the following is the MOST intrusive type of testing against a production system?

A. White box testing
B. War dialing
C. Vulnerability testing
D. Penetration testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 300
The IT department has installed new wireless access points but discovers that the signal extends far into the parking lot. Which of the following actions should be taken to correct this?

A. Disable the SSID broadcasting
B. Configure the access points so that MAC filtering is not used
C. Implement WEP encryption on the access points
D. Lower the power for office coverage only

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 301
Which of the following devices would be MOST useful to ensure availability when there are a large number of requests to a certain website?

A. Protocol analyzer
B. Load balancer
C. VPN concentrator

D. Web security gateway

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 302
Which of the following uses port 22 by default? (Select THREE).

A. SSH
B. SSL
C. TLS
D. SFTP
E. SCP

F. FTPS
G. SMTP
H. SNMP

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 303
Ann, a software developer, has installed some code to reactivate her account one week after her account has been disabled. Which of the following is this an example of? (Select TWO).

A. Rootkit
B. Logic Bomb
C. Botnet
D. Backdoor

E. Spyware

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 304
The string:

` or 1=1-- -

Represents which of the following?

A. Bluejacking
B. Rogue access point
C. SQL Injection
D. Client-side attacks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 305
Joe, an administrator, installs a web server on the Internet that performs credit card transactions for customer payments. Joe also sets up a second web server that looks like the first web server.

However, the second server contains fabricated files and folders made to look like payments were processed on this server but really were not. Which of the following is the second server?

A. DMZ
B. Honeynet
C. VLAN
D. Honeypot

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 306
Which of the following can Joe, a security administrator, implement on his network to capture attack details that are occurring while also protecting his production network?

A. Security logs
B. Protocol analyzer
C. Audit logs
D. Honeypot

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 307
Which of the following should Joe, a security manager, implement to reduce the risk of employees working in collusion to embezzle funds from his company?

A. Privacy Policy
B. Least Privilege
C. Acceptable Use
D. Mandatory Vacations

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 308
Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for multicast packets from the switches on the network. After investigation, she discovers that this is normal activity for her network. Which of the following BEST describes these results?

A. True negatives
B. True positives
C. False positives
D. False negatives

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 309
Joe, a security analyst, asks each employee of an organization to sign a statement saying that they understand how their activities may be monitored. Which of the following BEST describes this statement? (Select TWO).

A. Acceptable use policy
B. Risk acceptance policy
C. Privacy policy
D. Email policy
E. Security policy

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 310
A process in which the functionality of an application is tested without any knowledge of the internal mechanisms of the application is known as:

A. Black box testing
B. White box testing
C. Black hat testing

D. Gray box testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 311
Which of the following tools would allow Ann, the security administrator, to be able to BEST quantify all traffic on her network?

A. Honeypot
B. Port scanner
C. Protocol analyzer
D. Vulnerability scanner

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 312
Ann is starting a disaster recovery program. She has gathered specifics and team members for a meeting on site. Which of the following types of tests is this?

A. Structured walk through
B. Full Interruption test
C. Check list test
D. Table top exercise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 313
An internal auditing team would like to strengthen the password policy to support special characters. Which of the following types of password controls would achieve this goal?

A. Add reverse encryption

B. Password complexity

C. Increase password length

D. Allow single sign on

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 314
Ann, the software security engineer, works for a major software vendor. Which of the following practices should be implemented to help prevent race conditions, buffer overflows, and other similar vulnerabilities prior to each production release?

A. Product baseline report

B. Input validation

C. Patch regression testing

D. Code review

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 315
Ann, a security analyst, is preparing for an upcoming security audit. To ensure that she identifies unapplied security controls and patches without attacking or compromising the system, Ann would use which of the following?

A. Vulnerability scanning
B. SQL injection
C. Penetration testing
D. Antivirus update

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 316
Ann, the security administrator, received a report from the security technician, that an unauthorized new user account was added to the server over two weeks ago. Which of the following could have mitigated this event?

Real 242
CompTIA SY0-401 Exam

A. Routine log audits
B. Job rotation
C. Risk likelihood assessment
D. Separation of duties

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 317
Which of the following ports should be opened on a firewall to allow for NetBIOS communication? (Select TWO).

A. 110
B. 137
C. 139
D. 143
E. 161
F. 443

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 318
Joe, the systems administrator, is setting up a wireless network for his team's laptops only and needs to prevent other employees from accessing it. Which of the following would BEST address this?

A. Disable default SSID broadcasting.
B. Use WPA instead of WEP encryption.
C. Lower the access point's power settings.
D. Implement MAC filtering on the access point.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 319
Real 243
CompTIA SY0-401 Exam
After Ann, a user, logs into her banking websites she has access to her financial institution mortgage, credit card, and brokerage websites as well. Which of the following is being described?

A. Trusted OS
B. Mandatory access control

C. Separation of duties
D. Single sign-on

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 320
Which of the following is a way to implement a technical control to mitigate data loss in case of a mobile device theft?

A. Disk encryption
B. Encryption policy
C. Solid state drive
D. Mobile device policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
answer is updated.

QUESTION 321
When an order was submitted via the corporate website, an administrator noted special characters (e.g., ";--" and "or 1=1 --") were input instead of the expected letters and numbers.

Which of the following is the MOST likely reason for the unusual results?

A. The user is attempting to highjack the web server session using an open-source browser.
B. The user has been compromised by a cross-site scripting attack (XSS) and is part of a botnet performing DDoS attacks.
C. The user is attempting to fuzz the web server by entering foreign language characters which are incompatible with the website.
D. The user is sending malicious SQL injection strings in order to extract sensitive company or customer data via the website.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 322
When a communications plan is developed for disaster recovery and business continuity plans, the MOST relevant items to include would be: (Select TWO).

A. Methods and templates to respond to press requests, institutional and regulatory reporting requirements.
B. Methods to exchange essential information to and from all response team members, employees, suppliers, and customers.
C. Developed recovery strategies, test plans, post-test evaluation and update processes.
D. Defined scenarios by type and scope of impact and dependencies, with quantification of loss potential.
E. Methods to review and report on system logs, incident response, and incident handling.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 323
Key elements of a business impact analysis should include which of the following tasks?

A. Develop recovery strategies, prioritize recovery, create test plans, post-test evaluation, and update processes.
B. Identify institutional and regulatory reporting requirements, develop response teams and communication trees, and develop press release templates.
C. Employ regular preventive measures such as patch management, change management, antivirus and vulnerability scans, and reports to management.
D. Identify critical assets systems and functions, identify dependencies, determine critical downtime limit, define scenarios by type and scope of impact, and quantify loss potential.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 324
End-user awareness training for handling sensitive personally identifiable information would

include secure storage and transmission of customer:

A. Date of birth.
B. First and last name.
C. Phone number.
D. Employer name.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 325
Which of the following risk mitigation strategies will allow Ann, a security analyst, to enforce least privilege principles?

A. User rights reviews
B. Incident management
C. Risk based controls
D. Annual loss expectancy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 326
The security officer is preparing a read-only USB stick with a document of important personal phone numbers, vendor contacts, an MD5 program, and other tools to provide to employees. At which of the following points in an incident should the officer instruct employees to use this information?

A. Business Impact Analysis
B. First Responder
C. Damage and Loss Control
D. Contingency Planning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 327
To ensure proper evidence collection, which of the following steps should be preformed FIRST?

A. Take hashes from the live system
B. Review logs
C. Capture the system image
D. Copy all compromised files

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 328
Joe, the security administrator, has determined that one of his web servers is under attack. Which of the following can help determine where the attack originated from?

A. Capture system image
B. Record time offset
C. Screenshots
D. Network sniffing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 329
Joe, the system administrator, is performing an overnight system refresh of hundreds of user computers. The refresh has a strict timeframe and must have zero downtime during business hours. Which of the following should Joe take into consideration?

A. A disk-based image of every computer as they are being replaced.
B. A plan that skips every other replaced computer to limit the area of affected users.
C. An offsite contingency server farm that can act as a warm site should any issues appear.
D. A back-out strategy planned out anticipating any unforeseen problems that may arise.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 330
A program displays:

ERROR: this program has caught an exception and will now terminate.

Which of the following is MOST likely accomplished by the program's behavior?

A. Operating system's integrity is maintained
B. Program's availability is maintained
C. Operating system's scalability is maintained
D. User's confidentiality is maintained

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 331
A security administrator wants to deploy a physical security control to limit an individual's access into a sensitive area. Which of the following should be implemented?

A. Guards
B. CCTV
C. Bollards
D. Spike strip

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 332
A network administrator uses an RFID card to enter the datacenter, a key to open the server rack, and a username and password to logon to a server. These are examples of which of the following?

A. Multifactor authentication
B. Single factor authentication
C. Separation of duties
D. Identification
Real 248
CompTIA SY0-401 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
answer is up-to-date.

QUESTION 333
Which of the following results in datacenters with failed humidity controls? (Select TWO).

A. Excessive EMI
B. Electrostatic charge
C. Improper ventilation
D. Condensation
E. Irregular temperature

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 334
An online store wants to protect user credentials and credit card information so that customers can store their credit card information and use their card for multiple separate transactions.

Which of the following database designs provides the BEST security for the online store?

A. Use encryption for the credential fields and hash the credit card field
B. Encrypt the username and hash the password
C. Hash the credential fields and use encryption for the credit card field
D. Hash both the credential fields and the credit card field

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 335
A security administrator is reviewing the below output from a password auditing tool:

P@ss.

@pW1.

Real 249
CompTIA SY0-401 Exam
S3cU4

Which of the following additional policies should be implemented based on the tool's output?

A. Password age

B. Password history
C. Password length
D. Password complexity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 336
Joe, a user, in a coffee shop is checking his email over a wireless network. An attacker records the temporary credentials being passed to Joe's browser. The attacker later uses the credentials to impersonate Joe and creates SPAM messages. Which of the following attacks allows for this impersonation?

A. XML injection
B. Directory traversal
C. Header manipulation
D. Session hijacking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 337
A security architect wishes to implement a wireless network with connectivity to the company's internal network. Before they inform all employees that this network is being put in place, the architect wants to roll it out to a small test segment. Which of the following allows for greater secrecy about this network during this initial phase of implementation?

A. Disabling SSID broadcasting
B. Implementing WPA2 - TKIP
C. Implementing WPA2 - CCMP
D. Filtering test workstations by MAC address

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 338
Digital certificates can be used to ensure which of the following? (Select TWO).

A. Availability
B. Confidentiality
C. Verification
D. Authorization
E. Non-repudiation

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 339
A network administrator is looking for a way to automatically update company browsers so they import a list of root certificates from an online source. This online source will then be responsible for tracking which certificates are to be trusted or not trusted. Which of the following BEST describes the service that should be implemented to meet these requirements?

A. Trust model
B. Key escrow
C. OCSP
D. PKI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 340

A quality assurance analyst is reviewing a new software product for security, and has complete access to the code and data structures used by the developers. This is an example of which of the following types of testing?

A. Black box
B. Penetration

C. Gray box
D. White box

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 341
The security consultant is assigned to test a client's new software for security, after logs show targeted attacks from the Internet. To determine the weaknesses, the consultant has no access to the application program interfaces, code, or data structures. This is an example of which of the following types of testing?

A. Black box
B. Penetration
C. Gray box
D. White box

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 342
Which of the following types of cryptography should be used when minimal overhead is necessary for a mobile device?

A. Block cipher
B. Elliptical curve cryptography
C. Diffie-Hellman algorithm

D. Stream cipher

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 343
The server administrator has noted that most servers have a lot of free disk space and low memory utilization. Which of the following statements will be correct if the server administrator migrates to a virtual server environment?

Real 252
CompTIA SY0-401 Exam

A. The administrator will need to deploy load balancing and clustering.
B. The administrator may spend more on licensing but less on hardware and equipment.
C. The administrator will not be able to add a test virtual environment in the data center.
D. Servers will encounter latency and lowered throughput issues.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 344
Configuring key/value pairs on a RADIUS server is associated with deploying which of the following?

A. WPA2-Enterprise wireless network

B. DNS secondary zones
C. Digital certificates
D. Intrusion detection system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 345
A security analyst performs the following activities: monitors security logs, installs surveillance cameras and analyzes trend reports. Which of the following job responsibilities is the analyst performing? (Select TWO).

A. Detect security incidents
B. Reduce attack surface of systems
C. Implement monitoring controls
D. Hardening network devices
E. Prevent unauthorized access

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 346
A certificate used on an ecommerce web server is about to expire. Which of the following will

Real 253
CompTIA SY0-401 Exam
occur if the certificate is allowed to expire?

A. The certificate will be added to the Certificate Revocation List (CRL).
B. Clients will be notified that the certificate is invalid.
C. The ecommerce site will not function until the certificate is renewed.
D. The ecommerce site will no longer use encryption.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 347
An administrator needs to segment internal traffic between layer 2 devices within the LAN. Which of the following types of network design elements would MOST likely be used?

A. Routing
B. DMZ
C. VLAN
D. NAT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 348
The security administrator needs to restrict traffic on a layer 3 device to support FTP from a new remote site. Which of the following secure network administration principles will need to be implemented?

A. Implicit deny
B. VLAN management
C. Port security
D. Access control lists

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 349
Real 254
CompTIA SY0-401 Exam
After a network outage, a PC technician is unable to ping various network devices. The network administrator verifies that those devices are working properly and can be accessed securely.

Which of the following is the MOST likely reason the PC technician is unable to ping those devices?

A. ICMP is being blocked
B. SSH is not enabled
C. DNS settings are wrong
D. SNMP is not configured properly

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 350
The security administrator has been tasked to update all the access points to provide a more secure connection. All access points currently use WPA TKIP for encryption. Which of the following would be configured to provide more secure connections?

A. WEP
B. WPA2 CCMP
C. Disable SSID broadcast and increase power levels
D. MAC filtering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 351
After a recent security breach, the network administrator has been tasked to update and backup all router and switch configurations. The security administrator has been tasked to enforce stricter security policies. All users were forced to undergo additional user awareness training. All of these actions are due to which of the

following types of risk mitigation strategies?

A. Change management
B. Implementing policies to prevent data loss
C. User rights and permissions review
D. Lessons learned

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 352
Various network outages have occurred recently due to unapproved changes to network and security devices. All changes were made using various system credentials. The security analyst has been tasked to update the security policy. Which of the following risk mitigation strategies would also need to be implemented to reduce the number of network outages due to unauthorized changes?

A. User rights and permissions review
B. Configuration management
C. Incident management
D. Implement security controls on Layer 3 devices

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 353
A security analyst discovered data such as images and word documents hidden within different types of files. Which of the following cryptographic concepts describes what was discovered?

A. Symmetric encryption
B. Non-repudiation
C. Steganography
D. Hashing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 354
Which of the following concepts describes the use of a one way transformation in order to validate the integrity of a program?

A. Hashing

B. Key escrow

C. Non-repudiation

D. Steganography

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 355
Recent data loss on financial servers due to security breaches forced the system administrator to harden their systems. Which of the following algorithms with transport encryption would be implemented to provide the MOST secure web connections to manage and access these servers?

A. SSL

B. TLS

C. HTTP

D. FTP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 356
Which of the following provides a static record of all certificates that are no longer valid?

A. Private key
B. Recovery agent
C. CRLs
D. CA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 357
A company requires that a user's credentials include providing something they know and something they are in order to gain access to the network. Which of the following types of authentication is being described?

A. Biometrics
B. Kerberos
C. Token
D. Two-factor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 358
A company wants to ensure that all credentials for various systems are saved within a central database so that users only have to login once for access to all systems. Which of the following would accomplish this?

A. Multi-factor authentication
B. Smart card access
C. Same Sign-On
D. Single Sign-On

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 359
Physical documents must be incinerated after a set retention period is reached. Which of the following attacks does this action remediate?

A. Shoulder Surfing
B. Dumpster Diving
C. Phishing
D. Impersonation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 360
All executive officers have changed their monitor location so it cannot be easily viewed when passing by their offices. Which of the following attacks does this action remediate?

A. Dumpster Diving
B. Impersonation
C. Shoulder Surfing
D. Whaling

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 361
Which of the following protocols is vulnerable to man-in-the-middle attacks by NOT using end to end TLS encryption?

A. HTTPS
B. WEP
C. WPA
D. WPA 2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
answer is verified.

QUESTION 362
A security administrator has been tasked with setting up a new internal wireless network that must use end to end TLS. Which of the following may be used to meet this objective?

A. WPA
B. HTTPS
C. WEP
D. WPA 2

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 363

A server administrator notes that a legacy application often stops running due to a memory error. When reviewing the debugging logs, they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describe?

Real 259
CompTIA SY0-401 Exam

A. Zero-day
B. Buffer overflow
C. Cross site scripting
D. Malicious add-on

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 364
Key cards at a bank are not tied to individuals, but rather to organizational roles. After a break in, it becomes apparent that extra efforts must be taken to successfully pinpoint who exactly enters secure areas. Which of the following security measures can be put in place to mitigate the issue until a new key card system can be installed?

A. Bollards
B. Video surveillance
C. Proximity readers
D. Fencing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 365
After running into the data center with a vehicle, attackers were able to enter through the hole in the building and steal several key servers in the ensuing chaos. Which of the following security measures can be put in place to mitigate the issue from occurring in the future?

A. Fencing
B. Proximity readers
C. Video surveillance
D. Bollards

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 366
Real 260
CompTIA SY0-401 Exam
A CA is compromised and attacks start distributing maliciously signed software updates. Which of the following can be used to warn users about the malicious activity?

A. Key escrow
B. Private key verification
C. Public key verification
D. Certificate revocation list

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 367
After encrypting all laptop hard drives, an executive officer's laptop has trouble booting to the operating system. Now that it is successfully encrypted the helpdesk cannot retrieve the data.

Which of the following can be used to decrypt the information for retrieval?

A. Recovery agent
B. Private key
C. Trust models

D. Public key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 368
Which of the following devices is MOST likely being used when processing the following?

```
1 PERMIT IP ANY ANY EQ 80

2 DENY IP ANY ANY
```

A. Firewall
B. NIPS
C. Load balancer
D. URL filter

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 369
The security administrator at ABC company received the following log information from an external party:

```
10:45:01 EST, SRC 10.4.3.7:3056, DST 8.4.2.1:80, ALERT, Directory traversal

10:45:02 EST, SRC 10.4.3.7:3057, DST 8.4.2.1:80, ALERT, Account brute force

10:45:03 EST, SRC 10.4.3.7:3058, DST 8.4.2.1:80, ALERT, Port scan
```

The external party is reporting attacks coming from abc-company.com. Which of the following is the reason the ABC company's security administrator is unable to determine the origin of the attack?

A. A NIDS was used in place of a NIPS.
B. The log is not in UTC.
C. The external party uses a firewall.
D. ABC company uses PAT.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 370
The security administrator is implementing a malware storage system to archive all malware seen by the company into a central database. The malware must be categorized and stored based on similarities in the code. Which of the following should the security administrator use to identify similar malware?

A. TwoFish
B. SHA-512
C. Fuzzy hashes
D. HMAC

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 371
The security administrator installed a newly generated SSL certificate onto the company web server. Due to a mis-configuration of the website, a downloadable file containing one of the pieces of the key was available to the public. It was verified that the disclosure did not require a reissue of the certificate. Which of the following was MOST likely compromised?

A. The file containing the recovery agent's keys.
B. The file containing the public key.
C. The file containing the private key.
D. The file containing the server's encrypted passwords.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 372
Which of the following was launched against a company based on the following IDS log?

```
122.41.15.252 - - [21/May/2012:00:17:20 +1200] "GET

/index.php?username=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA A

AAA HTTP/1.1" 200 2731 "http://www.company.com/cgibin/

forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible;

MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"
```

A. SQL injection
B. Buffer overflow attack
C. XSS attack
D. Online password crack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 373
Real 263
CompTIA SY0-401 Exam
The security administrator is analyzing a user's history file on a Unix server to determine if the user was attempting to break out of a rootjail. Which of the following lines in the user's history log shows evidence that the user attempted to escape the rootjail?

A. cd ../../../../bin/bash
B. whoami
C. ls /root

D. sudo -u root

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 374
A software development company has hired a programmer to develop a plug-in module to an existing proprietary application. After completing the module, the developer needs to test the entire application to ensure that the module did not introduce new vulnerabilities. Which of the following is the developer performing when testing the application?

A. Black box testing
B. White box testing
C. Gray box testing
D. Design review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 375
A security administrator must implement all requirements in the following corporate policy:
Passwords shall be protected against offline password brute force attacks. Passwords shall be protected against online password brute force attacks. Which of the following technical controls must be implemented to enforce the corporate policy? (Select THREE).

A. Account lockout
B. Account expiration
C. Screen locks
D. Password complexity
E. Minimum password lifetime
F. Minimum password length

Correct Answer: ADF

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 376
Which of the following is a best practice for error and exception handling?

A. Log detailed exception but display generic error message
B. Display detailed exception but log generic error message
C. Log and display detailed error and exception messages
D. Do not log or display error or exception messages

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 377
A team of firewall administrators have access to a `master password list' containing service account passwords. Which of the following BEST protects the master password list?

A. File encryption
B. Password hashing
C. USB encryption
D. Full disk encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 378
An SSL/TLS private key is installed on a corporate web proxy in order to inspect HTTPS requests. Which of the following describes how this private key should be

stored so that it is protected from theft?

A. Implement full disk encryption
B. Store on encrypted removable media
C. Utilize a hardware security module
D. Store on web proxy file system
   Real 265
   CompTIA SY0-401 Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 379
An insurance company requires an account recovery process so that information created by an employee can be accessed after that employee is no longer with the firm. Which of the following is the BEST approach to implement this process?

A. Employee is required to share their password with authorized staff prior to leaving the firm
B. Passwords are stored in a reversible form so that they can be recovered when needed
C. Authorized employees have the ability to reset passwords so that the data is accessible
D. All employee data is exported and imported by the employee prior to them leaving the firm

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 380
A small company has a website that provides online customer support. The company requires an account recovery process so that customers who forget their passwords can regain access.

Which of the following is the BEST approach to implement this process?

A. Replace passwords with hardware tokens which provide two-factor authentication to the online customer support site.

B. Require the customer to physically come into the company's main office so that the customer can be authenticated prior to their password being reset.
C. Web-based form that identifies customer by another mechanism and then emails the customer their forgotten password.
D. Web-based form that identifies customer by another mechanism, sets a temporary password and forces a password change upon first login.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 381
A new MPLS network link has been established between a company and its business partner.

Real 266
CompTIA SY0-401 Exam
The link provides logical isolation in order to prevent access from other business partners. Which of the following should be applied in order to achieve confidentiality and integrity of all data across the link?

A. MPLS should be run in IPVPN mode.
B. SSL/TLS for all application flows.
C. IPSec VPN tunnels on top of the MPLS link.
D. HTTPS and SSH for all application flows.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 382
Which of the following authentication services should be replaced with a more secure alternative?

A. RADIUS
B. TACACS
C. TACACS+
D. XTACACS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 383
A financial company requires a new private network link with a business partner to cater for realtime and batched data flows.

Which of the following activities should be performed by the IT security staff member prior to establishing the link?

A. Baseline reporting
B. Design review
C. Code review
D. SLA reporting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 384
Which device monitors network traffic in a passive manner?

A. Sniffer
B. IDS
C. Firewall
D. Web browser

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 385
What is a system that is intended or designed to be broken into by an attacker?

A. Honeypot
B. Honeybucket
C. Decoy
D. Spoofing system

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 386
How must user accounts for exiting employees be handled?

A. Disabled, regardless of the circumstances
B. Disabled if the employee has been terminated
C. Deleted, regardless of the circumstances
D. Deleted if the employee has been terminated

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 387

Human Resources (HR) would like executives to undergo only two specific security training programs a year. Which of the following provides the BEST level of security training for the executives? (Select TWO).

A. Acceptable use of social media
B. Data handling and disposal
C. Zero day exploits and viruses
D. Phishing threats and attacks
E. Clean desk and BYOD
F. Information security awareness

Correct Answer: DF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 388
Which of the following provides data the best fault tolerance at the LOWEST cost?

A. Load balancing
B. Clustering
C. Server virtualization
D. RAID 6

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 389
The librarian wants to secure the public Internet kiosk PCs at the back of the library. Which of the following would be the MOST appropriate? (Select TWO).

A. Device encryption
B. Antivirus
C. Privacy screen

D. Cable locks

E. Remote wipe
Real 269
CompTIA SY0-401 Exam

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
answer is modified.

QUESTION 390
A system administrator wants to enable WPA2 CCMP. Which of the following is the only encryption used?

A. RC4

B. DES

C. 3DES

D. AES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 391
Two programmers write a new secure application for the human resources department to store personal identifiable information. The programmers make the application available to themselves using an uncommon port along with an ID and password only they know. This is an example of which of the following?

A. Root Kit

B. Spyware

C. Logic Bomb

D. Backdoor

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 392
Everyone in the accounting department has the ability to print and sign checks. Internal audit has asked that only one group of employees may print checks while only two other employees may sign the checks. Which of the following concepts would enforce this process?

A. Separation of Duties
Real 270
CompTIA SY0-401 Exam
B. Mandatory Vacations
C. Discretionary Access Control
D. Job Rotation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 393
The security department has implemented a new laptop encryption product in the environment. The product requires one user name and password at the time of boot up and also another password after the operating system has finished loading. This setup is using which of the following authentication types?

A. Two-factor authentication
B. Single sign-on
C. Multifactor authentication
D. Single factor authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 394
The Human Resources department has a parent shared folder setup on the server. There are two groups that have access, one called managers and one called

staff. There are many sub folders under the parent shared folder, one is called payroll. The parent folder access control list propagates all subfolders and all subfolders inherit the parent permission. Which of the following is the quickest way to prevent the staff group from gaining access to the payroll folder?

A. Remove the staff group from the payroll folder
B. Implicit deny on the payroll folder for the staff group
C. Implicit deny on the payroll folder for the managers group
D. Remove inheritance from the payroll folder

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 395
The finance department works with a bank which has recently had a number of cyber attacks. The finance department is concerned that the banking website certificates have been compromised. Which of the following can the finance department check to see if any of the bank's certificates are still valid?

A. Bank's CRL
B. Bank's private key
C. Bank's key escrow
D. Bank's recovery agent

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 396
Which of the following are examples of network segmentation? (Select TWO).

A. IDS
B. IaaS
C. DMZ
D. Subnet

E. IPS

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 397
Which of the following provides the strongest authentication security on a wireless network?

A. MAC filter
B. WPA2
C. WEP
D. Disable SSID broadcast

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 398
Which of the following provides the BEST explanation regarding why an organization needs to implement IT security policies?

A. To ensure that false positives are identified
B. To ensure that staff conform to the policy
C. To reduce the organizational risk
D. To require acceptable usage of IT systems

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 399
An incident response team member needs to perform a forensics examination but does not have the required hardware. Which of the following will allow the team member to perform the examination with minimal impact to the potential evidence?

A. Using a software file recovery disc
B. Mounting the drive in read-only mode
C. Imaging based on order of volatility
D. Hashing the image after capture

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 400
Which of the following allows an organization to store a sensitive PKI component with a trusted third party?

A. Trust model
B. Public Key Infrastructure
C. Private key
D. Key escrow

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 401
Which of the following security devices can be replicated on a Linux based computer using IP tables to inspect and properly handle network based traffic?

A. Sniffer
B. Router
C. Firewall
D. Switch

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 402
A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address:

A. Integrity of downloaded software.
B. Availability of the FTP site.
C. Confidentiality of downloaded software.
D. Integrity of the server logs.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 403
An administrator has successfully implemented SSL on srv4.comptia.com using wildcard certificate *.comptia.com, and now wishes to implement SSL on srv5.comptia.com. Which of the following files should be copied from srv4 to accomplish this?

A. certificate, private key, and intermediate certificate chain
B. certificate, intermediate certificate chain, and root certificate
C. certificate, root certificate, and certificate signing request
D. certificate, public key, and certificate signing request Real 274
CompTIA SY0-401 Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 404
When reviewing security logs, an administrator sees requests for the AAAA record of www.comptia.com. Which of the following BEST describes this type of record?

A. DNSSEC record
B. IPv4 DNS record
C. IPSEC DNS record
D. IPv6 DNS record

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 405
Which of the following practices reduces the management burden of access management?

A. Password complexity policies
B. User account audit
C. Log analysis and review
D. Group based privileges

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
answer is valid.

QUESTION 406
Which of the following helps to apply the proper security controls to information?

A. Data classification
B. Deduplication
C. Clean desk policy
D. Encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 407
Which of the following describes purposefully injecting extra input during testing, possibly causing an application to crash?

A. Input validation
B. Exception handling
C. Application hardening
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 408
Which of the following types of security services are used to support authentication for remote users and devices?

A. Biometrics
B. HSM
C. RADIUS
D. TACACS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 409
A Chief Information Security Officer (CISO) is tasked with outsourcing the analysis of security logs. These will need to still be reviewed on a regular basis to ensure

the security of the company has not been breached. Which of the following cloud service options would support this requirement?

A. SaaS
B. MaaS
C. IaaS
D. PaaS
Real 276
CompTIA SY0-401 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 410
A security administrator needs a locally stored record to remove the certificates of a terminated employee. Which of the following describes a service that could meet these requirements?

A. OCSP
B. PKI
C. CA
D. CRL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 411
A security analyst informs the Chief Executive Officer (CEO) that a security breach has just occurred. This results in the Risk Manager and Chief Information Officer (CIO) being caught unaware when the CEO asks for further information. Which of the following strategies should be implemented to ensure the Risk Manager and CIO are not caught unaware in the future?

A. Procedure and policy management
B. Chain of custody management

C. Change management
D. Incident management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 412
Which of the following relies on the use of shared secrets to protect communication?

A. RADIUS
B. Kerberos
C. PKI
Real 277
CompTIA SY0-401 Exam
D. LDAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 413
A security administrator wants to test the reliability of an application which accepts user provided parameters. The administrator is concerned with data integrity and availability. Which of the following should be implemented to accomplish this task?

A. Secure coding
B. Fuzzing
C. Exception handling
D. Input validation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 414
Which of the following concepts is a term that directly relates to customer privacy considerations?

A. Data handling policies
B. Personally identifiable information
C. Information classification
D. Clean desk policies

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 415
Which of the following is a Data Loss Prevention (DLP) strategy and is MOST useful for securing data in use?

A. Email scanning
B. Content discovery

C. Database fingerprinting
D. Endpoint protection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 416
Which of the following is a concern when encrypting wireless data with WEP?

A. WEP displays the plain text entire key when wireless packet captures are reassembled
B. WEP implements weak initialization vectors for key transmission
C. WEP uses a very weak encryption algorithm
D. WEP allows for only four pre-shared keys to be configured

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 417
A security administrator is tasked with calculating the total ALE on servers. In a two year period of time, a company has to replace five servers. Each server replacement has cost the company $4,000 with downtime costing $3,000. Which of the following is the ALE for the company?

A. $7,000
B. $10,000
C. $17,500
D. $35,000

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 418
ABC company has a lot of contractors working for them. The provisioning team does not always get notified that a contractor has left the company. Which of the following policies would prevent contractors from having access to systems in the event a contractor has left?

Real 279
CompTIA SY0-401 Exam

A. Annual account review
B. Account expiration policy
C. Account lockout policy
D. Account disablement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 419
The practice of marking open wireless access points is called which of the following?

A. War dialing
B. War chalking
C. War driving
D. Evil twin

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 420
Multi-tenancy is a concept found in which of the following?

A. Full disk encryption
B. Removable media
C. Cloud computing
D. Data loss prevention

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 421

Which of the following is a common coding error in which boundary checking is not performed?

A. Input validation

B. Fuzzing

C. Secure coding

D. Cross-site scripting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 422
While previously recommended as a security measure, disabling SSID broadcast is not effective against most attackers because network SSIDs are:

A. no longer used to authenticate to most wireless networks.

B. contained in certain wireless packets in plaintext.

C. contained in all wireless broadcast packets by default.

D. no longer supported in 802.11 protocols.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 423
One of the most consistently reported software security vulnerabilities that leads to major exploits is:

A. Lack of malware detection.
B. Attack surface decrease.
C. Inadequate network hardening.
D. Poor input validation.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 424
Public key certificates and keys that are compromised or were issued fraudulently are listed on which of the following?

Real 281
CompTIA SY0-401 Exam

A. PKI
B. ACL
C. CA
D. CRL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
updated.

QUESTION 425
One of the most basic ways to protect the confidentiality of data on a laptop in the event the device is physically stolen is to implement which of the following?

A. File level encryption with alphanumeric passwords
B. Biometric authentication and cloud storage
C. Whole disk encryption with two-factor authentication
D. BIOS passwords and two-factor authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 426
Users report that after downloading several applications, their systems' performance has noticeably decreased. Which of the following would be used to validate programs prior to installing them?

A. Whole disk encryption
B. SSH
C. Telnet
D. MD5

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 427
A malicious user is sniffing a busy encrypted wireless network waiting for an authorized client to connect to it. Only after an authorized client has connected and the hacker was able to capture the client handshake with the AP can the hacker begin a brute force attack to discover the encryption key. Which of the following attacks is taking place?

A. IV attack
B. WEP cracking
C. WPA cracking
D. Rogue AP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 428
Which of the following protocols is used by IPv6 for MAC address resolution?

A. NDP
B. ARP
C. DNS
D. NCP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 429
Which of the following provides dedicated hardware-based cryptographic functions to an operating system and its applications running on laptops and desktops?

A. TPM
B. HSM
C. CPU
D. FPU

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 430
Real 283
CompTIA SY0-401 Exam
Which of the following tests a number of security controls in the least invasive manner?

A. Vulnerability scan
B. Threat assessment
C. Penetration test
D. Ping sweep

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 431
When using PGP, which of the following should the end user protect from compromise? (Select TWO).

A. Private key
B. CRL details
C. Public key
D. Key password
E. Key escrow
F. Recovery agent

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 432

Which of the following disaster recovery strategies has the highest cost and shortest recovery time?

A. Warm site
B. Hot site
C. Cold site
D. Co-location site

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 433
In the case of a major outage or business interruption, the security office has documented the expected loss of earnings, potential fines and potential consequence to customer service. Which of the following would include the MOST detail on these objectives?

A. Business Impact Analysis
B. IT Contingency Plan
C. Disaster Recovery Plan
D. Continuity of Operations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 434
After visiting a website, a user receives an email thanking them for a purchase which they did not request. Upon investigation the security administrator sees the following source code in a pop-up window:

```
<HTML>

<body onload="document.getElementByID('badForm').submit()"> <form

id="badForm" action="shoppingsite.company.com/purchase.php"
```

method="post" <input name="Perform Purchase" value="Perform Purchase"

/> </form></body></HTML>

Which of the following has MOST likely occurred?

A. SQL injection
B. Cookie stealing
C. XSRF
D. XSS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 435
Real 285
CompTIA SY0-401 Exam
Which of the following ports should be used by a system administrator to securely manage a remote server?

A. 22
B. 69
C. 137
D. 445

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 436
Which of the following ports is used to securely transfer files between remote UNIX systems?

A. 21

B. 22
C. 69
D. 445

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 437
Which of the following is a security benefit of providing additional HVAC capacity or increased tonnage in a datacenter?

A. Increased availability of network services due to higher throughput
B. Longer MTBF of hardware due to lower operating temperatures
C. Higher data integrity due to more efficient SSD cooling
D. Longer UPS run time due to increased airflow

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 438
Real 286
CompTIA SY0-401 Exam
Fuzzing is a security assessment technique that allows testers to analyze the behavior of software applications under which of the following conditions?

A. Unexpected input
B. Invalid output
C. Parameterized input
D. Valid output

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 439
Which of the following types of wireless attacks would be used specifically to impersonate another WAP in order to gain unauthorized information from mobile users?

A. IV attack
B. Evil twin
C. War driving
D. Rogue access point

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 440
Which of the following types of application attacks would be used to identify malware causing security breaches that have NOT yet been identified by any trusted sources?

A. Zero-day
B. LDAP injection
C. XML injection
D. Directory traversal

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 441
Real 287
CompTIA SY0-401 Exam
Which of the following is built into the hardware of most laptops but is not setup for centralized management by default?

A. Whole disk encryption
B. TPM encryption
C. USB encryption
D. Individual file encryption

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 442
Which of the following is true about the recovery agent?

A. It can decrypt messages of users who lost their private key.
B. It can recover both the private and public key of federated users.
C. It can recover and provide users with their lost or private key.
D. It can recover and provide users with their lost public key.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 443
Which of the following MOST specifically defines the procedures to follow when scheduled system patching fails resulting in system outages?

A. Risk transference
B. Change management
C. Configuration management
D. Access control revalidation

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 444
Real 288
CompTIA SY0-401 Exam
A review of the company's network traffic shows that most of the malware infections are caused by users visiting gambling and gaming websites. The security manager wants to implement a solution that will block these websites, scan all web traffic for signs of malware, and block the malware before it enters the company network. Which of the following is suited for this purpose?

A. ACL
B. IDS
C. UTM
D. Firewall

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 445
Which of the following would the security engineer set as the subnet mask for the servers below to utilize host addresses on separate broadcast domains?

Server 1: 192.168.100.6

Server 2: 192.168.100.9

Server 3: 192.169.100.20

A. /24
B. /27
C. /28
D. /29
E. /30

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 446
Which of the following offerings typically allows the customer to apply operating system patches?

A. Software as a service
B. Public Clouds
C. Cloud Based Storage

D. Infrastructure as a service

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 447
A technician is unable to manage a remote server. Which of the following ports should be opened on the firewall for remote server management? (Select TWO).

A. 22
B. 135
C. 137
D. 143
E. 443
F. 3389

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 448
When designing a new network infrastructure, a security administrator requests that the intranet web server be placed in an isolated area of the network for security purposes. Which of the following design elements would be implemented to comply with the security administrator's request?

A. DMZ
B. Cloud services
C. Virtualization
D. Sandboxing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 449
At an organization, unauthorized users have been accessing network resources via unused network wall jacks. Which of the following would be used to stop unauthorized access?

A. Configure an access list.
B. Configure spanning tree protocol.
C. Configure port security.
D. Configure loop protection.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 450
Users report that they are unable to access network printing services. The security technician checks the router access list and sees that web, email, and secure shell are allowed. Which of the following is blocking network printing?

A. Port security
B. Flood guards
C. Loop protection
D. Implicit deny

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 451
Joe, a security administrator, believes that a network breach has occurred in the datacenter as a result of a misconfigured router access list, allowing outside access to an SSH server. Which of the following should Joe search for in the log files?

A. Failed authentication attempts
B. Network ping sweeps
C. Host port scans
D. Connections to port 22

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 452
Which of the following firewall types inspects Ethernet traffic at the MOST levels of the OSI

Real 291
CompTIA SY0-401 Exam
model?

A. Packet Filter Firewall
B. Stateful Firewall
C. Proxy Firewall

D. Application Firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 453
A security analyst needs to logon to the console to perform maintenance on a remote server.

Which of the following protocols would provide secure access?

A. SCP
B. SSH
C. SFTP
D. HTTPS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 454
Ann, a newly hired human resource employee, sent out confidential emails with digital signatures, to an unintended group. Which of the following would prevent her from denying accountability?

A. Email Encryption
B. Steganography
C. Non Repudiation
D. Access Control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 455
Real 292
CompTIA SY0-401 Exam
Ann, a technician, is attempting to establish a remote terminal session to an end user's computer using Kerberos authentication, but she cannot connect to the destination machine. Which of the following default ports should Ann ensure is open?

A. 22
B. 139
C. 443
D. 3389

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 456
Concurrent use of a firewall, content filtering, antivirus software and an IDS system would be considered components of:

A. Redundant systems.
B. Separation of duties.
C. Layered security.
D. Application control.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 457
Which of the following is a security risk regarding the use of public P2P as a method of collaboration?

A. Data integrity is susceptible to being compromised.
B. Monitoring data changes induces a higher cost.
C. Users are not responsible for data usage tracking.
D. Limiting the amount of necessary space for data storage.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 458
The method to provide end users of IT systems and applications with requirements related to acceptable use, privacy, new threats and trends, and use of social networking is:

A. Security awareness training.
B. BYOD security training.
C. Role-based security training.
D. Legal compliance training.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 459
After an audit, it was discovered that the security group memberships were not properly adjusted for employees' accounts when they moved from one role to another. Which of the following has the organization failed to properly implement? (Select TWO).

A. Mandatory access control enforcement.
B. User rights and permission reviews.
C. Technical controls over account management.
D. Account termination procedures.
E. Management controls over account management.
F. Incident management and response plan.

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 460
A security technician wishes to gather and analyze all Web traffic during a particular time period.

Which of the following represents the BEST approach to gathering the required data?

A. Configure a VPN concentrator to log all traffic destined for ports 80 and 443.
B. Configure a proxy server to log all traffic destined for ports 80 and 443.
C. Configure a switch to log all traffic destined for ports 80 and 443.
D. Configure a NIDS to log all traffic destined for ports 80 and 443.
Real 294
CompTIA SY0-401 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 461
A security administrator suspects that an increase in the amount of TFTP traffic on the network is due to unauthorized file transfers, and wants to configure a firewall to block all TFTP traffic.

Which of the following would accomplish this task?

A. Deny TCP port 68
B. Deny TCP port 69
C. Deny UDP port 68
D. Deny UCP port 69

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 462
The network security engineer just deployed an IDS on the network, but the Chief Technical Officer (CTO) has concerns that the device is only able to detect known anomalies. Which of the following types of IDS has been deployed?

A. Signature Based IDS

B. Heuristic IDS
C. Behavior Based IDS
D. Anomaly Based IDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 463
Joe, a newly hired employee, has a corporate workstation that has been compromised due to several visits to P2P sites. Joe insisted that he was not aware of any company policy that prohibits the use of such web sites. Which of the following is the BEST method to deter employees from the improper use of the company's information systems?

Real 295
CompTIA SY0-401 Exam

A. Acceptable Use Policy
B. Privacy Policy

C. Security Policy

D. Human Resource Policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 464
The Chief Technical Officer (CTO) has tasked The Computer Emergency Response Team (CERT) to develop and update all Internal Operating Procedures and Standard Operating Procedures documentation in order to successfully respond to future incidents. Which of the following stages of the Incident Handling process is the team working on?

A. Lessons Learned

B. Eradication

C. Recovery

D. Preparation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 465
Company XYZ recently salvaged company laptops and removed all hard drives, but the Chief

Information Officer (CIO) is concerned about disclosure of confidential information. Which of the following is the MOST secure method to dispose of these hard drives?

A. Degaussing

B. Physical Destruction

C. Lock up hard drives in a secure safe

D. Wipe

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 466
A company has recently implemented a high density wireless system by having a junior technician install two new access points for every access point already deployed. Users are now reporting random wireless disconnections and slow network connectivity. Which of the following is the MOST likely cause?

A. The old APs use 802.11a
B. Users did not enter the MAC of the new APs
C. The new APs use MIMO
D. A site survey was not conducted

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 467
A company provides secure wireless Internet access for visitors and vendors working onsite. Some of the vendors using older technology report that they are unable to access the wireless network after entering the correct network information. Which of the following is the MOST likely reason for this issue?

A. The SSID broadcast is disabled.
B. The company is using the wrong antenna type.
C. The MAC filtering is disabled on the access point.
D. The company is not using strong enough encryption.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 468

A company is looking to reduce the likelihood of employees in the finance department being involved with money laundering. Which of the following controls would BEST mitigate this risk?

A. Implement privacy policies
B. Enforce mandatory vacations
C. Implement a security policy
D. Enforce time of day restrictions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
valid.

QUESTION 469
A company recently experienced data loss when a server crashed due to a midday power outage.

Which of the following should be used to prevent this from occurring again?

A. Recovery procedures
B. EMI shielding
C. Environmental monitoring
D. Redundancy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 470
Joe, a security administrator, is concerned with users tailgating into the restricted areas. Given a limited budget, which of the following would BEST assist Joe with detecting this activity?

A. Place a full-time guard at the entrance to confirm user identity.
B. Install a camera and DVR at the entrance to monitor access.
C. Revoke all proximity badge access to make users justify access.

D. Install a motion detector near the entrance.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 471
It is important to staff who use email messaging to provide PII to others on a regular basis to have confidence that their messages are not intercepted or altered during transmission. They are concerned about which of the following types of security control?

A. Integrity
B. Safety
C. Availability

D. Confidentiality

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 472
A security manager requires fencing around the perimeter, and cipher locks on all entrances. The manager is concerned with which of the following security controls?

A. Integrity
B. Availability
C. Confidentiality
D. Safety

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 473
A security engineer is reviewing log data and sees the output below:

```
POST: /payload.php HTTP/1.1

HOST: localhost

Accept: */*

Referrer: http://localhost/

*******

HTTP/1.1 403 Forbidden

Connection: close
```

Log: Access denied with 403. Pattern matches form bypass Which of the following technologies was MOST likely being used to generate this log?

A. Host-based Intrusion Detection System
B. Web application firewall
C. Network-based Intrusion Detection System
D. Stateful Inspection Firewall
E. URL Content Filter

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 474
A security team has identified that the wireless signal is broadcasting into the parking lot. To reduce the risk of an attack against the wireless network from the parking lot, which of the following controls should be used? (Select TWO).

A. Antenna placement
B. Interference
C. Use WEP
D. Single Sign on
E. Disable the SSID
F. Power levels

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 475
An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to integrate the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal?

A. Unified Threat Management
B. Virtual Private Network
C. Single sign on
D. Role-based management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 476
A company's legacy server requires administration using Telnet. Which of the following protocols could be used to secure communication by offering encryption at a lower OSI layer? (Select TWO).

A. IPv6
B. SFTP
C. IPSec
D. SSH

E. IPv4

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 477
Joe, the Chief Technical Officer (CTO), is concerned about new malware being introduced into the corporate network. He has tasked the security engineers to implement a technology that is capable of alerting the team when unusual traffic is on the network. Which of the following types of technologies will BEST address this scenario?

A. Application Firewall
B. Anomaly Based IDS
C. Proxy Firewall
D. Signature IDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 478
Which of the following describes the purpose of an MOU?

A. Define interoperability requirements
B. Define data backup process
C. Define onboard/offboard procedure
D. Define responsibilities of each party

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 479
The security manager received a report that an employee was involved in illegal activity and has saved data to a workstation's hard drive. During the investigation, local law enforcement's criminal division confiscates the hard drive as evidence. Which of the following forensic procedures is involved?

A. Chain of custody
B. System image
C. Take hashes
D. Order of volatility

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 480
Environmental control measures include which of the following?

A. Access list
B. Lighting
C. Motion detection
D. EMI shielding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 481
Which of the following is the BEST concept to maintain required but non-critical server availability?

A. SaaS site
B. Cold site
C. Hot site

D. Warm site

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
updated.

QUESTION 482
Prior to leaving for an extended vacation, Joe uses his mobile phone to take a picture of his family in the house living room. Joe posts the picture on a popular social media site together with the message: "Heading to our two weeks vacation to Italy." Upon returning home, Joe discovers that the house was burglarized. Which of the following is the MOST likely reason the house was burglarized if nobody knew Joe's home address?

A. Joe has enabled the device access control feature on his mobile phone.
B. Joe's home address can be easily found using the TRACEROUTE command.
C. The picture uploaded to the social media site was geo-tagged by the mobile phone.
D. The message posted on the social media site informs everyone the house will be empty.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 483
Which of the following technical controls helps to prevent Smartphones from connecting to a corporate network?

A. Application white listing
B. Remote wiping
C. Acceptable use policy
D. Mobile device management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 484
Which of the following would prevent a user from installing a program on a company-owned mobile device?

A. White-listing
B. Access control lists
C. Geotagging

D. Remote wipe

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 485
Which of the following can be used to maintain a higher level of security in a SAN by allowing isolation of mis-configurations or faults?

A. VLAN
B. Protocol security
C. Port security
D. VSAN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 486
The act of magnetically erasing all of the data on a disk is known as:

A. Wiping
B. Dissolution

C. Scrubbing
D. Degaussing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 487
Joe, a network security engineer, has visibility to network traffic through network monitoring tools.

However, he's concerned that a disgruntled employee may be targeting a server containing the company's financial records. Which of the following security mechanism would be MOST appropriate to confirm Joe's suspicion?

Real 304
CompTIA SY0-401 Exam

A. HIDS
B. HIPS
C. NIPS
D. NIDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 488
Joe, a technician at the local power plant, notices that several turbines had ramp up in cycles during the week. Further investigation by the system engineering team determined that a timed .exe file had been uploaded to the system control console during a visit by international contractors. Which of the following actions should Joe recommend?

A. Create a VLAN for the SCADA
B. Enable PKI for the MainFrame
C. Implement patch management

D. Implement stronger WPA2 Wireless

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 489
A system administrator has been instructed by the head of security to protect their data at-rest.

Which of the following would provide the strongest protection?

A. Prohibiting removable media
B. Incorporating a full-disk encryption system
C. Biometric controls on data center entry points
D. A host-based intrusion detection system

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 490
An Information Systems Security Officer (ISSO) has been placed in charge of a classified peer-

topeer network that cannot connect to the Internet. The ISSO can update the antivirus definitions manually, but which of the following steps is MOST important?

A. A full scan must be run on the network after the DAT file is installed.
B. The signatures must have a hash value equal to what is displayed on the vendor site.
C. The definition file must be updated within seven days.
D. All users must be logged off of the network prior to the installation of the definition file.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 491
Ann has taken over as the new head of the IT department. One of her first assignments was to implement AAA in preparation for the company's new telecommuting policy. When she takes inventory of the organizations existing network infrastructure, she makes note that it is a mix of several different vendors. Ann knows she needs a method of secure centralized access to the company's network resources. Which of the following is the BEST service for Ann to implement?

A. RADIUS
B. LDAP
C. SAML
D. TACACS+

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 492
A group policy requires users in an organization to use strong passwords that must be changed every 15 days. Joe and Ann were hired 16 days ago. When Joe logs into the network, he is prompted to change his password; when Ann logs into the network, she is not prompted to change her password. Which of the following BEST explains why Ann is not required to change her password?

A. Ann's user account has administrator privileges.
B. Joe's user account was not added to the group policy.
C. Ann's user account was not added to the group policy.
D. Joe's user account was inadvertently disabled and must be re-created.
Real 306
CompTIA SY0-401 Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 493
A new web server has been provisioned at a third party hosting provider for processing credit card transactions. The security administrator runs the netstat command on the server and notices that ports 80, 443, and 3389 are in a `listening' state. No other ports are open. Which of the following services should be disabled to ensure secure communications?

A. HTTPS
B. HTTP
C. RDP
D. TELNET

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 494
Several employee accounts appear to have been cracked by an attacker. Which of the following should the security administrator implement to mitigate password cracking attacks? (Select TWO).

A. Increase password complexity
B. Deploy an IDS to capture suspicious logins
C. Implement password history
D. Implement monitoring of logins
E. Implement password expiration
F. Increase password length

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 495
A cafe provides laptops for Internet access to their customers. The cafe is located in the center corridor of a busy shopping mall. The company has experienced

several laptop thefts from the cafe during peek shopping hours of the day. Corporate has asked that the IT department provide a

solution to eliminate laptop theft. Which of the following would provide the IT department wit the BEST solution?

A. Attach cable locks to each laptop
B. Require each customer to sign an AUP
C. Install a GPS tracking device onto each laptop

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 496
A company hired Joe, an accountant. The IT administrator will need to create a new account for

Joe. The company uses groups for ease of management and administration of user accounts.

Joe will need network access to all directories, folders and files within the accounting department.

Which of the following configurations will meet the requirements?

A. Create a user account and assign the user account to the accounting group.
B. Create an account with role-based access control for accounting.
C. Create a user account with password reset and notify Joe of the account creation.
D. Create two accounts: a user account and an account with full network administration rights.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 497
Ann, the network administrator, has learned from the helpdesk that employees are accessing the wireless network without entering their domain credentials upon

connection. Once the connection is made, they cannot reach any internal resources, while wired network connections operate smoothly. Which of the following is MOST likely occurring?

A. A user has plugged in a personal access point at their desk to connect to the network wirelessly.
B. The company is currently experiencing an attack on their internal DNS servers.
C. The company's WEP encryption has been compromised and WPA2 needs to be implemented Real 308
CompTIA SY0-401 Exam
instead.
D. An attacker has installed an access point nearby in an attempt to capture company information.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 498
Ann works at a small company and she is concerned that there is no oversight in the finance department; specifically, that Joe writes, signs and distributes paychecks, as well as other expenditures. Which of the following controls can she implement to address this concern?

A. Mandatory vacations
B. Time of day restrictions
C. Least privilege
D. Separation of duties

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 499
A hospital IT department wanted to secure its doctor's tablets. The IT department wants operating system level security and the ability to secure the data from alteration. Which of the following methods would MOST likely work?

A. Cloud storage
B. Removal Media

C. TPM
D. Wiping

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 500
Which of the following common access control models is commonly used on systems to ensure a "need to know" based on classification levels?

Real 309
CompTIA SY0-401 Exam

A. Role Based Access Controls
B. Mandatory Access Controls
C. Discretionary Access Controls
D. Access Control List

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 501
A company's security administrator wants to manage PKI for internal systems to help reduce costs. Which of the following is the FIRST step the security administrator should take?

A. Install a registration server.
B. Generate shared public and private keys.
C. Install a CA
D. Establish a key escrow policy.

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 502
A network consists of various remote sites that connect back to two main locations. Pete, the security administrator, needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

A. Block port 23 on the L2 switch at each remote site
B. Block port 23 on the network firewall
C. Block port 25 on the L2 switch at each remote site
D. Block port 25 on the network firewall

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 503
Pete, a security administrator, is informed that people from the HR department should not have access to the accounting department's server, and the accounting department should not have access to the HR department's server. The network is separated by switches. Which of the following is designed to keep the HR department users from accessing the accounting department's server and vice-versa?

A. ACLs
B. VLANs

C. DMZs
D. NATS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 504
Which of the following is BEST utilized to actively test security controls on a particular system?

A. Port scanning
B. Penetration test
C. Vulnerability scanning
D. Grey/Gray box

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 505
Which of the following has serious security implications for large organizations and can potentially allow an attacker to capture conversations?

A. Subnetting
B. NAT
C. Jabber
D. DMZ

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 506
Real 311
CompTIA SY0-401 Exam
Upper management decides which risk to mitigate based on cost. This is an example of:

A. Qualitative risk assessment
B. Business impact analysis
C. Risk management framework
D. Quantitative risk assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 507
Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts?

A. Availability
B. Integrity
C. Accounting
D. Confidentiality

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 508
Which of the following should be used when a business needs a block cipher with minimal key size for internal encryption?

A. AES
B. Blowfish

C. RC5
D. 3DES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 509
Real 312
CompTIA SY0-401 Exam
Which of the following best practices makes a wireless network more difficult to find?

A. Implement MAC filtering
B. UseWPA2-PSK
C. Disable SSD broadcast
D. Power down unused WAPs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 510
The use of social networking sites introduces the risk of:

A. Disclosure of proprietary information
B. Data classification issues
C. Data availability issues
D. Broken chain of custody

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 511
Which the following flags are used to establish a TCP connection? (Select TWO).

A. PSH
B. ACK
C. SYN
D. URG
E. FIN

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 512
Which of the following describes the process of removing unnecessary accounts and services from an application to reduce risk exposure?

A. Error and exception handling
B. Application hardening
C. Application patch management
D. Cross-site script prevention

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 513

Which of the following MUST Matt, a security administrator, implement to verify both the integrity and authenticity of a message while requiring a shared secret?

A. RIPEMD
B. MD5
C. SHA
D. HMAC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 514
Visitors entering a building are required to close the back door before the front door of the same entry room is open. Which of the following is being described?

A. Tailgating
B. Fencing
C. Screening
D. Mantrap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 515
Real 314
CompTIA SY0-401 Exam
Which of the following software allows a network administrator to inspect the protocol header in order to troubleshoot network issues?

A. URL filter
B. Spam filter
C. Packet sniffer
D. Switch

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 516
Which of the following ports would be blocked if Pete, a security administrator, wants to deny access to websites?

A. 21
B. 25
C. 80
D. 3389

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 517
Which of the following would Pete, a security administrator, do to limit a wireless signal from penetrating the exterior walls?

A. Implement TKIP encryption
B. Consider antenna placement
C. Disable the SSID broadcast
D. Disable WPA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 518
Real 315

Which of the following is where an unauthorized device is found allowing access to a network?

A. Bluesnarfing
B. Rogue access point
C. Honeypot
D. IV attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 519
Which of the following attacks allows access to contact lists on cellular phones?

A. War chalking
B. Blue jacking
C. Packet sniffing
D. Bluesnarfing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 520
Which of the following can hide confidential or malicious data in the whitespace of other files (e.g. JPEGs)?

A. Hashing
B. Transport encryption
C. Digital signatures
D. Steganography

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 521
Which of the following identifies certificates that have been compromised or suspected of being

compromised?

A. Certificate revocation list
B. Access control list
C. Key escrow registry
D. Certificate authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 522
Which of the following BEST allows Pete, a security administrator, to determine the type, source, and flags of the packet traversing a network for troubleshooting purposes?

A. Switches
B. Protocol analyzers
C. Routers
D. Web security gateways

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 523
Which of the following is the MOST important step for preserving evidence during forensic procedures?

A. Involve law enforcement
B. Chain of custody
C. Record the time of the incident
D. Report within one hour of discovery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 524
Real 317
CompTIA SY0-401 Exam
Highly sensitive data is stored in a database and is accessed by an application on a DMZ server. The disk drives on all servers are fully encrypted. Communication between the application server and end-users is also encrypted. Network ACLs prevent any connections to the database server except from the application server. Which of the following can still result in exposure of the sensitive data in the database server?

A. SQL Injection
B. Theft of the physical database server
C. Cookies
D. Cross-site scripting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
corrected.

QUESTION 525
The fundamental information security principals include confidentiality, availability and which of the following?

A. The ability to secure data against unauthorized disclosure to external sources
B. The capacity of a system to resist unauthorized changes to stored information
C. The confidence with which a system can attest to the identity of a user
D. The characteristic of a system to provide uninterrupted service to authorized users

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 526
Which of the following is the MOST likely cause of users being unable to verify a single user's email signature and that user being unable to decrypt sent messages?

A. Unmatched key pairs
B. Corrupt key escrow
C. Weak public key
D. Weak private key

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 527
Full disk encryption is MOST effective against which of the following threats?

A. Denial of service by data destruction
B. Eavesdropping emanations
C. Malicious code
D. Theft of hardware

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 528
Which of the following may cause Jane, the security administrator, to seek an ACL work around?

A. Zero day exploit
B. Dumpster diving
C. Virus outbreak
D. Tailgating

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 529
In order to use a two-way trust model the security administrator MUST implement which of the following?

A. DAC
B. PKI
C. HTTPS
D. TPM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 530
Which of the following would a security administrator use to verify the integrity of a file?

A. Time stamp

B. MAC times
C. File descriptor
D. Hash

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 531
Which of the following is a best practice when securing a switch from physical access?

A. Disable unnecessary accounts
B. Print baseline configuration
C. Enable access lists
D. Disable unused ports

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 532
A security administrator needs to image a large hard drive for forensic analysis. Which of the following will allow for faster imaging to a second hard drive?

A. cp /dev/sda /dev/sdb bs=8k
B. tail -f /dev/sda > /dev/sdb bs=8k
C. dd in=/dev/sda out=/dev/sdb bs=4k
D. locate /dev/sda /dev/sdb bs=4k

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 533
Real 320
CompTIA SY0-401 Exam
Sara, an employee, tethers her smartphone to her work PC to bypass the corporate web security gateway while connected to the LAN. While Sara is out at lunch her PC is compromised via the tethered connection and corporate data is stolen. Which of the following would BEST prevent this from occurring again?

A. Disable the wireless access and implement strict router ACLs.
B. Reduce restrictions on the corporate web security gateway.
C. Security policy and threat awareness training.
D. Perform user rights and permissions reviews.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 534
Which of the following can be implemented if a security administrator wants only certain devices connecting to the wireless network?

A. Disable SSID broadcast
B. Install a RADIUS server
C. Enable MAC filtering
D. Lowering power levels on the AP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 535
Which of the following malware types typically allows an attacker to monitor a user's computer, is characterized by a drive-by download, and requires no user interaction?

A. Virus
B. Logic bomb
C. Spyware
D. Adware

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 536
Which of the following malware types may require user interaction, does not hide itself, and is commonly identified by marketing pop-ups based on browsing habits?

A. Botnet
B. Rootkit
C. Adware
D. Virus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 537
Which of the following is characterized by an attack against a mobile device?

A. Evil twin
B. Header manipulation
C. Blue jacking
D. Rogue AP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 538
Which of the following application attacks is used against a corporate directory service where there are unknown servers on the network?

A. Rogue access point
B. Zero day attack
C. Packet sniffing
D. LDAP injection

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
answer is up-to-date.

QUESTION 539
Which of the following protocols allows for the LARGEST address space?

A. IPX
B. IPv4
C. IPv6
D. Appletalk

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 540
Who should be contacted FIRST in the event of a security breach?

A. Forensics analysis team
B. Internal auditors

C. Incident response team

D. Software vendors

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 541
A security administrator examines a network session to a compromised database server with a packet analyzer. Within the session there is a repeated series of the hex character 90 (x90).

Which of the following attack types has occurred?

A. Buffer overflow

B. Cross-site scripting

C. XML injection

D. SQL injection

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 542
Which of the following is an example of a false negative?

A. The IDS does not identify a buffer overflow.

B. Anti-virus identifies a benign application as malware.

C. Anti-virus protection interferes with the normal operation of an application.

D. A user account is locked out after the user mistypes the password too many times.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 543
Which of the following access controls enforces permissions based on data labeling at specific levels?

A. Mandatory access control
B. Separation of duties access control
C. Discretionary access control
D. Role based access control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 544
Sara, a security administrator, manually hashes all network device configuration files daily and compares them to the previous days' hashes. Which of the following security concepts is Sara using?

A. Confidentiality
B. Compliance
C. Integrity
D. Availability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 545
Which of the following would be used to identify the security posture of a network without actually exploiting any weaknesses?

A. Penetration test

B. Code review
C. Vulnerability scan
D. Brute Force scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 546
Which of the following authentication services uses a ticket granting system to provide access?

A. RADIUS
B. LDAP
C. TACACS+
D. Kerberos

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 547
Matt, a security administrator, wants to configure all the switches and routers in the network in order to securely monitor their status. Which of the following protocols would he need to configure on each device?

A. SMTP
B. SNMPv3
C. IPSec
D. SNMP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 325
CompTIA SY0-401 Exam

QUESTION 548
Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access. Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO).

A. Disable the wired ports
B. Use channels 1, 4 and 7 only
C. Enable MAC filtering
D. Disable SSID broadcast
E. Switch from 802.11a to 802.11b

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 549
The public key is used to perform which of the following? (Select THREE).

A. Validate the CRL
B. Validate the identity of an email sender
C. Encrypt messages
D. Perform key recovery
E. Decrypt messages
F. Perform key escrow

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 550
Which of the following is BEST used to break a group of IP addresses into smaller network segments or blocks?

A. NAT
B. Virtualization
C. NAC
D. Subnetting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
answer is well modified.

QUESTION 551
Which of the following would BEST be used to calculate the expected loss of an event, if the likelihood of an event occurring is known? (Select TWO).

A. DAC
B. ALE
C. SLE
D. ARO
E. ROI

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 552
An administrator wants to minimize the amount of time needed to perform backups during the week. It is also acceptable to the administrator for restoration to take an extended time frame.

Which of the following strategies would the administrator MOST likely implement?

A. Full backups on the weekend and incremental during the week

B. Full backups on the weekend and full backups every day
C. Incremental backups on the weekend and differential backups every day
D. Differential backups on the weekend and full backups every day

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 553
Which of the following can be utilized in order to provide temporary IT support during a disaster, where the organization sets aside funds for contingencies, but does not necessarily have a dedicated site to restore those services?

A. Hot site
B. Warm site
C. Cold site
D. Mobile site

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 554
Which of the following is BEST utilized to identify common misconfigurations throughout the enterprise?

A. Vulnerability scanning
B. Port scanning
C. Penetration testing
D. Black box

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 555
Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

A. CCTV system access
B. Dial-up access
C. Changing environmental controls
D. Ping of death

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 556
Which of the following policies is implemented in order to minimize data loss or theft?

A. PII handling
B. Password policy
C. Chain of custody
D. Zero day exploits

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 557
Which of the following provides the HIGHEST level of confidentiality on a wireless network?

A. Disabling SSID broadcast
B. MAC filtering
C. WPA2
D. Packet switching

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 558
A security administrator is aware that a portion of the company's Internet-facing network tends to be non-secure due to poorly configured and patched systems. The business owner has accepted the risk of those systems being compromised, but the administrator wants to determine the degree to which those systems can be used to gain access to the company intranet. Which of the following should the administrator perform?

A. Patch management assessment
B. Business impact assessment
C. Penetration test
D. Vulnerability assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 559
Which of the following should be implemented to stop an attacker from mapping out addresses

and/or devices on a network?

A. Single sign on
B. IPv6
C. Secure zone transfers
D. VoIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 560
Sara, the Chief Information Officer (CIO), has requested an audit take place to determine what services and operating systems are running on the corporate network. Which of the following should be used to complete this task?

A. Fingerprinting and password crackers
B. Fuzzing and a port scan
C. Vulnerability scan and fuzzing
D. Port scan and fingerprinting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 561
Matt, a systems security engineer, is determining which credential-type authentication to use within a planned 802.1x deployment. He is looking for a method that does not require a client certificate, has a server side certificate, and uses TLS tunnels for encryption. Which credential type authentication method BEST fits these requirements?

A. EAP-TLS
B. EAP-FAST
C. PEAP-CHAP
D. PEAP-MSCHAPv2

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
corrected and modified.

QUESTION 562
Matt, the Chief Information Security Officer (CISO), tells the network administrator that a security company has been hired to perform a penetration test against his network. The security company asks Matt which type of testing would be most beneficial for him. Which of the following BEST describes what the security company might do during a black box test?

A. The security company is provided with all network ranges, security devices in place, and logical maps of the network.
B. The security company is provided with no information about the corporate network or physical locations.
C. The security company is provided with limited information on the network, including all network diagrams.
D. The security company is provided with limited information on the network, including some subnet ranges and logical network diagrams.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 563
Corporate IM presents multiple concerns to enterprise IT. Which of the following concerns should Jane, the IT security manager, ensure are under control? (Select THREE).

A. Authentication
B. Data leakage
C. Compliance
D. Malware

E. Non-repudiation

F. Network loading

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 564
Account lockout is a mitigation strategy used by Jane, the administrator, to combat which of the following attacks? (Select TWO).

A. Spoofing

B. Man-in-the-middle

C. Dictionary

D. Brute force

E. Privilege escalation

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 565
Which of the following controls mitigates the risk of Matt, an attacker, gaining access to a company network by using a former employee's credential?

A. Account expiration

B. Password complexity

C. Account lockout

D. Dual factor authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 566
Pete, the Chief Executive Officer (CEO) of a company, has increased his travel plans for the next two years to improve business relations. Which of the following would need to be in place in case something happens to Pete?

A. Succession planning
B. Disaster recovery
C. Separation of duty
D. Removing single loss expectancy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 567
In order to prevent and detect fraud, which of the following should be implemented?

A. Job rotation
B. Risk analysis
C. Incident management
D. Employee evaluations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 568
Which of the following BEST represents the goal of a vulnerability assessment?

A. To test how a system reacts to known threats
B. To reduce the likelihood of exploitation
C. To determine the system's security posture
D. To analyze risk mitigation strategies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 569
An administrator notices an unusual spike in network traffic from many sources. The administrator suspects that:

A. it is being caused by the presence of a rogue access point.
B. it is the beginning of a DDoS attack.
C. the IDS has been compromised.
D. the internal DNS tables have been poisoned.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 570
A customer service department has a business need to send high volumes of confidential information to customers electronically. All emails go through a DLP scanner. Which of the following is the BEST solution to meet the business needs and protect confidential information?

A. Automatically encrypt impacted outgoing emails
B. Automatically encrypt impacted incoming emails
C. Monitor impacted outgoing emails
D. Prevent impacted outgoing emails

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 571
Which of the following cryptographic algorithms is MOST often used with IPSec?

A. Blowfish
B. Twofish
C. RC4
D. HMAC

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 572
Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

A. Common access card
B. Role based access control
C. Discretionary access control
D. Mandatory access control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 573

Pete, a security administrator, has observed repeated attempts to break into the network. Which of the following is designed to stop an intrusion on the network?

Real 334
CompTIA SY0-401 Exam

A. NIPS
B. HIDS
C. HIPS
D. NIDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 574
Which of the following would Pete, a security administrator, MOST likely implement in order to allow employees to have secure remote access to certain internal network services such as file servers?

A. Packet filtering firewall
B. VPN gateway
C. Switch
D. Router

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 575
Which of the following should be done before resetting a user's password due to expiration?

A. Verify the user's domain membership.
B. Verify the user's identity.
C. Advise the user of new policies.

D. Verify the proper group membership.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 576
Which of the following hardware based encryption devices is used as a part of multi-factor authentication to access a secured computing system?

A. Database encryption
B. USB encryption
C. Whole disk encryption
D. TPM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 577
Establishing a published chart of roles, responsibilities, and chain of command to be used during a disaster is an example of which of the following?

A. Fault tolerance
B. Succession planning
C. Business continuity testing
D. Recovery point objectives

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 578
In PKI, a key pair consists of: (Select TWO).

A. A key ring
B. A public key
C. A private key
D. Key escrow
E. A passphrase

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 579
Speaking a passphrase into a voice print analyzer is an example of which of the following security concepts?

Real 336
CompTIA SY0-401 Exam

A. Two factor authentication
B. Identification and authorization
C. Single sign-on
D. Single factor authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 580
Which of the following secure file transfer methods uses port 22 by default?

A. FTPS
B. SFTP
C. SSL
D. S/MIME

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 581
While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?

A. EAP-TLS
B. PEAP
C. WEP
D. WPA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 582
Due to limited resources, a company must reduce their hardware budget while still maintaining availability. Which of the following would MOST likely help them achieve their objectives?

A. Virtualization
B. Remote access
C. Network access control
D. Blade servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 583
A user has several random browser windows opening on their computer. Which of the following programs can be installed on his machine to help prevent this from happening?

A. Antivirus
B. Pop-up blocker
C. Spyware blocker
D. Anti-spam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 584
A company is installing a new security measure that would allow one person at a time to be authenticated to an area without human interaction. Which of the following does this describe?

A. Fencing
B. Mantrap
C. A guard
D. Video surveillance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 585
When employees that use certificates leave the company they should be added to which of the following?

Real 338
CompTIA SY0-401 Exam

A. PKI
B. CA
C. CRL
D. TKIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 586
Several departments within a company have a business need to send high volumes of confidential information to customers via email. Which of the following is the BEST solution to mitigate unintentional exposure of confidential information?

A. Employ encryption on all outbound emails containing confidential information.
B. Employ exact data matching and prevent inbound emails with Data Loss Prevention.
C. Employ hashing on all outbound emails containing confidential information.
D. Employ exact data matching and encrypt inbound e-mails with Data Loss Prevention.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 587
An administrator is looking to implement a security device which will be able to not only detect network intrusions at the organization level, but help defend against them as well. Which of the following is being described here?

A. NIDS
B. NIPS
C. HIPS
D. HIDS

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 588
A company has implemented PPTP as a VPN solution. Which of the following ports would need to be opened on the firewall in order for this VPN to function properly? (Select TWO).

A. UDP 1723
B. TCP 500
C. TCP 1723
D. UDP 47
E. TCP 47

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 589
Mike, a user, states that he is receiving several unwanted emails about home loans. Which of the following is this an example of?

A. Spear phishing
B. Hoaxes
C. Spoofing

D. Spam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 590
Which of the following must a user implement if they want to send a secret message to a coworker by embedding it within an image?

A. Transport encryption
B. Steganography
C. Hashing
D. Digital signature

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 591
Real 340
CompTIA SY0-401 Exam
Pete, a network administrator, is implementing IPv6 in the DMZ. Which of the following protocols must he allow through the firewall to ensure the web servers can be reached via IPv6 from an IPv6 enabled Internet host?

A. TCP port 443 and IP protocol 46
B. TCP port 80 and TCP port 443
C. TCP port 80 and ICMP
D. TCP port 443 and SNMP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 592
Sara, a security technician, has received notice that a vendor coming in for a presentation will require access to a server outside of the network. Currently, users are only able to access remote sites through a VPN connection. How could Sara BEST accommodate the vendor?

A. Allow incoming IPSec traffic into the vendor's IP address.
B. Set up a VPN account for the vendor, allowing access to the remote site.
C. Turn off the firewall while the vendor is in the office, allowing access to the remote site.
D. Write a firewall rule to allow the vendor to have access to the remote site.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 593
Which of the following is the BEST method for ensuring all files and folders are encrypted on all corporate laptops where the file structures are unknown?

A. Folder encryption
B. File encryption
C. Whole disk encryption
D. Steganography

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 594
Encryption used by RADIUS is BEST described as:

A. Quantum
B. Elliptical curve

C. Asymmetric

D. Symmetric

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 595
Which of the following is used by the recipient of a digitally signed email to verify the identity of the sender?

A. Recipient's private key

B. Sender's public key

C. Recipient's public key

D. Sender's private key

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 596
A security analyst has been tasked with securing a guest wireless network. They recommend the company use an authentication server but are told the funds are not available to set this up.

Which of the following BEST allows the analyst to restrict user access to approved devices?

A. Antenna placement

B. Power level adjustment

C. Disable SSID broadcasting

D. MAC filtering

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
answer is modified.

QUESTION 597
A supervisor in the human resources department has been given additional job duties in the accounting department. Part of their new duties will be to check the daily balance sheet calculations on spreadsheets that are restricted to the accounting group. In which of the following ways should the account be handled?

A. The supervisor should be allowed to have access to the spreadsheet files, and their membership in the human resources group should be terminated.
B. The supervisor should be removed from the human resources group and added to the accounting group.
C. The supervisor should be added to the accounting group while maintaining their membership in the human resources group.
D. The supervisor should only maintain membership in the human resources group.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 598
Which of the following security benefits would be gained by disabling a terminated user account rather than deleting it?

A. Retention of user keys
B. Increased logging on access attempts
C. Retention of user directories and files
D. Access to quarantined files

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 599
Which of the following security architecture elements also has sniffer functionality? (Select TWO).

A. HSM

B. IPS

C. SSL accelerator
Real 343
CompTIA SY0-401 Exam

D. WAP

E. IDS

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 600
Jane, an IT security technician, needs to create a way to secure company mobile devices. Which of the following BEST meets this need?

A. Implement voice encryption, pop-up blockers, and host-based firewalls.

B. Implement firewalls, network access control, and strong passwords.

C. Implement screen locks, device encryption, and remote wipe capabilities.

D. Implement application patch management, antivirus, and locking cabinets.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 601
Which of the following should a security technician implement to identify untrusted certificates?

A. CA

B. PKI

C. CRL

D. Recovery agent

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 602
Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?

A. Certification authority
B. Key escrow

C. Certificate revocation list
D. Registration authority

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 603
Sara, a security engineer, is testing encryption ciphers for performance. Which of the following ciphers offers strong encryption with the FASTEST speed?

A. 3DES
B. Blowfish
C. Serpent
D. AES256

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 604
Which of the following is an authentication method that can be secured by using SSL?

A. RADIUS
B. LDAP
C. TACACS+
D. Kerberos

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 605
The Chief Security Officer (CSO) is concerned about misuse of company assets and wishes to determine who may be responsible. Which of the following would be the BEST course of action?

A. Create a single, shared user account for every system that is audited and logged based upon time of use.

B. Implement a single sign-on application on equipment with sensitive data and high-profile shares.
C. Enact a policy that employees must use their vacation time in a staggered schedule.
D. Separate employees into teams led by a person who acts as a single point of contact for observation purposes.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 606
Jane, a VPN administrator, was asked to implement an encryption cipher with a MINIMUM effective security of 128-bits. Which of the following should Jane select for the tunnel encryption?

A. Blowfish
B. DES
C. SHA256
D. HMAC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 607
Which of the following uses both a public and private key?

A. RSA
B. AES
C. MD5
D. SHA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 608
Which of the following would Matt, a security administrator, use to encrypt transmissions from an internal database to an internal server, keeping in mind that the encryption process must add as little latency to the process as possible?

A. ECC
B. RSA
C. SHA
D. 3DES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 609
A database administrator receives a call on an outside telephone line from a person who states that they work for a well-known database vendor. The caller states there have been problems applying the newly released vulnerability patch for their database system, and asks what version is being used so that they can assist. Which of the following is the BEST action for the administrator to take?

A. Thank the caller, report the contact to the manager, and contact the vendor support line to verify any reported patch issues.
B. Obtain the vendor's email and phone number and call them back after identifying the number of systems affected by the patch.
C. Give the caller the database version and patch level so that they can receive help applying the patch.
D. Call the police to report the contact about the database systems, and then check system logs for attack attempts.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 610
The datacenter manager is reviewing a problem with a humidity factor that is too low. Which of the following environmental problems may occur?

A. EMI emanations
B. Static electricity
C. Condensation
D. Dry-pipe fire suppression

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 611
A UNIX administrator would like to use native commands to provide a secure way of connecting to other devices remotely and to securely transfer files. Which of the following protocols could be utilized? (Select TWO).

A. RDP
B. SNMP
C. FTP
D. SCP
E. SSH

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 612
A network administrator has purchased two devices that will act as failovers for each other. Which of the following concepts does this BEST illustrate?

A. Authentication
B. Integrity
C. Confidentiality
D. Availability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 613
Matt, the network engineer, has been tasked with separating network traffic between virtual machines on a single hypervisor. Which of the following would he implement to BEST address this requirement? (Select TWO).

A. Virtual switch
B. NAT
C. System partitioning
Real 348
CompTIA SY0-401 Exam
D. Access-list

E. Disable spanning tree
F. VLAN

Correct Answer: AF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 614
Which of the following BEST describes a demilitarized zone?

A. A buffer zone between protected and unprotected networks.
B. A network where all servers exist and are monitored.
C. A sterile, isolated network segment with access lists.
D. A private network that is protected by a firewall and a VLAN.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 615
XYZ Corporation is about to purchase another company to expand its operations. The CEO is concerned about information leaking out, especially with the cleaning crew that comes in at night.

The CEO would like to ensure no paper files are leaked. Which of the following is the BEST policy to implement?

A. Social media policy
B. Data retention policy
C. CCTV policy
D. Clean desk policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 616
In intrusion detection system vernacular, which account is responsible for setting the security

policy for an organization?

A. Supervisor
B. Administrator
C. Root
D. Director

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 617
Which of the following is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead?

A. Enticement
B. Entrapment
C. Deceit
D. Sting

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 618

Which of the following types of logs could provide clues that someone has been attempting to compromise the SQL Server database?

A. Event
B. SQL_LOG
C. Security
D. Access

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 619
Real 350
CompTIA SY0-401 Exam
Pete, the system administrator, has concerns regarding users losing their company provided

smartphones. Pete's focus is on equipment recovery. Which of the following BEST addresses his concerns?

A. Enforce device passwords.
B. Use remote sanitation.
C. Enable GPS tracking.
D. Encrypt stored data.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 620
A security administrator wants to deploy security controls to mitigate the threat of company employees' personal information being captured online. Which of the following would BEST serve this purpose?

A. Anti-spyware
B. Antivirus

C. Host-based firewall
D. Web content filter

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 621
Which of the following statements is MOST likely to be included in the security awareness training about P2P?

A. P2P is always used to download copyrighted material.
B. P2P can be used to improve computer system response.
C. P2P may prevent viruses from entering the network.
D. P2P may cause excessive network bandwidth.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 622
A company's chief information officer (CIO) has analyzed the financial loss associated with the company's database breach. They calculated that one single breach could cost the company $1,000,000 at a minimum. Which of the following documents is the CIO MOST likely updating?

A. Succession plan
B. Continuity of operation plan

C. Disaster recovery plan
D. Business impact analysis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 623
After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service?

A. Succession planning
B. Disaster recovery plan
C. Information security plan
D. Business impact analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 624
Which of the following wireless protocols could be vulnerable to a brute-force password attack? (Select TWO).

A. WPA2-PSK
B. WPA - EAP - TLS
C. WPA2-CCMP
D. WPA -CCMP
E. WPA - LEAP
Real 352
CompTIA SY0-401 Exam
F. WEP

Correct Answer: AE
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 625
An auditor is given access to a conference room to conduct an analysis. When they connect their laptop's Ethernet cable into the wall jack, they are not able to get a connection to the Internet but have a link light. Which of the following is MOST likely causing this issue?

A. Ethernet cable is damaged
B. The host firewall is set to disallow outbound connections
C. Network Access Control
D. The switch port is administratively shutdown

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 626
Which of the following types of trust models is used by a PKI?

A. Transitive
B. Open source
C. Decentralized
D. Centralized

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 627
A technician has implemented a system in which all workstations on the network will receive security updates on the same schedule. Which of the following concepts does this illustrate?

A. Patch management

B. Application hardening
Real 353
CompTIA SY0-401 Exam

C. White box testing

D. Black box testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 628
Which of the following offers the LEAST amount of protection against data theft by USB drives?

A. DLP

B. Database encryption

C. TPM

D. Cloud computing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 629
A security administrator develops a web page and limits input into their fields on the web page as well as filters special characters in output. The administrator is trying to prevent which of the following attacks?

A. Spoofing

B. XSS

C. Fuzzing

D. Pharming

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 630
Sara, a hacker, is completing a website form to request a free coupon. The site has a field that limits the request to 3 or fewer coupons. While submitting the form, Sara runs an application on her machine to intercept the HTTP POST command and change the field from 3 coupons to 30.

Real 354
CompTIA SY0-401 Exam
Which of the following was used to perform this attack?

A. SQL injection
B. XML injection
C. Packet sniffer
D. Proxy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 631
Several users report to the administrator that they are having issues downloading files from the file server. Which of the following assessment tools can be used to determine if there is an issue with the file server?

A. MAC filter list
B. Recovery agent
C. Baselines
D. Access list

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 632
When a new network drop was installed, the cable was run across several fluorescent lights. The users of the new network drop experience intermittent connectivity. Which of the following environmental controls was MOST likely overlooked during installation?

A. Humidity sensors
B. EMI shielding
C. Channel interference
D. Cable kinking

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 633
An administrator configures all wireless access points to make use of a new network certificate authority. Which of the following is being used?

A. WEP
B. LEAP
C. EAP-TLS
D. TKIP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 634
A security analyst noticed a colleague typing the following command:

`Telnet some-host 443'

Which of the following was the colleague performing?

A. A hacking attempt to the some-host web server with the purpose of achieving a distributed denial of service attack.
B. A quick test to see if there is a service running on some-host TCP/443, which is being routed correctly and not blocked by a firewall.
C. Trying to establish an insecure remote management session. The colleague should be using SSH or terminal services instead.
D. A mistaken port being entered because telnet servers typically do not listen on port 443.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 635
An information bank has been established to store contacts, phone numbers and other records.

An application running on UNIX would like to connect to this index server using port 88. Which of the following authentication services would this use this port by default?

Real 356
CompTIA SY0-401 Exam

A. Kerberos
B. TACACS+
C. Radius
D. LDAP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 636
A database administrator contacts a security administrator to request firewall changes for a connection to a new internal application. The security administrator notices that the new application uses a port typically monopolized by a virus. The security administrator denies the request and suggests a new port or service be used to complete the application's task. Which of the following is the security administrator practicing in this example?

A. Explicit deny
B. Port security
C. Access control lists
D. Implicit deny

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 637
Which of the following BEST describes a SQL Injection attack?

A. The attacker attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information.
B. The attacker attempts to have the receiving server run a payload using programming commonly found on web servers.
C. The attacker overwhelms a system or application, causing it to crash and bring the server down to cause an outage.
D. The attacker overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 638
Digital signatures are used for ensuring which of the following items? (Select TWO).

A. Confidentiality
B. Integrity
C. Non-Repudiation
D. Availability
E. Algorithm strength

Correct Answer: BC
Section: (none)

Explanation

Explanation/Reference:
answer is verified.

QUESTION 639
Matt, an administrator, is concerned about the wireless network being discovered by war driving.

Which of the following can be done to mitigate this?

A. Enforce a policy for all users to authentic through a biometric device.
B. Disable all SSID broadcasting.
C. Ensure all access points are running the latest firmware.
D. Move all access points into public access areas.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 640
A company wants to ensure that its hot site is prepared and functioning. Which of the following would be the BEST process to verify the backup datacenter is prepared for such a scenario?

A. Site visit to the backup data center
B. Disaster recovery plan review
C. Disaster recovery exercise
D. Restore from backup

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 641
Which of the following are restricted to 64-bit block sizes? (Select TWO).

A. PGP
B. DES
C. AES256
D. RSA
E. 3DES
F. AES

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 642
Public keys are used for which of the following?

A. Decrypting wireless messages
B. Decrypting the hash of an electronic signature
C. Bulk encryption of IP based email traffic
D. Encrypting web browser traffic

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 643
Which of the following is a requirement when implementing PKI if data loss is unacceptable?

A. Web of trust
B. Non-repudiation
C. Key escrow
D. Certificate revocation list

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
appropriate answer.

QUESTION 644
Which of the following is true about PKI? (Select TWO).

A. When encrypting a message with the public key, only the public key can decrypt it.
B. When encrypting a message with the private key, only the private key can decrypt it.
C. When encrypting a message with the public key, only the CA can decrypt it.
D. When encrypting a message with the public key, only the private key can decrypt it.
E. When encrypting a message with the private key, only the public key can decrypt it.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 645
The recovery agent is used to recover the:

A. Root certificate
B. Key in escrow
C. Public key
D. Private key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 646

Which of the following is true about the CRL?

A. It should be kept public
B. It signs other keys
C. It must be kept secret
D. It must be encrypted

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 647
A password history value of three means which of the following?

A. Three different passwords are used before one can be reused.
B. A password cannot be reused once changed for three years.
C. After three hours a password must be re-entered to continue.
D. The server stores passwords in the database for three days.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 648
A user has forgotten their account password. Which of the following is the BEST recovery strategy?

A. Upgrade the authentication system to use biometrics instead.
B. Temporarily disable password complexity requirements.
C. Set a temporary password that expires upon first use.
D. Retrieve the user password from the credentials database.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 649
Allowing unauthorized removable devices to connect to computers increases the risk of which of the following?

A. Data leakage prevention
B. Data exfiltration
C. Data classification
D. Data deduplication

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 650
A computer is put into a restricted VLAN until the computer's virus definitions are up-to-date.

Which of the following BEST describes this system type?

A. NAT
B. NIPS
C. NAC
D. DMZ

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 651

A technician is investigating intermittent switch degradation. The issue only seems to occur when the buildings roof air conditioning system runs. Which of the following would reduce the connectivity issues?

A. Adding a heat deflector
B. Redundant HVAC systems
C. Shielding
D. Add a wireless network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 652
According to company policy an administrator must logically keep the Human Resources department separated from the Accounting department. Which of the following would be the simplest way to accomplish this?

A. NIDS
B. DMZ
C. NAT
D. VLAN

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 653
Which of the following tools will allow a technician to detect security-related TCP connection anomalies?

A. Logical token
B. Performance monitor
C. Public key infrastructure
D. Trusted platform module

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 654
A technician is reviewing the logical access control method an organization uses. One of the senior managers requests that the technician prevent staff members from logging on during nonworking days. Which of the following should the technician implement to meet managements request?

A. Enforce Kerberos
B. Deploy smart cards
C. Time of day restrictions
D. Access control lists

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 655
Without validating user input, an application becomes vulnerable to all of the following EXCEPT:

A. Buffer overflow.
B. Command injection.
C. Spear phishing.
D. SQL injection.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 656

To protect corporate data on removable media, a security policy should mandate that all removable devices use which of the following?

A. Full disk encryption
B. Application isolation
C. Digital rights management
D. Data execution prevention

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 657
Which of the following wireless security technologies continuously supplies new keys for WEP?

A. TKIP
B. Mac filtering
C. WPA2
D. WPA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 658
Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company?

A. Rootkit
B. Logic bomb
C. Worm
D. Botnet

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 659
Which of the following application security principles involves inputting random data into a program?

A. Brute force attack
B. Sniffing
C. Fuzzing
D. Buffer overflow

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 660
Which of the following is an important step in the initial stages of deploying a host-based firewall?

A. Selecting identification versus authentication
B. Determining the list of exceptions
C. Choosing an encryption algorithm
D. Setting time of day restrictions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 661
Identifying a list of all approved software on a system is a step in which of the following practices?

A. Passively testing security controls
B. Application hardening
C. Host software baselining
D. Client-side targeting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
answer is updated.

QUESTION 662
Which of the following BEST describes using a smart card and typing in a PIN to gain access to a system?

A. Biometrics
B. PKI
C. Single factor authentication
D. Multifactor authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 663
An administrator has advised against the use of Bluetooth phones due to bluesnarfing concerns.

Which of the following is an example of this threat?

A. An attacker using the phone remotely for spoofing other phone numbers
B. Unauthorized intrusions into the phone to access data
C. The Bluetooth enabled phone causing signal interference with the network
D. An attacker using exploits that allow the phone to be disabled

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 664
Which of the following is the difference between identification and authentication of a user?

A. Identification tells who the user is and authentication tells whether the user is allowed to logon to a system.
B. Identification tells who the user is and authentication proves it.
C. Identification proves who the user is and authentication is used to keep the users data secure.
D. Identification proves who the user is and authentication tells the user what they are allowed to do.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 665
The marketing department wants to distribute pens with embedded USB drives to clients. In the past this client has been victimized by social engineering attacks which led to a loss of sensitive data. The security administrator advises the marketing department not to distribute the USB pens due to which of the following?

A. The risks associated with the large capacity of USB drives and their concealable nature
B. The security costs associated with securing the USB drives over time
C. The cost associated with distributing a large volume of the USB pens
D. The security risks associated with combining USB drives and cell phones on a network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 666
An administrator wishes to hide the network addresses of an internal network when connecting to the Internet. The MOST effective way to mask the network address of the users would be by passing the traffic through a:

A. stateful firewall

B. packet-filtering firewall

C. NIPS

D. NAT

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 667
A security administrator forgets their card to access the server room. The administrator asks a coworker if they could use their card for the day. Which of the following is the administrator using
to gain access to the server room?

A. Man-in-the-middle

B. Tailgating

C. Impersonation

D. Spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 668
A security administrator has implemented a policy to prevent data loss. Which of the following is the BEST method of enforcement?

A. Internet networks can be accessed via personally-owned computers.

B. Data can only be stored on local workstations.

C. Wi-Fi networks should use WEP encryption by default.

D. Only USB devices supporting encryption are to be used.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 669
Symmetric encryption utilizes __________, while asymmetric encryption utilizes _________.

A. Public keys, one time
B. Shared keys, private keys
C. Private keys, session keys
D. Private keys, public keys

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 670
The main corporate website has a service level agreement that requires availability 100% of the time, even in the case of a disaster. Which of the following would be required to meet this demand?

A. Warm site implementation for the datacenter
B. Geographically disparate site redundant datacenter
C. Localized clustering of the datacenter
D. Cold site implementation for the datacenter

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 671
Which of the following is a vulnerability associated with disabling pop-up blockers?

A. An alert message from the administrator may not be visible
B. A form submitted by the user may not open
C. The help window may not be displayed
D. Another browser instance may execute malicious code

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 672
A security technician needs to open ports on a firewall to allow for domain name resolution.

Which of the following ports should be opened? (Select TWO).

A. TCP 21
B. TCP 23
C. TCP 53
D. UDP 23
E. UDP 53

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
answer is valid.

QUESTION 673
During an anonymous penetration test, Jane, a system administrator, was able to identify a shared print spool directory, and was able to download a document from the spool. Which statement BEST describes her privileges?

A. All users have write access to the directory.
B. Jane has read access to the file.
C. All users have read access to the file.

D. Jane has read access to the directory.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 674
An IT security technician is actively involved in identifying coding issues for her company.

Which of the following is an application security technique that can be used to identify unknown weaknesses within the code?

A. Vulnerability scanning
B. Denial of service
C. Fuzzing
D. Port scanning

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 675
Which of the following data security techniques will allow Matt, an IT security technician, to encrypt a system with speed as its primary consideration?

A. Hard drive encryption
B. Infrastructure as a service
C. Software based encryption
D. Data loss prevention

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 676
Matt, a forensic analyst, wants to obtain the digital fingerprint for a given message. The message is 160-bits long. Which of the following hashing methods would Matt have to use to obtain this digital fingerprint?

A. SHA1
B. MD2
C. MD4
D. MD5

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 677
A system administrator is notified by a staff member that their laptop has been lost. The laptop contains the user's digital certificate. Which of the following will help resolve the issue? (Select TWO).

A. Revoke the digital certificate
B. Mark the key as private and import it
C. Restore the certificate using a CRL
D. Issue a new digital certificate
E. Restore the certificate using a recovery agent

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 678
A security engineer is given new application extensions each month that need to be secured prior to implementation. They do not want the new extensions to invalidate or interfere with existing application security. Additionally, the engineer wants to ensure that the new requirements are approved by the appropriate personnel. Which of the following should be in place to meet these two goals? (Select TWO).

A. Patch Audit Policy
B. Change Control Policy
C. Incident Management Policy
D. Regression Testing Policy
E. Escalation Policy
F. Application Audit Policy

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 679
During an audit, the security administrator discovers that there are several users that are no longer employed with the company but still have active user accounts. Which of the following should be performed?

A. Account recovery
B. Account disablement
C. Account lockouts
D. Account expiration

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 680
A system administrator has concerns regarding their users accessing systems and secured areas using others' credentials. Which of the following can BEST address this concern?

A. Create conduct policies prohibiting sharing credentials.
B. Enforce a policy shortening the credential expiration timeframe.
C. Implement biometric readers on laptops and restricted areas.

D. Install security cameras in areas containing sensitive systems.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 681
A network administrator has a separate user account with rights to the domain administrator group. However, they cannot remember the password to this account and are not able to login to the server when needed. Which of the following is MOST accurate in describing the type of issue the administrator is experiencing?

A. Single sign-on
B. Authorization
C. Access control
D. Authentication

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 682
Jane has implemented an array of four servers to accomplish one specific task. This is BEST known as which of the following?

A. Clustering
B. RAID
C. Load balancing
D. Virtualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 683
Which of the following security account management techniques should a security analyst implement to prevent staff, who has switched company roles, from exceeding privileges?

A. Internal account audits
B. Account disablement
C. Time of day restriction
D. Password complexity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 684
To ensure compatibility with their flagship product, the security engineer is tasked to recommend an encryption cipher that will be compatible with the majority of third party software and hardware vendors. Which of the following should be recommended?

A. SHA
B. MD5
C. Blowfish
D. AES

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 685
After a new firewall has been installed, devices cannot obtain a new IP address. Which of the following ports should Matt, the security administrator, open on the firewall?

A. 25
B. 68

C. 80
D. 443

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 686
A system administrator has noticed that users change their password many times to cycle back to the original password when their passwords expire. Which of the following would BEST prevent this behavior?

A. Assign users passwords based upon job role.
B. Enforce a minimum password age policy.
C. Prevent users from choosing their own passwords.
D. Increase the password expiration time frame.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 687
The systems administrator notices that many employees are using passwords that can be easily guessed or are susceptible to brute force attacks. Which of the following would BEST mitigate this risk?

A. Enforce password rules requiring complexity.
B. Shorten the maximum life of account passwords.
C. Increase the minimum password length.
D. Enforce account lockout policies.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 688
Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are botnets and viruses. Which of the following explains the difference between these two types of malware?

A. Viruses are a subset of botnets which are used as part of SYN attacks.
B. Botnets are a subset of malware which are used as part of DDoS attacks.
C. Viruses are a class of malware which create hidden openings within an OS.
D. Botnets are used within DR to ensure network uptime and viruses are not.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 689
A security analyst implemented group-based privileges within the company active directory. Which of the following account management techniques should be undertaken regularly to ensure least privilege principles?

A. Leverage role-based access controls.
B. Perform user group clean-up.
C. Verify smart card access controls.
D. Verify SHA-256 for password hashes.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 690
A technician has just installed a new firewall onto the network. Users are reporting that they cannot reach any website. Upon further investigation, the technician determines that websites can be reached by entering their IP addresses. Which of the following ports may have been closed to cause this issue?

A. HTTP
B. DHCP
C. DNS
D. NetBIOS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 691
The system administrator has been notified that many users are having difficulty connecting to the company's wireless network. They take a new laptop and physically go to the access point and connect with no problems. Which of the following would be the MOST likely cause?

A. The certificate used to authenticate users has been compromised and revoked.
B. Multiple war drivers in the parking lot have exhausted all available IPs from the pool to deny access.
C. An attacker has gained access to the access point and has changed the encryption keys.
D. An unauthorized access point has been configured to operate on the same channel.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 692
The systems administrator wishes to implement a hardware-based encryption method that could also be used to sign code. They can achieve this by:

A. Utilizing the already present TPM.
B. Configuring secure application sandboxes.
C. Enforcing whole disk encryption.
D. Moving data and applications into the cloud.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 693
The Chief Information Security Officer (CISO) has mandated that all IT systems with credit card data be segregated from the main corporate network to prevent unauthorized access and that access to the IT systems should be logged. Which of the following would BEST meet the CISO's requirements?

A. Sniffers
B. NIDS
C. Firewalls
D. Web proxies
E. Layer 2 switches

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 694
One of the servers on the network stops responding due to lack of available memory. Server administrators did not have a clear definition of what action should have taken place based on the available memory. Which of the following would have BEST kept this incident from occurring?

A. Set up a protocol analyzer
B. Set up a performance baseline
C. Review the systems monitor on a monthly basis
D. Review the performance monitor on a monthly basis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 695
Used in conjunction, which of the following are PII? (Select TWO).

A. Marital status
B. Favorite movie
C. Pet's name
D. Birthday
E. Full name

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 696
Which of the following is the BEST way to prevent Cross-Site Request Forgery (XSRF) attacks?

A. Check the referrer field in the HTTP header
B. Disable Flash content
C. Use only cookies for authentication
D. Use only HTTPS URLs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 697
Which of the following practices is used to mitigate a known security vulnerability?

A. Application fuzzing
B. Patch management
C. Password cracking

D. Auditing security logs

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
answer is updated.

QUESTION 698
Real 378
CompTIA SY0-401 Exam
Which of the following would Jane, an administrator, use to detect an unknown security vulnerability?

A. Patch management
B. Application fuzzing
C. ID badge
D. Application configuration baseline

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 699
When reviewing a digital certificate for accuracy, which of the following would Matt, a security administrator, focus on to determine who affirms the identity of the certificate owner?

A. Trust models
B. CRL
C. CA
D. Recovery agent

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 700
Which of the following is a notification that an unusual condition exists and should be investigated?

A. Alert

B. Trend
C. Alarm
D. Trap

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 701
Real 379
CompTIA SY0-401 Exam
If you don't know the MAC address of a Linux-based machine, what command-line utility can you use to ascertain it?

A. macconfig
B. ifconfig
C. ipconfig
D. config

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 702
Users are utilizing thumb drives to connect to USB ports on company workstations. A technician is concerned that sensitive files can be copied to the USB drives. Which of the following mitigation techniques would address this concern? (Select TWO).

A. Disable the USB root hub within the OS.
B. Install anti-virus software on the USB drives.
C. Disable USB within the workstations BIOS.
D. Apply the concept of least privilege to USB devices.
E. Run spyware detection against all workstations.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 703
An administrator is assigned to monitor servers in a data center. A web server connected to the Internet suddenly experiences a large spike in CPU activity. Which of the following is the MOST likely cause?

A. Spyware
B. Trojan
C. Privilege escalation
D. DoS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 704
Why would a technician use a password cracker?

A. To look for weak passwords on the network
B. To change a users passwords when they leave the company
C. To enforce password complexity requirements
D. To change users passwords if they have forgotten them

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 705
Which of the following explains the difference between a public key and a private key?

A. The public key is only used by the client while the private key is available to all.
Both keys are mathematically related.
B. The private key only decrypts the data while the public key only encrypts the data.
Both keys are mathematically related.
C. The private key is commonly used in symmetric key decryption while the public key is used in asymmetric key decryption.
D. The private key is only used by the client and kept secret while the public key is available to all.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 706
Requiring technicians to report spyware infections is a step in which of the following?

A. Routine audits
B. Change management
C. Incident management
D. Clean desk policy

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 707
An organization is recovering data following a datacenter outage and determines that backup copies of files containing personal information were stored in an unsecure location, because the sensitivity was unknown. Which of the following activities should occur to prevent this in the future?

A. Business continuity planning
B. Quantitative assessment
C. Data classification
D. Qualitative assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 708
Which of the following provides the LEAST availability?

A. RAID 0
B. RAID 1
C. RAID 3
D. RAID 5

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 709
FTP/S uses which of the following TCP ports by default?

A. 20 and 21
B. 139 and 445
C. 443 and 22
D. 989 and 990

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 710
Which of the following is mainly used for remote access into the network?

A. XTACACS
B. TACACS+
C. Kerberos
D. RADIUS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 711
Which of the following types of data encryption would Matt, a security administrator, use to encrypt a specific table?

A. Full disk
B. Individual files
C. Database
D. Removable media

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 712
Several users' computers are no longer responding normally and sending out spam email to the users' entire contact list. This is an example of which of the following?

A. Trojan virus
B. Botnet
C. Worm outbreak
D. Logic bomb

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Real 383
CompTIA SY0-401 Exam

Explanation:

QUESTION 713
Sara, an attacker, is recording a person typing in their ID number into a keypad to gain access to the building. Sara then calls the helpdesk and informs them that their PIN no longer works and would like to change it. Which of the following attacks occurred LAST?

A. Phishing
B. Shoulder surfing
C. Impersonation
D. Tailgating

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 714
A company replaces a number of devices with a mobile appliance, combining several functions.

Which of the following descriptions fits this new implementation? (Select TWO).

A. Cloud computing
B. Virtualization
C. All-in-one device
D. Load balancing
E. Single point of failure

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 715
Which of the following risks could IT management be mitigating by removing an all-in-one device?

A. Continuity of operations
B. Input validation
C. Single point of failure
Real 384
CompTIA SY0-401 Exam
D. Single sign on

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 716
Which of the following could a security administrator implement to mitigate the risk of tailgating for a large organization?

A. Train employees on correct data disposal techniques and enforce policies.

B. Only allow employees to enter or leave through one door at specified times of the day.
C. Only allow employees to go on break one at a time and post security guards 24/7 at each entrance.
D. Train employees on risks associated with social engineering attacks and enforce policies.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 717
Which of the following concepts defines the requirement for data availability?

A. Authentication to RADIUS
B. Non-repudiation of email messages
C. Disaster recovery planning
D. Encryption of email messages

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 718
Pete, a security engineer, is trying to inventory all servers in a rack. The engineer launches RDP sessions to five different PCs and notices that the hardware properties are similar. Additionally, the MAC addresses of all five servers appear on the same switch port. Which of the following is MOST likely the cause?

A. The system is running 802.1x.
B. The system is using NAC.
C. The system is in active-standby mode.
D. The system is virtualized.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 719
Sara, a security administrator, is noticing a slow down in the wireless network response. Sara launches a wireless sniffer and sees a large number of ARP packets being sent to the AP. Which of the following type of attacks is underway?

A. IV attack
B. Interference
C. Blue jacking
D. Packet sniffing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 720
Pete, the security administrator, has been notified by the IDS that the company website is under attack. Analysis of the web logs show the following string, indicating a user is trying to post a comment on the public bulletin board.

INSERT INTO message `<script>source=http://evilsite</script>

This is an example of which of the following?

A. XSS attack
B. XML injection attack
C. Buffer overflow attack
D. SQL injection attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
answer is verified.

QUESTION 721

Which of the following techniques describes the use of application isolation during execution to prevent system compromise if the application is compromised?

A. Least privilege
B. Sandboxing
C. Black box
D. Application hardening

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 722
Matt, an IT administrator, wants to protect a newly built server from zero day attacks. Which of the following would provide the BEST level of protection?

A. HIPS
B. Antivirus
C. NIDS
D. ACL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 723
Jane, an IT administrator, is implementing security controls on a Microsoft Windows based kiosk used at a bank branch. This kiosk is used by the public for Internet banking. Which of the following controls will BEST protect the kiosk from general public users making system changes?

A. Group policy implementation
B. Warning banners
C. Command shell restrictions
D. Host based firewall

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Q1000
Sara, the Chief Information Officer (CIO), has tasked the IT department with redesigning the network to rely less on perimeter firewalls, to implement a standard operating environment for client devices, and to disallow personally managed devices on the network. Which of the following is Sara's GREATEST concern?

A. Malicious internal attacks
B. Data exfiltration
C. Audit findings
D. Incident response

Answer: B

Explanation:
Q1001
Which of the following data loss prevention strategies mitigates the risk of replacing hard drives that cannot be sanitized?

A. Virtualization
B. Patch management
C. Full disk encryption
D. Database encryption

Answer: C

Explanation:
Q1002
Which of the following does Jane, a software developer, need to do after compiling the source code of a program to attest the authorship of the binary?

A. Place Jane's name in the binary metadata
B. Use Jane's private key to sign the binary
C. Use Jane's public key to sign the binary

D. Append the source code to the binary

Answer: B

Explanation:
Q1003
The annual loss expectancy can be calculated by:

A. Dividing the annualized rate of return by single loss expectancy.
B. Multiplying the annualized rate of return and the single loss expectancy.
C. Subtracting the single loss expectancy from the annualized rate of return.
D. Adding the single loss expectancy and the annualized rate of return.

Answer: B

Explanation:
Q1004
Which of the following should Jane, the security administrator, do FIRST when an employee reports the loss of a corporate mobile device?

A. Remotely lock the device with a PIN
B. Enable GPS location and record from the camera
C. Remotely uninstall all company software
D. Remotely initiate a device wipe

Answer: D

Explanation:
Q1005
An application company sent out a software patch for one of their applications on Monday. The company has been receiving reports about intrusion attacks from their customers on Tuesday.

Which of the following attacks does this describe?

A. Zero day

B. Directory traversal
C. Logic bomb
D. Session hijacking

Answer: A

Explanation:
Q1006
Which of the following protocols would be implemented to secure file transfers using SSL?

A. TFTP
B. SCP
C. SFTP

D. FTPS

Answer: D

Explanation:
Q1007
Which of the following are used to implement VPNs? (Select TWO).

A. SFTP
B. IPSec
C. HTTPS
D. SNMP
E. SSL

Answer: B,E

Explanation:
Q1008
A company recently implemented a TLS on their network. The company is MOST concerned with:

A. Confidentiality
B. Availability

C. Integrity
D. Accessibility

Answer: A

Explanation:
Q1009
Which of the following describes how an attacker can send unwanted advertisements to a mobile device?

A. Man-in-the-middle
B. Bluejacking
C. Bluesnarfing
D. Packet sniffing

Answer: B

Explanation:
Q1010

A network device that protects an enterprise based only on source and destination addresses is

BEST described as:

A. IDS.
B. ACL.
C. Stateful packet filtering.
D. Simple packet filtering.

Answer: D

Explanation:
Q1011
A human resources employee receives an email from a family member stating there is a new virus going around. In order to remove the virus, a user must delete the Boot.ini file from the system immediately. This is an example of which of the following?

Real 391
CompTIA SY0-401 Exam

A. Hoax
B. Spam
C. Whaling
D. Phishing

Answer: A

Explanation:
Q1012
A third party application has the ability to maintain its own user accounts or it may use single sign- on. To use single sign-on, the application is requesting the following information: OU=Users,

DC=Domain, DC=COM. This application is requesting which of the following authentication services?

A. TACACS+
B. RADIUS
C. LDAP
D. Kerberos

Answer: C

Explanation:
Q1013

Power and data cables from the network center travel through the building's boiler room. Which of the following should be used to prevent data emanation?

A. Video monitoring
B. EMI shielding
C. Plenum CAT6 UTP
D. Fire suppression

Answer: B

Explanation:
Q1014
Which of the following must a security administrator implement to isolate public facing servers

from both the corporate network and the Internet?

A. NAC
B. IPSec
C. DMZ
D. NAT

Answer: C

Explanation:
Q1015
Which of the following protocols provides fast, unreliable file transfer?

A. TFTP
B. SFTP
C. Telnet
D. FTPS

Answer: A

Explanation:
Q1016
Which of the following digital certificate management practices will ensure that a lost certificate is not compromised?

A. Key escrow
B. Non-repudiation
C. Recovery agent

D. CRL

Answer: D

Explanation:
Q1017
A recent computer breach has resulted in the incident response team needing to perform a forensics examination. Upon examination, the forensics examiner determines that they cannot tell which captured hard drive was from the device in question.

Which of the following would have prevented the confusion experienced during this examination?

A. Perform routine audit
B. Chain of custody
C. Evidence labeling
D. Hashing the evidence

Answer: C

Explanation:
Q1018
An IT staff member was entering the datacenter when another person tried to piggyback into the datacenter as the door was opened. While the IT staff member attempted to QUESTION NO: the other individual by politely asking to see their badge, the individual refused and ran off into the datacenter. Which of the following should the IT staff member do NEXT?

A. Call the police while tracking the individual on the closed circuit television system
B. Contact the forensics team for further analysis
C. Chase the individual to determine where they are going and what they are doing
D. Contact the onsite physical security team with a description of the individual

Answer: D

Explanation:
Q1019
During a recent user awareness and training session, a new staff member asks the Chief Information Security Officer (CISO) why the company does not allow personally owned devices into the company facilities. Which of the following represents how the CISO should respond?

A. Company A views personally owned devices as creating an unacceptable risk to the organizational IT systems.
B. Company A has begun to see zero-day attacks against personally owned devices disconnected from the network.
C. Company A believes that staff members should be focused on their work while in the company's facilities.

D. Company A has seen social engineering attacks against personally owned devices and does not allow their use.

Answer: A

Explanation:

Q1020

A customer has provided an email address and password to a website as part of the login process. Which of the following BEST describes the email address?

A. Identification
B. Authorization
C. Access control
D. Authentication

Answer: A

Explanation:

Q1021

Which of the following is designed to ensure high availability of web based applications?

A. Proxies
B. Load balancers
C. URL filtering
D. Routers

Answer: B

Explanation:

Q1022

The administrator would like to implement hardware assisted full disk encryption on laptops.

Which of the following would MOST likely be used to meet this goal?

A. TPM

B. USB Drive
C. Key Escrow
D. PKI

Answer: A

Explanation:
Q1023
Jane, a security administrator, wants to harden the web server. Which of the following could she perform to accomplish this task?

A. Implement remote sanitization
B. Disable unnecessary services
C. Install mantraps in the datacenter
D. Compare baseline configurations

Answer: B

Explanation:
Q1024
Which of the following policies could be implemented to help prevent users from displaying their login credentials in open view for everyone to see?

A. Privacy
B. Clean desk
C. Job rotation
D. Password complexity

Answer: B

Explanation:
Q1025
Which of the following is another, more common, name for EAPOL?

A. LDAP

B. 802.1X
C. LDAPS
D. 802.12

Answer: B

Explanation:
Q1026
If you don't know the MAC address of a Windows-based machine, what command-line utility can you use to ascertain it?

A. macconfig
B. ifconfig

C. ipconfig
D. config

Answer: C

Explanation:
Q1027
In the Windows world, what tool is used to disable a port?

A. System Manager
B. System Monitor
C. Performance Monitor
D. Windows Firewall

Answer: D

Explanation:
Q1028
A set of standardized system images with a pre-defined set of applications is used to build enduser workstations. The security administrator has scanned every workstation to create a current inventory of all applications that are installed on active workstations and is documenting which applications are out-of-date and could be exploited. The security administrator is determining the:

A. Attack surface.
B. Application hardening effectiveness.
C. Application baseline.
D. OS hardening effectiveness.

Answer: A

Explanation:
Q1029
A perimeter survey finds that the wireless network within a facility is easily reachable outside of the physical perimeter. Which of the following should be adjusted to mitigate this risk?

A. CCMP
B. MAC filter
C. SSID broadcast
D. Power level controls

Answer: D

Explanation:
Q1030
Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

A. Protocol analyzer
B. Vulnerability scan
C. Penetration test
D. Port scanner

Answer: B

Explanation:
Q1031
An administrator values transport security strength above network speed when implementing an SSL VPN. Which of the following encryption ciphers would BEST meet their needs?

A. SHA256
B. RC4
C. 3DES
D. AES128

Answer: D

Explanation:
Q1032
All of the following are encryption types EXCEPT:

A. Full disk
B. SMIME
C. File and folder
D. RADIUS

Answer: D

Explanation:
Q1033
Which of the following is used by Matt, a security administrator, to lower the risks associated with electrostatic discharge, corrosion, and thermal breakdown?

A. Temperature and humidity controls
B. Routine audits
C. Fire suppression and EMI shielding
D. Hot and cold aisles

Answer: A

Explanation:
Q1034
When integrating source material from an open source project into a highly secure environment, which of the following precautions should prevent hidden threats?

A. Design review
B. Code review
C. Risk assessment
D. Vulnerability scan

Answer: B

Explanation:
Q1035
Which of the following would MOST likely belong in the DMZ? (Select TWO).

A. Finance servers
B. Backup servers
C. Web servers
D. SMTP gateways
E. Laptops

Answer: C,D

Explanation:
Q1036
When verifying file integrity on a remote system that is bandwidth limited, which of the following tool combinations provides the STRONGEST confidence?

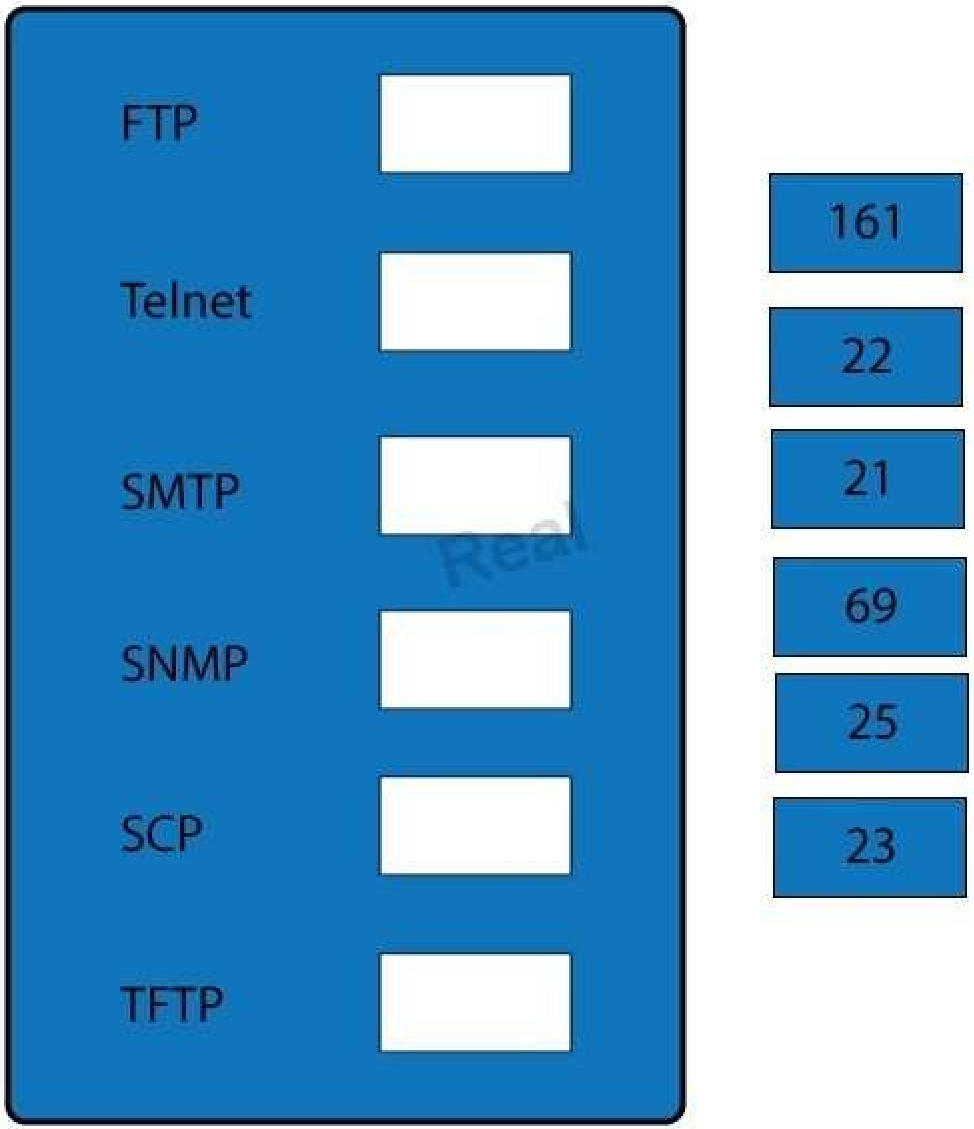
A. MD5 and 3DES
B. MD5 and SHA-1
C. SHA-256 and RSA
D. SHA-256 and AES

Answer: B

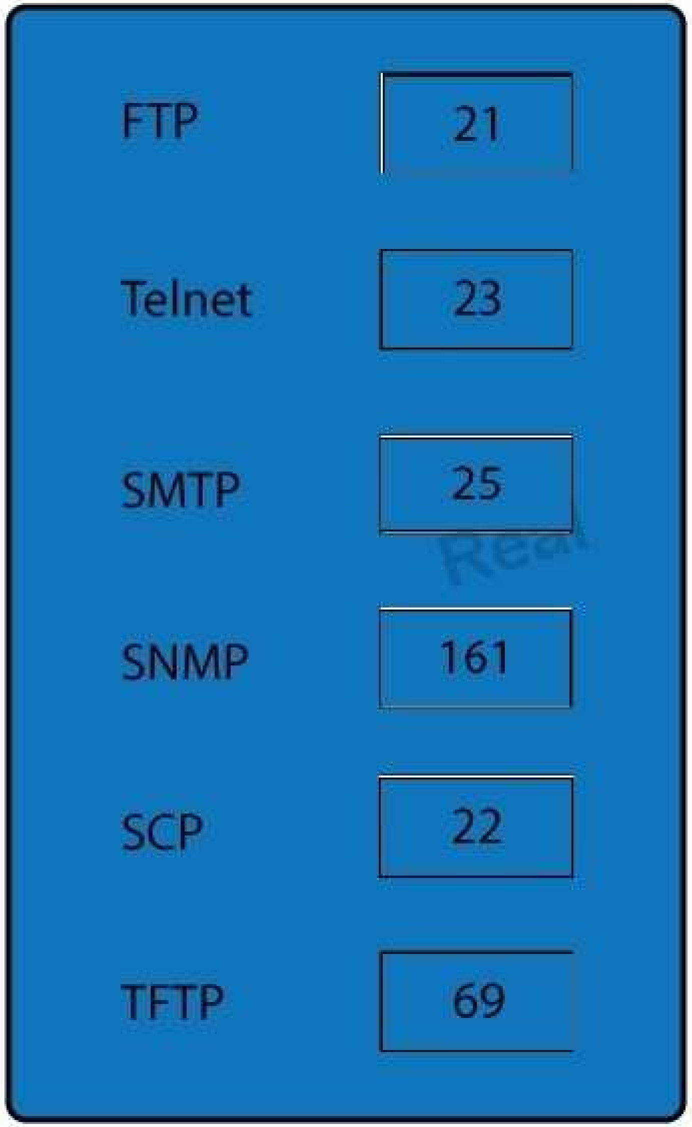
Real 400

QUESTION 724
Drag and drop the correct protocol to its default port.

Select and Place:



Correct Answer:

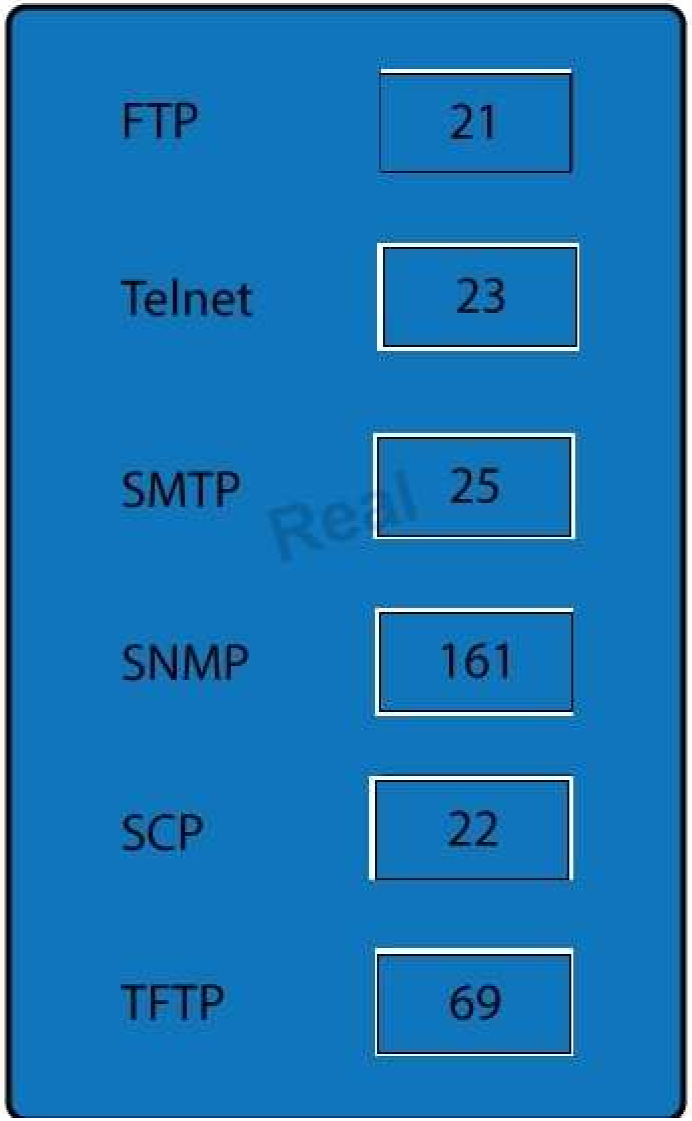


FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

Section: (none)

Explanation

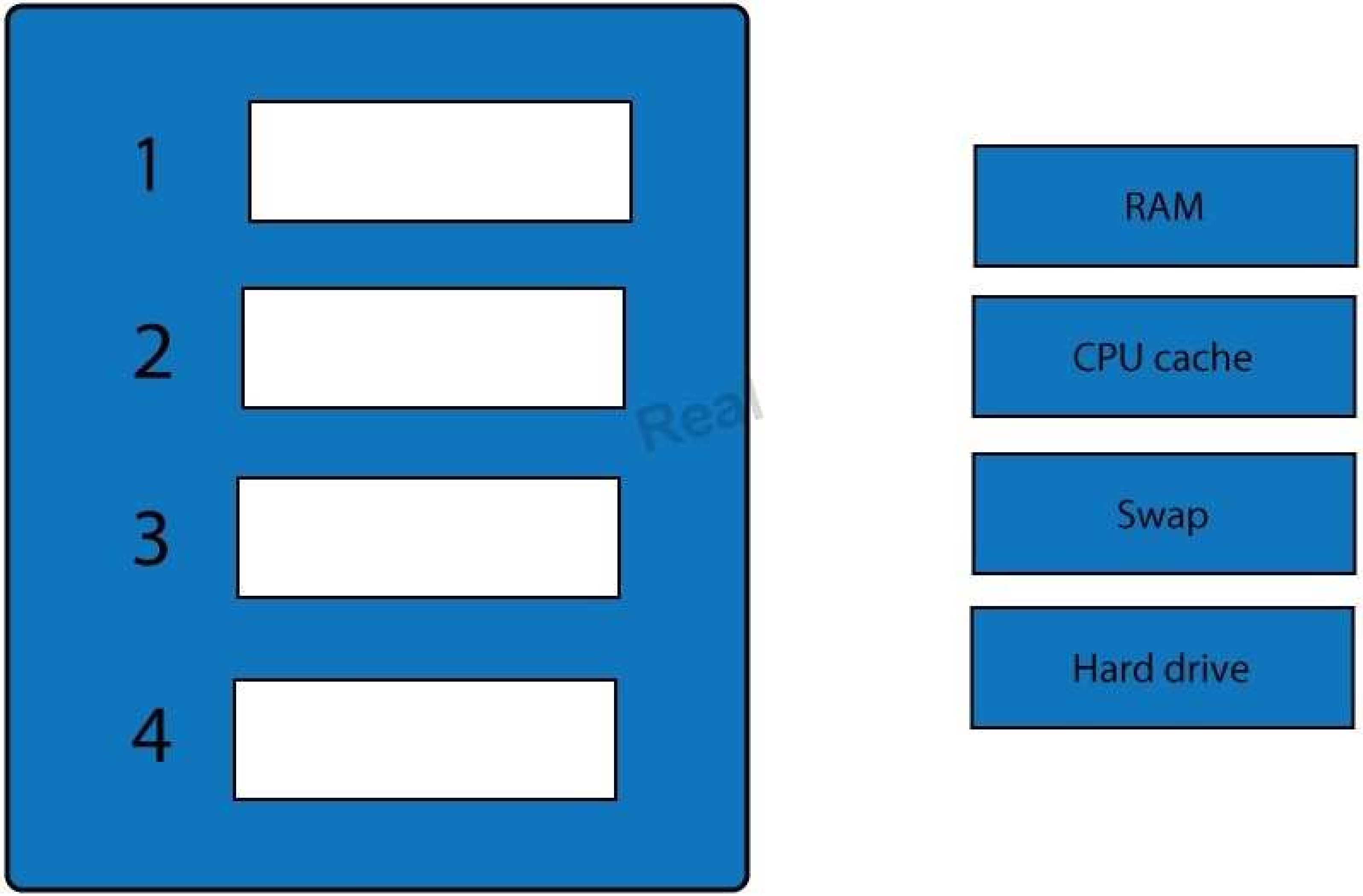
Explanation/Reference:



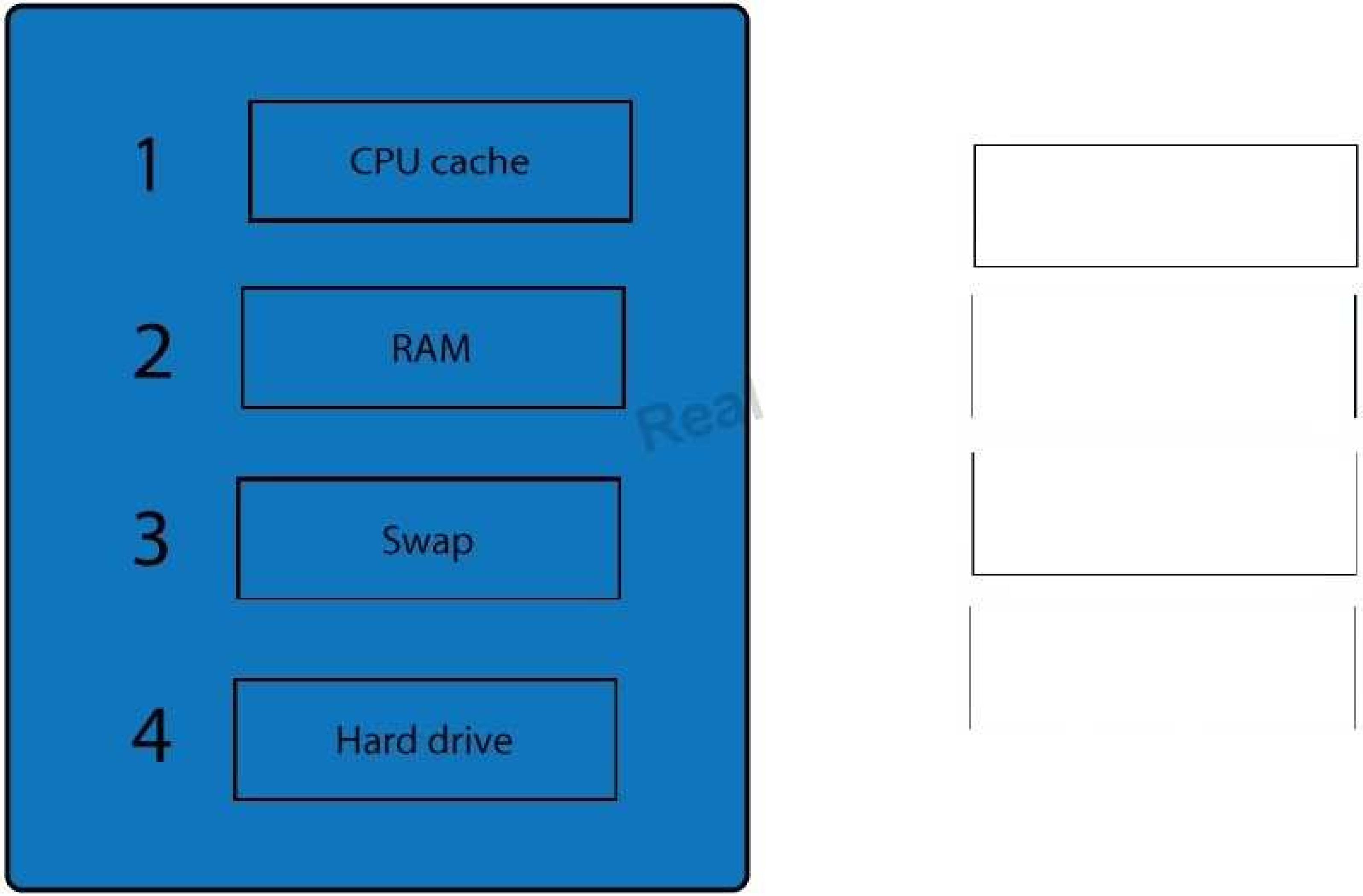
FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

QUESTION 725
A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

Select and Place:



Correct Answer:



1 CPU cache

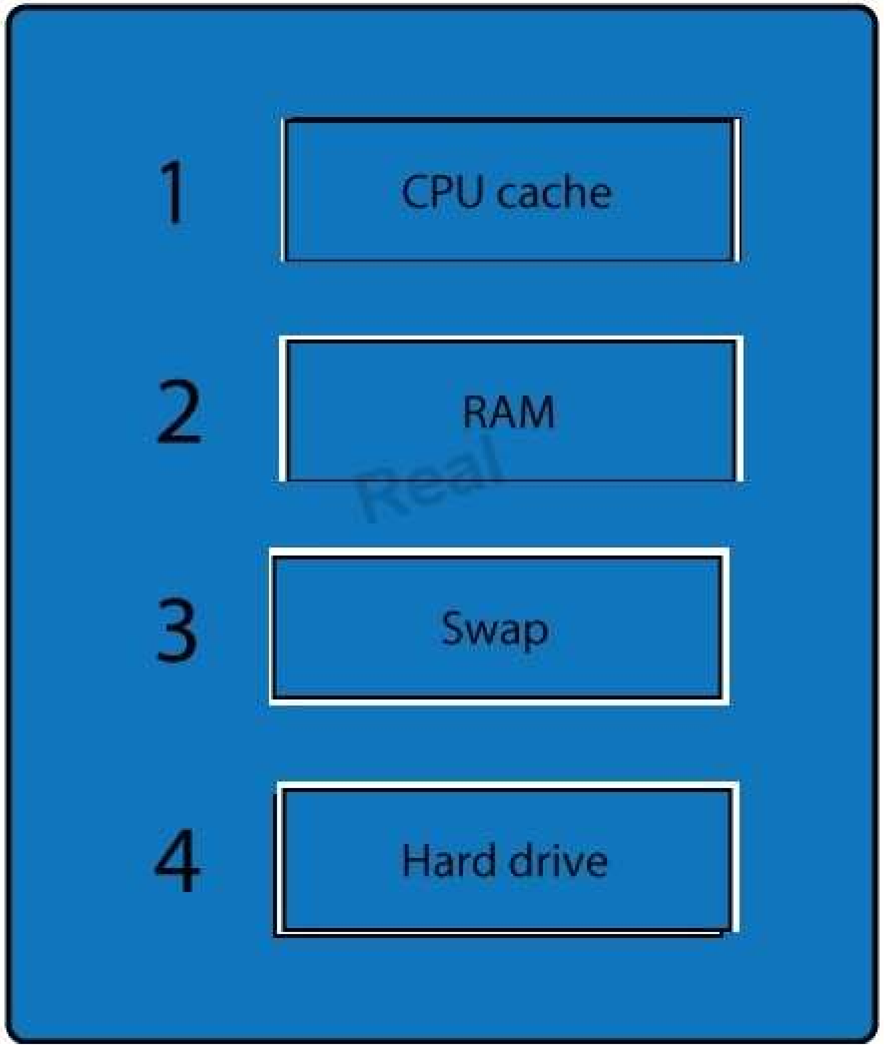
2 RAM

3 Swap

4 Hard drive

Section: (none)
Explanation

Explanation/Reference:



1 CPU cache

2 RAM

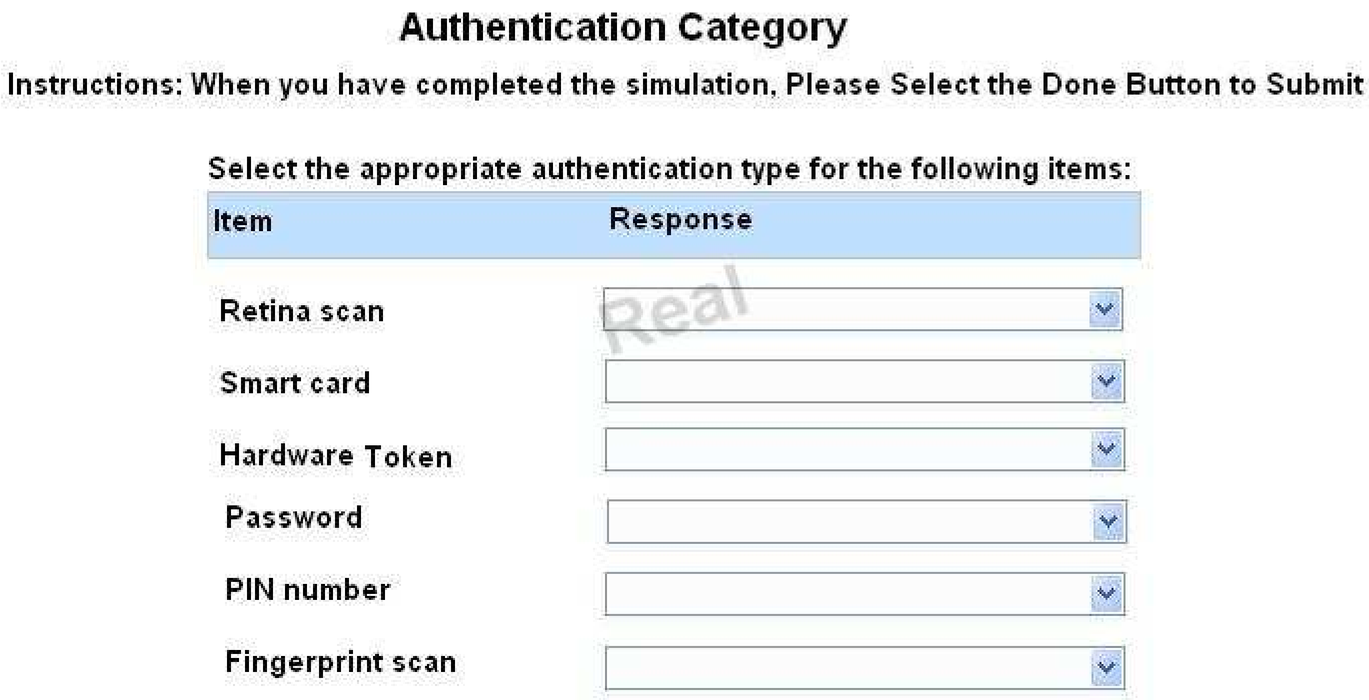
3 Swap

4 Hard drive

QUESTION 726

For each of the given items, select the appropriate authentication category from the dropdown choices.

Instructions: When you have completed the simu-lation, please select the Done button to submit.



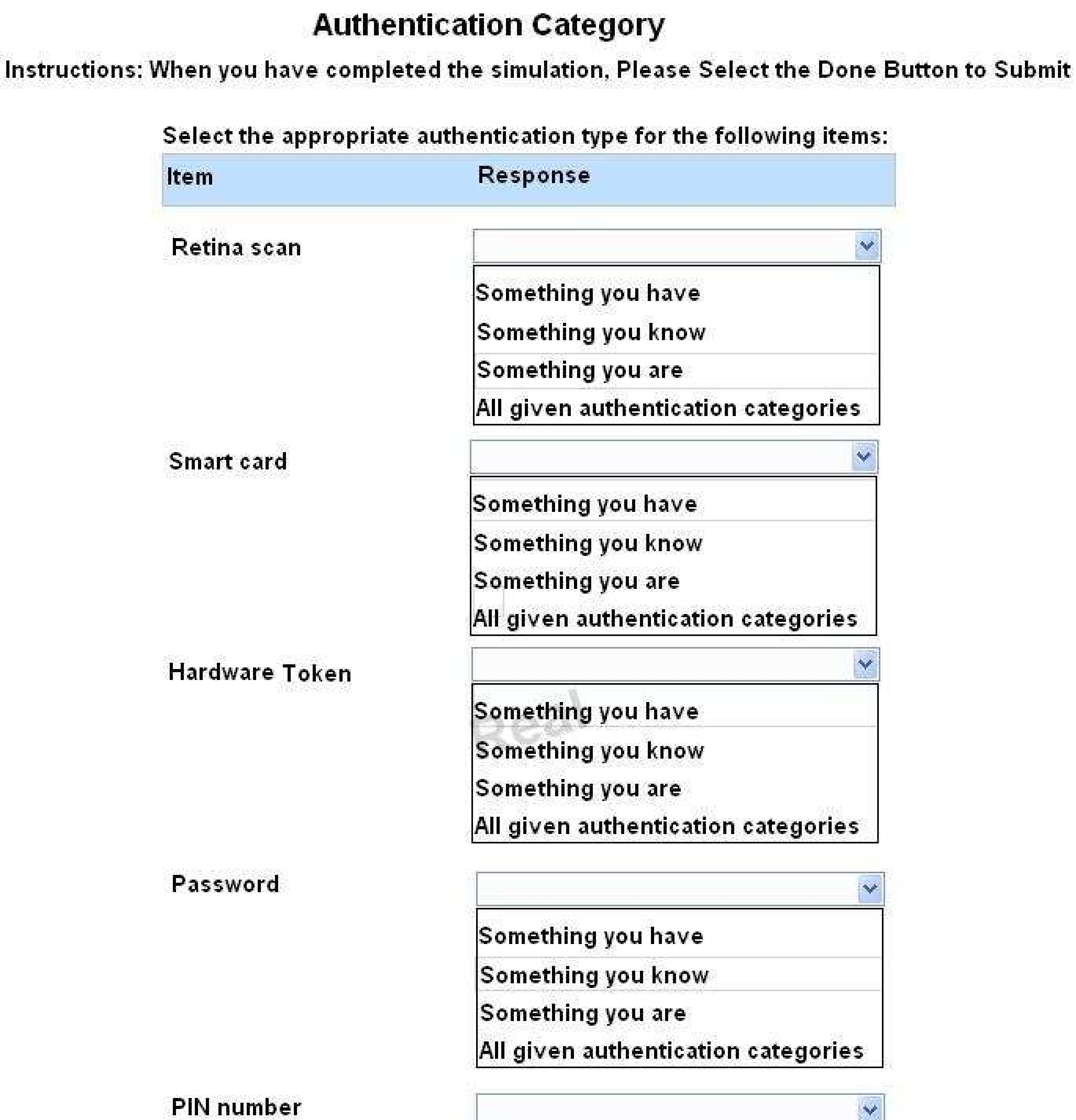
Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	
Smart card	
Hardware Token	
Password	
PIN number	
Fingerprint scan	

Hot Area:



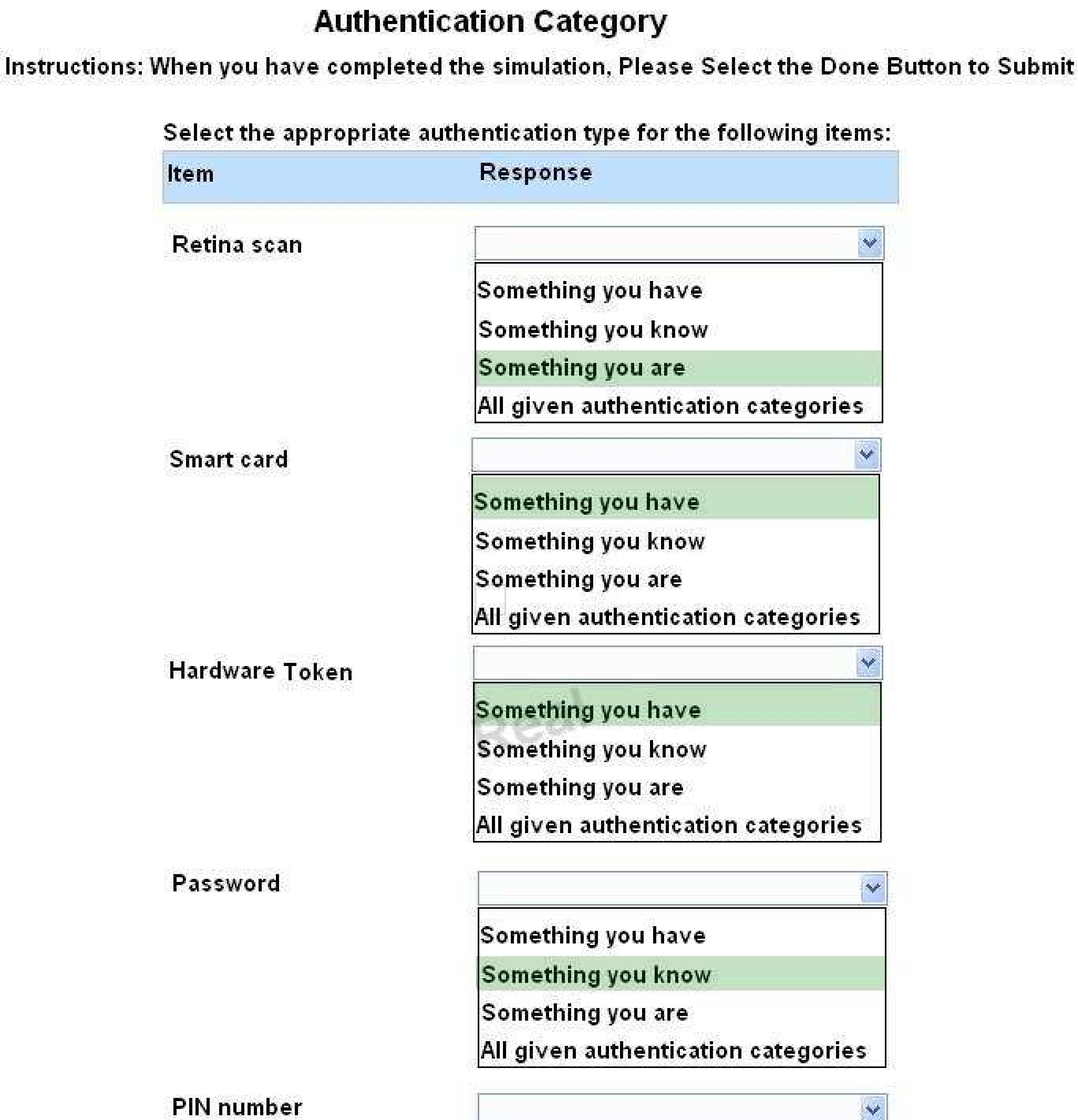
Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	Something you have Something you know Something you are All given authentication categories
Smart card	Something you have Something you know Something you are All given authentication categories
Hardware Token	Something you have Something you know Something you are All given authentication categories
Password	Something you have Something you know Something you are All given authentication categories
PIN number	

Correct Answer:



Authentication Category

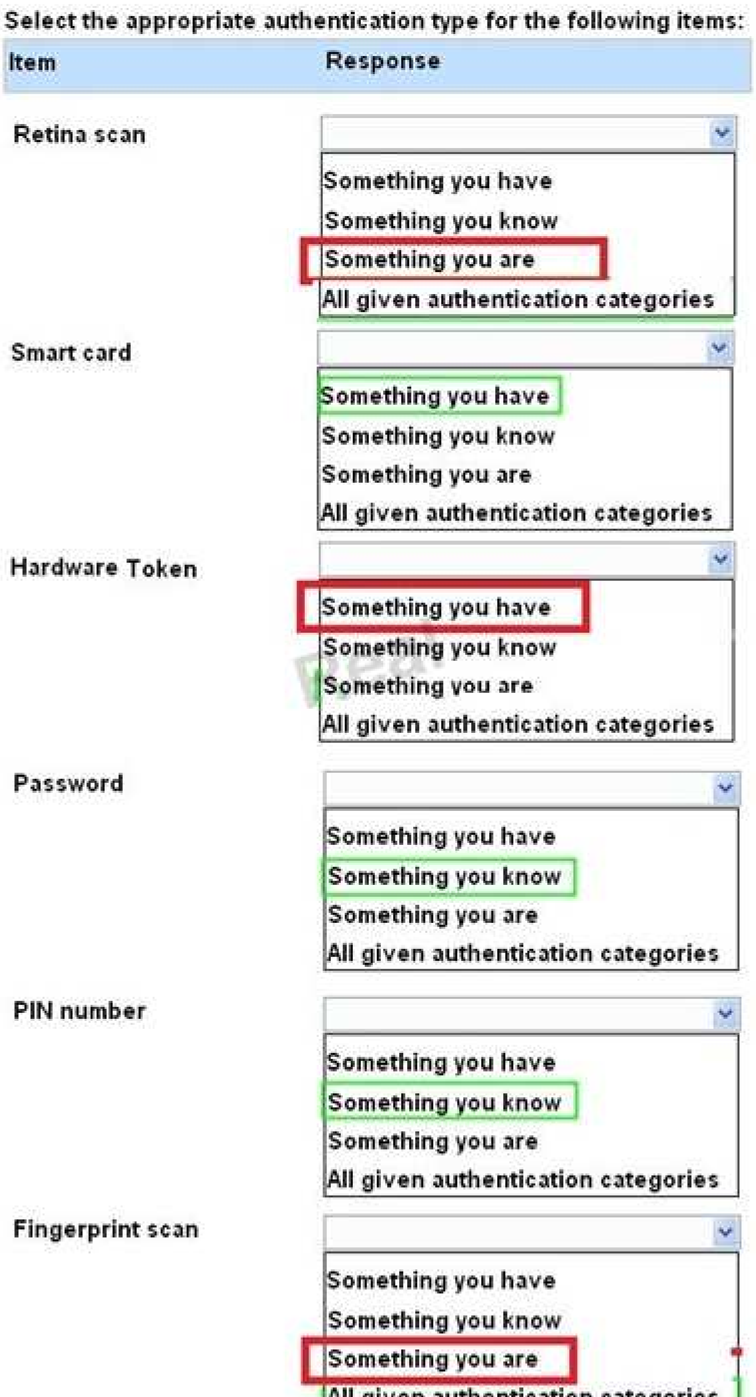
Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	Something you have Something you know [✓ Something you are] All given authentication categories
Smart card	[✓ Something you have] Something you know Something you are All given authentication categories
Hardware Token	[✓ Something you have] Something you know Something you are All given authentication categories
Password	Something you have [✓ Something you know] Something you are All given authentication categories
PIN number	

Section: (none)
Explanation

Explanation/Reference:



Select the appropriate authentication type for the following items:

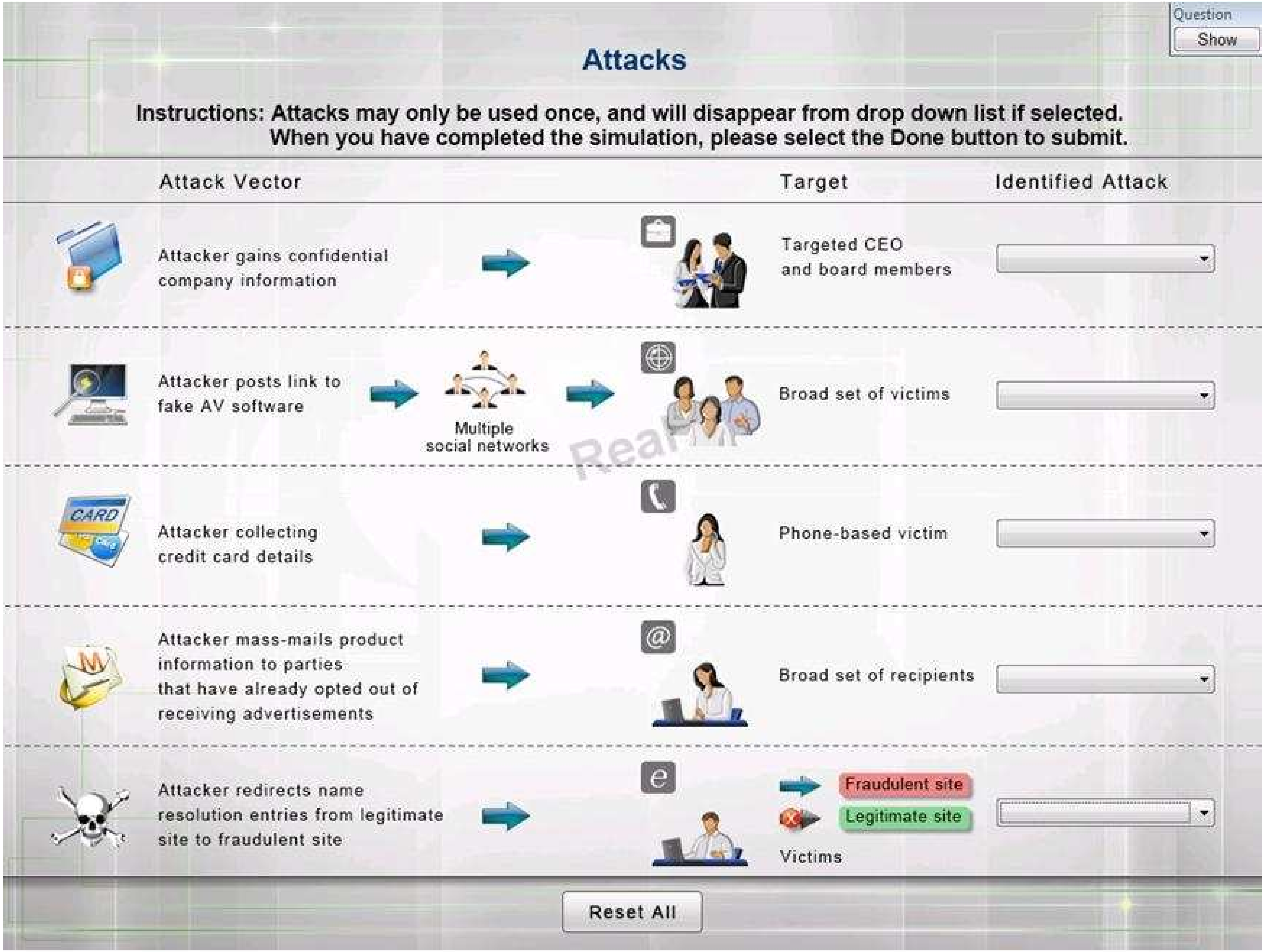
Item	Response
Retina scan	Something you have Something you know [✓ Something you are] All given authentication categories
Smart card	[✓ Something you have] Something you know Something you are All given authentication categories
Hardware Token	[✓ Something you have] Something you know Something you are All given authentication categories
Password	Something you have [✓ Something you know] Something you are All given authentication categories
PIN number	Something you have [✓ Something you know] Something you are All given authentication categories
Fingerprint scan	Something you have Something you know [✓ Something you are] All given authentication categories

QUESTION 727

Select the appropriate attack from each drop down list to label the corresponding illustrated attack

Instructions: Attacks may only be used once, and will disappear from drop down list if selected.

When you have completed the simulation, please select the Done button to submit.

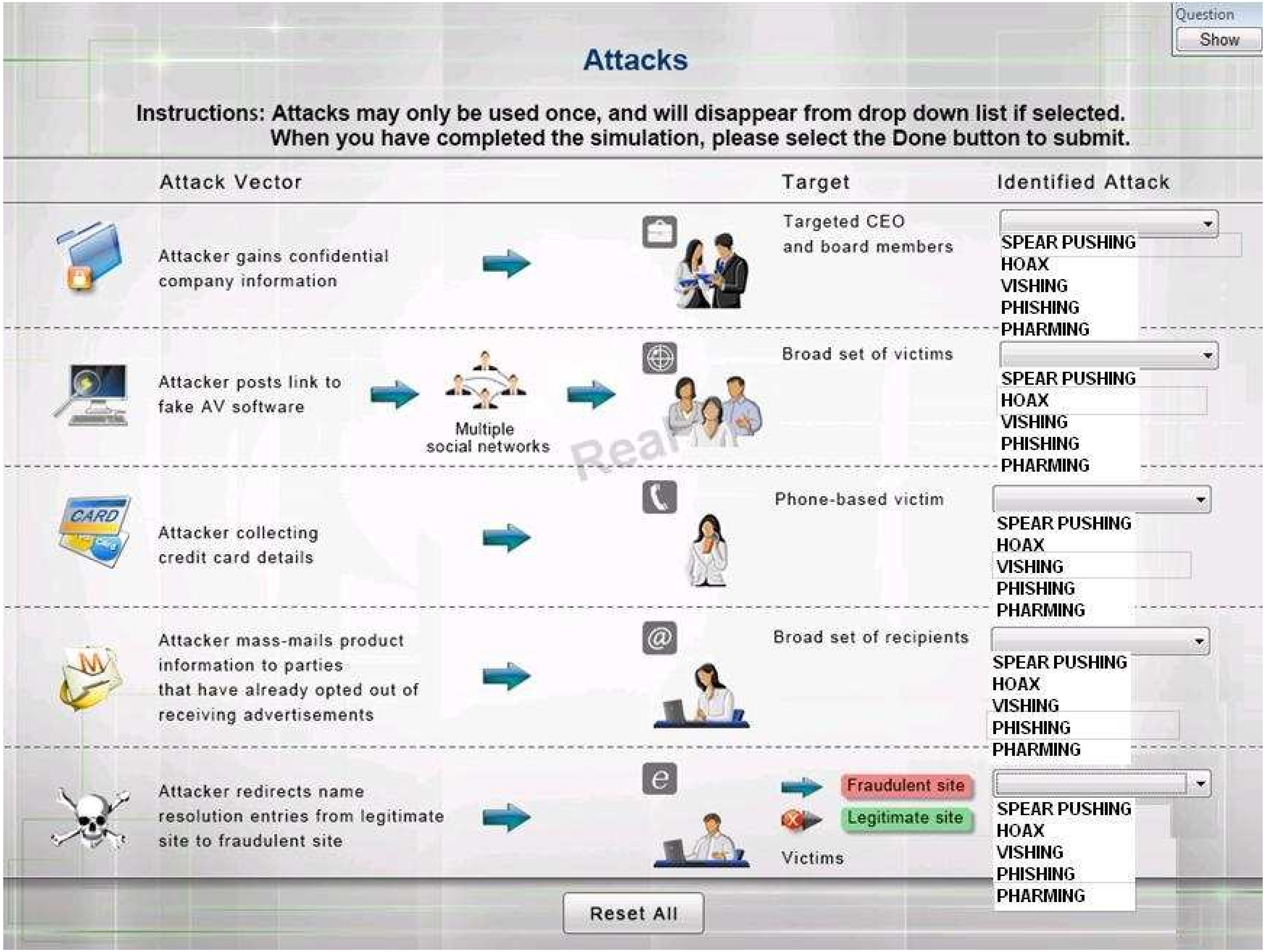


Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Attack Vector		Target	Identified Attack
Attacker gains confidential company information		Targeted CEO and board members	
Attacker posts link to fake AV software	Multiple social networks	Broad set of victims	
Attacker collecting credit card details		Phone-based victim	
Attacker mass-mails product information to parties that have already opted out of receiving advertisements		Broad set of recipients	
Attacker redirects name resolution entries from legitimate site to fraudulent site		Fraudulent site Legitimate site Victims	

Hot Area:

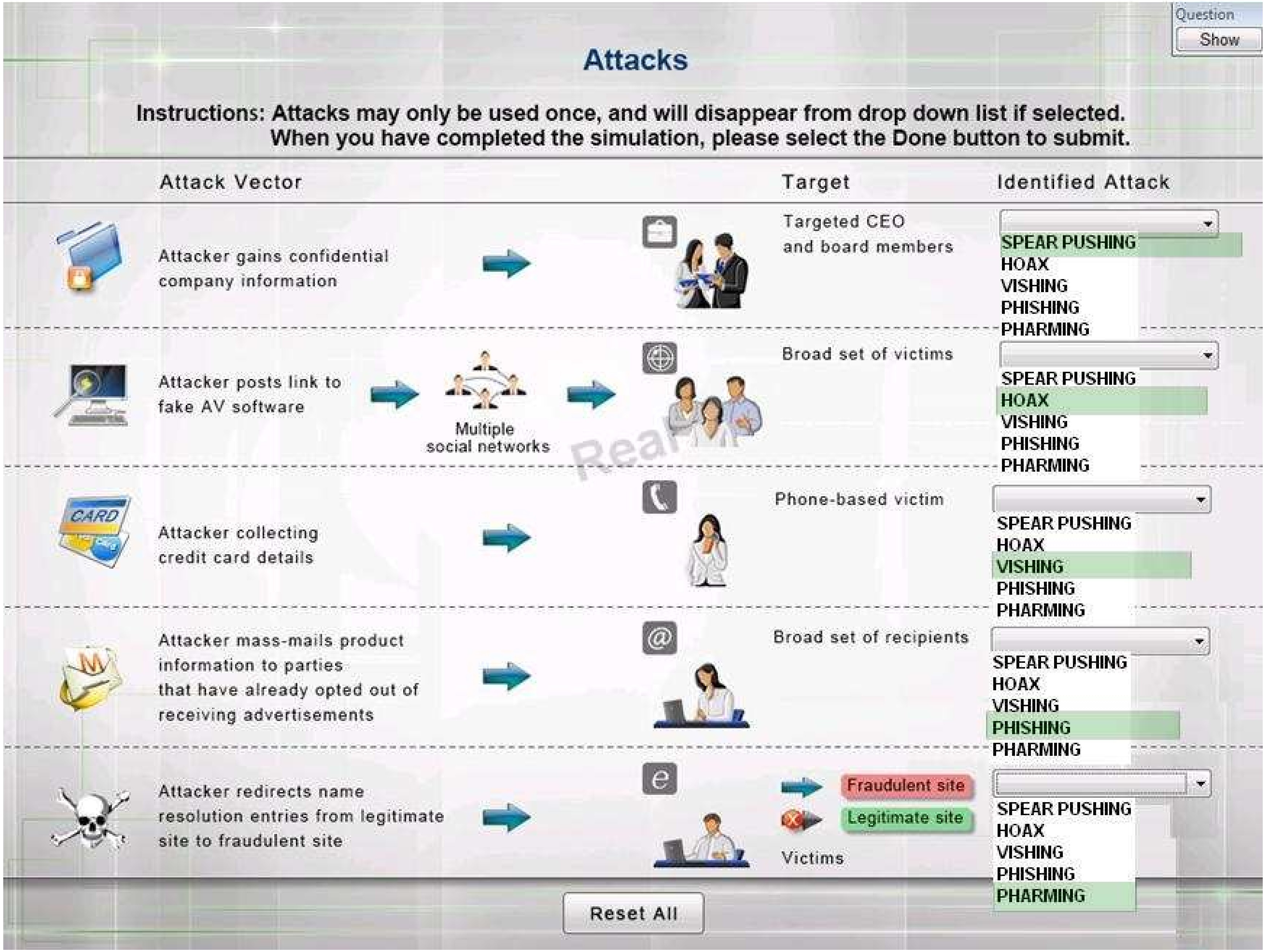


Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Attack Vector	Target	Identified Attack
Attacker gains confidential company information	Targeted CEO and board members	SPEAR PUSHING HOAX VISHING PHISHING PHARMING
Attacker posts link to fake AV software → Multiple social networks	Broad set of victims	SPEAR PUSHING HOAX VISHING PHISHING PHARMING
Attacker collecting credit card details	Phone-based victim	SPEAR PUSHING HOAX VISHING PHISHING PHARMING
Attacker mass-mails product information to parties that have already opted out of receiving advertisements	Broad set of recipients	SPEAR PUSHING HOAX VISHING PHISHING PHARMING
Attacker redirects name resolution entries from legitimate site to fraudulent site	Fraudulent site Legitimate site Victims	SPEAR PUSHING HOAX VISHING PHISHING PHARMING

Correct Answer:



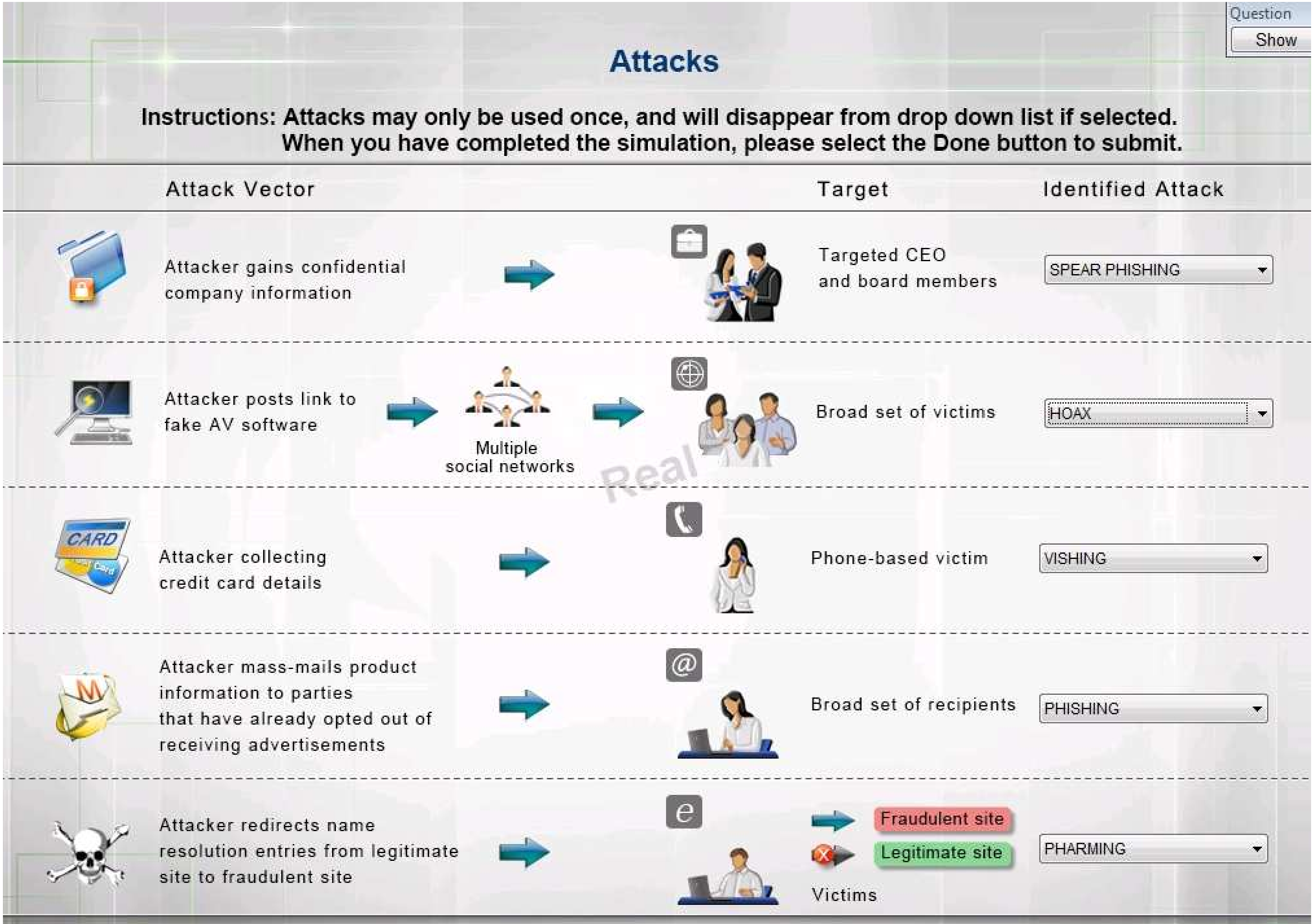
Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Attack Vector		Target	Identified Attack
Attacker gains confidential company information		Targeted CEO and board members	[✓ SPEAR PUSHING] HOAX VISHING PHISHING PHARMING
Attacker posts link to fake AV software	Multiple social networks	Broad set of victims	SPEAR PUSHING [✓ HOAX] VISHING PHISHING PHARMING
Attacker collecting credit card details		Phone-based victim	SPEAR PUSHING HOAX [✓ VISHING] PHISHING PHARMING
Attacker mass-mails product information to parties that have already opted out of receiving advertisements		Broad set of recipients	SPEAR PUSHING HOAX VISHING [✓ PHISHING] PHARMING
Attacker redirects name resolution entries from legitimate site to fraudulent site		Fraudulent site Legitimate site Victims	SPEAR PUSHING HOAX VISHING PHISHING [✓ PHARMING]

Section: (none)
Explanation

Explanation/Reference:



Attacks

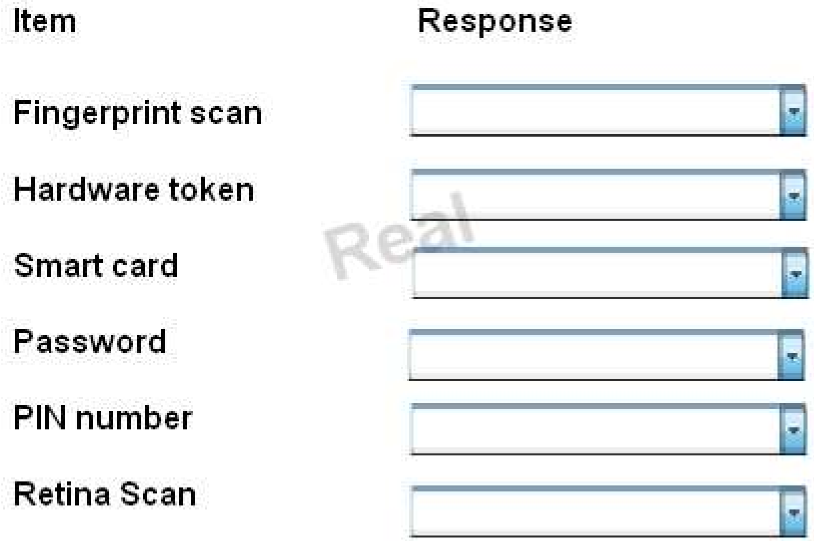
Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Attack Vector		Target	Identified Attack
Attacker gains confidential company information	→	Targeted CEO and board members	SPEAR PHISHING ▾
Attacker posts link to fake AV software	→ Multiple social networks →	Broad set of victims	HOAX ▾
Attacker collecting credit card details	→	Phone-based victim	VISHING ▾
Attacker mass-mails product information to parties that have already opted out of receiving advertisements	→	Broad set of recipients	PHISHING ▾
Attacker redirects name resolution entries from legitimate site to fraudulent site	→	→ Fraudulent site ☒ Legitimate site Victims	PHARMING ▾

QUESTION 728

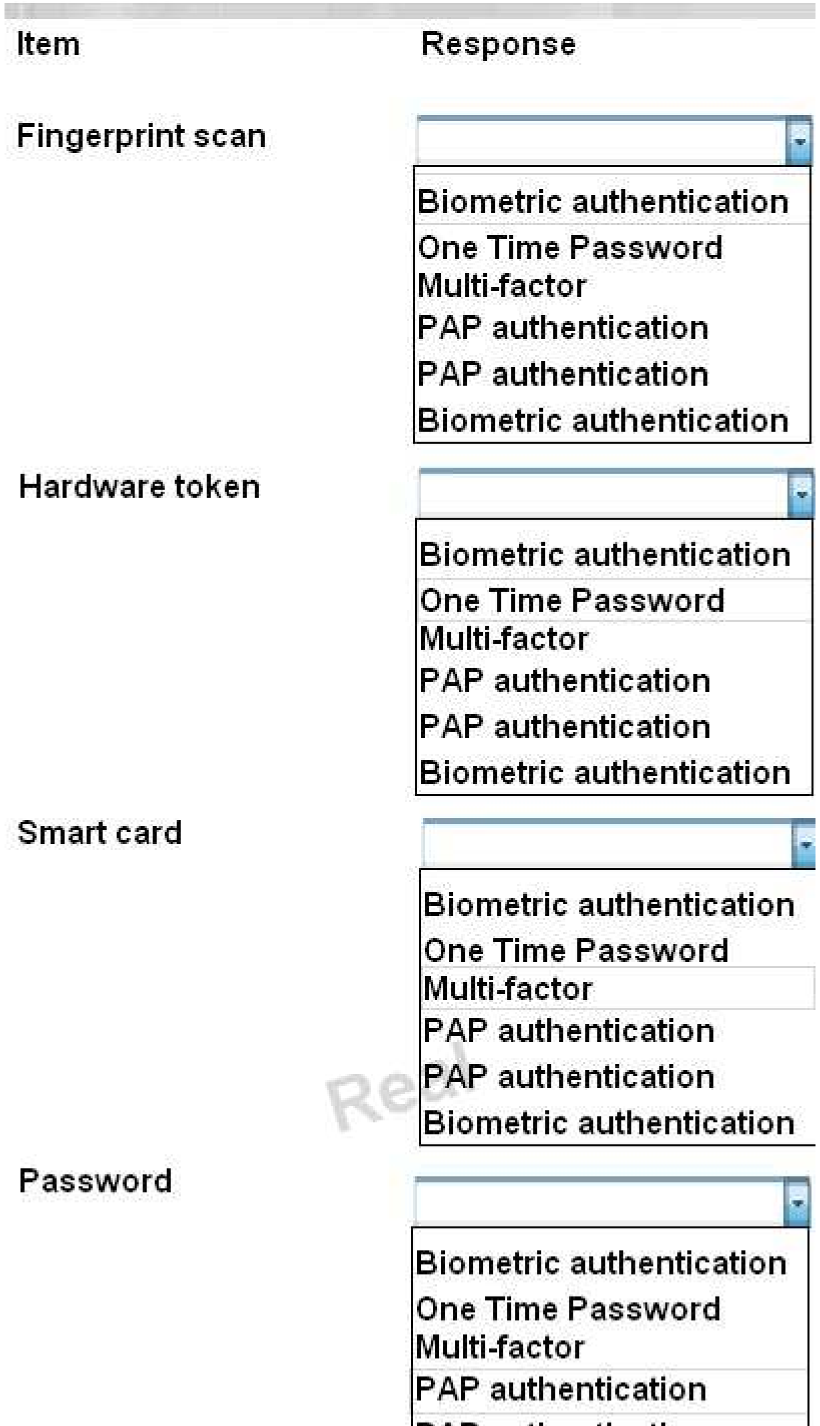
For each of the given items, select the appropriate authentication category from the drop down choices.

Select the appropriate authentication type for the following items:



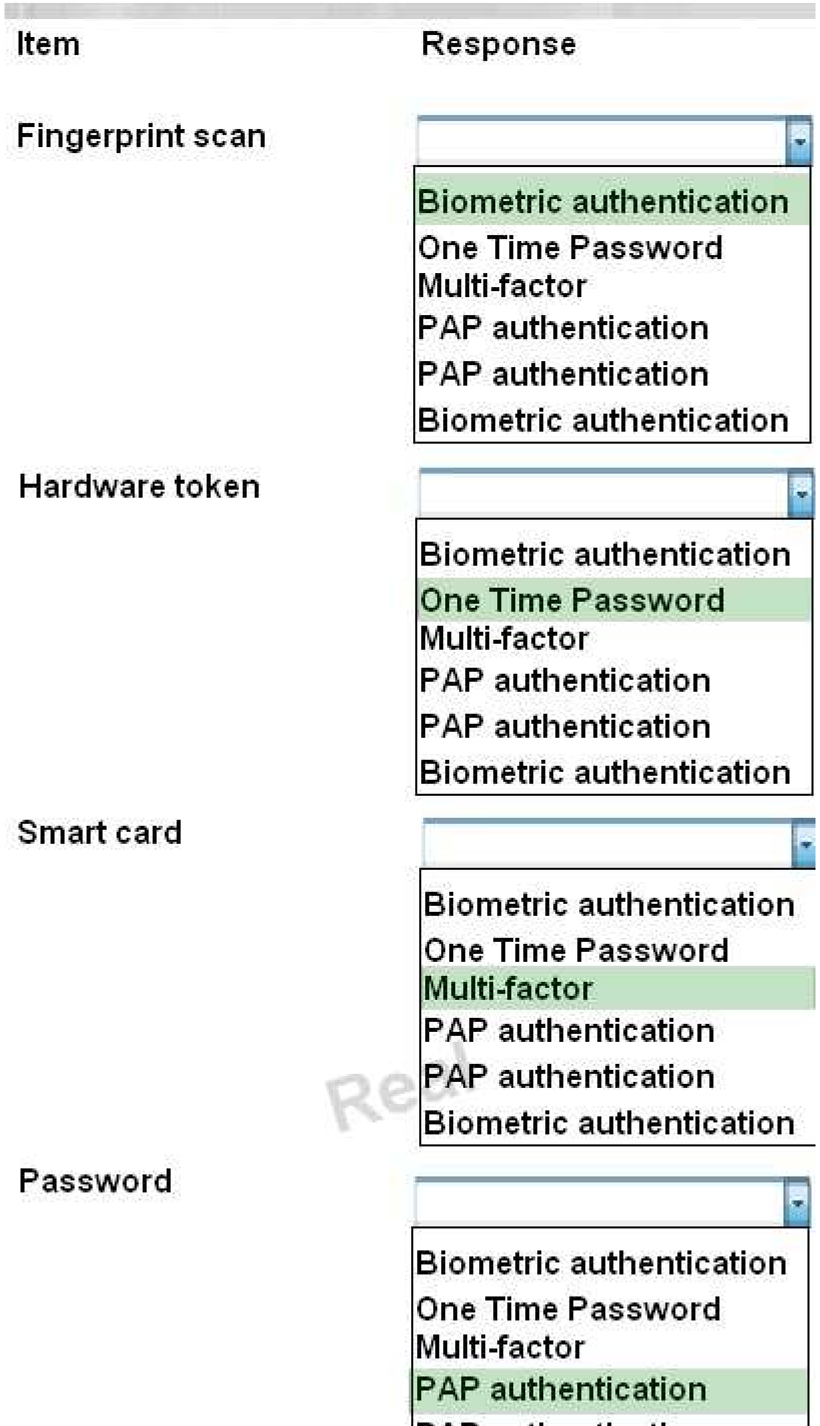
Item	Response
Fingerprint scan	
Hardware token	
Smart card	
Password	
PIN number	
Retina Scan	

Hot Area:



Item	Response
Fingerprint scan	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Password	Biometric authentication One Time Password Multi-factor PAP authentication

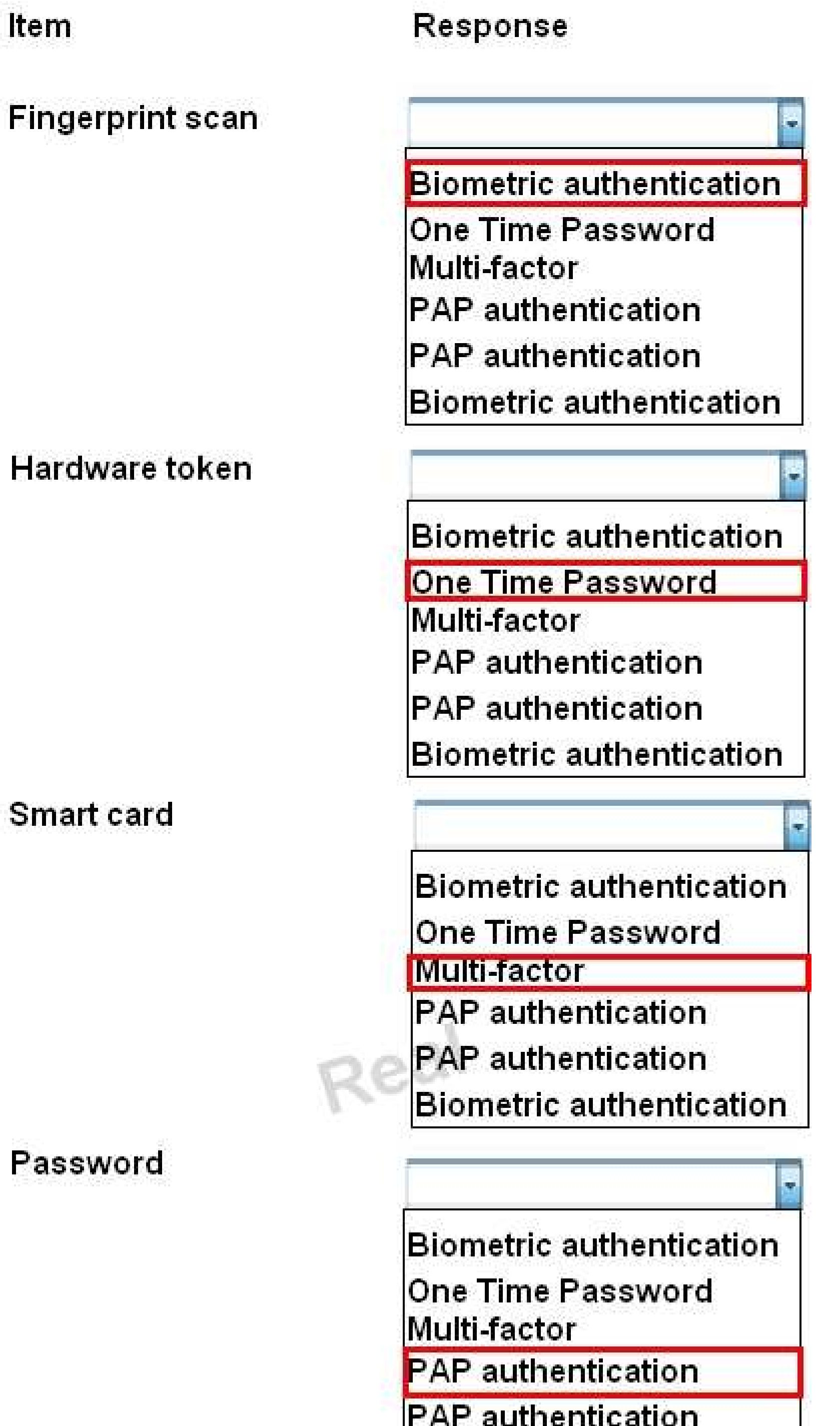
Correct Answer:



Item	Response
Fingerprint scan	[✓ Biometric authentication] One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	Biometric authentication [✓ One Time Password] Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	Biometric authentication One Time Password [✓ Multi-factor] PAP authentication PAP authentication Biometric authentication
Password	Biometric authentication One Time Password Multi-factor [✓ PAP authentication]

Section: (none)
Explanation

Explanation/Reference:



Item Response

Fingerprint scan

[✓ Biometric authentication]
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication

Hardware token

Biometric authentication
[✓ One Time Password]
Multi-factor
PAP authentication
PAP authentication
Biometric authentication

Smart card

Biometric authentication
One Time Password
[✓ Multi-factor]
PAP authentication
PAP authentication
Biometric authentication

Password

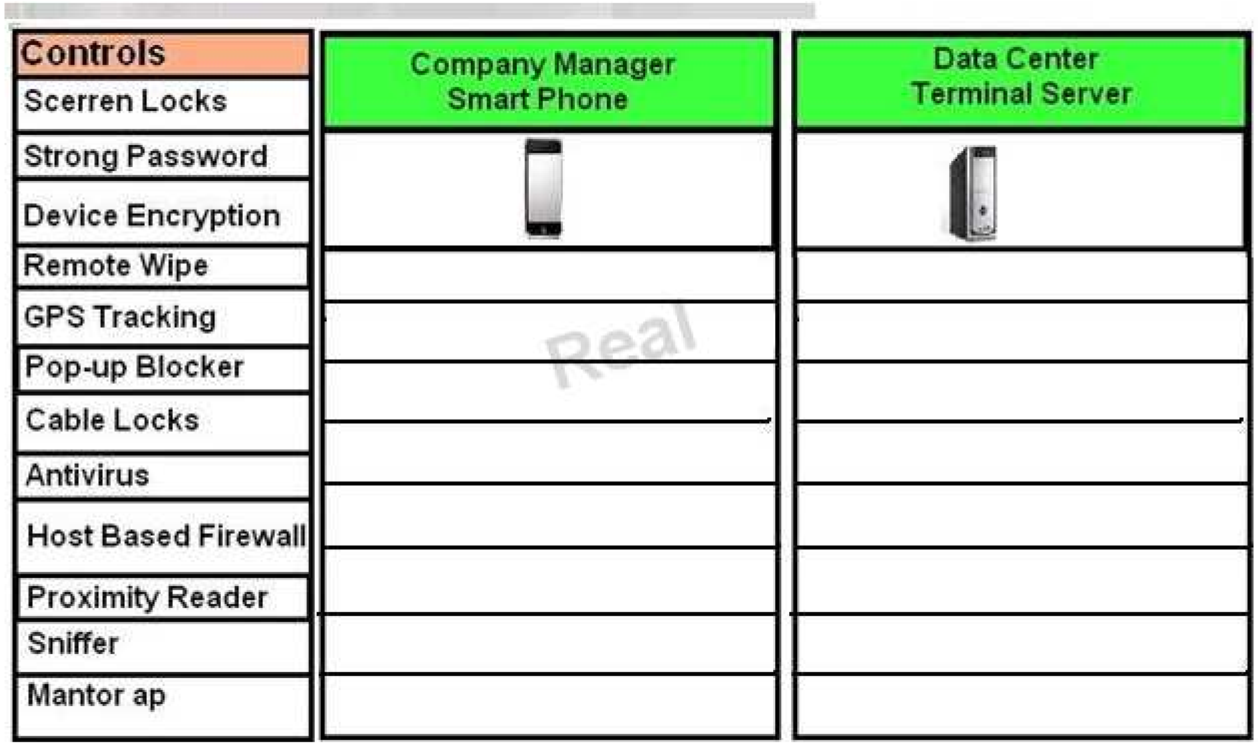
Biometric authentication
One Time Password
Multi-factor
[✓ PAP authentication]
PAP authentication

QUESTION 729

A Security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and Drop the applicable controls to each asset type.

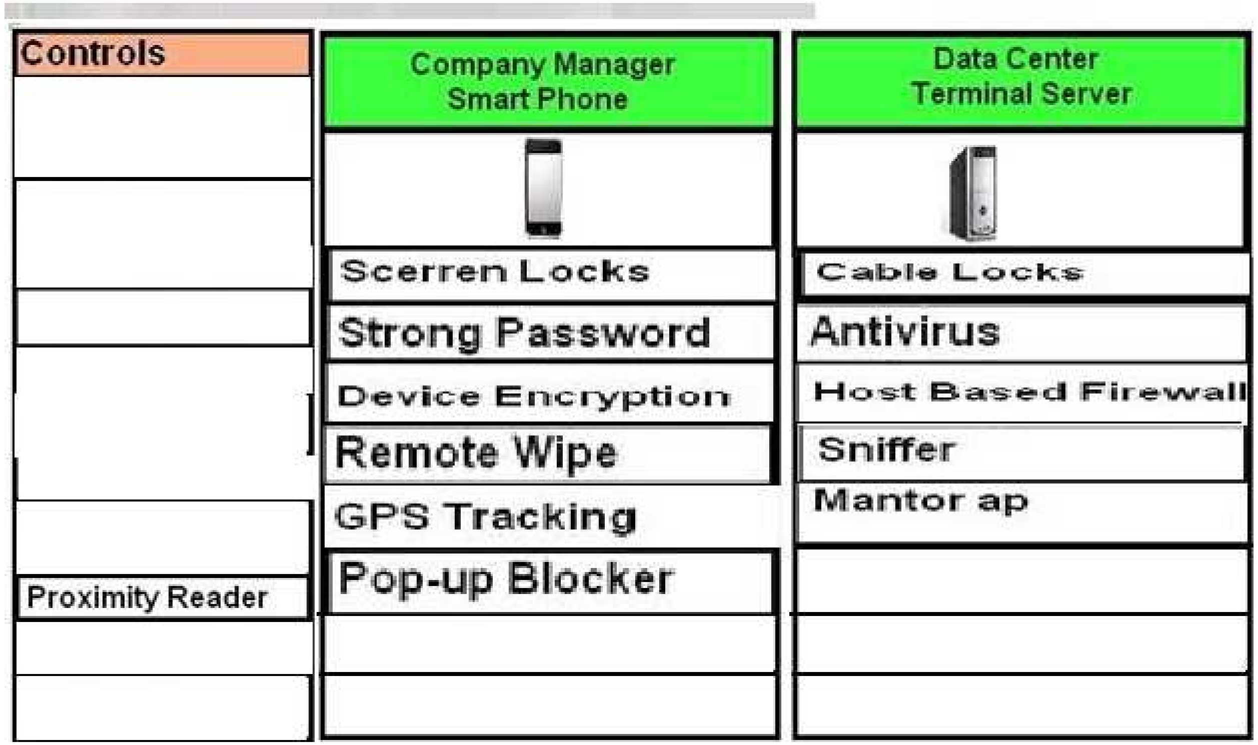
Instructions: Controls can be used multiple times and not all placeholders needs to be filled. When you have completed the simulation, Please select Done to submit.

Select and Place:



Controls	Company Manager Smart Phone	Data Center Terminal Server
Scerren Locks		
Strong Password		
Device Encryption		
Remote Wipe		
GPS Tracking		
Pop-up Blocker		
Cable Locks		
Antivirus		
Host Based Firewall		
Proximity Reader		
Sniffer		
Mantor ap		

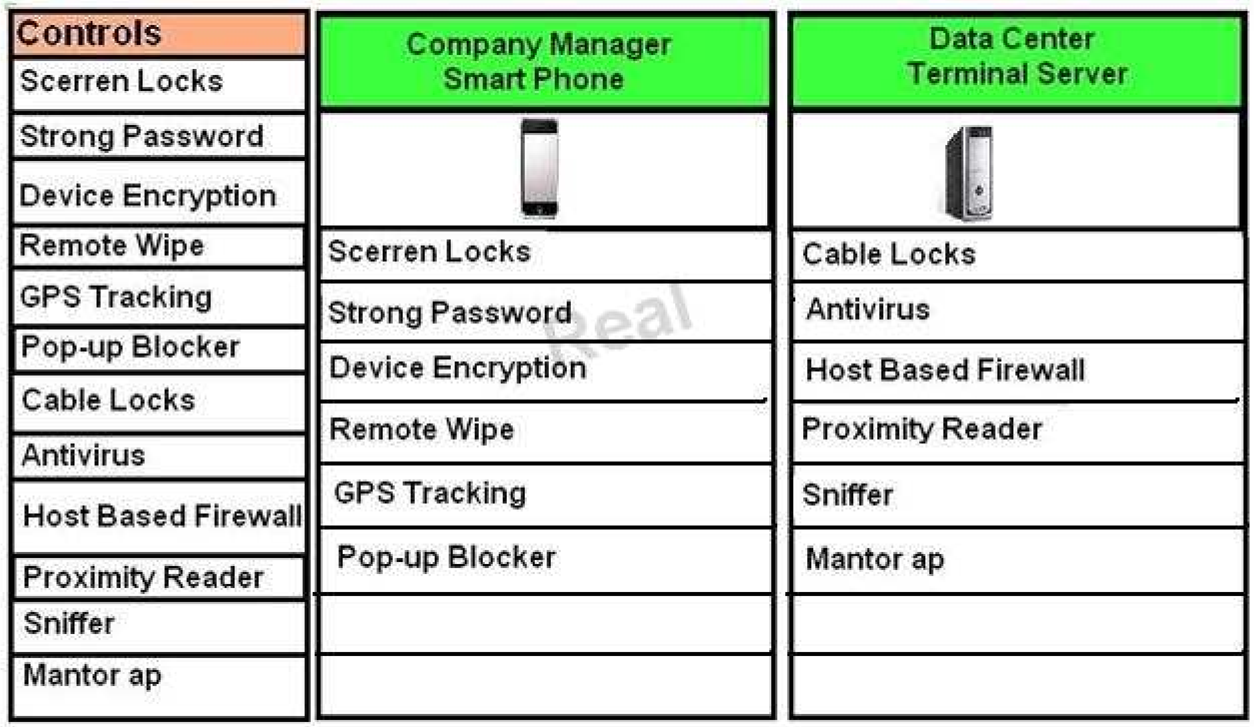
Correct Answer:



Controls	Company Manager Smart Phone	Data Center Terminal Server
	Scerren Locks	Cable Locks
	Strong Password	Antivirus
	Device Encryption	Host Based Firewall
	Remote Wipe	Sniffer
	GPS Tracking	Mantor ap
Proximity Reader	Pop-up Blocker	

Section: (none)
Explanation

Explanation/Reference:

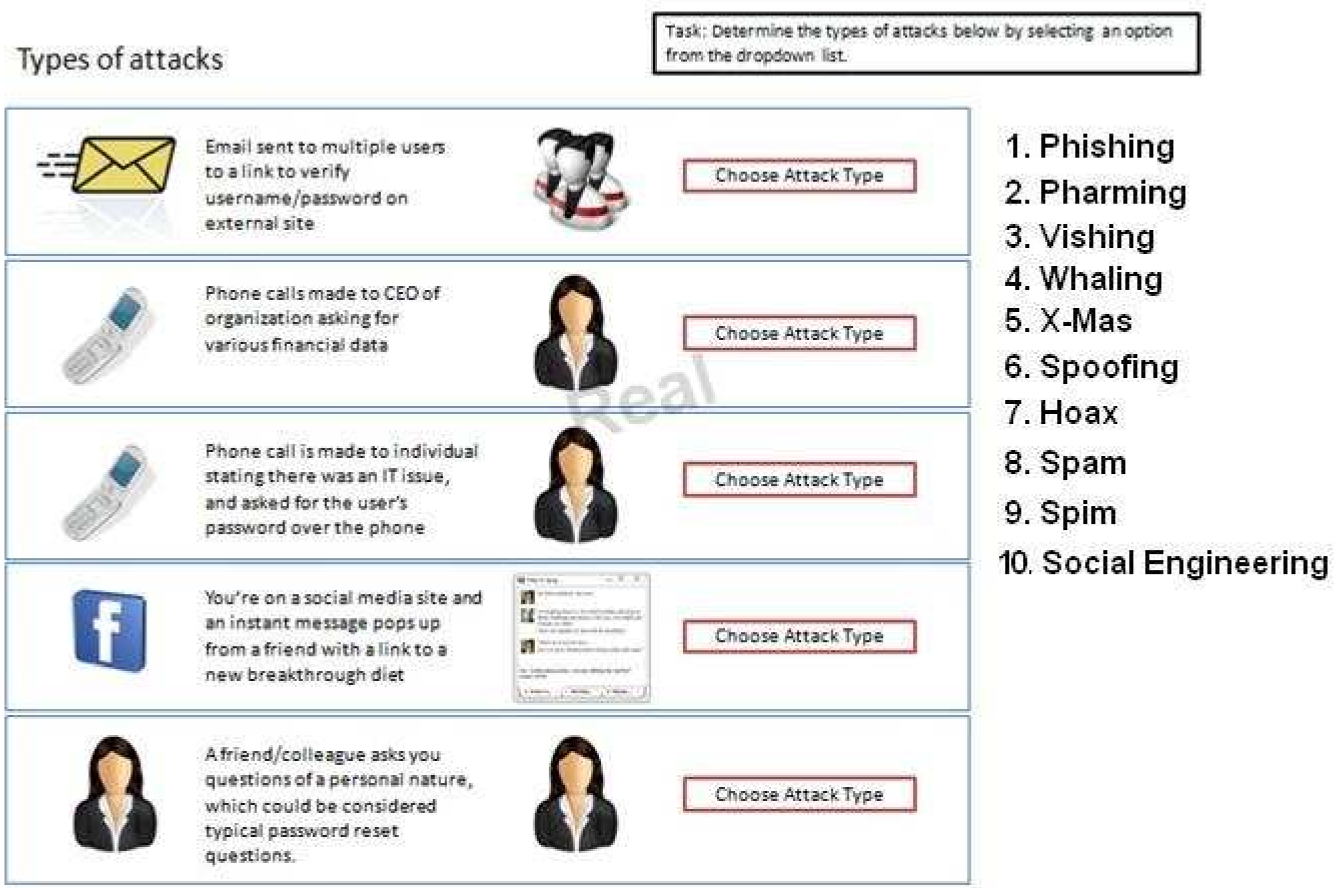


Controls
Scerren Locks
Strong Password
Device Encryption
Remote Wipe
GPS Tracking
Pop-up Blocker
Cable Locks
Antivirus
Host Based Firewall
Proximity Reader
Sniffer
Mantor ap

Company Manager Smart Phone	Data Center Terminal Server
Scerren Locks	Cable Locks
Strong Password	Antivirus
Device Encryption	Host Based Firewall
Remote Wipe	Proximity Reader
GPS Tracking	Sniffer
Pop-up Blocker	Mantor ap

QUESTION 730
Determine the types of attacks below by selecting an option from the dropdown list.
Determine the types of Attacks from right to specific action.

Select and Place:



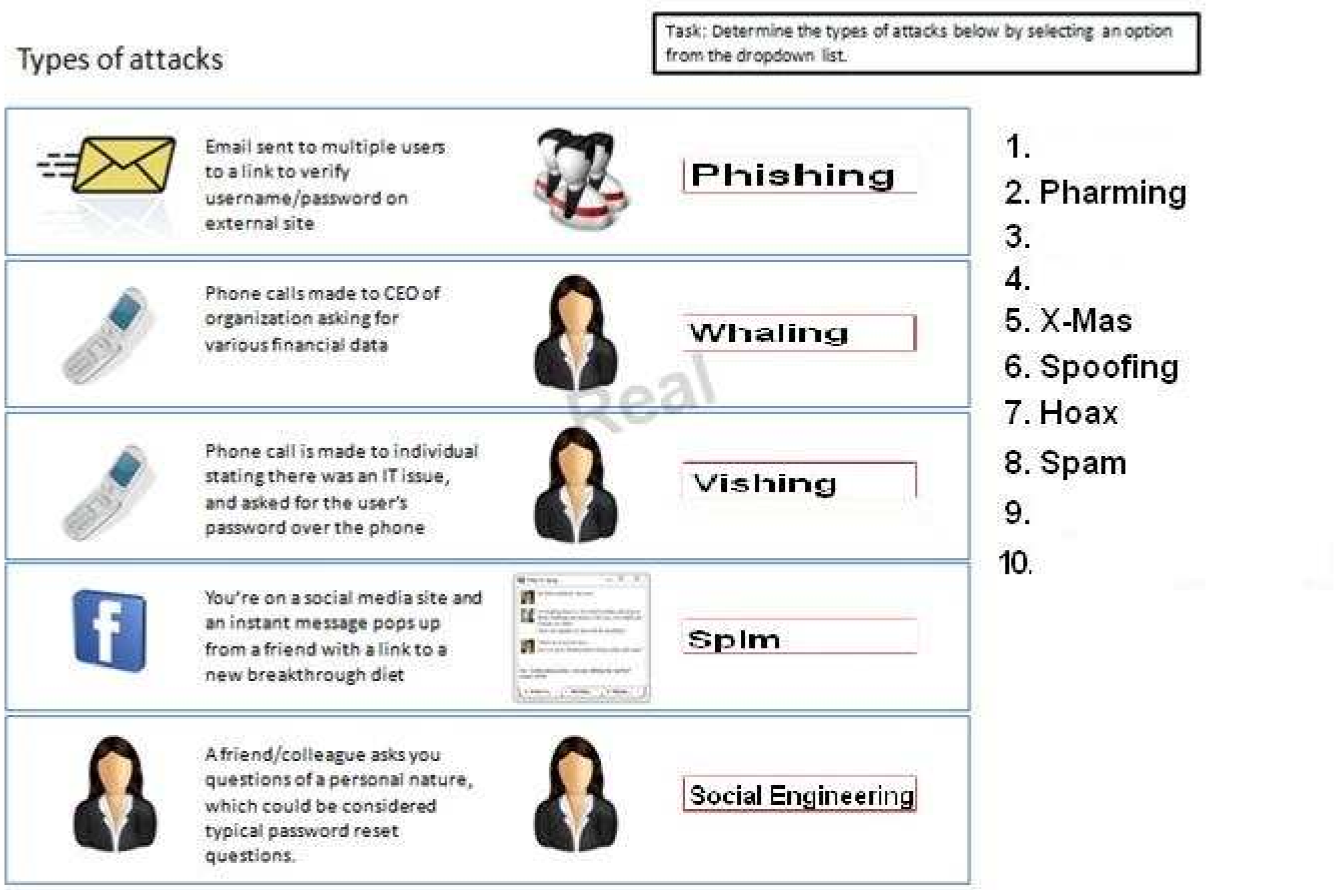
Types of attacks

Task: Determine the types of attacks below by selecting an option from the dropdown list.

Email sent to multiple users to a link to verify username/password on external site	Choose Attack Type
Phone calls made to CEO of organization asking for various financial data	Choose Attack Type
Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone	Choose Attack Type
You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet	Choose Attack Type
A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.	Choose Attack Type

1. Phishing
2. Pharming
3. Vishing
4. Whaling
5. X-Mas
6. Spoofing
7. Hoax
8. Spam
9. Spim
10. Social Engineering

Correct Answer:



Types of attacks

Task: Determine the types of attacks below by selecting an option from the dropdown list.

Email sent to multiple users to a link to verify username/password on external site	Phishing
Phone calls made to CEO of organization asking for various financial data	Whaling
Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone	Vishing
You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet	Splm
A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.	Social Engineering

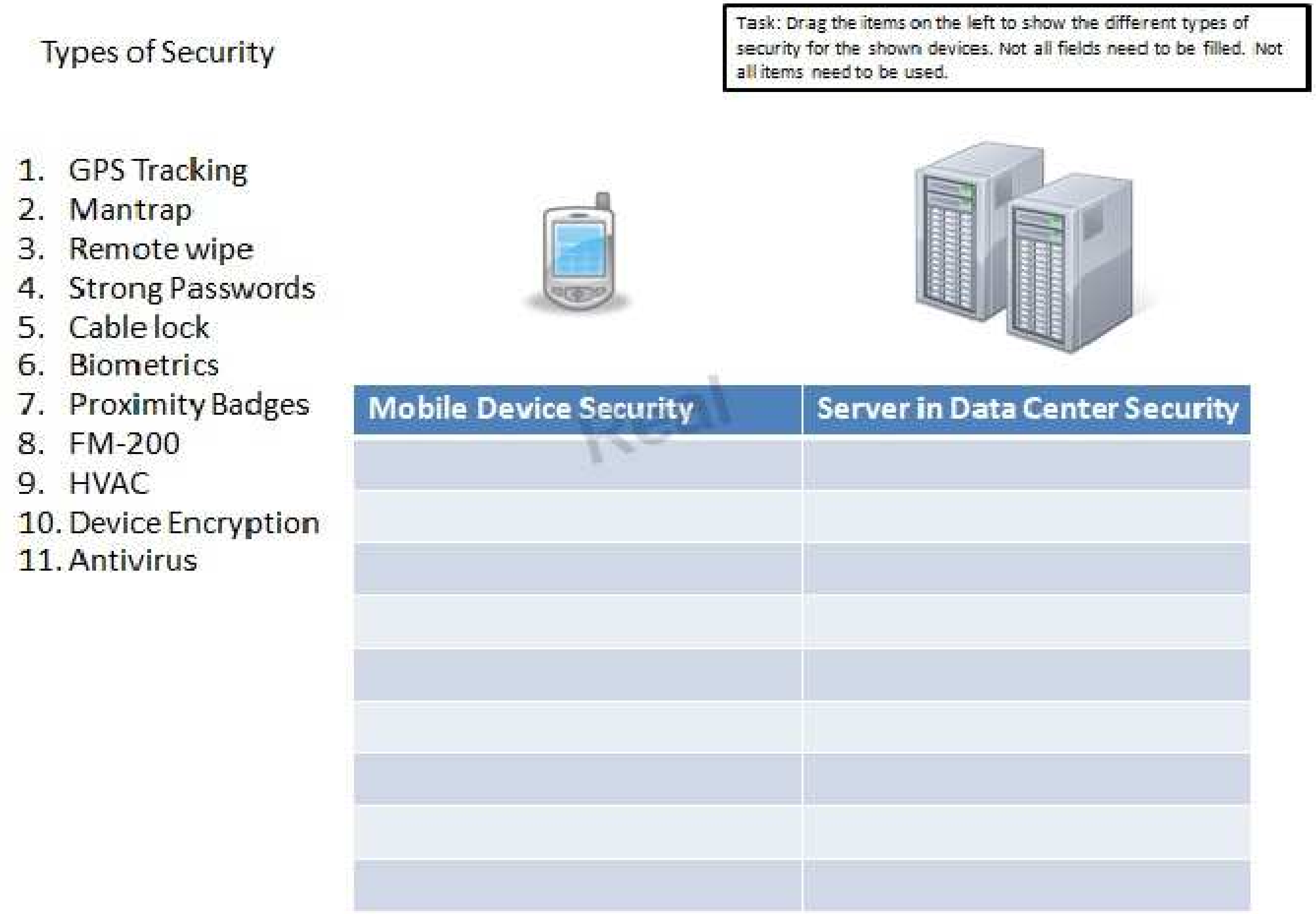
1.
2. Pharming
3.
4.
5. X-Mas
6. Spoofing
7. Hoax
8. Spam
9.
10.

Section: (none)
Explanation

Explanation/Reference:

QUESTION 731
Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.

Select and Place:



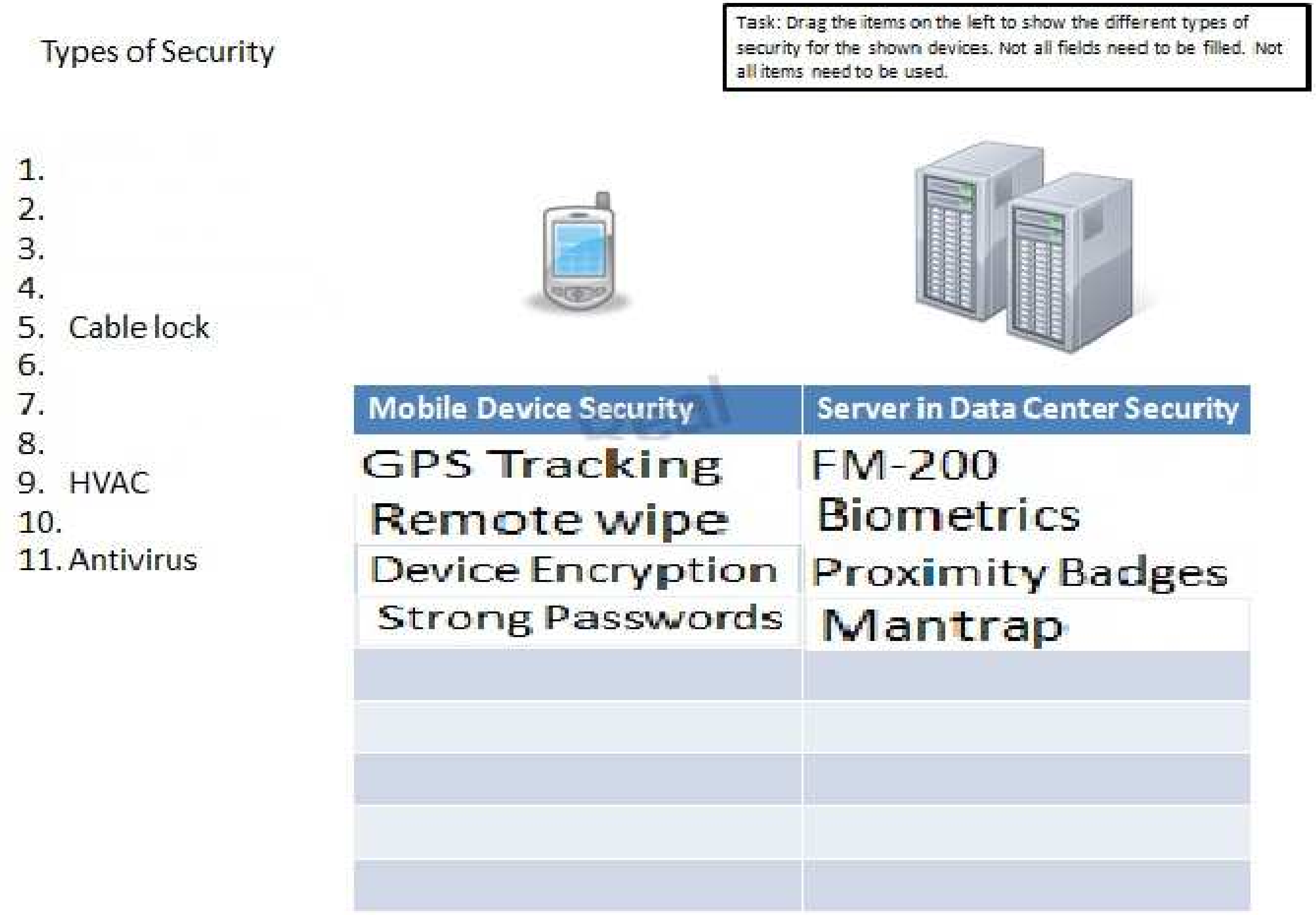
Types of Security

1. GPS Tracking
2. Mantrap
3. Remote wipe
4. Strong Passwords
5. Cable lock
6. Biometrics
7. Proximity Badges
8. FM-200
9. HVAC
10. Device Encryption
11. Antivirus

Task: Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.

Mobile Device Security	Server in Data Center Security

Correct Answer:



Types of Security

1.
2.
3.
4.
5. Cable lock
6.
7.
8.
9. HVAC
10.
11. Antivirus

Task: Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.

Mobile Device Security	Server in Data Center Security
GPS Tracking	FM-200
Remote wipe	Biometrics
Device Encryption	Proximity Badges
Strong Passwords	Mantrap

Section: (none)
Explanation

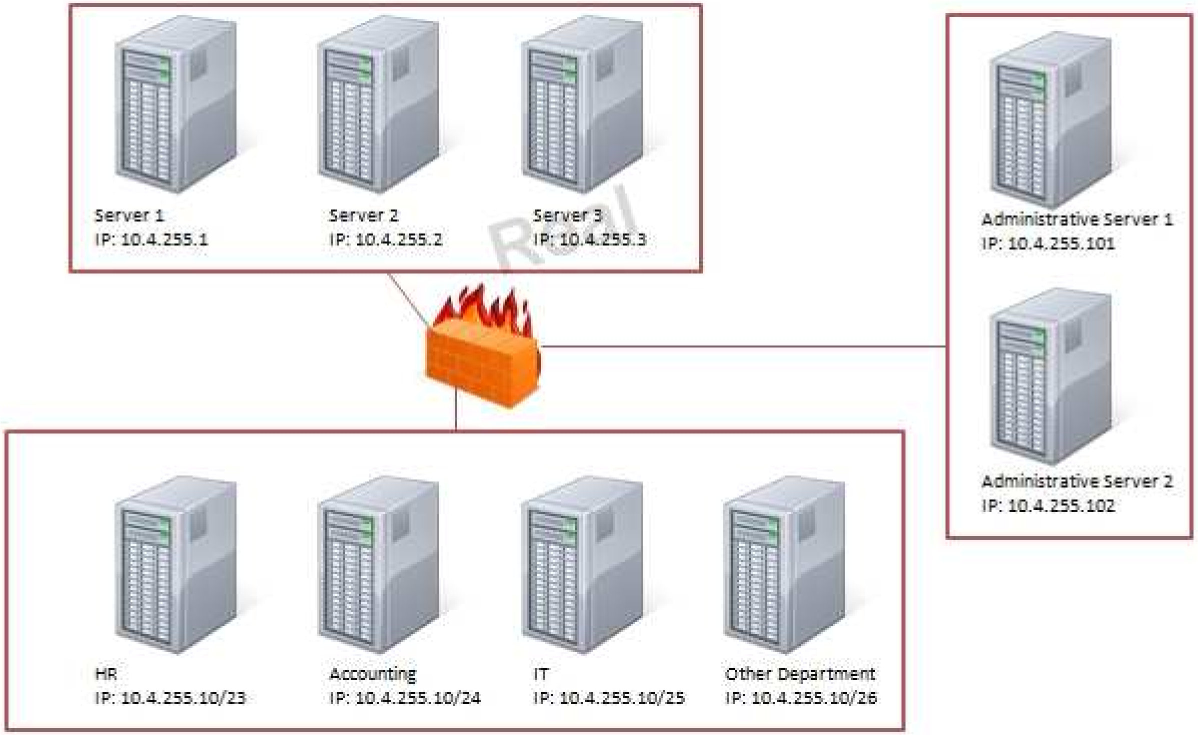
Explanation/Reference:
Mobile Device Security
Server in Data Center Security

QUESTION 732

Configure the Firewall

Task: Configure the firewall (fill out the table) to allow these four rules:

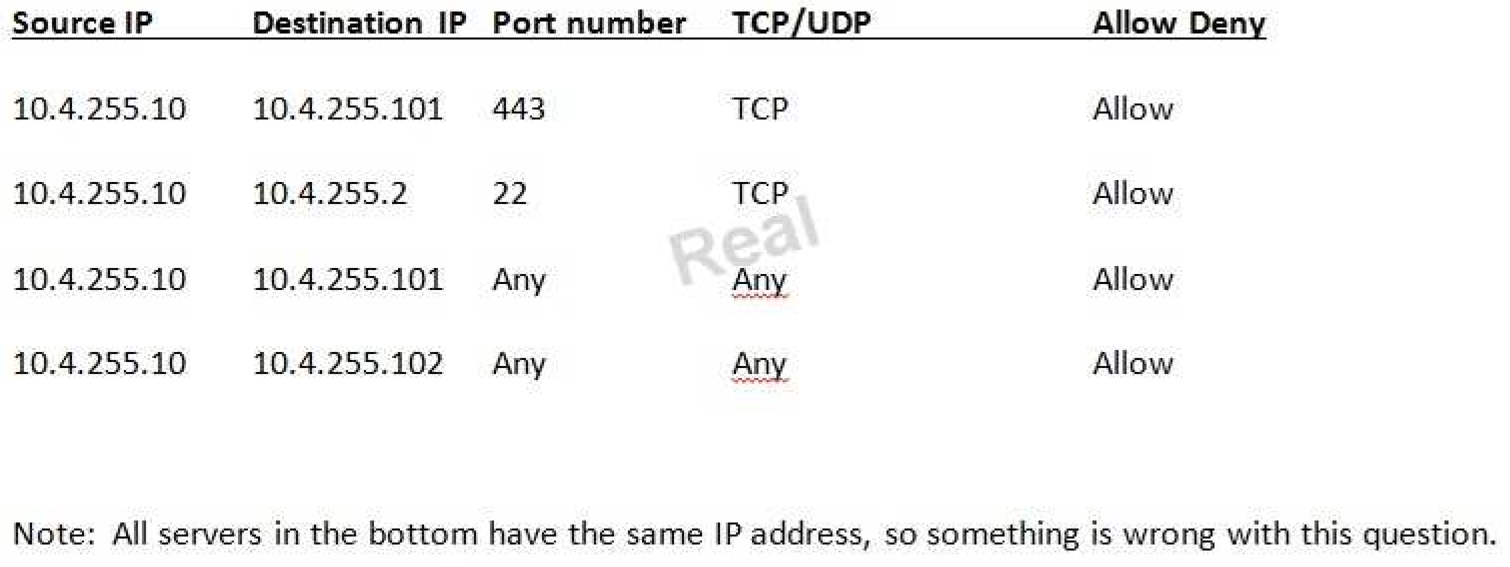
1. Only allow the Accounting computer to have HTTPS access to the Administrative server.
2. Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
3. Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

Correct Answer: Use the following answer for this simulation task.
Section: (none)
Explanation

Explanation/Reference:
below table has all the answers required for this question

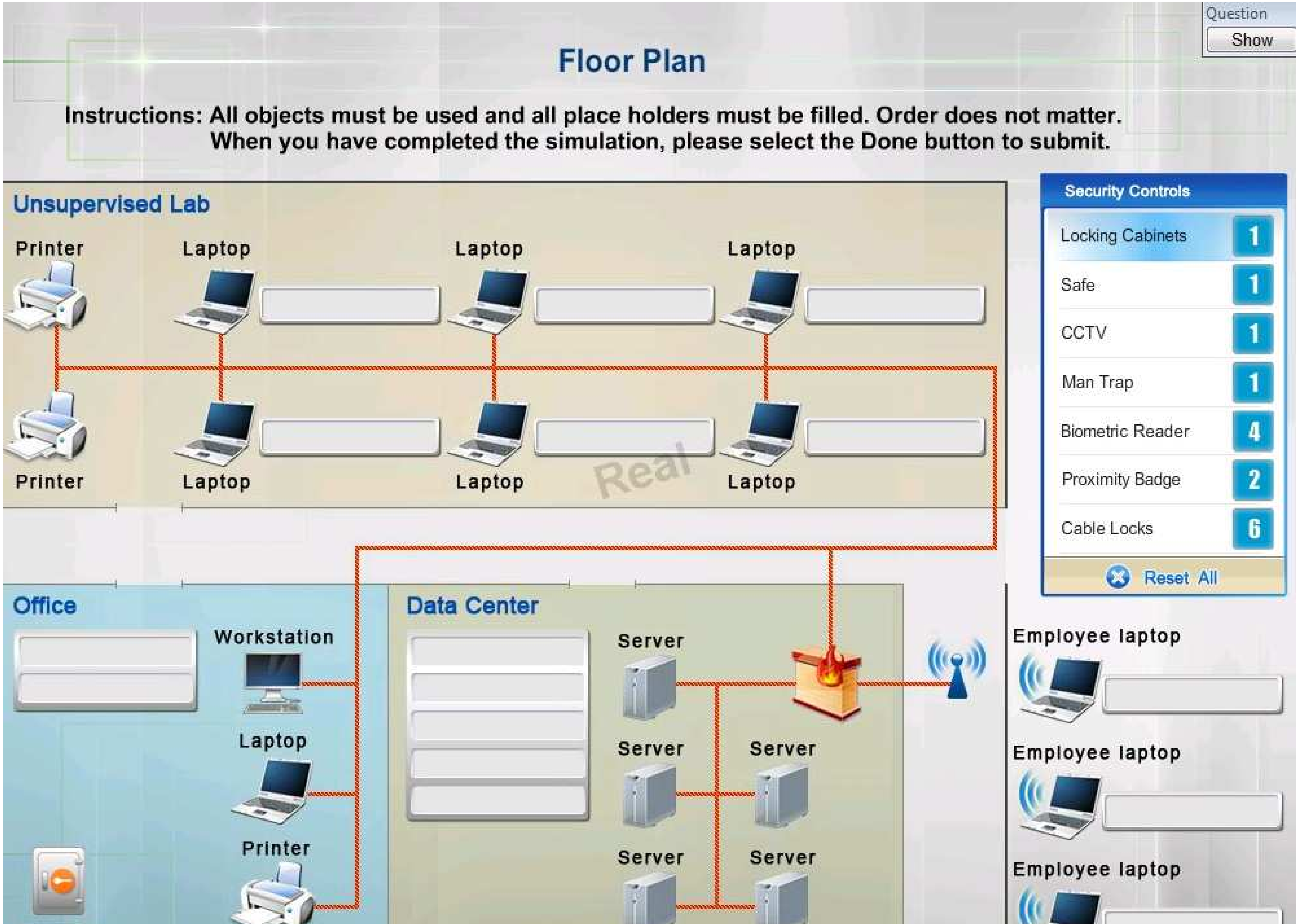


Source IP	Destination IP	Port number	TCP/UDP	Allow Deny
10.4.255.10	10.4.255.101	443	TCP	Allow
10.4.255.10	10.4.255.2	22	TCP	Allow
10.4.255.10	10.4.255.101	Any	Any	Allow
10.4.255.10	10.4.255.102	Any	Any	Allow

Note: All servers in the bottom have the same IP address, so something is wrong with this question.

QUESTION 733
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan-Instructions: All objects must be used and all place holders must be filled Order does not matter When you have completed the simulation, please select the Done button to submit.

Select and Place:



Question

Show

Floor Plan

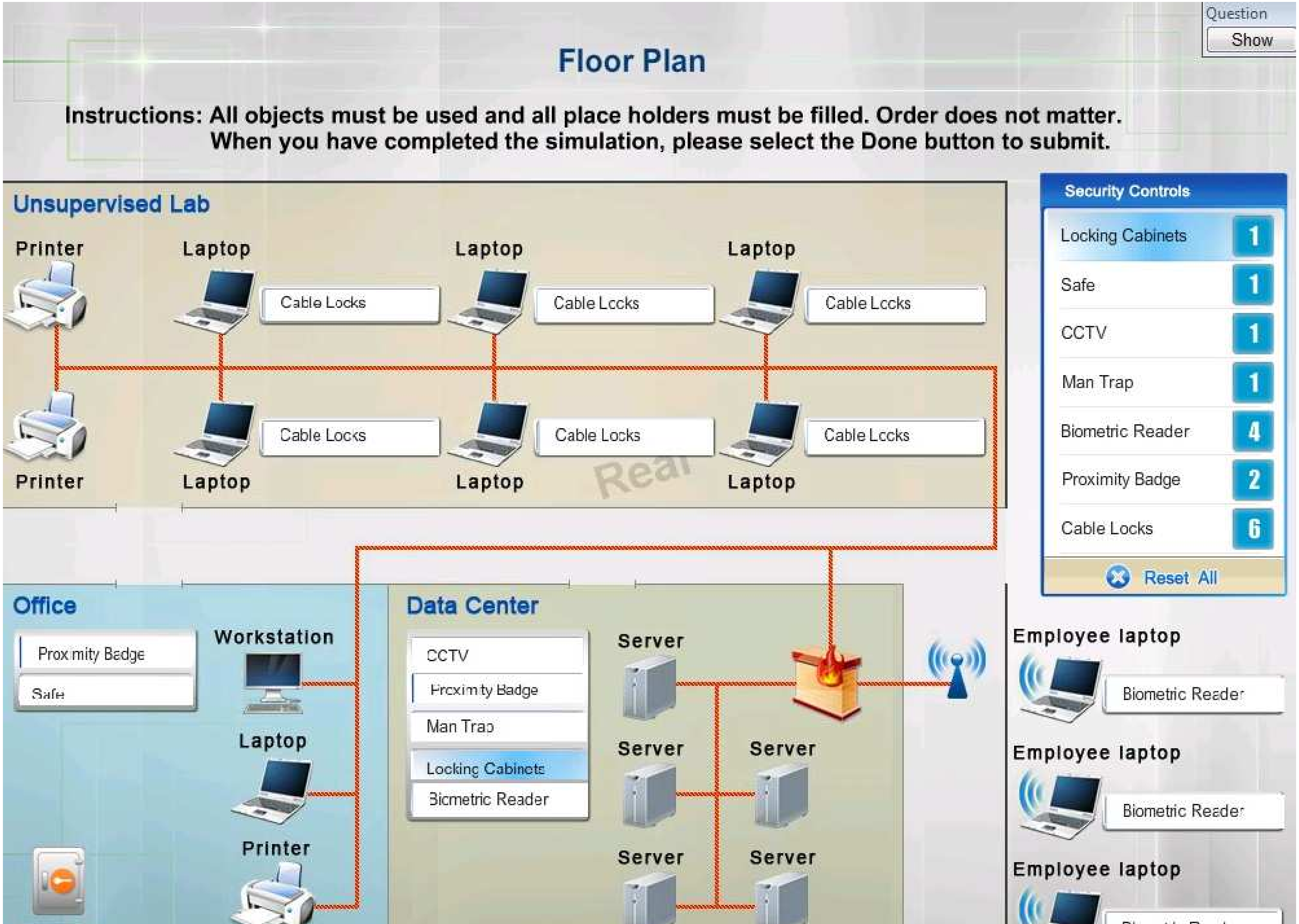
Instructions: All objects must be used and all place holders must be filled. Order does not matter.
When you have completed the simulation, please select the Done button to submit.

Security Controls

Locking Cabinets	1
Safe	1
CCTV	1
Man Trap	1
Biometric Reader	4
Proximity Badge	2
Cable Locks	6

Reset All

Correct Answer:



Floor Plan

Instructions: All objects must be used and all place holders must be filled. Order does not matter.
When you have completed the simulation, please select the Done button to submit.

Security Controls

Locking Cabinets	1
Safe	1
CCTV	1
Man Trap	1
Biometric Reader	4
Proximity Badge	2
Cable Locks	6

Unsupervised Lab

- Laptop: Cable Locks
- Laptop: Cable Locks
- Laptop: Cable Locks
- Laptop: Cable Locks
- Laptop: Cable Locks
- Laptop: Cable Locks

Office

- Proximity Badge
- Safe

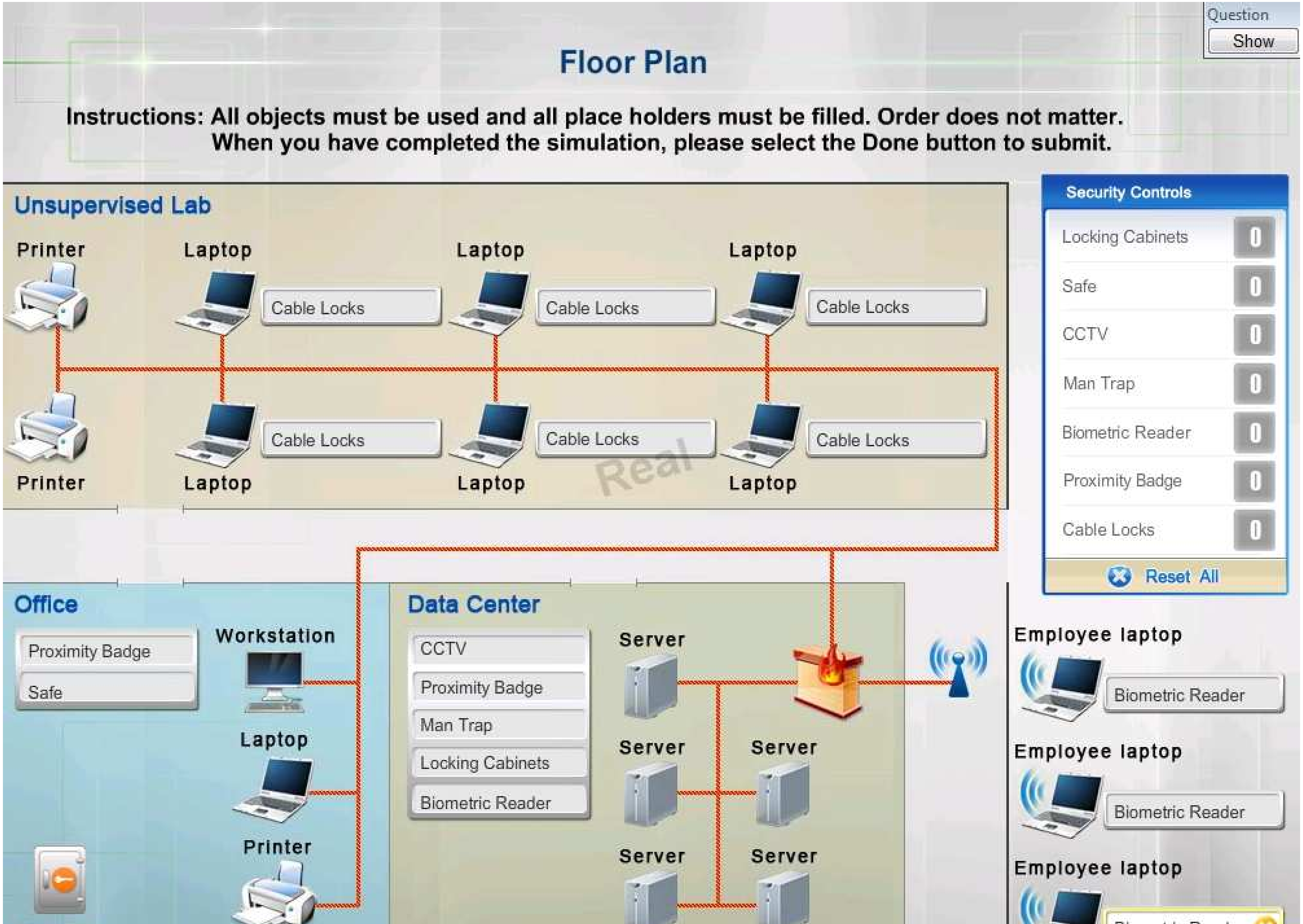
Data Center

- CCTV
- Proximity Badge
- Man Trap
- Locking Cabinets
- Biometric Reader

- Employee laptop: Biometric Reader
- Employee laptop: Biometric Reader
- Employee laptop

Section: (none)
Explanation

Explanation/Reference:



Floor Plan

Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.

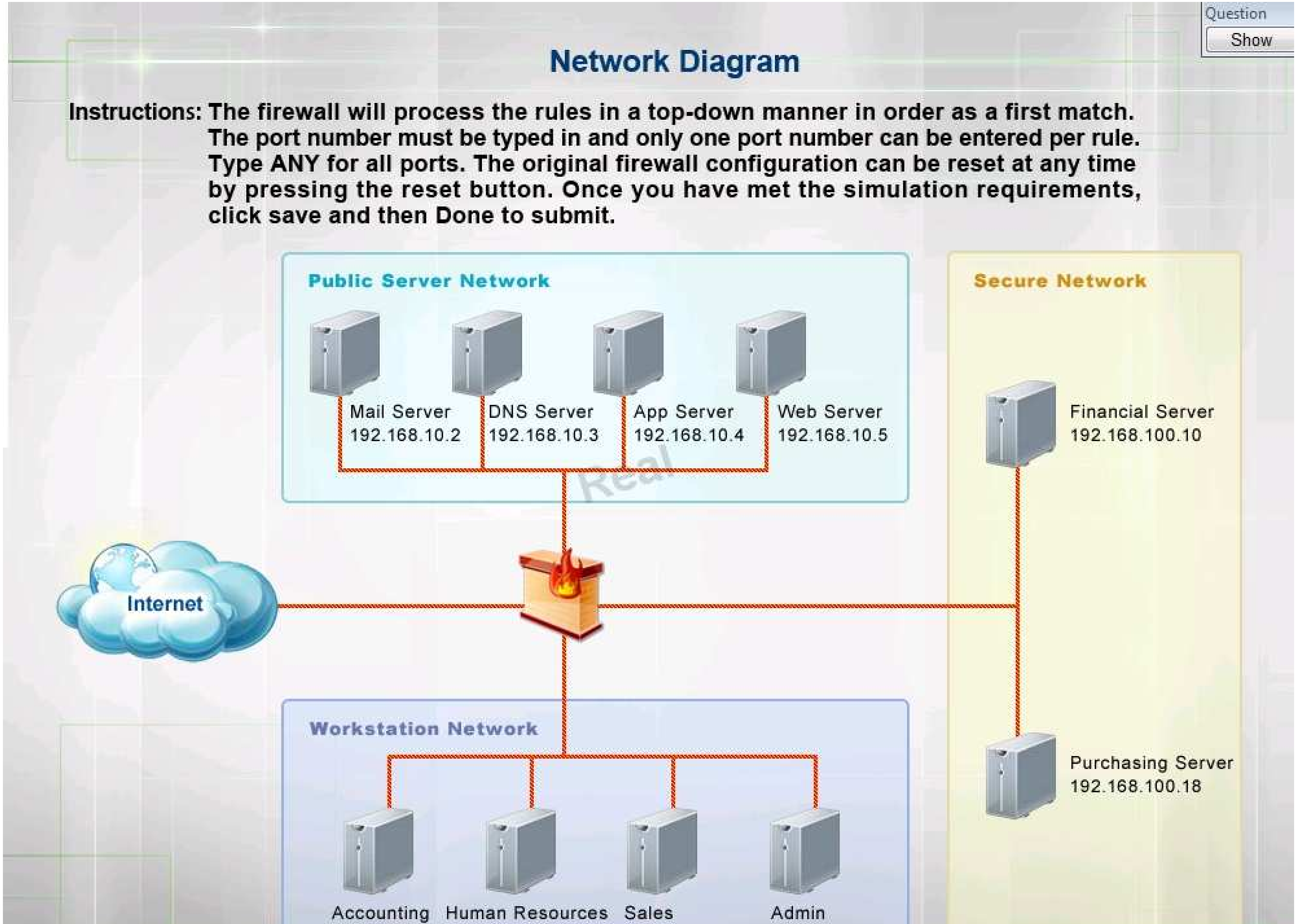
Security Controls	
Locking Cabinets	0
Safe	0
CCTV	0
Man Trap	0
Biometric Reader	0
Proximity Badge	0
Cable Locks	0

QUESTION 734

The security administrator has installed a new firewall which implements an implicit DENY policy by default Click on the firewall and configure it to allow ONLY the following communication.

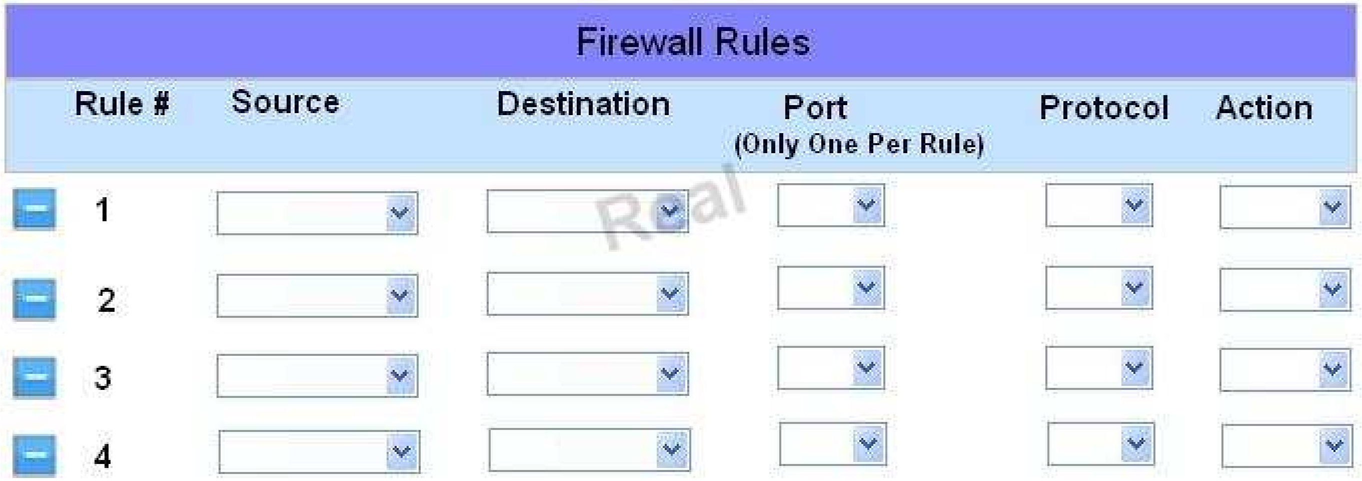
1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port
3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

Instructions: The firewall will process the rules in a top-down manner in order as a first match The port number must be typed in and only one port number can be entered per rule Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.



Network Diagram

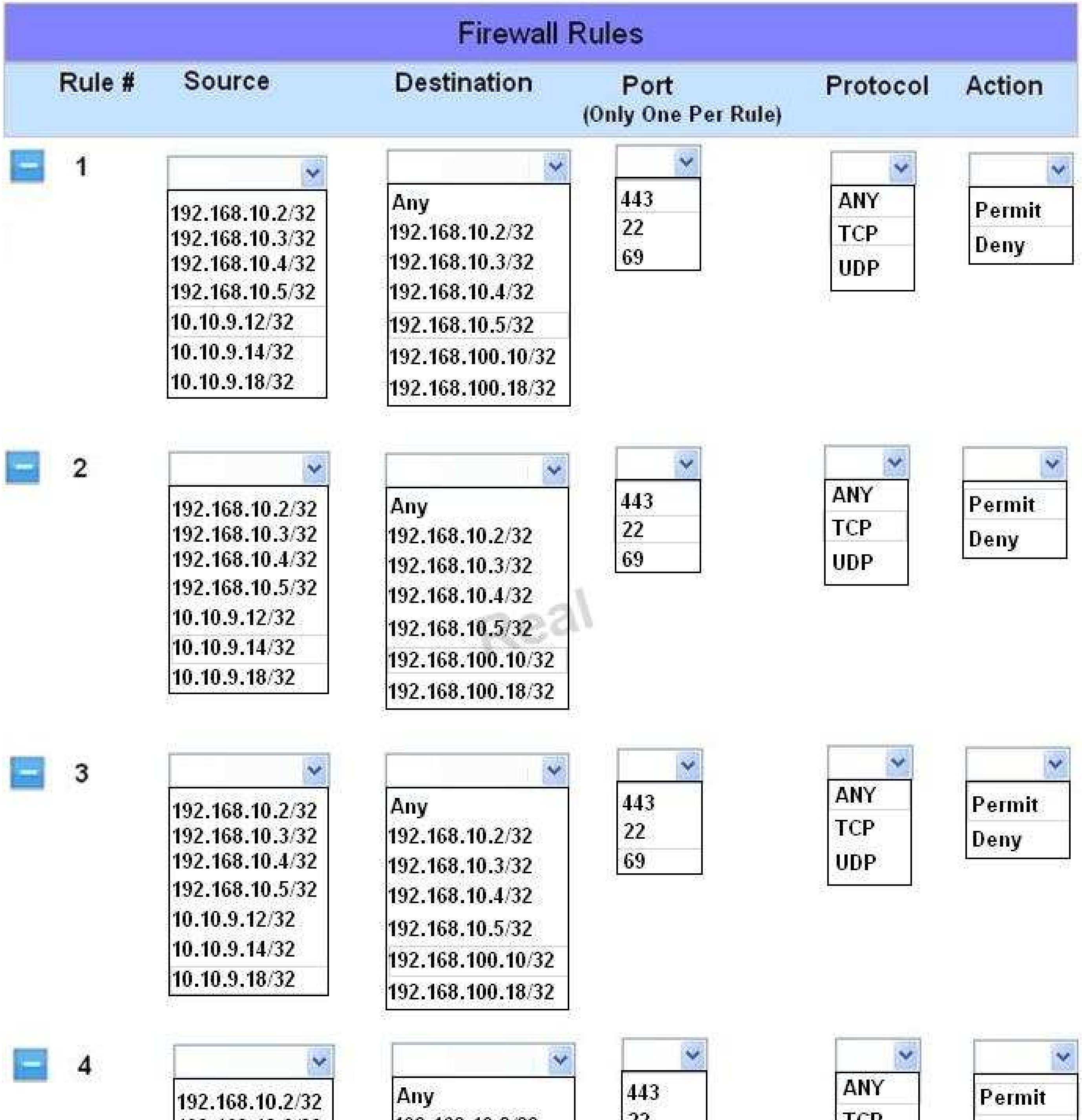
Instructions: The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.



Firewall Rules

	Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
−	1					
−	2					
−	3					
−	4					

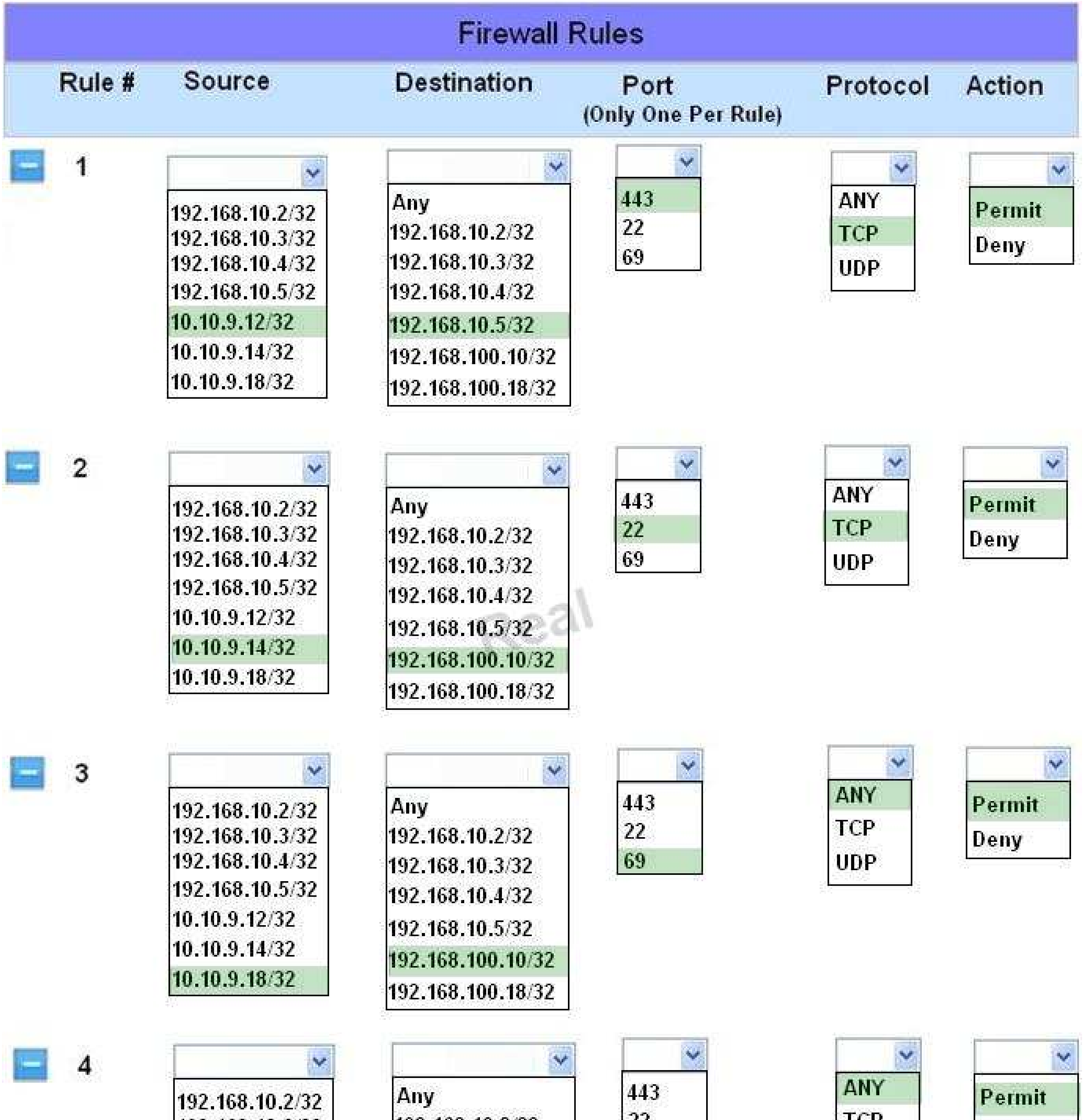
Hot Area:



Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
2	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
3	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
4	192.168.10.2/32	Any	443	ANY	Permit

Correct Answer:

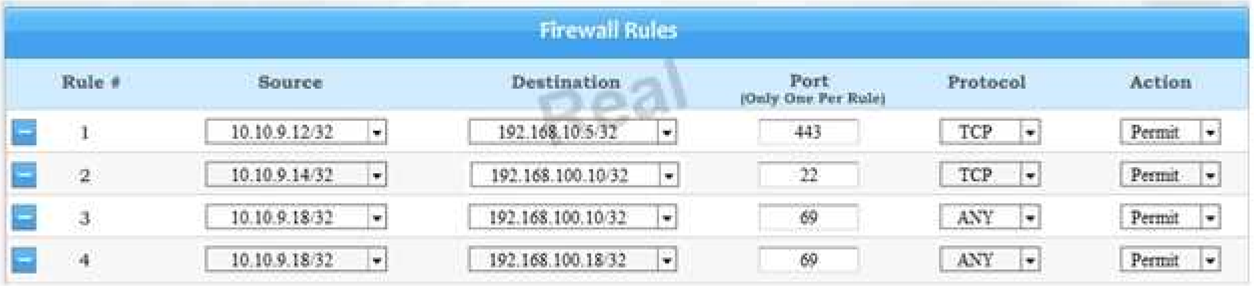


Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 [✓ 10.10.9.12/32] 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 [✓ 192.168.10.5/32] 192.168.100.10/32 192.168.100.18/32	[✓ 443] 22 69	ANY [✓ TCP] UDP	[✓ Permit] Deny
2	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 [✓ 10.10.9.14/32] 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 [✓ 192.168.100.10/32] 192.168.100.18/32	443 [✓ 22] 69	ANY [✓ TCP] UDP	[✓ Permit] Deny
3	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 [✓ 10.10.9.18/32]	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 [✓ 192.168.100.10/32] 192.168.100.18/32	443 22 [✓ 69]	[✓ ANY] TCP UDP	[✓ Permit] Deny
4	192.168.10.2/32 192.168.10.3/32	Any 192.168.10.2/32	443 22	[✓ ANY] TCP	[✓ Permit]

Section: (none)
Explanation

Explanation/Reference:



Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	10.10.9.12/32	192.168.10.5/32	443	TCP	Permit
2	10.10.9.14/32	192.168.100.10/32	22	TCP	Permit
3	10.10.9.18/32	192.168.100.10/32	69	ANY	Permit
4	10.10.9.18/32	192.168.100.18/32	69	ANY	Permit

QUESTION 735
An achievement in providing worldwide Internet security was the signing of certificates associated with which of the following protocols?

A. TCP/IP
B. SSL
C. SCP
D. SSH

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 736
A Chief Information Security Officer (CISO) wants to implement two-factor authentication within the company. Which of the following would fulfill the CISO's requirements?

A. Username and password
B. Retina scan and fingerprint scan
C. USB token and PIN
D. Proximity badge and token

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 737
Which of the following can a security administrator implement on mobile devices that will help prevent unwanted people from viewing the data if the device is left unattended?

A. Screen lock
B. Voice encryption
C. GPS tracking
D. Device encryption

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 738
Which of the following would a security administrator implement in order to identify a problem between two systems that are not communicating properly?

A. Protocol analyzer
B. Baseline report
C. Risk assessment
D. Vulnerability scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 739
Which of the following can result in significant administrative overhead from incorrect reporting?

A. Job rotation
B. Acceptable usage policies
C. False positives
D. Mandatory vacations

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 740
A security administrator wants to perform routine tests on the network during working hours when certain applications are being accessed by the most people.
Which of the following would allow the security administrator to test the lack of security controls for those applications with the least impact to the system?

A. Penetration test
B. Vulnerability scan
C. Load testing
D. Port scanner
Real 3
CompTIA SY0-401 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 741
Which of the following risk concepts requires an organization to determine the number of failures per year?

A. SLE
B. ALE
C. MTBF

D. Quantitative analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 742
A system security analyst using an enterprise monitoring tool notices an unknown internal host exfiltrating files to several foreign IP addresses. Which of the following would be an appropriate mitigation technique?

A. Disabling unnecessary accounts
B. Rogue machine detection
C. Encrypting sensitive files
D. Implementing antivirus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 743
Three of the primary security control types that can be implemented are.

A. Supervisory, subordinate, and peer.
B. Personal, procedural, and legal.
C. Operational, technical, and management.
D. Mandatory, discretionary, and permanent.
Real 4
CompTIA SY0-401 Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 744
The helpdesk reports increased calls from clients reporting spikes in malware infections on their systems. Which of the following phases of incident response is MOST appropriate as a FIRST response?

A. Recovery
B. Follow-up
C. Validation
D. Identification
E. Eradication
F. Containment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 745
Sara, the Chief Information Officer (CIO), has tasked the IT department with redesigning the network to rely less on perimeter firewalls, to implement a standard operating environment for client devices, and to disallow personally managed devices on the network. Which of the following is Sara's GREATEST concern?

A. Malicious internal attacks
B. Data exfiltration
C. Audit findings
D. Incident response

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 746
Which of the following data loss prevention strategies mitigates the risk of replacing hard drives that cannot be sanitized?

A. Virtualization
B. Patch management
C. Full disk encryption
D. Database encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 747
Which of the following does Jane, a software developer, need to do after compiling the source code of a program to attest the authorship of the binary?

A. Place Jane's name in the binary metadata
B. Use Jane's private key to sign the binary
C. Use Jane's public key to sign the binary

D. Append the source code to the binary

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 748
The annual loss expectancy can be calculated by:

A. Dividing the annualized rate of return by single loss expectancy.
B. Multiplying the annualized rate of return and the single loss expectancy.

C. Subtracting the single loss expectancy from the annualized rate of return.
D. Adding the single loss expectancy and the annualized rate of return.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 749
Which of the following should Jane, the security administrator, do FIRST when an employee reports the loss of a corporate mobile device?

A. Remotely lock the device with a PIN
B. Enable GPS location and record from the camera
C. Remotely uninstall all company software
D. Remotely initiate a device wipe

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 750
An application company sent out a software patch for one of their applications on Monday. The company has been receiving reports about intrusion attacks from their customers on Tuesday. Which of the following attacks does this describe?

A. Zero day

B. Directory traversal
C. Logic bomb
D. Session hijacking

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 751
Which of the following protocols would be implemented to secure file transfers using SSL?

A. TFTP
B. SCP
C. SFTP
D. FTPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 752
Which of the following are used to implement VPNs? (Select TWO).

A. SFTP
B. IPSec
C. HTTPS
D. SNMP
E. SSL

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
answer is valid.

QUESTION 753
A company recently implemented a TLS on their network. The company is MOST concerned with:

A. Confidentiality
B. Availability

C. Integrity
D. Accessibility

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 754
Which of the following describes how an attacker can send unwanted advertisements to a mobile device?

A. Man-in-the-middle
B. Bluejacking
C. Bluesnarfing
D. Packet sniffing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 755
A network device that protects an enterprise based only on source and destination addresses is BEST described as:

A. IDS.
B. ACL.
C. Stateful packet filtering.
D. Simple packet filtering.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 756
A human resources employee receives an email from a family member stating there is a new virus going around. In order to remove the virus, a user must delete the Boot.ini file from the system immediately. This is an example of which of the following? CompTIA SY0-401 Exam
Real 391

A. Hoax
B. Spam
C. Whaling
D. Phishing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 757
A third party application has the ability to maintain its own user accounts or it may use single signon.
To use single sign-on, the application is requesting the following information:
OU=Users,
DC=Domain, DC=COM. This application is requesting which of the following authentication services?

A. TACACS+
B. RADIUS
C. LDAP
D. Kerberos

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 758
Power and data cables from the network center travel through the building's boiler room.
Which of
the following should be used to prevent data emanation?

A. Video monitoring
B. EMI shielding
C. Plenum CAT6 UTP
D. Fire suppression

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 759
Which of the following must a security administrator implement to isolate public facing servers

from both the corporate network and the Internet?

A. NAC
B. IPSec
C. DMZ
D. NAT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 760
Which of the following protocols provides fast, unreliable file transfer?

A. TFTP
B. SFTP
C. Telnet
D. FTPS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 761
Which of the following digital certificate management practices will ensure that a lost certificate is not compromised?

A. Key escrow
B. Non-repudiation
C. Recovery agent
D. CRL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 762
A recent computer breach has resulted in the incident response team needing to perform a

forensics examination. Upon examination, the forensics examiner determines that they cannot tell which captured hard drive was from the device in question. Which of the following would have prevented the confusion experienced during this examination?

A. Perform routine audit

B. Chain of custody
C. Evidence labeling
D. Hashing the evidence

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 763
An IT staff member was entering the datacenter when another person tried to piggyback into the datacenter as the door was opened. While the IT staff member attempted to QUESTION NO: the other individual by politely asking to see their badge, the individual refused and ran off into the datacenter. Which of the following should the IT staff member do NEXT?

A. Call the police while tracking the individual on the closed circuit television system
B. Contact the forensics team for further analysis
C. Chase the individual to determine where they are going and what they are doing
D. Contact the onsite physical security team with a description of the individual

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 764
During a recent user awareness and training session, a new staff member asks the Chief Information Security Officer (CISO) why the company does not allow personally owned devices into the company facilities. Which of the following represents how the CISO should respond?

A. Company A views personally owned devices as creating an unacceptable risk to the organizational IT systems.
B. Company A has begun to see zero-day attacks against personally owned devices disconnected from the network.
C. Company A believes that staff members should be focused on their work while in the company's facilities.
CompTIA SY0-401 Exam

Real 394

D. Company A has seen social engineering attacks against personally owned devices and does not allow their use.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 765
A customer has provided an email address and password to a website as part of the login process. Which of the following BEST describes the email address?

A. Identification
B. Authorization
C. Access control
D. Authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 766
Which of the following is designed to ensure high availability of web based applications?

A. Proxies
B. Load balancers
C. URL filtering
D. Routers

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 767
The administrator would like to implement hardware assisted full disk encryption on laptops. Which of the following would MOST likely be used to meet this goal?

A. TPM

B. USB Drive

C. Key Escrow

D. PKI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 768
Jane, a security administrator, wants to harden the web server. Which of the following could she perform to accomplish this task?

A. Implement remote sanitization

B. Disable unnecessary services

C. Install mantraps in the datacenter

D. Compare baseline configurations

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 769
Which of the following policies could be implemented to help prevent users from displaying their login credentials in open view for everyone to see?

A. Privacy
B. Clean desk
C. Job rotation
D. Password complexity

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 770
Which of the following is another, more common, name for EAPOL?

A. LDAP

B. 802.1X
C. LDAPS
D. 802.12

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 771
If you don't know the MAC address of a Windows-based machine, what command-line utility can you use to ascertain it?

A. macconfig
B. ifconfig
C. ipconfig
D. config

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 772
In the Windows world, what tool is used to disable a port?

A. System Manager
B. System Monitor
C. Performance Monitor
D. Windows Firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 773
A set of standardized system images with a pre-defined set of applications is used to build enduser workstations. The security administrator has scanned every workstation to create a current inventory of all applications that are installed on active workstations and is documenting which applications are out-of-date and could be exploited. The security administrator is determining the:

A. Attack surface.
B. Application hardening effectiveness.
C. Application baseline.
D. OS hardening effectiveness.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 774
A perimeter survey finds that the wireless network within a facility is easily reachable outside of the physical perimeter. Which of the following should be adjusted to mitigate this risk?

A. CCMP
B. MAC filter
C. SSID broadcast
D. Power level controls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 775
Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

A. Protocol analyzer
B. Vulnerability scan
C. Penetration test
D. Port scanner

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 776
An administrator values transport security strength above network speed when implementing an SSL VPN. Which of the following encryption ciphers would BEST meet their needs? CompTIA SY0-401 Exam Real 398

A. SHA256
B. RC4
C. 3DES
D. AES128

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 777
All of the following are encryption types EXCEPT:

A. Full disk
B. SMIME
C. File and folder
D. RADIUS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 778
Which of the following is used by Matt, a security administrator, to lower the risks associated with electrostatic discharge, corrosion, and thermal breakdown?

A. Temperature and humidity controls
B. Routine audits
C. Fire suppression and EMI shielding
D. Hot and cold aisles

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 779
When integrating source material from an open source project into a highly secure environment, which of the following precautions should prevent hidden threats? CompTIA SY0-401 Exam Real 399

A. Design review
B. Code review
C. Risk assessment
D. Vulnerability scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 780
Which of the following would MOST likely belong in the DMZ? (Select TWO).

A. Finance servers
B. Backup servers
C. Web servers
D. SMTP gateways
E. Laptops

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 781

When verifying file integrity on a remote system that is bandwidth limited, which of the following tool combinations provides the STRONGEST confidence?

A. MD5 and 3DES
B. MD5 and SHA-1
C. SHA-256 and RSA
D. SHA-256 and AES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
corrected.

QUESTION 782
Which of the following protocols operates at the HIGHEST level of the OSI model?

A. ICMP
B. IPSec
C. SCP
D. TCP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 783
Joe, the system administrator, has been asked to calculate the Annual Loss Expectancy (ALE) for a $5,000 server, which often crashes. In the past year, the server has crashed 10 times, requiring a system reboot to recover with only 10% loss of data or function. Which of the following is the ALE of this server?

Real 5
CompTIA SY0-401 Exam

A. $500
B. $5,000

C. $25,000
D. $50,000

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 784
Which of the following should an administrator implement to research current attack methodologies?

A. Design reviews
B. Honeypot
C. Vulnerability scanner
D. Code reviews

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
answer is valid.

QUESTION 785
Which of the following can be implemented in hardware or software to protect a web server from cross-site scripting attacks?

A. Intrusion Detection System
B. Flood Guard Protection
C. Web Application Firewall
D. URL Content Filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 786
Which of the following means of wireless authentication is easily vulnerable to spoofing?

Real 6
CompTIA SY0-401 Exam

A. MAC Filtering
B. WPA - LEAP
C. WPA - PEAP
D. Enabled SSID

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 787
The BEST methods for a web developer to prevent the website application code from being vulnerable to cross-site request forgery (XSRF) are to: (Select TWO).

A. permit redirection to Internet-facing web URLs.
B. ensure all HTML tags are enclosed in angle brackets, e.g., "<" and ">".
C. validate and filter input on the server side and client side.
D. use a web proxy to pass website requests between the user and the application.
E. restrict and sanitize use of special characters in input and URLs.

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 788
Jane, a security administrator, needs to implement a secure wireless authentication method that uses a remote RADIUS server for authentication.

Which of the following is an authentication method Jane should use?

A. WPA2-PSK
B. WEP-PSK
C. CCMP
D. LEAP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 789
Real 7
CompTIA SY0-401 Exam
Computer evidence at a crime scene is documented with a tag stating who had possession of the evidence at a given time.

Which of the following does this illustrate?

A. System image capture
B. Record time offset
C. Order of volatility
D. Chain of custody

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 790
A network administrator is configuring access control for the sales department which has high employee turnover. Which of the following is BEST suited when assigning user rights to individuals in the sales department?

A. Time of day restrictions
B. Group based privileges
C. User assigned privileges

D. Domain admin restrictions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 791
Which of the following is being tested when a company's payroll server is powered off for eight hours?

A. Succession plan
B. Business impact document
C. Continuity of operations plan
D. Risk assessment plan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 792
A security analyst, Ann, is reviewing an IRC channel and notices that a malicious exploit has been created for a frequently used application. She notifies the software vendor and asks them for remediation steps, but is alarmed to find that no patches are available to mitigate this vulnerability.

Which of the following BEST describes this exploit?

A. Malicious insider threat
B. Zero-day
C. Client-side attack
D. Malicious add-on

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 793
A security administrator has concerns about new types of media which allow for the mass distribution of personal comments to a select group of people. To mitigate the risks involved with this media, employees should receive training on which of the following?

A. Peer to Peer
B. Mobile devices
C. Social networking
D. Personally owned devices

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 794
A network administrator is responsible for securing applications against external attacks. Every month, the underlying operating system is updated. There is no process in place for other software updates.

Which of the following processes could MOST effectively mitigate these risks?

Real 9
CompTIA SY0-401 Exam

A. Application hardening
B. Application change management
C. Application patch management
D. Application firewall review

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 795
A software developer is responsible for writing the code on an accounting application. Another software developer is responsible for developing code on a system in human resources. Once a year they have to switch roles for several weeks.

Which of the following practices is being implemented?

A. Mandatory vacations
B. Job rotation
C. Least privilege
D. Separation of duties

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 796
A network engineer is designing a secure tunneled VPN. Which of the following protocols would be the MOST secure?

A. IPsec
B. SFTP
C. BGP
D. PPTP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 797
Real 10
CompTIA SY0-401 Exam
Which of the following implementation steps would be appropriate for a public wireless hot-spot?

A. Reduce power level

B. Disable SSID broadcast
C. Open system authentication
D. MAC filter

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 798
Which of the following is a step in deploying a WPA2-Enterprise wireless network?

A. Install a token on the authentication server
B. Install a DHCP server on the authentication server
C. Install an encryption key on the authentication server
D. Install a digital certificate on the authentication server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 799
Which of the following controls would allow a company to reduce the exposure of sensitive systems from unmanaged devices on internal networks?

A. 802.1x
B. Data encryption
C. Password strength
D. BGP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 800
Which of the following preventative controls would be appropriate for responding to a directive to

reduce the attack surface of a specific host?

A. Installing anti-malware
B. Implementing an IDS
C. Taking a baseline configuration
D. Disabling unnecessary services

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 801
A security manager must remain aware of the security posture of each system. Which of the following supports this requirement?

A. Training staff on security policies
B. Establishing baseline reporting
C. Installing anti-malware software
D. Disabling unnecessary accounts/services

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 802
Deploying a wildcard certificate is one strategy to:

A. Secure the certificate's private key.
B. Increase the certificate's encryption key length.
C. Extend the renewal date of the certificate.
D. Reduce the certificate management burden.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 803
The security administrator needs to manage traffic on a layer 3 device to support FTP from a new remote site. Which of the following would need to be implemented?

A. Implicit deny
B. VLAN management
C. Port security
D. Access control lists

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 804
Which of the following ports is used for SSH, by default?

A. 23
B. 32
C. 12
D. 22

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 805
A network administrator has been tasked with securing the WLAN. Which of the following cryptographic products would be used to provide the MOST secure environment for the WLAN?

A. WPA2 CCMP
B. WPA
C. WPA with MAC filtering
D. WPA2 TKIP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 806
A server with the IP address of 10.10.2.4 has been having intermittent connection issues. The logs

Real 13
CompTIA SY0-401 Exam
show repeated connection attempts from the following IPs:

10.10.3.16

10.10.3.23

212.178.24.26

217.24.94.83

These attempts are overloading the server to the point that it cannot respond to traffic. Which of the following attacks is occurring?

A. XSS
B. DDoS
C. DoS
D. Xmas

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 807
Which of the following ciphers would be BEST used to encrypt streaming video?

A. RSA
B. RC4
C. SHA1
D. 3DES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 808
A user attempting to log on to a workstation for the first time is prompted for the following information before being granted access: username, password, and a four-digit security pin that was mailed to him during account registration. This is an example of which of the following?

A. Dual-factor authentication
B. Multifactor authentication

C. Single factor authentication
D. Biometric authentication

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 809
Which of the following ports and protocol types must be opened on a host with a host-based firewall to allow incoming SFTP connections?

A. 21/UDP
B. 21/TCP
C. 22/UDP
D. 22/TCP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 810
A user, Ann, is reporting to the company IT support group that her workstation screen is blank other than a window with a message requesting payment or else her hard drive will be formatted. Which of the following types of malware is on Ann's workstation?

A. Trojan
B. Spyware
C. Adware
D. Ransomware

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
answer is corrected.

QUESTION 811
Real 50

Which of the following controls can be implemented together to prevent data loss in the event of theft of a mobile device storing sensitive information? (Select TWO).

A. Full device encryption
B. Screen locks
C. GPS
D. Asset tracking
E. Inventory control

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 812
A way to assure data at-rest is secure even in the event of loss or theft is to use:

A. Full device encryption.
B. Special permissions on the file system.
C. Trusted Platform Module integration.
D. Access Control Lists.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 813
A security audit identifies a number of large email messages being sent by a specific user from their company email account to another address external to the company. These messages were sent prior to a company data breach, which prompted the security audit. The user was one of a few people who had access to the leaked data. Review of the suspect's emails show they consist mostly of pictures of the user at various locations during a recent vacation. No suspicious activities from other users who have access to the data were discovered.

Which of the following is occurring?

A. The user is encrypting the data in the outgoing messages.
B. The user is using steganography.
C. The user is spamming to obfuscate the activity.
D. The user is using hashing to embed data in the emails.
Real 51
CompTIA SY0-401 Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 814
A security analyst is reviewing firewall logs while investigating a compromised web server. The following ports appear in the log:

22, 25, 445, 1433, 3128, 3389, 6667

Which of the following protocols was used to access the server remotely?

A. LDAP
B. HTTP
C. RDP
D. HTTPS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 815
An organization does not want the wireless network name to be easily discovered. Which of the following software features should be configured on the access points?

A. SSID broadcast

B. MAC filter
C. WPA2
D. Antenna placement

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 816
A computer is suspected of being compromised by malware. The security analyst examines the computer and finds that a service called Telnet is running and connecting to an external website

over port 443. This Telnet service was found by comparing the system's services to the list of standard services on the company's system image. This review process depends on:

A. MAC filtering.
B. System hardening.
C. Rogue machine detection.
D. Baselining.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 817
A software developer wants to prevent stored passwords from being easily decrypted. When the password is stored by the application, additional text is added to each password before the password is hashed. This technique is known as:

A. Symmetric cryptography.
B. Private key cryptography.
C. Salting.

D. Rainbow tables.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 818
In which of the following steps of incident response does a team analyze the incident and determine steps to prevent a future occurrence?

A. Mitigation
B. Identification
C. Preparation
D. Lessons learned

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 819
A security technician has been asked to recommend an authentication mechanism that will allow users to authenticate using a password that will only be valid for a predefined time interval. Which of the following should the security technician recommend?

A. CHAP
B. TOTP
C. HOTP
D. PAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 820
A security administrator must implement a wireless encryption system to secure mobile devices' communication. Some users have mobile devices which only support 56-bit encryption. Which of the following wireless encryption methods should be implemented?

A. RC4
B. AES
C. MD5
D. TKIP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 821
After a security incident involving a physical asset, which of the following should be done at the beginning?

A. Record every person who was in possession of assets, continuing post-incident.
B. Create working images of data in the following order: hard drive then RAM.
C. Back up storage devices so work can be performed on the devices immediately.
D. Write a report detailing the incident and mitigation suggestions.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 822
Which of the following is the GREATEST security risk of two or more companies working together under a Memorandum of Understanding?

A. Budgetary considerations may not have been written into the MOU, leaving an entity to absorb more cost than intended at signing.
B. MOUs have strict policies in place for services performed between the entities and the penalties for compromising a partner are high.
C. MOUs are generally loose agreements and therefore may not have strict guidelines in place to protect sensitive data between the two entities.
D. MOUs between two companies working together cannot be held to the same legal standards as SLAs.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 823
Joe, a user, reports to the system administrator that he is receiving an error stating his certificate has been revoked. Which of the following is the name of the database repository for these certificates?

A. CSR
B. OSCP
C. CA
D. CRL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 824
A software company has completed a security assessment. The assessment states that the company should implement fencing and lighting around the property. Additionally, the assessment states that production releases of their software should be digitally signed. Given the recommendations, the company was deficient in which of the following core security areas? (Select TWO).

A. Fault tolerance
B. Encryption
C. Availability
D. Integrity
E. Safety
F. Confidentiality

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 825
A user was reissued a smart card after the previous smart card had expired. The user is able to log into the domain but is now unable to send digitally signed or encrypted email. Which of the following would the user need to perform?

A. Remove all previous smart card certificates from the local certificate store.
B. Publish the new certificates to the global address list.
C. Make the certificates available to the operating system.
D. Recover the previous smart card certificates.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 826
Users are encouraged to click on a link in an email to obtain exclusive access to the newest version of a popular Smartphone. This is an example of.

A. Scarcity
B. Familiarity
C. Intimidation
D. Trust

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 827

Real 56
CompTIA SY0-401 Exam
Which of the following types of attacks involves interception of authentication traffic in an attempt to gain unauthorized access to a wireless network?

A. Near field communication
B. IV attack
C. Evil twin
D. Replay attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 828
Which of the following is a BEST practice when dealing with user accounts that will only need to be active for a limited time period?

A. When creating the account, set the account to not remember password history.
B. When creating the account, set an expiration date on the account.
C. When creating the account, set a password expiration date on the account.
D. When creating the account, set the account to have time of day restrictions.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 829
Which of the following types of authentication packages user credentials in a ticket?

A. Kerberos
B. LDAP
C. TACACS+
D. RADIUS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 830
Real 57
CompTIA SY0-401 Exam
Which of the following is required to allow multiple servers to exist on one physical server?

A. Software as a Service (SaaS)
B. Platform as a Service (PaaS)
C. Virtualization
D. Infrastructure as a Service (IaaS)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: