Comptia Actualtests SY0-301 Exam Bundle

Number: SY0-301
Passing Score: 800
Time Limit: 120 min
File Version: 20.2

Comptia SY0-301 Exam Bundle

Exam Name: Comptia CompTIA Security+ Certification Exam 2011 version

For Full Set of Questions please visit: http://www.actualtests.com/exam-SY0-301.htm

Actualtests

QUESTION 1
Which of the following is the BEST approach to perform risk mitigation of user access control rights?

A. Conduct surveys and rank the results.
B. Perform routine user permission reviews.
C. Implement periodic vulnerability scanning.
D. Disable user accounts that have not been used within the last two weeks.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
All of the following are valid cryptographic hash functions EXCEPT:

A. RIPEMD.
B. RC4.
C. SHA-512.
D. MD4.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
In regards to secure coding practices, why is input validation important?

A. It mitigates buffer overflow attacks.
B. It makes the code more readable.
C. It provides an application configuration baseline.
D. It meets gray box testing standards.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check?

A. Firewall
B. Application
C. IDS
D. Security

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
Which of the following application security testing techniques is implemented when an automated system generates random input data?

A. Fuzzing
B. XSRF
C. Hardening
D. Input validation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
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 7
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 8
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 9
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 10
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 11
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:

~ 9

QUESTION 12
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:

~ 10

QUESTION 13
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:

~ 11

QUESTION 14
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 15
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:
Explanation:

QUESTION 16
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:
Explanation:

QUESTION 17
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:

~ 13

QUESTION 18
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 19
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 20
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
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 22
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 23
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
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 25
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 26
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?

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 27
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 28

Please be aware that if you do not accept these terms you will not be allowed to take this CompTIA exam and you will forfeit the fee paid.

A. RETURN TO EXAM
B. EXIT EXAM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
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 30
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 31
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 32
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 33
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:
Explanation:

QUESTION 34
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
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 36
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 37
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 38
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 39
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 40
Which of the following can Pete, a security administrator, use to distribute the processing effort 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 41
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 42
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 43
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 44
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 45
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 46
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 47
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 48
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 49
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 50
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 51
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:
Explanation:

QUESTION 52
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 53
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 54
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 55
Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability?

A. Twofish
B. Diffie-Hellman
C. ECC
D. RSA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
Methods to test the responses of software and web applications to unusual or unexpected inputs is known as:

A. Brute force.
B. HTML encoding.
C. Web crawling.
D. Fuzzing.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 57
Which statement is TRUE about the operation of a packet sniffer?

A. It can only have one interface on a management network.
B. They are required for firewall operation and stateful inspection.
C. The Ethernet card must be placed in promiscuous mode.
D. It must be placed on a single virtual LAN interface.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
Which of the following BEST explains the use of an HSM within the company servers?

A. Thumb drives present a significant threat which is mitigated by HSM.
B. Software encryption can perform multiple functions required by HSM.
C. Data loss by removable media can be prevented with DLP.
D. Hardware encryption is faster than software encryption.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 59
Matt, a security analyst, needs to implement encryption for company data and also prevent theft of company data. Where and how should Matt meet this requirement?

A. Matt should implement access control lists and turn on EFS.
B. Matt should implement DLP and encrypt the company database.
C. Matt should install Truecrypt and encrypt the company server.
D. Matt should install TPMs and encrypt the company database.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 47

QUESTION 60
Which of the following does full disk encryption prevent?

A. Client side attacks
B. Clear text access
C. Database theft
D. Network-based attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 61
Which of the following encompasses application patch management?

A. Configuration management
B. Policy management
C. Cross-site request forgery
D. Fuzzing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

~ 49

QUESTION 62
Pete, a developer, writes an application. Jane, the security analyst, knows some things about the overall application but does not have all the details. Jane needs to review the software before it is released to production. Which of the following reviews should Jane conduct?

A. Gray Box Testing
B. Black Box Testing
C. Business Impact Analysis
D. White Box Testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 63
Pete, the security engineer, would like to prevent wireless attacks on his network. Pete has implemented a security control to limit the connecting MAC addresses to a single port. Which of the following wireless attacks would this address?

A. Interference
B. Man-in-the-middle
C. ARP poisoning
D. Rogue access point

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 64
Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide?

A. No competition with the company's official social presence
B. Protection against malware introduced by banner ads
C. Increased user productivity based upon fewer distractions
D. Elimination of risks caused by unauthorized P2P file sharing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 65
A network stream needs to be encrypted. Sara, the network administrator, has selected a cipher which will encrypt 8 bits at a time before sending the data across the network. Which of the following has Sara selected?

A. Block cipher
B. Stream cipher
C. CRC
D. Hashing algorithm

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 66
A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site were facing the wrong direction to capture the incident. The analyst ensures the cameras are turned to face the proper direction. Which of the following types of controls is being used?

A. Detective
B. Deterrent
C. Corrective
D. Preventive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 67
An IT auditor tests an application as an authenticated user. This is an example of which of the following types of testing?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 68
Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

A. EAP-MD5
B. WEP
C. PEAP-MSCHAPv2
D. EAP-TLS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 69
A security analyst needs to ensure all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended?

A. DMZ
B. Cloud computing
C. VLAN
D. Virtualization

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
Which of the following network devices is used to analyze traffic between various network interfaces?

A. Proxies
B. Firewalls
C. Content inspection
D. Sniffers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 71
Layer 7 devices used to prevent specific types of html tags are called:

A. Firewalls.
B. Content filters.
C. Routers.
D. NIDS.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 72
A security administrator has been tasked to ensure access to all network equipment is controlled by a central server such as TACACS+. This type of implementation supports which of the following risk mitigation strategies?

A. User rights and permissions review
B. Change management
C. Data loss prevention
D. Implement procedures to prevent data theft

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 73
A corporation is looking to expand their data center but has run out of physical space in which to store hardware. Which of the following would offer the ability to expand while keeping their current data center operated by internal staff?

A. Virtualization
B. Subnetting
C. IaaS
D. SaaS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 74
After viewing wireless traffic, an attacker notices the following networks are being broadcasted by local access points:

Corpnet

Coffeeshop

FreePublicWifi

Using this information the attacker spoofs a response to make nearby laptops connect back to a malicious device. Which of the following has the attacker created?

A. Infrastructure as a Service
B. Load balancer
C. Evil twin
D. Virtualized network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 75
After a recent breach, the security administrator performs a wireless survey of the corporate network. The security administrator notices a problem with the following output:

MACSSIDENCRYPTIONPOWERBEACONS

00:10:A1:36:12:CCMYCORPWPA2 CCMP601202

```
00:10:A1:49:FC:37MYCORPWPA2 CCMP709102

FB:90:11:42:FA:99MYCORPWPA2 CCMP403031

00:10:A1:AA:BB:CCMYCORPWPA2 CCMP552021

00:10:A1:FA:B1:07MYCORPWPA2 CCMP306044
```

Given that the corporate wireless network has been standardized, which of the following attacks is underway?

A. Evil twin
B. IV attack
C. Rogue AP
D. DDoS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 76
Input validation is an important security defense because it:

A. rejects bad or malformed data.
B. enables verbose error reporting.
C. protects mis-configured web servers.
D. prevents denial of service attacks.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 77
In order to maintain oversight of a third party service provider, the company is going to implement a Governance, Risk, and Compliance (GRC) system. This system is promising to provide overall security posture coverage. Which of the following is the MOST important activity that should be considered?

A. Continuous security monitoring
B. Baseline configuration and host hardening
C. Service Level Agreement (SLA) monitoring
D. Security alerting and trending

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 78

The Chief Information Officer (CIO) has mandated web based Customer Relationship Management (CRM) business functions be moved offshore to reduce cost, reduce IT overheads, and improve availability. The Chief Risk Officer (CRO) has agreed with the CIO's direction but has mandated that key authentication systems be run within the organization's network. Which of the following would BEST meet the CIO and CRO's requirements?

A. Software as a Service
B. Infrastructure as a Service
C. Platform as a Service
D. Hosted virtualization service

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 79
Which of the following provides the BEST application availability and is easily expanded as demand grows?

A. Server virtualization
B. Load balancing
C. Active-Passive Cluster
D. RAID 6

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 80
Which of the following wireless security measures can an attacker defeat by spoofing certain properties of their network interface card?

A. WEP
B. MAC filtering
C. Disabled SSID broadcast
D. TKIP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 81
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 82
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 83
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:
Explanation:

QUESTION 84
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 85
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 86
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 87
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 88
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:
Explanation:

QUESTION 89
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 90
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:
Explanation:

QUESTION 91
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 92
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 93
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 94
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 95
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 96
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 97
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:

Topic 3, Volume C

QUESTION 98
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:

~ 71

QUESTION 99
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 100
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 101
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:
Explanation:

QUESTION 102
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 103
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:
Explanation:

QUESTION 104
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:
Explanation:

QUESTION 105
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 106
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 107
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

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 108
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 109
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:
Explanation:

~ 75

QUESTION 110
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 111
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 112
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:
Explanation:

QUESTION 113
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 114
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 115
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 116
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 117
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:

~ 78

QUESTION 118
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 119
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 120
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:

~ 79

QUESTION 121
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 122
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 123
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:

Explanation:

QUESTION 124
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 125
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 126
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 127
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 128
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.

D. time offset can be calculated.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 129
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 130
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:

~ 83

QUESTION 131
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 132
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:
Explanation:

QUESTION 133
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 134
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:

~ 85

QUESTION 135
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. 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 136
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 137
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 138
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 139
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 140
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:
Explanation:

QUESTION 141
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 142
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 143
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 144
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:
Explanation:

QUESTION 145
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:
Explanation:

~ 90

QUESTION 146
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 147
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 148
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 149
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 150
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 151
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 152
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 153
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 154
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 155
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 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:

~ 94

QUESTION 156
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 157
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 158
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 159
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 160
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 161
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?

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 162
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 163
Which of the following is true about an email that was signed by User A and sent to User B?

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 164
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 165
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 166
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?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 167
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 168
Which of the following is BEST carried out immediately after a security breach is discovered?

A. Risk transference
B. Access control revalidation

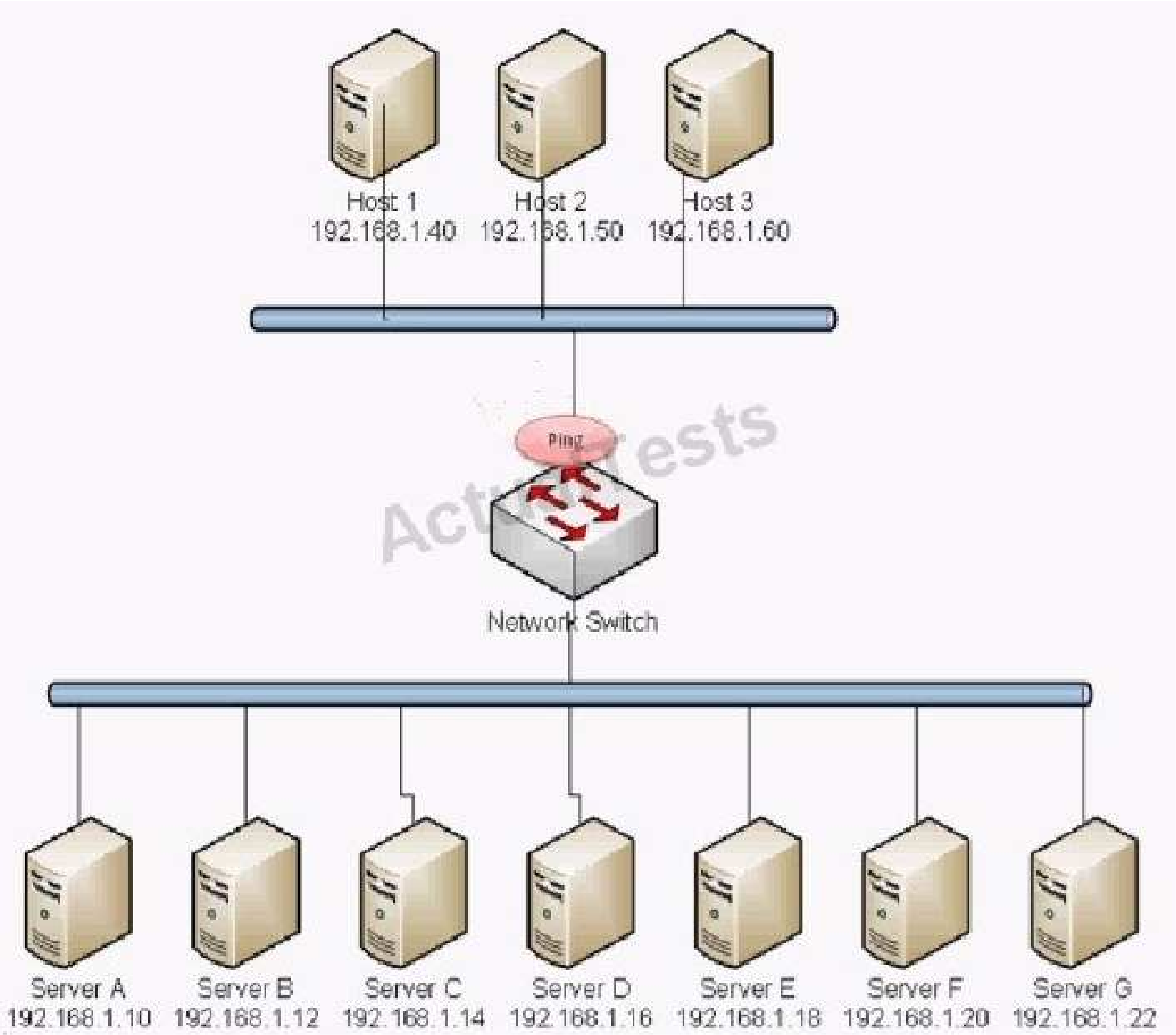
C. Change management

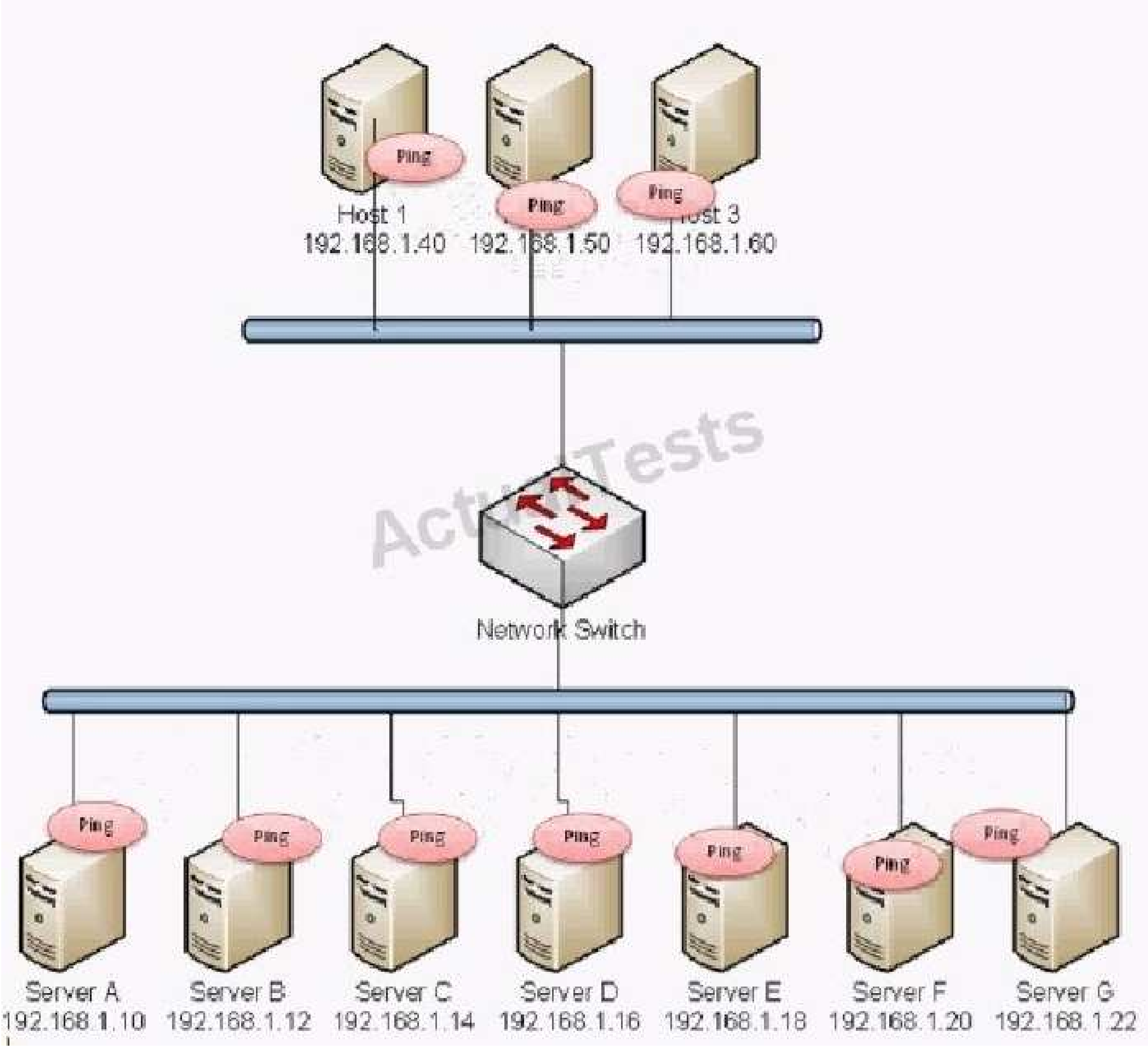
D. Incident management

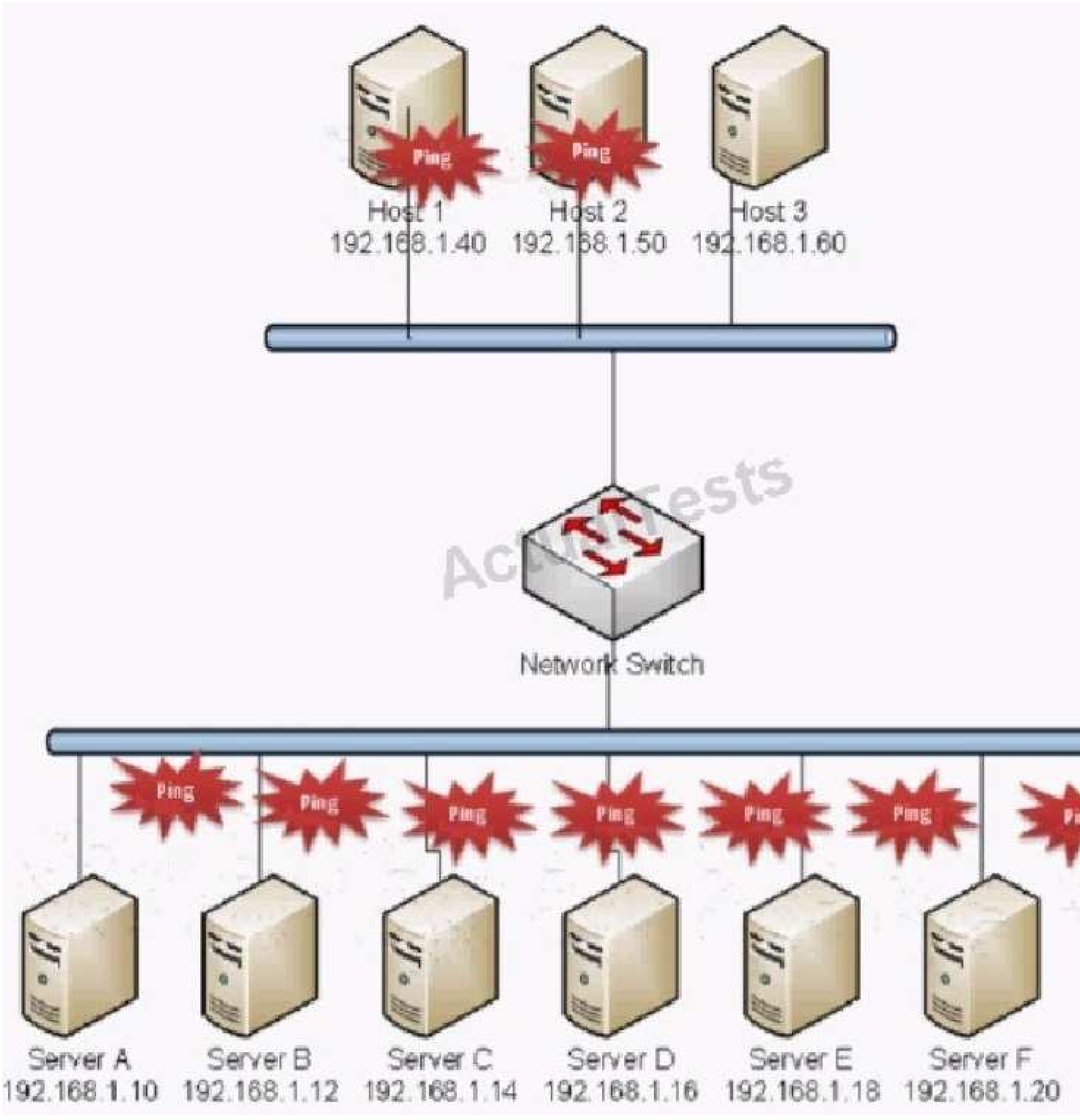
Correct Answer: D
Section: (none)
Explanation

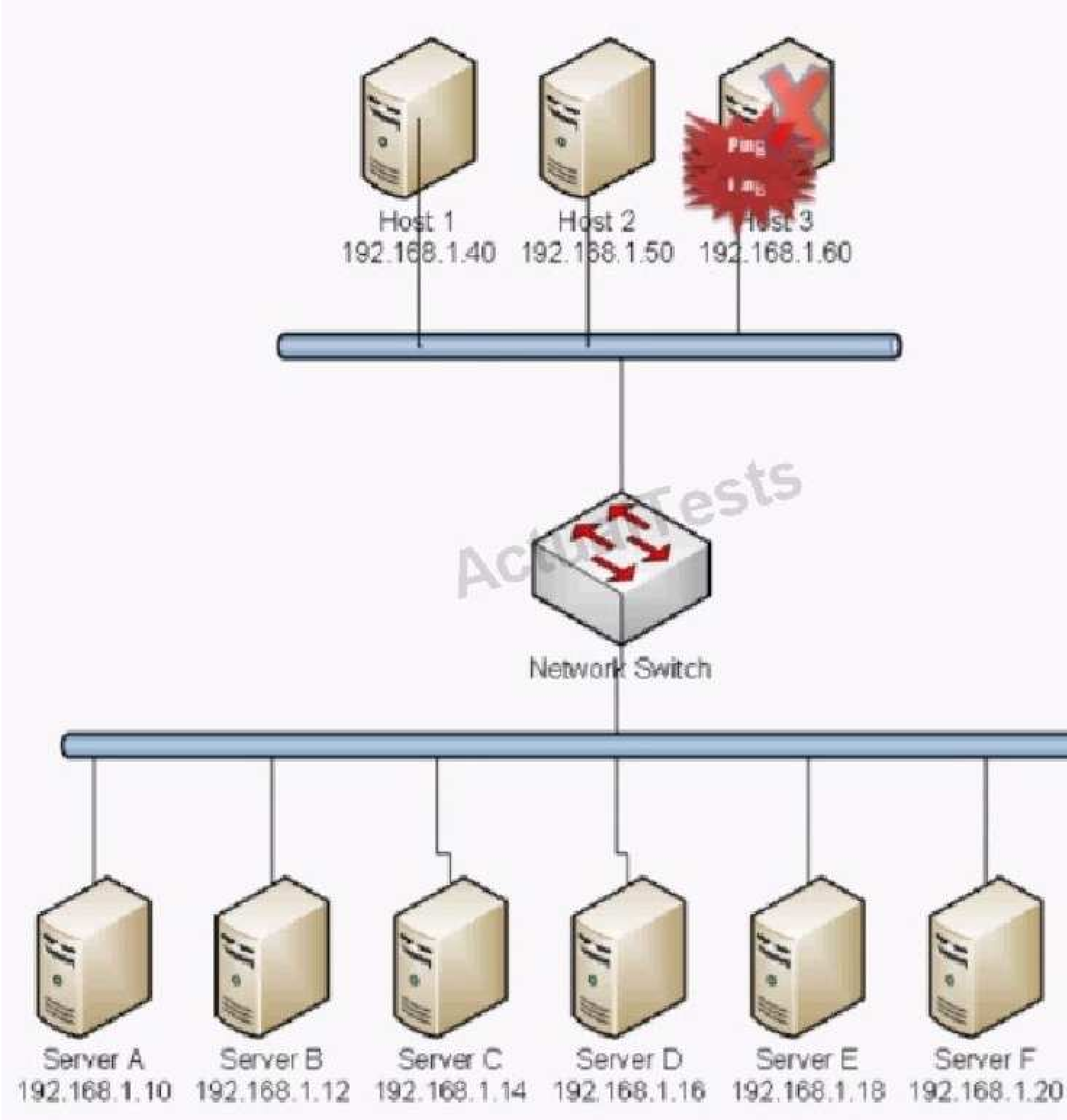
Explanation/Reference:
Explanation:

QUESTION 169
-- Exhibit




Ping
Ping
Ping
Host 1
192.168.1.40
192.168.1.50
ost 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
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



-- Exhibit --

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

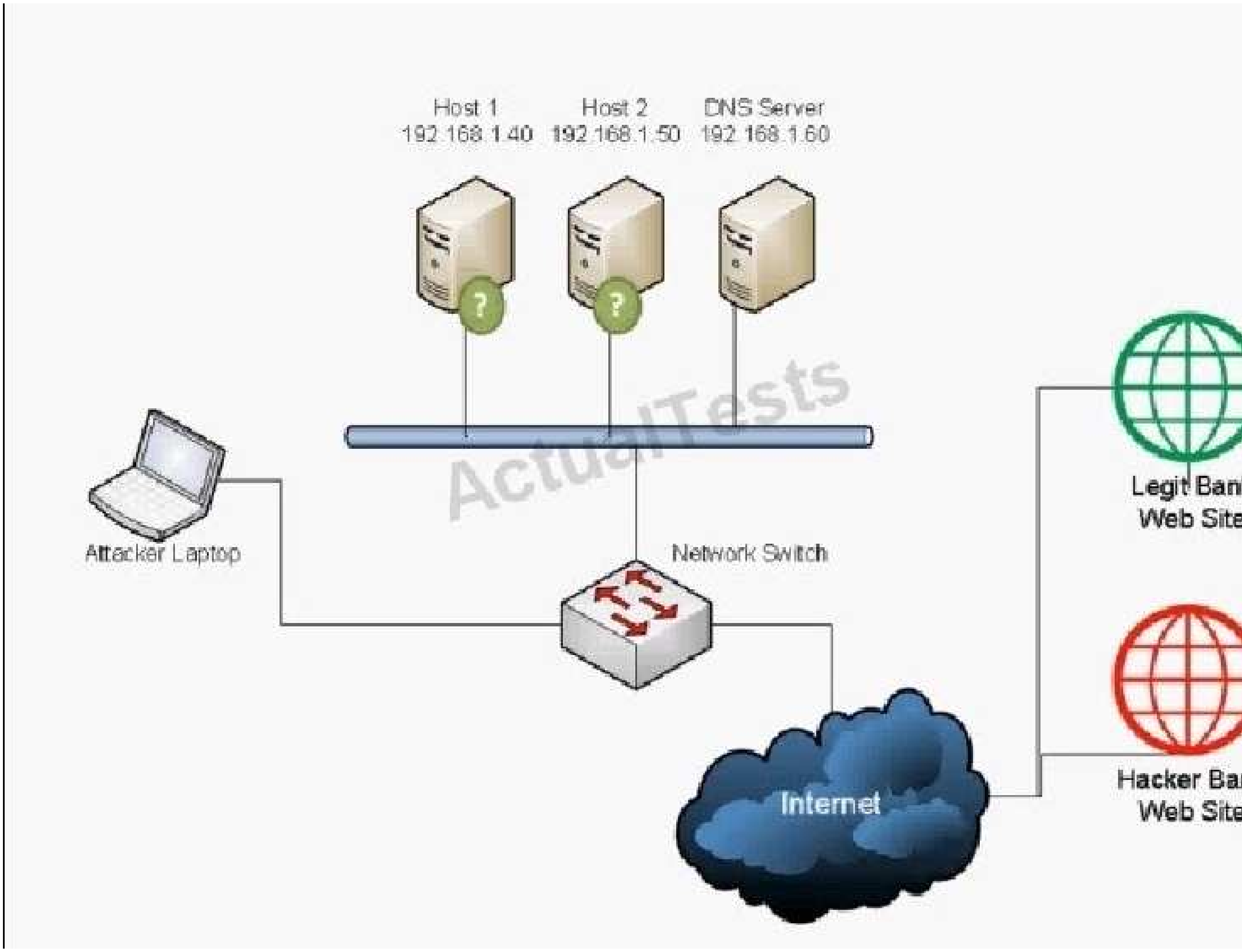
A. Smurf Attack
B. Man in the middle
C. Backdoor

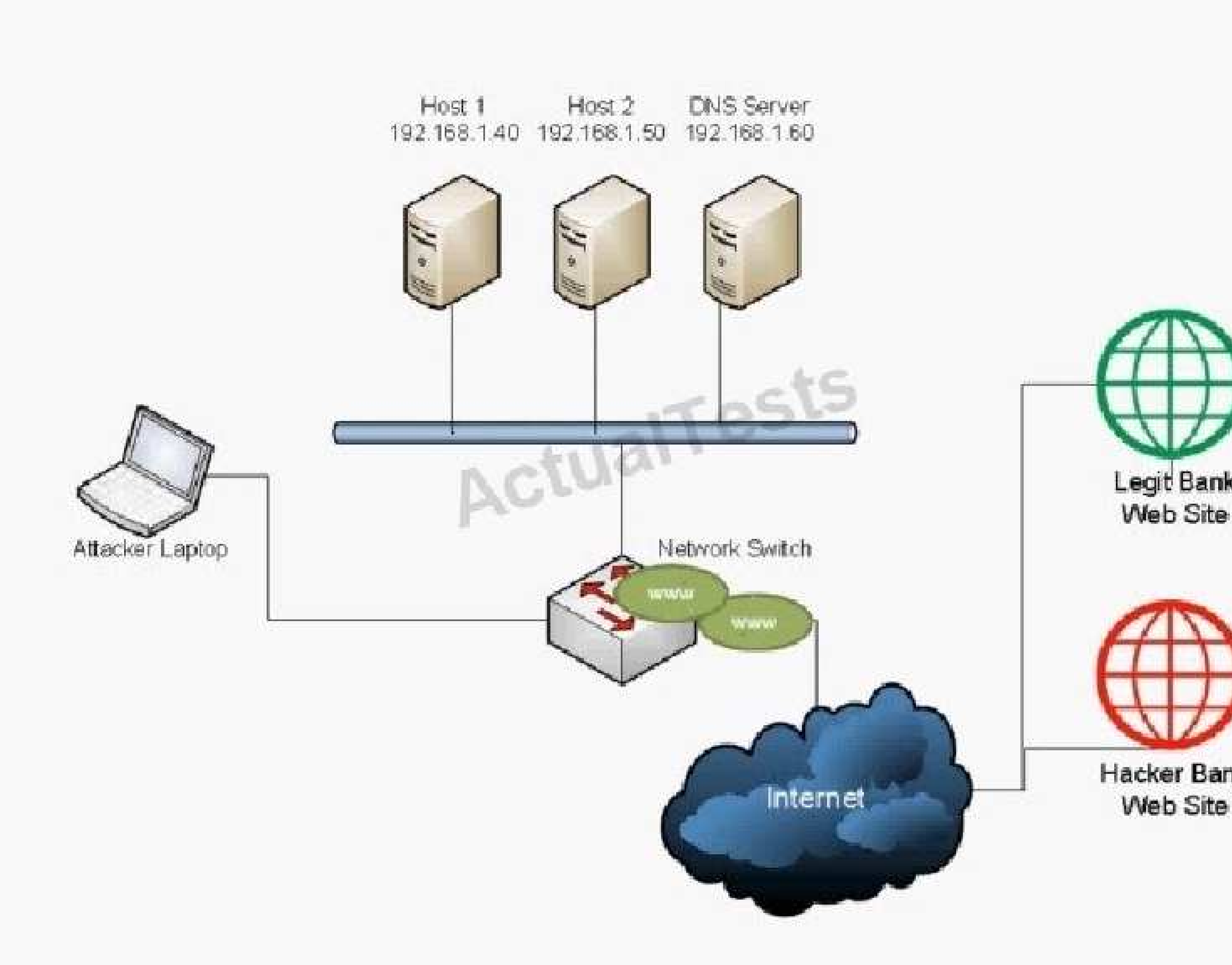
D. Replay
E. Spear Phishing
F. Xmas Attack
G. Blue Jacking
H. Ping of Death

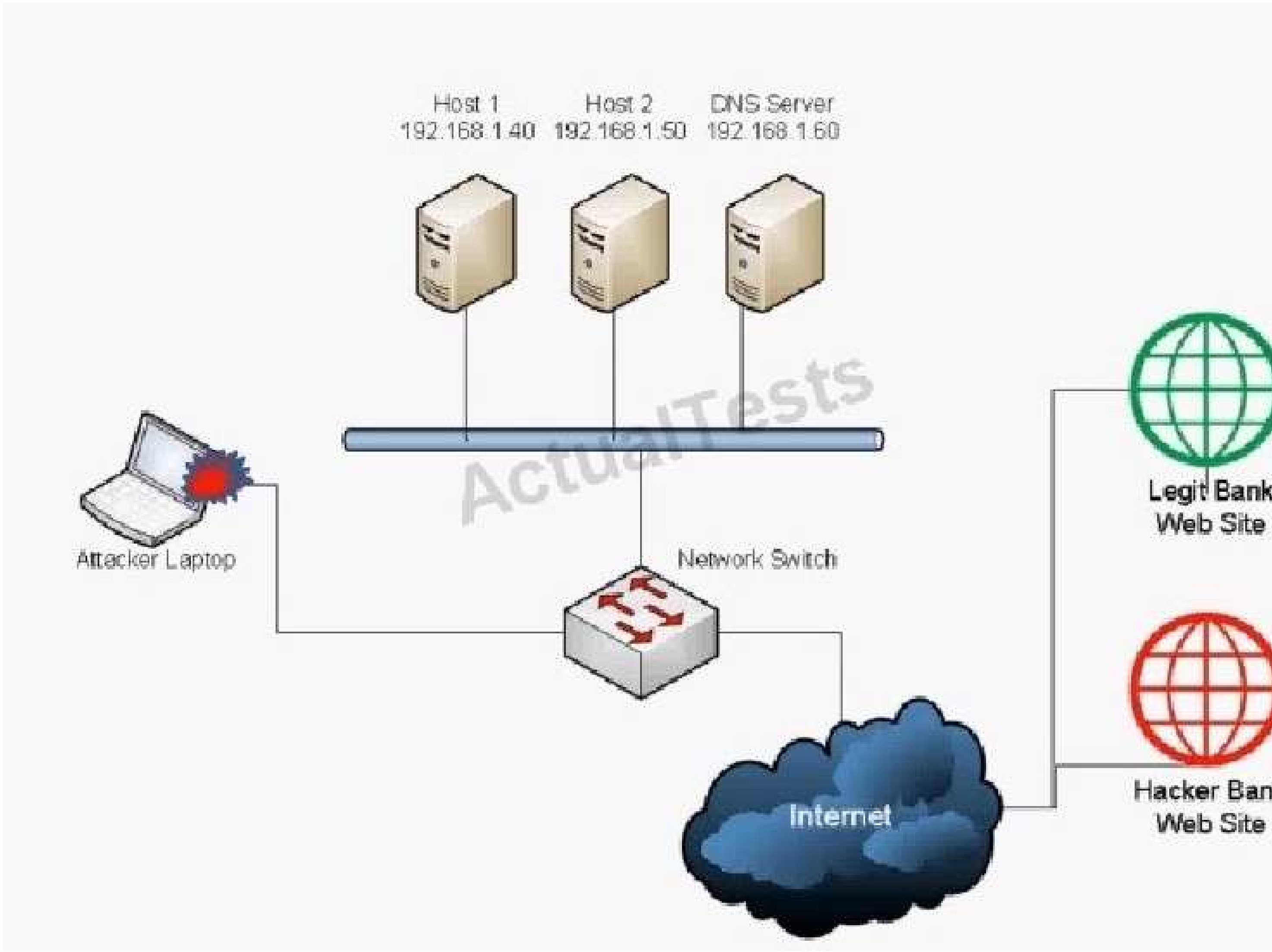
Correct Answer: A
Section: (none)
Explanation

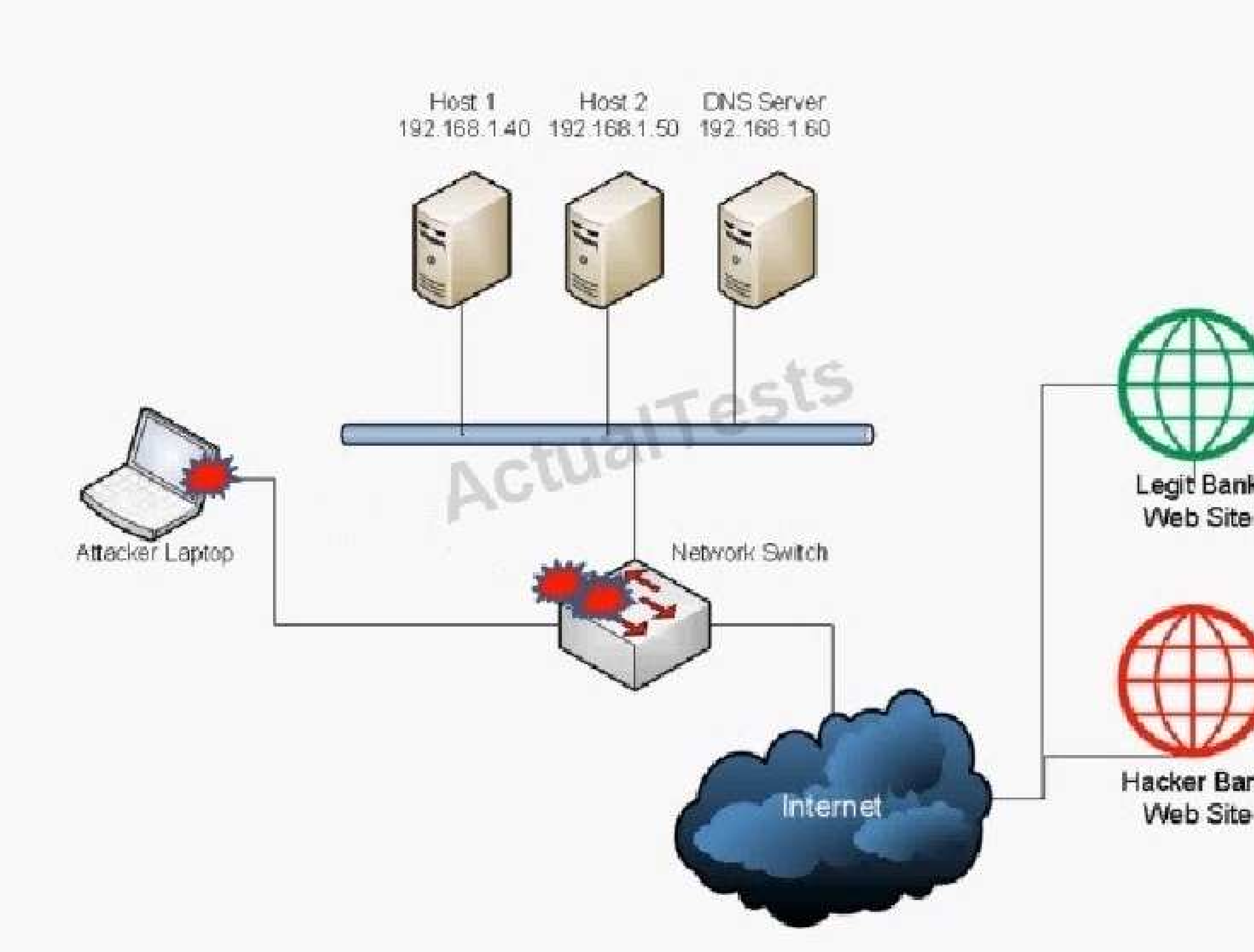
Explanation/Reference:
Explanation:

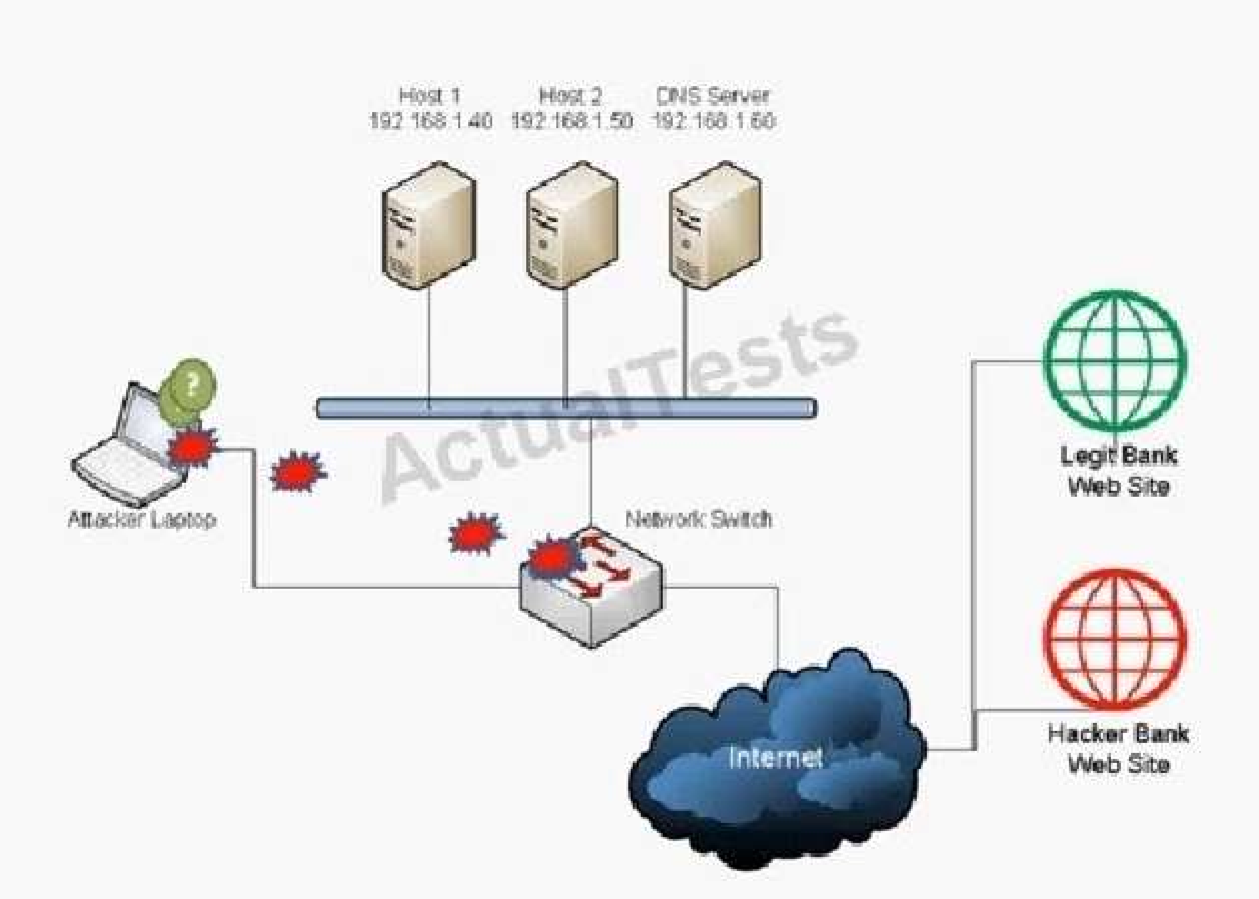
QUESTION 170
-- Exhibit

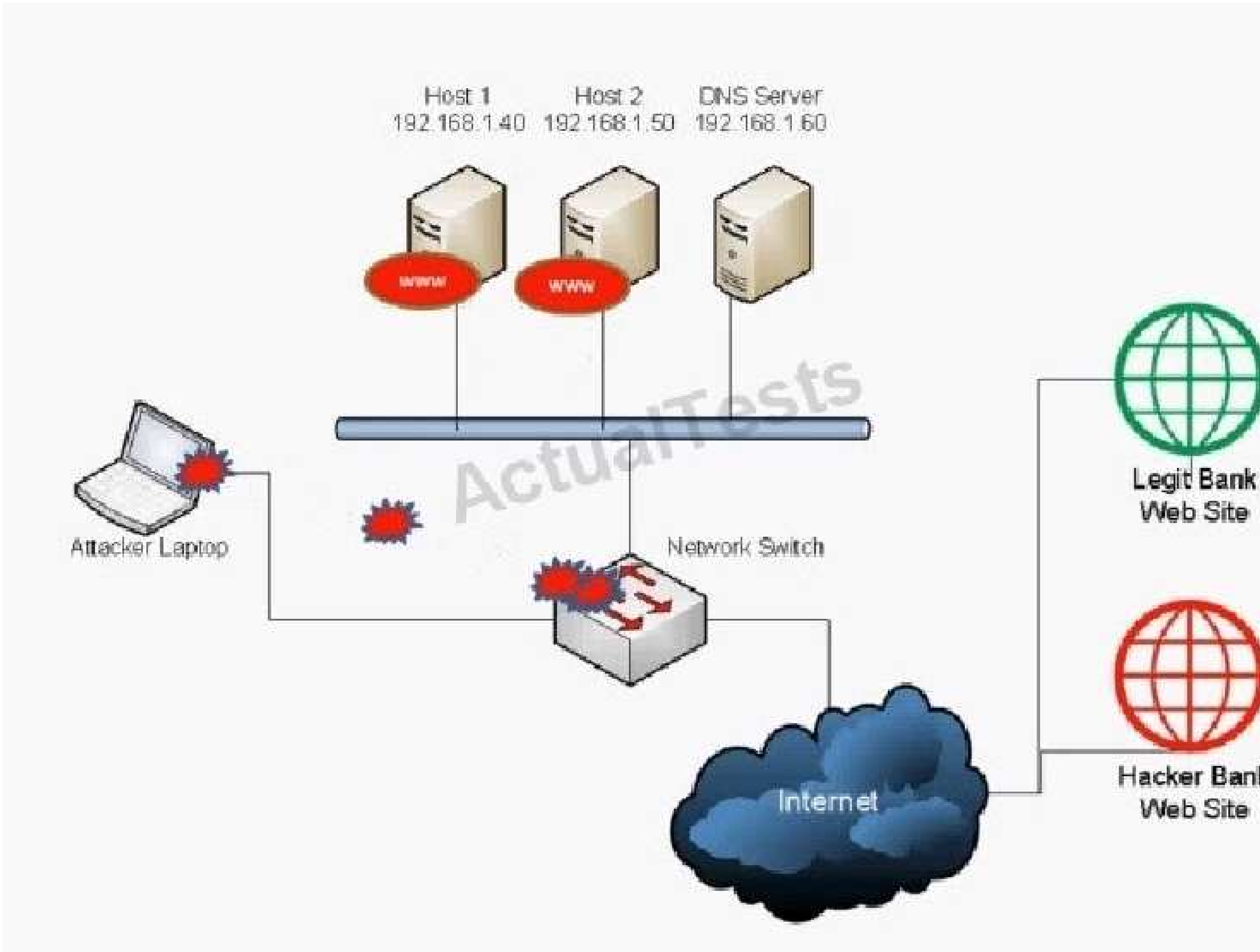


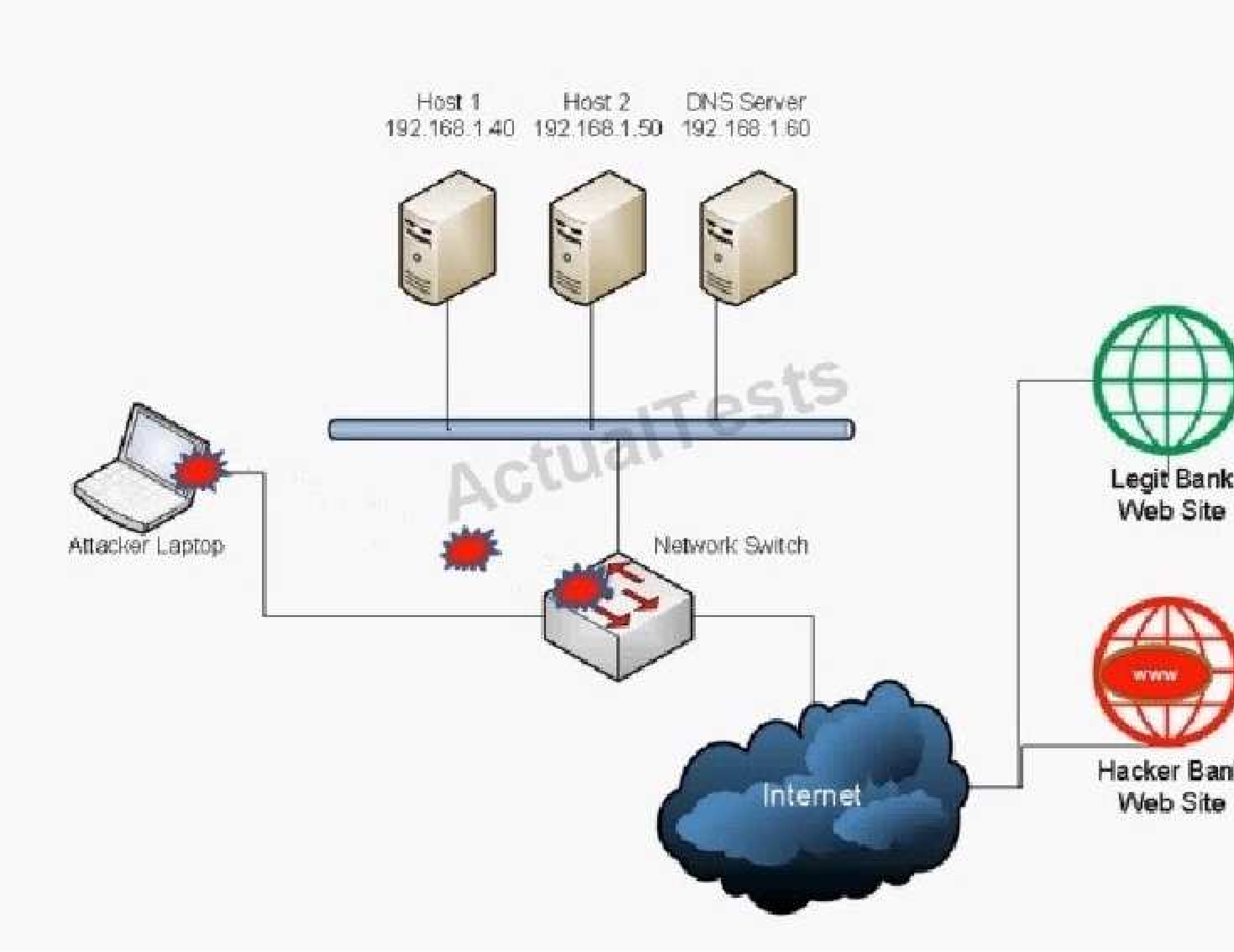

Host 1
192.168.1.40
Host 2
192.168.1.50
DNS Server
192.168.1.60
Attacker Laptop
Network Switch
www
www
Internet
Legit Bank
Web Site
Hacker Ban
Web Site


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 Ban
Web Site


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 Ban
Web Site


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
www
www
Attacker Laptop
Network Switch
Internet
Legit Bank
Web Site
Hacker Bank
Web Site



-- Exhibit --

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

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 171
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:
Explanation:

QUESTION 172
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 173
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 174
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:
Explanation:

QUESTION 175
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 176
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: