

SY0-501.exam.45q

Number: SY0-501
Passing Score: 800
Time Limit: 120 min
File Version: 1



<https://www.gratisexam.com/>

Comptia SY0-501

CompTIA Security+ Certification Exam

<https://www.gratisexam.com/>

Exam A

QUESTION 1

HOTSPOT

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.



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
 <p>Attacker gains confidential company information</p>	 <p>Targeted CEO and board members</p>	<div>▼</div> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 <p>Attacker posts link to fake AV software</p>	 <p>Multiple social networks</p>  <p>Broad set of victims</p>	<div>▼</div> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 <p>Attacker collecting credit card details</p>	 <p>Phone-based victim</p>	<div>▼</div> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK
 <p>Attacker mass-mails product information to parties that have already opted out of receiving advertisements</p>	  <p>Broad set of recipients</p>	<div>▼</div> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX 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
 <p>Attacker gains confidential company information</p>	 <p>Targeted CEO and board members</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>
 <p>Attacker posts link to fake AV software</p>	 <p>Multiple social networks</p>  <p>Broad set of victims</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>
 <p>Attacker collecting credit card details</p>	 <p>Phone-based victim</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING SPEAR PHISHING SPOOFING SPAM XMAS ATTACK </div>
 <p>Attacker mass-mails product information to parties that have already opted out of receiving advertisements</p>	 <p>Broad set of recipients</p>	<div> <input type="text"/> <ul style="list-style-type: none"> SPIM VISHING PHISHING WHALING HOAX PHARMING </div>

Section: (none)

Explanation

Explanation/Reference:

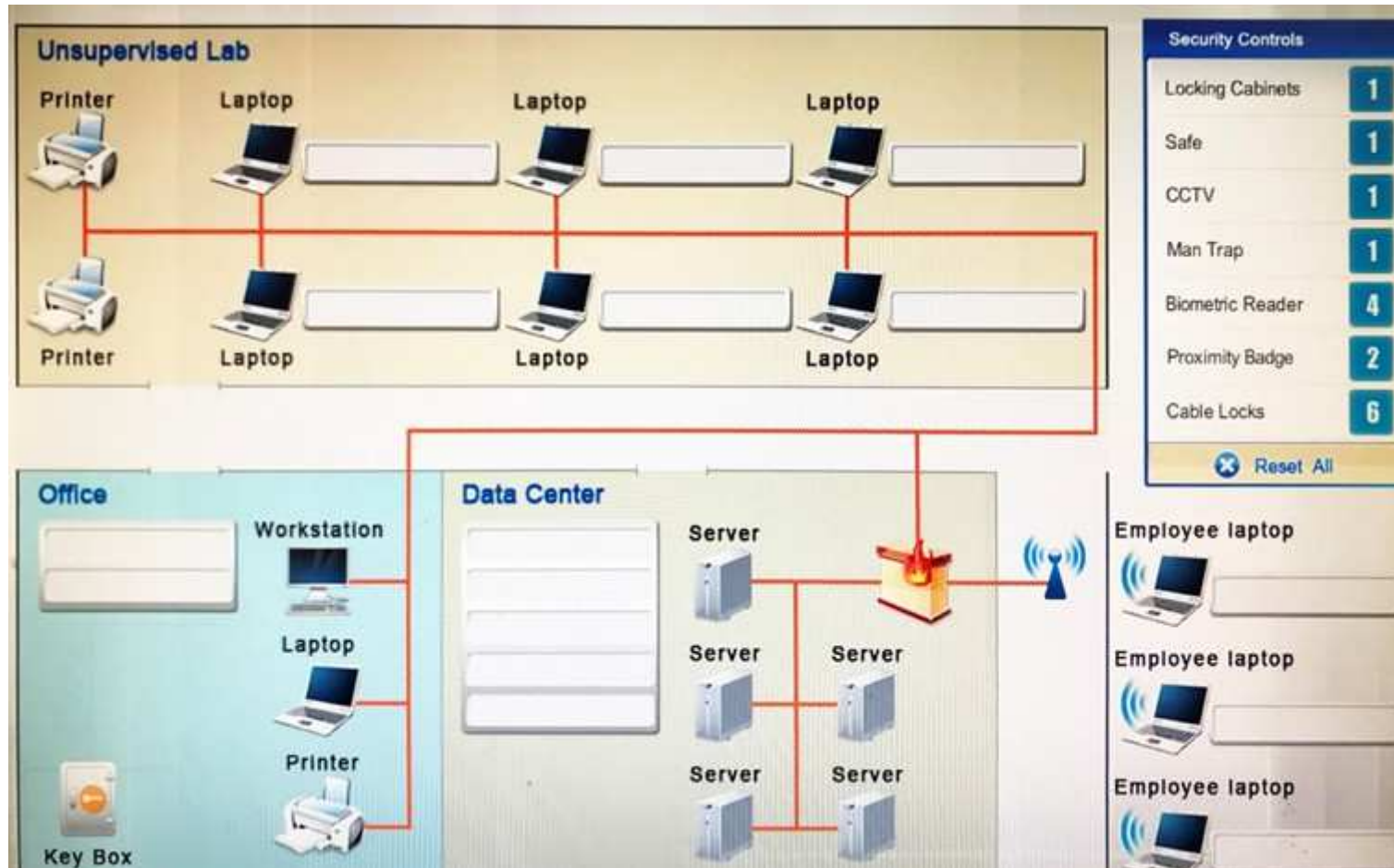
QUESTION 2

DRAG DROP

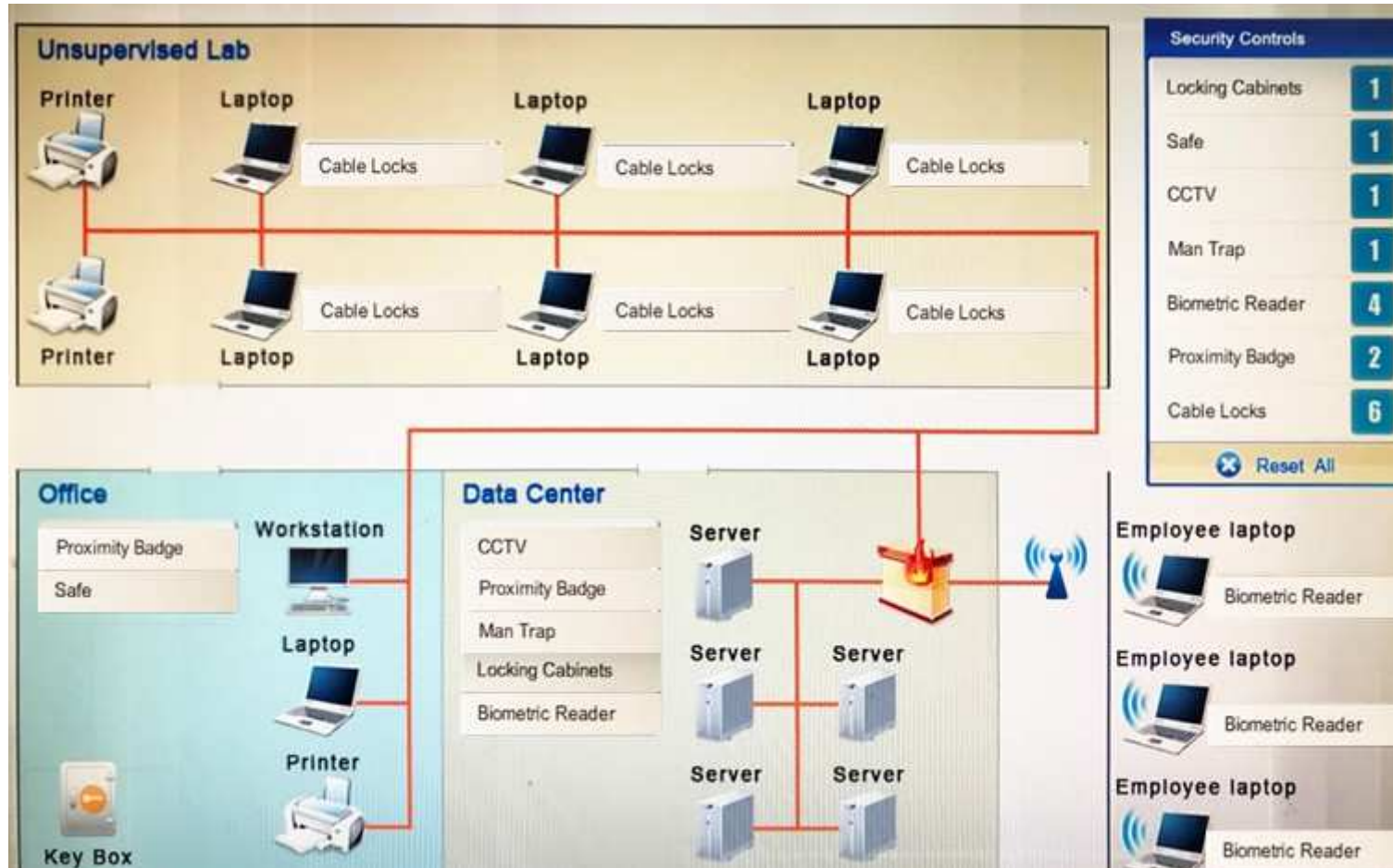
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.

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:



Correct Answer:



Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Which of the following would a security specialist be able to determine upon examination of a server's certificate?

- A. CA public key
- B. Server private key
- C. CSR
- D. OID

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.0:6666. Which of the following should the security analyst do to determine if the compromised system still has an active connection?

- A. `tracert`
- B. `netstat`
- C. `ping`
- D. `nslookup`

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?



<https://www.gratisexam.com/>

- A. The recipient can verify integrity of the software patch.
- B. The recipient can verify the authenticity of the site used to download the patch.

<https://www.gratisexam.com/>

- C. The recipient can request future updates to the software using the published MD5 value.
- D. The recipient can successfully activate the new software patch.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

Refer to the following code:

```
public class rainbow {  
    public static void main (String [] args) {  
        object blue = null;  
        blue.hashCode (); }  
}
```

Which of the following vulnerabilities would occur if this is executed?

- A. Page exception
- B. Pointer deference
- C. NullPointerException
- D. Missing null check

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened. The network and security teams perform the following actions:

- Shut down all network shares.
- Run an email search identifying all employees who received the malicious message.
- Reimage all devices belonging to users who opened the attachment.

Next, the teams want to re-enable the network shares. Which of the following BEST describes this phase of the incident response process?

- A. Eradication
- B. Containment
- C. Recovery
- D. Lessons learned

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

- A. RTO
- B. RPO
- C. MTBF
- D. MTTR

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

Which of the following types of keys is found in a key escrow?

- A. Public
- B. Private
- C. Shared

D. Session

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

A security analyst is reviewing the following output from an IPS:

```
[**] [1:2467:7] EXPLOIT IGMP IGAP message overflow attempt [**]  
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]  
07/30-19:45:02.238185 250.19.18.71 -> 250.19.18.22  
IGMP TTL:255 TOS: 0x0 ID: 9742 IpLen:20 DgmLen: 502 MF  
Frag offset: 0x1FFF Frag Size: 0x01E2  
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0367]
```

Given this output, which of the following can be concluded? (Select two.)

- A. The source IP of the attack is coming from 250.19.18.22.
- B. The source IP of the attack is coming from 250.19.18.71.
- C. The attacker sent a malformed IGAP packet, triggering the alert.
- D. The attacker sent a malformed TCP packet, triggering the alert.
- E. The TTL value is outside of the expected range, triggering the alert.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords. Which of the following technical controls would help prevent these policy violations? (Select two.)

- A. Password expiration
- B. Password length
- C. Password complexity
- D. Password history
- E. Password lockout

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

Which of the following types of cloud infrastructures would allow several organizations with similar structures and interests to realize the benefits of shared storage and resources?

- A. Private
- B. Hybrid
- C. Public
- D. Community

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

A company is currently using the following configuration:

- IAS server with certificate-based EAP-PEAP and MSCHAP
- Unencrypted authentication via PAP

A security administrator needs to configure a new wireless setup with the following configurations:

- PAP authentication method
- PEAP and EAP provide two-factor authentication

Which of the following forms of authentication are being used? (Select two.)

- A. PAP
- B. PEAP
- C. MSCHAP
- D. PEAP- MSCHAP
- E. EAP
- F. EAP-PEAP

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

An auditor wants to test the security posture of an organization by running a tool that will display the following:

JIMS	<00> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered
JIMS	<00> UNIQUE	Registered

Which of the following commands should be used?

- A. nbtstat
- B. nc
- C. arp
- D. ipconfig

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

A company determines that it is prohibitively expensive to become compliant with new credit card regulations. Instead, the company decides to purchase insurance to cover the cost of any potential loss. Which of the following is the company doing?

- A. Transferring the risk
- B. Accepting the risk
- C. Avoiding the risk
- D. Migrating the risk

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:

- There is no standardization.
- Employees ask for reimbursement for their devices.
- Employees do not replace their devices often enough to keep them running efficiently.
- The company does not have enough control over the devices.

Which of the following is a deployment model that would help the company overcome these problems?

- A. BYOD
- B. VDI
- C. COPE
- D. CYOD

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

A botnet has hit a popular website with a massive number of GRE-encapsulated packets to perform a DDoS attack. News outlets discover a certain type of refrigerator was exploited and used to send outbound packets to the website that crashed. To which of the following categories does the refrigerator belong?



<https://www.gratisexam.com/>

- A. SoC
- B. ICS
- C. IoT
- D. MFD

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

Users report the following message appears when browsing to the company's secure site: `This website cannot be trusted`. Which of the following actions should a security analyst take to resolve these messages? (Select two.)

- A. Verify the certificate has not expired on the server.
- B. Ensure the certificate has a .pfx extension on the server.
- C. Update the root certificate into the client computer certificate store.
- D. Install the updated private key on the web server.
- E. Have users clear their browsing history and relaunch the session.

Correct Answer: AC

<https://www.gratisexam.com/>

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

When trying to log onto a company's new ticketing system, some employees receive the following message: `Access denied: too many concurrent sessions`. The ticketing system was recently installed on a small VM with only the recommended hardware specifications. Which of the following is the MOST likely cause for this error message?

- A. Network resources have been exceeded.
- B. The software is out of licenses.
- C. The VM does not have enough processing power.
- D. The firewall is misconfigured.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.

The IT security department finds the following security configuration for the accounts payable module:

- `New Vendor Entry - Required Role: Accounts Payable Clerk`
- `New Vendor Approval - Required Role: Accounts Payable Clerk`
- `Vendor Payment Entry - Required Role: Accounts Payable Clerk`
- `Vendor Payment Approval - Required Role: Accounts Payable Manager`

Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?

- A. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager
- B. New Vendor Entry - Required Role: Accounts Payable Manager
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager
- C. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager
- D. New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Manager
Vendor Payment Entry - Required Role: Accounts Payable Manager
Vendor Payment Approval - Required Role: Accounts Payable Manager

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?

- A. Time-of-day restrictions
- B. Permission auditing and review
- C. Offboarding
- D. Account expiration

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

Which of the following security controls does an iris scanner provide?

- A. Logical
- B. Administrative
- C. Corrective
- D. Physical
- E. Detective

F. Deterrent

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

As part of a new industry regulation, companies are required to utilize secure, standardized OS settings. A technical must ensure the OS settings are hardened. Which of the following is the BEST way to do this?



<https://www.gratisexam.com/>

- A. Use a vulnerability scanner.
- B. Use a configuration compliance scanner.
- C. Use a passive, in-line scanner.
- D. Use a protocol analyzer.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

A user has attempted to access data at a higher classification level than the user's account is currently authorized to access. Which of the following access control models has been applied to this user's account?

- A. MAC
- B. DAC
- C. RBAC
- D. ABAC

<https://www.gratisexam.com/>

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

- A. An attacker can access and change the printer configuration.
- B. SNMP data leaving the printer will not be properly encrypted.
- C. An MITM attack can reveal sensitive information.
- D. An attacker can easily inject malicious code into the printer firmware.
- E. Attackers can use the PCL protocol to bypass the firewall of client computers.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

An organization finds that most help desk calls are regarding account lockout due to a variety of applications running on different systems. Management is looking for a solution to reduce the number of account lockouts while improving security. Which of the following is the BEST solution for this organization?

- A. Create multiple application accounts for each user.
- B. Provide secure tokens.
- C. Implement SSO.
- D. Utilize role-based access control.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

Hostname	IP address	MAC	MAC filter
DadPC	192.168.1.10	00:1D:1A:44:17:B5	On
MomPC	192.168.1.15	21:13:D6:C5:42:A2	Off
JuniorPC	192.168.2.16	42:A7:D1:25:11:52	On
Unknown	192.168.1.18	10:B3:22:1A:FF:21	Off

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

- A. Apply MAC filtering and see if the router drops any of the systems.
- B. Physically check each of the authorized systems to determine if they are logged onto the network.
- C. Deny the "unknown" host because the hostname is not known and MAC filtering is not applied to this host.
- D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Select two.)

- A. USB-attached hard disk
- B. Swap/pagefile
- C. Mounted network storage
- D. ROM
- E. RAM

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

A systems administrator is reviewing the following information from a compromised server:

Process	DEP	Local Address	Remote Address
LSASS	YES	0.0.0.0	10.210.100.62
APACHE	NO	0.0.0.0	10.130.210.20
MySQL	NO	127.0.0.1	127.0.0.1
TFTP	YES	191.168.1.10	10.34.221.96

Given the above information, which of the following processes was MOST likely exploited via a remote buffer overflow attack?

- A. Apache
- B. LSASS
- C. MySQL
- D. TFTP

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

An attacker compromises a public CA and issues unauthorized X.509 certificates for Company.com. In the future, Company.com wants to mitigate the impact of similar incidents. Which of the following would assist Company.com with its goal?

- A. Certificate pinning
- B. Certificate stapling
- C. Certificate chaining
- D. Certificate with extended validation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

A high-security defense installation recently begun utilizing large guard dogs that bark very loudly and excitedly at the slightest provocation. Which of the following types of controls does this BEST describe?



<https://www.gratisexam.com/>

- A. Deterrent
- B. Preventive
- C. Detective
- D. Compensating

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are MOST likely occurring? (Select two.)

- A. Replay
- B. Rainbow tables
- C. Brute force
- D. Pass the hash
- E. Dictionary

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

Ann, an employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:

- Slow performance
- Word documents, PDFs, and images no longer opening
- A pop-up

Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?

- A. Spyware
- B. Crypto-malware
- C. Rootkit
- D. Backdoor

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

- A. Obtain a list of passwords used by the employee.
- B. Generate a report on outstanding projects the employee handled.
- C. Have the employee surrender company identification.
- D. Have the employee sign an NDA before departing.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment?

- A. A perimeter firewall and IDS
- B. An air gapped computer network
- C. A honeypot residing in a DMZ
- D. An ad hoc network with NAT
- E. A bastion host

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production?

- A. Roll back changes in the test environment
- B. Verify the hashes of files
- C. Archive and compress the files
- D. Update the secure baseline

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

A user clicked an email link that led to a website than infected the workstation with a virus. The virus encrypted all the network shares to which the user had access. The virus was not deleted or blocked by the company's email filter, website filter, or antivirus. Which of the following describes what occurred?

- A. The user's account was over-privileged.
- B. Improper error handling triggered a false negative in all three controls.
- C. The email originated from a private email server with no malware protection.
- D. The virus was a zero-day attack.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment of DNSSEC at the organization?



<https://www.gratisexam.com/>

- A. LDAP
- B. TPM
- C. TLS
- D. SSL
- E. PKI

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm?

- A. Vulnerability scanning
- B. Penetration testing
- C. Application fuzzing
- D. User permission auditing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

Which of the following technologies employ the use of SAML? (Select two.)

- A. Single sign-on
- B. Federation
- C. LDAP
- D. Secure token
- E. RADIUS

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

Which of the following specifically describes the exploitation of an interactive process to access otherwise restricted areas of the OS?

- A. Privilege escalation
- B. Pivoting
- C. Process affinity
- D. Buffer overflow

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

After a user reports slow computer performance, a system administrator detects a suspicious file, which was installed as part of a freeware software package. The systems administrator reviews the output below:

```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address          Foreign Address        State                   Process
TCP    0.0.0.0:135             0.0.0.0:0               LISTENING               RpcSs| [svchost.exe]
TCP    0.0.0.0:445             0.0.0.0:0               LISTENING               [svchost.exe]

TCP    192.168.1.10:5000      10.37.213.20           ESTABLISHED             winserver.exe
UDP    192.168.1.10:1900     *.*.                   SSDPSVR
```

Based on the above information, which of the following types of malware was installed on the user's computer?

- A. RAT
- B. Keylogger
- C. Spyware
- D. Worm
- E. Bot

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

Which of the following network vulnerability scan indicators BEST validates a successful, active scan?

- A. The scan job is scheduled to run during off-peak hours.
- B. The scan output lists SQL injection attack vectors.
- C. The scan data identifies the use of privileged-user credentials.
- D. The scan results identify the hostname and IP address.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

An analyst wants to implement a more secure wireless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?

- A. PEAP
- B. EAP
- C. WPA2
- D. RADIUS

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



<https://www.gratisexam.com/>

<https://www.gratisexam.com/>