CompTIA

Exam Questions SY0-501

CompTIA Security+ Certification Exam

NEW QUESTION 1
- (Exam Topic 1)
Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications. Which of the following best describes what she will do?

A. Enter random or invalid data into the application in an attempt to cause it to fault
B. Work with the developers to eliminate horizontal privilege escalation opportunities
C. Test the applications for the existence of built-in- back doors left by the developers
D. Hash the application to verify it won't cause a false positive on the HIPS

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords. The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Select two.)

A. The portal will function as a service provider and request an authentication assertion.
B. The portal will function as an identity provider and issue an authentication assertion.
C. The portal will request an authentication ticket from each network that is transitively trusted.
D. The back-end networks will function as an identity provider and issue an authentication assertion.
E. The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store.
F. The back-end networks will verify the assertion token issued by the portal functioning as the identity provider.

Answer: AB

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 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 5
- (Exam Topic 1)
In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?

A. Elasticity
B. Scalability
C. High availability
D. Redundancy

Answer: A

Explanation:
Elasticity is defined as "the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible".

NEW QUESTION 6
- (Exam Topic 1)
Which of the following would a security specialist be able to determine upon examination of a server's certificate?

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

Answer: D

NEW QUESTION 7
- (Exam Topic 1)
An organization's file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

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

Answer: C

NEW QUESTION 8
- (Exam Topic 1)
A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network. Which of the following should be implemented in the administrator does not want to provide the wireless password or he certificate to the employees?

A. WPS
B. 802.1x
C. WPA2-PSK
D. TKIP

Answer: A

NEW QUESTION 9
- (Exam Topic 1)
A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are MOST likely occurring? (Select two.)

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

Answer: CE

NEW QUESTION 10
- (Exam Topic 1)
A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:

There is no standardization.

Employees ask for reimbursement for their devices.

Employees do not replace their devices often enough to keep them running efficiently.

The company does not have enough control over the devices.

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

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

Answer: D

NEW QUESTION 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 15
- (Exam Topic 1)
A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

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

Answer: B

NEW QUESTION 19
- (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 20
- (Exam Topic 1)
Which of the following occurs when the security of a web application relies on JavaScript for input validation?

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

Answer: A

NEW QUESTION 21
- (Exam Topic 1)
A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.0:6666. Which of the following should the
security analyst do to determine if the compromised system still has an active connection?

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

Answer: B

NEW QUESTION 23
- (Exam Topic 1)
A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

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

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 32
- (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 33
- (Exam Topic 1)
A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm?

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

Answer: A

NEW QUESTION 36
- (Exam Topic 1)
An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call.
The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

A. Give the application team administrator access during off-hours.
B. Disable other critical applications before granting the team access.
C. Give the application team read-only access.
D. Share the account with the application team.

Answer: C

NEW QUESTION 37
- (Exam Topic 1)
A user has attempted to access data at a higher classification level than the user's account is currently authorized to access. Which of the following access control models has been applied to this user's account?

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

Answer: A

NEW QUESTION 39
- (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.

Attacks

**Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.**

Attack Vector	Target	Identified Attack
Attacker gains confidential company information	Targeted CEO and board members	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker posts link to fake AV software → Multiple social networks	Broad set of victims	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker collecting credit card details	Phone-based victim	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker mass-mails product information to parties that have already opted out of receiving advertisements	Broad set of recipients	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker redirects name resolution entries from legitimate site to fraudulent site	Fraudulent site / Legitimate site / Victims	WHALING — SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK

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 41
- (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 46
- (Exam Topic 1)
A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

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

Answer: B

NEW QUESTION 50
- (Exam Topic 1)
A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select two.)

A. Generate an X.509-compliant certificate that is signed by a trusted CA.
B. Install and configure an SSH tunnel on the LDAP server.
C. Ensure port 389 is open between the clients and the servers using the communication.
D. Ensure port 636 is open between the clients and the servers using the communication.
E. Remote the LDAP directory service role from the server.

Answer: AD

NEW QUESTION 55
- (Exam Topic 1)
Which of the following attacks specifically impact data availability?

A. DDoS
B. Trojan
C. MITM
D. Rootkit

Answer: A

Explanation:
Reference: https://www.netscout.com/what-is-ddos

NEW QUESTION 60
- (Exam Topic 2)
A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls.
Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

A. Password complexity policies
B. Hardware tokens
C. Biometric systems
D. Role-based permissions
E. One time passwords
F. Separation of duties
G. Multifactor authentication
H. Single sign-on
I. Lease privilege

Answer: DFI

NEW QUESTION 63
- (Exam Topic 2)
A technician suspects that a system has been compromised. The technician reviews the following log entry: WARNING- hash mismatch:
C:\Window\SysWOW64\user32.dll
WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll
Based solely ono the above information, which of the following types of malware is MOST likely installed on the system?

A. Rootkit
B. Ransomware
C. Trojan
D. Backdoor

Answer: A

NEW QUESTION 66
- (Exam Topic 2)
Which of the following AES modes of operation provide authentication? (Select two.)

A. CCM
B. CBC
C. GCM
D. DSA
E. CFB

Answer: AC

NEW QUESTION 69
- (Exam Topic 2)
An administrator is configuring access to information located on a network file server named "Bowman". The files are located in a folder named "BalkFiles". The files are only for use by the "Matthews" division and should be read-only. The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model. Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files.
The administrator configures the file share according to the following table:

Share permissions

1	Everyone	Full control

File system permissions

2	Bowman\Users	Modify	Inherited
3	Domain\Matthews	Read	Not inherited
4	Bowman\System	Full control	Inherited
5	Bowman\Administrators	Full control	Not inherited

Which of the following rows has been misconfigured?

A. Row 1
B. Row 2
C. Row 3
D. Row 4
E. Row 5

Answer: D

NEW QUESTION 70
- (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 75
- (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 80
- (Exam Topic 2)
Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

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

Answer: A

NEW QUESTION 85
- (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 86
- (Exam Topic 2)
The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN.
Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance
C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

Answer: C

NEW QUESTION 89
- (Exam Topic 2)
AChief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

A. Implement time-of-day restrictions.
B. Audit file access times.
C. Secretly install a hidden surveillance camera.
D. Require swipe-card access to enter the lab.

Answer: D

NEW QUESTION 92
- (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 97
- (Exam Topic 2)
Which of the following cryptographic algorithms is irreversible?

A. RC4
B. SHA-256
C. DES
D. AES

Answer: B

NEW QUESTION 100
- (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 101
- (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 103
- (Exam Topic 2)
An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts BEST represents the risk described in this scenario?

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

Answer: A

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

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

Answer: C

NEW QUESTION 109
- (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 111
- (Exam Topic 2)
After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

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

Answer: B

NEW QUESTION 116
- (Exam Topic 2)
A system's administrator has finished configuring firewall ACL to allow access to a new web server.

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

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

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

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

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

Answer: B

NEW QUESTION 117
- (Exam Topic 2)
After a routine audit, a company discovers that engineering documents have been leaving the network on a particular port. The company must allow outbound traffic on this port, as it has a legitimate business use. Blocking the port would cause an outage. Which of the following technology controls should the company implement?

A. NAC
B. Web proxy
C. DLP
D. ACL

Answer: C

NEW QUESTION 120
- (Exam Topic 2)
A user of the wireless network is unable to gain access to the network. The symptoms are:
1.) Unable to connect to both internal and Internet resources
2.) The wireless icon shows connectivity but has no network access
The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.
Which of the following is the MOST likely cause of the connectivity issues?

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

Answer: A

NEW QUESTION 122
- (Exam Topic 2)
During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users.
Which of the following could best prevent this from occurring again?

A. Credential management
B. Group policy management
C. Acceptable use policy
D. Account expiration policy

Answer: B

NEW QUESTION 127
- (Exam Topic 2)
A security analyst accesses corporate web pages and inputs random data in the forms. The response received includes the type of database used and SQL commands that the database accepts. Which of the following should the security analyst use to prevent this vulnerability?

A. Application fuzzing
B. Error handling
C. Input validation
D. Pointer dereference

Answer: C

NEW QUESTION 128
- (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 129
- (Exam Topic 2)
A user is presented with the following items during the new-hire onboarding process:
-Laptop
-Secure USB drive
-Hardware OTP token
-External high-capacity HDD
-Password complexity policy
-Acceptable use policy
-HASP key
-Cable lock
Which of the following is one component of multifactor authentication?

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

Answer: C

NEW QUESTION 133
- (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 136
- (Exam Topic 2)
A portable data storage device has been determined to have malicious firmware. Which of the following is the BEST course of action to ensure data confidentiality?

A. Format the device
B. Re-image the device
C. Perform virus scan in the device
D. Physically destroy the device

Answer: C

NEW QUESTION 138
- (Exam Topic 2)
A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Select two.)

A. Ping
B. Ipconfig
C. Tracert
D. Netstat
E. Dig
F. Nslookup

Answer: BC

NEW QUESTION 140
- (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 142
- (Exam Topic 3)
A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

A. RSA
B. TwoFish
C. Diffie-Helman
D. NTLMv2
E. RIPEMD

Answer: B

NEW QUESTION 146
- (Exam Topic 3)
A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

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

Answer: A

NEW QUESTION 147
- (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 149
- (Exam Topic 3)
Which of the following is the LEAST secure hashing algorithm?

A. SHA1
B. RIPEMD
C. MD5
D. DES

Answer: C

NEW QUESTION 150
- (Exam Topic 3)
An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times. Which of the following describes this type of attack?

A. Integer overflow attack
B. Smurf attack

C. Replay attack
D. Buffer overflow attack
E. Cross-site scripting attack

Answer: C

NEW QUESTION 153
- (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 157
- (Exam Topic 3)
Which of the following is the summary of loss for a given year?

A. MTBF
B. ALE
C. SLA
D. ARO

Answer: B

NEW QUESTION 160
- (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 165
- (Exam Topic 3)
Which of the following can affect electrostatic discharge in a network operations center?

A. Fire suppression
B. Environmental monitoring
C. Proximity card access
D. Humidity controls

Answer: D

NEW QUESTION 168
- (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 172
- (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 173
- (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 175
- (Exam Topic 3)
Joe notices there are several user accounts on the local network generating spam with embedded malicious code. Which of the following technical control should Joe put in place to BEST reduce these incidents?

A. Account lockout
B. Group Based Privileges
C. Least privilege
D. Password complexity

Answer: A

NEW QUESTION 179
- (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 181
- (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 185
- (Exam Topic 3)
Which of the following is commonly used for federated identity management across multiple organizations?

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

Answer: A

NEW QUESTION 187

- (Exam Topic 3)
An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?

A. Find two identical messages with different hashes
B. Find two identical messages with the same hash
C. Find a common has between two specific messages
D. Find a common hash between a specific message and a random message

Answer: A

NEW QUESTION 189
- (Exam Topic 3)
A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base.
Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

A. Peer review
B. Component testing
C. Penetration testing
D. Vulnerability testing

Answer: C

Explanation:
A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

NEW QUESTION 190
- (Exam Topic 3)
An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure areA. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are. The controls used by the receptionist are in place to prevent which of the following types of attacks?

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

Answer: C

NEW QUESTION 194
- (Exam Topic 3)
A security administrator is developing training for corporate users on basic security principles for personal email accounts. Which of the following should be mentioned as the MOST secure way for password recovery?

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

Answer: B

NEW QUESTION 199
- (Exam Topic 3)
A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.
Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

NEW QUESTION 202
- (Exam Topic 3)
The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administer has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled. Which of the following would further obscure the presence of the wireless network?

A. Upgrade the encryption to WPA or WPA2
B. Create a non-zero length SSID for the wireless router
C. Reroute wireless users to a honeypot
D. Disable responses to a broadcast probe request

Answer: D

NEW QUESTION 206
- (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 211
- (Exam Topic 3)
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

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

Answer: C

NEW QUESTION 214
- (Exam Topic 3)
A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued. Which of the following should the administrator submit to receive a new certificate?

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

Answer: D

NEW QUESTION 217
- (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 218
- (Exam Topic 3)
After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

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

Answer: D

NEW QUESTION 222
- (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 223
- (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 224
- (Exam Topic 4)
Which of the following is the BEST choice for a security control that represents a preventive and corrective logical control at the same time?

A. Security awareness training
B. Antivirus
C. Firewalls
D. Intrusion detection system

Answer: B

NEW QUESTION 229
- (Exam Topic 4)
Which of the following strategies should a systems architect use to minimize availability risks due to insufficient storage capacity?

A. High availability

B. Scalability
C. Distributive allocation
D. Load balancing

Answer: B

NEW QUESTION 233
- (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 234
- (Exam Topic 4)
Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.
Which of the following authentication methods should be deployed to achieve this goal?

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

Answer: C

NEW QUESTION 237
- (Exam Topic 4)
The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems.
The help desk is receive reports that users are experiencing the following error when attempting to log in to their previous system:
Logon Failure: Access Denied
Which of the following can cause this issue?

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

Answer: C

NEW QUESTION 240
- (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 241
- (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 246
- (Exam Topic 4)
A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL. Which of the following is the attacker most likely utilizing?

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

Answer: A

NEW QUESTION 250
- (Exam Topic 4)
Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

A. Remote exploit
B. Amplification
C. Sniffing
D. Man-in-the-middle

Answer: A

NEW QUESTION 255
- (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 257
- (Exam Topic 4)
A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party. Which of the following actions did the company take regarding risks related to its email and collaboration services?

A. Transference
B. Acceptance
C. Mitigation
D. Deterrence

Answer: A

NEW QUESTION 260
- (Exam Topic 4)
While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack. Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Select two)

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

Answer: AD

NEW QUESTION 262
- (Exam Topic 4)
An organization wants to utilize a common, Internet-based third-party provider for authorization and authentication. The provider uses a technology based on OAuth 2.0 to provide required services. To which of the following technologies is the provider referring?

A. Open ID Connect
B. SAML
C. XACML
D. LDAP

Answer: A

NEW QUESTION 265
- (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.

```
VPN log:
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
Corporate firewall log:
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: d administrator has been given the following
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
Workstation host firewall log:
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersit-11111.com(https) (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hacksrmite11111.com(https) (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp) (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
```

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 267
- (Exam Topic 4)
During a recent audit, it was discovered that many services and desktops were missing security patches. Which of the following BEST describes the assessment that was performed to discover this issue?

A. Network mapping
B. Vulnerability scan
C. Port Scan
D. Protocol analysis

Answer: B

NEW QUESTION 268
- (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 271
- (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 276
- (Exam Topic 4)
A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following should the engineer implement if the design requires client MAC address to be visible across the tunnel?

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

Answer: D

NEW QUESTION 278
- (Exam Topic 4)
A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network. Which of the following is the MOST likely method used to gain access to the other host?

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

Answer: B

NEW QUESTION 281
- (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 285
- (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 290
- (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 294
- (Exam Topic 5)
A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted. Which of the following types of attack is the caller performing?

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

Answer: C

NEW QUESTION 295
- (Exam Topic 5)
A security technician is configuring an access management system to track and record user actions. Which of the following functions should the technician configure?

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

Answer: A

NEW QUESTION 298
- (Exam Topic 5)
A security administrator is diagnosing a server where the CPU utilization is at 100% for 24 hours. The main culprit of CPU utilization is the antivirus program. Which of the following issue could occur if left unresolved? (Select TWO)

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

Answer: BE

NEW QUESTION 299
- (Exam Topic 5)
A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it. The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer contact information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls. Which of the following will be the MOST efficient security control to implement to lower this risk?

A. Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact information.
B. Restrict screen capture features on the devices when using the custom application and the contact information.
C. Restrict contact information storage dataflow so it is only shared with the customer application.
D. Require complex passwords for authentication when accessing the contact information.

Answer: C

NEW QUESTION 301
- (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 305
- (Exam Topic 5)
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:
c:\nslookup - querytype=MX comptia.org
Server: Unknown Address: 198.51.100.45
comptia.org MX preference=10, mail exchanger = 92.68.102.33 comptia.org MX preference=20, mail exchanger = exchg1.comptia.org exchg1.comptia.org internet address = 192.168.102.67
Which of the following should the penetration tester conclude about the command output?

A. The public/private views on the Comptia.org DNS servers are misconfigured.
B. Comptia.org is running an older mail server, which may be vulnerable to exploits.
C. The DNS SPF records have not been updated for Comptia.org.
D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack.

Answer: D

NEW QUESTION 308
- (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 309
- (Exam Topic 5)
While troubleshooting a client application connecting to the network, the security administrator notices the following error: Certificate is not valid. Which of the following is the BEST way to check if the digital certificate is valid?

A. PKI
B. CRL
C. CSR
D. IPSec

Answer: B

NEW QUESTION 314
- (Exam Topic 5)
A security auditor is testing perimeter security in a building that is protected by badge readers. Which of the following types of attacks would MOST likely gain access?

A. Phishing
B. Man-in-the-middle
C. Tailgating
D. Watering hole
E. Shoulder surfing

Answer: C

NEW QUESTION 319
- (Exam Topic 5)
A procedure differs from a policy in that it:

A. is a high-level statement regarding the company's position on a topic.
B. sets a minimum expected baseline of behavior.
C. provides step-by-step instructions for performing a task.
D. describes adverse actions when violations occur.

Answer: C

NEW QUESTION 322
- (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 325
- (Exam Topic 5)
Several workstations on a network are found to be on OS versions that are vulnerable to a specific attack. Which of the following is considered to be a corrective action to combat this vulnerability?

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

Answer: D

NEW QUESTION 327
- (Exam Topic 5)
A systems administrator has isolated an infected system from the network and terminated the malicious process from executing. Which of the following should the administrator do NEXT according to the incident response process?

A. Restore lost data from a backup.
B. Wipe the system.
C. Document the lessons learned.
D. Determine the scope of impact.

Answer: A

NEW QUESTION 328
- (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 333
- (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 334
- (Exam Topic 5)
A company is performing an analysis of the corporate enterprise network with the intent of identifying what will cause losses in revenue, referrals, and/or reputation when out of commission. Which of the following is an element of a BIA that is being addressed?

A. Mission-essential function
B. Single point of failure
C. backup and restoration plans
D. Identification of critical systems

Answer: A

Explanation:
The BIA is composed of the following three steps: Determine mission/business processes and recovery criticality. Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.

NEW QUESTION 338
- (Exam Topic 5)
A security administrator has written a script that will automatically upload binary and text-based configuration files onto a remote server using a scheduled task. The configuration files contain sensitive information. Which of the following should the administrator use? (Select TWO)

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

Answer: CE

NEW QUESTION 343
- (Exam Topic 5)
A systems administrator wants to generate a self-signed certificate for an internal website. Which of the following steps should the systems administrator complete prior to installing the certificate on the server?

A. Provide the private key to a public CA.
B. Provide the public key to the internal CA.
C. Provide the public key to a public CA.
D. Provide the private key to the internal CA.
E. Provide the public/private key pair to the internal CA
F. Provide the public/private key pair to a public CA.

Answer: D

NEW QUESTION 344
- (Exam Topic 5)
Ann, a customer, is reporting that several important files are missing from her workstation. She recently
received communication from an unknown party who is requesting funds to restore the files. Which of the following attacks has occurred?

A. Ransomware
B. Keylogger
C. Buffer overflow
D. Rootkit

Answer: A

NEW QUESTION 348
- (Exam Topic 5)
A company stores highly sensitive data files used by the accounting system on a server file share. The accounting system uses a service account named accounting-svc to access the file share. The data is protected will a full disk encryption, and the permissions are set as follows:
File system permissions: Users = Read Only Share permission: accounting-svc = Read Only
Given the listed protections are in place and unchanged, to which of the following risks is the data still subject?

A. Exploitation of local console access and removal of data
B. Theft of physical hard drives and a breach of confidentiality
C. Remote exfiltration of data using domain credentials
D. Disclosure of sensitive data to third parties due to excessive share permissions

Answer: A

NEW QUESTION 351
- (Exam Topic 5)
Upon entering an incorrect password, the logon screen displays a message informing the user that the password does not match the username provided and is not the required length of 12 characters. Which of the following secure coding techniques should a security analyst address with the application developers to follow security best practices?

A. Input validation
B. Error handling
C. Obfuscation
D. Data exposure

Answer: B

NEW QUESTION 353
- (Exam Topic 5)
A bank uses a wireless network to transmit credit card purchases to a billing system.
Which of the following would be MOST appropriate to protect credit card information from being accessed by unauthorized individuals outside of the premises?

A. Air gap
B. Infrared detection
C. Faraday cage
D. Protected distributions

Answer: C

NEW QUESTION 355
- (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 359

- (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 361
- (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 362
- (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 367
- (Exam Topic 5)
An active/passive configuration has an impact on:

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

Answer: C

NEW QUESTION 372
- (Exam Topic 5)
A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFIenabled baby monitor while the baby's parents were sleeping.
Which of the following BEST describes how the intruder accessed the monitor?

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

Answer: D

NEW QUESTION 374
- (Exam Topic 5)
Joe, a user, has been trying to send Ann, a different user, an encrypted document via email. Ann has not received the attachment but is able to receive the header information. Which of the following is MOST likely preventing Ann from receiving the encrypted file?

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

Answer: B

NEW QUESTION 377
- (Exam Topic 5)
After a recent internal breach, a company decided to regenerate and reissue all certificates used in the transmission of confidential information. The company places the greatest importance on confidentiality and non-repudiation, and decided to generate dual key pairs for each client. Which of the following BEST describes how the company will use these certificates?

A. One key pair will be used for encryption and decryptio
B. The other will be used to digitally sign the data.
C. One key pair will be used for encryptio
D. The other key pair will provide extended validation.
E. Data will be encrypted once by each key, doubling the confidentiality and non-repudiation strength.
F. One key pair will be used for internal communication, and the other will be used for external communication.

Answer: A

NEW QUESTION 378
- (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 379
......

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 1)
Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications. Which of the following best describes what she will do?

A. Enter random or invalid data into the application in an attempt to cause it to fault
B. Work with the developers to eliminate horizontal privilege escalation opportunities
C. Test the applications for the existence of built-in- back doors left by the developers
D. Hash the application to verify it won't cause a false positive on the HIPS

Answer: A

NEW QUESTION 2
- (Exam Topic 1)
A company has three divisions, each with its own networks and services. The company decides to make its secure web portal accessible to all employees utilizing their existing usernames and passwords. The security administrator has elected to use SAML to support authentication. In this scenario, which of the following will occur when users try to authenticate to the portal? (Select two.)

A. The portal will function as a service provider and request an authentication assertion.
B. The portal will function as an identity provider and issue an authentication assertion.
C. The portal will request an authentication ticket from each network that is transitively trusted.
D. The back-end networks will function as an identity provider and issue an authentication assertion.
E. The back-end networks will request authentication tickets from the portal, which will act as the third-party service provider authentication store.
F. The back-end networks will verify the assertion token issued by the portal functioning as the identity provider.

Answer: AB

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 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 5
- (Exam Topic 1)
In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?

A. Elasticity
B. Scalability
C. High availability
D. Redundancy

Answer: A

Explanation:
Elasticity is defined as "the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible".

NEW QUESTION 6
- (Exam Topic 1)
Which of the following would a security specialist be able to determine upon examination of a server's certificate?

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

Answer: D

NEW QUESTION 7
- (Exam Topic 1)
An organization's file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

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

Answer: C

NEW QUESTION 8
- (Exam Topic 1)
A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network. Which of the following should be implemented in the administrator does not want to provide the wireless password or he certificate to the employees?

A. WPS
B. 802.1x
C. WPA2-PSK
D. TKIP

Answer: A

NEW QUESTION 9
- (Exam Topic 1)
A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are MOST likely occurring? (Select two.)

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

Answer: CE

NEW QUESTION 10
- (Exam Topic 1)
A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:

▶ There is no standardization.

▶ Employees ask for reimbursement for their devices.

▶ Employees do not replace their devices often enough to keep them running efficiently.

▶ The company does not have enough control over the devices.
Which of the following is a deployment model that would help the company overcome these problems?

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

Answer: D

NEW QUESTION 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 15
- (Exam Topic 1)
A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the MOST likely risk in this situation?

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

Answer: B

NEW QUESTION 19
- (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 20
- (Exam Topic 1)
Which of the following occurs when the security of a web application relies on JavaScript for input validation?

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

Answer: A

NEW QUESTION 21
- (Exam Topic 1)
A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.0:6666. Which of the following should the
security analyst do to determine if the compromised system still has an active connection?

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

Answer: B

NEW QUESTION 23
- (Exam Topic 1)
A company is terminating an employee for misbehavior. Which of the following steps is MOST important in the process of disengagement from this employee?

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

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 32
- (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 33
- (Exam Topic 1)
A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm?

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

Answer: A

NEW QUESTION 36
- (Exam Topic 1)
An application team is performing a load-balancing test for a critical application during off-hours and has requested access to the load balancer to review which servers are up without having the administrator on call.
The security analyst is hesitant to give the application team full access due to other critical applications running on the load balancer. Which of the following is the BEST solution for security analyst to process the request?

A. Give the application team administrator access during off-hours.
B. Disable other critical applications before granting the team access.
C. Give the application team read-only access.
D. Share the account with the application team.

Answer: C

NEW QUESTION 37
- (Exam Topic 1)
A user has attempted to access data at a higher classification level than the user's account is currently authorized to access. Which of the following access control models has been applied to this user's account?

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

Answer: A

NEW QUESTION 39
- (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.

Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.

Attack Vector	Target	Identified Attack
Attacker gains confidential company information	Targeted CEO and board members	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker posts link to fake AV software → Multiple social networks	Broad set of victims	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker collecting credit card details	Phone-based victim	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker mass-mails product information to parties that have already opted out of receiving advertisements	Broad set of recipients	SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK
Attacker redirects name resolution entries from legitimate site to fraudulent site	Fraudulent site / Legitimate site / Victims	WHALING — SPIM / VISHING / PHISHING / WHALING / HOAX / PHARMING / SPEAR PHISHING / SPOOFING / SPAM / XMAS ATTACK

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 41
- (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 46
- (Exam Topic 1)
A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

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

Answer: B

NEW QUESTION 50
- (Exam Topic 1)
A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select two.)

A. Generate an X.509-compliant certificate that is signed by a trusted CA.
B. Install and configure an SSH tunnel on the LDAP server.
C. Ensure port 389 is open between the clients and the servers using the communication.
D. Ensure port 636 is open between the clients and the servers using the communication.
E. Remote the LDAP directory service role from the server.

Answer: AD

NEW QUESTION 55
- (Exam Topic 1)
Which of the following attacks specifically impact data availability?

A. DDoS
B. Trojan
C. MITM
D. Rootkit

Answer: A

Explanation:
Reference: https://www.netscout.com/what-is-ddos

NEW QUESTION 60
- (Exam Topic 2)
A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls.
Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

A. Password complexity policies
B. Hardware tokens
C. Biometric systems
D. Role-based permissions
E. One time passwords
F. Separation of duties
G. Multifactor authentication
H. Single sign-on
I. Lease privilege

Answer: DFI

NEW QUESTION 63
- (Exam Topic 2)
A technician suspects that a system has been compromised. The technician reviews the following log entry: WARNING- hash mismatch: C:\Window\SysWOW64\user32.dll
WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll
Based solely ono the above information, which of the following types of malware is MOST likely installed on the system?

A. Rootkit
B. Ransomware
C. Trojan
D. Backdoor

Answer: A

NEW QUESTION 66
- (Exam Topic 2)
Which of the following AES modes of operation provide authentication? (Select two.)

A. CCM
B. CBC
C. GCM
D. DSA
E. CFB

Answer: AC

NEW QUESTION 69
- (Exam Topic 2)
An administrator is configuring access to information located on a network file server named "Bowman". The files are located in a folder named "BalkFiles". The files are only for use by the "Matthews" division and should be read-only. The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model. Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files.
The administrator configures the file share according to the following table:

Share permissions

1	Everyone	Full control

File system permissions

2	Bowman\Users	Modify	Inherited
3	Domain\Matthews	Read	Not inherited
4	Bowman\System	Full control	Inherited
5	Bowman\Administrators	Full control	Not inherited

Which of the following rows has been misconfigured?

A. Row 1
B. Row 2
C. Row 3
D. Row 4
E. Row 5

Answer: D

NEW QUESTION 70
- (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 75
- (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 80
- (Exam Topic 2)
Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

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

Answer: A

NEW QUESTION 85
- (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 86
- (Exam Topic 2)
The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN.
Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance
C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

Answer: C

NEW QUESTION 89
- (Exam Topic 2)
AChief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

A. Implement time-of-day restrictions.
B. Audit file access times.
C. Secretly install a hidden surveillance camera.
D. Require swipe-card access to enter the lab.

Answer: D

NEW QUESTION 92
- (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 97
- (Exam Topic 2)
Which of the following cryptographic algorithms is irreversible?

A. RC4
B. SHA-256
C. DES
D. AES

Answer: B

NEW QUESTION 100
- (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 101
- (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 103
- (Exam Topic 2)
An organization's primary datacenter is experiencing a two-day outage due to an HVAC malfunction. The node located in the datacenter has lost power and is no longer operational, impacting the ability of all users to connect to the alternate datacenter. Which of the following BIA concepts BEST represents the risk described in this scenario?

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

Answer: A

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

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

Answer: C

NEW QUESTION 109
- (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 111
- (Exam Topic 2)
After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

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

Answer: B

NEW QUESTION 116
- (Exam Topic 2)
A system's administrator has finished configuring firewall ACL to allow access to a new web server.

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

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

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

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

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

Answer: B

NEW QUESTION 117
- (Exam Topic 2)
After a routine audit, a company discovers that engineering documents have been leaving the network on a particular port. The company must allow outbound traffic on this port, as it has a legitimate business use. Blocking the port would cause an outage. Which of the following technology controls should the company implement?

A. NAC
B. Web proxy
C. DLP
D. ACL

Answer: C

NEW QUESTION 120
- (Exam Topic 2)
A user of the wireless network is unable to gain access to the network. The symptoms are:
1.) Unable to connect to both internal and Internet resources
2.) The wireless icon shows connectivity but has no network access
The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.
Which of the following is the MOST likely cause of the connectivity issues?

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

Answer: A

NEW QUESTION 122
- (Exam Topic 2)
During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users.
Which of the following could best prevent this from occurring again?

A. Credential management
B. Group policy management
C. Acceptable use policy
D. Account expiration policy

Answer: B

NEW QUESTION 127
- (Exam Topic 2)
A security analyst accesses corporate web pages and inputs random data in the forms. The response received includes the type of database used and SQL commands that the database accepts. Which of the following should the security analyst use to prevent this vulnerability?

A. Application fuzzing
B. Error handling
C. Input validation
D. Pointer dereference

Answer: C

NEW QUESTION 128
- (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 129
- (Exam Topic 2)
A user is presented with the following items during the new-hire onboarding process:
-Laptop
-Secure USB drive
-Hardware OTP token
-External high-capacity HDD
-Password complexity policy
-Acceptable use policy
-HASP key
-Cable lock
Which of the following is one component of multifactor authentication?

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

Answer: C

NEW QUESTION 133
- (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 136
- (Exam Topic 2)
A portable data storage device has been determined to have malicious firmware. Which of the following is the BEST course of action to ensure data confidentiality?

A. Format the device
B. Re-image the device
C. Perform virus scan in the device
D. Physically destroy the device

Answer: C

NEW QUESTION 138
- (Exam Topic 2)
A security administrator suspects a MITM attack aimed at impersonating the default gateway is underway. Which of the following tools should the administrator use to detect this attack? (Select two.)

A. Ping
B. Ipconfig
C. Tracert
D. Netstat
E. Dig
F. Nslookup

Answer: BC

NEW QUESTION 140
- (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 142
- (Exam Topic 3)
A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

A. RSA
B. TwoFish
C. Diffie-Helman
D. NTLMv2
E. RIPEMD

Answer: B

NEW QUESTION 146
- (Exam Topic 3)
A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

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

Answer: A

NEW QUESTION 147
- (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 149
- (Exam Topic 3)
Which of the following is the LEAST secure hashing algorithm?

A. SHA1
B. RIPEMD
C. MD5
D. DES

Answer: C

NEW QUESTION 150
- (Exam Topic 3)
An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times. Which of the following describes this type of attack?

A. Integer overflow attack
B. Smurf attack

C. Replay attack
D. Buffer overflow attack
E. Cross-site scripting attack

Answer: C

NEW QUESTION 153
- (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 157
- (Exam Topic 3)
Which of the following is the summary of loss for a given year?

A. MTBF
B. ALE
C. SLA
D. ARO

Answer: B

NEW QUESTION 160
- (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 165
- (Exam Topic 3)
Which of the following can affect electrostatic discharge in a network operations center?

A. Fire suppression
B. Environmental monitoring
C. Proximity card access
D. Humidity controls

Answer: D

NEW QUESTION 168
- (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 172
- (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 173
- (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 175
- (Exam Topic 3)
Joe notices there are several user accounts on the local network generating spam with embedded malicious code. Which of the following technical control should Joe put in place to BEST reduce these incidents?

A. Account lockout
B. Group Based Privileges
C. Least privilege
D. Password complexity

Answer: A

NEW QUESTION 179
- (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 181
- (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 185
- (Exam Topic 3)
Which of the following is commonly used for federated identity management across multiple organizations?

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

Answer: A

NEW QUESTION 187

- (Exam Topic 3)
An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?

A. Find two identical messages with different hashes
B. Find two identical messages with the same hash
C. Find a common has between two specific messages
D. Find a common hash between a specific message and a random message

Answer: A

NEW QUESTION 189
- (Exam Topic 3)
A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base.
Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

A. Peer review
B. Component testing
C. Penetration testing
D. Vulnerability testing

Answer: C

Explanation:
A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

NEW QUESTION 190
- (Exam Topic 3)
An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure areA. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to the secure are. The controls used by the receptionist are in place to prevent which of the following types of attacks?

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

Answer: C

NEW QUESTION 194
- (Exam Topic 3)
A security administrator is developing training for corporate users on basic security principles for personal email accounts. Which of the following should be mentioned as the MOST secure way for password recovery?
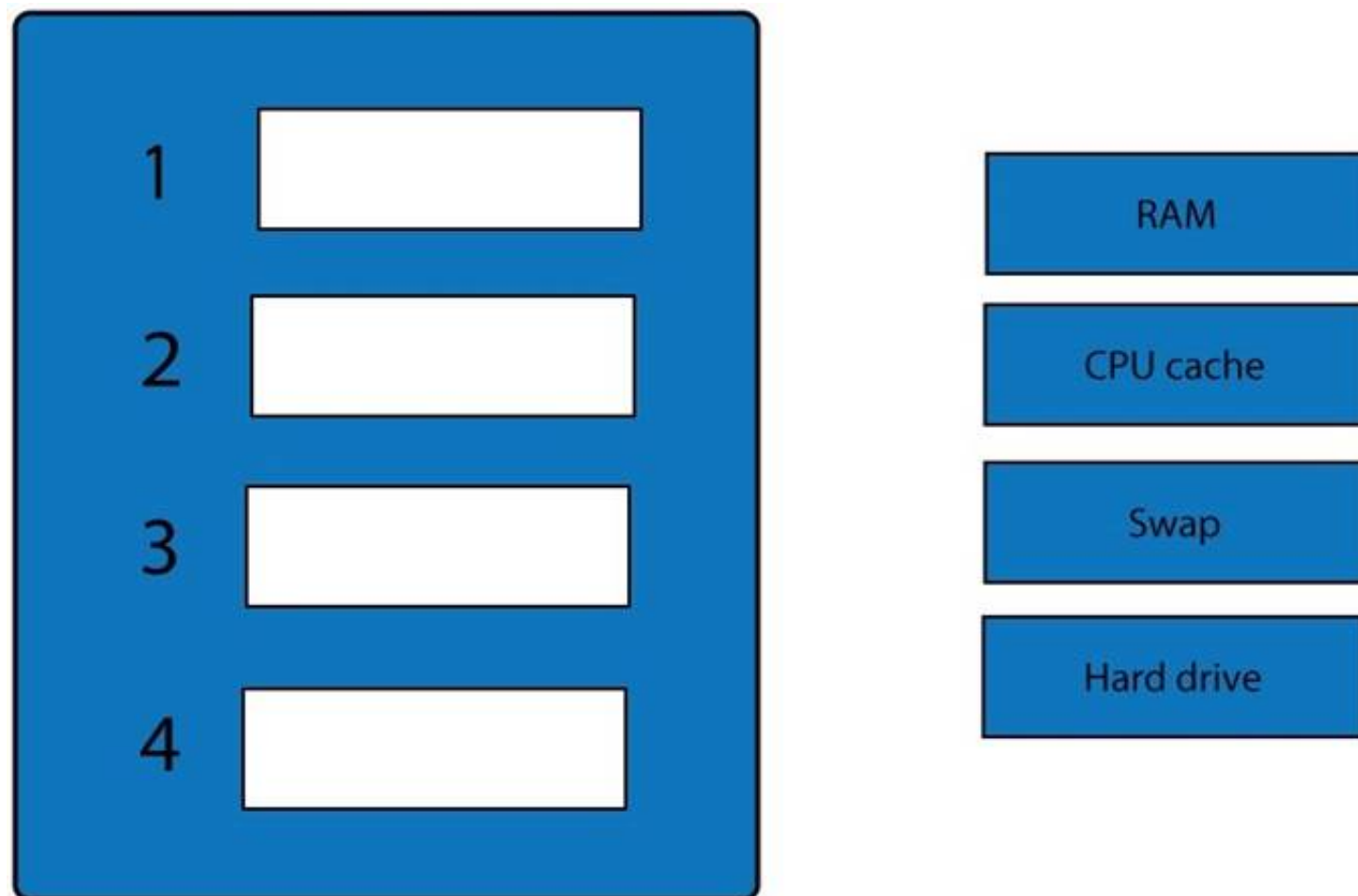
A. Utilizing a single Qfor password recovery
B. Sending a PIN to a smartphone through text message
C. Utilizing CAPTCHA to avoid brute force attacks
D. Use a different e-mail address to recover password

Answer: B

NEW QUESTION 199
- (Exam Topic 3)
A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.
Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

NEW QUESTION 202
- (Exam Topic 3)
The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administer has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled. Which of the following would further obscure the presence of the wireless network?

A. Upgrade the encryption to WPA or WPA2
B. Create a non-zero length SSID for the wireless router
C. Reroute wireless users to a honeypot
D. Disable responses to a broadcast probe request

Answer: D

NEW QUESTION 206
- (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 211
- (Exam Topic 3)
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

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

Answer: C

NEW QUESTION 214
- (Exam Topic 3)
A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued. Which of the following should the administrator submit to receive a new certificate?

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

Answer: D

NEW QUESTION 217
- (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 218
- (Exam Topic 3)
After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

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

Answer: D

NEW QUESTION 222
- (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 223
- (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 224
- (Exam Topic 4)
Which of the following is the BEST choice for a security control that represents a preventive and corrective logical control at the same time?

A. Security awareness training
B. Antivirus
C. Firewalls
D. Intrusion detection system

Answer: B

NEW QUESTION 229
- (Exam Topic 4)
Which of the following strategies should a systems architect use to minimize availability risks due to insufficient storage capacity?

A. High availability

B. Scalability
C. Distributive allocation
D. Load balancing

Answer: B

NEW QUESTION 233
- (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 234
- (Exam Topic 4)
Users in a corporation currently authenticate with a username and password. A security administrator wishes to implement two-factor authentication to improve security.
Which of the following authentication methods should be deployed to achieve this goal?

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

Answer: C

NEW QUESTION 237
- (Exam Topic 4)
The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems.
The help desk is receive reports that users are experiencing the following error when attempting to log in to their previous system:
Logon Failure: Access Denied
Which of the following can cause this issue?

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

Answer: C

NEW QUESTION 240
- (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 241
- (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 246
- (Exam Topic 4)
A malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL. Which of the following is the attacker most likely utilizing?

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

Answer: A

NEW QUESTION 250
- (Exam Topic 4)
Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

A. Remote exploit
B. Amplification
C. Sniffing
D. Man-in-the-middle

Answer: A

NEW QUESTION 255
- (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 257
- (Exam Topic 4)
A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party. Which of the following actions did the company take regarding risks related to its email and collaboration services?

A. Transference
B. Acceptance
C. Mitigation
D. Deterrence

Answer: A

NEW QUESTION 260
- (Exam Topic 4)
While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack. Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Select two)

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

Answer: AD

NEW QUESTION 262
- (Exam Topic 4)
An organization wants to utilize a common, Internet-based third-party provider for authorization and authentication. The provider uses a technology based on OAuth 2.0 to provide required services. To which of the following technologies is the provider referring?

A. Open ID Connect
B. SAML
C. XACML
D. LDAP

Answer: A

NEW QUESTION 265
- (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.

```
VPN log:
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
Corporate firewall log:
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: d administrator has been given the following
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
Workstation host firewall log:
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersit-11111.com(https) (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hacks-mit11111.com(https) (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp) (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
```

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 267
- (Exam Topic 4)
During a recent audit, it was discovered that many services and desktops were missing security patches. Which of the following BEST describes the assessment that was performed to discover this issue?

A. Network mapping
B. Vulnerability scan
C. Port Scan
D. Protocol analysis

Answer: B

NEW QUESTION 268
- (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 271
- (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 276
- (Exam Topic 4)
A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following should the engineer implement if the design requires client MAC address to be visible across the tunnel?

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

Answer: D

NEW QUESTION 278
- (Exam Topic 4)
A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network. Which of the following is the MOST likely method used to gain access to the other host?

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

Answer: B

NEW QUESTION 281
- (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 285
- (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 290
- (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 294
- (Exam Topic 5)
A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted. Which of the following types of attack is the caller performing?

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

Answer: C

NEW QUESTION 295
- (Exam Topic 5)
A security technician is configuring an access management system to track and record user actions. Which of the following functions should the technician configure?

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

Answer: A

NEW QUESTION 298
- (Exam Topic 5)
A security administrator is diagnosing a server where the CPU utilization is at 100% for 24 hours. The main culprit of CPU utilization is the antivirus program. Which of the following issue could occur if left unresolved? (Select TWO)

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

Answer: BE

NEW QUESTION 299
- (Exam Topic 5)
A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it. The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer contact
information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls. Which of the following will be the MOST efficient security control to implement to lower this risk?

A. Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact information.
B. Restrict screen capture features on the devices when using the custom application and the contact information.
C. Restrict contact information storage dataflow so it is only shared with the customer application.
D. Require complex passwords for authentication when accessing the contact information.

Answer: C

NEW QUESTION 301
- (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 305
- (Exam Topic 5)
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet:
c:\nslookup - querytype=MX comptia.org
Server: Unknown Address: 198.51.100.45
comptia.org MX preference=10, mail exchanger = 92.68.102.33 comptia.org MX preference=20, mail exchanger = exchg1.comptia.org exchg1.comptia.org internet address = 192.168.102.67
Which of the following should the penetration tester conclude about the command output?

A. The public/private views on the Comptia.org DNS servers are misconfigured.
B. Comptia.org is running an older mail server, which may be vulnerable to exploits.
C. The DNS SPF records have not been updated for Comptia.org.
D. 192.168.102.67 is a backup mail server that may be more vulnerable to attack.

Answer: D

NEW QUESTION 308
- (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 309
- (Exam Topic 5)
While troubleshooting a client application connecting to the network, the security administrator notices the following error: Certificate is not valid. Which of the following is the BEST way to check if the digital certificate is valid?

A. PKI
B. CRL
C. CSR
D. IPSec

Answer: B

NEW QUESTION 314
- (Exam Topic 5)
A security auditor is testing perimeter security in a building that is protected by badge readers. Which of the following types of attacks would MOST likely gain access?

A. Phishing
B. Man-in-the-middle
C. Tailgating
D. Watering hole
E. Shoulder surfing

Answer: C

NEW QUESTION 319
- (Exam Topic 5)
A procedure differs from a policy in that it:

A. is a high-level statement regarding the company's position on a topic.
B. sets a minimum expected baseline of behavior.
C. provides step-by-step instructions for performing a task.
D. describes adverse actions when violations occur.

Answer: C

NEW QUESTION 322
- (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 325
- (Exam Topic 5)
Several workstations on a network are found to be on OS versions that are vulnerable to a specific attack. Which of the following is considered to be a corrective action to combat this vulnerability?

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

Answer: D

NEW QUESTION 327
- (Exam Topic 5)
A systems administrator has isolated an infected system from the network and terminated the malicious process from executing. Which of the following should the administrator do NEXT according to the incident response process?

A. Restore lost data from a backup.
B. Wipe the system.
C. Document the lessons learned.
D. Determine the scope of impact.

Answer: A

NEW QUESTION 328
- (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 333
- (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 334
- (Exam Topic 5)
A company is performing an analysis of the corporate enterprise network with the intent of identifying what will cause losses in revenue, referrals, and/or reputation when out of commission. Which of the following is an element of a BIA that is being addressed?

A. Mission-essential function
B. Single point of failure
C. backup and restoration plans
D. Identification of critical systems

Answer: A

Explanation:
The BIA is composed of the following three steps: Determine mission/business processes and recovery criticality. Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.

NEW QUESTION 338
- (Exam Topic 5)
A security administrator has written a script that will automatically upload binary and text-based configuration files onto a remote server using a scheduled task. The configuration files contain sensitive information. Which of the following should the administrator use? (Select TWO)

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

Answer: CE

NEW QUESTION 343
- (Exam Topic 5)
A systems administrator wants to generate a self-signed certificate for an internal website. Which of the following steps should the systems administrator complete prior to installing the certificate on the server?

A. Provide the private key to a public CA.
B. Provide the public key to the internal CA.
C. Provide the public key to a public CA.
D. Provide the private key to the internal CA.
E. Provide the public/private key pair to the internal CA.
F. Provide the public/private key pair to a public CA.

Answer: D

NEW QUESTION 344
- (Exam Topic 5)
Ann, a customer, is reporting that several important files are missing from her workstation. She recently
received communication from an unknown party who is requesting funds to restore the files. Which of the following attacks has occurred?

A. Ransomware
B. Keylogger
C. Buffer overflow
D. Rootkit

Answer: A

NEW QUESTION 348
- (Exam Topic 5)
A company stores highly sensitive data files used by the accounting system on a server file share. The accounting system uses a service account named
accounting-svc to access the file share. The data is protected will a full disk encryption, and the permissions are set as follows:
File system permissions: Users = Read Only Share permission: accounting-svc = Read Only
Given the listed protections are in place and unchanged, to which of the following risks is the data still subject?

A. Exploitation of local console access and removal of data
B. Theft of physical hard drives and a breach of confidentiality
C. Remote exfiltration of data using domain credentials
D. Disclosure of sensitive data to third parties due to excessive share permissions

Answer: A

NEW QUESTION 351
- (Exam Topic 5)
Upon entering an incorrect password, the logon screen displays a message informing the user that the password does not match the username provided and is not
the required length of 12 characters. Which of the following secure coding techniques should a security analyst address with the application developers to follow
security best practices?

A. Input validation
B. Error handling
C. Obfuscation
D. Data exposure

Answer: B

NEW QUESTION 353
- (Exam Topic 5)
A bank uses a wireless network to transmit credit card purchases to a billing system.
Which of the following would be MOST appropriate to protect credit card information from being accessed by unauthorized individuals outside of the premises?

A. Air gap
B. Infrared detection
C. Faraday cage
D. Protected distributions

Answer: C

NEW QUESTION 355
- (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 359

- (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 361
- (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 362
- (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 367
- (Exam Topic 5)
An active/passive configuration has an impact on:

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

Answer: C

NEW QUESTION 372
- (Exam Topic 5)
A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFIenabled baby monitor while the baby's parents were sleeping.
Which of the following BEST describes how the intruder accessed the monitor?

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

Answer: D

NEW QUESTION 374
- (Exam Topic 5)
Joe, a user, has been trying to send Ann, a different user, an encrypted document via email. Ann has not received the attachment but is able to receive the header information. Which of the following is MOST likely preventing Ann from receiving the encrypted file?

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

Answer: B

NEW QUESTION 377
- (Exam Topic 5)
After a recent internal breach, a company decided to regenerate and reissue all certificates used in the transmission of confidential information. The company places the greatest importance on confidentiality and non-repudiation, and decided to generate dual key pairs for each client. Which of the following BEST describes how the company will use these certificates?

A. One key pair will be used for encryption and decryptio
B. The other will be used to digitally sign the data.
C. One key pair will be used for encryptio
D. The other key pair will provide extended validation.
E. Data will be encrypted once by each key, doubling the confidentiality and non-repudiation strength.
F. One key pair will be used for internal communication, and the other will be used for external communication.

Answer: A

NEW QUESTION 378
- (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 379
......

Relate Links

100% Pass Your SY0-501 Exam with Exambible Prep Materials

https://www.exambible.com/SY0-501-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/