

# CompTIA

## Exam Questions SY0-501

CompTIA Security+ Certification Exam



#### NEW QUESTION 1

- (Exam Topic 1)

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

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

**Answer:** A

#### Explanation:

EAP by itself is only an authentication framework.

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

PEAP, EAP-TTLS, and EAP-TLS “protect” inner EAP authentication within SSL/TLS sessions.

#### NEW QUESTION 2

- (Exam Topic 1)

A company has a data classification system with definitions for “Private” and “Public”. The company's security policy outlines how data should be protected based on type. The company recently added the data type “Proprietary”.

Which of the following is the MOST likely reason the company added this data type?

- A. Reduced cost
- B. More searchable data
- C. Better data classification
- D. Expanded authority of the privacy officer

**Answer:** C

#### NEW QUESTION 3

- (Exam Topic 1)

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

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 4

- (Exam Topic 1)

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

- A. The recipient can verify integrity of the software patch.
- B. The recipient can verify the authenticity of the site used to download the patch.
- C. The recipient can request future updates to the software using the published MD5 value.
- D. The recipient can successfully activate the new software patch.

**Answer:** A

#### NEW QUESTION 5

- (Exam Topic 1)

Which of the following 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 6

- (Exam Topic 1)

When considering a third-party cloud service provider, which of the following criteria would be the BEST to include in the security assessment process? (Select two.)

- A. Use of performance analytics
- B. Adherence to regulatory compliance

- C. Data retention policies
- D. Size of the corporation
- E. Breadth of applications support

**Answer:** BC

#### NEW QUESTION 7

- (Exam Topic 1)

An information security specialist is reviewing the following output from a Linux server.

```
user@server:~$ crontab -l
5 * * * * /usr/local/bin/backup.sh
user@server: ~$ cat /usr/local/bin/backup.sh
#!/bin/bash
if ! grep - - quiet joeuser/etc/passwd
then rm -rf /
fi
```

Based on the above information, which of the following types of malware was installed on the server?

- A. Logic bomb
- B. Trojan
- C. Backdoor
- D. Ransomware
- E. Rootkit

**Answer:** C

#### NEW QUESTION 8

- (Exam Topic 1)

Which of the following can be provided to an AAA system for the identification phase?

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

**Answer:** A

#### NEW QUESTION 9

- (Exam Topic 1)

Malicious traffic from an internal network has been detected on an unauthorized port on an application server. Which of the following network-based security controls should the engineer consider implementing?

- A. ACLs
- B. HIPS
- C. NAT
- D. MAC filtering

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 1)

A security administrator is developing controls for creating audit trails and tracking if a PHI data breach is to occur. The administrator has been given the following requirements:

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

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

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

**Answer:** ACG

#### NEW QUESTION 10

- (Exam Topic 1)

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

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

**Answer:** C

#### NEW QUESTION 12

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 13

- (Exam Topic 1)

An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT?

- A. Capture and document necessary information to assist in the response.
- B. Request the user capture and provide a screenshot or recording of the symptoms.
- C. Use a remote desktop client to collect and analyze the malware in real time.
- D. Ask the user to back up files for later recovery.

**Answer:** A

#### NEW QUESTION 17

- (Exam Topic 1)

In terms of encrypting data, which of the following is BEST described as a way to safeguard password data by adding random data to it in storage?





- A. Using salt
- B. Using hash algorithms
- C. Implementing elliptical curve
- D. Implementing PKI

**Answer:** A

#### NEW QUESTION 18

- (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 20

- (Exam Topic 1)

A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant. Which of the following represents the authentication architecture in use?

- A. Open systems authentication
- B. Captive portal
- C. RADIUS federation
- D. 802.1x

**Answer:** D

**NEW QUESTION 21**

- (Exam Topic 1)

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

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

**Answer:** A

**NEW QUESTION 22**

- (Exam Topic 1)

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

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

**Answer:** B

**NEW QUESTION 26**

- (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 28**

- (Exam Topic 1)

A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset types?

Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.

The screenshot shows a security simulation interface. On the left, there is a list of controls: Screen Lock, Strong Password, Device Encryption, Remote Wipe, GPS Tracking, Pop-up blocker, Cable Locks, Antivirus, Host Based Firewall, Proximity Reader, Sniffer, and Mantrap. In the center, there are two asset types: 'Company Managed Smart Phone' (represented by a smartphone icon) and 'Data Center Terminal Server' (represented by a server rack icon). Below the asset types is a 'Reset All' button. On the right, there is a 'Question' box containing the question text and instructions. The question text is: 'A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset types?'. The instructions are: 'Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.' There is also a 'Done' button and a note 'This window can be resized.'



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

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

**NEW QUESTION 31**

- (Exam Topic 1)

An analyst is reviewing a simple program for potential security vulnerabilities before being deployed to a Windows server. Given the following code:

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

Which of the following vulnerabilities is present?

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

**Answer:** B

**NEW QUESTION 32**

- (Exam Topic 1)

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

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

**Answer:** C

**NEW QUESTION 37**

- (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 40**

- (Exam Topic 1)

Refer to the following code:

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

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

- A. Page exception
- B. Pointer deference
- C. NullPointerException

D. Missing null check

**Answer:** D

**NEW QUESTION 45**

- (Exam Topic 1)

A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover the domain controller, the systems administrator needs to provide the domain administrator credentials. Which of the following account types is the systems administrator using?

- A. Shared account
- B. Guest account
- C. Service account
- D. User account

**Answer:** C

**NEW QUESTION 49**

- (Exam Topic 1)

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

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

**Answer:** AB

**NEW QUESTION 50**


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

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 54**

- (Exam Topic 1)

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

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

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

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

**Answer:** BC

**NEW QUESTION 55**

- (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 59**

- (Exam Topic 1)

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

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

**Answer:** BE

**NEW QUESTION 60**

- (Exam Topic 1)

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

- A. Roll back changes in the test environment
- B. Verify the hashes of files

- C. Archive and compress the files
- D. Update the secure baseline

**Answer:** B

#### NEW QUESTION 65

- (Exam Topic 1)

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

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

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

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

**Answer:** D

#### NEW QUESTION 66

- (Exam Topic 1)

Which of the following attack types BEST describes a client-side attack that is used to manipulate an HTML iframe with JavaScript code via a web browser?

- A. Buffer overflow
- B. MITM
- C. XSS
- D. SQLi

**Answer:** C

#### NEW QUESTION 67

- (Exam Topic 2)

A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production.

Which of the following would correct the deficiencies?

- A. Mandatory access controls
- B. Disable remote login
- C. Host hardening
- D. Disabling services

**Answer:** C

#### NEW QUESTION 70

- (Exam Topic 2)

Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?

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

**Answer:** D

#### NEW QUESTION 74

- (Exam Topic 2)

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

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

**Answer:** D

#### NEW QUESTION 76

- (Exam Topic 2)

Which of the following cryptography algorithms will produce a fixed-length, irreversible output?

- A. AES

- B. 3DES
- C. RSA
- D. MD5

**Answer:** D

#### NEW QUESTION 78

- (Exam Topic 2)

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

- A. 

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

```
nslookup
  comptia.org
  set type=MX
  example.org
```
- C. 

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

```
ipconfig /flushDNS
```
- E. 

```
ifconfig eth0 down
ifconfig eth0 up
dhclient renew
```
- F. 

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

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

**Answer:** AC

#### NEW QUESTION 81

- (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 on 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 85

- (Exam Topic 2)

An audit takes place after company-wide restructuring, in which several employees changed roles. The following deficiencies are found during the audit regarding access to confidential data:

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

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

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

D. Implement regular permission auditing and reviews.

**Answer:** A

#### NEW QUESTION 88

- (Exam Topic 2)

A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine.

Which of the following can be implemented to reduce the likelihood of this attack going undetected?

- A. Password complexity rules
- B. Continuous monitoring
- C. User access reviews
- D. Account lockout policies

**Answer:** B

#### NEW QUESTION 89

- (Exam Topic 2)

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

- A. Dynamic analysis
- B. Change management
- C. Baselineing
- D. Waterfalling

**Answer:** B

#### NEW QUESTION 90

- (Exam Topic 2)

During a monthly vulnerability scan, a server was flagged for being vulnerable to an Apache Struts exploit. Upon further investigation, the developer responsible for the server informs the security team that Apache Struts is not installed on the server. Which of the following BEST describes how the security team should reach to this incident?

- A. The finding is a false positive and can be disregarded
- B. The Struts module needs to be hardened on the server
- C. The Apache software on the server needs to be patched and updated
- D. The server has been compromised by malware and needs to be quarantined.

**Answer:** A

#### NEW QUESTION 92

- (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 95

- (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 96

- (Exam Topic 2)

An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware, the attacker is provided with access to the infected machine.

Which of the following is being described?

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

**Answer:** A

#### NEW QUESTION 101

- (Exam Topic 2)

Before an infection was detected, several of the infected devices attempted to access a URL that was similar to the company name but with two letters transposed.

Which of the following BEST describes the attack vector used to infect the devices?

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

**Answer:** C

#### NEW QUESTION 103

- (Exam Topic 2)

A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account. This is an example of which of the following attacks?

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

**Answer:** C

#### NEW QUESTION 104

- (Exam Topic 2)

An in-house penetration tester is using a packet capture device to listen in on network communications. This is an example of:

- A. Passive reconnaissance
- B. Persistence
- C. Escalation of privileges
- D. Exploiting the switch

**Answer:** D

#### NEW QUESTION 108

- (Exam Topic 2)

Which of the following are methods to implement HA in a web application server environment? (Select two.)

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

**Answer:** AB

#### NEW QUESTION 109

- (Exam Topic 2)

A security analyst is performing a quantitative risk analysis. The risk analysis should show the potential monetary loss each time a threat or event occurs. Given this requirement, which of the following concepts would assist the analyst in determining this value? (Select two.)

- A. ALE
- B. AV
- C. ARO
- D. EF

E. ROI

**Answer:** BD

**NEW QUESTION 114**

- (Exam Topic 2)

A development team has adopted a new approach to projects in which feedback is iterative and multiple iterations of deployments are provided within an application's full life cycle. Which of the following software development methodologies is the development team using?

- A. Waterfall
- B. Agile
- C. Rapid
- D. Extreme

**Answer:** B

**NEW QUESTION 116**

- (Exam Topic 2)

Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures.

Which of the following should be implemented to correct this issue?

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

**Answer:** B

**NEW QUESTION 118**

- (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 from the vendor. Which of the following BEST describes the reason why the vulnerability exists?

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

**Answer:** B

**NEW QUESTION 123**

- (Exam Topic 2)

A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable.

Which of the following MUST be implemented to support this requirement?

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

**Answer:** C

**NEW QUESTION 127**

- (Exam Topic 2)

Which of the following cryptographic algorithms is irreversible?

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

**Answer:** B

**NEW QUESTION 128**

- (Exam Topic 2)

A manager suspects that an IT employee with elevated database access may be knowingly modifying financial transactions for the benefit of a competitor. Which of the following practices should the manager implement to validate the concern?

- A. Separation of duties
- B. Mandatory vacations
- C. Background checks
- D. Security awareness training

**Answer:** A

#### NEW QUESTION 130

- (Exam Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 132

- (Exam Topic 2)

A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts.

Which of the following subnets would BEST meet the requirements?

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

**Answer: B**

#### NEW QUESTION 136

- (Exam Topic 2)

A Chief Information Officer (CIO) drafts an agreement between the organization and its employees. The agreement outlines ramifications for releasing information without consent and/or approvals. Which of the following BEST describes this type of agreement?

- A. ISA
- B. NDA
- C. MOU
- D. SLA

**Answer: B**

#### NEW QUESTION 139

- (Exam Topic 2)

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

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

**Answer: B**

#### NEW QUESTION 143

- (Exam Topic 2)

A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting without the knowledge of the user. Which of the following mobile device capabilities should the user disable to achieve the stated goal?

- A. Device access control
- B. Location based services
- C. Application control
- D. GEO-Tagging

**Answer: D**

#### NEW QUESTION 148

- (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 151

- (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 152

- (Exam Topic 2)

A company's AUP requires:

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

An auditor is reviewing the following report:

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

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

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

**Answer:** C

#### NEW QUESTION 155

- (Exam Topic 2)

A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients. Which of the following is being used?

- A. Gray box vulnerability testing
- B. Passive scan
- C. Credentialed scan
- D. Bypassing security controls

**Answer:** A

#### NEW QUESTION 160

- (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 165

- (Exam Topic 2)

A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network.

Which of the following security measures did the technician MOST likely implement to cause this Scenario?

- A. Deactivation of SSID broadcast
- B. Reduction of WAP signal output power
- C. Activation of 802.1X with RADIUS
- D. Implementation of MAC filtering
- E. Beacon interval was decreased



**Answer:** A

**NEW QUESTION 167**

- (Exam Topic 2)

An administrator has concerns regarding the traveling sales team who works primarily from smart phones. Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

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

**Answer:** B

**NEW QUESTION 169**

- (Exam Topic 2)

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

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

**Answer:** AE

**NEW QUESTION 171**

- (Exam Topic 2)

A network technician is setting up a segmented network that will utilize a separate ISP to provide wireless access to the public area for a company. Which of the following wireless security methods should the technician implement to provide basic accountability for access to the public network?

- A. Pre-shared key
- B. Enterprise
- C. Wi-Fi Protected setup
- D. Captive portal

**Answer:** D

**NEW QUESTION 174**

- (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 178**

- (Exam Topic 2)

Company policy requires the use of passphrases instead of 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 181**

- (Exam Topic 2)

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

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

**Answer: C**

#### **NEW QUESTION 185**

- (Exam Topic 2)

Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field.

Which of the following has the application programmer failed to implement?

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

**Answer: C**

#### **NEW QUESTION 186**

- (Exam Topic 2)

As part of the SDLC, a third party is hired to perform a penetration test. The third party will have access to the source code, integration tests, and network diagrams. Which of the following BEST describes the assessment being performed?

- A. Black box
- B. Regression
- C. White box
- D. Fuzzing

**Answer: C**

#### **NEW QUESTION 191**

- (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 193**

- (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 196**

- (Exam Topic 3)

A security team wants to establish an Incident Response plan. The team has never experienced an incident. Which of the following would BEST help them establish plans and procedures?

- A. Table top exercises
- B. Lessons learned
- C. Escalation procedures
- D. Recovery procedures

**Answer: A**

#### **NEW QUESTION 201**

- (Exam Topic 3)

An organization is moving its human resources system to a cloud services provider.

The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords. Which of the following options meets all of these requirements?

- A. Two-factor authentication
- B. Account and password synchronization

- C. Smartcards with PINS
- D. Federated authentication

**Answer:** D

#### NEW QUESTION 204

- (Exam Topic 3)

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

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

**Answer:** C

#### NEW QUESTION 206

- (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 207

- (Exam Topic 3)

A security administrator has been asked to implement a VPN that will support remote access over IPSEC. Which of the following is an encryption algorithm that would meet this requirement?

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

**Answer:** B

#### NEW QUESTION 210

- (Exam Topic 3)

An employee uses RDP to connect back to the office network. If RDP is misconfigured, which of the following security exposures would this lead to?

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

**Answer:** D

#### NEW QUESTION 213

- (Exam Topic 3)

A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes.

Which of the following risk management strategies BEST describes management's response?

- A. Deterrence
- B. Mitigation
- C. Avoidance
- D. Acceptance

**Answer:** C

#### NEW QUESTION 216

- (Exam Topic 3)

The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next 10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.

Which of the following categories BEST describes what she is looking for?

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

**Answer:** D

#### NEW QUESTION 218

- (Exam Topic 3)

Anne, the Chief Executive Officer (CEO), has reported that she is getting multiple telephone calls from someone claiming to be from the helpdesk. The caller is asking to verify her network authentication credentials because her computer is broadcasting across the network. This is MOST likely which of the following types of attacks?

- A. Vishing
- B. Impersonation
- C. Spim
- D. Scareware

**Answer:** A

#### NEW QUESTION 221

- (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 225

- (Exam Topic 3)

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

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

**Answer:** D

#### NEW QUESTION 227

- (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 231

- (Exam Topic 3)

Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

- A. MOU
- B. ISA
- C. BPA
- D. SLA

**Answer:** D

#### NEW QUESTION 232

- (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 233

- (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 238

- (Exam Topic 3)

A Security Officer on a military base needs to encrypt several smart phones that will be going into the field. Which of the following encryption solutions should be deployed in this situation?

- A. Elliptic curve
- B. One-time pad
- C. 3DES
- D. AES-256

**Answer:** D

#### NEW QUESTION 243

- (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 248

- (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 252

- (Exam Topic 3)

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

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

**Answer:** B

#### NEW QUESTION 253

- (Exam Topic 3)

Which of the following use the SSH protocol?

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

**Answer:** BF

#### NEW QUESTION 254

- (Exam Topic 3)

An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient.

Which of the following capabilities would be MOST appropriate to consider implementing in response to the new requirement?

- A. Transitive trust
- B. Symmetric encryption
- C. Two-factor authentication
- D. Digital signatures
- E. One-time passwords

**Answer:** D

#### NEW QUESTION 259

- (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 Q for 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 261

- (Exam Topic 3)

Which of the following is the GREATEST risk to a company by allowing employees to physically bring their personal smartphones to work?

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

**Answer:** A

#### NEW QUESTION 264

- (Exam Topic 3)

A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN. Which of the following protocols should be used?

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

**Answer:** A

#### NEW QUESTION 268

- (Exam Topic 3)

An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection. Which of the following AES modes of operation would meet this integrity-only requirement?

- A. HMAC
- B. PCBC
- C. CBC
- D. GCM
- E. CFB

**Answer:** A

#### NEW QUESTION 269

- (Exam Topic 3)

A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability. In order to prevent similar situations in the future, the company should improve which of the following?

- A. Change management procedures
- B. Job rotation policies
- C. Incident response management
- D. Least privilege access controls

**Answer:** A

#### NEW QUESTION 273

- (Exam Topic 3)

New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority. In case of a fire where electricity is

cut, which of the following should be taken into consideration when installing the new locks?

- A. Fail safe
- B. Fault tolerance
- C. Fail secure
- D. Redundancy

**Answer:** A

#### NEW QUESTION 275

- (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 administrator 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 276

- (Exam Topic 3)

A network operations manager has added a second row of server racks in the datacenter. These racks face the opposite direction of the first row of racks. Which of the following is the reason the manager installed the racks this way?

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

**Answer:** B

#### NEW QUESTION 280

- (Exam Topic 3)

Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

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

**Answer:** A

#### NEW QUESTION 284

- (Exam Topic 3)

Having adequate lighting on the outside of a building is an example of which of the following security controls?

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

**Answer:** A

#### NEW QUESTION 286

- (Exam Topic 4)

An incident involving a workstation that is potentially infected with a virus has occurred. The workstation may have sent confidential data to an unknown internet server. Which of the following should a security analyst do FIRST?

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

**Answer:** A

#### NEW QUESTION 287

- (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 288**

- (Exam Topic 4)

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

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

**Answer:** C

**NEW QUESTION 292**

- (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 from 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 294**

- (Exam Topic 4)

Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

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

**Answer:** C

**NEW QUESTION 297**

- (Exam Topic 4)

A security analyst has set up a network tap to monitor network traffic for vulnerabilities. Which of the following techniques would BEST describe the approach the analyst has taken?

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

**Answer:** D

**NEW QUESTION 301**

- (Exam Topic 4)

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

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

**Answer:** AE

**NEW QUESTION 303**

- (Exam Topic 4)

A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated. Which of the following options will provide the best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

- A. Put the VoIP network into a different VLAN than the existing data network.
- B. Upgrade the edge switches from 10/100/1000 to improve network speed
- C. Physically separate the VoIP phones from the data network
- D. Implement flood guards on the data network



**Answer:** A

**NEW QUESTION 304**

- (Exam Topic 4)

A user needs to send sensitive information to a colleague using PKI. Which of the following concepts apply when a sender encrypts the message hash with the sender's private key? (Select TWO)

- A. Non-repudiation
- B. Email content encryption
- C. Steganography
- D. Transport security
- E. Message integrity

**Answer:** AE

**NEW QUESTION 307**

- (Exam Topic 4)

A penetration tester harvests potential usernames from a social networking site. The penetration tester then uses social engineering to attempt to obtain associated passwords to gain unauthorized access to shares on a network server.

Which of the following methods is the penetration tester MOST likely using?

- A. Escalation of privilege
- B. SQL injection
- C. Active reconnaissance
- D. Proxy server

**Answer:** C

**NEW QUESTION 308**

- (Exam Topic 4)

A network technician is trying to determine the source of an ongoing network based attack. Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?

- A. Proxy
- B. Protocol analyzer
- C. Switch
- D. Firewall

**Answer:** B

**NEW QUESTION 312**

- (Exam Topic 4)

A security analyst is working on a project that requires the implementation of a stream cipher. Which of the following should the analyst use?

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

**Answer:** C

**NEW QUESTION 313**

- (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 316**

- (Exam Topic 4)

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

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

**Answer:** D

#### NEW QUESTION 320

- (Exam Topic 4)

When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

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

**Answer:** B

#### NEW QUESTION 321

- (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 322

- (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 325

- (Exam Topic 4)

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

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

**Answer:** AD

#### NEW QUESTION 328

- (Exam Topic 4)

As part of a new BYOD rollout, a security analyst has been asked to find a way to securely store company data on personal devices. Which of the following would BEST help to accomplish this?

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

**Answer:** B

#### NEW QUESTION 332

- (Exam Topic 4)

Which of the following allows an auditor to test proprietary-software compiled code for security flaws?

- A. Fuzzing
- B. Static review
- C. Code signing
- D. Regression testing

**Answer:** A

#### NEW QUESTION 334

- (Exam Topic 4)

A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network. The access the

server using RDP on a port other than the typical registered port for the RDP protocol?

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

**Answer:** A

#### NEW QUESTION 337

- (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 338

- (Exam Topic 4)

After a security incident, management is meeting with involved employees to document the incident and its aftermath. Which of the following BEST describes this phase of the incident response process?

- A. Lessons learned
- B. Recovery
- C. Identification
- D. Preparation

**Answer:** A

#### NEW QUESTION 343

- (Exam Topic 4)

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

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

**Answer:** DE

#### NEW QUESTION 346

- (Exam Topic 4)

An attack that is using interference as its main attack to impede network traffic is which of the following?

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

**Answer:** C

#### NEW QUESTION 350

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 352

- (Exam Topic 4)

Ann, a user, states that her machine has been behaving erratically over the past week. She has experienced slowness and input lag and found text files that appear to contain pieces of her emails or online conversations with coworkers. The technician runs a standard virus scan but detects nothing. Which of the

following types of malware has infected the machine?

- A. Ransomware
- B. Rootkit
- C. Backdoor
- D. Keylogger

**Answer:** D

#### NEW QUESTION 354

- (Exam Topic 4)

Which of the following could occur when both strong and weak ciphers are configured on a VPN concentrator? (Select TWO)

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

**Answer:** AE

#### NEW QUESTION 356

- (Exam Topic 4)

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

- A. Disable the compromised accounts
- B. Update WAF rules to block social networks
- C. Remove the compromised accounts with all AD groups
- D. Change the compromised accounts' passwords
- E. Disable the open relay on the email server
- F. Enable sender policy framework

**Answer:** EF

#### Explanation:

Sender Policy Framework (SPF) is a simple email-validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain comes from a host authorized by that domain's administrators. In a Small Business Server environment, you may have to prevent your Microsoft Exchange Server-based server from being used as an open relay SMTP server for unsolicited commercial e-mail messages, or spam.

You may also have to clean up the Exchange server's SMTP queues to delete the unsolicited commercial email messages.

If your Exchange server is being used as an open SMTP relay, you may experience one or more of the following symptoms:

The Exchange server cannot deliver outbound SMTP mail to a growing list of e-mail domains. Internet browsing is slow from the server and from local area network (LAN) clients.

Free disk space on the Exchange server in the location of the Exchange information store databases or the Exchange information store transaction logs is reduced more rapidly than you expect.

The Microsoft Exchange information store databases spontaneously dismount. You may be able to manually mount the stores by using Exchange System Manager, but the stores may dismount on their own after they run for a short time. For more information, click the following article number to view the article in the Microsoft Knowledge Base.

#### NEW QUESTION 357

- (Exam Topic 4)

Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

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

**Answer:** D

#### NEW QUESTION 362

- (Exam Topic 4)

Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

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

**Answer:** D

#### NEW QUESTION 366

- (Exam Topic 4)

A security analyst is investigating a security breach. Upon inspection of the audit and 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 368

- (Exam Topic 4)

The administrator installs database software to encrypt each field as it is written to disk. Which of the following describes the encrypted data?

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

**Answer:** B

#### NEW QUESTION 369

- (Exam Topic 4)

A vice president at a manufacturing organization is concerned about desktops being connected to the network. Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?

- A. Put the desktops in the DMZ.
- B. Create a separate VLAN for the desktops.
- C. Air gap the desktops.
- D. Join the desktops to an ad-hoc network.

**Answer:** C

#### NEW QUESTION 370

- (Exam Topic 4)

An external contractor, who has not been given information about the software or network architecture, is conducting a penetration test. Which of the following BEST describes the test being performed?

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

**Answer:** A

#### NEW QUESTION 375

- (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 380

- (Exam Topic 4)

A network administrator adds an ACL to allow only HTTPS connections from 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 192.168.2.3 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 381

- (Exam Topic 4)

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

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

**Answer:** B

#### NEW QUESTION 383

- (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 386

- (Exam Topic 5)

Which of the following metrics are used to calculate the SLE? (Select TWO)

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

**Answer:** BC

#### NEW QUESTION 388

- (Exam Topic 5)

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

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

**Answer:** D

#### NEW QUESTION 389

- (Exam Topic 5)

When sending messages using symmetric encryption, which of the following must happen FIRST?

- A. Exchange encryption key
- B. Establish digital signatures
- C. Agree on an encryption method
- D. Install digital certificates

**Answer:** C

#### NEW QUESTION 392

- (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 395

- (Exam Topic 5)

A technician is configuring a load balancer for the application team to accelerate the network performance of their applications. The applications are hosted on multiple servers and must be redundant. Given this scenario, which of the following would be the BEST method of configuring the load balancer?

- A. Round-robin
- B. Weighted
- C. Least connection
- D. Locality-based

**Answer:** D

#### NEW QUESTION 398

- (Exam Topic 5)

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

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

**Answer:** B

#### NEW QUESTION 401

- (Exam Topic 5)

Ann, a user, reports she is unable to access an application from her desktop. A security analyst verifies Ann's access and checks the SIEM for any errors. The security analyst reviews the log file from Ann's system and notices the following output:

```
2017--08-21 10:48:12 DROPTCP 172.20.89.232 239.255.255.255 443
1900 250 ----- RECEIVE 2017--08-21 10:48:12 DROPUDP
192.168.72.205 239.255.255.255 443 1900 250 ----- RECEIVE
```

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

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

E. Network-based firewall

**Answer: C**

#### NEW QUESTION 402

- (Exam Topic 5)

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

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

**Answer: D**

#### NEW QUESTION 403

- (Exam Topic 5)

A hacker has a packet capture that contains:

```
....Joe Smith.....E289F21CD33E4F57890DDEA5CF267ED2..  
....Jane.Doe.....AD1FAB10D33E4F57890DDEA5CF267ED2..  
....John.Key.....3374E9E7E33E4F57890DDEA5CF267ED2..
```

Which of the following tools will the hacker use against this type of capture?

- A. Password cracker
- B. Vulnerability scanner
- C. DLP scanner
- D. Fuzzer

**Answer: A**

#### NEW QUESTION 408

- (Exam Topic 5)

Two users must encrypt and transmit large amounts of data between them. Which of the following should they use to encrypt and transmit the data?

- A. Symmetric algorithm
- B. Hash function
- C. Digital signature
- D. Obfuscation

**Answer: A**

#### NEW QUESTION 411

- (Exam Topic 5)

Which of the following is the BEST reason to run an untested application in a sandbox?

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

**Answer: C**

#### NEW QUESTION 414

- (Exam Topic 5)

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

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

**Answer: C**

#### NEW QUESTION 416

- (Exam Topic 5)

A security architect has convened a meeting to discuss an organization's key management policy. The organization has a reliable internal key management system, and some argue that it would be best to manage the cryptographic keys internally as opposed to using a solution from a third party. The company should use:

- A. the current internal key management system.
- B. a third-party key management system that will reduce operating costs.
- C. risk benefits analysis results to make a determination.
- D. a software solution including secure key escrow capabilities.

**Answer:** C

**NEW QUESTION 420**

- (Exam Topic 5)

Which of the following types of penetration test will allow the tester to have access only to password hashes prior to the penetration test?

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

**Answer:** B

**NEW QUESTION 424**

- (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 427**

- (Exam Topic 5)

A security analyst is inspecting the results of a recent internal vulnerability scan that was performed against intranet services. The scan reports include the following critical-rated vulnerability:

Title: Remote Command Execution vulnerability in web server Rating: Critical (CVSS 10.0) Threat actor: any remote user of the web server

Confidence: certain

Recommendation: apply vendor patches

Which of the following actions should the security analyst perform FIRST?

- A. Escalate the issue to senior management.
- B. Apply organizational context to the risk rating.
- C. Organize for urgent out-of-cycle patching.
- D. Exploit the server to check whether it is a false positive.

**Answer:** B

**NEW QUESTION 430**

- (Exam Topic 5)

A user typically works remotely over the holidays using a web-based VPN to access corporate resources. The user reports getting untrusted host errors and being unable to connect. Which of the following is MOST likely the case?

- A. The certificate has expired
- B. The browser does not support SSL
- C. The user's account is locked out
- D. The VPN software has reached the seat license maximum

**Answer:** A

**NEW QUESTION 431**

- (Exam Topic 5)

A company is allowing a BYOD policy for its staff. Which of the following is a best practice that can decrease the risk of users jailbreaking mobile devices?

- A. Install a corporately monitored mobile antivirus on the devices.
- B. Prevent the installation of applications from a third-party application store.
- C. Build a custom ROM that can prevent jailbreaking.
- D. Require applications to be digitally signed.

**Answer:** D

**NEW QUESTION 432**

- (Exam Topic 5)

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

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

**Answer:** D



#### NEW QUESTION 437

- (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 440

- (Exam Topic 5)

An organization has several production-critical SCADA supervisory systems that cannot follow the normal 30-day patching policy. Which of the following BEST maximizes the protection of these systems from malicious software?

- A. Configure a firewall with deep packet inspection that restricts traffic to the systems.
- B. Configure a separate zone for the systems and restrict access to known ports.
- C. Configure the systems to ensure only necessary applications are able to run.
- D. Configure the host firewall to ensure only the necessary applications have listening ports

**Answer:** A

#### NEW QUESTION 444

- (Exam Topic 5)

A security engineer must install the same x.509 certificate on three different servers. The client application that connects to the server performs a check to ensure the certificate matches the host name. Which of the following should the security engineer use?

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

**Answer:** D

#### **Explanation:**

SAN = Subject Alternate Names

#### NEW QUESTION 449

- (Exam Topic 5)

A stock trading company had the budget for enhancing its secondary datacenter approved. Since the main site is a hurricane-affected area and the disaster recovery site is 100 mi (161 km) away, the company wants to ensure its business is always operational with the least amount of man hours needed. Which of the following types of disaster recovery sites should the company implement?

- A. Hot site
- B. Warm site
- C. Cold site
- D. Cloud-based site

**Answer:** D

#### NEW QUESTION 452

- (Exam Topic 5)

When attackers use a compromised host as a platform for launching attacks deeper into a company's network, it is said that they are:

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

**Answer:** D

#### NEW QUESTION 456

- (Exam Topic 5)

Due to regulatory requirements, server in a global organization must use time synchronization. Which of the following represents the MOST secure method of time synchronization?

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

**Answer:** B

#### NEW QUESTION 457



- (Exam Topic 5)

Which of the following threats has sufficient knowledge to cause the MOST danger to an organization?

- A. Competitors
- B. Insiders
- C. Hacktivists
- D. Script kiddies

**Answer: B**

#### NEW QUESTION 460

- (Exam Topic 5)

A cybersecurity analyst is looking into the payload of a random packet capture file that was selected for analysis. The analyst notices that an internal host had a socket established with another internal host over a non-standard port.

Upon investigation, the origin host that initiated the socket shows this output:

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

```
tracert 8.8.8.8
```

```
taskkill /pid 9487
```

```
usera@host>
```

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

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

**Answer: C**

#### NEW QUESTION 464

- (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 465

- (Exam Topic 5)

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

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

**Answer: A**

#### NEW QUESTION 467

- (Exam Topic 5)

Which of the following should a security analyst perform FIRST to determine the vulnerabilities of a legacy system?

- A. Passive scan
- B. Aggressive scan
- C. Credentialed scan
- D. Intrusive scan

**Answer: A**

#### NEW QUESTION 470

- (Exam Topic 5)

Which of the following is the proper order for logging a user into a system from the first step to the last step?

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

**Answer:** A

#### NEW QUESTION 475

- (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 478

- (Exam Topic 5)

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

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

**Answer:** CD

#### NEW QUESTION 481

- (Exam Topic 5)

After attempting to harden a web server, a security analyst needs to determine if an application remains vulnerable to SQL injection attacks. Which of the following would BEST assist the analyst in making this determination?

- A. tracer
- B. Fuzzer
- C. nslookup
- D. Nmap
- E. netcat

**Answer:** B

#### NEW QUESTION 485

- (Exam Topic 5)

Ann is the IS manager for several new systems in which the classification of the systems' data are being decided. She is trying to determine the sensitivity level of the data being processed. Which of the following people should she consult to determine the data classification?

- A. Steward
- B. Custodian
- C. User
- D. Owner

**Answer:** D

#### NEW QUESTION 490

- (Exam Topic 5)

A systems administrator is configuring a system that uses data classification labels.

Which of the following will the administrator need to implement to enforce access control?

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

**Answer:** B

#### NEW QUESTION 492

- (Exam Topic 5)

A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFlenabled 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 493

- (Exam Topic 5)

Which of the following is an asymmetric function that generates a new and separate key every time it runs?

- A. RSA
- B. DSA
- C. DHE
- D. HMAC
- E. PBKDF2

**Answer:** C

#### NEW QUESTION 498

- (Exam Topic 5)

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

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

**Answer:** CE

#### NEW QUESTION 500

- (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 503

- (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 505

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### SY0-501 Practice Exam Features:

- \* SY0-501 Questions and Answers Updated Frequently
- \* SY0-501 Practice Questions Verified by Expert Senior Certified Staff
- \* SY0-501 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SY0-501 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SY0-501 Practice Test Here](#)**