Exam Questions SY0-501

CompTIA Security+ Certification Exam

https://www.2passeasy.com/dumps/SY0-501/

NEW QUESTION 1
- (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 2
- (Exam Topic 1)
Which of the following best describes routine in which semicolons, dashes, quotes, and commas are removed from a string?

A. Error handling to protect against program exploitation
B. Exception handling to protect against XSRF attacks.
C. Input validation to protect against SQL injection.
D. Padding to protect against string buffer overflows.

Answer: C

NEW QUESTION 3
- (Exam Topic 1)
After a user reports stow 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
TCP   0.0.0.0:135       0.0.0.0:0               LISTENING       RpcSs [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 *.*                                     SSDPSVR
```

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 4
- (Exam Topic 1)
A company's user lockout policy is enabled after five unsuccessful login attempts. The help desk notices a user is repeatedly locked out over the course of a workweek. Upon contacting the user, the help desk discovers the user is on vacation and does not have network access. Which of the following types of attacks are MOST likely occurring? (Select two.)

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

Answer: CE

NEW QUESTION 5
- (Exam Topic 1)
Multiple employees receive an email with a malicious attachment that begins to encrypt their hard drives and mapped shares on their devices when it is opened.
The network and security teams perform the following actions:

- Shut down all network shares.
- Run an email search identifying all employees who received the malicious message.
- Reimage all devices belonging to users who opened the attachment.

Next, the teams want to re-enable the network shares. Which of the following BEST describes this phase of the incident response process?

A. Eradication
B. Containment
C. Recovery

D. Lessons learned

Answer: C

NEW QUESTION 6
- (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 7
- (Exam Topic 1)
An organization has determined it can tolerate a maximum of three hours of downtime. Which of the following has been specified?

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

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:

- There is no standardization.
- Employees ask for reimbursement for their devices.
- Employees do not replace their devices often enough to keep them running efficiently.
- The company does not have enough control over the devices.

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

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

Answer: D

NEW QUESTION 9
- (Exam Topic 1)
Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone. Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Select two.)

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

Answer: BE

NEW QUESTION 10
- (Exam Topic 1)
A senior incident response manager receives a call about some external IPs communicating with internal computers during off hours. Which of the following types of malware is MOST likely causing this issue?

A. Botnet
B. Ransomware
C. Polymorphic malware
D. Armored virus

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 13
- (Exam Topic 1)
A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees.
Which of the following would provide strong security and backward compatibility when accessing the wireless network?

A. Open wireless network and SSL VPN
B. WPA using a preshared key
C. WPA2 using a RADIUS back-end for 802.1x authentication
D. WEP with a 40-bit key

Answer: C

NEW QUESTION 16
- (Exam Topic 1)
A database backup schedule consists of weekly full backups performed on Saturday at 12:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?

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

Answer: B

NEW QUESTION 20
- (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 22
- (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 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 28
- (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 30
- (Exam Topic 1)
A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select two.)

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

Answer: AD

NEW QUESTION 33
- (Exam Topic 1)
An employer requires that employees use a key-generating app on their smartphones to log into corporate applications. In terms of authentication of an individual, this type of access policy is BEST defined as:

A. Something you have.
B. Something you know.
C. Something you do.
D. Something you are.

Answer: A

NEW QUESTION 34
- (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 38
- (Exam Topic 1)
A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.

Hostname	IP address	MAC	MAC filter
DadPC	192.168.1.10	00:1D:1A:44:17:B5	On
MomPC	192.168.1.15	21:13:D6:C5:42:A2	Off
JuniorPC	192.168.2.16	42:A7:D1:25:11:52	On
Unknown	192.168.1.18	10:B3:22:1A:FF:21	Off

Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

A. Apply MAC filtering and see if the router drops any of the systems.
B. Physically check each of the authorized systems to determine if they are logged onto the network.
C. Deny the “unknown” host because the hostname is not known and MAC filtering is not applied to this host.
D. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.

Answer: C

NEW QUESTION 40
- (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 43
- (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 46
- (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 50
- (Exam Topic 2)
A technician suspects that a system has been compromised. The technician reviews the following log entry: WARNING- hash mismatch: C:\Window\SysWOW64\user32.dll
WARNING- hash mismatch: C:\Window\SysWOW64\kernel32.dll
Based solely ono the above information, which of the following types of malware is MOST likely installed on the system?

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

Answer: A

NEW QUESTION 53
- (Exam Topic 2)
A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a
brute force attack on all accounts that has been previously logged into that machine.
Which of the following can be implemented to reduce the likelihood of this attack going undetected?

A. Password complexity rules
B. Continuous monitoring

C. User access reviews
D. Account lockout policies

Answer: B

NEW QUESTION 55
- (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. Baselining
D. Waterfalling

Answer: B

NEW QUESTION 58
- (Exam Topic 2)
During a monthly vulnerability scan, a server was flagged for being vulnerable to an Apache Struts exploit. Upon further investigation, the developer responsible for the server informs the security team that Apache Struts is not installed on the server. Which of the following BEST describes how the security team should reach to this incident?

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

Answer: A

NEW QUESTION 61
- (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 62
- (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 67
- (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 71
- (Exam Topic 2)
Which of the following are methods to implement HA in a web application server environment? (Select two.)

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

Answer: AB

NEW QUESTION 73
- (Exam Topic 2)
To reduce disk consumption, an organization's legal department has recently approved a new policy setting the data retention period for sent email at six months. Which of the following is the BEST way to ensure this
goal is met?

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

Answer: A

NEW QUESTION 78
- (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 80
- (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 83
- (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 85
- (Exam Topic 2)
A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another. Which of the following should the security administrator do to rectify this issue?

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

Answer: B

NEW QUESTION 89
- (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 90
- (Exam Topic 2)
AChief Executive Officer (CEO) suspects someone in the lab testing environment is stealing confidential information after working hours when no one else is around. Which of the following actions can help to prevent this specific threat?

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

Answer: D

NEW QUESTION 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 99
- (Exam Topic 2)
AChief Information Officer (CIO) drafts an agreement between the organization and its employees. The agreement outlines ramifications for releasing information without consent and/or approvals. Which of the following BEST describes this type of agreement?

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

Answer: B

NEW QUESTION 100
- (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 103
- (Exam Topic 2)
A user of the wireless network is unable to gain access to the network. The symptoms are:
1.) Unable to connect to both internal and Internet resources
2.) The wireless icon shows connectivity but has no network access
The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate.
Which of the following is the MOST likely cause of the connectivity issues?

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

Answer: A

NEW QUESTION 104
- (Exam Topic 2)
A group of non-profit agencies wants to implement a cloud service to share resources with each other and minimize costs. Which of the following cloud deployment models BEST describes this type of effort?

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

Answer: C

NEW QUESTION 106
- (Exam Topic 2)
A user is presented with the following items during the new-hire onboarding process:
-Laptop
-Secure USB drive
-Hardware OTP token
-External high-capacity HDD
-Password complexity policy
-Acceptable use policy
-HASP key
-Cable lock
Which of the following is one component of multifactor authentication?

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

Answer: C

NEW QUESTION 109
- (Exam Topic 2)
As part of the SDLC, a third party is hired to perform a penetration test. The third party will have access to the source code, integration tests, and network diagrams. Which of the following BEST describes the assessment being performed?

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

Answer: C

NEW QUESTION 114
- (Exam Topic 3)
Phishing emails frequently take advantage of high-profile catastrophes reported in the news. Which of the following principles BEST describes the weakness being exploited?

A. Intimidation
B. Scarcity
C. Authority
D. Social proof

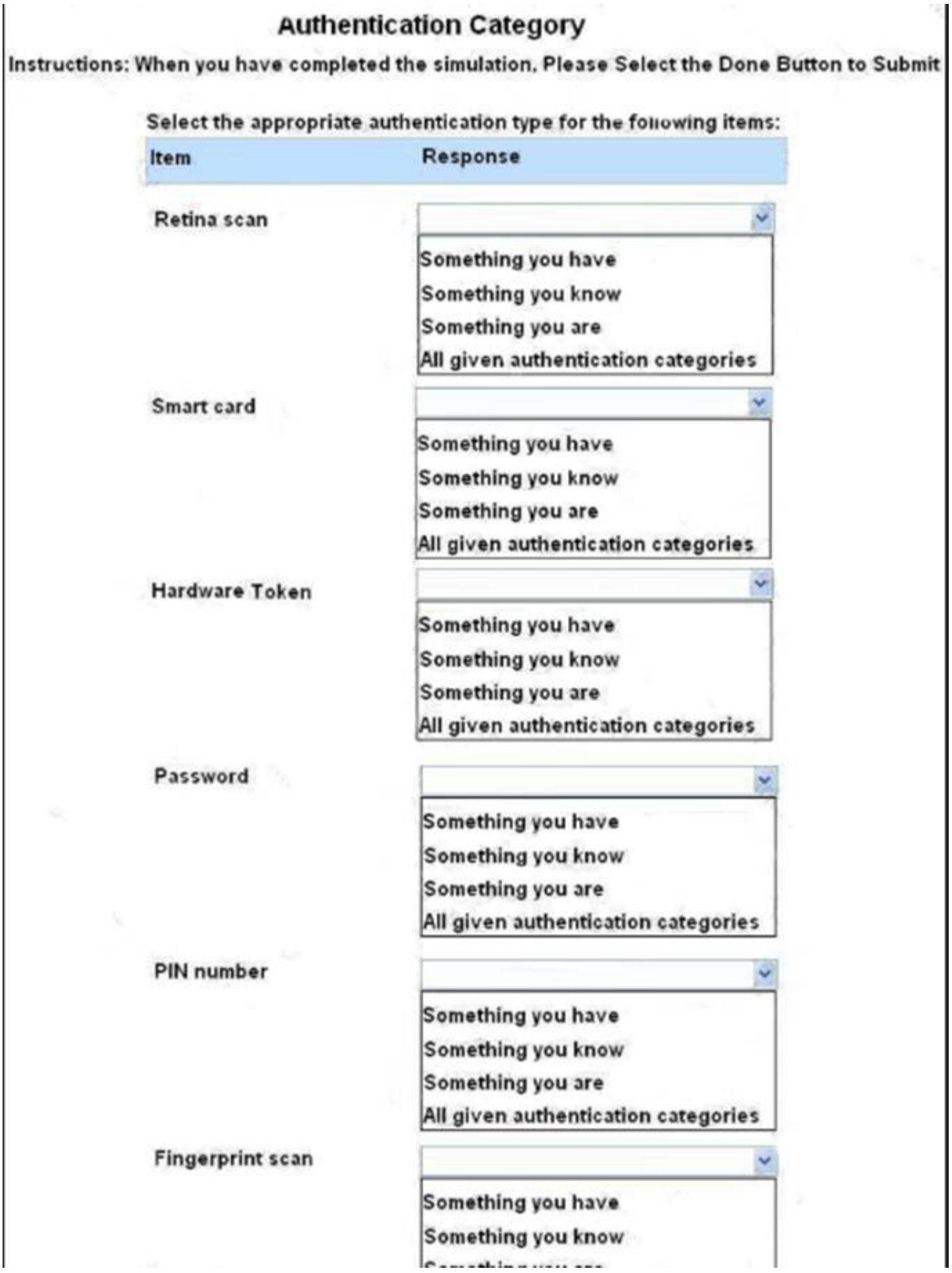
Answer: D

NEW QUESTION 118
- (Exam Topic 3)
A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

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

Answer: B

NEW QUESTION 121
- (Exam Topic 3)
For each of the given items, select the appropriate authentication category from the dropdown choices. Instructions: When you have completed the simulation, please select the Done button to submit.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Something you are includes fingerprints, retina scans, or voice recognition. Something you have includes smart cards, token devices, or keys.
Something you know includes a password, codes, PINs, combinations, or secret phrases. Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.
Something you do includes your typing rhythm, a secret handshake, or a private knock
http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle http://en.wikipedia.org/wiki/Smart_card#Security

NEW QUESTION 122
- (Exam Topic 3)
A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources. Which of the following should be implemented?

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

Answer: B

NEW QUESTION 127
- (Exam Topic 3)
A security team wants to establish an Incident Response plan. The team has never experienced an incident. Which of the following would BEST help them establish plans and procedures?

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

Answer: A

NEW QUESTION 132
- (Exam Topic 3)
An organization is moving its human resources system to a cloud services provider.
The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords. Which of the following options meets all of these requirements?

A. Two-factor authentication
B. Account and password synchronization
C. Smartcards with PINS
D. Federated authentication

Answer: D

NEW QUESTION 137
- (Exam Topic 3)
A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

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

Answer: A

NEW QUESTION 141
- (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 143
- (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 147
- (Exam Topic 3)
Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys. Which of the following can be implemented to enable users to share encrypted data while abiding by company policies?

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

Answer: B

NEW QUESTION 152
- (Exam Topic 3)
A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations. Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)

A. SCP

B. TFTP
C. SNMP
D. FTP
E. SMTP
F. FTPS

Answer: AF

NEW QUESTION 156
- (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 160
- (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 164
- (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 169
- (Exam Topic 3)
Which of the following attack types is being carried out where a target is being sent unsolicited messages via Bluetooth?

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

Answer: B

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

NEW QUESTION 172
- (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 174

- (Exam Topic 3)
Which of the following use the SSH protocol?

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

Answer: BF

NEW QUESTION 175
- (Exam Topic 3)
During an application design, the development team specifics 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 176
- (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 180
- (Exam Topic 3)
A system administrator needs to implement 802.1x whereby when a user logs into the network, the authentication server communicates to the network switch and assigns the user to the proper VLAN. Which of the following protocols should be used?

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

Answer: A

NEW QUESTION 183
- (Exam Topic 3)
The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate severs at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?

A. Implement deduplication at the network level between the two locations
B. Implement deduplication on the storage array to reduce the amount of drive space needed
C. Implement deduplication on the server storage to reduce the data backed up
D. Implement deduplication on both the local and remote servers

Answer: B

NEW QUESTION 186
- (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 189
- (Exam Topic 3)
The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected. Which of the following is required to complete the certificate chain?

A. Certificate revocation list
B. Intermediate authority
C. Recovery agent
D. Root of trust

Answer: B

NEW QUESTION 194
- (Exam Topic 3)
Which of the following technologies would be MOST appropriate to utilize when testing a new software patch before a company-wide deployment?

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

Answer: B

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

NEW QUESTION 195
- (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 197
- (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 render.
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.

Public Cafe
Available Security Controls
128-bit key
64-bit key
Pre-share Key
PKI certificate
SSH Key
Pin Pad
Reset All
Save
Exit

Help Desk
Available Security Controls
Iris Scanner
Thumbprint Scanner
Password
Proximity Badge
Voice Recognition
Pin Pad
Reset All
Save
Exit

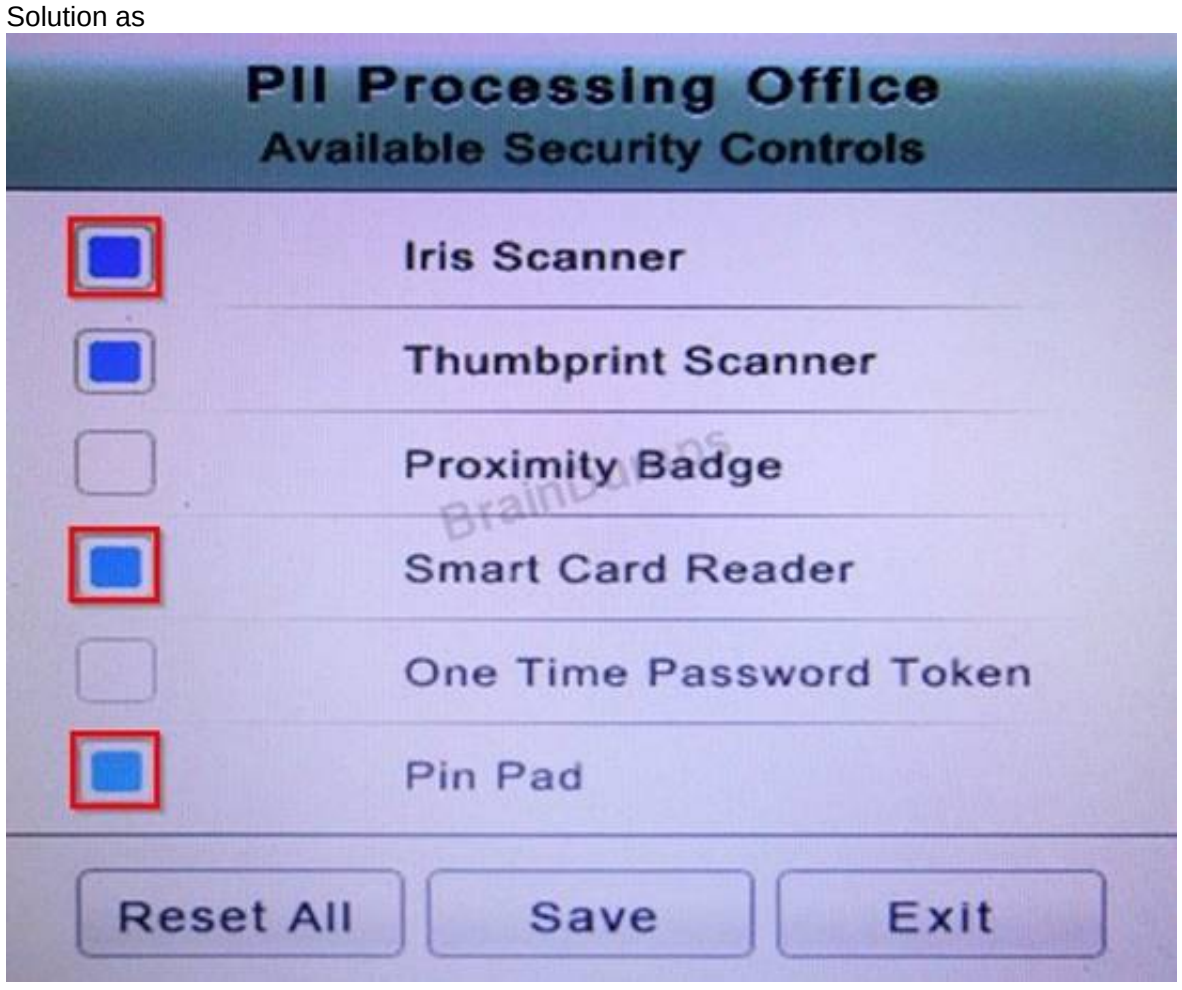
Data Center
Available Security Controls
Iris Scanner
Thumbprint Scanner
Mantrap
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Solution as



Public Cafe
Available Security Controls
128-bit key
64-bit key
Pre-share Key
PKI certificate
SSH Key
Pin Pad
Reset All
Save
Exit

Data Center
Available Security Controls
Iris Scanner
Thumbprint Scanner
Mantrap
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit

CEO's Office
Available Security Controls
Iris Scanner
Thumbprint Scanner
Username/Password
Smart Card Reader
Voice Recognition
Pin Pad
Reset All
Save
Exit

NEW QUESTION 199
- (Exam Topic 3)
Having adequate lighting on the outside of a building is an example of which of the following security controls?

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

Answer: A

NEW QUESTION 204
- (Exam Topic 4)
A datacenter manager has been asked to prioritize critical system recovery priorities. Which of the following is the MOST critical for immediate recovery?

A. Communications software
B. Operating system software
C. Weekly summary reports to management
D. Financial and production software

Answer: B

NEW QUESTION 207
- (Exam Topic 4)
To determine the ALE of a particular risk, which of the following must be calculated? (Select two.)

A. ARO
B. ROI
C. RPO
D. SLE
E. RTO

Answer: AD

NEW QUESTION 211
- (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 215
- (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 pro-vide 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 218
- (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 221
- (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 222
- (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 226
- (Exam Topic 4)
A security auditor is putting together a report for the Chief Executive Officer (CEO) on personnel security and its impact on the security posture of the whole organization. Which of the following would be the MOST important factor to consider when it comes to personnel security?

A. Insider threats
B. Privilege escalation
C. Hacktivist
D. Phishing through social media
E. Corporate espionage

Answer: A

NEW QUESTION 227
- (Exam Topic 4)
A company's loss control department identifies theft as a recurring loss type over the past year. Based on the department's report, the Chief Information Officer (CIO) wants to detect theft of datacenter equipment. Which of the following controls should be implemented?

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

Answer: C

NEW QUESTION 230
- (Exam Topic 4)
Which of the following BEST describes a network-based attack that can allow an attacker to take full control of a vulnerable host?

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

Answer: A

NEW QUESTION 235
- (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 238
- (Exam Topic 4)
A company recently replaced its unsecure email server with a cloud-based email and collaboration solution that is managed and insured by a third party. Which of

the following actions did the company take regarding risks related to its email and collaboration services?

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

Answer: A

NEW QUESTION 241
- (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 246
- (Exam Topic 4)
While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack. Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Select two)

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

Answer: AD

NEW QUESTION 250
- (Exam Topic 4)
A web developer improves client access to the company's REST API. Authentication needs to be tokenized but not expose the client's password. Which of the following methods would BEST meet the developer's requirements?

A. SAML
B. LDAP
C. OAuth
D. Shibboleth

Answer: A

NEW QUESTION 253
- (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 256
- (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 259
- (Exam Topic 4)
The administrator installs database software to encrypt each field as it is written to disk. Which of the following describes the encrypted data?

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

Answer: B

NEW QUESTION 260
- (Exam Topic 4)
A security engineer wants to implement a site-to-site VPN that will require SSL certificates for mutual authentication. Which of the following should the engineer implement if the design requires client MAC address to be visible across the tunnel?

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

Answer: D

NEW QUESTION 265
- (Exam Topic 4)
A third-party penetration testing company was able to successfully use an ARP cache poison technique to gain root access on a server. The tester successfully moved to another server that was not in the original network. Which of the following is the MOST likely method used to gain access to the other host?

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

Answer: B

NEW QUESTION 270
- (Exam Topic 4)
Which of the following penetration testing concepts is being used when an attacker uses public Internet databases to enumerate and learn more about a target?

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

Answer: A

NEW QUESTION 272
- (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 273
- (Exam Topic 4)
An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server. Which of the following will most likely fix the uploading issue for the users?

A. Create an ACL to allow the FTP service write access to user directories
B. Set the Boolean selinux value to allow FTP home directory uploads
C. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
D. Configure the FTP daemon to utilize PAM authentication pass through user permissions

Answer: A

NEW QUESTION 276
- (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 l 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 277
- (Exam Topic 5)
A help desk technician receives a phone call from an individual claiming to be an employee of the organization and requesting assistance to access a locked account. The help desk technician asks the individual to provide proof of identity before access can be granted. Which of the following types of attack is the caller performing?

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

Answer: C

NEW QUESTION 282
- (Exam Topic 5)
An organization's employees currently use three different sets of credentials to access multiple internal resources. Management wants to make this process less complex. Which of the following would be the BEST option to meet this goal?

A. Transitive trust
B. Single sign-on
C. Federation
D. Secure token

Answer: B

NEW QUESTION 284
- (Exam Topic 5)
A security administrator is reviewing the following PowerShell script referenced in the Task Scheduler on a database server:

```
$members = GetADGroupMemeber -Identity "Domain Admins" -Recursive | Select - ExpandProperty
name
if ($members -notcontains "JohnDoe"){
Remove-Item -path C:\Database -recurse -force
}
```

Which of the following did the security administrator discover?

A. Ransomeware
B. Backdoor
C. Logic bomb
D. Trojan

Answer: C

NEW QUESTION 288
- (Exam Topic 5)
An organization is expanding its network team. Currently, it has local accounts on all network devices, but with growth, it wants to move to centrally managed authentication. Which of the following are the BEST solutions for the organization? (Select TWO)

A. TACACS+
B. CHAP
C. LDAP
D. RADIUS
E. MSCHAPv2

Answer: AD

NEW QUESTION 293
- (Exam Topic 5)
A security analyst is reviewing patches on servers. One of the servers is reporting the following error message in the WSUS management console:
The computer has not reported status in 30 days.
Given this scenario, which of the following statements BEST represents the issue with the output above?

A. The computer in QUESTION NO: has not pulled the latest ACL policies for the firewall.
B. The computer in QUESTION NO: has not pulled the latest GPO policies from the management server.
C. The computer in QUESTION NO: has not pulled the latest antivirus definitions from the antivirus program.
D. The computer in QUESTION NO: has not pulled the latest application software updates.

Answer: D

NEW QUESTION 294
- (Exam Topic 5)
Which of the following would be considered multifactor authentication?

A. Hardware token and smart card

B. Voice recognition and retina scan
C. Strong password and fingerprint
D. PIN and security QUESTION NO:s

Answer: C

NEW QUESTION 299
- (Exam Topic 5)
An organization has implemented an IPSec VPN access for remote users. Which of the following IPSec modes would be the MOST secure for this organization to implement?

A. Tunnel mode
B. Transport mode
C. AH-only mode
D. ESP-only mode

Answer: A

Explanation:
In both ESP and AH cases with IPSec Transport mode, the IP header is exposed. The IP header is not exposed in IPSec Tunnel mode.

NEW QUESTION 303
- (Exam Topic 5)
A software developer is concerned about DLL hijacking in an application being written. Which of the following is the MOST viable mitigation measure of this type of attack?

A. The DLL of each application should be set individually
B. All calls to different DLLs should be hard-coded in the application
C. Access to DLLs from the Windows registry should be disabled
D. The affected DLLs should be renamed to avoid future hijacking

Answer: B

NEW QUESTION 307
- (Exam Topic 5)
A security administrator installed a new network scanner that identifies new host systems on the network. Which of the following did the security administrator install?

A. Vulnerability scanner
B. Network-based IDS
C. Rogue system detection
D. Configuration compliance scanner

Answer: C

NEW QUESTION 311
- (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 316
- (Exam Topic 5)
When it comes to cloud computing, if one of the requirements for a project is to have the most control over the systems in the cloud, which of the following is a service model that would be BEST suited for this goal?

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

Answer: A

NEW QUESTION 318
- (Exam Topic 5)
A penetration tester has written an application that performs a bit-by-bit XOR 0xFF operation on binaries prior to transmission over untrusted mediA. Which of the following BEST describes the action performed by this type of application?

A. Hashing
B. Key exchange

C. Encryption
D. Obfusication

Answer: D

NEW QUESTION 322
- (Exam Topic 5)
Due to regulatory requirements, server in a global organization must use time synchronization. Which of the following represents the MOST secure method of time synchronization?

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

Answer: B

NEW QUESTION 325
- (Exam Topic 5)
Which of the following is a deployment concept that can be used to ensure only the required OS access is exposed to software applications?

A. Staging environment
B. Sandboxing
C. Secure baseline
D. Trusted OS

Answer: B

NEW QUESTION 329
- (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 331
- (Exam Topic 5)
An incident response manager has started to gather all the facts related to a SIEM alert showing multiple systems may have been compromised.
The manager has gathered these facts:
The breach is currently indicated on six user PCs One service account is potentially compromised Executive management has been notified
In which of the following phases of the IRP is the manager currently working?

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

Answer: D

NEW QUESTION 332
- (Exam Topic 5)
Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter. Which of the following is being described?

A. Service level agreement
B. Memorandum of understanding
C. Business partner agreement
D. Interoperability agreement

Answer: A

NEW QUESTION 334
- (Exam Topic 5)
A company offers SaaS, maintaining all customers' credentials and authenticating locally. Many large customers have requested the company offer some form of federation with their existing authentication infrastructures. Which of the following would allow customers to manage authentication and authorizations from within their existing organizations?

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

Answer: A

NEW QUESTION 338
- (Exam Topic 5)
Which of the following is the proper order for logging a user into a system from the first step to the last step?

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

Answer: A

NEW QUESTION 342
- (Exam Topic 5)
Attackers have been using revoked certificates for MITM attacks to steal credentials from employees of Company.com. Which of the following options should Company.com implement to mitigate these attacks?

A. Captive portal
B. OCSP stapling
C. Object identifiers
D. Key escrow
E. Extended validation certificate

Answer: B

NEW QUESTION 345
- (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 350
- (Exam Topic 5)
Which of the following is used to validate the integrity of data?

A. CBC
B. Blowfish
C. MD5
D. RSA

Answer: C

NEW QUESTION 355
- (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 360
- (Exam Topic 5)
A systems administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees. Which of the following would provide strong security and backward compatibility when accessing the wireless network?

A. Open wireless network and SSL VPN
B. WPA using a preshared key
C. WPA2 using a RADIUS back-end for 802.1x authentication
D. WEP with a 40-bit key

Answer: A

NEW QUESTION 365

- (Exam Topic 5)
Joe, a salesman, was assigned to a new project that requires him to travel to a client site. While waiting for a flight, Joe, decides to connect to the airport wireless network without connecting to a VPN, and the sends confidential emails to fellow colleagues. A few days later, the company experiences a data breach. Upon investigation, the company learns Joe's emails were intercepted. Which of the following MOST likely caused the data breach?

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

Answer: A

NEW QUESTION 366
- (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 370
- (Exam Topic 5)
A security technician has been receiving alerts from several servers that indicate load balancers have had a significant increase in traffic. The technician initiates a system scan. The scan results illustrate that the disk space on several servers has reached capacity. The scan also indicates that incoming internet traffic to the servers has increased. Which of the following is the MOST likely cause of the decreased disk space?

A. Misconfigured devices
B. Logs and events anomalies
C. Authentication issues
D. Unauthorized software

Answer: D

NEW QUESTION 375
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SY0-501 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SY0-501 Product From:

https://www.2passeasy.com/dumps/SY0-501/

Money Back Guarantee

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