Vendor: CompTIA

Exam Code: SY0-401

Exam Name: CompTIA Security+ Certification Exam

Version: Demo

DEMO

QUESTION 1
Which of the following technologies can store multi-tenant data with different security requirements?

A. Data loss prevention
B. Trusted platform module
C. Hard drive encryption
D. Cloud computing

Correct Answer: D

QUESTION 2
Which of the following wireless security technologies continuously supplies new keys for WEP?

A. TKIP
B. Mac filtering
C. WPA2
D. WPA

Correct Answer: A

QUESTION 3
An administrator would like to review the effectiveness of existing security in the enterprise. Which of the following would be the BEST place to start?

A. Review past security incidents and their resolution
B. Rewrite the existing security policy
C. Implement an intrusion prevention system
D. Install honey pot systems

Correct Answer: C

QUESTION 4
Review the following diagram depicting communication between PC1 and PC2 on each side of a router. Analyze the network traffic logs which show communication between the two computers as captured by the computer with IP 10.2.2.10.

DIAGRAM

PC1 PC2

[192.168.1.30]--------[INSIDE 192.168.1.1 router OUTSIDE 10.2.2.1]---------[10.2.2.10] LOGS

10:30:22, SRC 10.2.2.1:3030, DST 10.2.2.10:80, SYN

10:30:23, SRC 10.2.2.10:80, DST 10.2.2.1:3030, SYN/ACK

10:30:24, SRC 10.2.2.1:3030, DST 10.2.2.10:80, ACK Given the above information, which of the following can be inferred about the above environment?

A. 192.168.1.30 is a web server.
B. The web server listens on a non-standard port.
C. The router filters port 80 traffic.
D. The router implements NAT.

Correct Answer: D

QUESTION 5

Pete, a security administrator, has observed repeated attempts to break into the network. Which of the following is designed to stop an intrusion on the network?

A. NIPS
B. HIDS
C. HIPS
D. NIDS

Correct Answer: A

QUESTION 6
After an assessment, auditors recommended that an application hosting company should contract with additional data providers for redundant high speed Internet connections. Which of the following is MOST likely the reason for this recommendation? (Select TWO).

A. To allow load balancing for cloud support
B. To allow for business continuity if one provider goes out of business
C. To eliminate a single point of failure
D. To allow for a hot site in case of disaster
E. To improve intranet communication speeds

Correct Answer: BC

QUESTION 7
The Chief Technical Officer (CTO) has tasked The Computer Emergency Response Team (CERT) to develop and update all Internal Operating Procedures and Standard Operating Procedures documentation in order to successfully respond to future incidents. Which of the following stages of the Incident Handling process is the team working on?

A. Lessons Learned
B. Eradication
C. Recovery
D. Preparation

Correct Answer: D

QUESTION 8
Which of the following should be considered to mitigate data theft when using CAT5 wiring?

A. CCTV
B. Environmental monitoring
C. Multimode fiber
D. EMI shielding

Correct Answer: D

QUESTION 9
Used in conjunction, which of the following are PII? (Select TWO).

A. Marital status
B. Favorite movie
C. Pet's name
D. Birthday
E. Full name

Correct Answer: DE

QUESTION 10

A victim is logged onto a popular home router forum site in order to troubleshoot some router configuration issues. The router is a fairly standard configuration and has an IP address of

192.168.1.1. The victim is logged into their router administrative interface in one tab and clicks a forum link in another tab. Due to clicking the forum link, the home router reboots. Which of the following attacks MOST likely occurred?

A. Brute force password attack
B. Cross-site request forgery
C. Cross-site scripting
D. Fuzzing

Correct Answer: B

QUESTION 11
A recent spike in virus detections has been attributed to end-users visiting www.compnay.com. The business has an established relationship with an organization using the URL of www.company.com but not with the site that has been causing the infections. Which of the following would BEST describe this type of attack?

A. Typo squatting
B. Session hijacking
C. Cross-site scripting
D. Spear phishing

Correct Answer: A

QUESTION 12
Which of the following attacks impact the availability of a system? (Select TWO).

A. Smurf
B. Phishing
C. Spim
D. DDoS
E. Spoofing

Correct Answer: AD

QUESTION 13
A database administrator receives a call on an outside telephone line from a person who states that they work for a well-known database vendor. The caller states there have been problems applying the newly released vulnerability patch for their database system, and asks what version is being used so that they can assist. Which of the following is the BEST action for the administrator to take?

A. Thank the caller, report the contact to the manager, and contact the vendor support line to verify any reported patch issues.
B. Obtain the vendor's email and phone number and call them back after identifying the number of systems affected by the patch.
C. Give the caller the database version and patch level so that they can receive help applying the patch.
D. Call the police to report the contact about the database systems, and then check system logs for attack attempts.

Correct Answer: A

QUESTION 14
An IT security technician is actively involved in identifying coding issues for her company.

Which of the following is an application security technique that can be used to identify unknown weaknesses within the code?

A. Vulnerability scanning
B. Denial of service
C. Fuzzing
D. Port scanning

Correct Answer: C

QUESTION 15
The systems administrator wishes to implement a hardware-based encryption method that could also be used to sign code. They can achieve this by:

A. Utilizing the already present TPM.
B. Configuring secure application sandboxes.
C. Enforcing whole disk encryption.
D. Moving data and applications into the cloud.

Correct Answer: A

QUESTION 16
It has been discovered that students are using kiosk tablets intended for registration and scheduling to play games and utilize instant messaging. Which of the following could BEST eliminate this issue?

A. Device encryption
B. Application control
C. Content filtering
D. Screen-locks

Correct Answer: B

QUESTION 17
Which of the following will allow Pete, a security analyst, to trigger a security alert because of a tracking cookie?

A. Network based firewall
B. Anti-spam software
C. Host based firewall
D. Anti-spyware software

Correct Answer: D

QUESTION 18
A system administrator needs to ensure that certain departments have more restrictive controls to their shared folders than other departments. Which of the following security controls would be implemented to restrict those departments?

A. User assigned privileges
B. Password disablement
C. Multiple account creation
D. Group based privileges

Correct Answer: D

QUESTION 19
Which of the following is the BEST reason for placing a password lock on a mobile device?

A. Prevents an unauthorized user from accessing owner's data
B. Enables remote wipe capabilities

C. Stops an unauthorized user from using the device again
D. Prevents an unauthorized user from making phone calls

Correct Answer: A

QUESTION 20
Which of the following is an XML based open standard used in the exchange of authentication and authorization information between different parties?

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

Correct Answer: B

QUESTION 21
Several employee accounts appear to have been cracked by an attacker. Which of the following should the security administrator implement to mitigate password cracking attacks? (Select TWO).

A. Increase password complexity
B. Deploy an IDS to capture suspicious logins
C. Implement password history
D. Implement monitoring of logins
E. Implement password expiration
F. Increase password length

Correct Answer: AF

QUESTION 22
To ensure compatibility with their flagship product, the security engineer is tasked to recommend an encryption cipher that will be compatible with the majority of third party software and hardware vendors. Which of the following should be recommended?

A. SHA
B. MD5
C. Blowfish
D. AES

Correct Answer: D

QUESTION 23
While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?

A. EAP-TLS
B. PEAP
C. WEP
D. WPA

Correct Answer: C

QUESTION 24
Which of the following protocols uses an asymmetric key to open a session and then establishes a symmetric key for the remainder of the session?

A. SFTP
B. HTTPS

C. TFTP
D. TLS

Correct Answer: D

QUESTION 25
The IT department has installed new wireless access points but discovers that the signal extends far into the parking lot. Which of the following actions should be taken to correct this?

A. Disable the SSID broadcasting
B. Configure the access points so that MAC filtering is not used
C. Implement WEP encryption on the access points
D. Lower the power for office coverage only

Correct Answer: D

QUESTION 26
A risk assessment team is concerned about hosting data with a cloud service provider (CSP) which of the following findings would justify this concern?

A. The CPS utilizes encryption for data at rest and in motion
B. The CSP takes into account multinational privacy concerns
C. The financial review indicates the company is a startup
D. SLA state service tickets will be resolved in less than 15 minutes

Correct Answer: B

QUESTION 27
A computer on a company network was infected with a zero-day exploit after an employee accidently opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidently opened it. Which of the following should be done to prevent this scenario from occurring again in the future?

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

Correct Answer: C

QUESTION 28
A small IT security form has an internal network composed of laptops, servers, and printers. The network has both wired and wireless segments and supports VPN access from remote sites. To protect the network from internal and external threats, including social engineering attacks, the company decides to implement stringent security controls. Which of the following lists is the BEST combination of security controls to implement?

A. Disable SSID broadcast, require full disk encryption on servers, laptop, and personally owned electronic devices, enable MAC filtering on WAPs, require photographic ID to enter the building.
B. Enable port security; divide the network into segments for servers, laptops, public and remote users; apply ACLs to all network equipment; enable MAC filtering on WAPs; and require two-factor authentication for network access.
C. Divide the network into segments for servers, laptops, public and remote users; require the use of one time pads for network key exchange and access; enable MAC filtering ACLs on all servers.
D. Enable SSID broadcast on a honeynet; install monitoring software on all corporate equipment' install CCTVs to deter social engineering; enable SE Linux in permissive mode.

Correct Answer: B

QUESTION 29
A security guard has informed the Chief information Security Officer that a person with a tablet has been walking around the building. The guard also noticed strange white markings in different areas of the parking lot. The person is attempting which of the following types of attacks?

A. Jamming
B. War chalking
C. Packet sniffing
D. Near field communication

Correct Answer: B

QUESTION 30
A security Operations Center was scanning a subnet for infections and found a contaminated machine. One of the administrators disabled the switch port that the machine was connected to, and informed a local technician of the infection. Which of the following steps did the administrator perform?

A. Escalation
B. Identification
C. Notification
D. Quarantine
E. Preparation

Correct Answer: CD

Trying our product !

★ 100% Guaranteed Success

★ 100% Money Back Guarantee

★ 365 Days Free Update

★ Instant Download After Purchase

★ 24x7 Customer Support

★ Average 99.9% Success Rate

★ More than 69,000 Satisfied Customers Worldwide

★ Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: