JK0-015

CompTIA E2C Security+ (2008 Edition) Exam

Version 4.1

QUESTION NO: 1

Which of the following devices would be used to gain access to a secure network without affecting network connectivity?

A. Router
B. Vampire tap
C. Firewall
D. Fiber-optic splicer

Answer: B

QUESTION NO: 2

After disabling SSID broadcast for all wireless routers on the network, the administrator noticed that the Same unauthorized users were still accessing the network. Which of the following did the administrator fail to do?

A. Re-enable the SSID.
B. Disallow 802.11a traffic on the network.
C. Change the SSID.
D. Enable ARP cache spoofing protection.

Answer: C

QUESTION NO: 3

Exploitation of the 5-day grace period for domain name registration is referred to as:

A. domain name poisoning.
B. domain name kiting.
C. domain name lookup.
D. domain name service.

Answer: B

QUESTION NO: 4

Which of the following ports is susceptible to DNS poisoning?

A. 23
B. 53
C. 80
D. 8080

Answer: B

QUESTION NO: 5

Why is an ad-hoc network a security risk?

A. An ad-hoc network allows access to another computer at the same level of the logged in user, compromising information.

B. An ad-hoc network allows access to the nearest access point which may allow a direct connection to another computer.
C. An ad-hoc network allows access to the nearest access point which may give elevated rights to the connecting user.
D. An ad-hoc network allows access to another computer but with no rights so files cannot be copied or changed.

Answer: A
Explanation:

A wireless network operates in one of two modes, ad-hoc or infrastructure. In the *ad hoc* mode, each station is a peer to the other stations and communicates directly with other stations within the network. No AP is involved. All stations can send Beacon and Probe frames.

QUESTION NO: 6

Which of the following is a benefit of network access control (NAC)?

A. A user is able to distribute connections to the network for load balancing using a centralized list of approved devices.
B. A user is able to distribute connections to the network using cached credentials on a local machine.
C. A user is able to control connections to the network using a centralized list of approved devices.
D. A user is able to control connections to the network using cached credentials on a local machine.

Answer: C

QUESTION NO: 7

Which of the following is the FINAL phase of disaster recovery?

A. Notify all personnel that a disaster has taken place.
B. Hold a follow-up meeting to review lessons learned.
C. Perform a full recovery so all devices are back in working order.
D. Restore all network connectivity.

Answer: B

QUESTION NO: 8

Which of the following security threats MOST frequently uses IRC to communicate with a remote host?

A. Botnets
B. Phishing
C. Spam
D. Worm

Answer: A

QUESTION NO: 9

When used properly, a one time pad is considered an unbreakable algorithm because:

A. the key is not reused.
B. it is a symmetric key.
C. it uses a stream cipher.
D. it is based on the generation of random numbers.

Answer: A

QUESTION NO: 10

Which of the following allows remote access servers to authenticate to a central server?

A. WLAN properties
B. Authentication protocols
C. Password authentication
D. RADIUS

Answer: D

QUESTION NO: 11

Which of the following is the BEST course of action to ensure an email server is not an open relay?

A. Require authentication for all outbound SMTP traffic.
B. Require authentication for all inbound and outbound SMTP traffic.
C. Block all inbound traffic on SMTP port 25.
D. Require authentication for all inbound SMTP traffic.

Answer: A

QUESTION NO: 12

Which of the following security threats would MOST likely use IRC?

A. Botnets
B. Adware
C. Logic bombs

D. Spam

Answer: A

QUESTION NO: 13

A user contacts technical support stating they received notification in a web browser that their computer is infected with a virus. Which of the following would help prevent this in the future?

A. Anti-Spyware
B. Spam blocker
C. Antivirus
D. Pop-up blocker

Answer: D

QUESTION NO: 14

An administrator wants to make sure that network machines stay up-to-date with current solutions, which of the following should be done on a regular basis to help facilitate this need?

A. Group policy updates
B. Patch management
C. Driver updates
D. Configuration baselines

Answer: B

QUESTION NO: 15

Which of the following is the main disadvantage of implementing a certificate revocation list?

A. Revocation is not instantaneous.
B. It is a single point of failure and expensive to maintain.
C. Only a certain number of certificates can be revoked.
D. The CRL database cannot be duplicated.

Answer: B

QUESTION NO: 16

On which of the following algorithms is PGP based?

A. RSA
B. MD5
C. WPA
D. DES

Answer: A

QUESTION NO: 17

Employee A sends employee B an encrypted message along with a digital signature. Employee B wants to make sure that the message is truly from employee A. Which of the following will employee B do to verify the source of the message?

A. Use employee B's private key to unencrypted the message.
B. Use employee A's private key to verify the digital signature.
C. Use employee B's public key to unencrypted the message.
D. Use employee A's public key to verify the digital signature.

Answer: D

QUESTION NO: 18

Employee A wants to send employee B an encrypted message that will identify employee A as the source of the message. Which of the following will employee A do to accomplish this? (Select TWO).

A. Use employee A's private key to sign the message.
B. Use the message application to mark the message as urgent.
C. Use only symmetric encryption to send the message.
D. Use employee B's private key to encrypt the message.
E. Use employee B's public key to encrypt the message.
F. Use employee A's public key to sign the message.

Answer: A, E

QUESTION NO: 19

Which of the following groups should be able to view the results of the risk assessment for an organization? (Select TWO).

A. HR employees
B. Information security employees
C. All employees
D. Executive management
E. Vendors

Answer: B, D

QUESTION NO: 20

Which of the following describes the role of a proxy server?

A. Analyzes packets
B. Serves as a honeypot
C. Blocks access to the network
D. Forwards requests for services from a client

Answer: D

QUESTION NO: 21

A recent risk assessment has identified vulnerabilities on a production server. The technician realizes it was recently re-imaged after a component failed on it. Which of the following is the FIRST item to assess when attempting to mitigate the risk?

A. If all current service packs and hotfixes were re-applied
B. If the spam filters have been properly applied
C. If all device drivers were updated
D. If the firewall ruleset does not allow incoming traffic to the vulnerable port

Answer: A

QUESTION NO: 22

NIDS can be used to help secure a network from threats MOST effectively by watching network traffic in order to:

A. verify adequate bandwidth is being provided for existing traffic.
B. inspect and analyze data being passed through SSH tunnels.
C. ensure proper password strength.
D. observe if any systems are communicating using unauthorized protocols.

Answer: D

QUESTION NO: 23

Which of the following is the BEST solution for an administrator to implement in order to learn more about the zeroday exploit attacks on the internal network?

A. A Honeypot
B. A stateful firewall
C. A HIDS
D. An IDS

Answer: A

QUESTION NO: 24

An administrator is having difficulty getting staff to adhere to group policy directives regarding streaming audio. Bandwidth utilization increases around the time that a popular radio show is broadcast. Which of the following is the BEST solution to implement?

A. Enforce group policy
B. Change the password policy
C. Deploy content filters
D. Implement time of day restrictions

Answer: C

QUESTION NO: 25

Which of the following is the BEST way for an attacker to conceal their identity?

A. Shoulder surfing
B. Deleting the cookies
C. Increase the max size of the log
D. Disable logging

Answer: D

QUESTION NO: 26

Which of the following logs would show that someone has been querying information about a Company's networks?

A. System logs for patch and reboot events
B. DNS logs for zone transfers
C. Application logs for service start and stop events
D. Security logs for failed logon attempts

Answer: B

QUESTION NO: 27

Which of the following determines if traffic is blocked or allowed?

A. Access Control List (ACL)
B. Network-based Intrusion Detection System (NIDS)
C. Username and passwords
D. Logical keys

Answer: A

QUESTION NO: 28

Which of the following is the primary location where global policies are implemented in an organization?

A. Physical memory
B. Domain
C. User documentation
D. Security group

Answer: B

QUESTION NO: 29

Which of the following provides a security buffer, after passing through a firewall, by separating a network and still allowing access to that network?

A. VLAN
B. DMZ
C. NAC
D. NAT

Answer: B

QUESTION NO: 30

In the event of a fire, the MOST appropriate setting for electronic cipher locks would be to:

A. allow personnel to exit the building only after security confirms the threat and electronically releases all locks.
B. allow personnel to exit the building without any forms of authentication.
C. allow personnel to exit the building using only a photo ID badge.
D. allow personnel to exit the building only after using a valid swipe card and key.

Answer: B

QUESTION NO: 31

Which of the following protocols uses a three-way handshake during communication with multiple hosts?

A. SMTP
B. UDP
C. TCP
D. RDP

Answer: C

QUESTION NO: 32

A number of users on the company network have been contracting viruses from required social networking sites.
Which of the following would be MOST effective to prevent this from happening?

A. NIDS
B. Firewall
C. Proxy server
D. Honeypot

Answer: C

QUESTION NO: 33

A user logs onto a laptop with an encrypted hard drive. There is one password for unlocking the encryption and one password for logging onto the network. Both passwords are synchronized and used to login to the machine. Which of the following authentication types is this?

A. Biometric
B. Single sign-on
C. Three factor
D. Two factor

Answer: B

QUESTION NO: 34

A call center uses 50 remote representatives to handle calls for clients. The representatives run software based IP phones on their laptops, and connect back to the call center over the Internet. However, one of the representatives reports that they can no longer connect to the call center PBX. Which of the following is the reason that only this call center representative is unable to connect to the PBX?

A. The representative has a disk defragmentation program installed.
B. The call center has placed the firewall on the edge of the network.
C. The representative has a mis-configured software firewall.
D. The call center has recently installed HIDS.

Answer: C

QUESTION NO: 35

A network administrator is alerted to an incident on a file server. The alerting application is a file integrity checker. Which of the following is a possible source of this HIDS alert?

A. ARP poisoning
B. DDOS
C. Teardrop attack
D. Rootkit

Answer: D

QUESTION NO: 36

A NIPS is primarily used for which of the following purposes?

A. To monitor network traffic in promiscuous mode
B. To alert the administrator to known anomalies
C. To log any known anomalies
D. To take action against known threats

Answer: D

QUESTION NO: 37

Which of the following should be done FIRST after creating a formal disaster recovery plan?

A. Test the plan.