N10-006 - Quiz E – Answers Provided

Periodically you will face a question where you do not agree with the answer. That purposely happens because the wrong answer has been purposely inserted. When you find that situation raise the issue in the course discussion board under the discussion area relating to this Quiz.

1. A wireless network technician for a local retail store is installing encrypted access points within the store for real-time inventory verification, as well as remote price checking capabilities, while employees are away from the registers. The store is in a fully occupied strip mall that has multiple neighbors allowing guest access to the wireless networks. There are a finite known number of approved handheld devices needing to access the store's wireless network. Which of the following is the BEST security method to implement on the access points?

A. Port forwarding

*B. MAC filtering

C. TLS/TTLS

D. IP ACL

2. A network technician has set up an FTP server for the company to distribute software updates for their products. Each vendor is provided with a unique username and password for security. Several vendors have discovered a virus in one of the security updates. The company tested all files before uploading them but retested the file and found the virus. Which of the following could the technician do for vendors to validate the proper security patch?

A. Use TFTP for tested and secure downloads

B. Require biometric authentication for patch updates

*C. Provide an MD5 hashfor each file

D. Implement a RADIUS authentication

3. During a check of the security control measures of the company network assets, a network administrator is explaining the difference between the security controls at the company. Which of the following would be identified as physical security controls? (Select THREE).

A. RSA

B. Passwords

*C. Man traps

*D. Biometrics

*E. Cipher locks

F. VLANs

G. 3DES

4. Which of the following physical security controls prevents an attacker from gaining access to a network closet?

A. CCTVs

*B. Proximity readers

C. Motion sensors

D. IP cameras

5. A technician needs to install software onto company laptops to protect local running services, from external threats. Which of the following should the technician vinstall and configure on the laptops if the threat is network based?

A. A cloud-based antivirus system with a heuristic and signature based engine

B. A network based firewall which blocks all inbound communication

*C. A host-based firewall which allows all outbound communication

D. A HIDS to inspect both inbound and outbound network communication

6. A technician is setting up a computer lab. Computers on the same subnet need to communicate with each other using peer to peer communication. Which of the following would the technician MOST likely configure?

A. Hardware firewall

B. Proxy server

*C. Software firewall

D. GRE tunneling

7. A firewall ACL is configured as follows:

- 10. Deny Any Trust to Any DMZ eq to TCP port 22

- 11. Allow 10.200.0.0/16 to Any DMZ eq to Any

- 12. Allow 10.0.0.0/8 to Any DMZ eq to TCP ports 80, 443

- 13. Deny Any Trust to Any DMZ eq to Any

A technician notices that users in the 10.200.0.0/16 network are unable to SSH into servers in the DMZ. The company wants 10.200.0.0/16 to be able to use any protocol, but restrict the rest of the 10.0.0.0/8 subnet to web browsing only. Reordering the ACL in which of the following manners would meet the company's objectives?

*A. 11, 10, 12, 13

B. 12, 10, 11, 13

C. 13, 10, 12, 11

D. 13, 12, 11, 10

8. A technician is installing a surveillance system for a home network. The technician is unsure which ports need to be opened to allow remote access to the system. Which of the following should the technician perform?

A. Disable the network based firewall

B. Implicit deny all traffic on network

C. Configure a VLAN on Layer 2 switch

*D. Add the system to the DMZ

9. The ability to make access decisions based on an examination of Windows registry settings, antivirus software, and AD membership status is an example of which of the following NAC features?

A. Quarantine network

B. Persistent agents

*C. Posture assessment

D. Non-persistent agents

10. Which of the following types of network would be set up in an office so that customers could access the Internet but not be given access to internal resources such as printers and servers?

A. Quarantine network

B. Core network

*C. Guest network

D. Wireless network

11. Which of the following is a security benefit gained from setting up a guest wireless network?

A. Optimized device bandwidth

*B. Isolatedcorporate resources

C. Smaller ACL changes

D. Reduced password resets

12. Ann, a network technician, was asked to remove a virus. Issues were found several levels deep within the directory structure. To ensure the virus has not infected the .mp4 files in the directory, she views one of the files and believes it contains illegal material. Which of the following forensics actions should Ann perform?

A. Erase the files created by the virus

*B. Stop and escalate to the proper authorities

C. Check the remaining directories for more .mp4 files

D. Copy the information to a network drive to preserve the evidence

13. A network technician was tasked to respond to a compromised workstation. The technician documented the scene, took the machine offline, and left the PC under a cubicle overnight. Which of the following steps of incident handling has been incorrectly performed?

A. Document the scene

B. Forensics report

C. Evidence collection

*D. Chain of custody

14. A network technician is using a network monitoring system and notices that every device on a particular segment has lost connectivity. Which of the following should the network technician do NEXT?

A. Establish a theory of probable cause.

B. Document actions and findings.

C. Determine next steps to solvethe problem.

*D. Determine if anything has changed.

15. A user calls the help desk and states that he was working on a spreadsheet and was unable to print it. However, his colleagues are able to print their documents to the same shared printer. Which of the following should be the FIRST question the helpdesk asks?

A. Does the printer have toner?

B. Are there any errors on the printer display?

*C. Is the user able to access any network resources?

D. Is the printer powered up?

16. A network technician has detected duplicate IP addresses on the network. After testing the behavior of rogue DHCP servers, the technician believes that the issue is related to an unauthorized home router. Which of the following should the technician do NEXT in the troubleshooting methodology?

A. Document the findings and action taken.

*B. Establish a plan to locate the rogue DHCP server.

C. Remove the rogue DHCP server from the network.

D. Identify the root cause of the problem.

17. A technician is troubleshooting a client's connection to a wireless network. The client is asked to run a "getinfo" command to list information about the existing condition.

- myClient$ wificard --getinfo

- agrCtlRSSI:-72

- agrExtRSSI:0

- state:running

- op mode: station

- lastTxRate:178

- MaxRate:300

- 802.11 auth:open

- link auth:wpa2-psk

- BSSID:0F:33:AE:F1:02:0A

- SSID:CafeWireless

- Channel:149,1

Given this output, which of the following has the technician learned about the wireless network? (Select TWO).

A. The WAP is using RC4 encryption

B. The WAP is using 802.11a

*C. The WAP is using AES encryption

D. The WAP isusing the 2.4GHz channel

*E. The WAP is using the 5GHz channel

F. The WAP is using 802.11g

18. An administrator only has telnet access to a remote workstation. Which of the following utilities will identify if the workstation uses DHCP?

A. tracert

B. ping

C. dig

*D. ipconfig

E. netstat

19. A network technician is performing a tracert command to troubleshoot a website-related issue. The following output is received for each hop in the tracert:

- 1 * * * Request timed out.

- 2 * * * Request timed out.

- 3 * * * Request timed out.

The technician would like to see the results of the tracert command. Which of the following will allow the technician to perform tracert on external sites but not allow outsiders to discover information from inside the network?

A. Enable split horizon to allow internal tracert commands to pass through the firewall

B. Enable IGMP messages out and block IGMP messages into the network

*C. Configure the firewall to allow echo reply in and echo request out of the network

D. Install a backdoor to access the router to allow tracert messages to pass through

20. A network technician has received comments from several users that cannot reach a particular website. Which of the following commands would provide the BEST

information about the path taken across the network to this website?

A. ping

B. netstat

C. telnet

*D. tracert