N10-006 - Quiz J – 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. In the past, a company has experienced several network breaches as a result of end-user actions. To help mitigate future breaches, which of the following documents should the security team ensure are up-to-date and enforced for all employees? (Select TWO)

*A. Memorandum of understanding

B. Data classification document

C. Service level agreement

D. Interconnection security agreement

E. Consent to monitor

*F. Acceptable use policy

2. The Chief Information Officer (CIO) wants to improve the security of the company's data. Which of the following is a management control that should be implemented to ensure employees are using encryption to transmit sensitive information?

*A. Policies

B. VPN

C. HTTPS

D. Standards

3. A client reports that half of the office is unable to access a shared resource. Which of the following should be used to troubleshoot the issue?

A. Data backups

*B. Network diagrams

C. Baseline information

D. Vendor documentation

4. An administrator needs to set up a space in the office where co-workers can relax. The administrator sets up several TV's with interconnected gaming systems in the office. Which of the following did the administrator set up?

*A. CAN

B. MAN

C. WAN

D. LAN

5. Channel bonding will improve which of the following wireless characteristics?

A. Signal strength

B. Encryption strength

C. Coverage area

*D. Connection speed

6. Users have reported poor network performance. A technician suspects a user may have maliciously flooded the network with ping request. Which of the following should the technician implement to avoid potential occurrences from happening in the future?

*A. Block all ICMP request

B. Update all antivirus software

C. Remove all suspected users from the network

D. Upgrade firmware on all network cards

7. A network technician is troubleshooting a network connection error, when pinging the default gateway no reply is received. The default gateway is found to be functioning properly but cannot connect to any workstations. At which of the following OSI layers could the problem exist? (Select TWO)

A. Presentation

B. Transport

C. Session

*D. Data link

E. Application

*F. Physical

8. A technician has determined the most likely cause of an issue and implement a solution. Which of the following is the NEXT step that should be taken?

A. Document the findings, actions, and outcomes

B. Duplicate the problem if possible

*C. Verify system functionality

D. Make an archival backup

9. An administrator has a physical server with a single NIC. The server needs to deploy two virtual machines. Each virtual machine needs two NIC's, one that connects to the network, and a second that is a server to server heartbeat connection between the two virtual machines. After deploying the virtual machines, which of the following should the administrator do to meet these requirements?

A. The administrator should create a virtual switch for each guest. The switches should be configured for inter-switch links and the primary NIC shouldhave a NAT to the corporate network

B. The administrator should create a virtual switch that is bridged to the corporate network and a second virtual switch that carries intra-VM communication only

*C. The administrator should create a virtual switch to bridge all of the connections to the network. The virtual heartbeat NICs should be set to addresses in an unused range

D. The administrator should install a second physical NIC onto the host, and then connect each guest machine's NICs to a dedicated physicalNIC

10. A network technician is asked to redesign an Ethernet network before new monitoring software is added to each host on the network. The new software will broadcast statistics from each host to a monitoring host for each of the five departments in the company. The added network traffic is a concern of management that must be addressed. Which of the following solutions should the technician design into the new network?

*A. Place each department in aseparate VLAN

B. Add a router and create a segment for all the monitoring host stations

C. Increase the number of switches on the network to reduce broadcasts

D. Increase the collision domain to compensate for the added broadcasts

11. A company has added several new employees, which has caused the network traffic to increase by 200%. The network traffic increase from the new employees was only expected to be 20% to 30%. The administration suspects that the network may have been compromised. Which of the following should the network administrator have done previously to minimize the possibility of a network breach?

A. Create VLANs to segment the network traffic

B. Place a network sniffer on segments with newemployees

*C. Provide end user awareness and training for employees

D. Ensure best practices were implemented when creating new user accounts

12. A network technician discovers an issue with spanning tree on the core switch. Which of the following troubleshooting steps should the network technician perform NEXT to resolve the issue?

A. Test a theory to determine the cause

B. Escalate to a senior technician

C. Identify the symptoms

*D. Establish a theory of probable cause

E. Establish a plan of action

13. Which of the following would be the BEST addition to a business continuity plan that would protect business from a catastrophic event such as a fire, tornado, or earthquake?

A. UPS and battery backups

B. Fire suppression systems

C. Building generator

*D. Hot sites or cold sites

E. NAS and tape backups

14. A network technician has created a network consisting of an external internet connection, a DMZ, an internal private network, and an administrative network. All routers and switches should be configured to accept SSH connections from which of the following network segments?

A. The internal network since it is private

*B. The admin private network allowing only admin access

C. The DMZ only allowing access from the segment with the servers

D. The internet connection to allow admin access from anywhere

15. A network technician needs to monitor the network to find a user that is browsing inappropriate websites. Which of the following would the technician use to view the website and find the user browsing it?

A. An SNMP GET

B. A top listener tool

C. An intrusion detection system

*D. Apacket sniffer

16. A network administrator receives a call asking for assistance with connecting to the network. The user asks for the IP address, subnet class, and VLAN required to access the network. This describes which of the following attacks?

*A. Social engineering

B. Spoofing

C. Zero-day attack

D. VLAN hopping

17. Which of the following cloud infrastructure designs includes on premise servers utilizing a centralized syslog server that is hosted at a third party organization for review?

*A. Hybrid

B. Public

C. Community

D. Private

18. A new threat is hiding traffic by sending TLS-encrypted traffic outbound over random ports. Which of the following technologies would be able to detect and block this traffic?

A. Intrusion detection system

B. Application aware firewall

*C. Stateful packet inspection

D. Stateless packet inspection

19. The network administrator is configuring a switch port for a file server with a dual NIC. The file server needs to be configured for redundancy and both ports on the NIC need to be combined for maximum throughput. Which of the following features on the switch should the network administrator use?

A. BPDU

*B. LACP

C. Spanning tree

D. Load balancing

20. A network technician is using telnet to connect to a router on a network that has been compromised. A new user and password has been added to the router with full rights. The technician is concerned that the regularly used administrator account has been compromised. After changing the password on all networking devices, which of the following should the technician perform to prevent the password for the administrator account from being sniffed on the network?

A. Use SNMPv1 for all configurations involving the router

B. Ensure the password is 10 characters, containing letter and numbers

C. Copy all configurations to routers using TFTP for secuirty

*D. Only allow administrators to access routers using port 22