N10-006 - Quiz I – 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. Ann, a system administrator, is troubleshooting an issue with a DNS server. She notices that the security logs have filled up and that they need to be cleared from the event viewer. She recalls this being a daily occurrence. Which of the following solutions would BEST resolve this problem?

A. Increase the maximum log size

B. Log into the DNS server every hour to check if the logs are full

*C. Install an event management tool

D. Delete the logs when full

2. Which of the following protocols were designed to avoid loops on a Layer 2 network? (Select TWO)

A. OSPF

B. RIPv2

C. 802.1q

*D. Spanning tree

*E. 802.1d

F. QoS

3. While implementing wireless access points into the network, one building is having connectivity issues due to light fixtures being replaced in the ceiling, while all other buildings' connectivity is performing as expected. Which of the following should be exchanged on the access points installed in the building with connectivity issues?

A. UTP patch cables

*B. Antenna

C. Power adapter

D. Security standard

4. A technician is attempting to resolve an issue with users on the network not being able to access websites. The technician pings the default gateway and DNS servers successfully. Pinging a website by

URL is unsuccessful but using a known IP address is successful. Which of the following will resolve the issue?

A. Update the HOST file with the URLs for all websites

B. Use NSLOOKUP to resolve URLs

C. Ensure ICMP messages can pass through the firewall

*D. Enable port 53 on the firewall

5. The Chief Information Officer (CIO) of an organization is concerned that the current locally-hosted, software threat solution is not agile enough. The CIO points to specific examples of zero-day threats that have recently taken a day or more to receive patches. The IT team is tasked with finding a solution that has a better chance of stopping emerging threats and stopping zero-day threats more quickly. Which of the following solutions would have the BEST chance of meeting these goals?

*A. Stateful firewall

B. Premise-based IDS

C. Host-based IDS

D. Cloud-based anti-malware

6. A network technician was tasked to install a network printer and share it to a group of five human resource employees. The technician plugged the device into a LAN jack, but was unable to obtain an IP address automatically. Which of the following is the cause of the problem?

A. DNS

B. Wrong TCP port

C. Split horizon

*D. DHCP scope

7. A technician is configuring a computer lab at a school. The computers need to be able to communicate with each other, but students using the computers should not be able to access the internet. Which of the following rules on the firewall should the technician configure for the lab computers?

A. Block all LAN to LAN traffic

B. Block all LAN to WAN traffic

*C. Block all WAN to LAN traffic

D. Block all WLAN to WAN traffic

8. A network administrator is noticing slow responds times from the server to hosts on the network. After adding several new hosts, the administrator realizes that CSMA/CD results in network slowness due to congestion at the server NIC. Which of the following should the network administrator do to the issue?

A. Add a honeypot to reduce traffic to the server

B. Update the Ethernet drivers to use 802.3

*C. Add additional network cards to the server

D. Disable CSMA/CD on the network

9. A technician wants to update the organization's disaster recovery plans. Which of the following will allow network devices to be replaced quickly in the event of a device failure?

A. Vendor documentation

*B. Archives/backups

C. Proper asset tagging and labeling

D. Network Baseline

10. A user is unable to connect to a server in another building. A technician is troubleshooting the issue and determines the following:

1) Client PC 1 has an IP address if 192.168.10.25/25

2) PC 1 can successfully ping its gateway of 192.168.10.1/25 which is an interface of router A

3) Server A is named 'BLDGBFILESRVR01' and has an IP address of 192.168.10.145/25

4) PC 2 with an IP address of 192.168.10.200/25 can successfully ping server A

However, when PC 1 pings server A, it receives a destination host unreachable responds. Which of the following is the MOST likely cause?

A. Link from router A to PC 1 are on different subnets

*B. Link from router A to server A is down

C. Link from PC 1 to router A has duplex issues

D. Link from server A top PC 2 is down

11. A technician wants to implement a network for testing remote devices before allowing them to connect to the corporate network. Which of the following could the technician implement?

A. High availability

B. MAN network

*C. Quarantine

D. Honeynet

12. Which of the following broadband WAN technologies would MOST likely be used to connect several remote branches that have no fiber or satellite connections?

A. OC12

*B. POTS

C. WiMax

D. OC3

13. A technician is troubleshooting a PC that is having intermittent connectivity issues. The technician notices that the STP cables pairs are not completely twisted near the connector. Which of the following is the issue?

*A. Cross-talk

B. 568A/568B mismatch

C. Tx/Rx reverse

D. Split pairs

14. Which of the following can be issued from the command line to find the layer 3 hops to a remote destination?

*A. traceroute

B. nslookup

C. ping

D. netstat

15. An administrator's network has OSPF for the internal routing protocol and has two interfaces that continue to flap. The administrator reviews the following output:

- Fast ethernet 0 is up, line protocol is up

- Int ip address is 10.20.130.5/25

- MTU 1500 bytes, BW10000 kbit, DLY 100 usec

- Reliability 255/255, Tx load 1/255, Rx load 1/255

- Encapsulation ospf, loopback not set

- Keep alive 10

- Full duplex, 100Mb/s, 100Base Tx/Fx

- Received 1052993 broadcasts

- 1258 input errors

- 983881 packet output, 768588 bytes

- 1747 output errors, 0 collisions, 423 resets

Which of the following problems would cause the interface flap?

A. Wrong IP address

B. Loopback not set

C. Bad wire

D. Inencapsulation

*E. Duplex mismatch

16. Which of the following allows a telecommunication company to test circuits to customers remotely?

A. VLAN

B. Toner Probe

C. RDP

*D. Smart Jack

E. VPN

17. A single mode fiber is no longer providing network connectivity to a remote site. Which of the following would be used to identify the location of the break?

A. MT-RJ

*B. OTDR

C. Media converter

D. Cable certifier

18. Users are reporting extreme slowness across the network every Friday. Which of the following should the network technician review first to narrow down the root cause of the problem?

A. Baseline

B. Bottleneck

*C. Utilization

D. Link status

19. A contractor was hired to troubleshoot congestion issues on the network. After a few of the switches have been reconfigured/upgraded by the contractor, congestion worsens and collisions increase. Which of the following is the BEST action to alleviate the situation?

A. Allow the contractor to reset switches to factory defaults

B. Check the cabling on all switches for improper crossover use

C. Document the changes thatwere made

*D. Downgrade firmware and restore backup configuration

20. An organization is involved in a civil court action and needs to ensure email messages are retained. Which of the following describes the requirement to archive and retain email traffic and other correspondence?

A. Chain of custody

*B. Legal hold

C. Divide and conquer

D. Persistent agents