N10-006 - Quiz D – 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 technician is configuring a managed switch and needs to enable 802.3af. Which of the following should the technician enable?

*A. PoE

B. Port bonding

C. VLAN

D. Trunking

2. A technician has finished configuring AAA on a new network device. However, the technician is unable to log into the device with LDAP credentials but is able to do so with a local user account. Which of the following is the MOST likely reason for the problem?

A. Username is misspelled is the device configuration file

B. IDS is blocking RADIUS

*C. Shared secret key is mismatched

D. Group policy has not propagated to the device

3. Multiple students within a networking lab are required to simultaneously access a single switch remotely. The administrator checks and confirms that the switch can be accessed using the console, but currently only one student can log in at a time. Which of the following should be done to this issue?

A. Increase installed memory and install a larger flash module.

B. Increase the number of VLANs configured on the switch.

C. Decrease the number of VLANs configured on the switch.

*D. Increase the number of virtual terminals available.

4. A company is experiencing very slow network speeds of 54Mbps. A technician has been hired to perform an assessment on the existing wireless network. The technician has recommended an 802.11n network infrastructure. Which of the following allows 802.11n to reach higher speeds?

A. MU-MIMO

B. LWAPP

C. PoE

*D. MIMO

5. A network technician must create a wireless link between two buildings in an office park utilizing the 802.11ac standard. The antenna chosen must have a small physical footprint and minimal weight as it will be mounted on the outside of the building. Which of the following antenna types is BEST suited for this solution?

A. Yagi

B. Omni-directional

C. Parabolic

*D. Patch

6. Which of the following concepts are MOST important for a company's long term health in the event of a disaster? (Select TWO).

*A. Redundancy

B. Implementing acceptable use policy

*C. Offsite backups

D. Uninterruptable power supplies

E. Vulnerability scanning

7. An organization notices a large amount of malware and virus incidents at one satellite office, but hardly any at another. All users at both sites are running the same company image and receive the same group policies. Which of the following has MOST likely been implemented at the site with the fewest security issues?

A. Consent to monitoring

B. Business continuity measures

C. Vulnerability scanning

*D. End-user awareness training

8. Which of the following technologies is designed to keep systems uptime running in the event of a disaster?

*A. High availability

B. Load balancing

C. Quality of service

D. Caching engines

9. A network technician is assisting the company with developing a new business continuity plan. Which of the following would be an appropriate suggestion to add to the plan?

*A. Build redundant links between core devices

B. Physically secure all network equipment

C. Maintain up-to-date configuration backups

D. Perform reoccurring vulnerability scans

10. Which of the following describes a smurf attack?

*A. Attack on a target using spoofed ICMP packets to flood it

B. Intercepting traffic intended for a target and redirecting it to another

C. Spoofed VLAN tags used to bypass authentication

D. Forging tags to bypass QoS policies in order to steal bandwidth

11. A malicious user floods a switch with frames hoping to redirect traffic to the user's server. Which of the following attacks is the user MOST likely using?

A. DNS poisoning

*B. ARP poisoning

C. Reflection

D. SYN attack

12. An attacker has connected to an unused VoIP phone port to gain unauthorized access to a network. This is an example of which of the following attacks?

A. Smurf attack

*B. VLAN hopping

C. Bluesnarfing

D. Spear phishing

13. Packet analysis reveals multiple GET and POST requests from an internal host to a URL without any response from the server. Which of the following is the BEST that describes this scenario?

*A. Compromised system

B. Smurf attack

C. SQL injection attack

D. Man-in-the-middle

14. A company wants to make sure that users are required to authenticate prior to being allowed on the network. Which of the following is the BEST way to accomplish this?

*A. 802.1x

B. 802.1p

C. Single sign-on

D. Kerberos

15. A company has decided to update their usage policy to allow employees to surf the web unrestricted from their work computers. Which of the following actions should the IT security team implement to help protect the network from attack as a result of this new policy?

*A. Install host-based anti-malware software

B. Implement MAC filtering on all wireless access points

C. Add an implicit deny to the core router ACL

D. Block port 80 outboundon the company firewall

E. Require users to utilize two-factor authentication

16. Which of the following would be the result of a user physically unplugging a VoIP phone and connecting it into another interface with switch port security enabled as the default setting?

A. The VoIP phone would request a new phone number from the unified communications server.

*B. The VoIP phone would cause the switch interface, that the user plugged into, to shutdown.

C. The VoIP phone would be able to receive incoming calls but will not be able to make outgoing calls.

D. The VoIP phone would request a different configuration from the unified communications server.

17. A network technician has been tasked to configure a new network monitoring tool that will examine interface settings throughout various network devices. Which of the following would need to be configured on each network device to provide that information in a secure manner?

A. S/MIME

B. SYSLOG

C. PGP

*D. SNMPv3

E. RSH

18. A technician wants to securely manage several remote network devices. Which of the following should be implemented to securely manage the devices?

A. WPA2

B. IPv6

*C. SNMPv3

D. RIPv2

19. A technician needs to secure web traffic for a new e-commerce website. Which of the following will secure traffic between a web browser and a website?

*A. SSL

B. DNSSEC

C. WPA2

D. MTU

20. A company has seen an increase in ransomware across the enterprise. Which of the following should be implemented to reduce the occurrences?

A. ARP inspection

B. Intrusion detection system

*C. Web content filtering

D. Port filtering