1. What is the primary purpose of a firewall in a network security infrastructure?

b) Filtering and controlling network traffic

2. What type of attack involves flooding a network with excessive traffic to disrupt normal operation?

a) Denial of Service (DoS)

3. Which encryption protocol is commonly used to secure wireless network communication?

b) WPA (Wi-Fi Protected Access)

4. What is the purpose of a VPN (Virtual Private Network) in a network security context?

Encrypting internet traffic and masking IP addresses

5. Patch management is the process of regularly updating software and firmware to address security vulnerabilities and improve system performance.

TRUE

6. A network administrator should perform regular backups of critical data to prevent data loss in the event of hardware failures, disasters, or security breaches.

TRUE

7. Traceroute is a network diagnostic tool used to identify the route and measure the latency of data packets between a source and destination device.

TRUE

8. Describe the steps involved in conducting a network vulnerability Assignment.

First define what parts of the network you will assess and set clear goals.then, gather information about the network and system .use vulnerability scanning tools to findweakness . analze the risk and prioritize them based on severity.report your findingswith details ,then suggest how fix the issues . after fixes are applied , re-scan to confirm everything is resolved .finally the whole process and plans regular chechks.

9. Demonstrate how to troubleshoot network connectivity issues using the ping command.

To troubleshoot network connectivity using ping command open the command prompt or terminal and type ping .if you receive replies with time values , the connection is working .if you get “request timed out” or “destination host unreacheble” there is likely a network issue. Start by pinging your local router to check local connectivity , then try an external site to test internet access.

10. Discuss the importance of regular network maintenance and the key tasks involved in maintaining network infrastructure.

Regular network maintenance is essential to keep a network secure, reliable, and efficient. It helps prevent security breaches by ensuring firewalls, antivirus software, and patches are up to date. Maintenance also improves performance by identifying slowdowns, replacing outdated hardware, and optimizing configurations. Key tasks include monitoring traffic, updating software, backing up data, managing user access, 23and performing regular security checks. Without proper

maintenance, networks are more prone to downtime, vulnerabilities, and poor performance, which can disrupt operations and lead to data loss or financial damage.