

Assignment module 6: Network Security, Maintenance, and Troubleshooting Procedures

Section 1: Multiple Choice

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 communications?	
b) WPA (Wi-Fi Protected Access)	
4. What is the purpose of a VPN (Virtual Private Network) in a network security context?	
a) Encryption	

Section 2: True or false

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

Ans:- 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.

Ans:- 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.

Ans:- True

Section 3: Short

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

Define parameters
Identify assets
Scan for vulnerabilities
Analyze results
Prioritize vulnerabilities
Create a report
Remediate
Repeat
Assign ownership

Section 4: Practical Application1

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

To troubleshoot network connectivity issues using the ping command, you can:

1. Open a command prompt or terminal depending on your operating system:
 - Windows: Open the Command Prompt
 - macOS or Linux: Open the Terminal
2. Type the ping command followed by the device's IP address or hostname:
 - For example, to ping a device with the IP address 192.168.1.1, type "ping 192.168.1.1" and press Enter
3. Interpret the results:
 - If the device responds, you'll see a series of responses that indicate the network round-trip time and other statistics
 - If the device doesn't respond, you might see "Request timed out" or "Destination host unreachable" messages

Section 5:

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

- **Security**

Network maintenance helps protect against cyberattacks and other threats by identifying and fixing vulnerabilities.

- **Performance**

Regular maintenance ensures that your network is running efficiently and reliably.

- **Disaster recovery**

Network maintenance helps ensure that you can recover data quickly in the event of a disaster.

- **Growth**

Network maintenance helps ensure that your network can handle growth as your organization expands.

- **Updating software and firmware:** Regular updates help maintain network security and performance.
- **Monitoring network performance:** Track traffic patterns, bandwidth usage, and identify bottlenecks.
- **Cleaning physical components:** Clean and maintain physical components like routers, switches, and servers.