

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?

ANSWER - b) Filtering and controlling network traffic.

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

ANSWER - a) Denial of Service (DoS).

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

ANSWER - b) WPA (Wi-Fi Protected Access).

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

ANSWER - c) To securely connect to a private network over the internet

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.

ANSWER – 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.

ANSWER – 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.

ANSWER – True

Section 3: Short

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

ANSWER -

1. Define Scope

Identify the systems, networks, and assets to be assessed.

2. Gather Information

Collect data on network devices, software, IP ranges, and open ports.

3. Scan for Vulnerabilities

Use tools like Nessus, OpenVAS, or Nmap to detect weaknesses.

4. Analyze Results

Evaluate findings to determine risk levels and prioritize threats.

5. Report Findings

Create a report detailing discovered vulnerabilities and suggested fixes.

6. Remediate Issues

Apply patches, change configurations, or update systems as needed.

7. Re-assess

Run another scan to confirm that vulnerabilities have been fixed.

Section 4: Practical

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

ANSWER - Done

Section 5:

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

ANSWER -

Regular network maintenance is a crucial aspect of managing any organization's IT infrastructure. It ensures the network operates efficiently, securely, and without interruptions. As businesses rely heavily on their networks for communication, data sharing, and day-to-day operations, even minor issues can lead to significant disruptions. Therefore, proactive maintenance helps prevent failures, improves performance, and enhances overall system security.

Importance of Regular Network Maintenance:

1. Ensures Network Reliability:

Maintenance helps identify potential issues before they escalate into major problems. This minimizes unexpected downtime and maintains productivity.

2. Enhances Security:

Cyber threats constantly evolve. Regular updates, patches, and security audits protect the network from vulnerabilities, malware, and unauthorized access.

3. Improves Performance:

Monitoring and optimizing network resources ensure that devices and applications run smoothly, reducing latency and improving user experience.

4. Supports Business Continuity:

In case of failures or disasters, well-maintained networks with proper backups and recovery plans help restore operations quickly.

5. Compliance with Standards:

Many industries have regulatory requirements regarding data security and network management. Regular maintenance helps organizations stay compliant.

Key Tasks in Network Maintenance:

1. Patch Management and Updates:

Regularly updating operating systems, firmware, and software ensures known vulnerabilities are fixed and new features are implemented securely.

2. Data Backup and Recovery Planning:

Scheduled backups protect critical data from loss due to hardware failure, human error, or cyberattacks. Testing recovery plans ensures data can be restored when needed.

3. Network Monitoring:

Continuous monitoring tools track traffic, bandwidth usage, and device status to detect unusual activity, slowdowns, or failures.

4. Security Audits and Access Control:

Regularly reviewing firewall settings, antivirus programs, and user access rights helps maintain a secure environment and prevents unauthorized entry.

5. Hardware Inspection:

Checking physical components like routers, switches, and cables ensures they are functioning correctly and are not at risk of failure due to wear and tear.

6. Performance Optimization:

Adjusting configurations, balancing loads, and clearing unused connections or applications helps enhance network speed and reliability.

7. Log Analysis and Documentation:

Reviewing system and security logs allows early detection of irregularities. Maintaining documentation helps in faster troubleshooting and compliance reporting.