

Assignment Module 6: Network Security, Maintenance and Troubleshooting

Section 1: Multiple Choice

1. What is the main purpose of a firewall in a network?

Answer: To monitor and control incoming and outgoing network traffic for security.

2. Which type of attack attempts to make a system unavailable to users?

Answer: Denial of Service (DoS) attack.

3. Which protocol is used to securely browse websites?

Answer: HTTPS.

4. What device is used to detect suspicious network activity?

Answer: Intrusion Detection System (IDS).

Section 2: True or False

5. Antivirus software helps protect systems from malware.

Answer: True.

6. A VPN provides an unencrypted connection over the internet.

Answer: False.

7. Regular software updates improve system security.

Answer: True.

Section 3: Short Answer

8. Explain the role of antivirus software in network security.

Antivirus software detects, prevents, and removes malicious software, protecting systems from viruses, worms, and other threats.

9. What is phishing?

Phishing is a cyberattack where attackers trick users into revealing sensitive information such as passwords or credit card details.

Section 4: Practical Application

10. Describe steps to secure a wireless network.

- **Change default router credentials.**
- **Enable WPA2/WPA3 encryption.**
- **Use a strong Wi-Fi password.**
- **Disable WPS.**
- **Update router firmware regularly.**

Section 5: Essay

11. Discuss the importance of network security maintenance and troubleshooting in an organization.

Network security maintenance and troubleshooting are essential for protecting organizational data and ensuring uninterrupted operations. Regular maintenance helps

identify vulnerabilities, apply security updates, and prevent cyber threats. Troubleshooting allows administrators to quickly detect and resolve network issues, reducing downtime. Security monitoring tools help detect unauthorized access and suspicious activity. Proper maintenance improves network performance and reliability. It also ensures compliance with security policies and standards. Routine backups and system checks protect critical data from loss. Effective troubleshooting minimizes business disruptions. Well-maintained networks improve user confidence and productivity. Overall, network security maintenance and troubleshooting are vital for a safe and stable network environment.