1. What is the primary purpose of a firewall in a network security infrastructure?
a) Encrypting network traffic
b) Filtering and controlling network traffic
c) Assigning IP addresses to devices
d) Authenticating users for network access

ANS:-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)
b) Phishing
c) Spoofing
d) Man-in-the-Middle (MitM)

ANS:-a) Denial of Service (DoS)

3. Which encryption protocol is commonly used to secure wireless network communications?
a) WEP (Wired Equivalent Privacy)
b) WPA (Wi-Fi Protected Access)
c) SSL/TLS (Secure Sockets Layer/Transport Layer Security)
d) AES (Advanced Encryption Standard)

ANS:-b) WPA (Wi-Fi Protected Access)

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

ANS:-A Virtual Private Network (VPN) enhances network security by creating a secure,
Encrypted tunnel for data transmission over the internet, protecting it from unauthorized access and interception.
Its primary purposes include ensuring data confidentiality, integrity, and privacy,

Especially on unsecured networks like public Wi-Fi. By masking the user's IP address and routing traffic through a remote server,
A VPN hides the user's location and identity, making it difficult for attackers, ISPs, or third parties to track online activities.
VPNs also enable secure remote access to private networks, allowing employees to connect to corporate resources safely.
Additionally, they can bypass geo-restrictions and censorship by simulating a connection from another region.
By using strong encryption protocols like AES and authentication mechanisms,
VPNs mitigate risks such as man-in-the-middle attacks, ensuring safe communication for sensitive data. However,

VPN effectiveness depends on the provider’s security practices and protocol strength.

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

ANS:-True

6.True or False: 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.True or False: 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

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

ANS:-Conducting a network vulnerability assessment involves several key steps.
First, planning defines the scope, objectives, and systems to be tested, ensuring proper authorization.
Next, information gathering collects data on network assets, configurations, and potential entry points using tools like Nmap.
Then,
Vulnerability scanning employs automated tools (e.g., Nessus, OpenVAS) to identify weaknesses such as outdated software or
Misconfigurations. Analysis follows, where scan results are evaluated to prioritize
Vulnerabilities based on severity and exploitability. Finally, reporting documents findings,
Including vulnerabilities, risks, and remediation recommendations.
Regular follow-ups ensure vulnerabilities are patched and the network remains secure.

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

ANS:-To troubleshoot network connectivity using the ping command, follow these

steps.
Open a command line (Command Prompt on Windows or Terminal on macOS/Linux).
First, test the local device by typing ping 127.0.0.1.
Successful replies confirm the network stack is functional; failure indicates local TCP/IP issues.
Next, ping the device's IP address (find via ipconfig or ifconfig), verifying the network interface.
Then, ping the default gateway (e.g., ping 192.168.1.1) to check local network connectivity;
Failure suggests router or connection issues. Ping an external IP like 8.8.8.8 to test internet access;
Failure points to ISP or router problems. Finally, ping a domain (e.g., ping google.com) to verify DNS resolution;
Failure here (if 8.8.8.8 works) indicates DNS issues. Use options like ping -t for continuous testing.
Analyze results for packet loss or high latency, and check cables, router, or DNS settings accordingly.

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

ANS:-
Regular network maintenance is crucial for ensuring a secure, reliable, and efficient network infrastructure.
It prevents downtime, enhances performance, and mitigates security risks, reducing the likelihood of costly outages or cyberattacks.
Proactive maintenance supports business continuity,
compliance,
and scalability while extending hardware lifespan and maintaining user trust through consistent connectivity.

Key tasks include:- monitoring network traffic with tools like Nagios to identify bottlenecks or anomalies.
Patch management updates software and firmware to address vulnerabilities, with testing to avoid disruptions.
Backups of critical data ensure recovery from failures or attacks.
Security management involves updating firewalls and conducting vulnerability scans.
Inventory management tracks devices and software, replacing outdated hardware.
Capacity planning anticipates future needs, upgrading resources as necessary.
Troubleshooting uses tools like ping to resolve issues quickly.
Documentation of changes and incidents aids auditing. User training on security practices minimizes risks.
These tasks ensure a robust, secure network.

11.
Which of the following best describes the purpose of a VPN (Virtual Private Network)?

a) Encrypting network traffic to prevent eavesdropping
b) Connecting multiple LANs (Local Area Networks) over a wide area network (WAN)
c) Authenticating users and controlling access to network resources
d) Reducing latency and improving network performance

ANS:-a) Encrypting network traffic to prevent eavesdropping