**Assignment module 6:**

**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.) WAP (Wi-Fi Protected Access)

4. Which of the following best describes the purpose of a VPN (Virtual

Private Network)?

**Answer:** a) Encrypting network traffic to prevent eavesdropping

**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:** Conducting a network vulnerability assessment involves a structured process that typically includes planning and scoping, vulnerability identification through scanning, analysis and prioritization of findings, remediation of identified vulnerabilities, and verification through reporting and continuous monitoring.

**Steps in conducting a network vulnerability:**

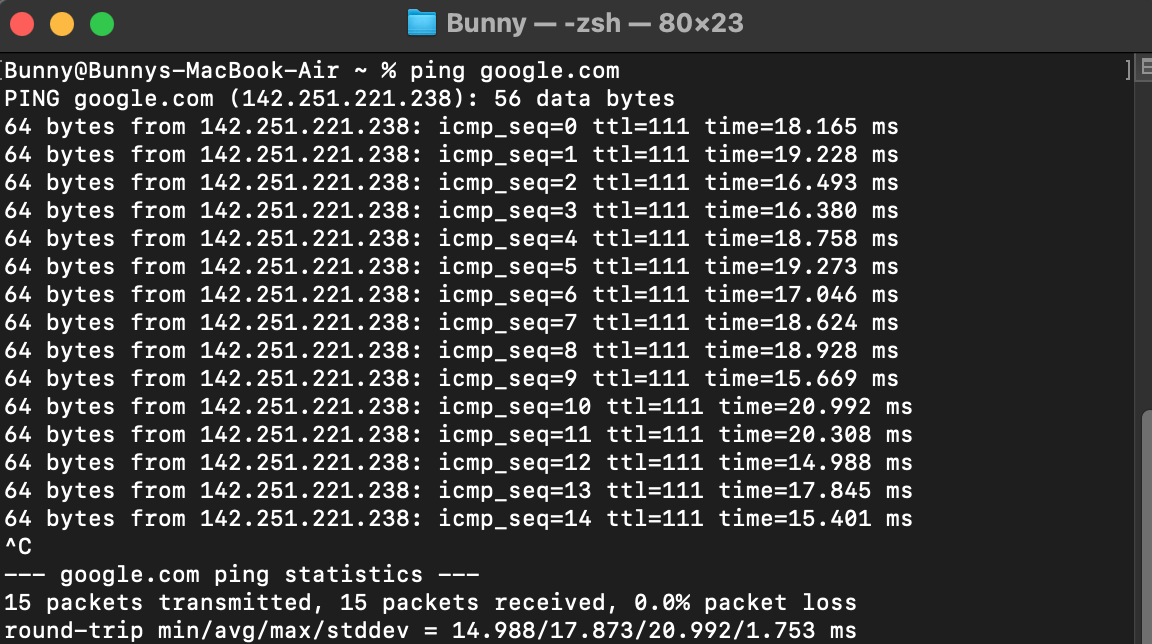
1. **Define Scope and Objectives (Planning):** Determine the specific areas of the network to be assessed, the goals of the assessment (e.g., compliance, security posture improvement), and the types of vulnerabilities to look for. This also involves identifying the stakeholders and allocating resources.
2. **Gather Information & Asset Identification:** Compile a comprehensive inventory of all network assets, including devices, operating systems, software, applications, and cloud services. This "foot printing" helps in understanding the network's composition and identifying what needs to be scanned.
3. **Choose and Configure Tools:** Select appropriate vulnerability scanning tools that align with your scope and objectives, then configure them with specific parameters like target IPs, port ranges, protocol types, and scan aggressiveness levels. Consider using authenticated scans for deeper insights and appropriate firewall rule adjustments.
4. **Scan for Vulnerabilities:** Execute the configured scans to actively search for vulnerabilities across the defined network segments. Monitor the scan progress to ensure it's running as expected and to identify any potential issues.
5. **Analyze and Prioritize Findings:** Interpret the raw scan results, which may include false positives that need to be filtered out. Prioritize identified vulnerabilities based on their severity, potential impact on the business, and the criticality of the affected assets, often using metrics like [CVSS](https://www.google.com/search?client=firefox-b-d&cs=1&sca_esv=a19e3038bac685ef&q=CVSS&sa=X&ved=2ahUKEwiwnK6AzOKOAxUbVmwGHSbEPHcQxccNegQIKxAB&mstk=AUtExfBn8PsvoUj5ay03eA2uWBqeliDzUEk0qFSw-_hIyH9-dV9w16xBYebDI2wbj6c9-JTUzQ6sWrt2ALp_0M-DGv0QCxYw95_bi-vyWdNLUrwsdp6TEg1NC-ZtMIG1N9wPg_SHoG5PhPOH4ysXX0lhiDY3DLqHwYbrXMuaPrXjQyIhuaM&csui=3) (Common Vulnerability Scoring System).
6. **Remediate and Mitigate Vulnerabilities:** Implement corrective actions to address the identified vulnerabilities. This typically involves applying patches, updating configurations, and making network changes to reduce the attack surface.
7. **Validate and Report:** After remediation, rescan the network to verify that the vulnerabilities have been successfully resolved and to ensure that no new issues have been introduced. Document the findings, actions taken, and remaining risks in a comprehensive report.

1. **Continuous Monitoring and Improvement:** Vulnerability management is an ongoing process. Regularly repeat vulnerability assessments, monitor for new threats, and continuously improve your security posture based on evolving risks and new vulnerabilities.

**Section 4: Practical Application**

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

**Answer:**

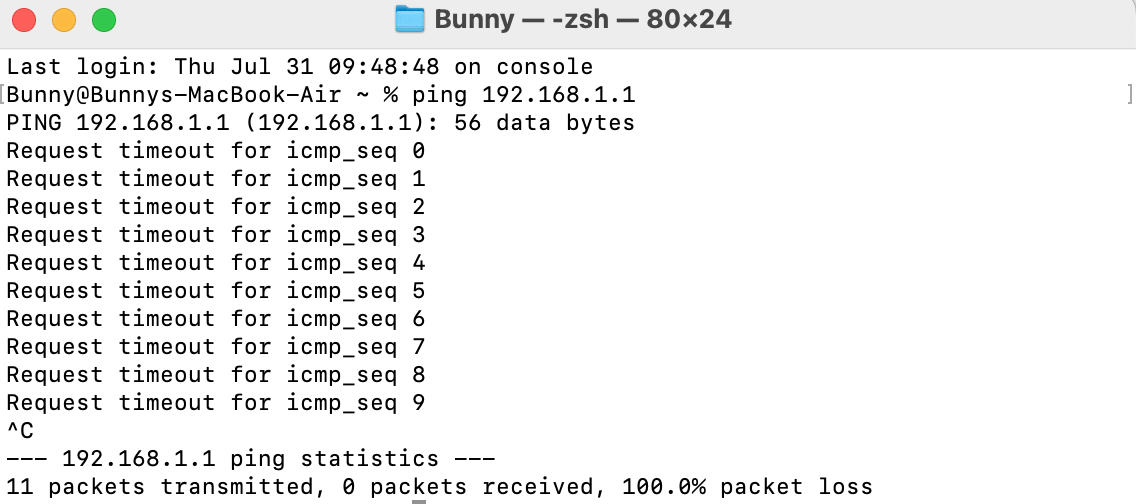
****

1. Open Terminal or Command Prompt.
2. Type Ping and IP Address or hostname in the terminal to check the connectivity of network.
3. Press Ctrl+C to stop the Hop Count. When Hop Count stop, we can see how many packets were transmit and received.
4. When we lost connectivity with network and we check the IP with Ping command, we can see that we loss 100% packet.

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

****

**Section 5: Essay**

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

**Answer:** Regular network maintenance is crucial for ensuring smooth, efficient, and secure operation of IT infrastructure. It prevents disruptions, enhances performance, and minimizes the risk of cyber threats and data breaches. Key tasks include troubleshooting, hardware/software updates, performance monitoring, security management, and planning for future growth.

**Importance of Regular Network Maintenance:**

1. **Reduced Downtime:** Proactive maintenance identifies and resolves issues before they cause major disruptions, minimizing downtime and its associated costs.
2. **Enhanced Security:** Regular updates, security checks, and vulnerability patching help protect the network from cyber threats, malware, and unauthorized access.
3. **Improved Performance:** Maintaining network components, optimizing configurations, and addressing performance bottlenecks ensures smooth and efficient operation.
4. **Cost Savings:** Preventing major issues through routine maintenance is often more cost-effective than dealing with the aftermath of a network crash.
5. **Business Continuity:** A well-maintained network supports business operations, enabling employees to work without interruptions and customers to receive consistent service.
6. **Scalability:** Regular maintenance ensures the network can adapt to future growth and increased workloads, accommodating new users and technologies.

1. **Compliance:** Maintaining a secure and well-documented network can help organizations comply with industry regulations and data privacy requirements.

**Key Tasks in Network Maintenance:**

1. **Troubleshooting:** Identifying and resolving network issues, including hardware failures, software glitches, and connectivity problems.
2. **Hardware and Software Management:** Installing, configuring, and updating network devices, servers, and software to ensure optimal performance and security.
3. **Performance Monitoring:** Regularly monitoring network performance metrics like speed, latency, and bandwidth utilization to identify areas for improvement.
4. **Security Management:** Implementing and maintaining security measures such as firewalls, intrusion detection systems, and access controls to protect the network from threats.
5. **Backup and Recovery:** Regularly backing up critical data and testing the recovery process to ensure business continuity in case of a disaster.
6. **Documentation:** Creating and maintaining accurate network documentation, including diagrams, configurations, and procedures, for efficient troubleshooting and future planning.
7. **Capacity Planning:** Monitoring network traffic and usage patterns to anticipate future needs and plan for upgrades or expansions.
8. **Compliance:** Ensuring that the network infrastructure and operations comply with relevant regulations and standards.