**Assignment - 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.) 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 answer**

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

**Answer:** A Network Vulnerability Assessment helps you find and fix weaknesses in your network before attackers can exploit them. Here is how to do it step by step:

**Steps in conducting a network vulnerability:**

1. **Define Scope and Plan:** Decide which devices, IP ranges, and systems you want to check. Get permission and inform your team. Avoid scanning sensitive or critical systems during working hours. This will Avoid disrupting normal operations and ensure everyone is clear about what is being tested.
2. **Scan Network for Vulnerabilities:** Now, it’s time to scan your network for security vulnerabilities, either manually or via automated [vulnerability scanner tools](https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/). Alongside the actual scan, you’ll use [threat intelligence](https://www.esecurityplanet.com/networks/threat-intelligence-and-analytics-staying-ahead-of-cyber-criminals/) and vulnerability databases to identify security flaws and weaknesses and filter out false positives. Do not be too concerned if your scan’s results show numerous network vulnerabilities; that is to be expected, especially the first time your organization starts to focus on vulnerability management and remediation.
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. **Analyze Results:** Your network vulnerability scan has likely returned massive amounts of vulnerability data, much of which is unstructured, now it is time to analyze and organize that data. Consider not only the criticality of a vulnerability and the likelihood of it being exploited but also what network resources will be impacted if an attack targets that vulnerability.
5. **Prioritize Vulnerabilities:** The most severe vulnerabilities in your vulnerability scans will need to be identified and addressed first. Critical vulnerabilities are security issues that are already causing damage and/or unwarranted access to the network and should be at the top of your risk prioritization list. Right below these vulnerabilities are the ones that have possible exploits malicious actors could take advantage of in the future.  This step is an important move toward making your vulnerability assessment data measurable and actionable.

1. **Create the Vulnerability Assessment Report:**  It is time to document your findings in a vulnerability assessment report. This report will detail all vulnerabilities that were discovered, along with their severity, potential attack vectors within the network, and possible solutions. Portions of this report can use technical jargon and instructions directed at the cybersecurity or vulnerability specialists who will be remediating and mitigating vulnerabilities.
2. **Use Results to Inform Remediation and Mitigation:** You may be able to remediate some of your most critical vulnerabilities with actual patches, but others will require lesser mitigation techniques. Regardless of the solutions you pursue, regularly refer back to your vulnerability assessment to ensure you are focusing on the right vulnerabilities in the right order.

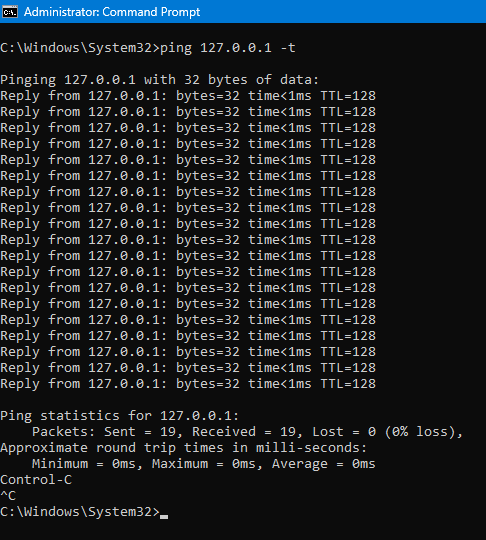
1. **Regularly Repeat Vulnerability Assessments:** Vulnerability assessments provide great snapshots of your [network security](https://www.esecurityplanet.com/networks/network-security/) landscape when they’re first conducted; but almost as soon as the assessment is complete, new applications, users, permissions, datasets, and other features change the landscape of your network and open it up to additional threats. It is necessary to continue cycling through the vulnerability assessment process because new vulnerabilities will emerge and existing vulnerabilities may grow more severe over time.

**Section 4: Practical Application**

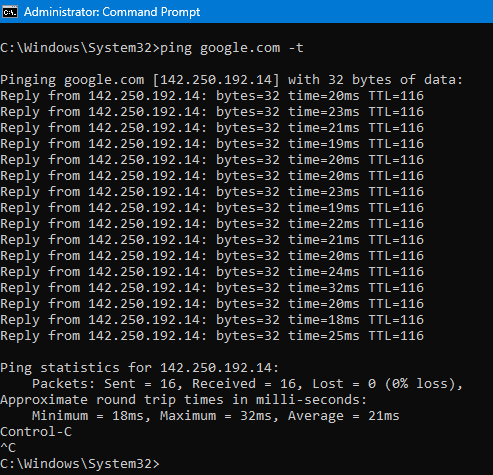
1. Demonstrate how to troubleshoot network connectivity issues using the ping command.

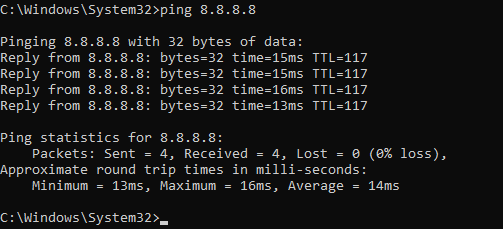
**Answer:**

1. Open Terminal or Command Prompt.
2. Type Ping and the loopback IP Address to check the connectivity of network.



3.) Type Ping and IP Address or hostname in the terminal to check the connectivity of network.





**Section 5: Essay**

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

**Answer:** Regular network maintenance is essential to keep your network **running smoothly, securely, and efficiently.** Without maintenance, your network is more likely to experience **slow performance, security issues, or even complete failure.**

**Importance of Regular Network Maintenance:**

1. **Reduces Downtime**
   * Fixes small problems before they become big ones.
   * Keeps the network available for users.
2. **Improves Performance**
   * Speeds up data transfer and avoids congestion.
   * Helps applications and services run better.
3. **Protects Against Cyber Threats**
   * Applies security patches and updates.
   * Prevents hacking, viruses, and data theft.
4. **Extends Equipment Life**
   * Keeps routers, switches, and cables in good condition.
   * Reduces the need for costly replacements.
5. **Prepares for Growth**
   * Keeps the network ready for adding new users or devices.
6. **Ensures Legal Compliance**
   * Helps meet data protection laws and industry standards.

**Key Tasks in Network Maintenance**

**1. Monitor Network Health**

* Use tools to check traffic, speed, and performance.
* Detect unusual activity or bottlenecks.

**2. Apply Updates & Security Patches**

* Regularly update firmware and software on network devices.
* Fix known vulnerabilities to protect against attacks.

**3. Back Up Device Configurations**

* Save settings for routers, switches, and firewalls.
* Allows quick recovery if a device fails or settings are lost.

**4. Inspect Hardware**

* Check cables, ports, and power supplies.
* Replace damaged or old components.

**5. Test Redundancy (Backup Systems)**

* Make sure backup internet lines or power sources work.
* Test failover systems to prevent service interruptions.

**6. Review User Access**

* Check who has access to what.
* Remove unused accounts and limit permissions.

**7. Update Network Documentation**

* Keep records of IP addresses, devices, and diagrams.
* Helps during troubleshooting and upgrades.

**8. Run Virus/Malware Scans**

* Scan all devices for threats.
* Prevents viruses from spreading on the network.

**9. Test Speed and Connectivity**

* Use commands like ping or tracert to check connection issues.
* Identify slow or broken links.

**10. Manage DHCP and VLAN Settings**

* Ensure IP address allocation is working properly.
* Keep VLANs organized by department or floor.