**Module 6 :- Networking**

**Section 1: Multiple Choice**

**1. What is the primary purpose of a firewall in a network security infrastructure?**

* **b) Filtering and controlling network traffic**

A firewall is used to filter and control incoming and outgoing network traffic based on predetermined security rules.

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

* **a) Denial of Service (DoS)**

A DoS attack floods a network with excessive traffic, making it unavailable to legitimate users.

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

* **b) WPA (Wi-Fi Protected Access)**

WPA (Wi-Fi Protected Access) is commonly used for securing wireless network communications, with WPA2 and WPA3 being the most secure versions.

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

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

A VPN encrypts network traffic to prevent unauthorized access and eavesdropping on data transmitted over the network.

**True or False:**

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

* **True**

Patch management involves updating software and firmware to fix security vulnerabilities, enhance performance, and maintain the system’s security.

**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.**

* **True**

Regular backups are crucial for preventing data loss due to hardware failures, disasters, or security breaches.

**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.**

* **True**

Traceroute is a diagnostic tool that shows the route and measures the latency of data packets as they travel through the network.

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

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

The main purpose of a VPN is to encrypt data traffic and ensure privacy and security during transmission.

**9. Describe the steps involved in conducting a network vulnerability assessment.**

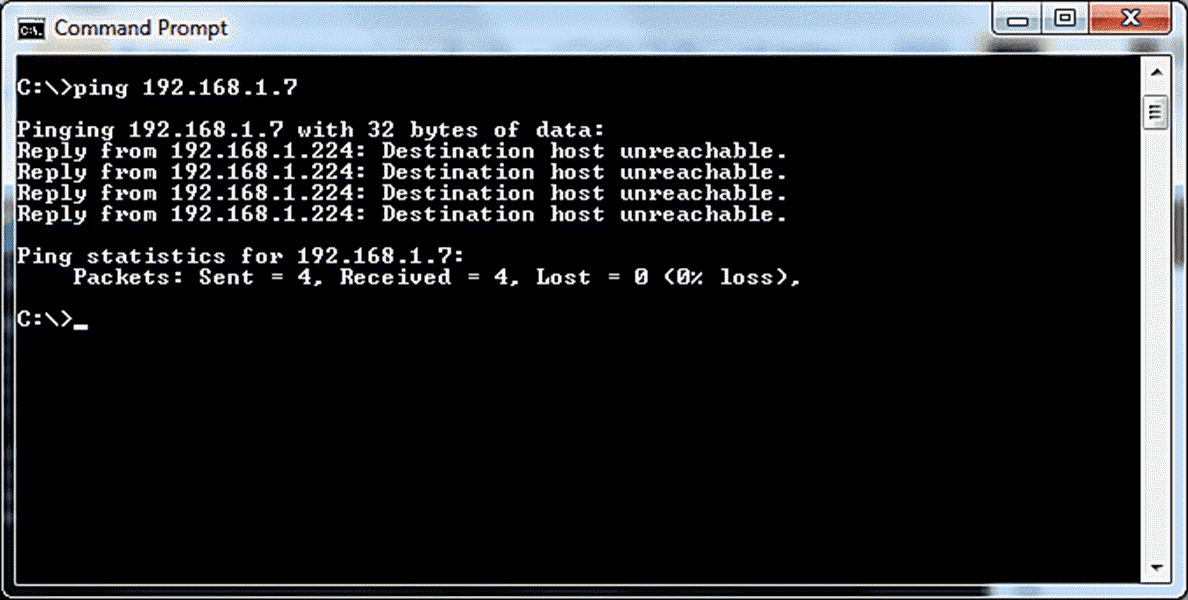
**Answer:**

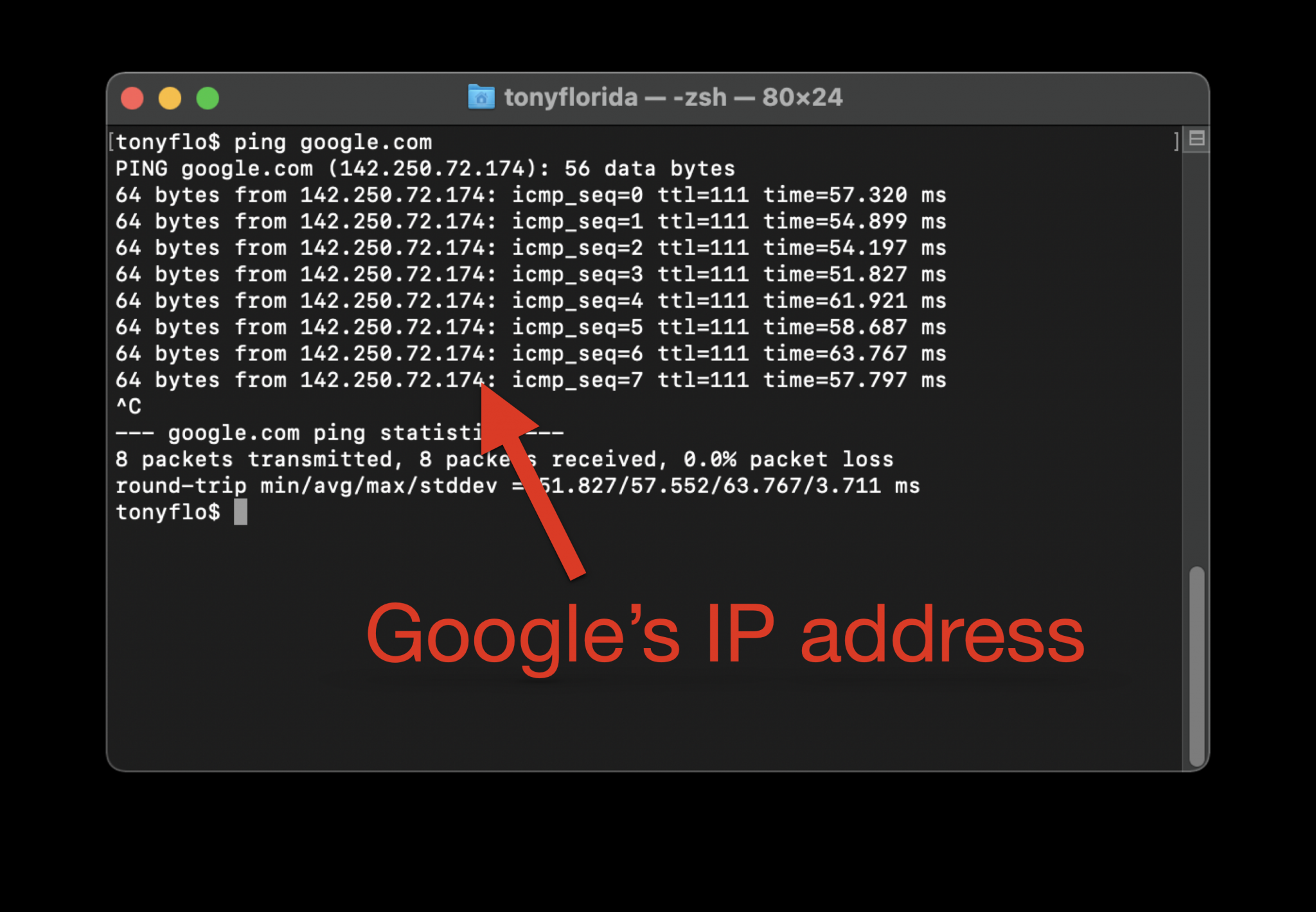
1. **Define Scope and Objectives**: Identify the systems, networks, and applications to be assessed, and set goals for the assessment.
2. **Identify Assets and Resources**: Inventory the network and connected devices to understand the components that need protection.
3. **Select Vulnerability Scanners**: Choose appropriate tools (such as Nessus, OpenVAS) to scan for vulnerabilities.
4. **Perform Vulnerability Scanning**: Run the vulnerability scanner on the network to identify potential weaknesses.
5. **Analyze Results**: Review the scan results and prioritize the vulnerabilities based on their severity and potential impact.
6. **Mitigate Vulnerabilities**: Apply patches, configurations, or other fixes to address the identified vulnerabilities.
7. **Verify and Retest**: After mitigation, retest the network to ensure that vulnerabilities are resolved.
8. **Report Findings**: Create a comprehensive report detailing the vulnerabilities, mitigations, and recommendations for further improvement.

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

**Answer:** **To troubleshoot network connectivity issues using the ping command, follow these steps:**

1. **Open Command Prompt:**
   * **Press Win + R, type cmd, and press Enter.**
2. **Ping a Local Device:**
   * **Type ping [IP address] (e.g., ping 192.168.1.1) and press Enter.**
   * **If you receive replies, the local network is functioning.**
3. **Ping an External Website:**
   * **Type ping [website] (e.g., ping www.google.com) and press Enter.**
   * **Successful replies indicate internet connectivity.**
4. **Interpret Results:**
   * **Replies with times (e.g., time=32ms) suggest a healthy connection.**
   * **Timeouts or errors may indicate issues like network congestion or device unavailability.**





**11. Importance of Regular Network Maintenance**

Regular network maintenance is essential to ensure **security**, **reliability**, and **optimal performance**. It helps prevent issues such as **security breaches**, **downtime**, and **performance degradation**. Maintenance also ensures **cost-efficiency** by addressing problems early and ensures **compliance** with industry regulations.

**Key Tasks Involved**

1. **Monitoring**: Continuously monitor network performance and traffic to detect issues.
2. **Updating Software**: Apply security patches, updates, and firmware upgrades.
3. **Backups**: Regularly back up critical data and configurations.
4. **Security Audits**: Conduct audits to check for vulnerabilities.
5. **Managing IP Addressing**: Keep track of IP usage and prevent conflicts.
6. **Hardware Inspections**: Inspect and replace outdated or failing hardware.
7. **Capacity Planning**: Plan for future network growth and scalability.
8. **Documentation**: Maintain updated records of network configurations and topologies.

These tasks ensure the network remains secure, reliable, and ready to meet business needs.