Cybersecurity Internship – Task 1

5. How can open ports be secured?

Open ports can be secured using the following methods: - Close Unused Ports: Only keep ports open that are essential for your system or service. - Use Firewalls: Configure firewalls to block unauthorized access to open ports. - Enable Port Knocking: This allows ports to appear closed until a specific sequence of network requests is received. - Apply Access Control Lists (ACLs): Limit access to ports based on IP address or user. - Use Secure Protocols: For example, use SSH instead of Telnet. - Regular Port Scanning: Continuously scan your network to detect and respond to new open ports. - Patch and Update Services: Ensure all services listening on ports are up to date to avoid exploitation of known vulnerabilities.

6. What is a firewall's role regarding ports?

A firewall acts as a gatekeeper for network traffic. It controls the flow of data to and from a system by allowing or blocking specific ports based on predefined security rules. Here's what it does: - Blocks Unwanted Traffic: Prevents access to unauthorized or suspicious ports. - Enforces Access Policies: Only allows specific ports needed for applications. - Protects Against Exploits: Shields vulnerable services running on open ports. - Monitors Traffic: Logs access attempts, helping in identifying and responding to threats.

7. What is a port scan and why do attackers perform it?

A port scan is a method used to identify open ports and the services running on them in a target network. It’s like knocking on doors to see which ones are unlocked. Attackers perform port scans to: - Discover Vulnerabilities: Identify which services are running and may be exploitable. - Perform Reconnaissance: Gather intel before launching a targeted attack. - Find Entry Points: Exploit open or misconfigured ports to gain access to systems. - Bypass Security: Detect firewall configurations and find weak points.

8. How does Wireshark complement port scanning?

Wireshark is a network packet analyzer that captures and inspects data packets in real time. It complements port scanning in several ways: - Verify Scan Results: Confirms whether scan attempts reach the destination. - Monitor Network Responses: Analyze how the system responds to scan probes. - Detect Stealthy Scans: Identifies techniques like slow or fragmented scans. - Analyze Protocols: Understand which services are running based on packet content. - Identify Anomalies: Helps detect unusual or malicious behavior triggered by scans.