Vulnerability scanning clear with more examples

Vulnerability scanning is the process of identifying security weaknesses in a network or system. This can be accomplished using a variety of tools and techniques, including:

1. Automated Vulnerability Scanners: These are tools that automatically scan networks or systems for known vulnerabilities, typically using a database of known vulnerabilities and their associated exploits.

Example tool: Nessus

2. Manual Vulnerability Scanning: This involves using manual techniques, such as reviewing system configurations, log files, and user access controls, to identify potential vulnerabilities.

Example technique: Reviewing firewall rules and access control lists.

3. Port Scanning: As discussed earlier, port scanning can be used to identify open ports and services running on a system. By identifying open ports, attackers can determine which services are available and attempt to exploit vulnerabilities associated with those services.

Example tool: Nmap

4. Vulnerability Databases: Vulnerability databases, such as the National Vulnerability Database (NVD) and the Common Vulnerabilities and Exposures (CVE) database, provide a central repository of known vulnerabilities and their associated exploits.

Example database: NVD

5. Web Application Scanning: Web applications are a common target for attackers, and vulnerability scanners that focus specifically on web applications can help identify vulnerabilities such as SQL injection and cross-site scripting (XSS) vulnerabilities.

Example tool: Burp Suite

6. Network Traffic Analysis: Network traffic analysis can help identify potential vulnerabilities, such as insecure protocols, unencrypted data transmissions, and

misconfigured network devices.

Example tool: Wireshark

Vulnerability scanning is an important component of a comprehensive security program, and can help organizations identify and remediate potential vulnerabilities before they can be exploited. It is important to use vulnerability scanning tools and techniques responsibly and ethically, as scanning systems without permission can be illegal and can result in severe consequences.