Assignment-2

Name: Ayush Aryan

Reg. No.:21BCT0316

1. **Nmap (Network Mapper)**:

   Nmap is a versatile network scanning tool used to discover hosts and services on a network. It can be used for network reconnaissance and vulnerability assessment.

2. **Wireshark**:

   Wireshark is a powerful network protocol analyzer. It allows users to capture and inspect data packets on a network, making it invaluable for network troubleshooting and security analysis.

3. **Metasploit**:

   Metasploit is a popular penetration testing framework that helps identify and exploit vulnerabilities in systems. It includes a vast collection of pre-built exploits and payloads for various targets.

4. **Burp Suite**:

Burp Suite is a web vulnerability scanner and proxy tool used for testing the security of web applications. It can identify issues like SQL injection, XSS, and CSRF.

5. **Aircrack-ng**:

Aircrack-ng is a suite of wireless network security tools. It is mainly used for assessing the security of Wi-Fi networks, including tools for capturing, cracking, and analyzing wireless packets.

6. **John the Ripper**:

John the Ripper is a popular password cracking tool. It can be used to crack various password hashes using different attack methods like dictionary attacks and brute force.

7. **Hydra**:

Hydra is a versatile password-cracking tool that supports various protocols and services, including SSH, FTP, HTTP, RDP, and more. It is highly configurable for brute-force and dictionary attacks.

8. **Gobuster**:

Gobuster is a directory and file brute-forcing tool. It helps penetration testers discover hidden files and directories on web servers, which can be useful for finding vulnerabilities.

9. **Snort**:

Snort is an open-source intrusion detection system (IDS) and intrusion prevention system (IPS). It analyzes network traffic for suspicious activities and can be customized with rules to detect specific threats.

10.   **Nikto**:

Nikto is a web server vulnerability scanner that checks web servers and web applications for known security issues. It provides detailed reports on potential weaknesses.