ASSIGNMENT WEEK -2

NAME: SHAZ ALAM **REG.NO 21BCY10221**

Kali Linux is a popular open-source penetration testing and ethical hacking distribution used by security professionals, hackers, and researchers for various cybersecurity tasks. Kali Linux comes pre-installed with a wide range of tools for assessing and securing computer systems. Here are 10 notable Kali Linux tools:

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

   Nmap is a powerful open-source network scanning tool used for discovering hosts and services on a network. It can be used for network reconnaissance, vulnerability scanning, and security auditing.

2. **Metasploit Framework:**

   Metasploit is a penetration testing framework that helps security professionals and hackers identify, exploit, and remediate vulnerabilities in computer systems. It provides a vast collection of exploits, payloads, and auxiliary modules.

3. **Wireshark:**

   Wireshark is a network protocol analyzer that allows users to capture and inspect network traffic. It's an essential tool for diagnosing network issues, analyzing packets, and detecting anomalies.

4. **Burp Suite:**

Burp Suite is a web vulnerability scanner and proxy tool designed for testing the security of web applications. It helps identify and exploit web application vulnerabilities like SQL injection, XSS, and CSRF.

5. **Hydra**:

Hydra is a fast and flexible password-cracking tool that supports various protocols and services, including SSH, FTP, HTTP, and more. It can be used for brute-forcing login credentials.

6. **Aircrack-ng:**

Aircrack-ng is a suite of tools for auditing wireless networks. It includes tools for capturing and cracking WEP and WPA/WPA2-PSK keys, making it useful for Wi-Fi penetration testing.

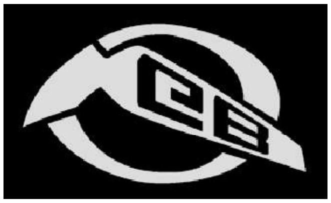
7. **Nikto:**

Nikto is a web server vulnerability scanner that checks web servers for known security issues and misconfigurations. It can help identify potential weaknesses in web applications and server setups.

8. **John the Ripper**:

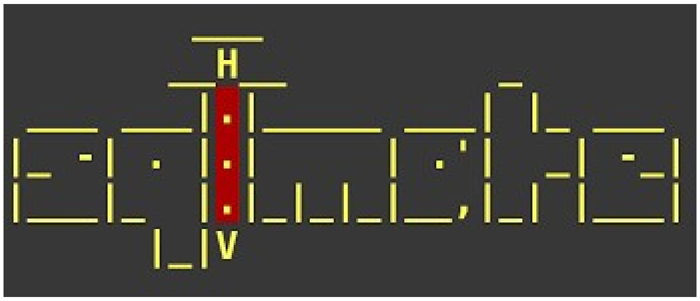
John the Ripper is a popular password cracking tool that can be used to crack various password hashes, including Unix crypt, Windows LM and NTLM, and more. It supports multiple attack modes and algorithms.

9. **Gobuster:**



Gobuster is a directory and file brute-forcing tool that helps identify hidden or unlinked resources on web servers. It's useful for finding hidden directories and files on web applications.

10. **SQL map:**



SQLmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications and databases. It can extract data, execute commands, and even provide a shell on vulnerable systems.