ASSIGNMENT-2 21BCE8673

Kali Linux is a popular Linux distribution designed for penetration testing, ethical hacking, and cybersecurity tasks. It comes pre-installed with a wide range of tools and software for various purposes, including network analysis, vulnerability assessment, digital forensics, and more.
These tools can be categorized into several main categories:
Information Gathering:
Nmap: Network mapping and port scanning tool.
Wireshark: Network protocol analyzer.
Recon-ng: Web reconnaissance framework.
theHarvester: Email and information gathering tool.
Vulnerability Analysis:
OpenVAS: Open Vulnerability Assessment System.
Nikto: Web server scanner.
Nexpose: Vulnerability management tool.
OWASP ZAP: Web application security scanner.
Exploitation Tools:
Metasploit Framework: Penetration testing and exploitation tool.
Burp Suite: Web vulnerability scanner and proxy.
BeEF: Browser exploitation framework.
Hydra: Password cracking tool.
Password Attacks:
John the Ripper: Password cracking tool.
Hashcat: Advanced password recovery utility.
Wireless Attacks:
Aircrack-ng: Wireless network security tool.
Reaver: WPS (Wi-Fi Protected Setup) PIN brute-forcing tool.
WiFite: Automated wireless attack tool.
Web Application Analysis:
Sqlmap: SQL injection vulnerability scanner.
WPScan: WordPress vulnerability scanner.
OWASP Mutillidae: Deliberately vulnerable web application for testing.
Forensics Tools:
Autopsy: Digital forensics platform.
Volatility: Memory forensics framework.
Sleuth Kit: Open-source digital investigation toolkit.
Social Engineering Tools:
SET (Social-Engineer Toolkit): Toolkit for social engineering attacks.
BeEF: Browser exploitation framework (also used for social engineering).
Post-Exploitation Tools:
PowerSploit: PowerShell-based post-exploitation framework.

Veil: Payload generator for creating undetectable payloads.
Reporting Tools:
Dradis: Collaboration and reporting tool.
MagicTree: Penetration tester's reporting tool.
Miscellaneous Tools:
Netcat: Network utility for reading/writing data across networks.
Gobuster: Directory/file brute-forcing tool.
Snort: Network intrusion detection and prevention system.

Kali Linux offers a vast collection of tools to support a wide range of cybersecurity tasks, from information gathering to penetration testing and digital forensics. Users should always use these tools responsibly and legally, respecting ethical guidelines and applicable laws and regulations.