Assignment 2

Kali Linux application on a website

Website – Warframe.com

1. Information Gathering
   Tool – dnsenum

   Information gathering: These tools are used to collect information about a target system or network, such as IP addresses, open ports, running services, and operating system. Some of the most popular information gathering tools in Kali Linux include Nmap, TheHarvester, and Metasploit Framework.

   There are other categories of tools like this, and the next 10 of them are:

2. Vulnerability analysis: These tools are used to scan a target system or network for known vulnerabilities. This information can then be used to exploit the vulnerabilities and gain unauthorized access to the system. Some of the most popular vulnerability analysis tools in Kali Linux include Nessus, OpenVAS, and Wfuzz.

3. Web application analysis: These tools are used to test the security of web applications. They can be used to identify vulnerabilities in the application's code, as well as in the underlying operating system and infrastructure. Some of the most popular web application analysis tools in Kali Linux include Burp Suite, OWASP ZAP, and SQLmap.

4. Database assessment: These tools are used to test the security of databases. They can be used to identify vulnerabilities in the database's schema, as well as in the underlying operating system and infrastructure. Some of the most popular database assessment tools in Kali Linux include SQLninja, DBPwAudit, and SQLite Browser.

5. Password attacks: These tools are used to crack passwords. They can be used to recover passwords from a variety of sources, such as hashed passwords, password files, and even live memory. Some of the most popular password attack tools in Kali Linux include John the Ripper, Hydra, and Aircrack-ng.

6. Wireless attacks: These tools are used to attack wireless networks. They can be used to crack wireless passwords, inject malicious code into wireless traffic, and even take control of wireless access points. Some of the most popular wireless attack tools in Kali Linux include Aircrack-ng, Kismet, and Reaver.

7. Reverse engineering: These tools are used to decompile and analyze software. This can be used to identify vulnerabilities in the software's code, as well as to develop exploits for those vulnerabilities. Some of the most popular reverse engineering tools in Kali Linux include Ghidra, IDA Pro, and Radare2.

8. Exploitation tools: These tools are used to exploit vulnerabilities in a target system or network. They can be used to gain unauthorized access to the system, install malware, or disrupt operations. Some of the most popular exploitation tools in Kali Linux include Metasploit Framework, BeEF, and SET.

9. Sniffing and spoofing: These tools are used to capture and analyze network traffic. This can be used to identify sensitive information being transmitted over the network, as well as to launch man-in-the-middle attacks. Some of the most popular sniffing and spoofing tools in Kali Linux include Wireshark, tcpdump, and ettercap.

10. Post exploitation: These tools are used to maintain and control access to a compromised system or network. They can be used to install backdoors, steal data, and launch further attacks. Some of the most popular post exploitation tools in Kali Linux include Meterpreter, Cobalt Strike, and Powershell Empire.

11. Forensics: These tools are used to collect and analyze digital evidence. This evidence can be used to investigate security incidents, as well as to prosecute criminals. Some of the most popular forensics tools in Kali Linux include The Sleuth Kit, Autopsy, and EnCase.