

ASSIGNMENT 2

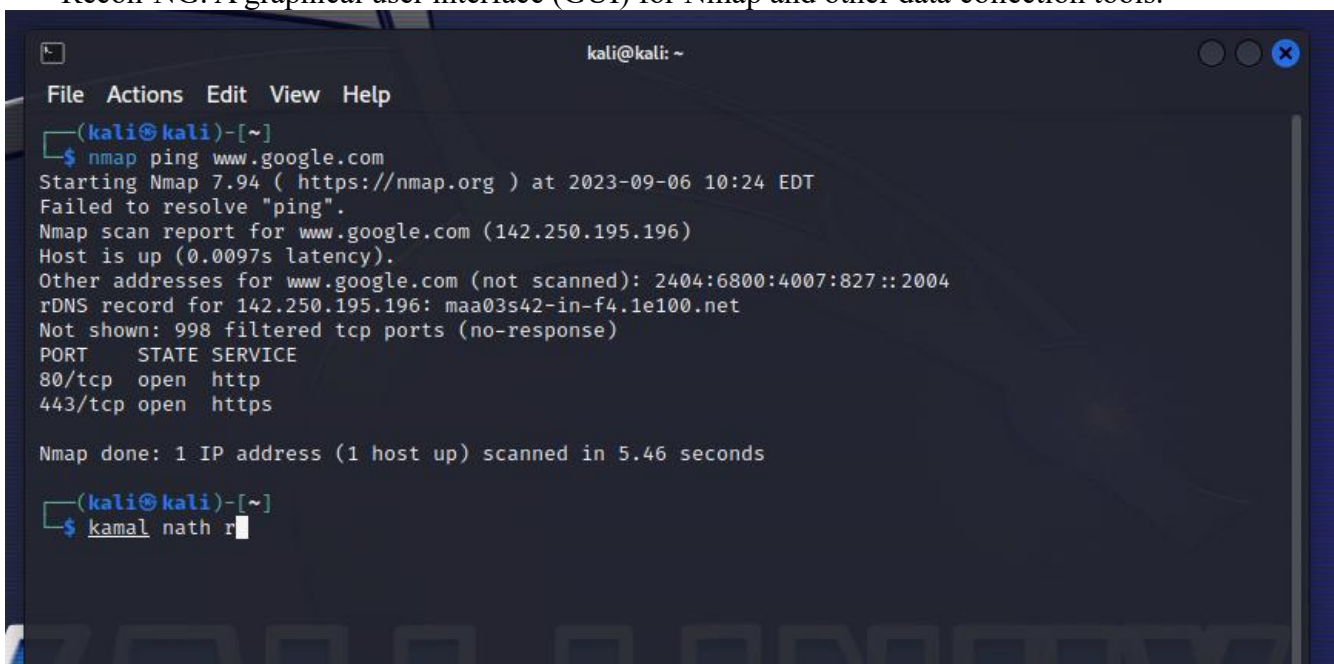
The 11 different tool categories in Kali Linux are listed below, along with a brief description of each one's purpose:

1. Tools for information collecting are used to obtain data on a target system, including its IP address, operating system, open ports, and active services. Utilizing this knowledge, an attack can be planned and weaknesses found. Several common methods for acquiring information are:

A network can be scanned for open ports and active services using the port scanner Nmap.

* TheHarvester: A device for gathering email addresses, social media profiles, and other data on a target.

* Recon-NG: A graphical user interface (GUI) for Nmap and other data collection tools.

A screenshot of a terminal window titled 'kali@kali: ~'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows a command prompt '(kali@kali)-[~]' followed by the command '\$ nmap ping www.google.com'. The output of the command is as follows:

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 10:24 EDT
Failed to resolve "ping".
Nmap scan report for www.google.com (142.250.195.196)
Host is up (0.0097s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4007:827::2004
rDNS record for 142.250.195.196: maa03s42-in-f4.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.46 seconds
```

Below the output, the prompt '(kali@kali)-[~]' is shown again, followed by the command '\$ kamal nath r' with a cursor at the end.

2. Tools for vulnerability analysis are used to find weaknesses in a target system. The system can be accessed and the vulnerabilities exploited using this knowledge. The following are some well-known vulnerability analysis tools:

* Nessus: A paid vulnerability scanner that can look for a variety of vulnerabilities.

* An open-source vulnerability scanner similar to Nessus is called OpenVAS.

* Metasploit: A penetration testing framework with numerous exploit modules and vulnerability scanners.

3. Tools for analyzing web apps are used to check their security. Finding security holes like as cross-site scripting (XSS), SQL injection, and unsecured direct object references are part of this process. The

*Burp Suite, a complete online application security testing suite, is one of the more well-known web application analysis tools.

* OWASP ZAP: A free and open-source scanner for online application security.

* Nikto: A scanner for web servers that can be used to find security holes.

4. Database assessment tools are used to check the databases' security. Finding security holes like SQL injection and unauthorized access are part of this. Some well-known database evaluation tools are:

* SQLMap, which allows for automated SQL injection assaults.

* DBPwned: A program that can be used to find compromised databases.

* MySQLTuner: A utility for optimizing the security of MySQL databases.

5. Tools used in password attacks are used to break passwords. Numerous techniques, including brute-force attacks, dictionary attacks, and rainbow tables, can be used to do this. Some well-known tools for password attacks are:

* John the Ripper, a prominent password cracker that may be used to break passwords in a number of different ways.

* Hydra: A program that enables the use of brute-force attacks on a number of services.

* Aircrack-ng: a program that decrypts Wi-Fi passwords.

6. Tools used in wireless attacks are used to target wireless networks. This entails locating wireless network weaknesses and using them to your advantage in order to enter the network. A few well-known wireless attack tools are:

* Aircrack-ng, which can be used to decipher Wi-Fi passwords.

* Kismet: A program for spotting and keeping tabs on wireless networks.

* Wireshark: A packet analyzer with the ability to record and examine wireless traffic.

7. Software application code can be analyzed using reverse engineering techniques. It is possible to do this to find code flaws and create exploits for them.

*IDA Pro, a for-profit reverse engineering tool;

*Ghidra, a free and open-source reverse engineering framework;

*Radare2, a free and open-source reverse engineering tool; and others are some of the most well-known reverse engineering tools.

8. Exploitation tools are employed to take advantage of holes in the target system. One might do this to get access to the system or to seize control of it. A few well-known exploitation tools are:

- * Metasploit, a penetration testing framework with several exploit modules.
- * A database of exploits for various vulnerabilities is called the exploit-db.
- * PacketStorm Security: This website provides access to a number of security tools, such as exploit modules.

9. Network data is recorded and altered using techniques called "sniffing and spoofing." This can be used to commit denial-of-service attacks or steal sensitive data. The following are some well-known tools for sniffing and spoofing network traffic:

- * Wireshark: A packet analyzer that can be used to record and examine network data;
- * tcpdump: A command-line packet analyzer;
- * ettercap: A program that can be used to sniff and spoof network traffic.

10. Post exploitation tools are utilized to keep a hacked system accessible. This comprises instruments for installing backdoors, obtaining information from the system, and sustaining persistence. The following are some well-known post-exploitation tools:

- * Meterpreter, a post-exploitation framework that comes with Metasploit.

Name: Kamalnath R
Reg No: 21BCE2844
Department: CSE