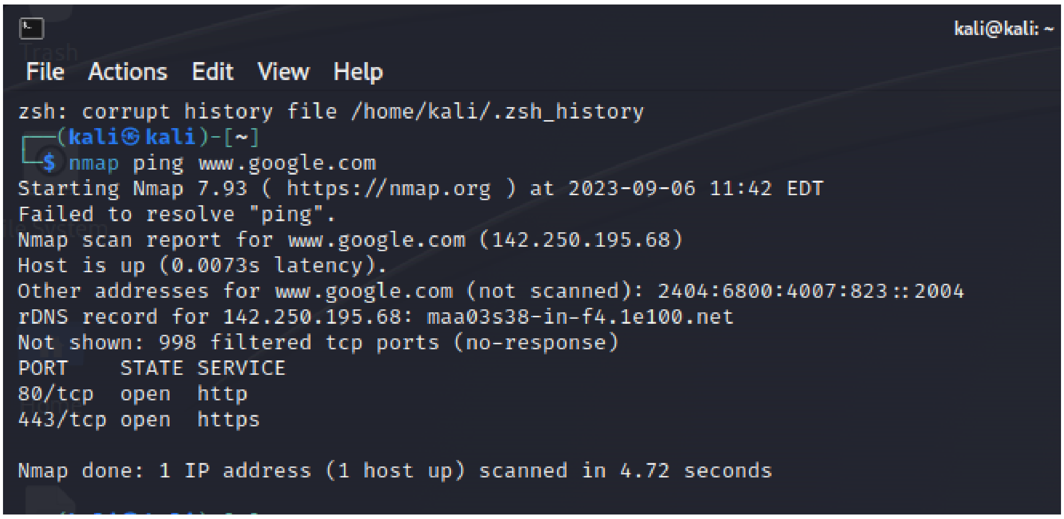
ASSIGNMENT 2

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

1. Information gathering tools: The IP address, operating system, open ports, and active services of a target system are all collected using information gathering tools. This information can be utilised to locate weak points and formulate an attack strategy. Among the often used tools for information collecting are:

- TheHarvester, which can be used to acquire email addresses, social media profiles, and other details about a target;
- Nmap, a port scanner that can be used to search a network for open ports and active services.
- Recon-NG is a graphical user interface (GUI) for Nmap and other tools for data collection.



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nmap ping www.google.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-06 11:42 EDT
Failed to resolve "ping".
Nmap scan report for www.google.com (142.250.195.68)
Host is up (0.0073s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4007:823::2004
rDNS record for 142.250.195.68: maa03s38-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 4.72 seconds
```

2. Vulnerability analysis tools: To find weaknesses in a target system, vulnerability analysis techniques are utilised. 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.
- Metasploit: A penetration testing framework with numerous exploit modules and vulnerability scanners.

3. Web application analysis tools: Tools for web application analysis are employed to evaluate the security of web applications. Cross-site scripting (XSS), SQL injection, and unsafe direct object references are a few examples of the vulnerabilities that must be found. The following are some well-known web application analysis tools:

- Burp Suite: A complete web application security testing suite.
- OWASP ZAP: A free tool for scanning web applications for security.
- Nikto: A web server vulnerability scanner that can be used to find holes in web servers.

4. Database assessment tools: Tools for database assessment are employed to evaluate the security of databases. Finding security holes like SQL injection and unauthorised access are part of this. Several well-liked database evaluation tools are:

- SQLMap: An instrument for automating SQL injection attacks is SQLMap.
- DBPwned: A programme that can be used to find compromised databases.
- MySQLTuner: A utility for optimising the security of MySQL databases.

5. Password attacks tools: are used to crack passwords. Numerous techniques, including brute-force attacks, dictionary attacks, and rainbow tables, can be used to do this. Several well-known tools for password assaults are:

- John the Ripper: Popular password breaker John the Ripper may be used to break passwords using a number of techniques.
- Hydra: A tool that enables the use of brute-force attacks against a number of services is called Hydra.
- Aircrack-ng: Wi-Fi passwords can be broken using Aircrack-ng.

6. Wireless attacks tools: To attack wireless networks, one must employ wireless attack tools. This entails locating wireless network weaknesses and using them to your advantage in order to enter the network. Several well-known wireless assault tools are:

- Aircrack-ng: Wi-Fi passwords can be broken using Aircrack-ng.
- Kismet: A programme for spotting and keeping tabs on wireless networks.
- Wireshark: Use the packet analyzer Wireshark to record and examine wireless traffic.

7. Reverse engineering tools: Tools for "reverse engineering" are used to examine a software application's source code. It is possible to do this to find code flaws and create exploits for them. Several well-liked reverse engineering instruments are:

- Ghidra: A framework for free and open-source reverse engineering.
- IDA Pro: An industrial reverse engineering tool is IDA Pro.
- Radare2: A free and open-source reverse engineering tool called Radare2.

8. Exploitation tools: To exploit weaknesses in a target system, one uses exploitation tools. One might do this to get access to the system or to seize control of it. Popular exploitation tools are as follows:

- Metasploit: Several exploit modules are included in the penetration testing framework known as Metasploit.
- Exploit-db: A database of exploits for various vulnerabilities is called the "exploit-db."
- PacketStorm Security: An online resource for security tools, such as exploit modules, is PacketStorm Security.

9. Sniffing and spoofing tools: Tools called "sniffing and spoofing" are used to intercept and alter network communication. This can be used to commit denial-of-service attacks or steal sensitive data. Several well-known sniffer and spoofing tools are:

- Wireshark: Use the packet analyzer Wireshark to record and examine wireless traffic.
- tcpdump: A command-line packet analyzer is tcpdump.
- ettercap: A device for sniffing and forging network communication.

10. Post exploitation tools: Tools called "post exploitation" are employed to keep a hacked system accessible. This comprises instruments for installing backdoors, obtaining information from the system, and sustaining persistence. Popular post-exploitation tools are as follows:

- Metasploit includes a post-exploitation framework called Meterpreter.

11. Forensics tools: To collect and examine data from a computer system or network, forensics tools are utilised. Investigating security incidents like malware infections or data breaches can be done using this evidence. Popular forensics instruments include:

- Sleuth Kit: A collection of tools for gathering and examining digital forensic data is called the Sleuth Kit.

- Forensic Toolkit: A commercial forensic suite called Forensic Toolkit (FTK) has a number of tools for analysing digital evidence.

- EnCase: A different for-profit forensic software package with a number of features for examining digital evidence.

Name: Tharunya Bala S

Reg. No.: 21BCE0076