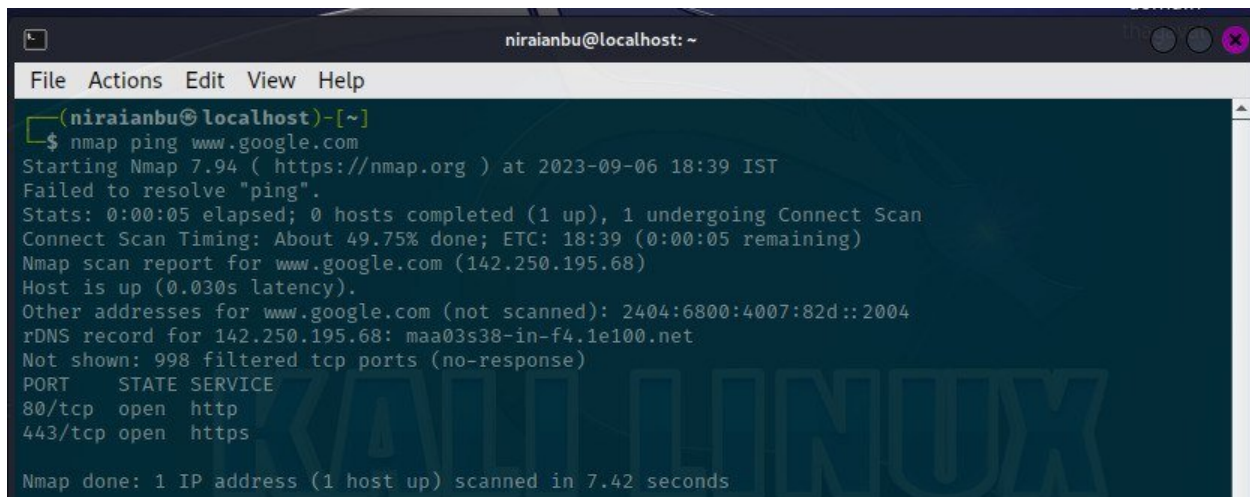


Assignment -2

1. **Information gathering tools** are used to collect information about a target system, such as its IP address, operating system, open ports, and running services. This information can be used to identify vulnerabilities and plan an attack. Some popular information gathering tools include:

- * Nmap: A port scanner that can be used to scan a network for open ports and running services.
- * TheHarvester: A tool that can be used to collect email addresses, social media profiles, and other information about a target.
- * Recon-NG: A graphical user interface (GUI) for Nmap and other information gathering tools.

A screenshot of a terminal window titled 'niraianbu@localhost: ~'. The terminal shows the command '\$ nmap ping www.google.com' being executed. The output indicates that the host is up and provides details about the scan, including the IP address 142.250.195.68 and open ports 80/tcp (http) and 443/tcp (https). The terminal also shows a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'.

```
niraianbu@localhost: ~  
File Actions Edit View Help  
~(niraianbu@localhost)-[~]  
$ nmap ping www.google.com  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-06 18:39 IST  
Failed to resolve "ping".  
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan  
Connect Scan Timing: About 49.75% done; ETC: 18:39 (0:00:05 remaining)  
Nmap scan report for www.google.com (142.250.195.68)  
Host is up (0.030s latency).  
Other addresses for www.google.com (not scanned): 2404:6800:4007:82d::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 7.42 seconds
```

Tool used – nmap

2. **Vulnerability analysis tools** are used to identify vulnerabilities in a target system. This information can be used to exploit the vulnerabilities and gain access to the system. Some popular vulnerability analysis tools include:

- * Nessus: A commercial vulnerability scanner that can scan for a wide range of vulnerabilities.
- * OpenVAS: An open-source vulnerability scanner that is similar to Nessus.
- * Metasploit: A penetration testing framework that includes a number of vulnerability scanners and exploit modules.

3. Web application analysis tools are used to test the security of web applications.

This includes identifying vulnerabilities such as cross-site scripting (XSS), SQL injection, and insecure direct object references. Some popular web application analysis tools include:

- * Burp Suite: A comprehensive web application security testing suite.
- * OWASP ZAP: An open-source web application security scanner.
- * Nikto: A web server scanner that can be used to identify vulnerabilities in web servers.

4. Database assessment tools are used to test the security of databases. This includes identifying vulnerabilities such as SQL injection and unauthorized access.

Some popular database assessment tools include:

- * SQLMap: A tool that can be used to automate SQL injection attacks.
- * DBPwned: A tool that can be used to identify databases that have been compromised.
- * MySQLTuner: A tool that can be used to tune MySQL databases for security.

5. Password attacks tools are used to crack passwords. This can be done using a variety of methods, such as brute-force attacks, dictionary attacks, and rainbow tables.

Some popular password attacks tools include:

- * John the Ripper: A popular password cracker that can be used to crack passwords using a variety of methods.
- * Hydra: A tool that can be used to perform brute-force attacks against a variety of services.
- * Aircrack-ng: A tool that can be used to crack Wi-Fi passwords.

6. Wireless attacks tools are used to attack wireless networks. This includes identifying vulnerabilities in wireless networks and exploiting them to gain access to the network. Some popular wireless attacks tools include:

- * Aircrack-ng: A tool that can be used to crack Wi-Fi passwords.
- * Kismet: A tool that can be used to detect and monitor wireless networks.
- * Wireshark: A packet analyzer that can be used to capture and analyze wireless traffic.

7. Reverse engineering tools are used to analyze the code of a software application.

This can be done to identify vulnerabilities in the code or to develop exploits for the vulnerabilities. Some popular reverse engineering tools include:

- * Ghidra: A free and open-source reverse engineering framework.
- * IDA Pro: A commercial reverse engineering tool.
- * Radare2: A free and open-source reverse engineering tool.

are used to exploit vulnerabilities in a target system. This can be done to gain access to the system or to take control of the system. Some popular exploitation tools include:

- * Metasploit: A penetration testing framework that includes a number of exploit modules.
- * Exploit-db: A database of exploits for a variety of vulnerabilities.
- * PacketStorm Security: A website that hosts a variety of security tools, including exploit modules.

9. Sniffing and spoofing tools are used to capture and modify network traffic. This can be used to steal sensitive information or to launch denial-of-service attacks. Some popular sniffing and spoofing tools include:

- * Wireshark: A packet analyzer that can be used to capture and analyze network traffic.
- * tcpdump: A command-line packet analyzer.
- * ettercap: A tool that can be used to sniff and spoof network traffic.

10. Post exploitation tools are used to maintain access to a compromised system.

This includes tools for gathering information from the system, installing backdoors, and maintaining persistence. Some popular post exploitation tools include:

- * Meterpreter: A post exploitation framework that is included with Metasploit.

11. Forensics tools are used to gather and analyze evidence from a computer system or network. This evidence can be used to investigate security incidents, such as data breaches or malware infections. Some popular forensics tools include:

- **The Sleuth Kit:** A suite of tools for extracting and analyzing digital forensic data.

- **Forensic Toolkit (FTK):** A commercial forensic suite that includes a variety of tools for analyzing digital evidence.
- **EnCase:** Another commercial forensic suite that includes a variety of tools for analyzing digital evidence.