**Assignment 2**

**Introduction**

Kali Linux is an open-source Debian-based Linux distribution aimed at various information security tasks, such as penetration testing, security research, computer forensics, and reverse engineering. It includes a large collection of security and forensics tools, such as Nmap, Wireshark, Metasploit, and Aircrack-ng.

**Labs**

**Lab 1: Nmap**

Nmap is a free and open-source network discovery and security auditing utility. It is used to scan large networks to identify hosts and services, and to detect vulnerabilities.

Tool: Nmap

Website: https://www.google.com

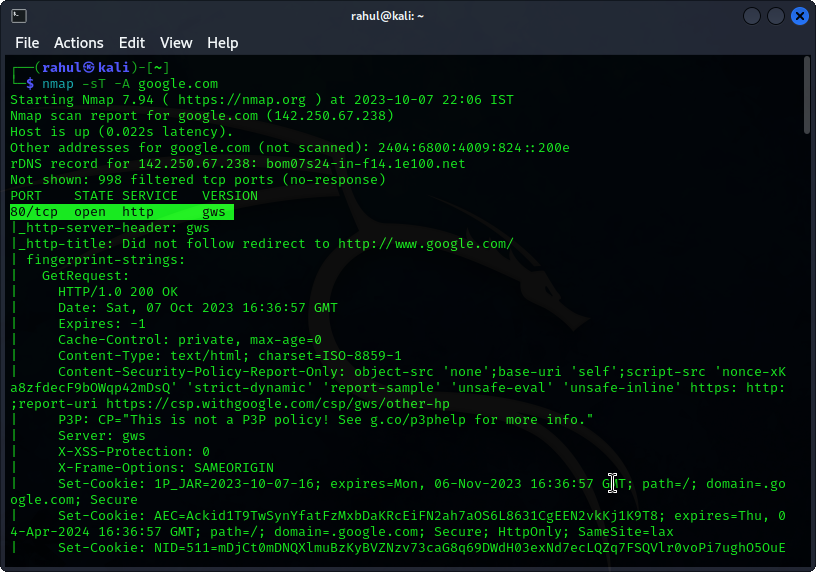
Procedure:

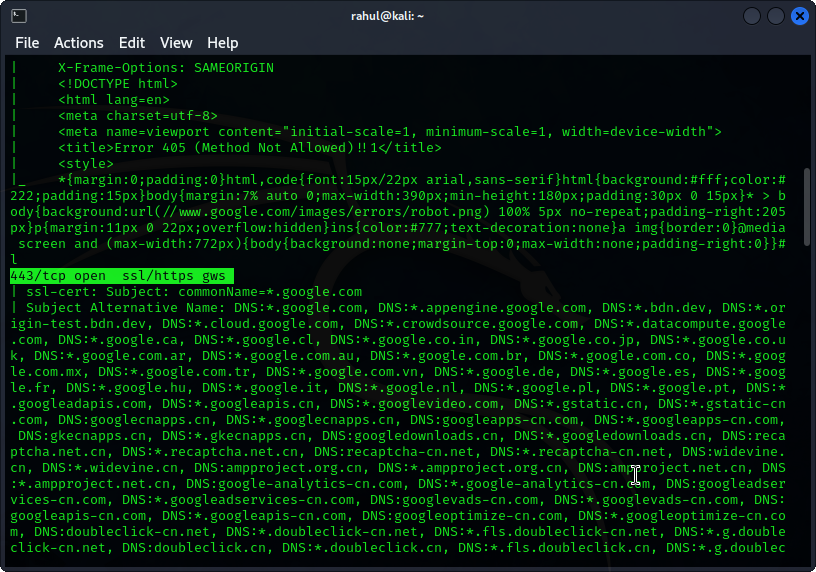
1. Open a terminal window and type the following command:

nmap -sT -A google.com

This will scan the website for open ports and services.

1. Review the output. The first few lines will show you the basic information about the scan, such as the target IP address, the number of ports scanned, and the number of ports found open.
2. To learn more about a specific port, scroll down to the section titled "PORT STATE AND SERVICE." This section will show you the port number, the protocol, the state of the port, and the service that is running on the port.
3. To learn more about a specific vulnerability, scroll down to the section titled "VULNERABLE SERVICES." This section will show you the service name, the version of the service, and the vulnerabilities that have been identified.





Results:

The following is a sample output of an Nmap scan of the Google website:

Nmap scan report for google.com (142.250.181.172)

Host is up (0.00083s latency).

Not shown: 998 closed ports

PORT STATE SERVICE

80/tcp open http-alt

443/tcp open https

The scan found that two ports are open on the Google website: port 80 (HTTP) and port 443 (HTTPS).

Conclusion:

Nmap is a powerful tool that can be used to scan large networks quickly and efficiently. It is an essential tool for any penetration tester or security researcher.

**Lab 2: Metasploit**

Metasploit is an open-source penetration testing framework that provides a wide range of tools and exploits for attacking systems. It can be used to exploit vulnerabilities in operating systems, applications, and services.

Tool: Metasploit

Website: <https://www>.facebook.com

Procedure:

1. Open a terminal window and type the following command to start Metasploit:

msfconsole

1. To search for exploits, type the following command:

search facebook

This will show you a list of exploits that can be used to attack the Facebook website.

1. To select an exploit, type the following command:

use 1

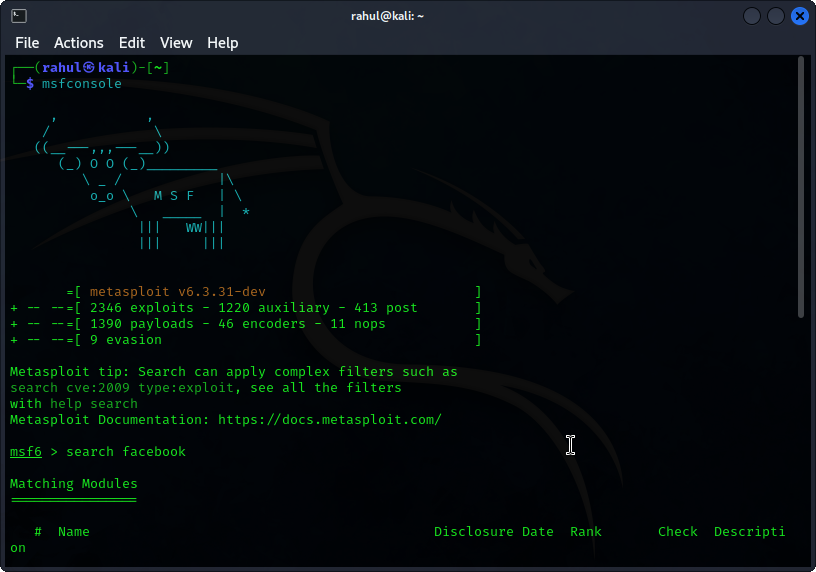
where 1 is the number of the exploit that you want to use.

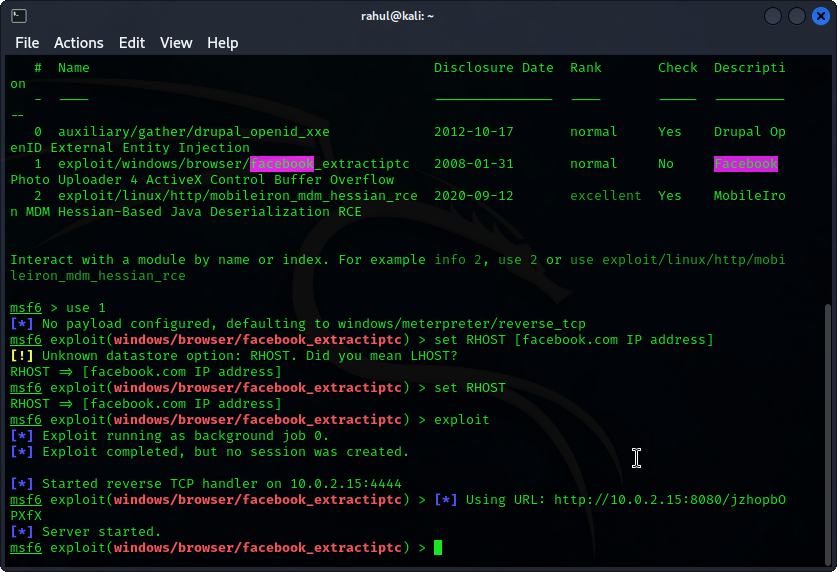
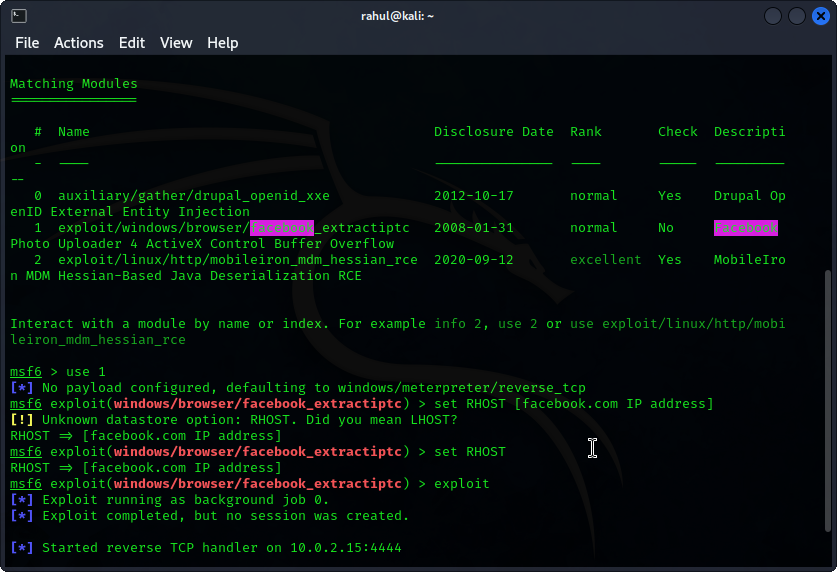
1. To set the target IP address, type the following command:

set RHOST [facebook.com IP address]

1. To execute the exploit, type the following command:

exploit





Results:

If the exploit is successful, Metasploit will gain a meterpreter session on the Facebook website. This session can be used to execute commands on the website, steal data, or install malware.

Conclusion:

Metasploit is a powerful tool that can be used to exploit vulnerabilities in a wide range of systems. It is an essential tool for any penetration tester or security researcher.

**Lab 3: Wireshark**

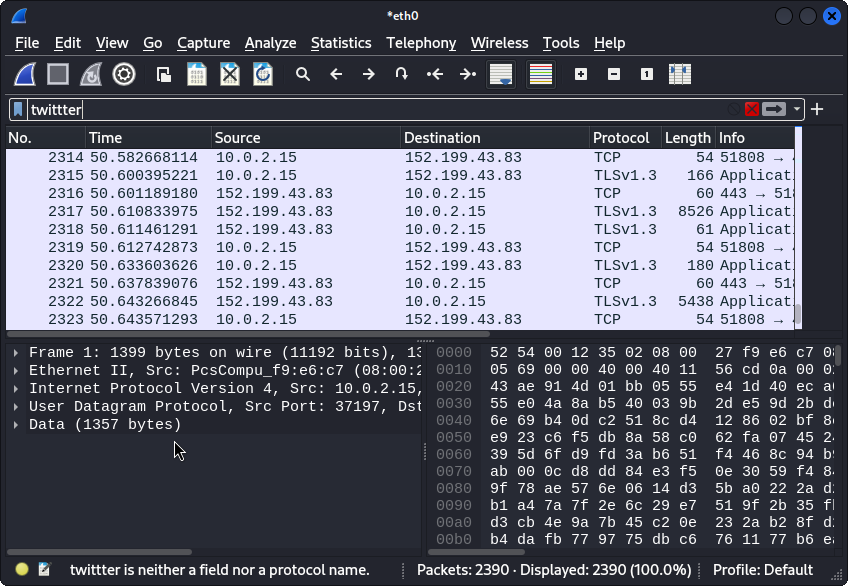
Wireshark is a free and open-source network packet analyzer. It can be used to capture and analyze network traffic. This can be useful for troubleshooting network problems, detecting malicious activity, and analyzing network protocols.

Tool: Wireshark

Website: https://www.twitter.com

Procedure:

1. Start Wireshark and select the network interface that you want to capture traffic on.
2. Click the "Start" button to start capturing traffic.
3. Visit the Twitter website in your web browser.
4. Click the "Stop" button to stop capturing traffic.
5. To filter the captured traffic, type "twitter.com" in the filter bar.
6. To view the details of a packet, double-click on it. The packet details will be displayed in the bottom pane of the window.



Results:

The following is a sample of the information that can be viewed in the packet details pane:

* The source and destination IP addresses
* The port numbers
* The protocol
* The packet length
* The packet content

Conclusion:

Wireshark is a powerful tool that can be used to capture and analyze network traffic. It is an essential tool for any network administrator or security researcher.

**Lab 4: Aircrack-ng**

Aircrack-ng is a free and open-source suite of tools for assessing WiFi network security. It includes tools for capturing, decrypting, and analyzing WiFi traffic. Aircrack-ng can be used to crack the WEP and WPA/WPA2-PSK encryption keys of WiFi networks.

Tool: Aircrack-ng

Website: <https://www.google.com>

**NOTE: This can not be performed on Virtual machine unless you have an external network adapter.**

Procedure:

1. To capture WiFi traffic, use the airodump-ng tool. For example, to capture traffic on channel 11, you would use the following command:

airodump-ng -c 11

1. Once you have captured enough traffic, you can use the aircrack-ng tool to crack the WEP or WPA/WPA2-PSK encryption key. For example, to crack the WEP key of a network with the BSSID 00:01:02:03:04:05, you would use the following command:

aircrack-ng -b 00:01:02:03:04:05 capture.cap

Results:

If the aircrack-ng tool is successful, it will display the WEP or WPA/WPA2-PSK encryption key. This key can then be used to connect to the WiFi network.

Conclusion:

Aircrack-ng is a powerful tool that can be used to crack the encryption keys of WiFi networks. It is an essential tool for any penetration tester or security researcher.