

**Batch: A2 Roll No.:16010421073 Experiment No.:3**

**Aim:** Experimenting with Kali.



**Resources needed: Pentesting set up**



**Theory:**

Kali Linux, a robust and specialized Linux distribution, stands as a beacon in cybersecurity, particularly for Vulnerability Assessment and Penetration Testing (VAPT). This purpose-built platform is meticulously crafted to equip security professionals and ethical hackers with a comprehensive suite of tools, allowing them to simulate real-world cyber threats in a controlled and ethical manner.

Kali Linux, derived from Debian, is tailored for VAPT, a proactive approach to securing information systems. The distribution integrates many pre-installed security tools covering every facet of the testing process. This includes reconnaissance, vulnerability identification, exploitation, post-exploitation analysis, and reporting. The ecosystem enables security experts to comprehensively assess the resilience of networks, applications, and systems against potential threats.

Core Tools and Capabilities:

1. Nmap - Unveiling Network Landscapes:

Nmap, the cornerstone of network exploration, is instrumental in mapping out hosts, identifying open ports, and scrutinizing services. Its flexibility allows practitioners to conduct scans such as SYN scans for stealth, UDP scans for unconventional protocols, and version detection for granular insights into target systems.

1. OpenVAS - Unearthing Vulnerabilities:

OpenVAS, integrated into Kali Linux, transforms the vulnerability assessment landscape. By employing a database of known vulnerabilities, it systematically scans target systems, providing a detailed report on potential weaknesses. Security professionals can leverage this information to address and mitigate risks proactively.

1. Metasploit - The Art of Exploitation:

Metasploit, a potent penetration testing framework, enables security practitioners to simulate cyber-attacks. Its vast collection of exploits and payloads caters to a diverse range of targets. With Metasploit, ethical hackers can validate the effectiveness of security measures and develop strategies to fortify defenses.

1. Wireshark - Decrypting Network Traffic:

Wireshark, a network protocol analyzer, dissects packets traversing the network. It aids in understanding network behavior, identifying anomalies, and uncovering potential security threats. Security professionals can utilize Wireshark to intercept and analyze communication, enhancing their ability to detect and counteract malicious activities.

1. Aircrack-ng - Securing Wireless Networks:

In the realm of wireless security, Aircrack-ng takes center stage. This toolset empowers security experts to audit and secure wireless networks. From capturing Wi-Fi handshakes to exploiting vulnerabilities in wireless protocols, Aircrack-ng is pivotal in fortifying organizations against wireless threats.

Ethical Considerations:

The exploration of Kali Linux for VAPT demands a principled approach. Practitioners must operate within the bounds of legal and ethical frameworks. Gaining proper authorization, respecting privacy, and adhering to responsible disclosure practices are paramount. The objective is not to exploit for malicious intent but to fortify defenses and cultivate a proactive security posture.



**Procedure:**

Exploring network landscapes using Nmap involves a stepwise discovery, scanning, and analysis process.

**Step 1: Install Nmap on Kali Linux**

Ensure that Nmap is installed on the Kali Linux system. If not, install it using the following command:

sudo apt-get update

sudo apt-get install nmap

**Step 2: Identify Target**

Determine the target network or IP address range to scan. This could be a specific IP address, a range of IP addresses, or an entire subnet.

**Step 3: Basic Ping Scan**

Perform a basic ping scan to identify live hosts on the network. This helps in narrowing down the scope of the scan.

nmap -sn <target>

Replace <target> with the IP address or range to scan. This command sends ICMP echo requests to discover live hosts without performing detailed port scans.

**Step 4: Port Scan for Common Ports**

Conduct a port scan to identify open ports on live hosts. This command scans the 1,000 most common ports.

nmap -p 1-1000 <target>

**Step 5: Intense Scan with Service Version Detection**

Perform a more comprehensive scan, including service version detection. This provides details about the services running on open ports.

nmap -sV <target>

**Step 6: Aggressive Scan with OS Detection**

Execute an aggressive scan that includes operating system detection. This attempts to identify the operating system of the target hosts.

nmap -A <target>

**Step 7: Output to a File**

Save the results to a file for later analysis or reporting. Replace <output\_file> with the desired file name.

nmap -A -oN <output\_file> <target>

**Step 8: Perform a Script Scan**

Nmap has a variety of scripts that can provide additional information about the target. Use the following command to default scripts against the target.

nmap -sC <target>

**Step 9: Explore UDP Ports**

Include UDP port scanning to identify services running on UDP ports.

nmap -sU <target>

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**OpenVAS**

Exploring vulnerabilities using OpenVAS involves a stepwise installation, configuration, and scanning process.

**Step 1: Install OpenVAS on Kali Linux**

Ensure that OpenVAS is installed on your Kali Linux system. You can install it using the following commands:

sudo apt-get update

sudo apt-get install openvas

During the installation, the prompt will be given to set up a password for the OpenVAS Administrator (admin).

**Step 2: Configure OpenVAS**

After installation, configure OpenVAS by running the following command:

sudo openvas-setup

Follow the prompts to set up the OpenVAS Manager, Scanner, and other components. This process may take some time as it downloads the necessary vulnerability databases.

**Step 3: Start OpenVAS Services**

Start the OpenVAS services with the following commands:

sudo systemctl start openvas-manager

sudo systemctl start openvas-scanner

sudo systemctl start openvas-gsa

Step 4: Access OpenVAS Web Interface

Open a web browser and navigate to the OpenVAS web interface using the following URL:

https://localhost:9392

Log in with the OpenVAS Administrator credentials set during the setup.

**Step 5: Update OpenVAS Feeds**

Update the vulnerability feeds to ensure that OpenVAS has the latest information. Go to the "Administration" tab and click on "Feeds." Click on the "Green Arrows" icon to update the feeds.

**Step 6: Create a Target**

Define a target for scanning. Go to the "Configuration" tab and click on "Targets." Click on the "Create Target" button and provide details such as the target's IP address or hostname.

**Step 7: Create a Task**

Create a scanning task associated with the target. Go to the "Scans" tab and click on "Tasks." Click the "Create Task" button, select the target, and configure scan parameters.

**Step 8: Run the Scan**

Initiate the vulnerability scan by selecting the created task and clicking the "Play" button. This will launch the scan against the specified target.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Metasploit**

Using Metasploit for penetration testing involves a stepwise installation, exploration, and exploitation process.

**Step 1: Install Metasploit on Kali Linux**

Ensure that Metasploit is installed on the Kali Linux system. If not, install it using the following commands:

sudo apt-get update

sudo apt-get install metasploit-framework

**Step 2:** Start Metasploit Console

Launch the Metasploit console by entering the following command in the terminal:

msfconsole

This opens the Metasploit Framework console, providing access to various modules and functionalities.

**Step 3:** Explore Modules

Explore available modules using the search command. For example, to search for exploits related to the Apache web server, type:

search apache

Review the results and select a module based on target and scenario.

**Step 4:** Select and Load an Exploit Module

Choose an exploit module from the list and load it into the Metasploit console using the use command. Replace <exploit\_module> with the name of the desired module:

use <exploit\_module>

**Step 5:** Configure the Exploit

Configure the exploit by setting the required parameters. Use the show options command to view and set the necessary options. For example:

show options

set RHOSTS <target\_IP>

set RPORT <target\_port>

**Step 6:** Verify Exploit Configuration

Double-check configuration using the *show options* command to ensure all required parameters are set correctly.

**Step 7:** Exploit the Target. Execute the exploit by typing:

exploit

This launches the attack against the target system. Metasploit will attempt to exploit the specified vulnerability.

**Step 8:** Post-Exploitation

Upon successful exploitation, the post-exploitation phase starts. Use various Metasploit commands and modules to gather information, escalate privileges, and explore the compromised system.

sysinfo

getuid

**Step 9:** Explore Post-Exploitation Modules

Use the post command to explore post-exploitation modules. These modules help in privilege escalation, data exfiltration, and lateral movement.

use post/multi/recon/local\_exploit\_suggester

**Step 10:** Generate Reports

Document findings and generate reports summarizing the penetration test. Use the db\_export command to export data to external tools for reporting.

db\_export -f xml -o /path/to/report.xml

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Output(Code with result Snapshot)**

* **Execute minimum 2 tools**

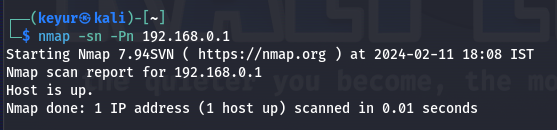
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Nmap**

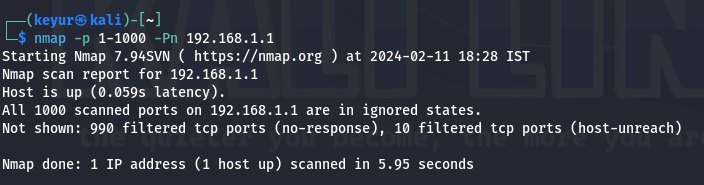
**Step 2: Identify Target**

192.168.29.1

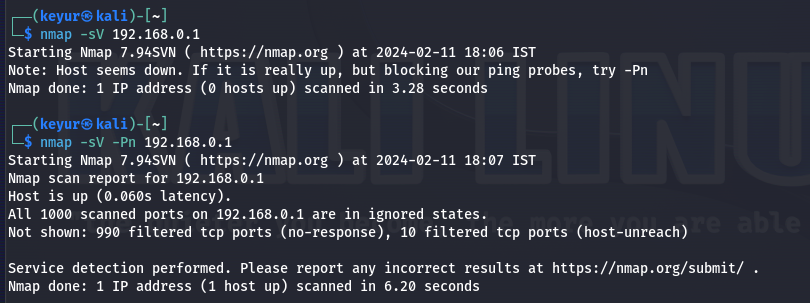
**Step 3: Basic Ping Scan**

****

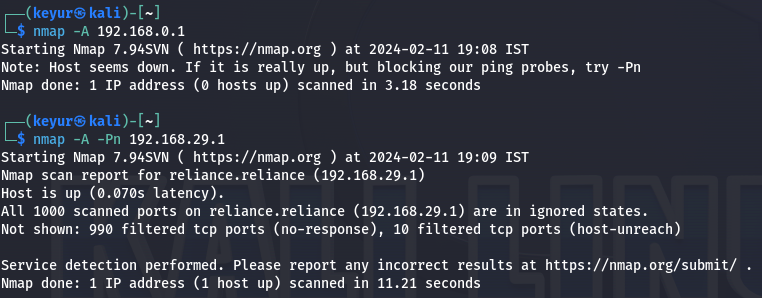
**Step 4: Port Scan for Common Ports**

****

**Step 5: Intense Scan with Service Version Detection**

****

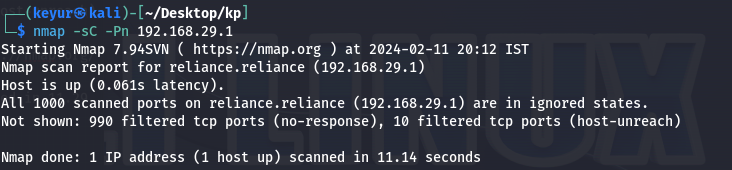
**Step 6: Aggressive Scan with OS Detection**

****

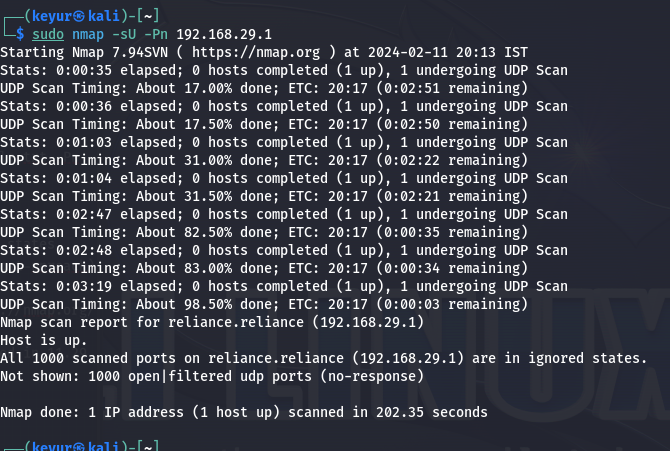
**Step 7: Output to a File**

****

**Step 8: Perform a Script Scan**

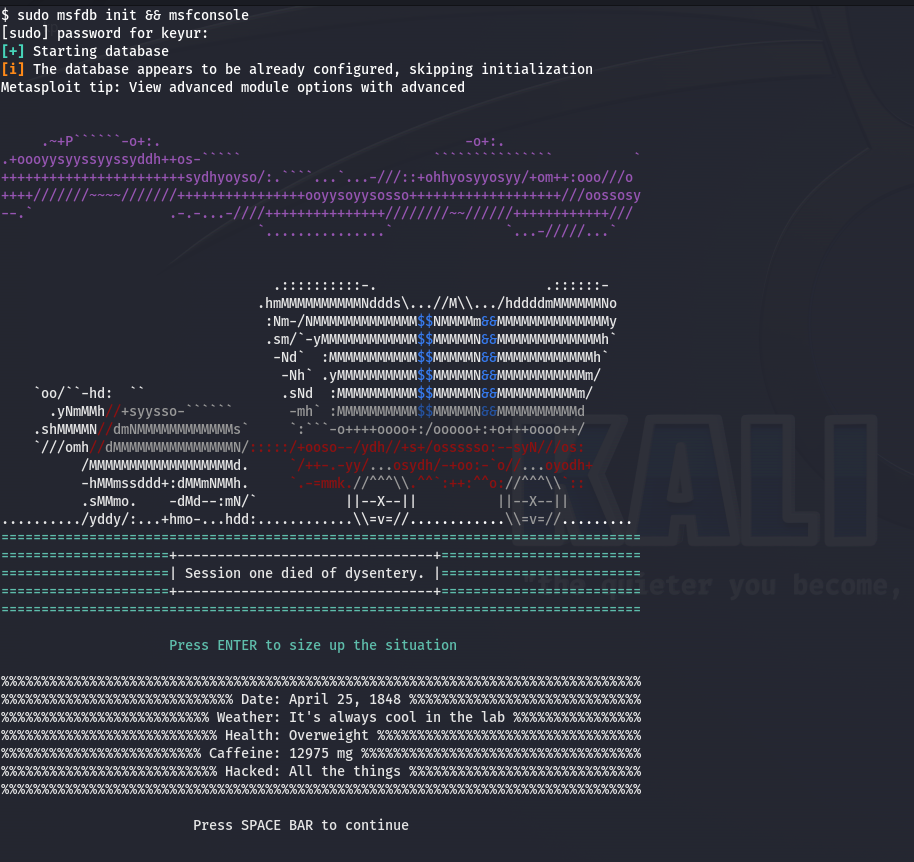
****

**Step 9: Explore UDP Ports**

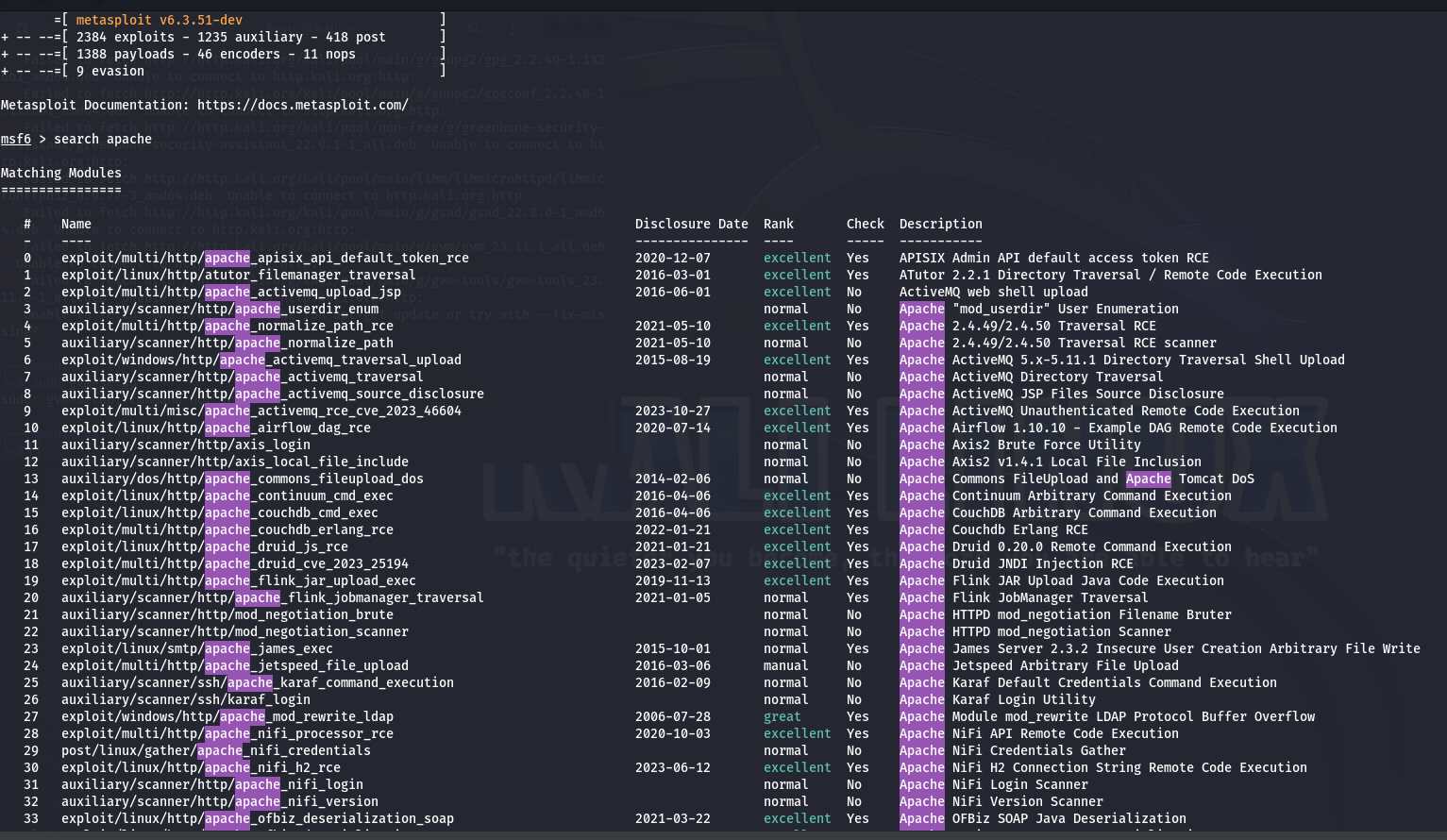
****

1. **Metasploit**

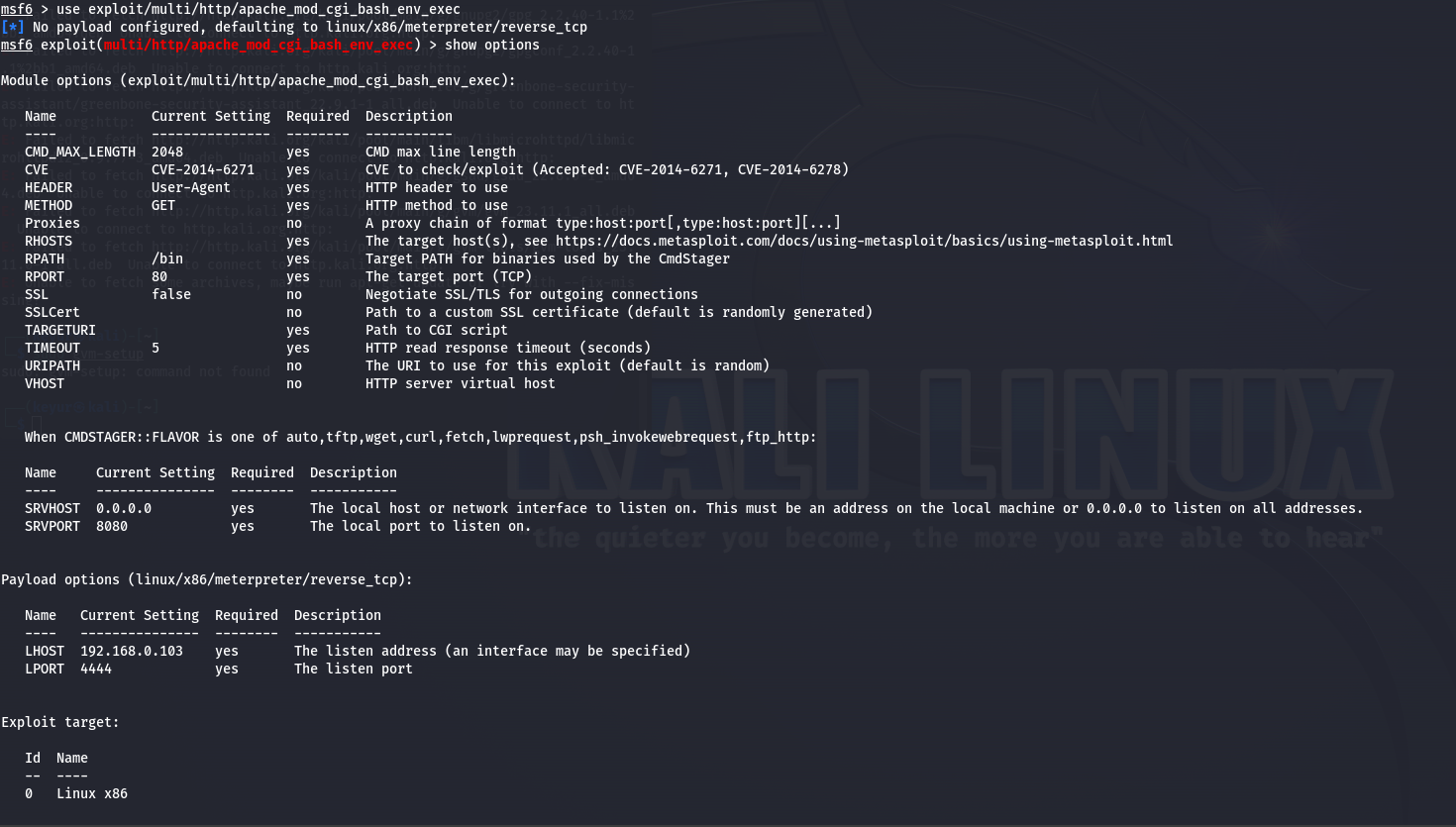
**Step 2: start msfconsole**

****

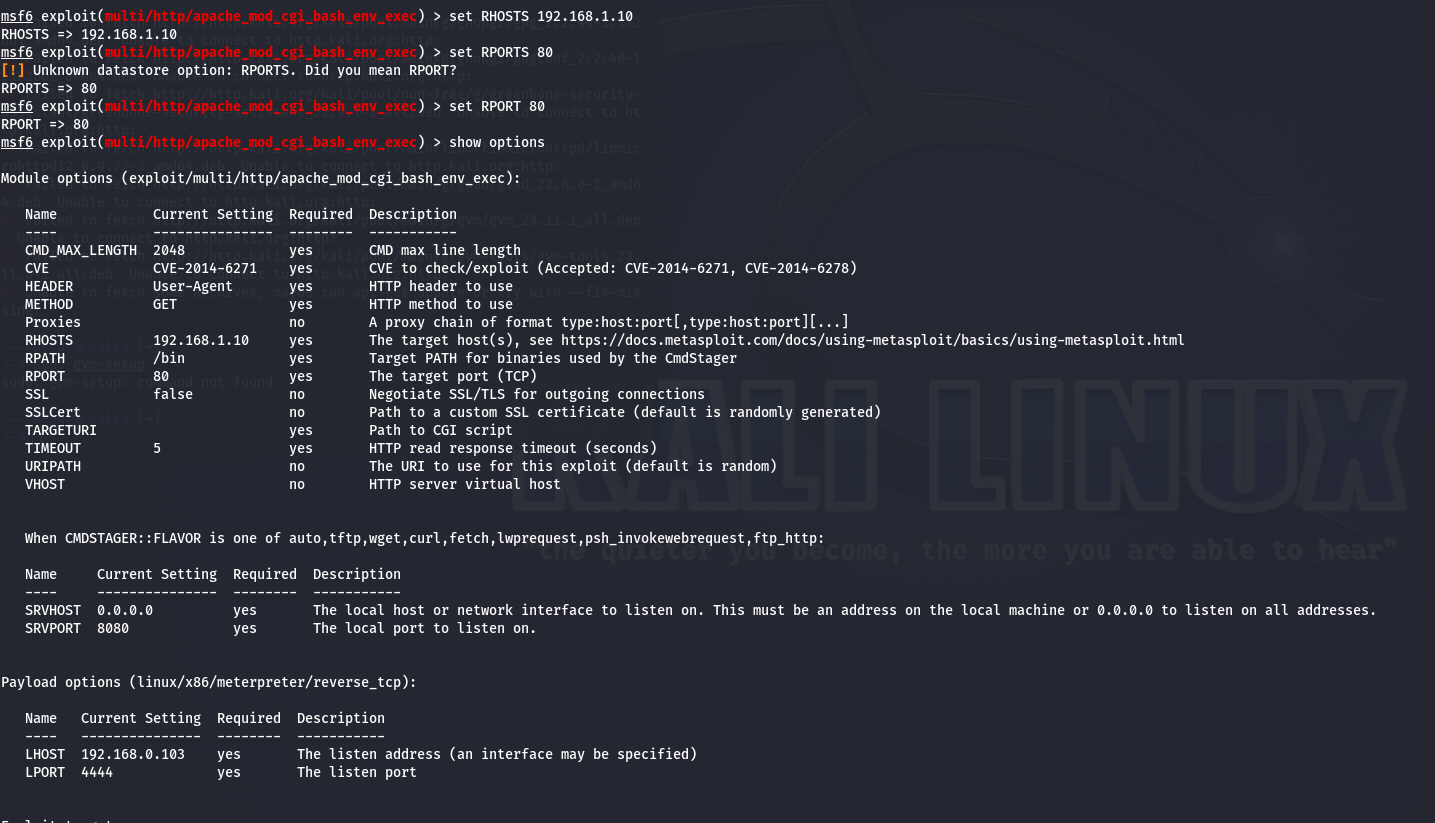
**Step 3: Explore Modules**

****

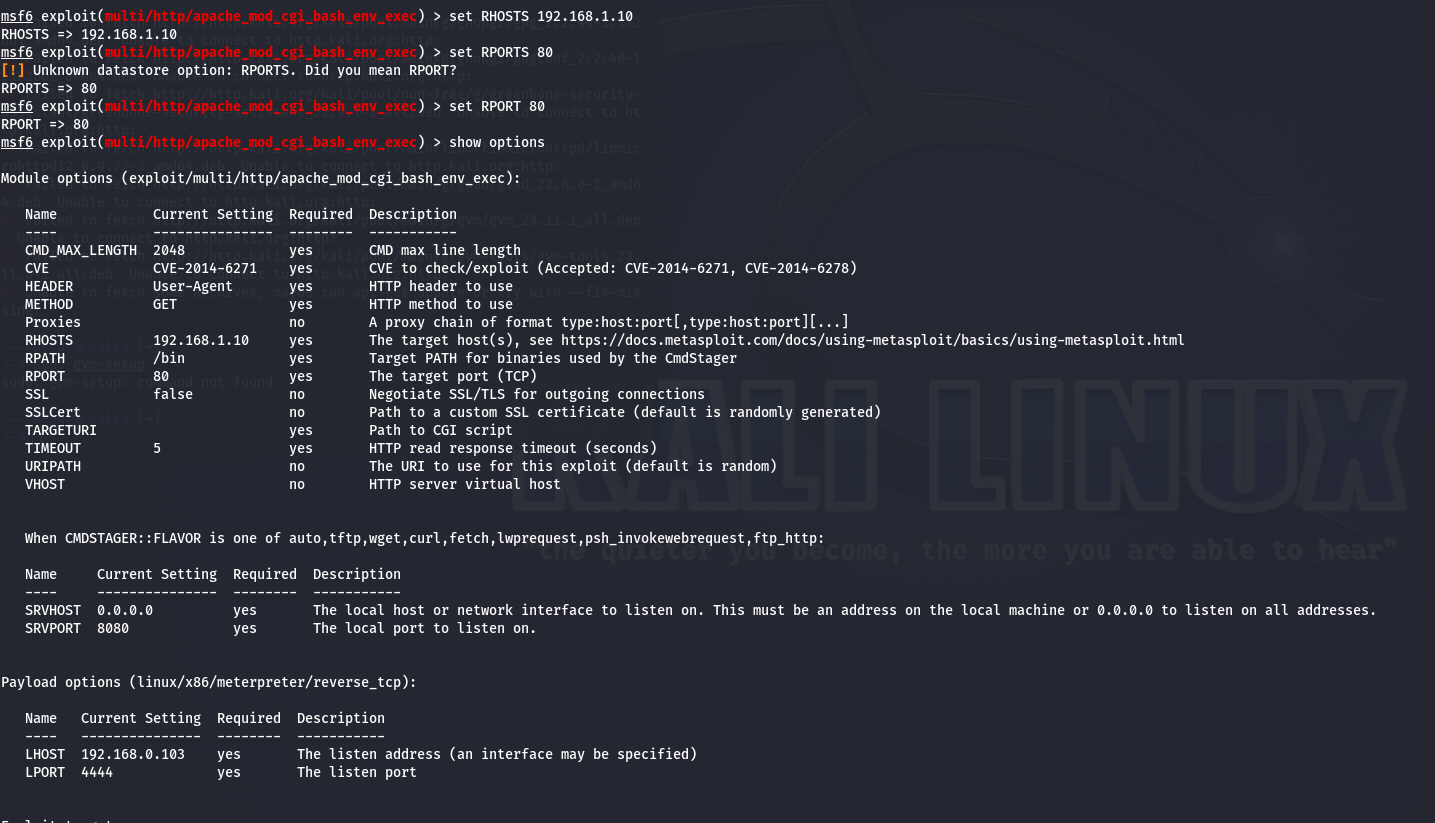
**Step 4:** Select and Load an Exploit Module



**Step 5:** Configure the Exploit



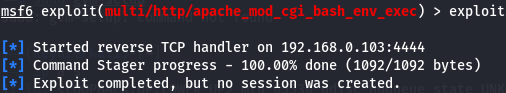
**Step 6:** Verify Exploit Configuration



**Step 7:** Exploit the Target. Execute the exploit by typing:

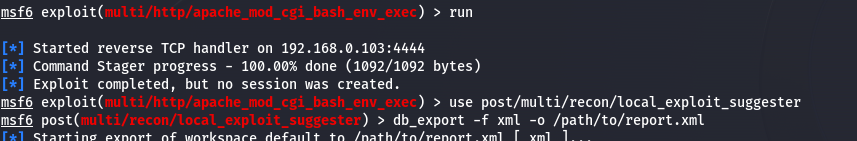
exploit



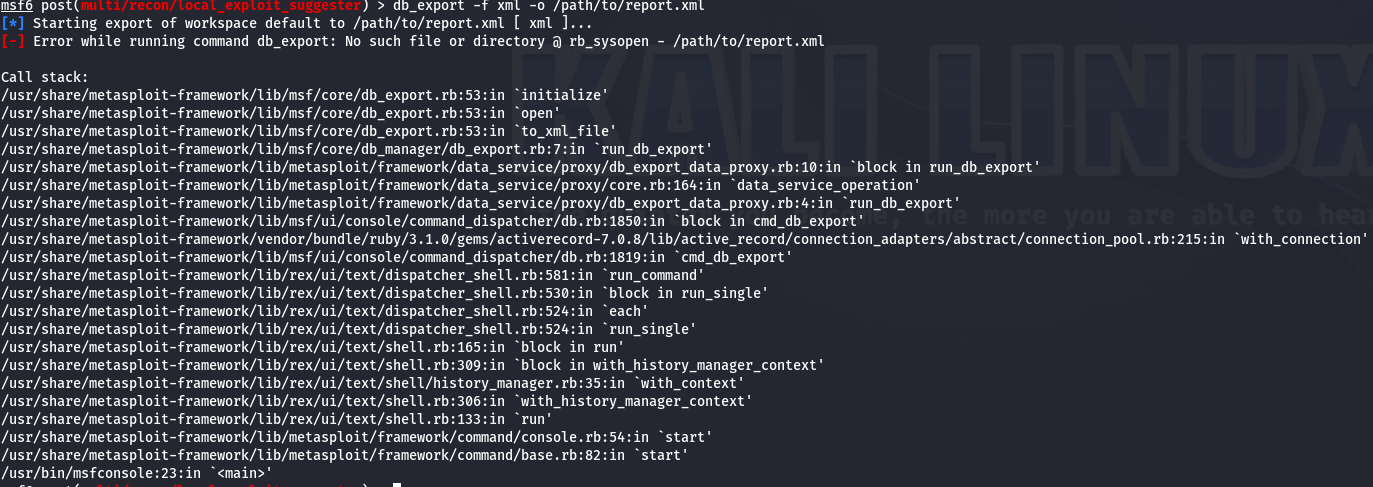


**Step 8:** Post-Exploitation

**Step 9:** Explore Post-Exploitation Modules



**Step 10:** Generate Reports



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

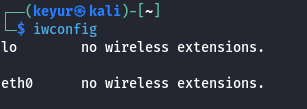
**Post Lab Questions:-**

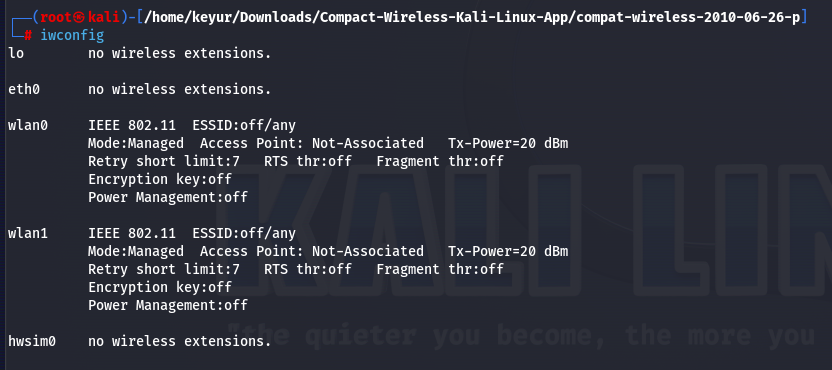
1. **You are tasked with securing a Wi-Fi network against potential attacks. You perform a wireless audit using Aircrack-ng as part of your security assessment.**

**Ans: i) Aircrack-ng**

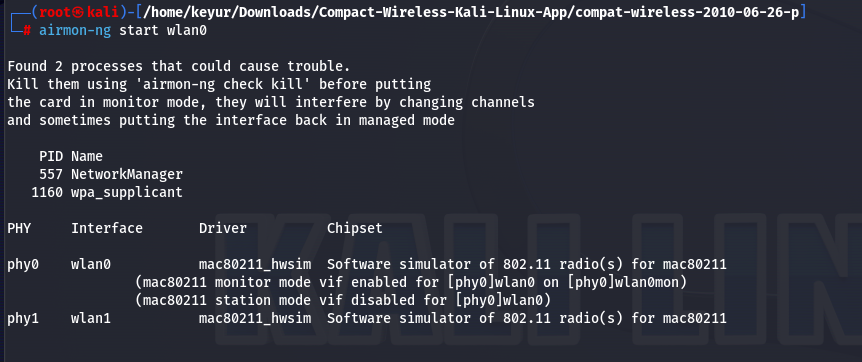


**ii) Identify the Wireless Network Interface:**

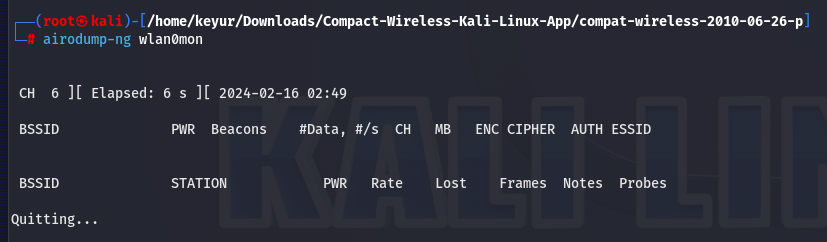


**iii) Using iwconfig command in root terminal.**

**iii) Put the Wireless Interface into Monitor Mode:**

****

**iv) Start Capturing Packets:**



1. **You are conducting a security assessment for an organization that relies heavily on wireless networks. Your goal is to identify potential vulnerabilities and weaknesses in their wireless infrastructure.**

**Ans:**  Identify the Wireless Network Interface:

**1. Information Gathering:**

* ***Network Architecture:*** Understand the layout and components of the wireless network, including access points, controllers, switches, and security appliances.
* ***Security Policies and Procedures:*** Review existing policies regarding wireless access, password management, device security, and incident response.
* ***Equipment Details:*** Obtain information about wireless access point models, firmware versions, and configuration settings.

**2. Vulnerability Scanning:**

* ***Automated Tools:*** Utilize specialized tools to scan for known vulnerabilities in access points, firmware, and network configurations.
* ***Manual Testing***: Conduct manual tests to identify misconfigurations, weak encryption protocols, and open ports on access points.

**3. Penetration Testing:**

* ***Simulate real-world attacks***: Employ techniques like password cracking, rogue access point deployment, and denial-of-service attacks to assess the network's resilience.
* ***Test for specific vulnerabilities:*** Focus on weaknesses identified during the scanning stage for deeper analysis and exploitation attempts.

**4. Wireless Traffic Analysis:**

* ***Capture and analyze wireless traffic:*** Look for unencrypted data, suspicious activity, and potential malware infections.
* ***Identify unauthorized devices:*** Detect unauthorized access points and connected devices that might pose security risks.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Outcomes:**

**CO1:** Realize that premise of vulnerability analysis and penetration testing(VAPT)

**Conclusion: (Conclusion to be based on the objectives and outcomes achieved)**

Explored various Kali-Linux core tools.

**Signature of faculty in charge with date** 

**References:**

1. https://www.guru99.com/kali-linux-tutorial.html
2. https://phoenixts.com/blog/learn-to-pen-test-with-kali-linux/
3. https://www.kali.org/docs/introduction/should-i-use-kali-linux/