**Lab Assignment - 7**

**Scenario:**

A cybersecurity expert is performing a penetration test on an Ubuntu system using Kali Linux. They start with reconnaissance by leveraging Metasploit’s port scanning modules to detect open TCP and UDP ports. After collecting necessary information, they generate a reverse shell payload with msfvenom and deploy it on the target. To gain access, they utilize Metasploit’s multi/handler module to capture the connection and interact with the compromised system via Meterpreter. During post-exploitation, the tester experiments with various Metasploit payloads to identify the most effective way to maintain access and execute commands on the target machine.

**Question:**

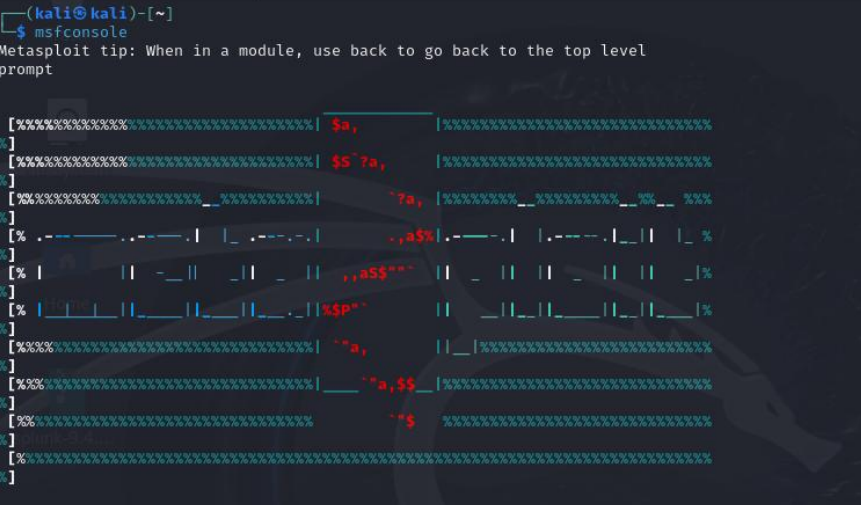
Outline the step-by-step process followed by a penetration tester when using Metasploit, starting from reconnaissance and moving through exploitation to post-exploitation. Provide the relevant commands and modules used in each stage. Additionally, research and describe at least three alternative Metasploit payloads (excluding reverse TCP) and explain how they are utilized in penetration testing scenarios.

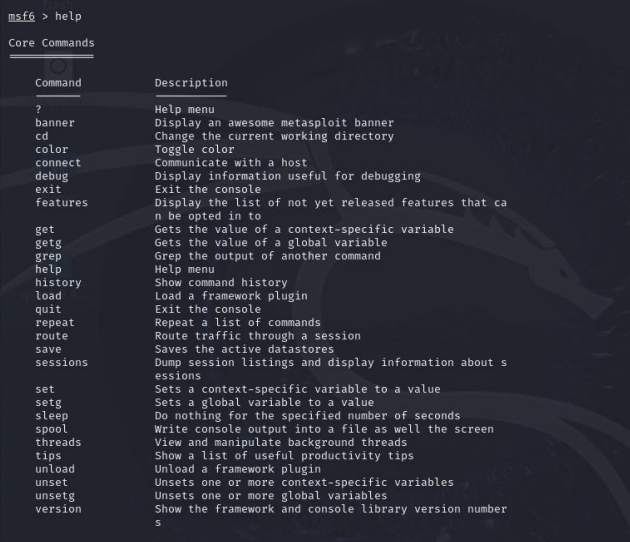
**Metasploit** is a robust framework designed for penetration testing and vulnerability exploitation. It offers a wide range of modules for reconnaissance, exploitation, post-exploitation, and privilege escalation. Supporting different payload types such as reverse shells, bind shells, and Meterpreter, it streamlines attacks through automation. Additionally, Metasploit seamlessly integrates with tools like Nmap and Burp Suite, enhancing its effectiveness in security assessments.

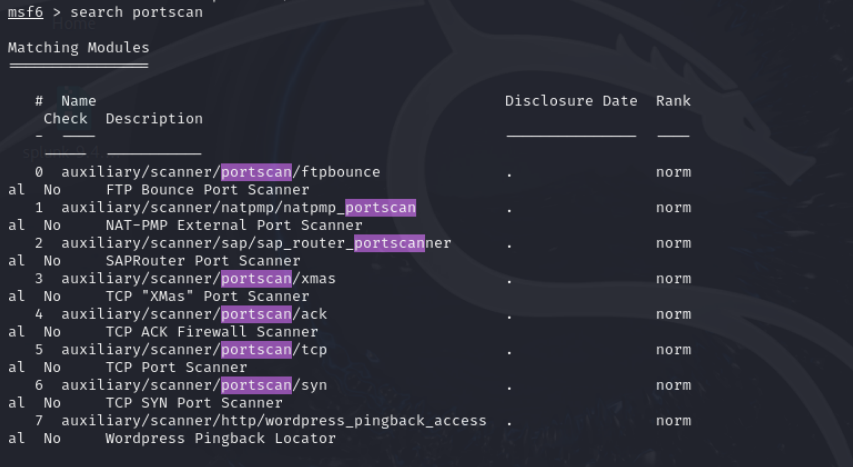
The **msfconsole** serves as the main command-line interface for Metasploit, providing an interactive environment for searching, configuring, and executing exploits. It features tab completion, scripting capabilities, and database integration to streamline workflow management. Key commands such as use, set, exploit, and sessions enable testers to navigate and manage compromised systems

10.0.2.15 – Ubuntu (ip)

10.0.2.4 – Kali (ip)

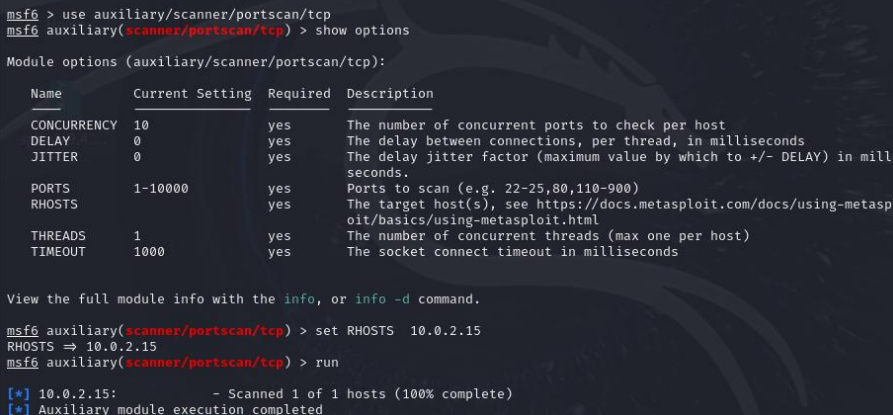




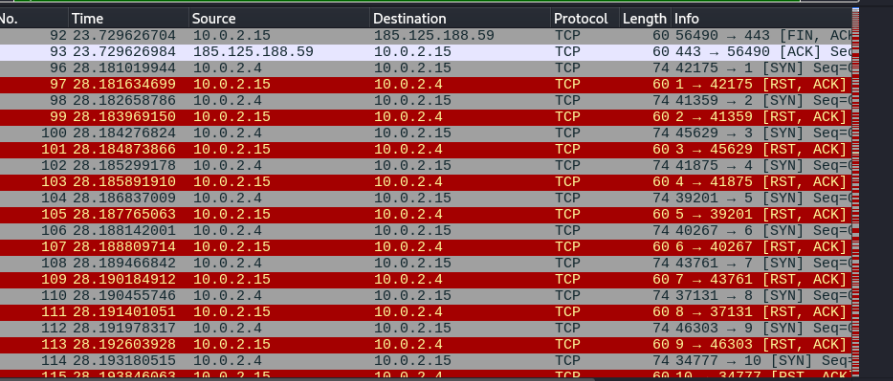


Use search portscan in msfconsole to find scanning modules. Common ones include tcp, udp, and syn scanners. Select a module with use, set target with set RHOSTS , and start scanning with run.

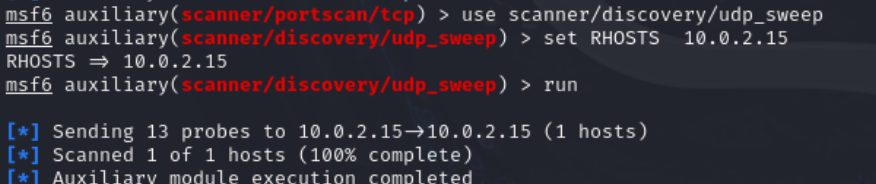
**Tcp Portscan**



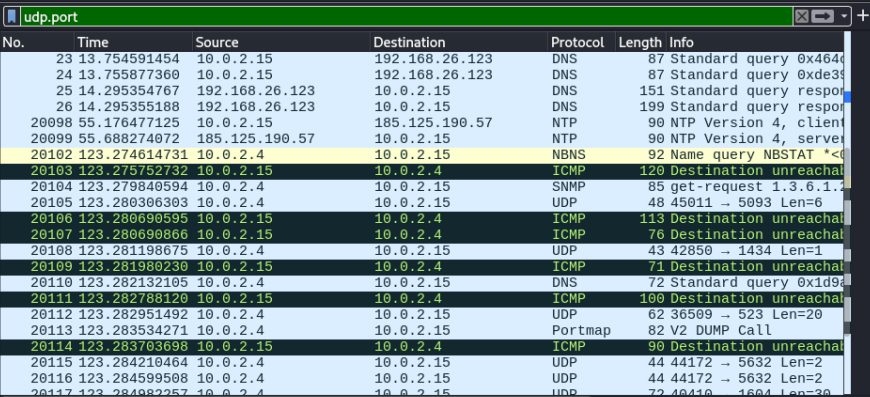
The auxiliary/scanner/portscan/tcp module in Metasploit performs a full TCP connect scan, completing the 3-way handshake (SYN, SYN-ACK, ACK) for each tested port. It provides reliable results but is more detectable than a SYN scan.



udp sweep



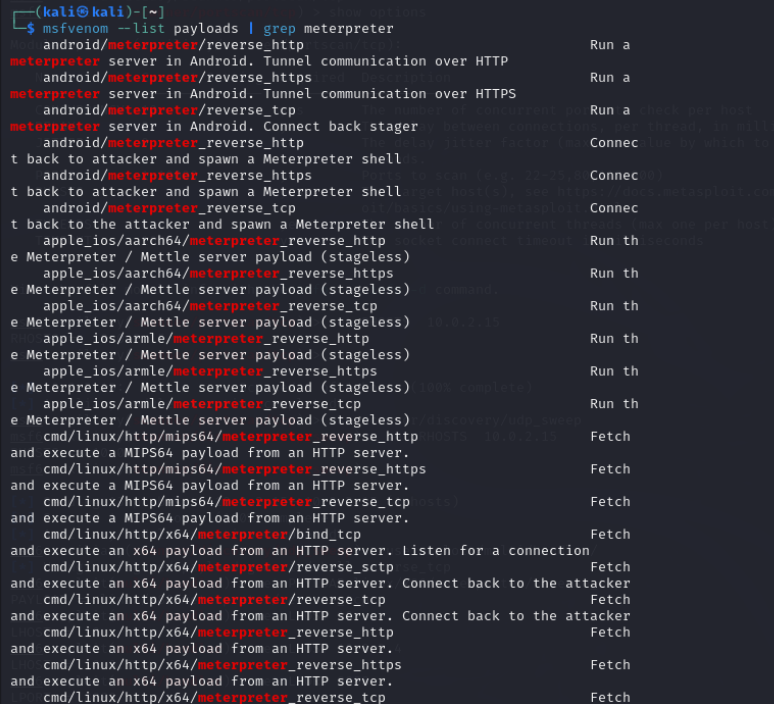
The scanner/discovery/udp\_sweep module in Metasploit is used to scan UDP ports on a target system. Unlike TCP, UDP does not establish a three-way handshake, making port detection dependent on responses or timeouts. As a result, UDP scanning is generally less reliable compared to TCP scans.

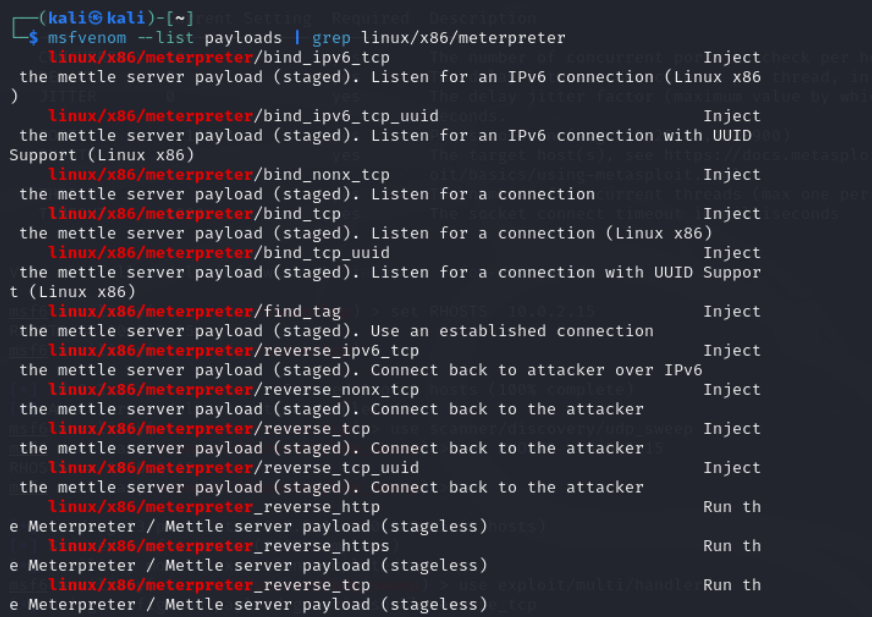


**Msfvenom & Meterpreter**

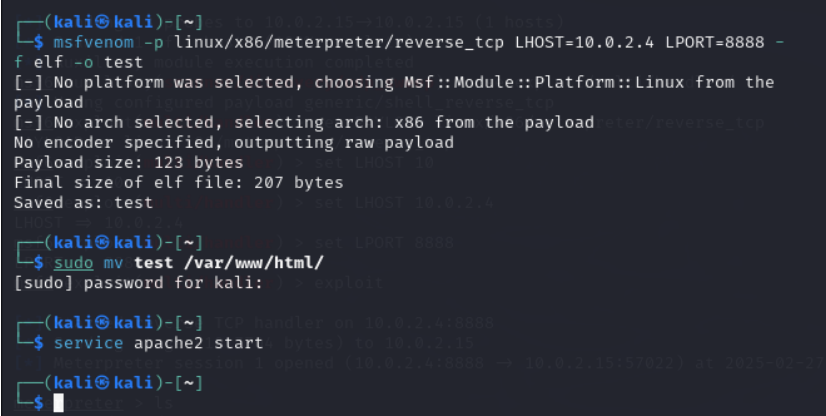
• **msfvenom** is a Metasploit tool used to generate and encode payloads for exploitation. It combines the functionality of msfpayload and msfencode into a single command-line utility. It supports various formats like EXE, ELF, APK, and raw shellcode for different target platforms.

• **Meterpreter** is an advanced, interactive payload in Metasploit that provides inmemory execution without writing files to disk, making it stealthy. It supports command execution, privilege escalation, file transfer, keylogging, webcam capture, and pivoting.

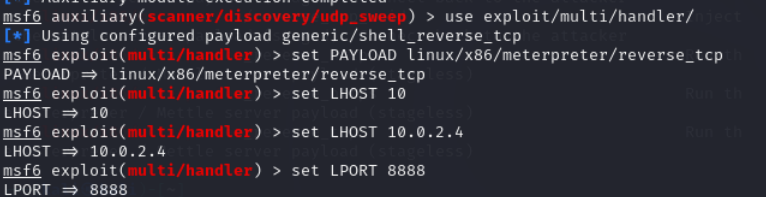




Reverse shell acquiring



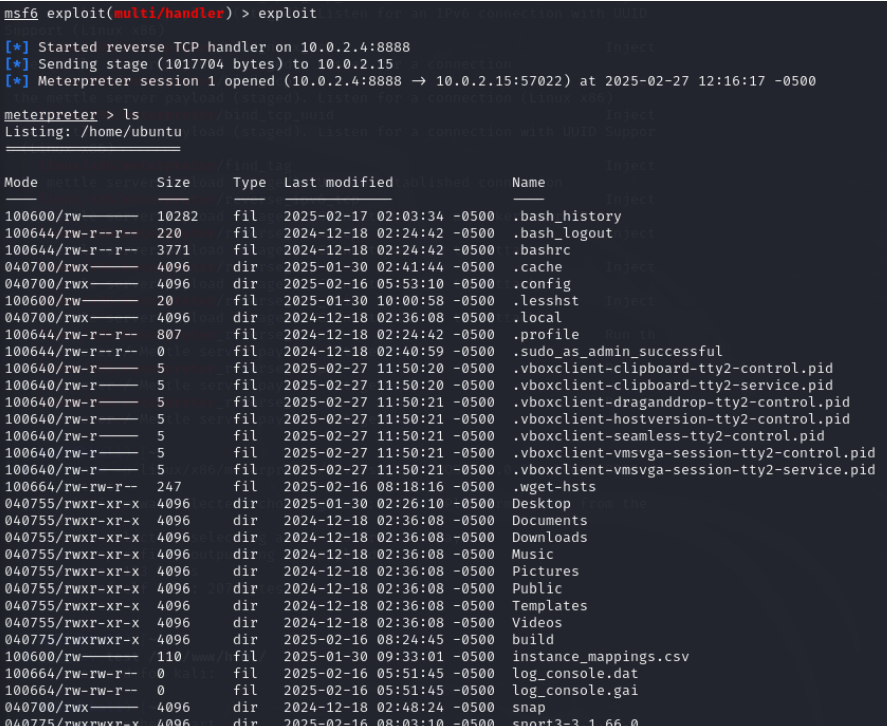
The payload is generated using msfvenom with the linux/x86/meterpreter/reverse\_tcp payload, specifying the attacker's IP (10.0.0.10) and port (7777). The output format is ELF, and the payload is saved as test. The generated file is moved to /var/www/html/ to be served via an HTTP server. The Apache web server is started to host the payload. This allows the target machine to download the file using wget.



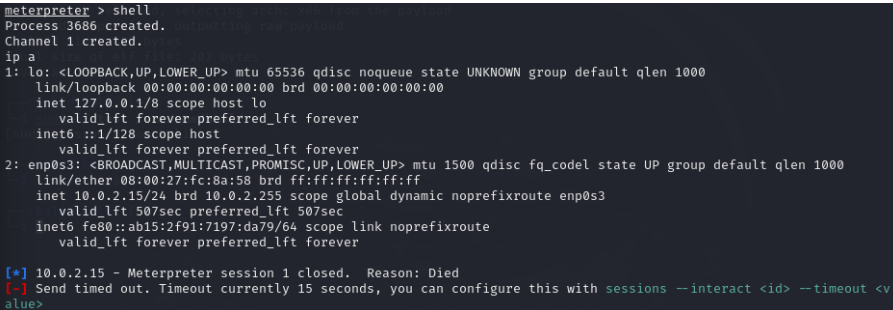
In Metasploit, the multi/handler module is used to listen for incoming connections. The payload is set to match the one generated earlier, with the same LHOST (10.0.2.4) and LPORT (8888).



The target machine downloads the payload from http://10.0.2.4/test using wget. Initially, execution is denied due to missing permissions, so chmod +x test is used to make it executable. The payload is then executed.



Metasploit’s handler receives the reverse shell connection, and a Meterpreter session is opened. The ls command lists the files in the compromised user's home directory, confirming access.



A Meterpreter shell is opened on the target, allowing command execution. The whoami command confirms the user context, and ip a displays network configuration, showing the target’s IP (10.0.2.15).