Assignment One

REPORT OPENSSH4.7

Eng : MUSTAFA ALI

Name: Abdelrahaman Salah Abdelraham Aboaresha

1. Vulnerability Name

OpenSSH 4.7p1 – Weak Authentication / Credential-Based Access

---

2. Affected Service

- **Service:** OpenSSH
- **Version:** 4.7p1
- **Port:** 22/tcp
- **Protocol:** SSH

---

3. Vulnerability Description

OpenSSH version 4.7p1 is considered an outdated SSH service that may be vulnerable to security weaknesses such as weak authentication configurations and poor credential management. In vulnerable systems like Metasploitable 2, default or easily guessable credentials can allow attackers to gain unauthorized remote access through SSH.

This vulnerability does not rely on exploiting memory corruption or buffer overflow, but rather on **misconfiguration and weak credentials**, which can lead to full system compromise.

---

4. Impact

If successfully exploited, this vulnerability allows an attacker to:

- Gain unauthorized access to the target system
- Execute commands remotely
- Obtain a remote shell on the victim machine
- Perform privilege escalation attacks
- Compromise system confidentiality and integrity

---

5. Attack Vector

- **Type:** Remote
- **Authentication Required:** Yes (weak/default credentials)
- **User Interaction:** None

---

6. Exploitation Method

The attacker connects to the SSH service using valid credentials. In the lab environment, weak default credentials (msfadmin : msfadmin) were used to successfully authenticate and execute commands on the target system.

Metasploit modules such as SSH login scanners can be used to automate this process.

---

7. Tools Used

- Kali Linux
- Metasploit Framework
- SSH Client

---

8. Severity

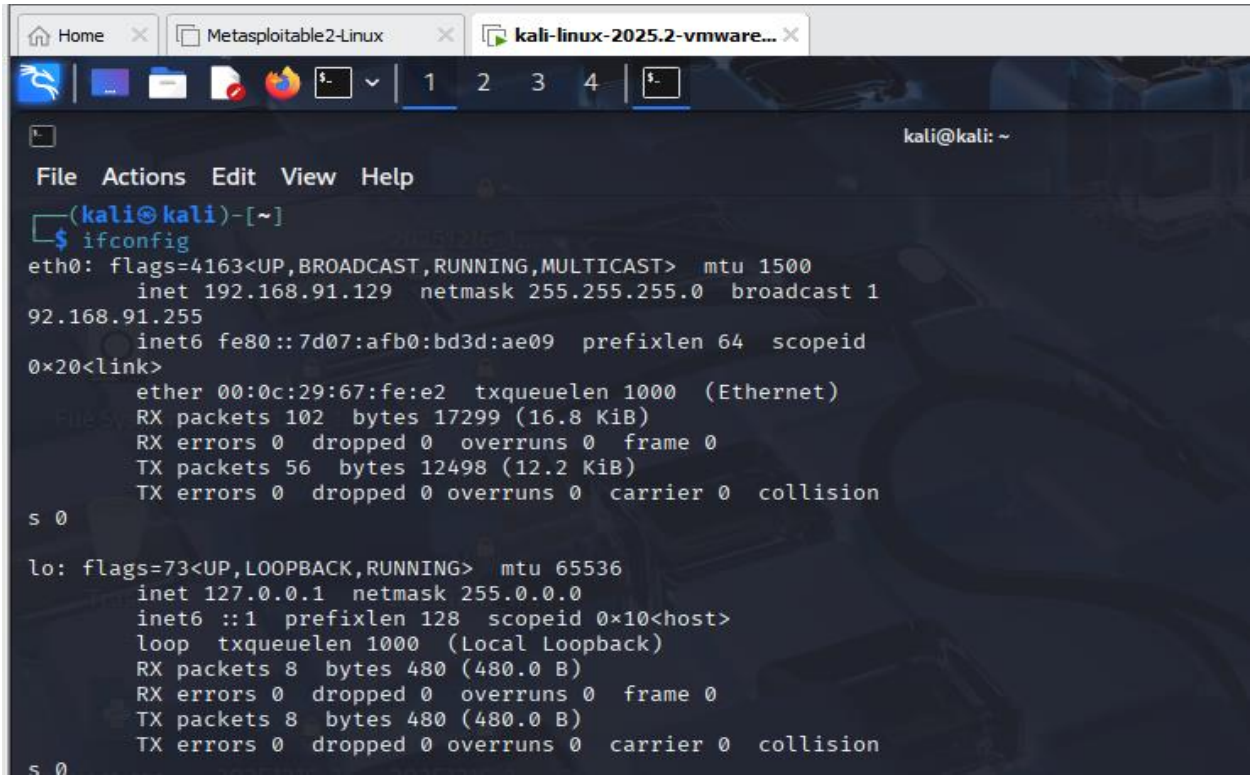
Medium to High

The severity depends on the strength of credentials and system configuration. In cases where default or weak passwords are used, the risk becomes high.

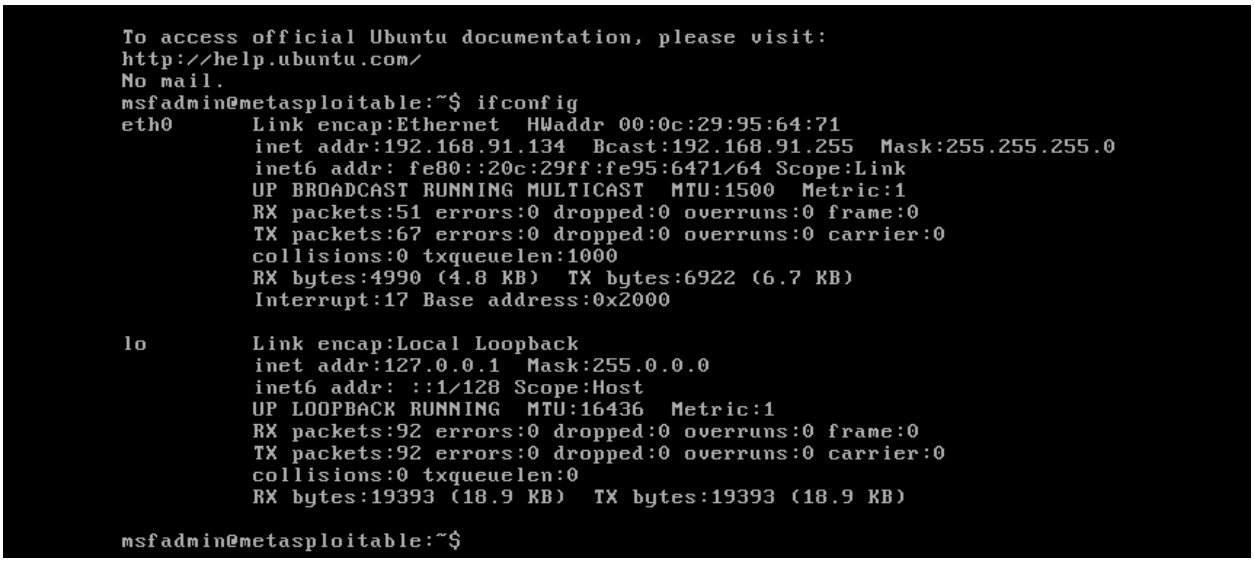
1-Identification IP

1- **ifconfig** Used to display the network interfaces and IP address of the Kali machine, which is required to set `LHOST` for reverse connections in Metasploit.

Ip of Kali Machine = 192.168.91.129



Ip of Metasploit Machine = 192.168.91.134



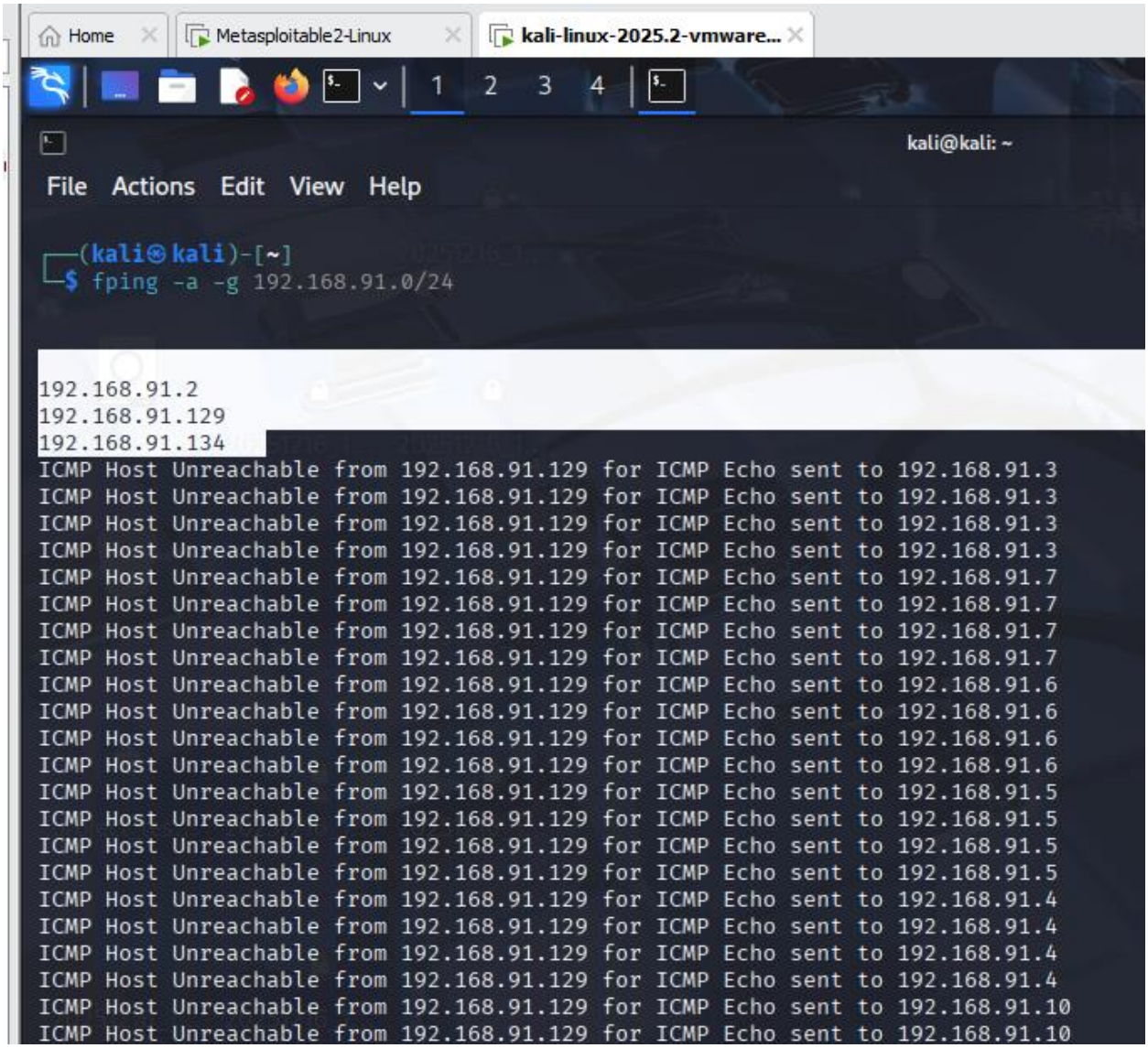
2-**Ping Sweep** technique for network scanning , which sends ICMP requests to multiple IP addresses to know which are Online (Up) or Offline

Command : fping -a -g 192.168.91.0/24

We find Three Hosts Up

Ip=192.168.91.2 ip=192.168.91.129 ip= 192.168.91.134

And Other is Unreacjable

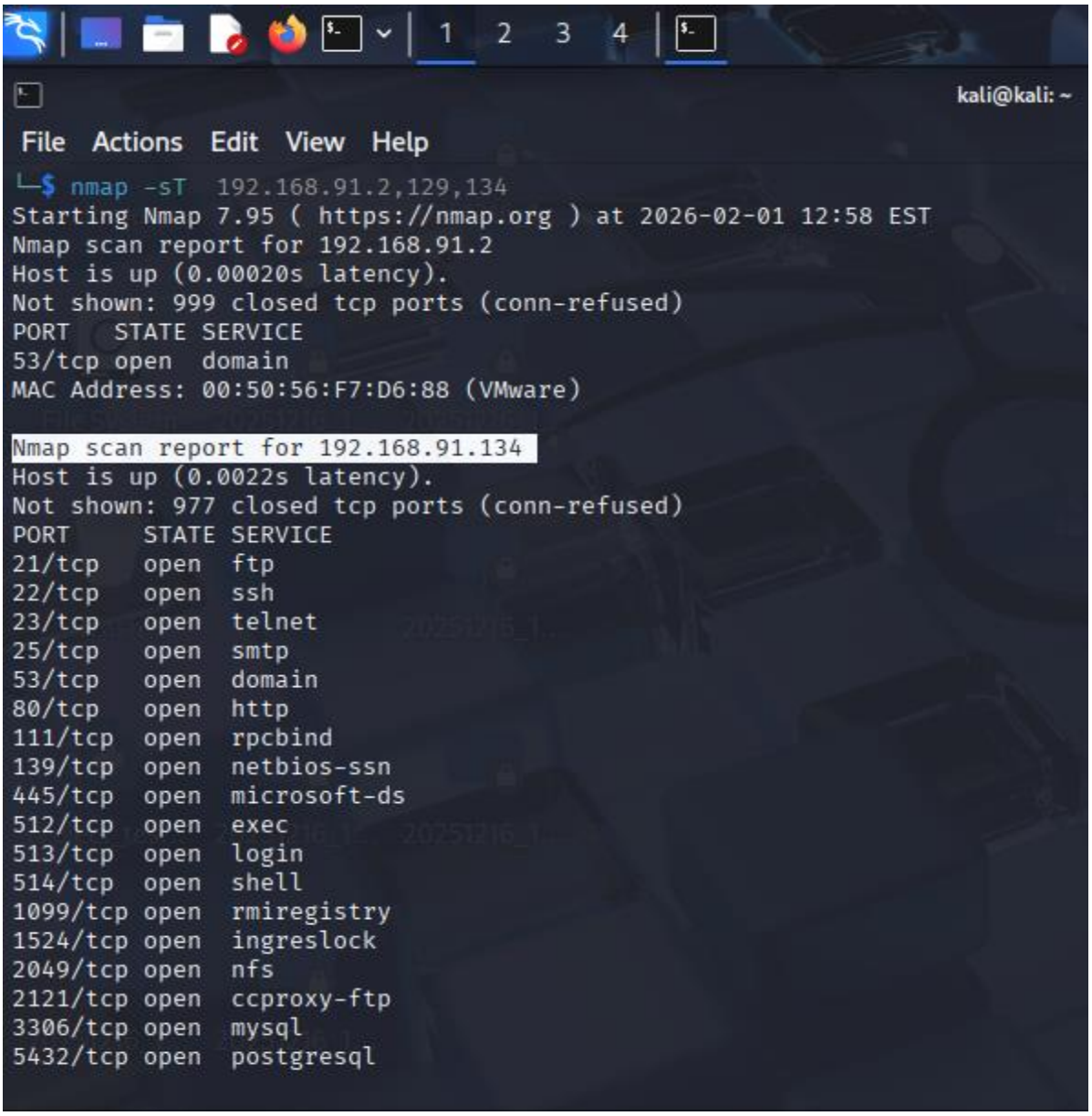


Okay we Know The Server Measploit Is Online (Up) With IP 192.168.91.134

2-Port Scanning Using Tool (nmap)

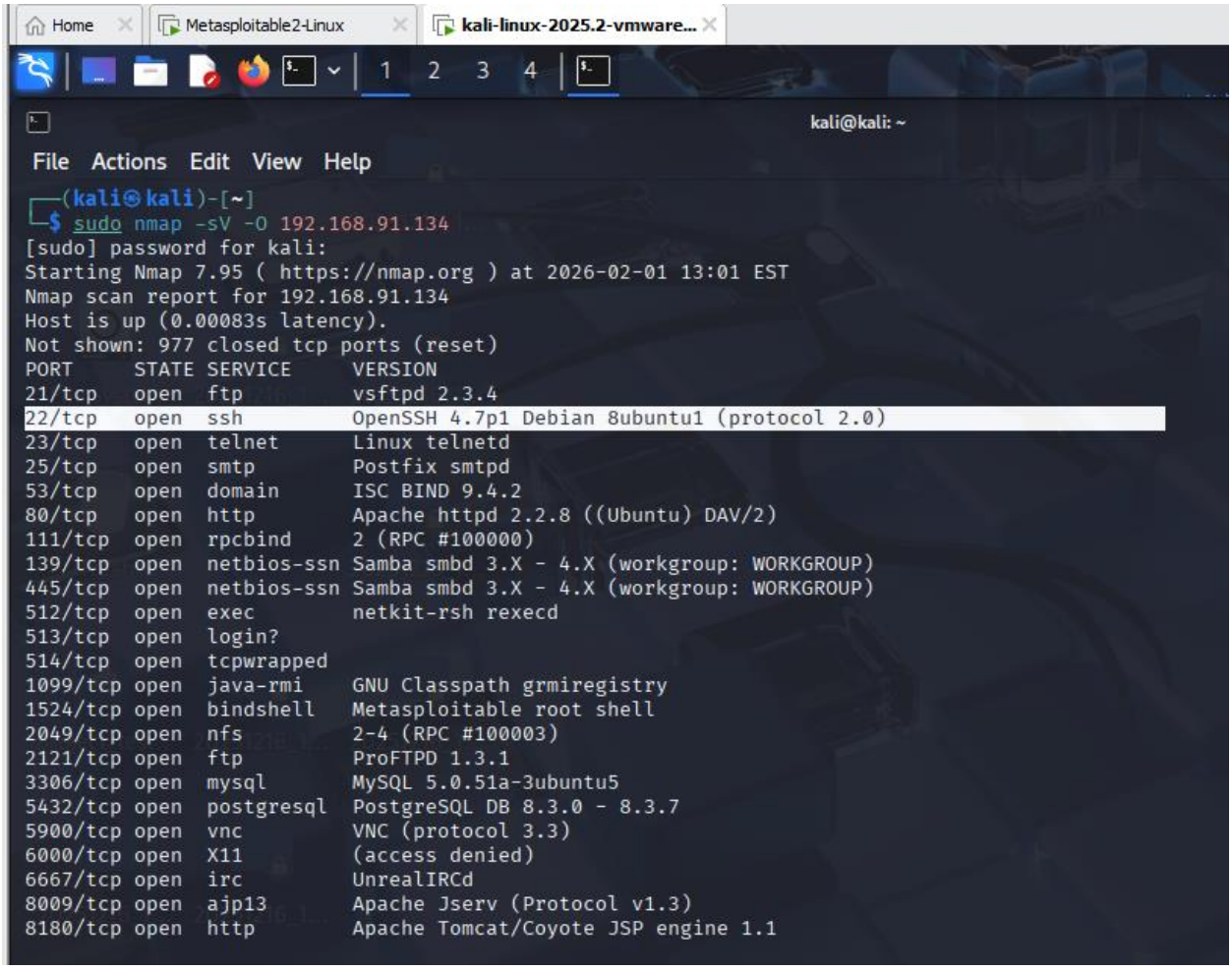
3-Used to perform **a TCP connect** scan to identify open ports and running services on the targetsystem (**nmap -sS 192.168.2.129.134**)

_Nmap Scan Report For Server 192.168.91.134 with each ports is Opening



4- sudo nmap -sS -sV -O 192.168.91.134
Used to detect running service**s**, their versions, and identify the target operating system.

We find the Version Of Services Port That I will detect it (OpenSSH 4.7p1)



3-Identification Vulnerability

3- To detect attacks, we must first check for vulnerabilities

We have three methosd

1-SearchSploit

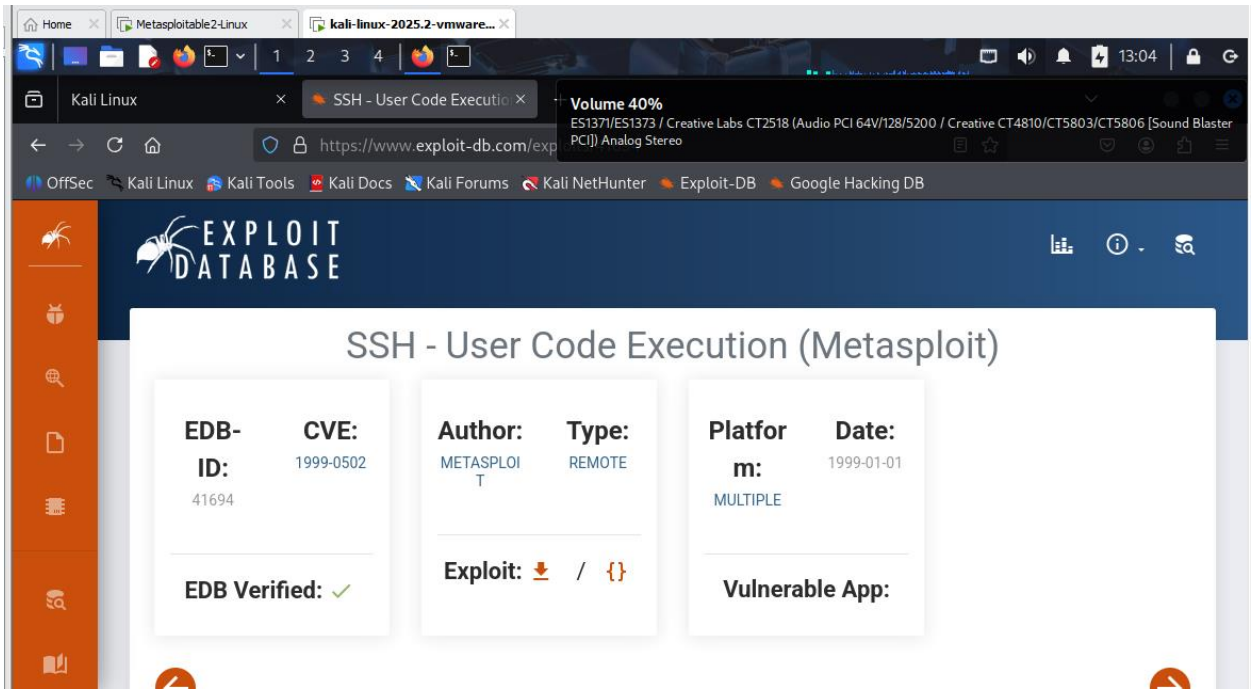
2-Expliotdatabase

3-Metasploite

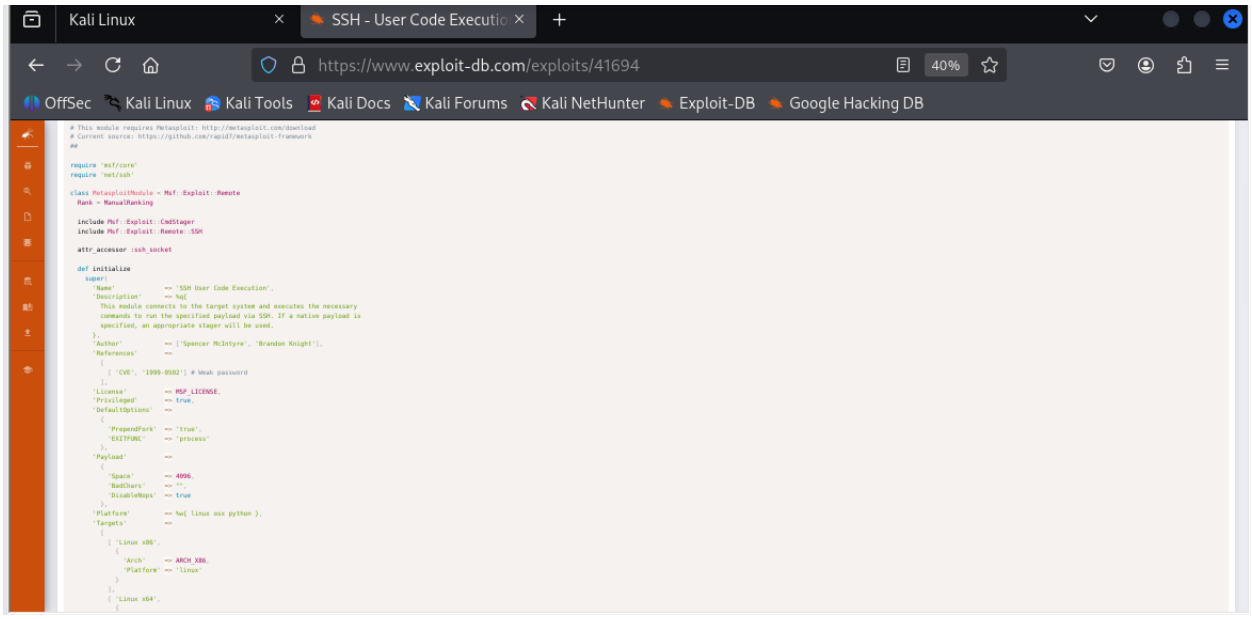
1-Expliotdatabase(Exploit DB)

A public repository used to search for known exploits related to discovered services and vulnerabilities.

SSh -User Code All Info



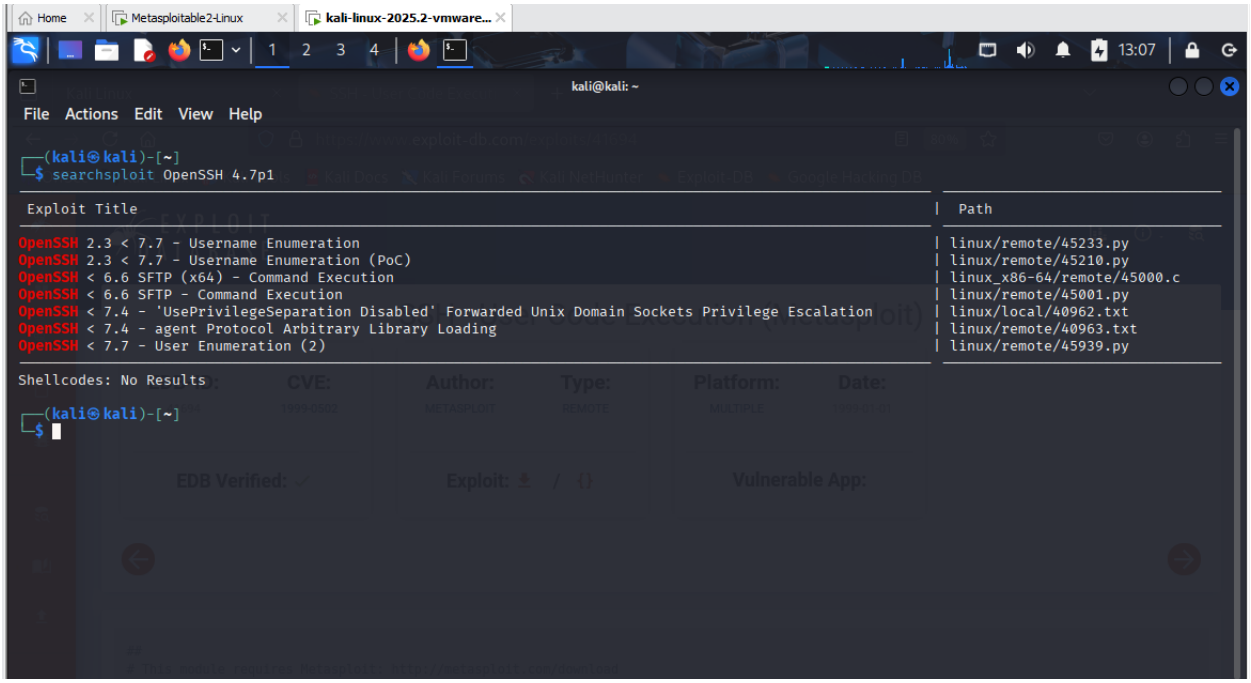
Pyhton code if you run it you will generate attack



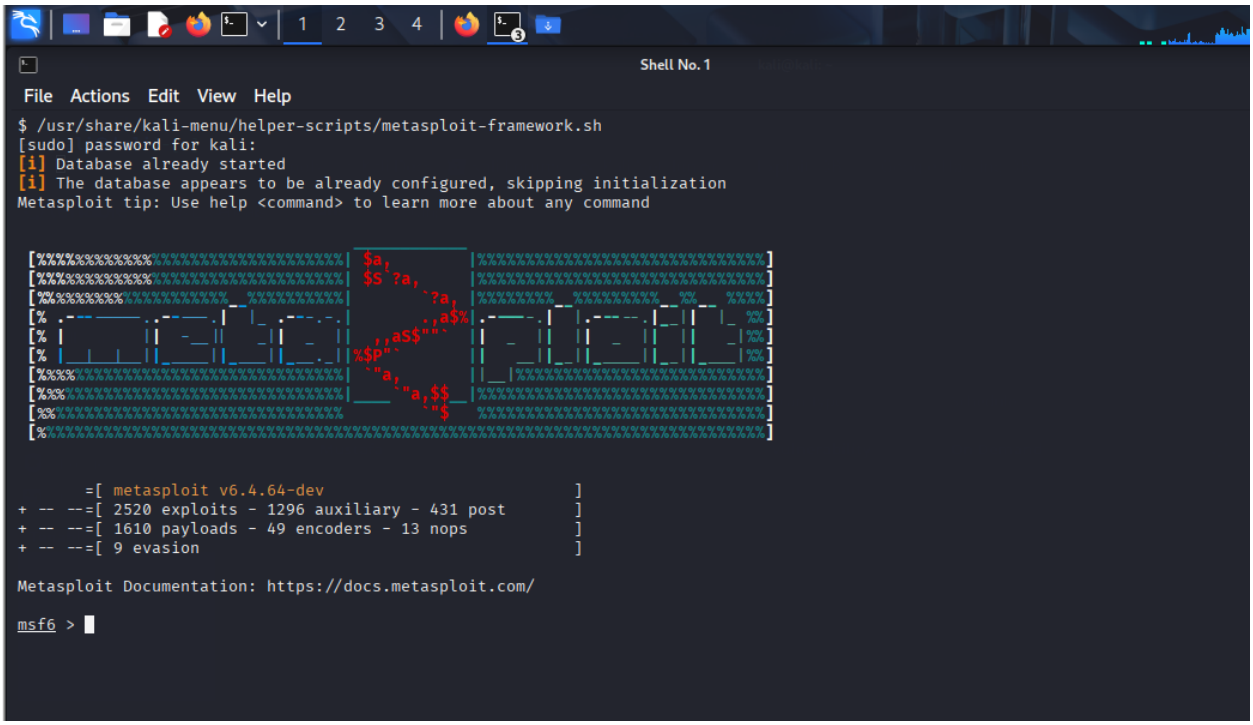
2-searchsploit:

A tool used to search the Exploit Database locally for known exploits related to detected services and versions.

Yes there are many way to Exploit This Version



4-Open Metasploit

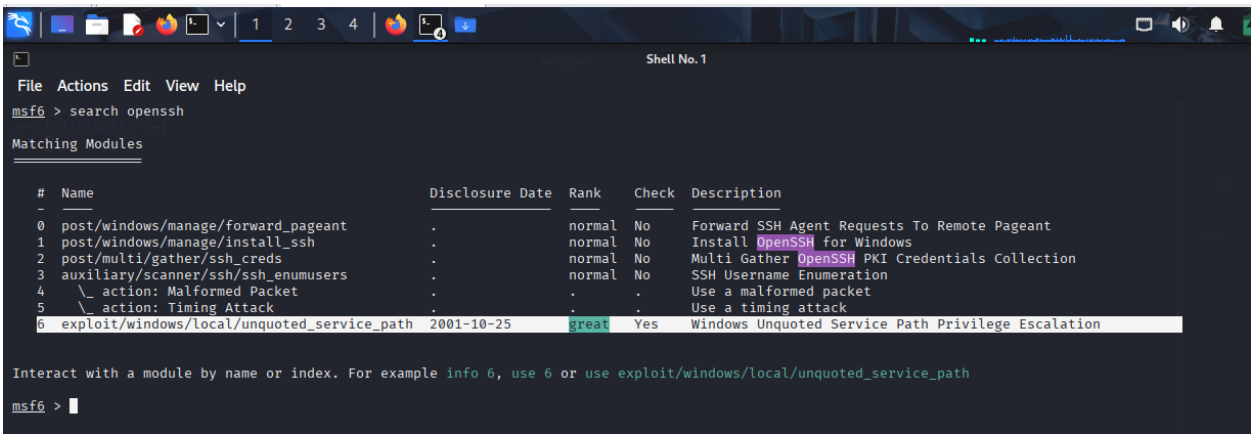


Search OpenSSH 4.7p1

We will Find 7 Module (0 to 6) each Module Work in one position Help you

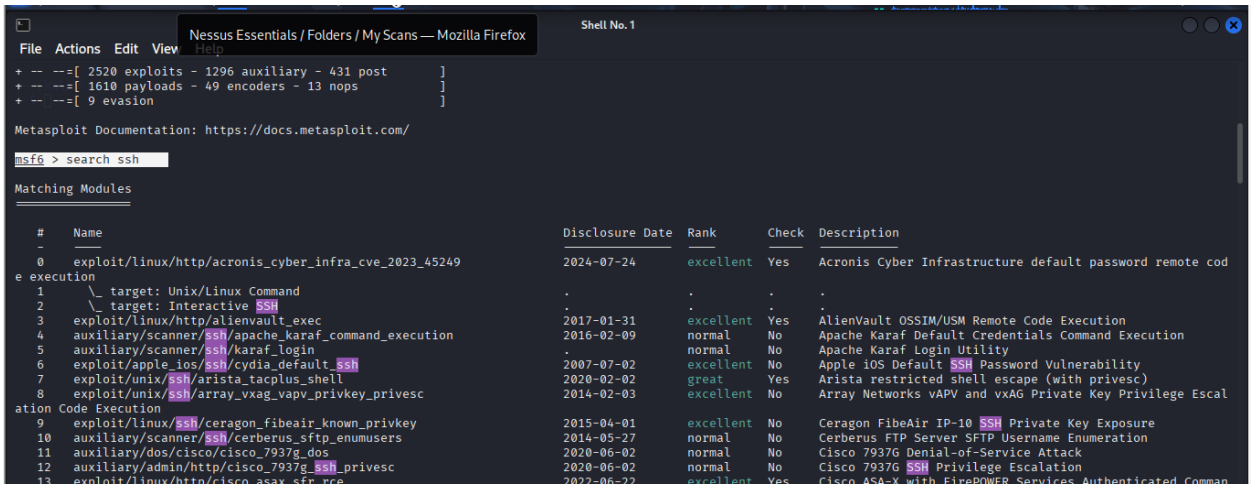
But id did not work with RHosts ip 192.168.91.134

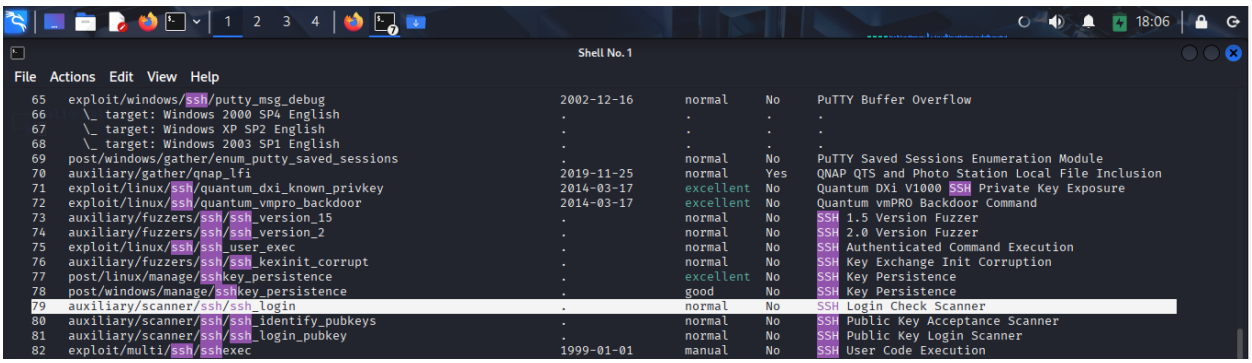
That must be opened session before by Meterpreter Session



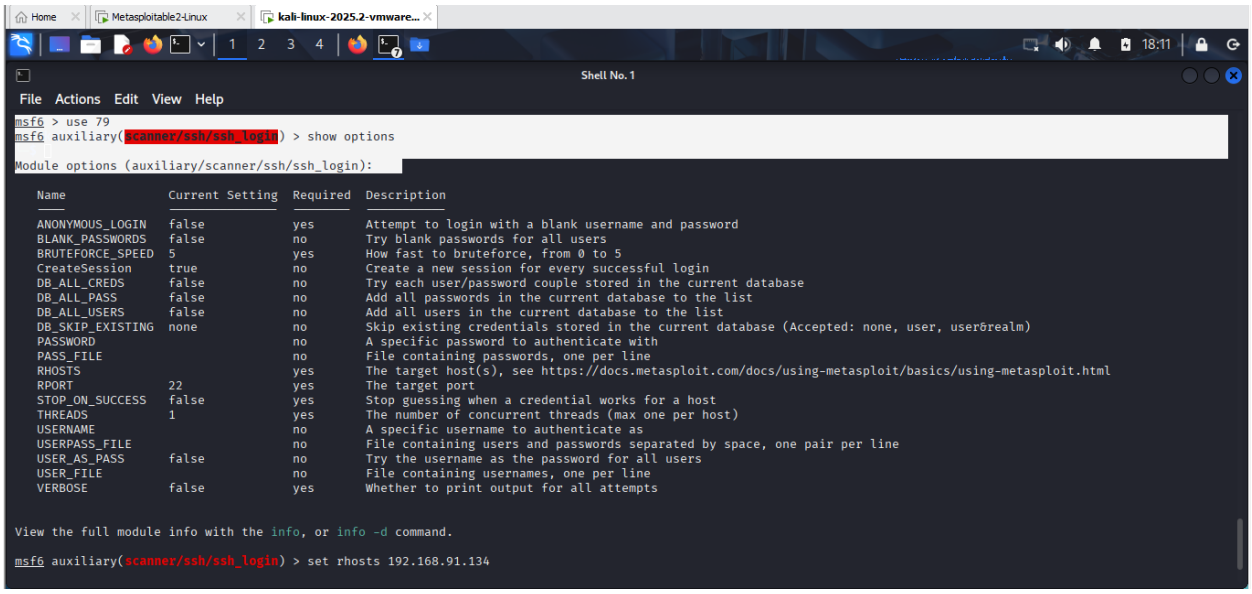
_First must Exploit Remote By SSH

-Search SSH we find The Module 79 auxiliary/scanner/ssh/ssh_login





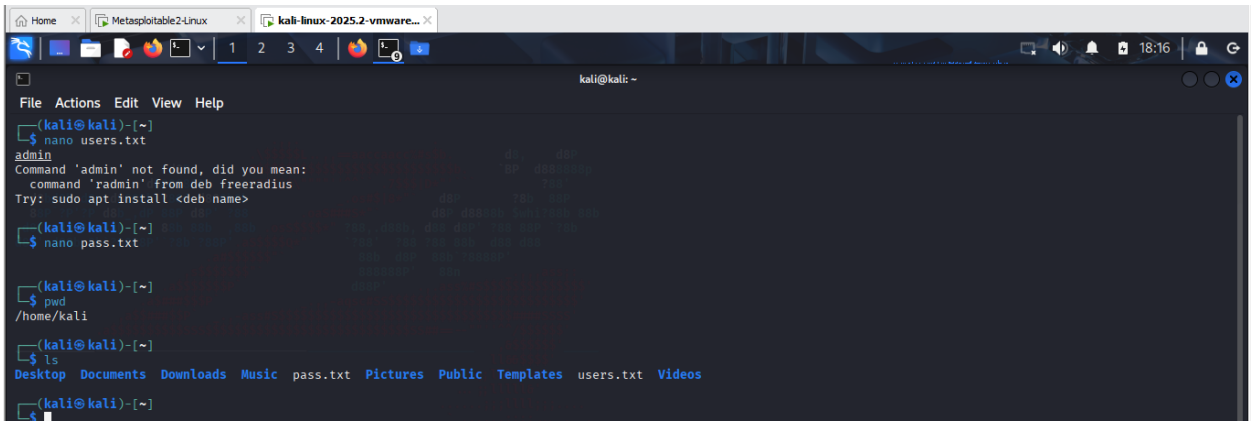
-Use Module 79 use auxiliary/scanner/ssh/ssh_login



-Brute Force Attack

Create List of Username users.txt

Creat List of Password pass.txt



After

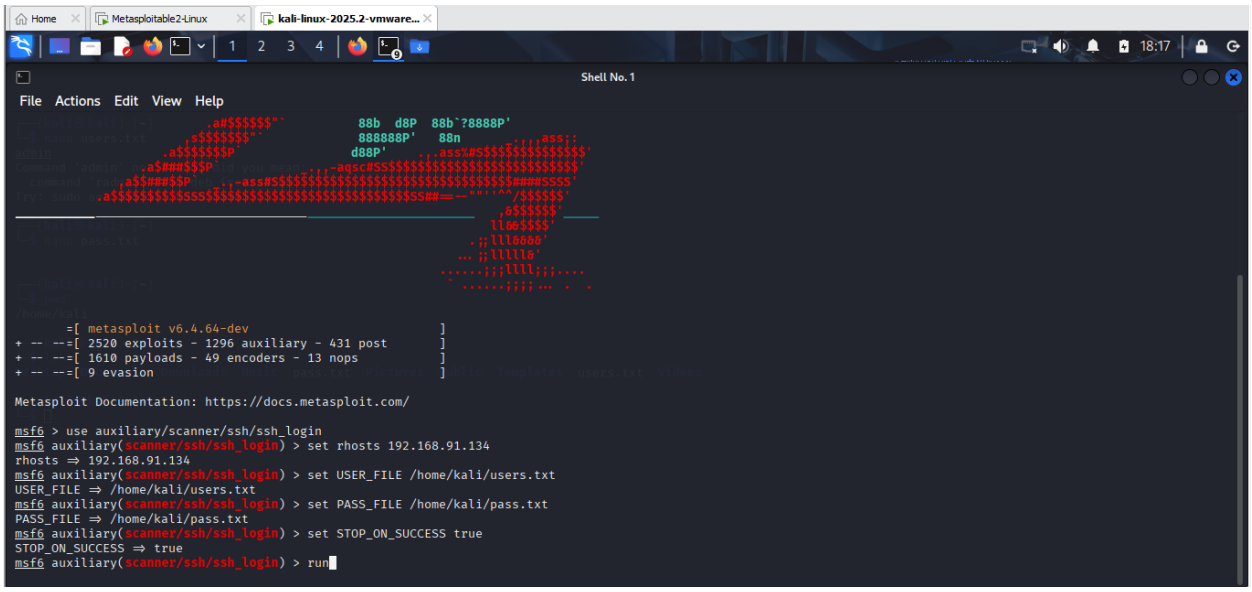
set RHOSTS 192.168.91.134

set USER_FILE users.txt

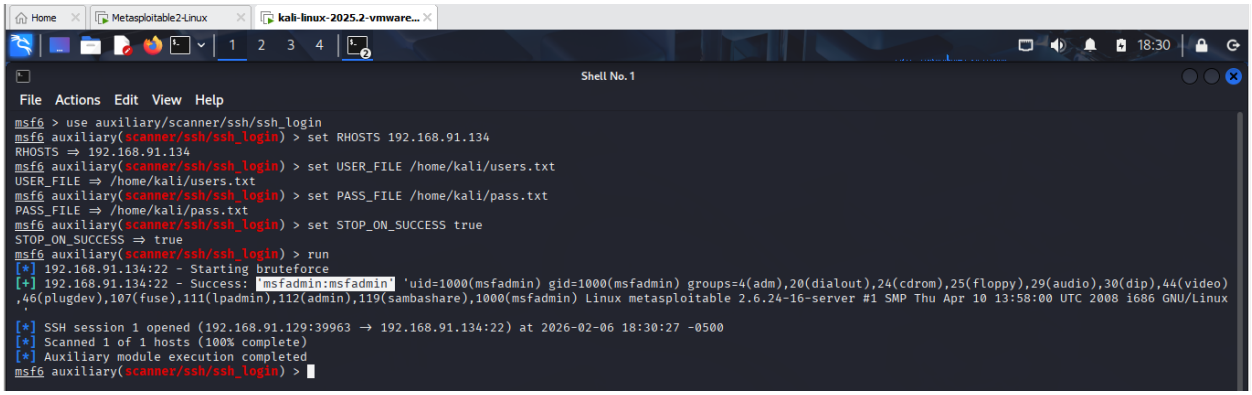
set PASS_FILE passwords.txt

set STOP_ON_SUCCESS true

run



Result Start Brureforce Success: 'msfadmin:msfadmin'



-ssh -oHostKeyAlgorithms=+ssh-rsa msfadmin@192.168.91.134

Session is Opened