5 July, 24

Exploiting 23 and 25 Telnet and SMTP Port Vulnerability on Metasploitable2:

Detailed Write-Up by Seerat E Marryum

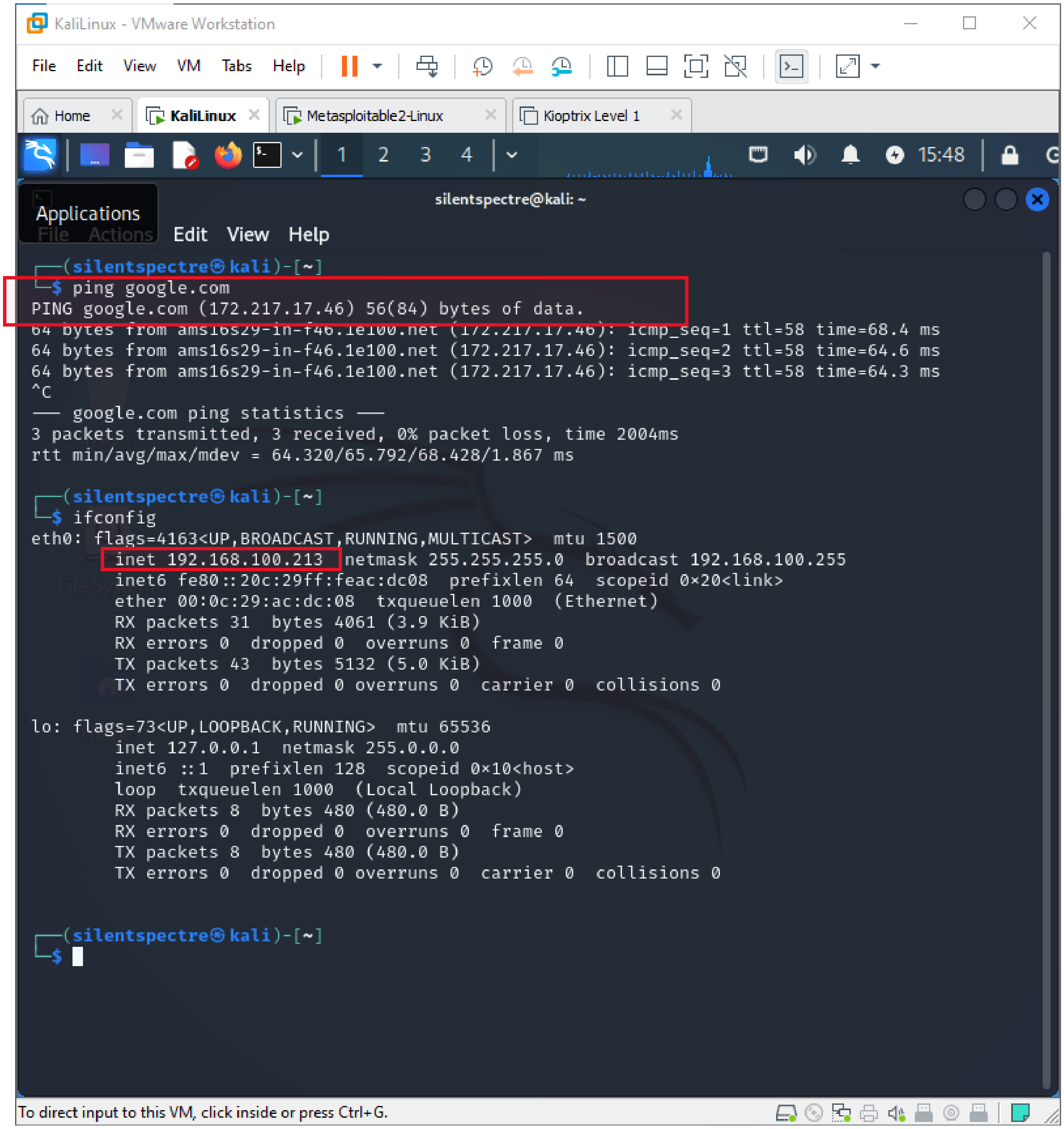
Check connectivity and the IP address of network we are connected to:

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

Check all the network devices connected on router

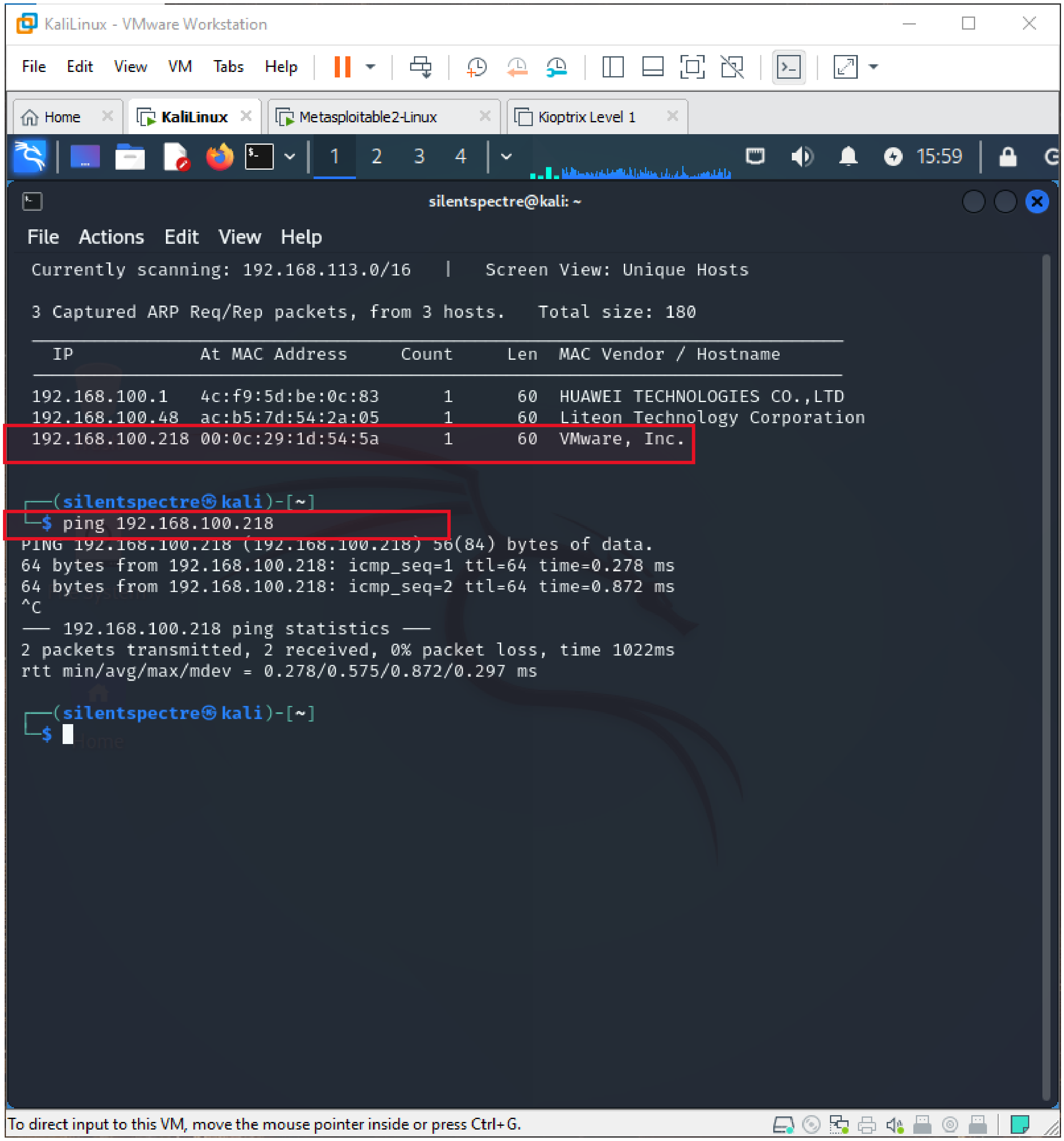
- **sudo netdiscover**

5 July, 24


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 0×20<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 0×10<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, 24

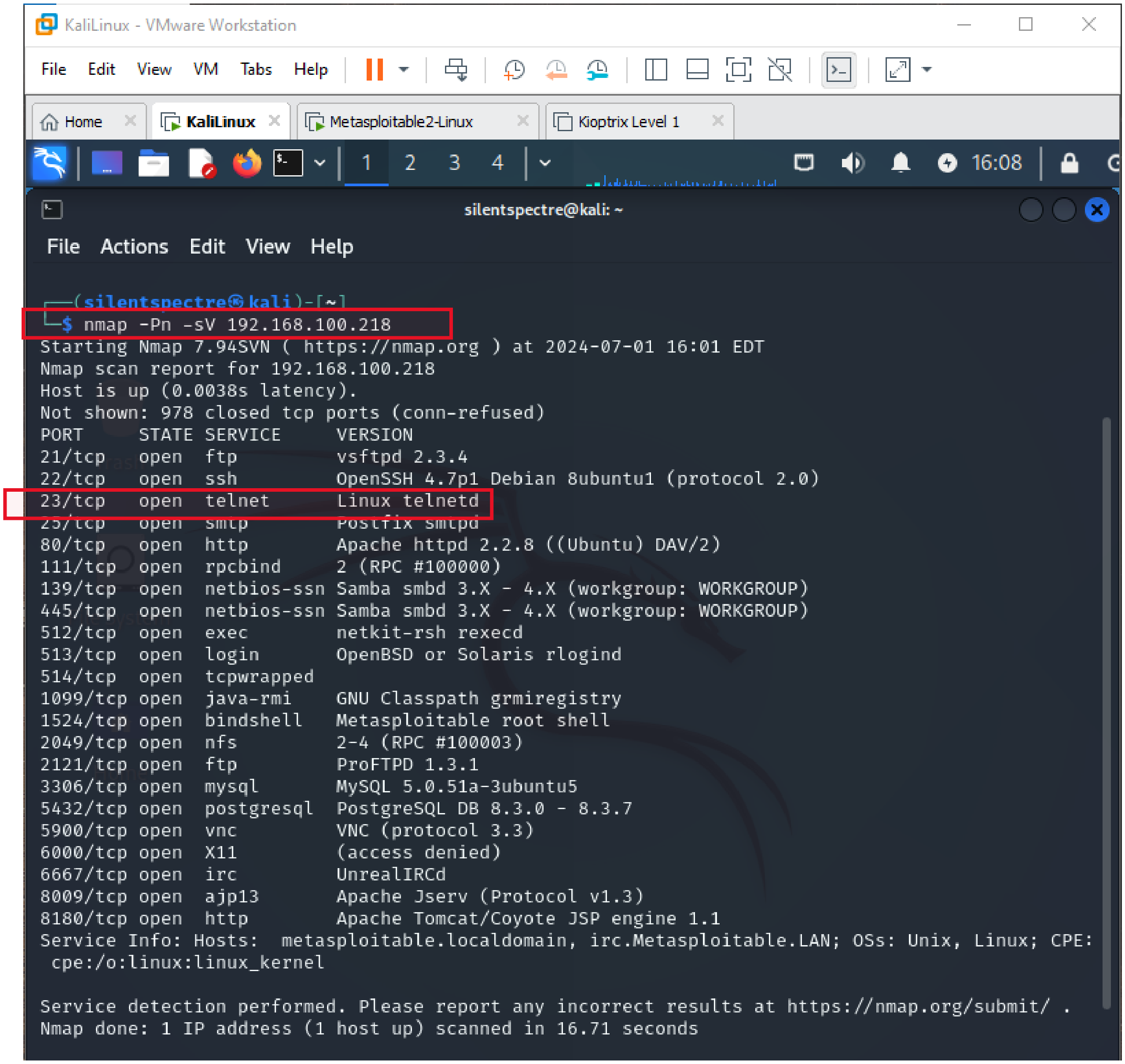

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
15:59
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
 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, 24

nmap scan -Pn -sV <ip>

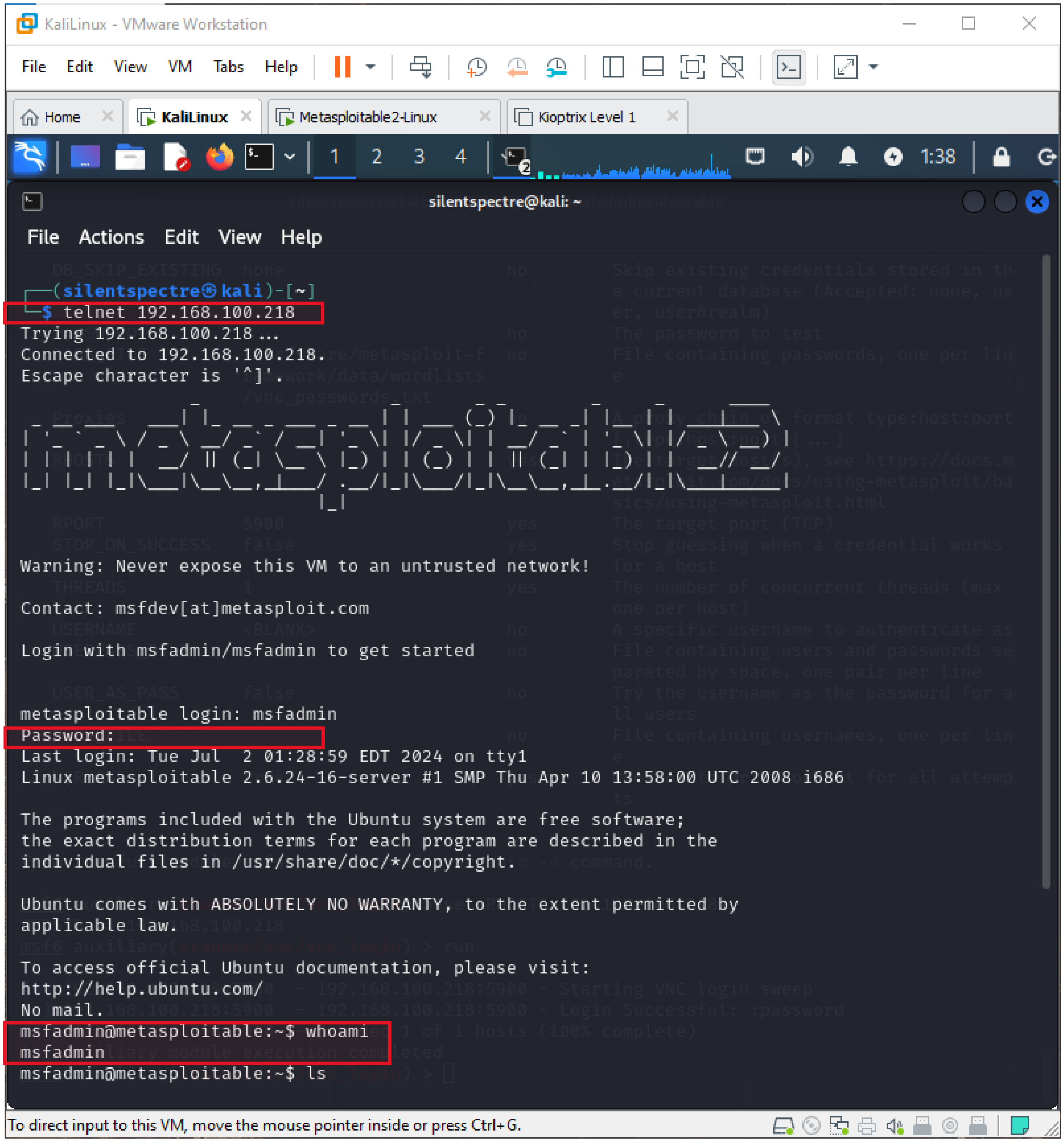


```
┌──(silentspectre㉿kali)-[~]
└─$ nmap -Pn -sV 192.168.100.218
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 16:01 EDT
Nmap scan report for 192.168.100.218
Host is up (0.0038s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp 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

Telnet:

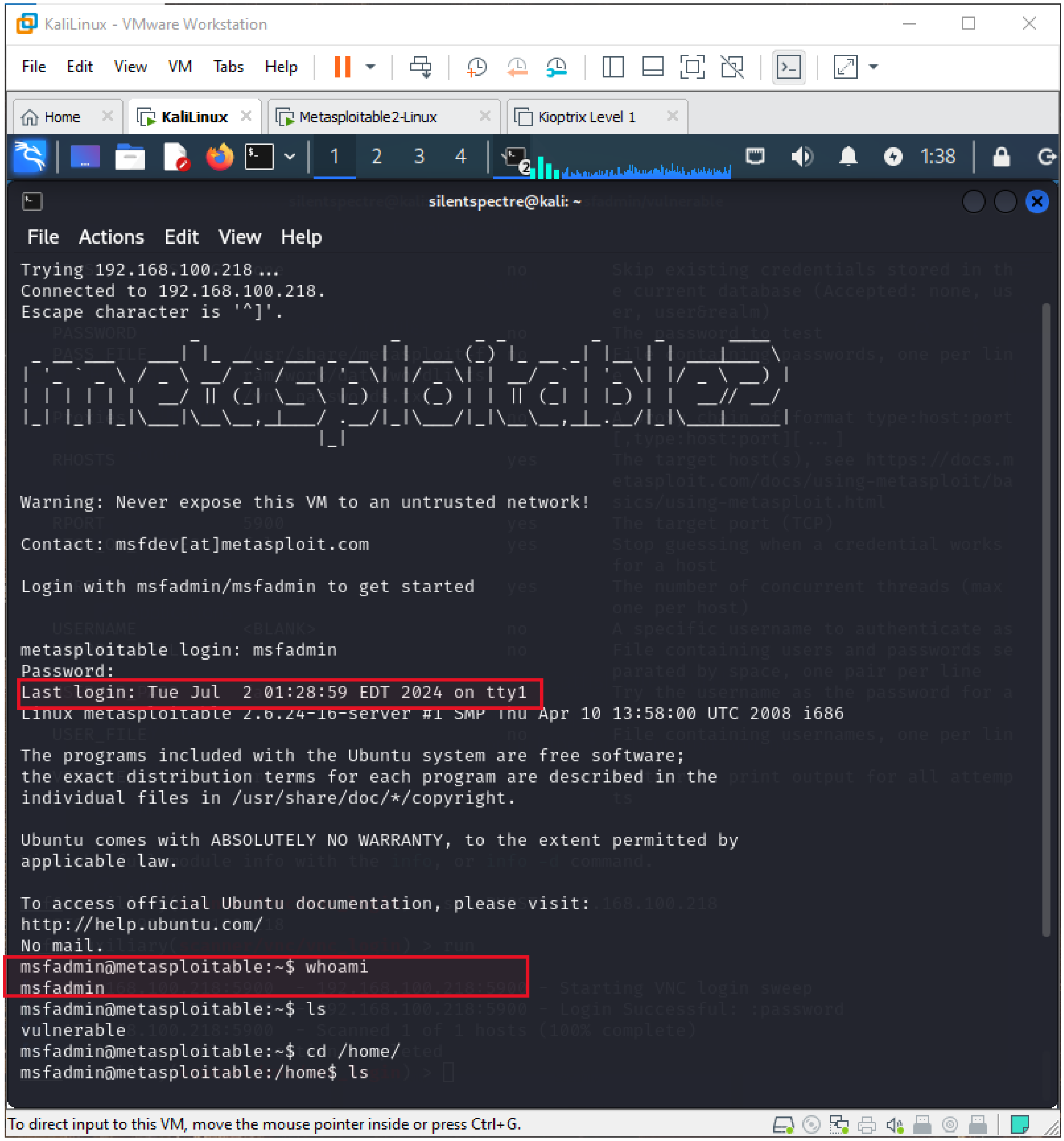
5 July, 24

Connect to port by this command: **telnet <target ip>** and put the password there and u are in.


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
1:38
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(silentspectre㉿kali)-[~]
└─$ telnet 192.168.100.218
Trying 192.168.100.218...
Connected to 192.168.100.218.
Escape character is '^]'.
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Jul  2 01:28:59 EDT 2024 on tty1
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.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ ls
```

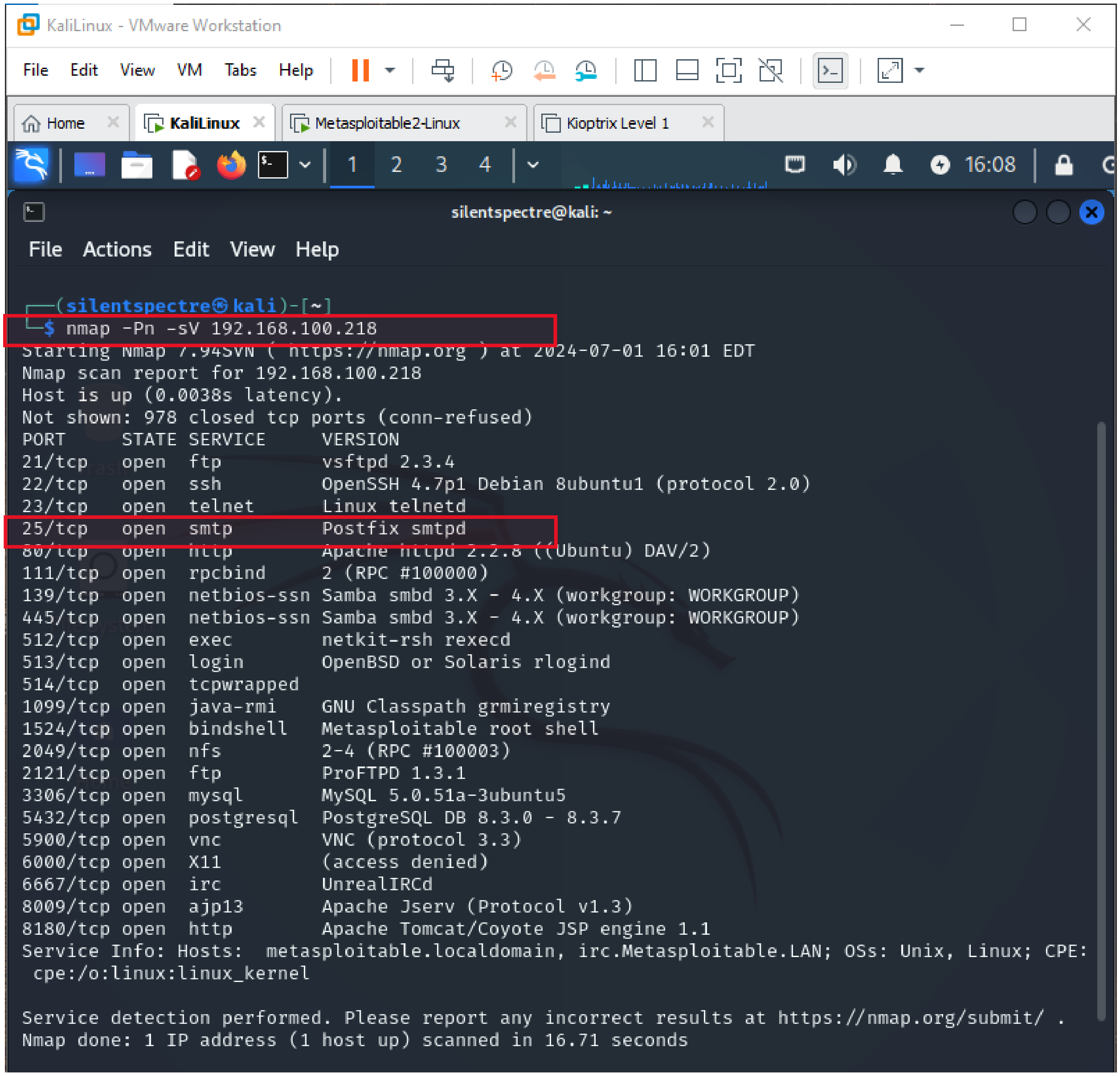
5 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
Kioptrix Level 1
1 2 3 4
1:38
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Trying 192.168.100.218...
Connected to 192.168.100.218.
Escape character is '^]'.
                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Jul  2 01:28:59 EDT 2024 on tty1
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.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd /home/
msfadmin@metasploitable:/home$ ls
```

SMTP:

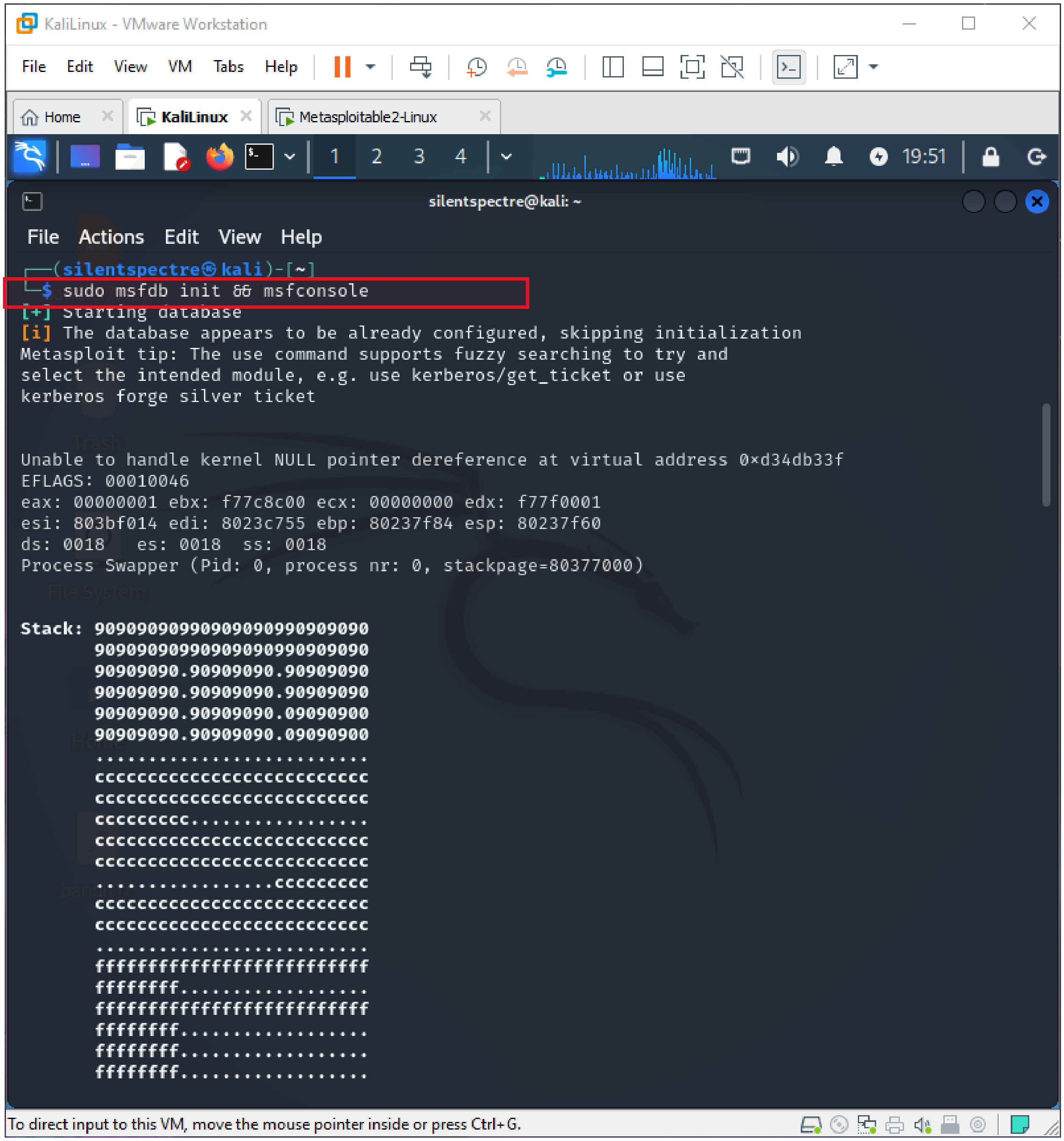
5 July, 24


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

```
┌──(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
```

Starting **msfdb** to use it as a tool for exploiting smtp port:

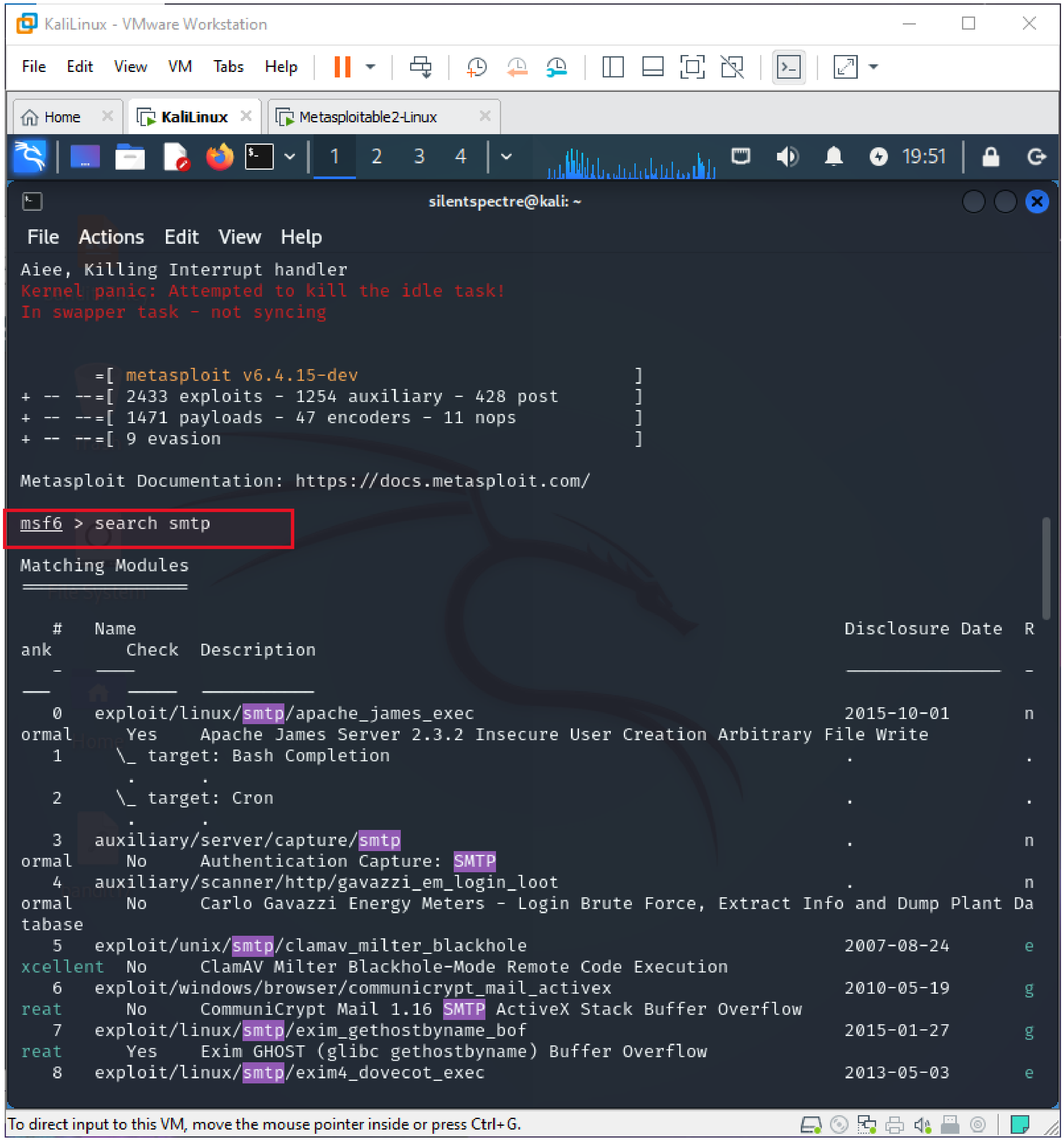
5 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
1 2 3 4
19:51
silentspectre@kali: ~
File Actions Edit View Help

```
┌──(silentspectre㉿kali)-[~]
└─$ sudo msfdb init && msfconsole
[+] Starting database
[i] The database appears to be already configured, skipping initialization
Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket


Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffff..................
       ffffffff..................
```

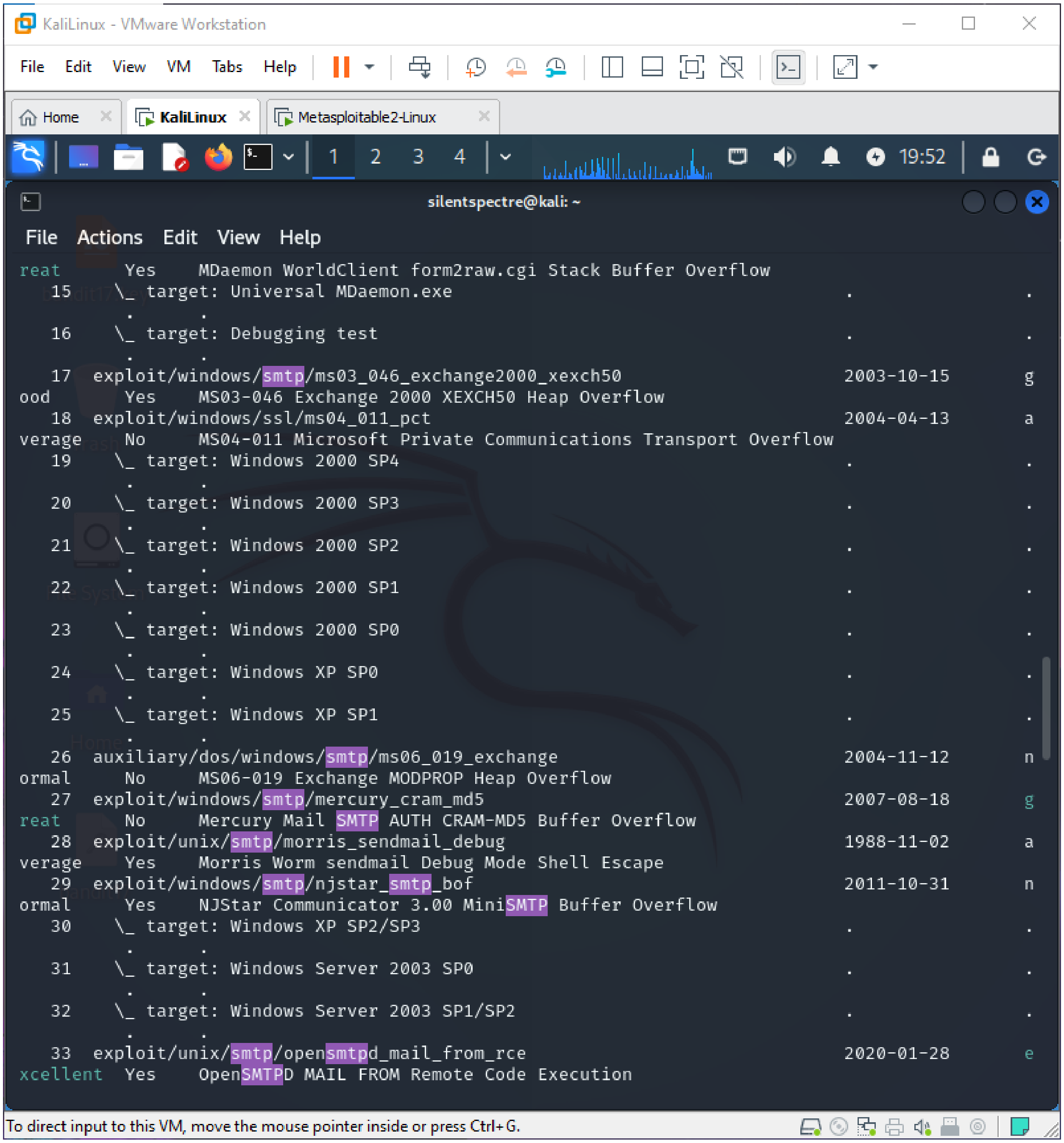
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

5 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
1 2 3 4
19:51
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing


       =[ 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 > search smtp

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

   #   Name                                                                   Disclosure Date  R
ank       Check  Description
   -   ----                                                                   ---------------  -
---       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                                   2015-10-01       n
ormal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
   1     \_ target: Bash Completion                                           .                .
          .      .
   2     \_ target: Cron                                                      .                .
          .      .
   3   auxiliary/server/capture/smtp                                          .                n
ormal     No     Authentication Capture: SMTP
   4   auxiliary/scanner/http/gavazzi_em_login_loot                           .                n
ormal     No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Da
tabase
   5   exploit/unix/smtp/clamav_milter_blackhole                              2007-08-24       e
xcellent  No     ClamAV Milter Blackhole-Mode Remote Code Execution
   6   exploit/windows/browser/communicrypt_mail_activex                      2010-05-19       g
reat      No     CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
   7   exploit/linux/smtp/exim_gethostbyname_bof                              2015-01-27       g
reat      Yes    Exim GHOST (glibc gethostbyname) Buffer Overflow
   8   exploit/linux/smtp/exim4_dovecot_exec                                  2013-05-03       e
```

5 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
1 2 3 4
19:52
silentspectre@kali: ~
File Actions Edit View Help

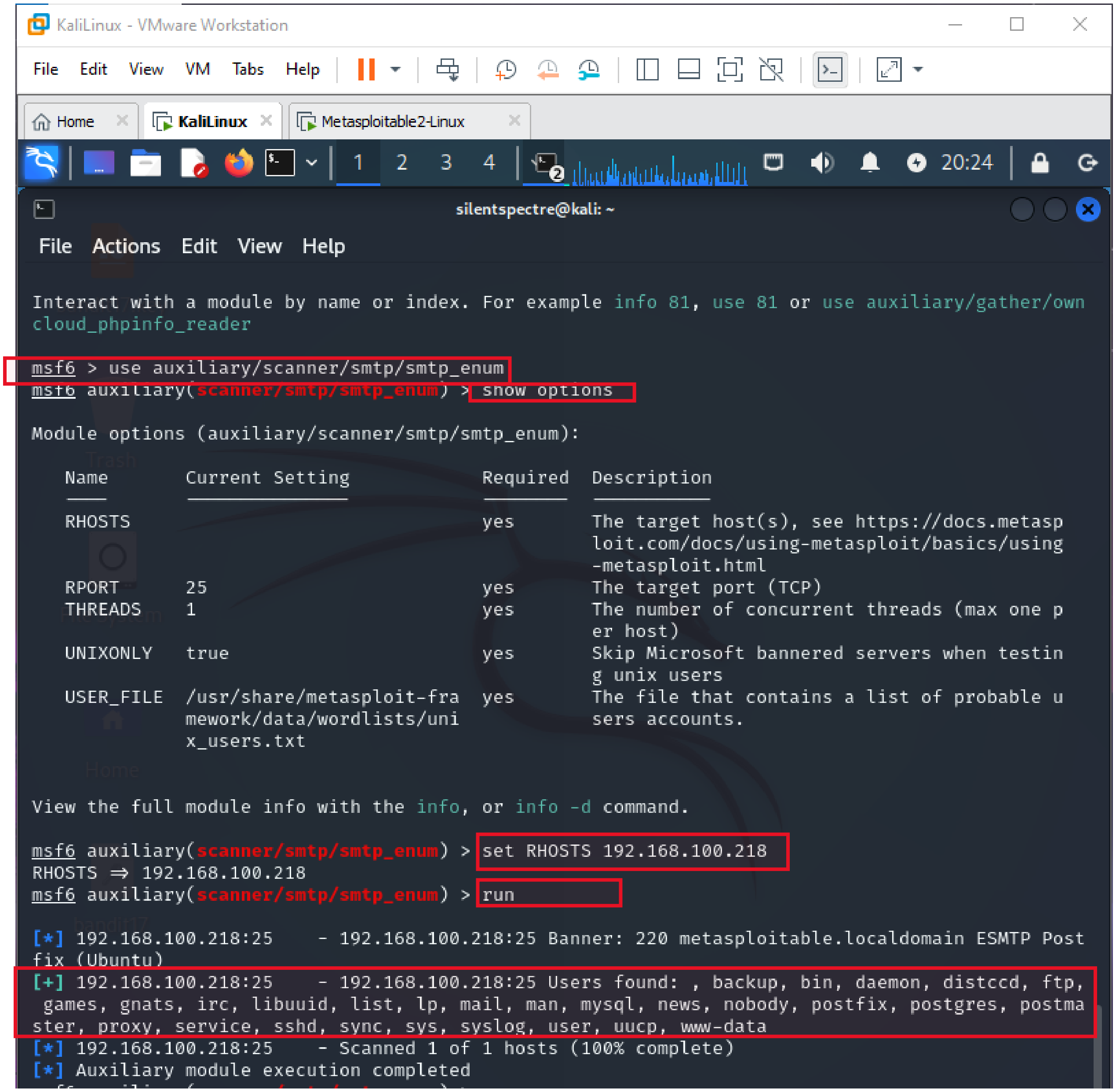
```
reat        Yes     MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
   15    \_ target: Universal MDaemon.exe                                   .         .
      .      .
   16    \_ target: Debugging test                                          .         .
      .      .
   17  exploit/windows/smtp/ms03_046_exchange2000_xexch50               2003-10-15    g
ood         Yes     MS03-046 Exchange 2000 XEXCH50 Heap Overflow
   18  exploit/windows/ssl/ms04_011_pct                                 2004-04-13    a
verage      No      MS04-011 Microsoft Private Communications Transport Overflow
   19    \_ target: Windows 2000 SP4                                        .         .
      .      .
   20    \_ target: Windows 2000 SP3                                        .         .
      .      .
   21    \_ target: Windows 2000 SP2                                        .         .
      .      .
   22    \_ target: Windows 2000 SP1                                        .         .
      .      .
   23    \_ target: Windows 2000 SP0                                        .         .
      .      .
   24    \_ target: Windows XP SP0                                          .         .
      .      .
   25    \_ target: Windows XP SP1                                          .         .
      .      .
   26  auxiliary/dos/windows/smtp/ms06_019_exchange                     2004-11-12    n
ormal       No      MS06-019 Exchange MODPROP Heap Overflow
   27  exploit/windows/smtp/mercury_cram_md5                            2007-08-18    g
reat        No      Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
   28  exploit/unix/smtp/morris_sendmail_debug                          1988-11-02    a
verage      Yes     Morris Worm sendmail Debug Mode Shell Escape
   29  exploit/windows/smtp/njstar_smtp_bof                             2011-10-31    n
ormal       Yes     NJStar Communicator 3.00 MiniSMTP Buffer Overflow
   30    \_ target: Windows XP SP2/SP3                                      .         .
      .      .
   31    \_ target: Windows Server 2003 SP0                                 .         .
      .      .
   32    \_ target: Windows Server 2003 SP1/SP2                             .         .
      .      .
   33  exploit/unix/smtp/opensmtpd_mail_from_rce                        2020-01-28    e
xcellent    Yes     OpenSMTPD MAIL FROM Remote Code Execution
```

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

Using module: **auxillary/scanner/smtp/smtp_enum**

Then setting **RHOSTS** to **target IP** and **run** the exploit.

5 July, 24

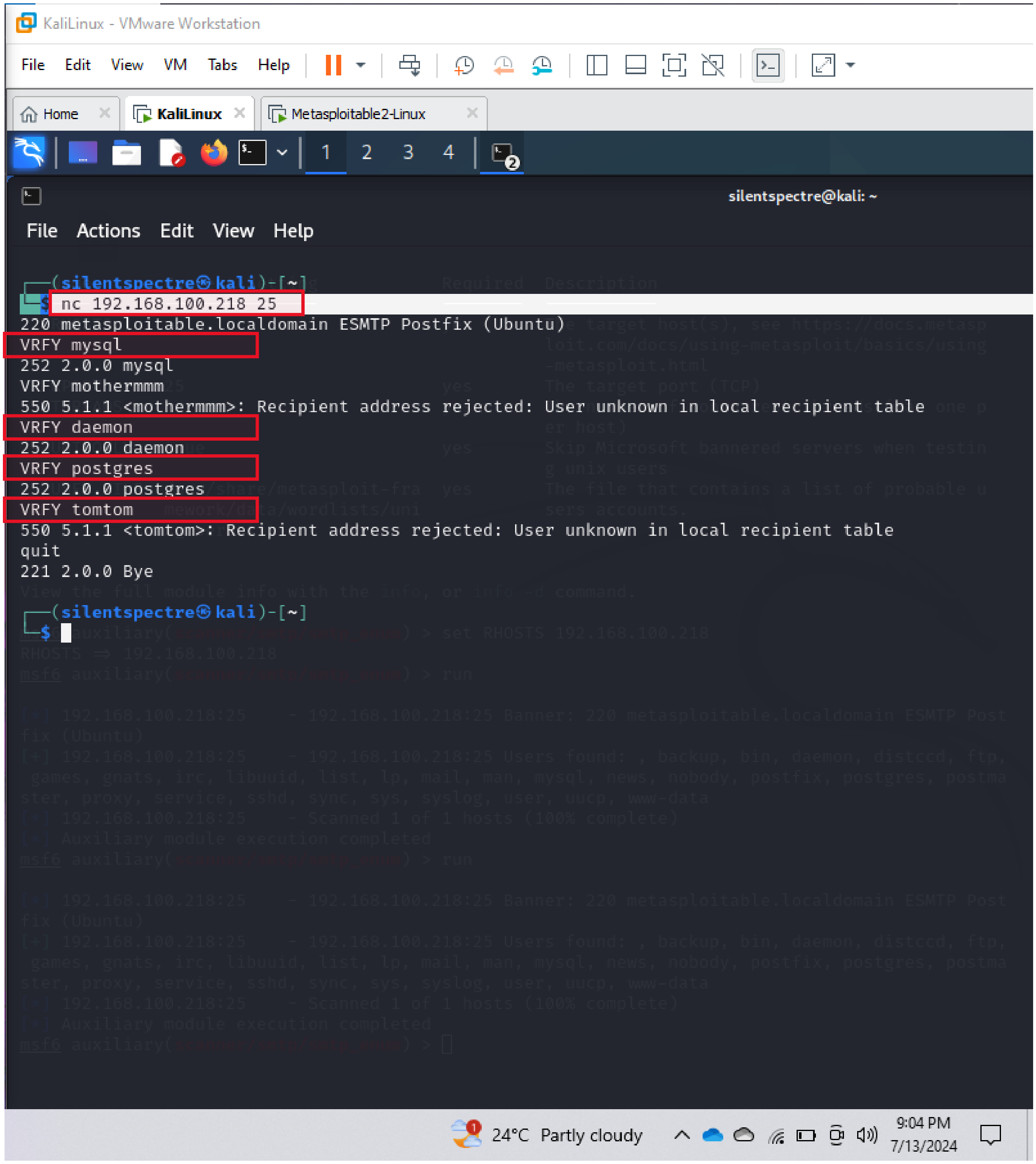

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Metasploitable2-Linux
1 2 3 4
20:24
silentspectre@kali: ~
File Actions Edit View Help

```
Interact with a module by name or index. For example info 81, use 81 or use auxiliary/gather/own
cloud_phpinfo_reader

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting           Required  Description
   ----       ---------------           --------  -----------
   RHOSTS                               yes       The target host(s), see https://docs.metasp
                                                  loit.com/docs/using-metasploit/basics/using
                                                  -metasploit.html
   RPORT      25                        yes       The target port (TCP)
   THREADS    1                         yes       The number of concurrent threads (max one p
                                                  er host)
   UNIXONLY   true                      yes       Skip Microsoft bannered servers when testin
                                                  g unix users
   USER_FILE  /usr/share/metasploit-fra yes       The file that contains a list of probable u
              mework/data/wordlists/uni           sers accounts.
              x_users.txt


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

msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.100.218
RHOSTS => 192.168.100.218
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.100.218:25    - 192.168.100.218:25 Banner: 220 metasploitable.localdomain ESMTP Post
fix (Ubuntu)
[+] 192.168.100.218:25    - 192.168.100.218:25 Users found: , backup, bin, daemon, distccd, ftp,
 games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postma
ster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.100.218:25    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

The command nc 192.168.100.218 25 uses nc (Netcat), a versatile networking tool, to connect to the IP address 192.168.100.218 on port 25:

The **VRFY** command is used to verify if a specific user or mailbox exists on the server.

5 July, 24



```
┌──(silentspectre㉿kali)-[~]
└─$ nc 192.168.100.218 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY mysql
252 2.0.0 mysql
VRFY mothermmm
550 5.1.1 <mothermmm>: Recipient address rejected: User unknown in local recipient table
VRFY daemon
252 2.0.0 daemon
VRFY postgres
252 2.0.0 postgres
VRFY tomtom
550 5.1.1 <tomtom>: Recipient address rejected: User unknown in local recipient table
quit
221 2.0.0 Bye

┌──(silentspectre㉿kali)-[~]
└─$ 
```