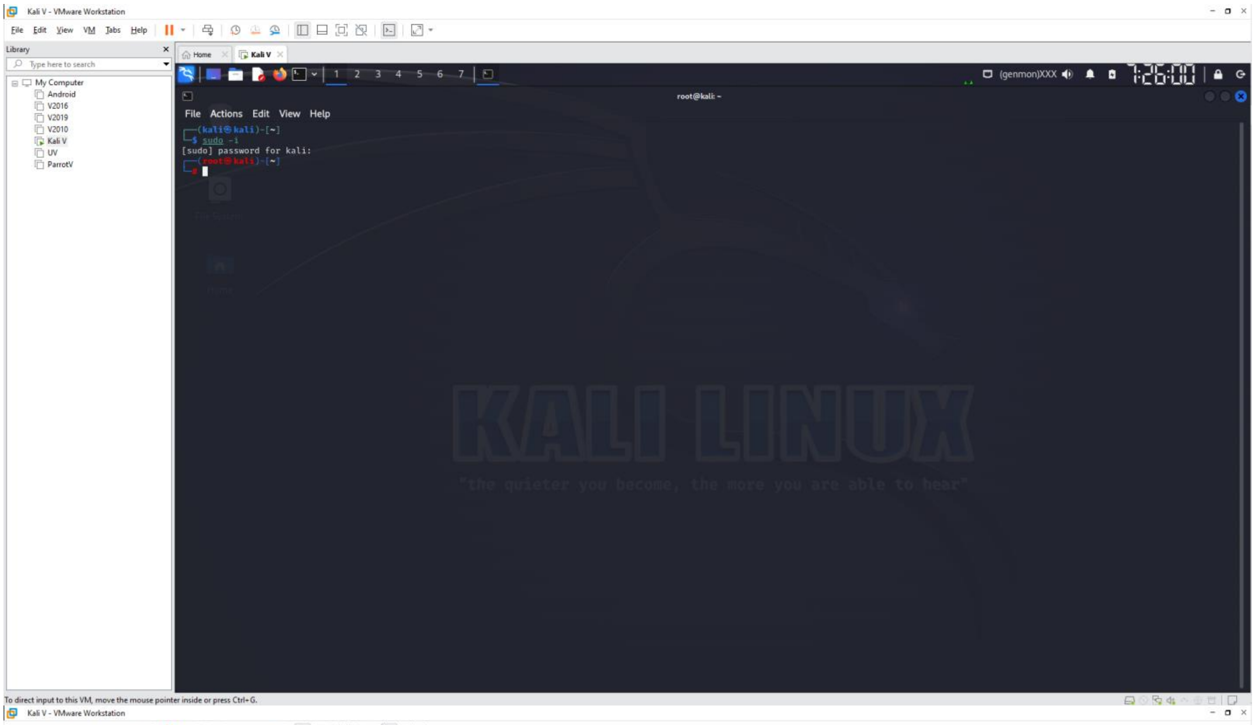
Lab #4: Enumerating Metasploitable 2

Course Name: Ethical Hacking and Offensive Security(HOD401)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 23/09/2023

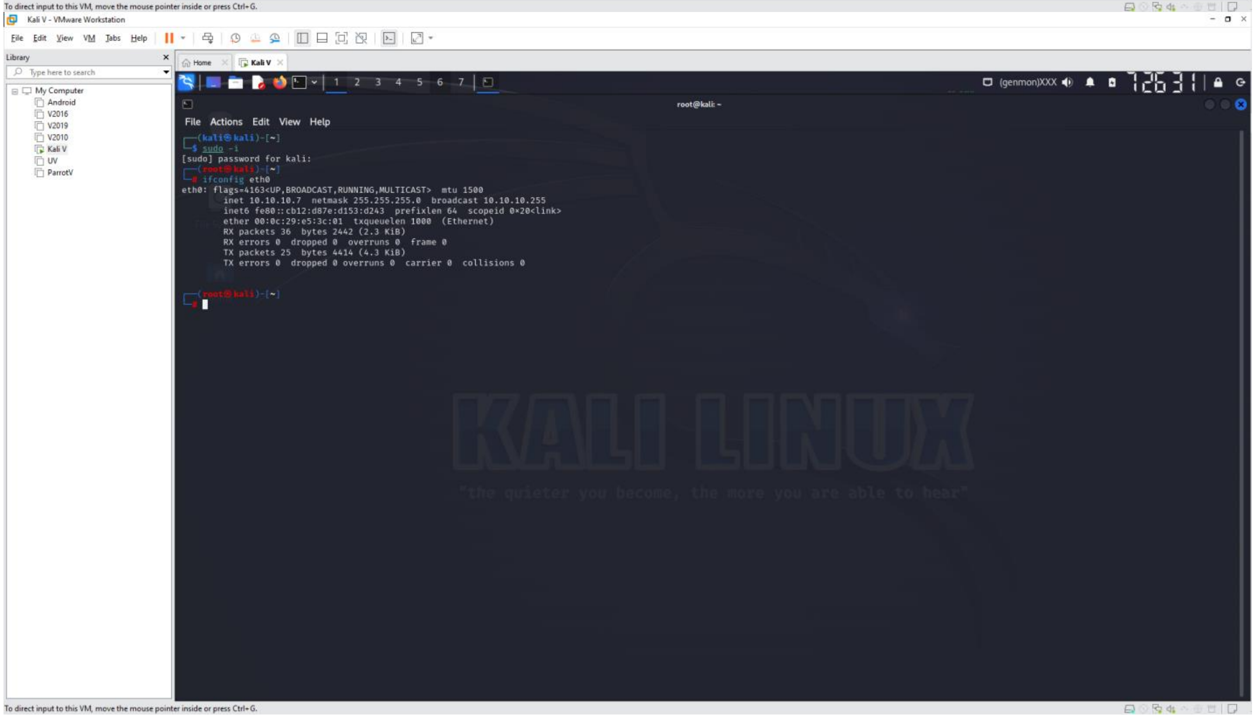
Lab Tasks

- Open Kali



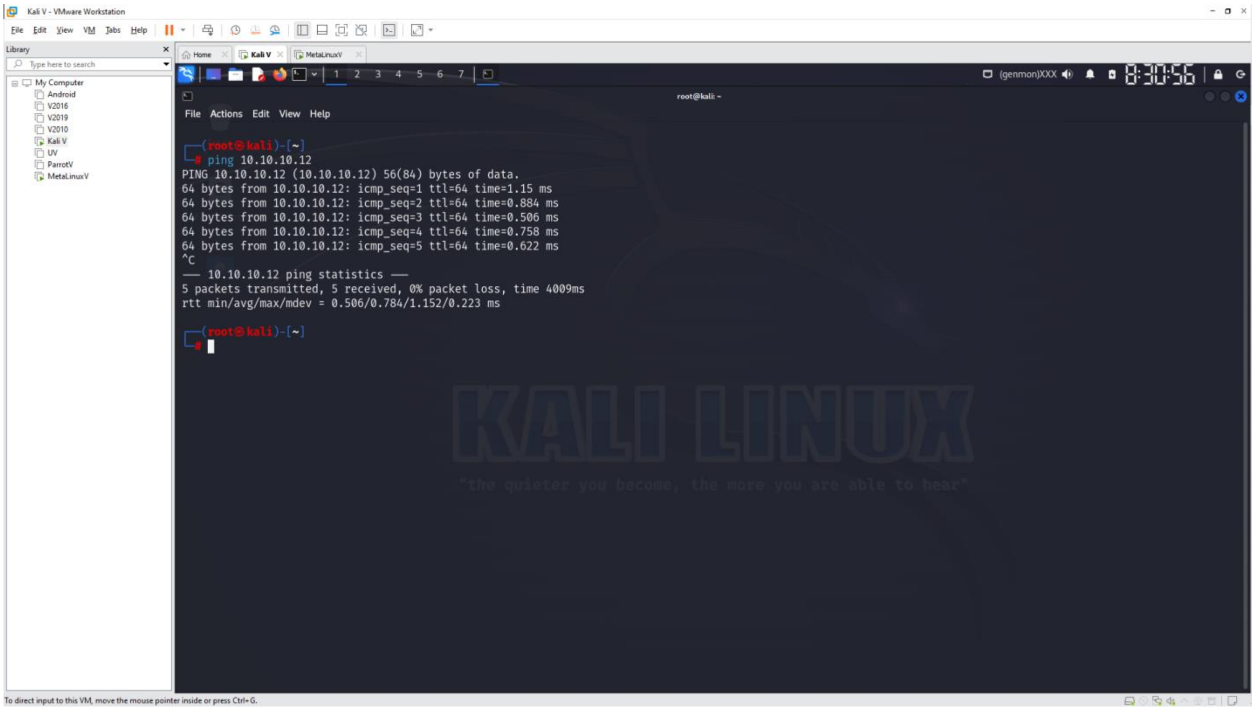
```
┌──(kali㉿kali)-[~]
└─$ sudo -i
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─#
```

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



```
┌──(kali㉿kali)-[~]
└─$ sudo -i
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.7  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::cb12:d87e:d153:d243  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e5:3c:01  txqueuelen 1000  (Ethernet)
        RX packets 36  bytes 2442 (2.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 4414 (4.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(root㉿kali)-[~]
└─#
```

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



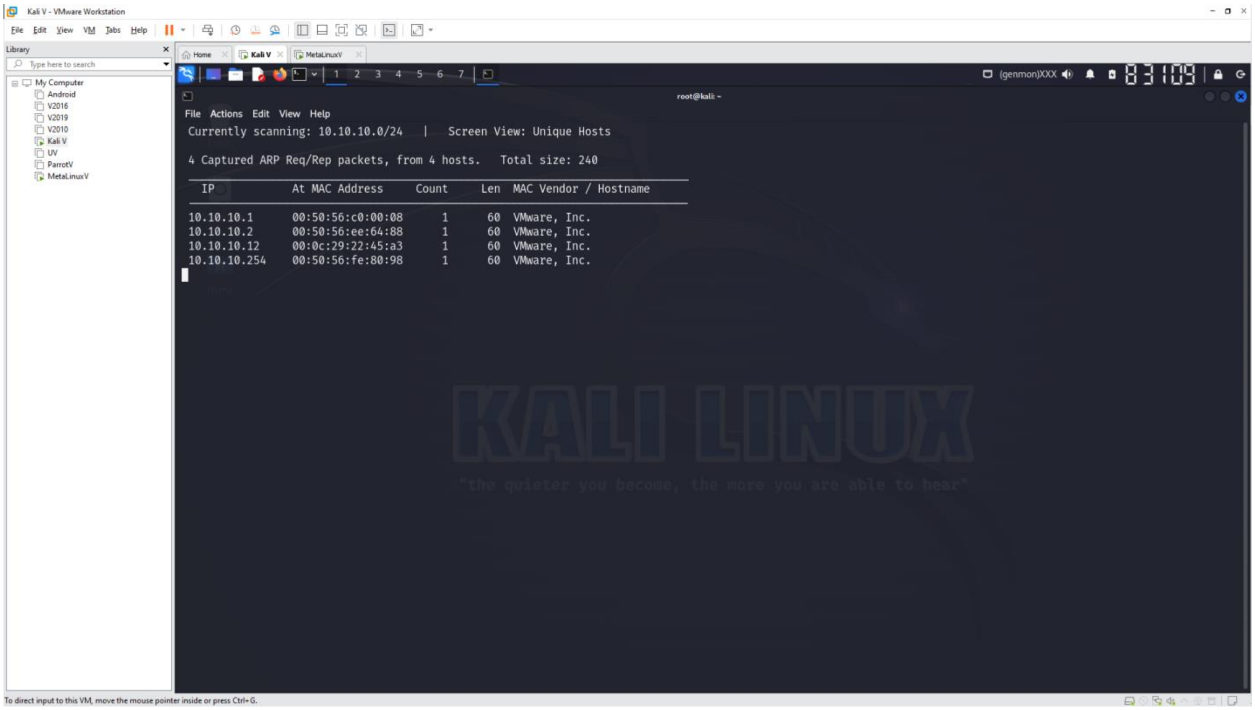
```
┌──(root㉿kali)-[~]
└─# ping 10.10.10.12
PING 10.10.10.12 (10.10.10.12) 56(84) bytes of data.
64 bytes from 10.10.10.12: icmp_seq=1 ttl=64 time=1.15 ms
64 bytes from 10.10.10.12: icmp_seq=2 ttl=64 time=0.884 ms
64 bytes from 10.10.10.12: icmp_seq=3 ttl=64 time=0.506 ms
64 bytes from 10.10.10.12: icmp_seq=4 ttl=64 time=0.758 ms
64 bytes from 10.10.10.12: icmp_seq=5 ttl=64 time=0.622 ms
^C
--- 10.10.10.12 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 0.506/0.784/1.152/0.223 ms

┌──(root㉿kali)-[~]
└─# 
```

Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
Kali V
MetaLinuxV
root@kali: ~
File Actions Edit View Help
(genmon)XXX
8:30:56
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Task 1: Finding Hosts & Open Ports

In Kali, execute this command to locate all hosts on your network.
Replace the subnet address below with the correct subnet for your machine. Usually all you need is the first 3 bytes of the IP address, as highlighted in the image above

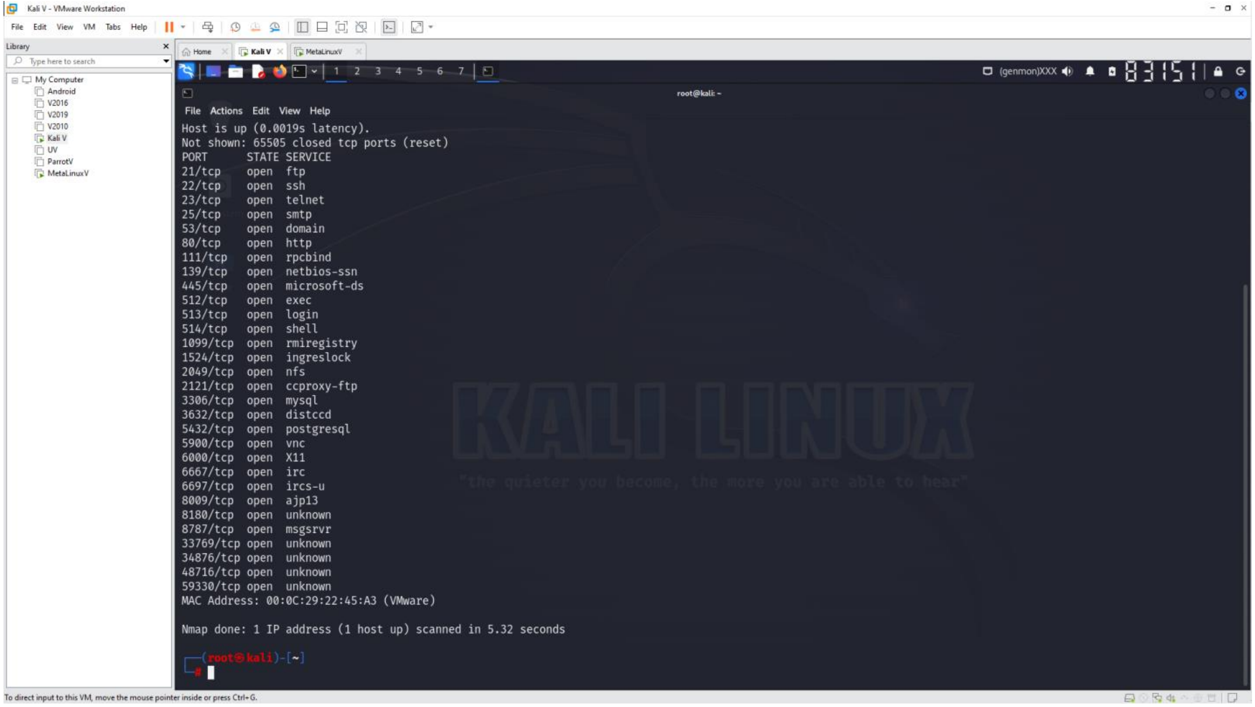
netdiscover -r 10.10.10.0/24



```
 Currently scanning: 10.10.10.0/24   |   Screen View: Unique Hosts

 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------

 10.10.10.1      00:50:56:c0:00:08      1      60  VMware, Inc.
 10.10.10.2      00:50:56:ee:64:88      1      60  VMware, Inc.
 10.10.10.12     00:0c:29:22:45:a3      1      60  VMware, Inc.
 10.10.10.254    00:50:56:fe:80:98      1      60  VMware, Inc.
```

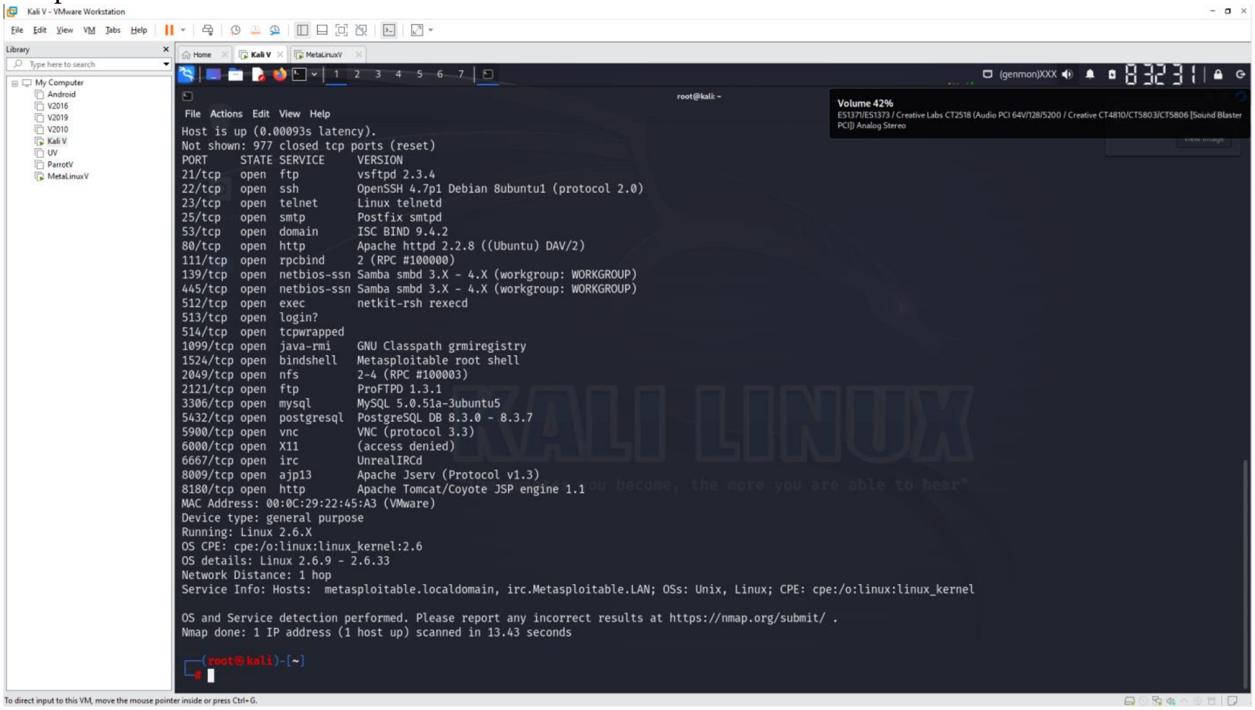
Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
Kali V
MetaLinuxV
root@kali: ~
File Actions Edit View Help
(genmon)XXX
8:31:09
KALI LINUX
"the quieter you become, the more you are able to hear"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

nmap -sS -p- 10.10.10.12



```
Host is up (0.0019s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
33769/tcp open  unknown
34876/tcp open  unknown
48716/tcp open  unknown
59330/tcp open  unknown
MAC Address: 00:0C:29:22:45:A3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.32 seconds

┌──(root㉿kali)-[~]
└─#
```

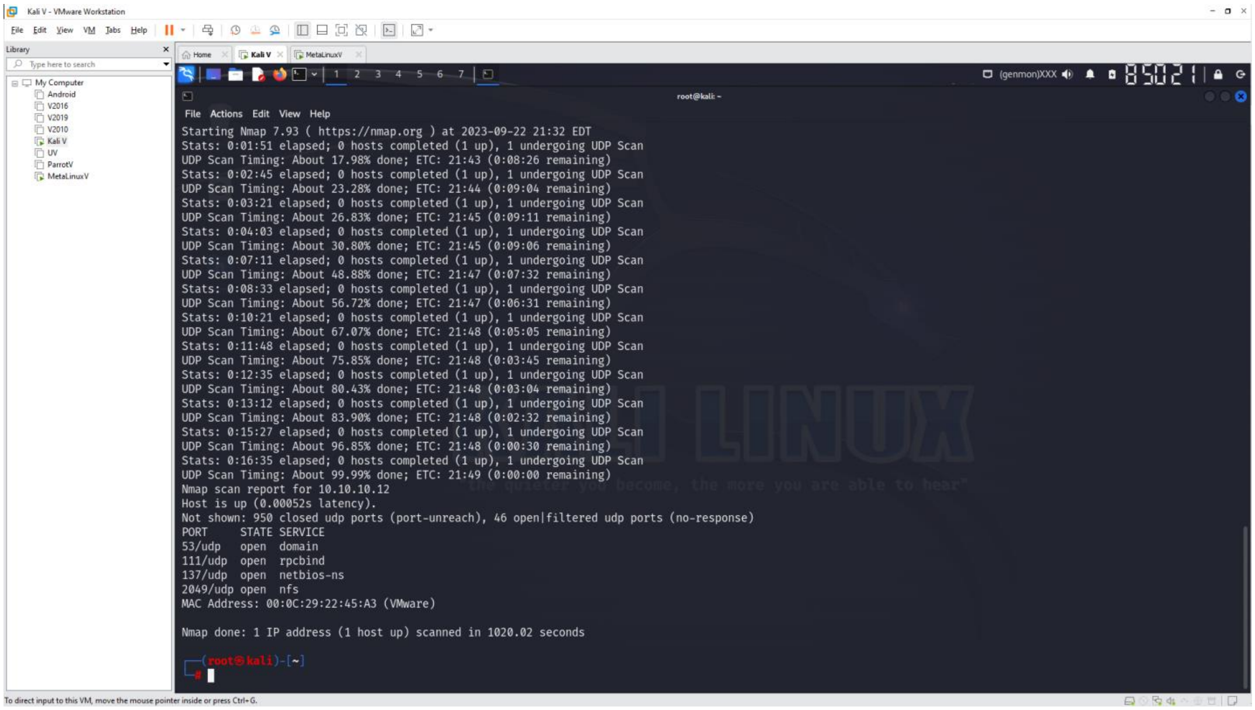
nmap -sS -sV -O 10.10.10.12



```
Host is up (0.00093s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:22:45:A3 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.43 seconds

┌──(root㉿kali)-[~]
└─#
```

Volume 42%
ES1371/ES1373 / Creative Labs CT2518 (Audio PCI 64V/128/5200 / Creative CT4810/CT5803/CT5806 [Sound Blaster PCI]) Analog Stereo

nmap -sU 10.10.10.12

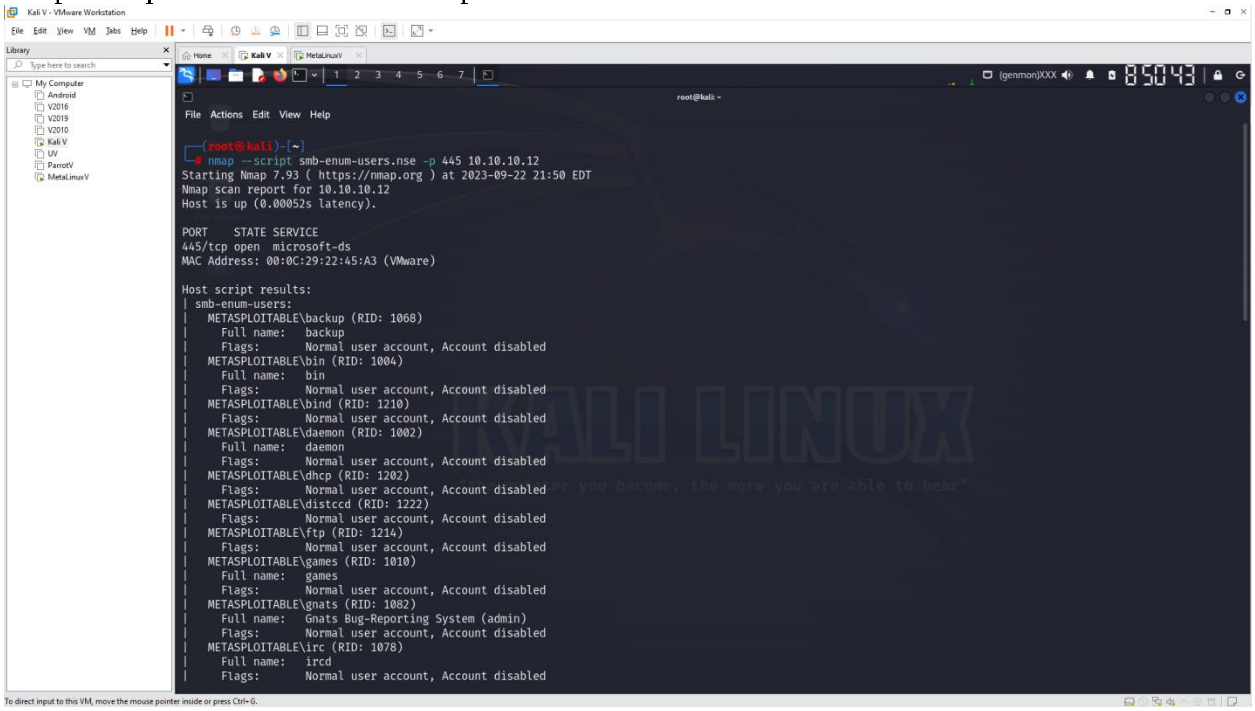


```
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-22 21:32 EDT
Stats: 0:01:51 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 17.98% done; ETC: 21:43 (0:08:26 remaining)
Stats: 0:02:45 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 23.28% done; ETC: 21:44 (0:09:04 remaining)
Stats: 0:03:21 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 26.83% done; ETC: 21:45 (0:09:11 remaining)
Stats: 0:04:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 30.80% done; ETC: 21:45 (0:09:06 remaining)
Stats: 0:07:11 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 48.88% done; ETC: 21:47 (0:07:32 remaining)
Stats: 0:08:33 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 56.72% done; ETC: 21:47 (0:06:31 remaining)
Stats: 0:10:21 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 67.07% done; ETC: 21:48 (0:05:05 remaining)
Stats: 0:11:48 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 75.85% done; ETC: 21:48 (0:03:45 remaining)
Stats: 0:12:35 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 80.43% done; ETC: 21:48 (0:03:04 remaining)
Stats: 0:13:12 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 83.90% done; ETC: 21:48 (0:02:32 remaining)
Stats: 0:15:27 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 96.85% done; ETC: 21:48 (0:00:30 remaining)
Stats: 0:16:35 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 21:49 (0:00:00 remaining)
Nmap scan report for 10.10.10.12
Host is up (0.00052s latency).
Not shown: 950 closed udp ports (port-unreach), 46 open|filtered udp ports (no-response)
PORT     STATE SERVICE
53/udp   open  domain
111/udp  open  rpcbind
137/udp  open  netbios-ns
2049/udp open  nfs
MAC Address: 00:0C:29:22:45:A3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1020.02 seconds

┌──(root㉿kali)-[~]
└─#
```

Task 2: Enumerating Users

Enumerating with Nmap

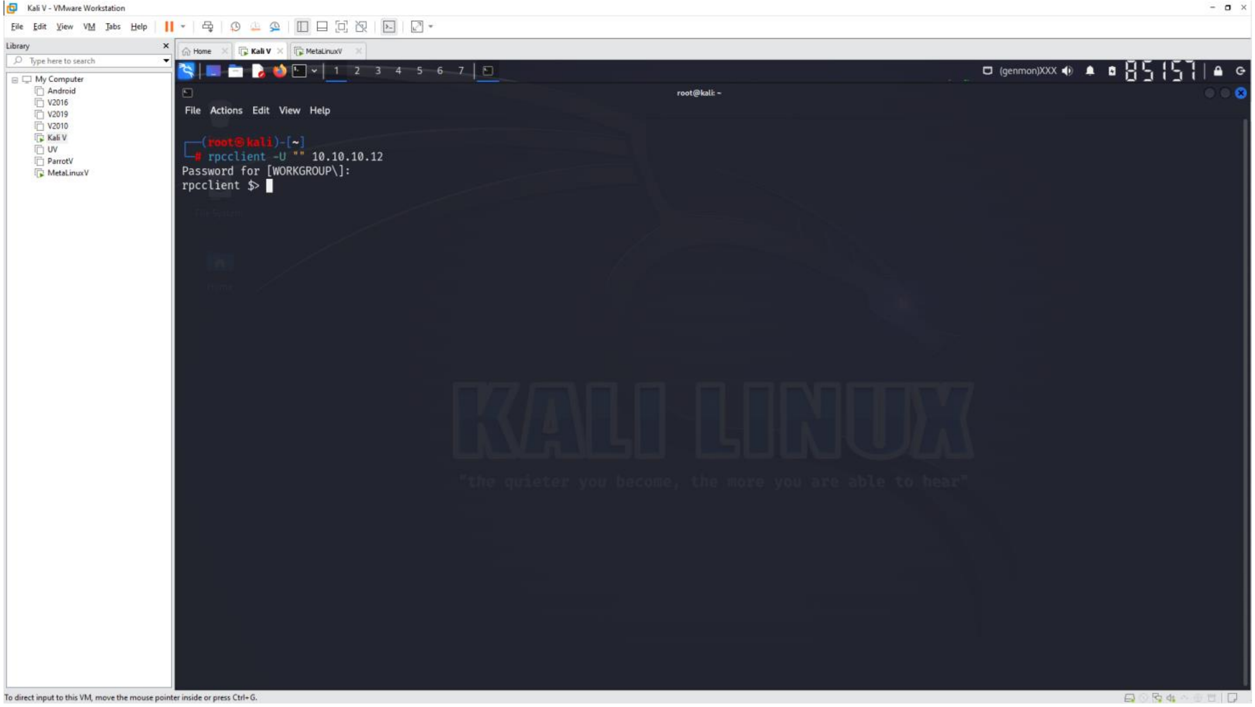
nmap --script smb-enum-users.nse -p 445 10.10.10.12



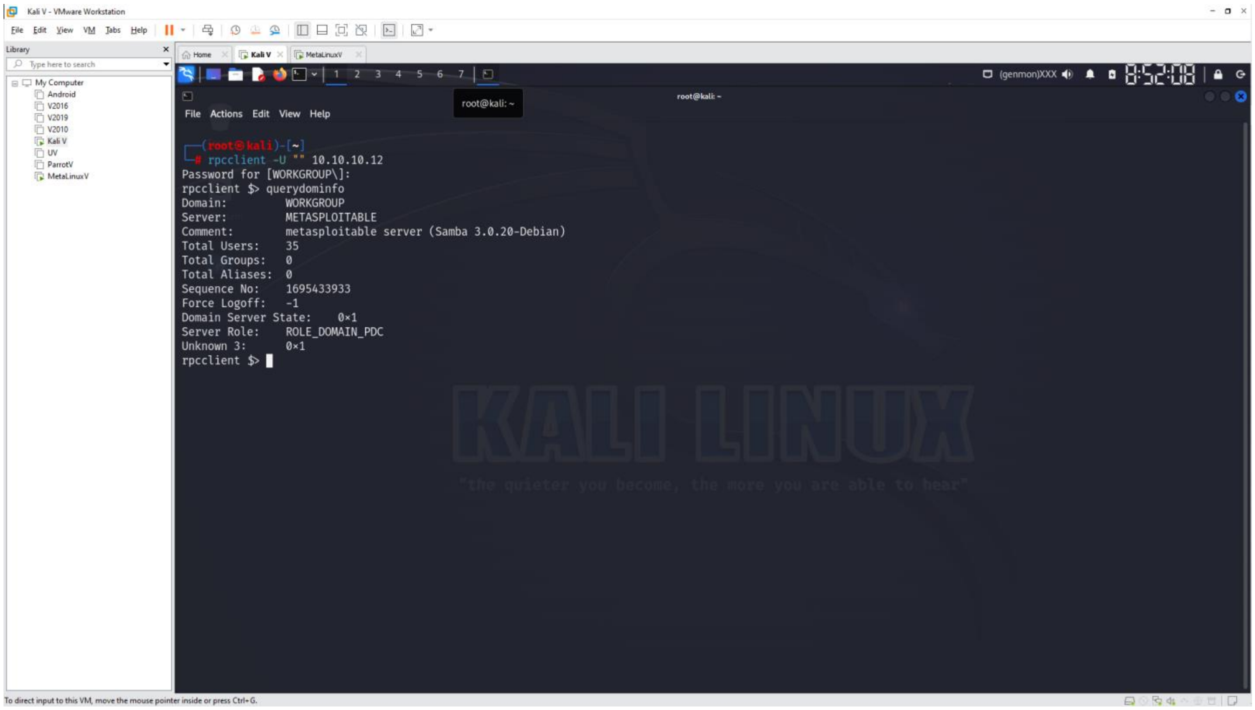
```
┌──(root㉿kali)-[~]
└─# nmap --script smb-enum-users.nse -p 445 10.10.10.12
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-22 21:50 EDT
Nmap scan report for 10.10.10.12
Host is up (0.00052s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:22:45:A3 (VMware)

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
|     Flags:       Normal user account, Account disabled
```

Enumerating with rpcclient

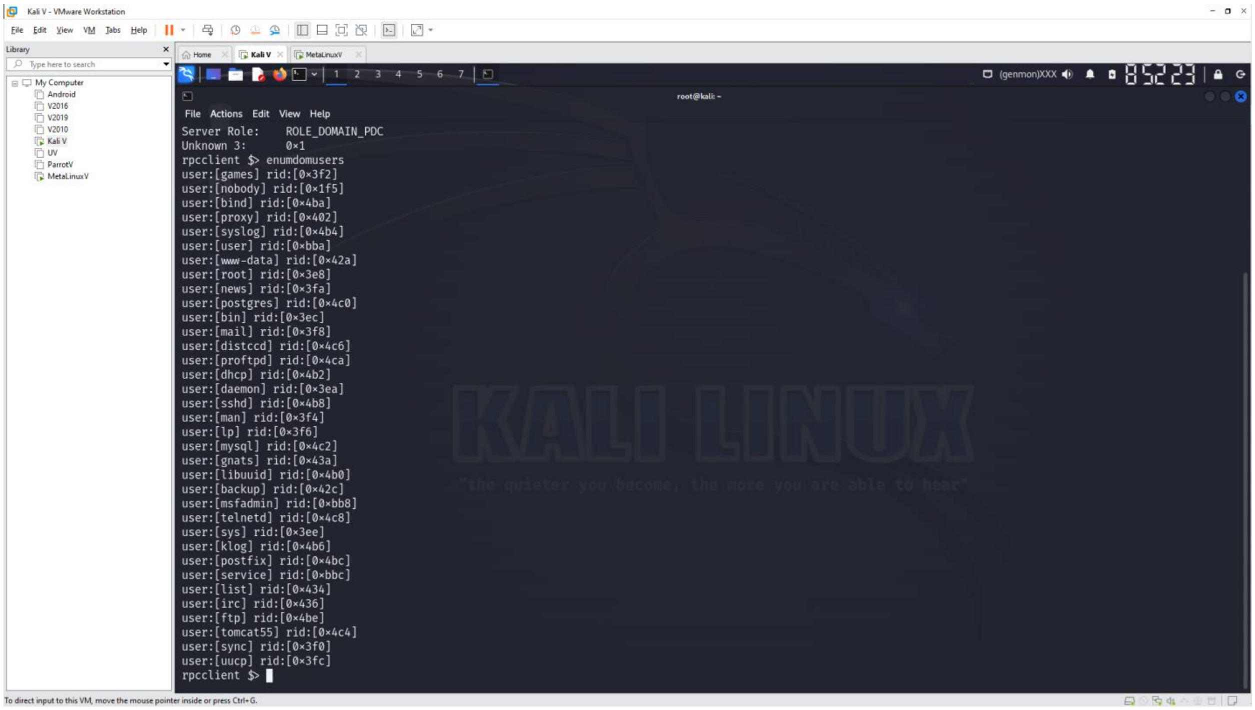
rpcclient -U "" 10.10.10.12



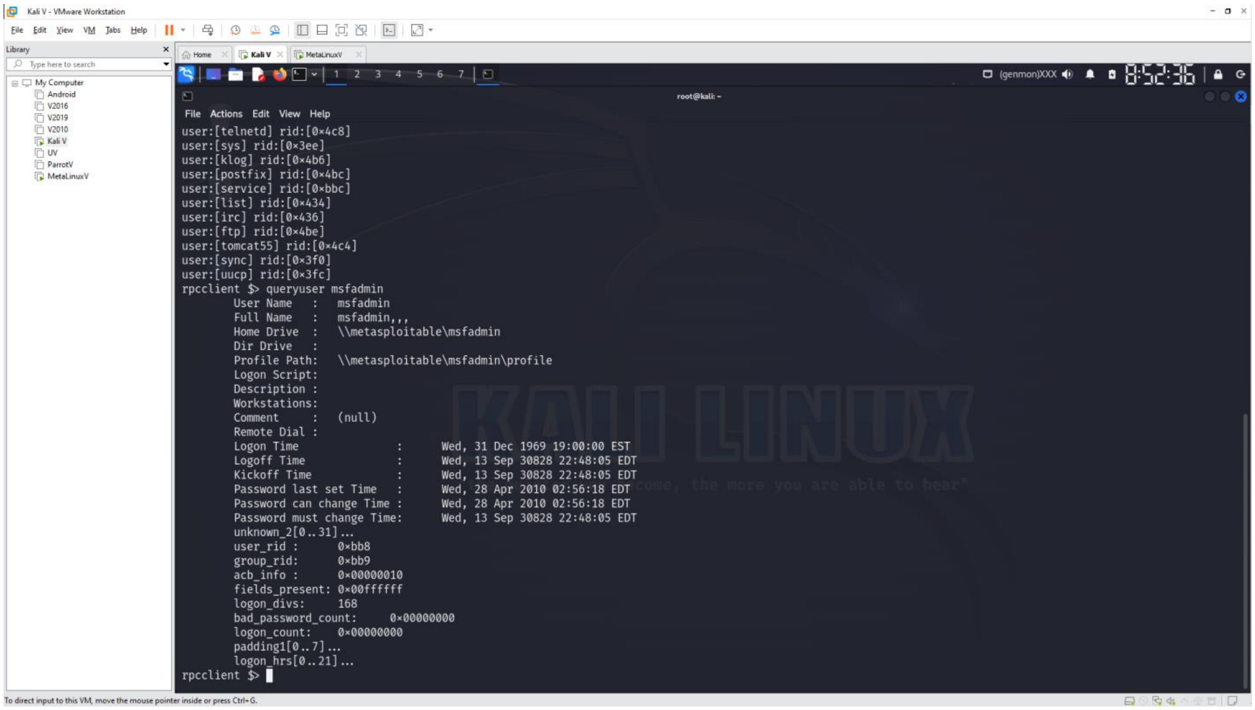
```
┌──(root㉿kali)-[~]
└─# rpcclient -U "" 10.10.10.12
Password for [WORKGROUP\]:
rpcclient $> 
```



```
┌──(root㉿kali)-[~]
└─# rpcclient -U "" 10.10.10.12
Password for [WORKGROUP\]:
rpcclient $> querydominfo
Domain:         WORKGROUP
Server:         METASPLOITABLE
Comment:        metasploitable server (Samba 3.0.20-Debian)
Total Users:    35
Total Groups:   0
Total Aliases:  0
Sequence No:    1695433933
Force Logoff:   -1
Domain Server State:    0x1
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> 
```

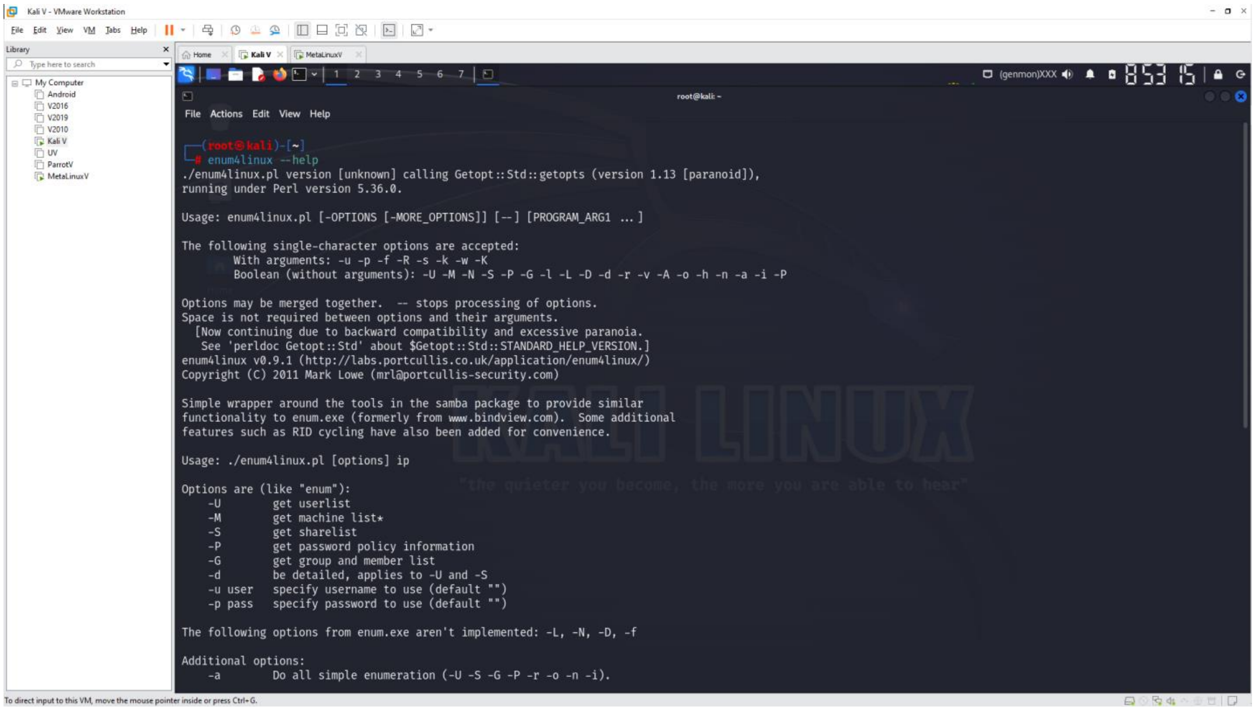


```
Server Role:    ROLE_DOMAIN_PDC
Unknown 3:      0x1
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
rpcclient $> 
```



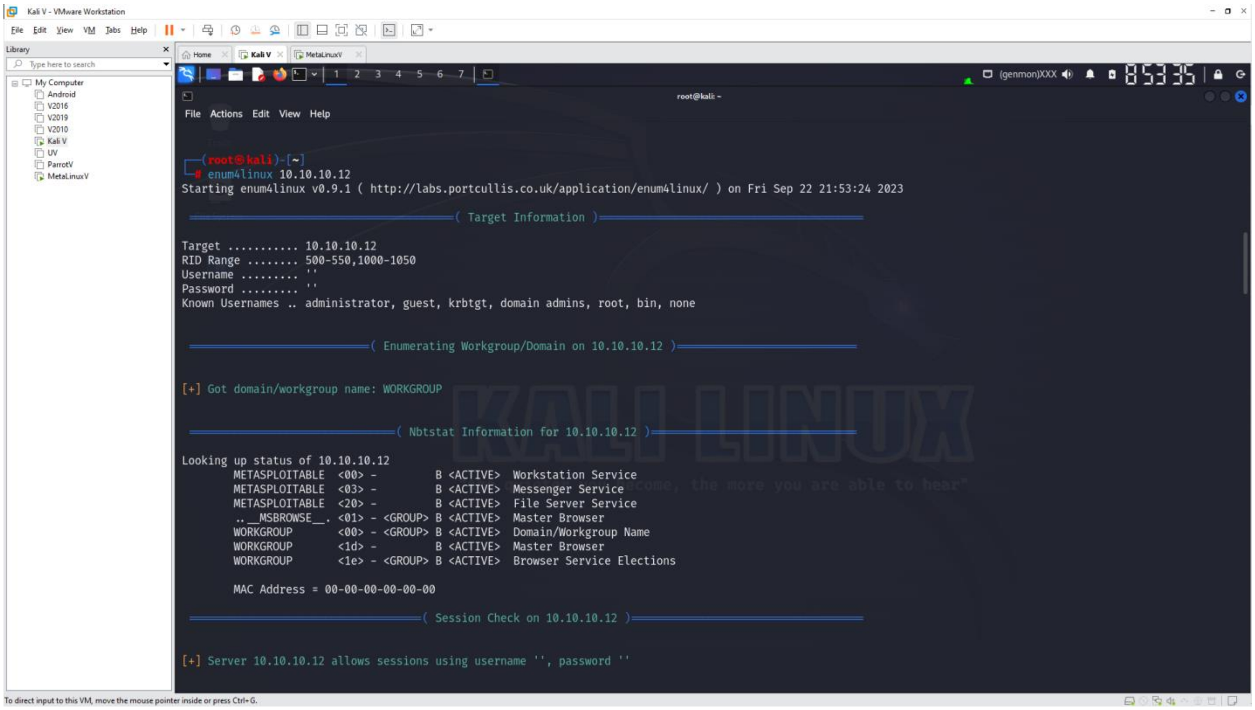
```
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
rpcclient $> queryuser msfadmin
        User Name   :   msfadmin
        Full Name   :   msfadmin,,,
        Home Drive  :   \\metasploitable\msfadmin
        Dir Drive   :
        Profile Path:   \\metasploitable\msfadmin\profile
        Logon Script:
        Description :
        Workstations:
        Comment     :   (null)
        Remote Dial :
        Logon Time               :      Wed, 31 Dec 1969 19:00:00 EST
        Logoff Time              :      Wed, 13 Sep 30828 22:48:05 EDT
        Kickoff Time             :      Wed, 13 Sep 30828 22:48:05 EDT
        Password last set Time   :      Wed, 28 Apr 2010 02:56:18 EDT
        Password can change Time :      Wed, 28 Apr 2010 02:56:18 EDT
        Password must change Time:      Wed, 13 Sep 30828 22:48:05 EDT
        unknown_2[0..31]...
        user_rid :      0xbb8
        group_rid:      0xbb9
        acb_info :      0x00000010
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000000
        padding1[0..7]...
        logon_hrs[0..21]...
rpcclient $> 
```

Enumerating with enum4linux



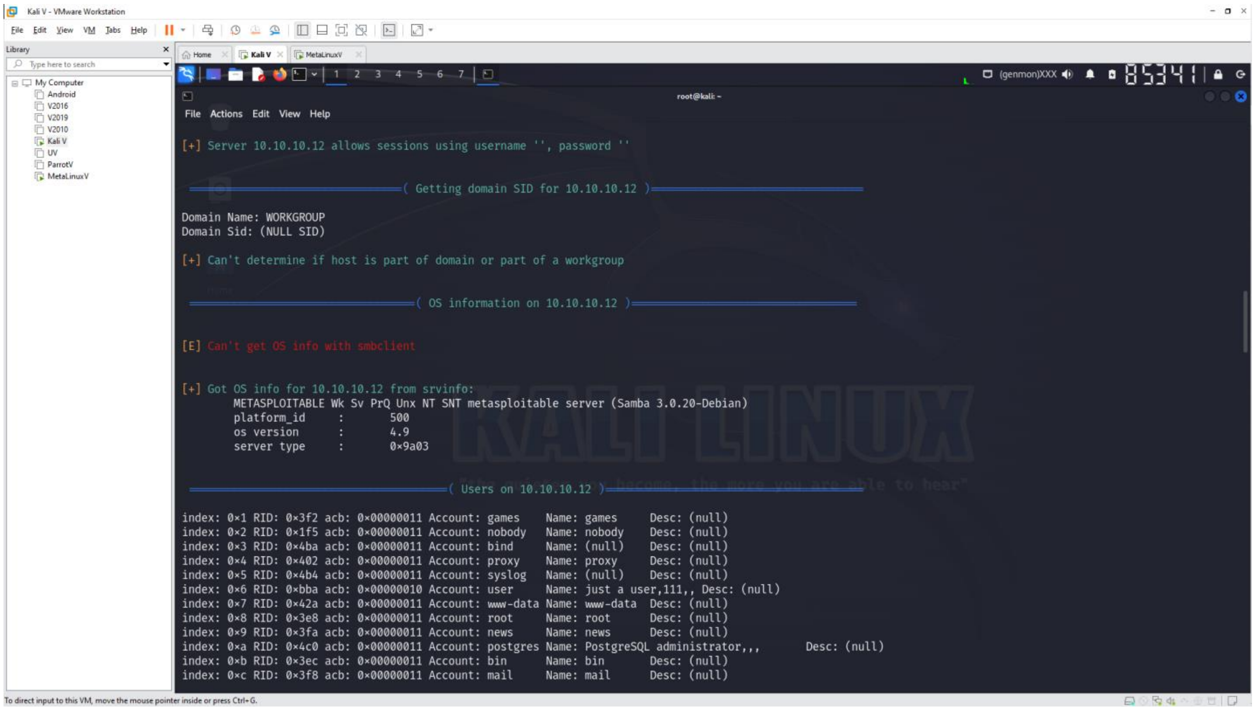
```
┌──(root㉿kali)-[~]
└─# enum4linux --help
./enum4linux.pl version [unknown] calling Getopt::Std::getopts (version 1.13 [paranoid]),
running under Perl version 5.36.0.

Usage: enum4linux.pl [-OPTIONS [-MORE_OPTIONS]] [--] [PROGRAM_ARG1 ...]

The following single-character options are accepted:
        With arguments: -u -p -f -R -s -k -w -K
        Boolean (without arguments): -U -M -N -S -P -G -l -L -D -d -r -v -A -o -h -n -a -i -P

Options may be merged together.  -- stops processing of options.
Space is not required between options and their arguments.
  [Now continuing due to backward compatibility and excessive paranoia.
   See 'perldoc Getopt::Std' about $Getopt::Std::STANDARD_HELP_VERSION.]
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com).  Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
```

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



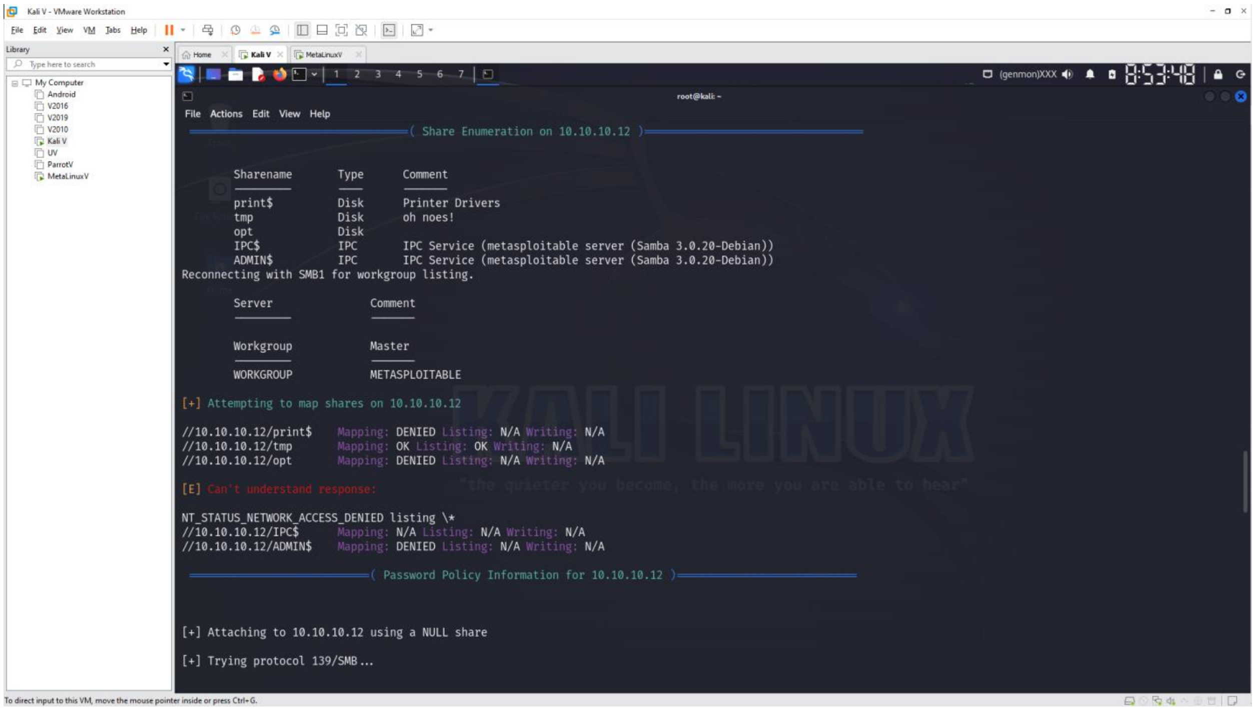
```
┌──(root㉿kali)-[~]
└─# enum4linux 10.10.10.12
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Sep 22 21:53:24 2023

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

Target ........... 10.10.10.12
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===========================( Enumerating Workgroup/Domain on 10.10.10.12 )===========================


[+] Got domain/workgroup name: WORKGROUP


 ===============================( Nbtstat Information for 10.10.10.12 )===============================

Looking up status of 10.10.10.12
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

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

 ===================================( Session Check on 10.10.10.12 )===================================


[+] Server 10.10.10.12 allows sessions using username '', password ''
```

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



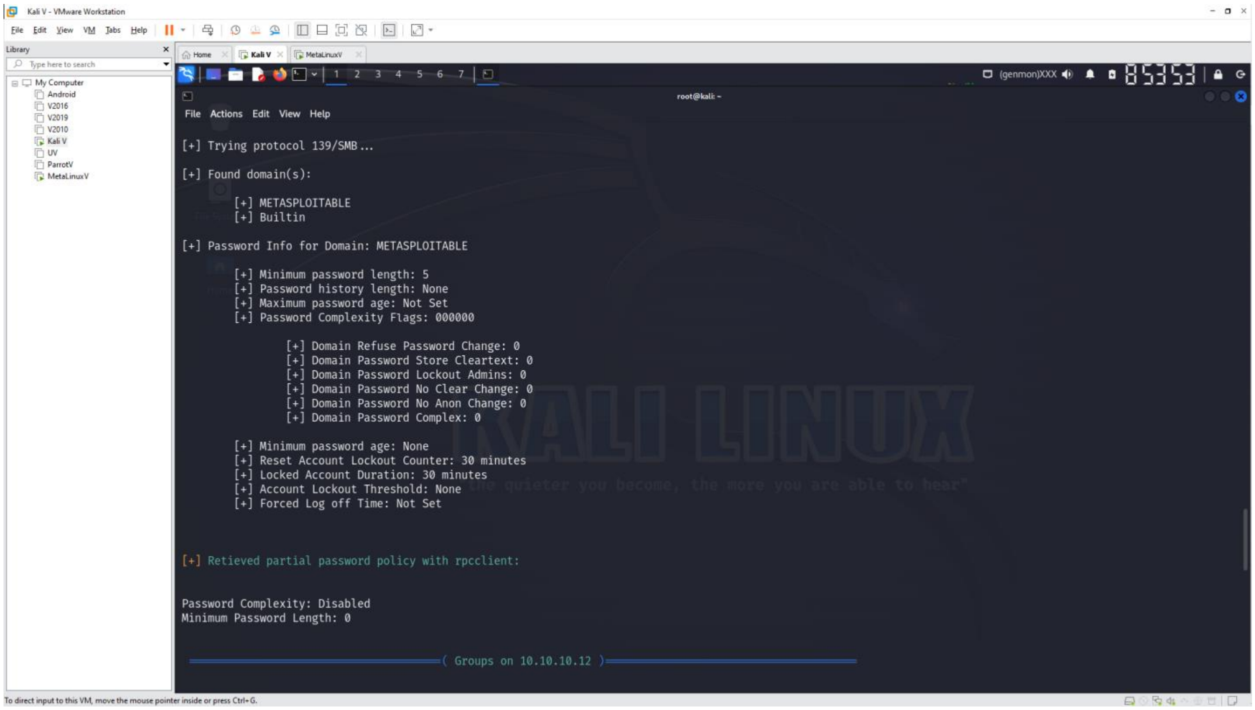
```
[+] Server 10.10.10.12 allows sessions using username '', password ''


 ══════════════════════════════( Getting domain SID for 10.10.10.12 )══════════════════════════════

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

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


 ════════════════════════════════( OS information on 10.10.10.12 )════════════════════════════════


[E] Can't get OS info with smbclient


[+] Got OS info for 10.10.10.12 from srvinfo:
        METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
        platform_id     :       500
        os version      :       4.9
        server type     :       0×9a03


 ═════════════════════════════════════( Users on 10.10.10.12 )═════════════════════════════════════

index: 0×1 RID: 0×3f2 acb: 0×00000011 Account: games    Name: games     Desc: (null)
index: 0×2 RID: 0×1f5 acb: 0×00000011 Account: nobody   Name: nobody    Desc: (null)
index: 0×3 RID: 0×4ba acb: 0×00000011 Account: bind     Name: (null)    Desc: (null)
index: 0×4 RID: 0×402 acb: 0×00000011 Account: proxy    Name: proxy     Desc: (null)
index: 0×5 RID: 0×4b4 acb: 0×00000011 Account: syslog   Name: (null)    Desc: (null)
index: 0×6 RID: 0×bba acb: 0×00000010 Account: user     Name: just a user,111,, Desc: (null)
index: 0×7 RID: 0×42a acb: 0×00000011 Account: www-data Name: www-data  Desc: (null)
index: 0×8 RID: 0×3e8 acb: 0×00000011 Account: root     Name: root      Desc: (null)
index: 0×9 RID: 0×3fa acb: 0×00000011 Account: news     Name: news      Desc: (null)
index: 0×a RID: 0×4c0 acb: 0×00000011 Account: postgres Name: PostgreSQL administrator,,,       Desc: (null)
index: 0×b RID: 0×3ec acb: 0×00000011 Account: bin      Name: bin       Desc: (null)
index: 0×c RID: 0×3f8 acb: 0×00000011 Account: mail     Name: mail      Desc: (null)
```

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

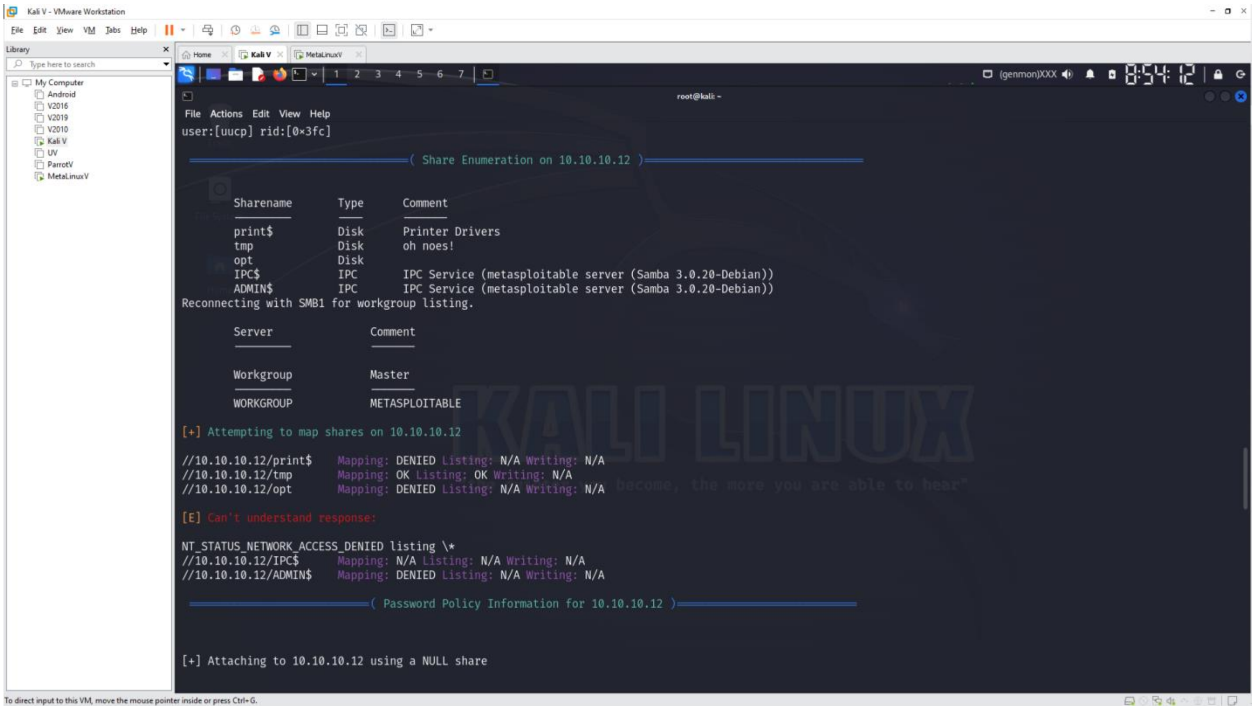


```
 ═══════════════════════════════( Share Enumeration on 10.10.10.12 )═══════════════════════════════


        Sharename       Type      Comment
        ─────────       ────      ───────
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ─────────            ───────

        Workgroup            Master
        ─────────            ───────
        WORKGROUP            METASPLOITABLE

[+] Attempting to map shares on 10.10.10.12

//10.10.10.12/print$    Mapping: DENIED Listing: N/A Writing: N/A
//10.10.10.12/tmp       Mapping: OK Listing: OK Writing: N/A
//10.10.10.12/opt       Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//10.10.10.12/IPC$      Mapping: N/A Listing: N/A Writing: N/A
//10.10.10.12/ADMIN$    Mapping: DENIED Listing: N/A Writing: N/A

 ═══════════════════════════( Password Policy Information for 10.10.10.12 )═══════════════════════════



[+] Attaching to 10.10.10.12 using a NULL share

[+] Trying protocol 139/SMB ...
```

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


Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
Kali V
MetaLinuxV
1 2 3 4 5 6 7
(genmon)XXX
8:53:53
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
[+] Trying protocol 139/SMB ...

[+] Found domain(s):

        [+] METASPLOITABLE
        [+] Builtin

[+] Password Info for Domain: METASPLOITABLE

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set



[+] Retieved partial password policy with rpcclient:


Password Complexity: Disabled
Minimum Password Length: 0


 ======================================( Groups on 10.10.10.12 )======================================
```


Kali V - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Android
V2016
V2019
V2010
Kali V
UV
ParrotV
MetaLinuxV
Home
Kali V
MetaLinuxV
1 2 3 4 5 6 7
(genmon)XXX
8:54:12
root@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
user:[uucp] rid:[0x3fc]

 ==================================( Share Enumeration on 10.10.10.12 )==================================


        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE

[+] Attempting to map shares on 10.10.10.12

//10.10.10.12/print$    Mapping: DENIED Listing: N/A Writing: N/A
//10.10.10.12/tmp       Mapping: OK Listing: OK Writing: N/A
//10.10.10.12/opt       Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//10.10.10.12/IPC$      Mapping: N/A Listing: N/A Writing: N/A
//10.10.10.12/ADMIN$    Mapping: DENIED Listing: N/A Writing: N/A

 ============================( Password Policy Information for 10.10.10.12 )============================



[+] Attaching to 10.10.10.12 using a NULL share
```