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: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)

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

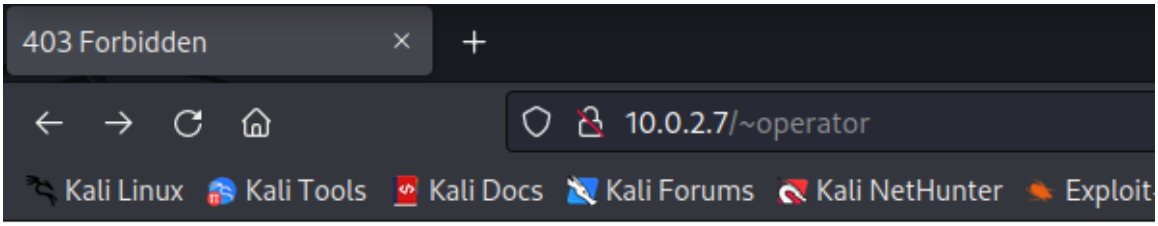
nikto:

```
+ 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

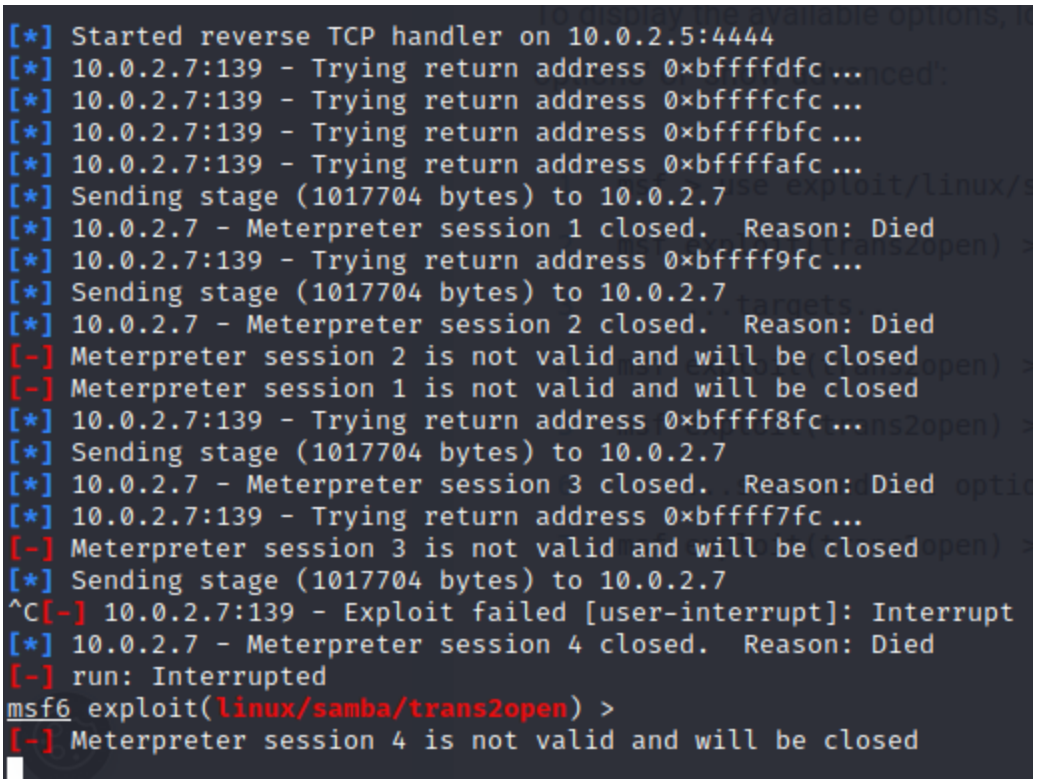
```
  9   auxiliary/scanner/sap/sap_soap_rfc_pfl_check_o
  10  auxiliary/scanner/sap/sap_soap_rfc_rzl_read_di
  11  auxiliary/scanner/smb/smb_enumusers_domain
  12  auxiliary/scanner/smb/smb_enum_gpp
  13  auxiliary/scanner/smb/smb_login
  14  auxiliary/scanner/smb/smb_lookupsid
  15  auxiliary/admin/smb/check_dir_file
  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) >
```

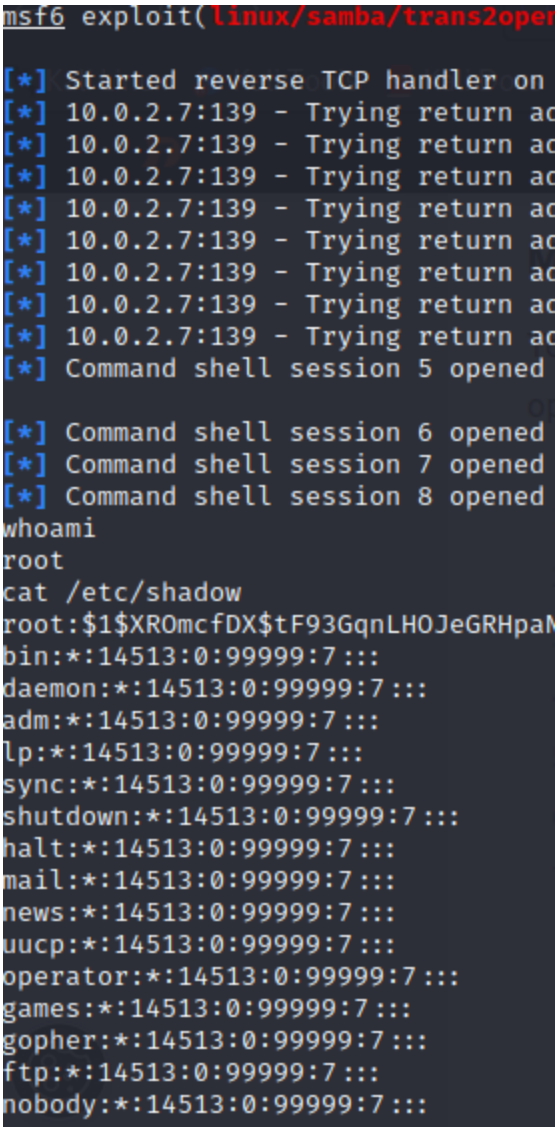
After I do some research on google finding out more about Samba 2.2.1 and I find several articles stating that it is vulnerable to an exploit called 'trans2open'. so i search metasploit to see if there is anything i can use

```
#  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

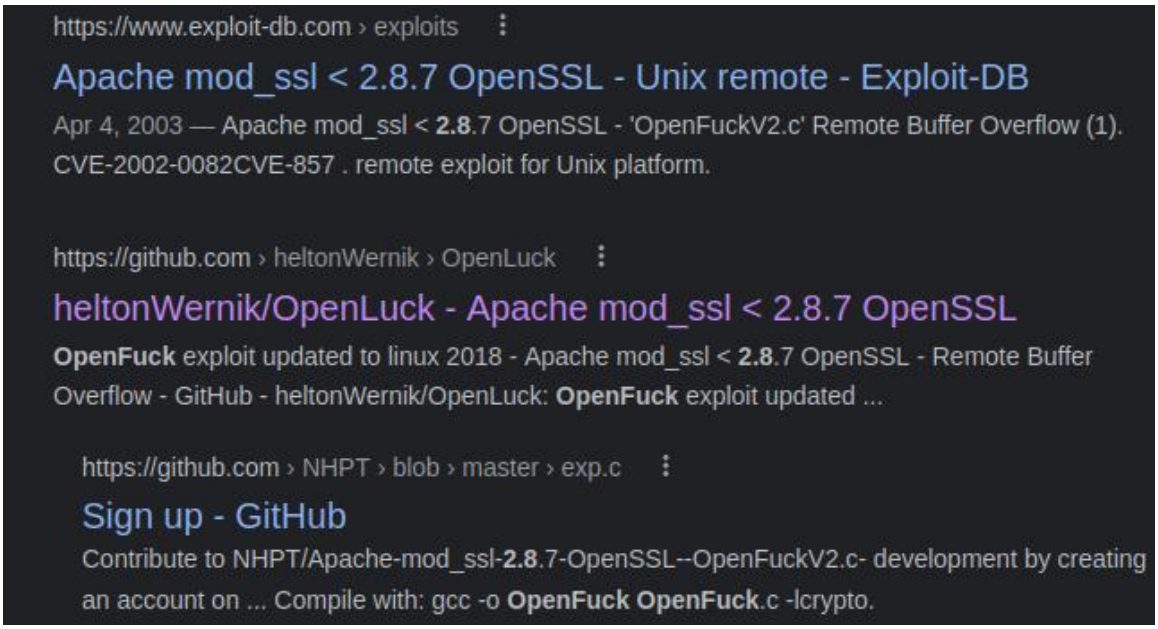


but the session will not open. I attempt to change the payload and try again

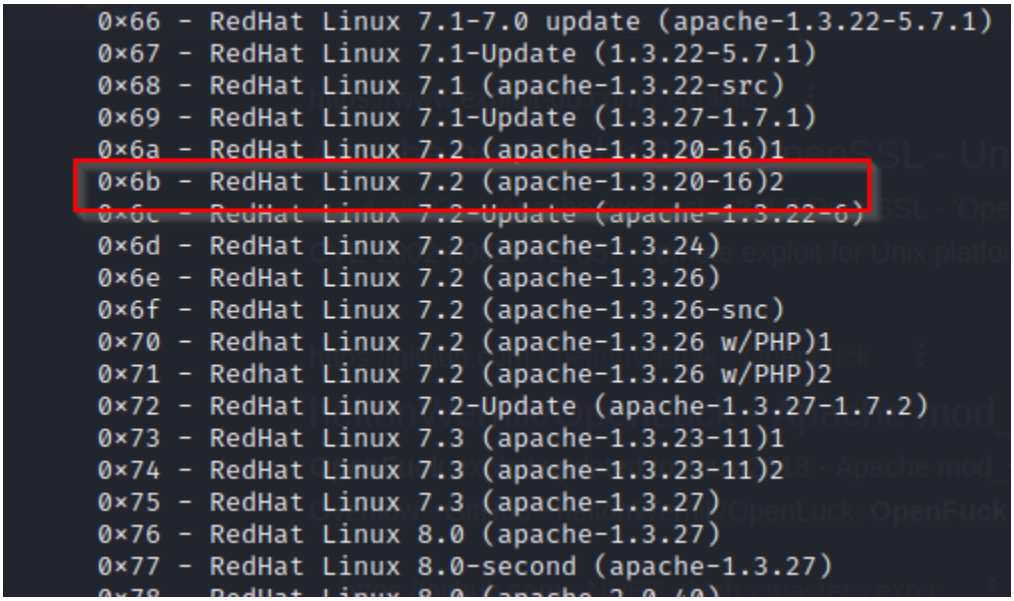


and root was achieved.

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.



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



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.

and root was achieved.