

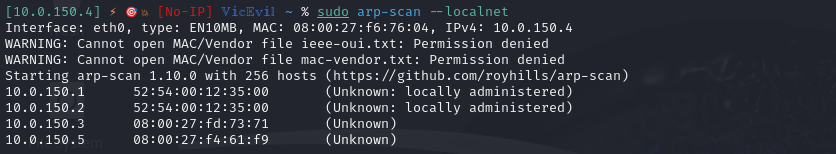
**SPRINGO 18**

**TEAM CHALLENGE**

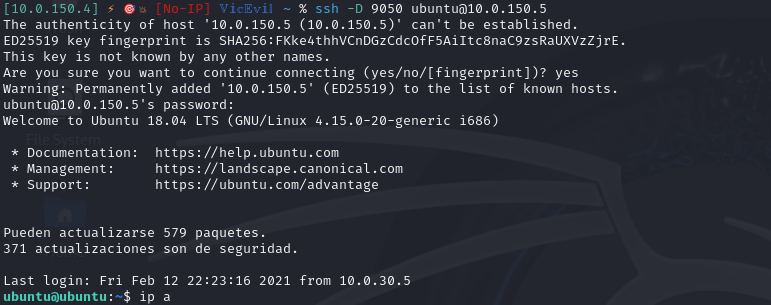
**RETO SSH - PIVOTING**

33412KALI Y PIVOTING EN MAQUINAS VIRTUALES

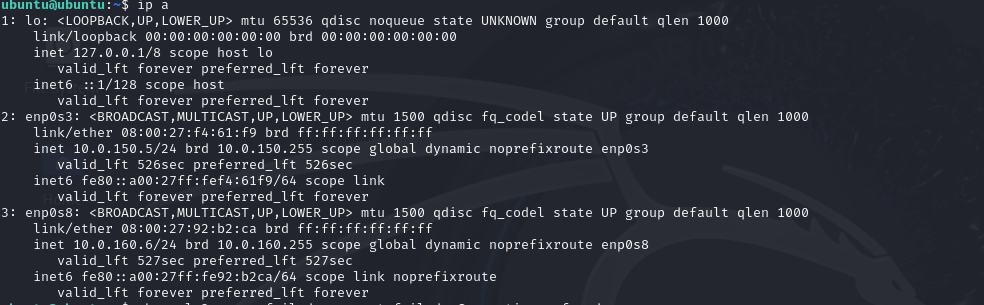
1 ESCANEO



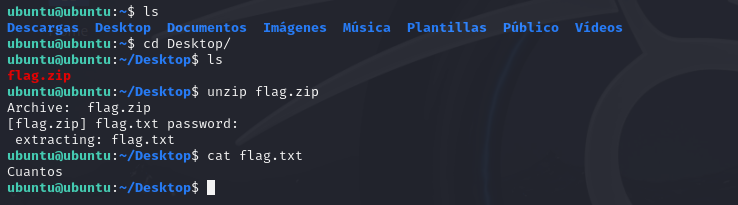
1. - PIVINTING 1 IP/.5
2. SSH -D ubuntu@IP.5 (tunel dinamico)



IPA

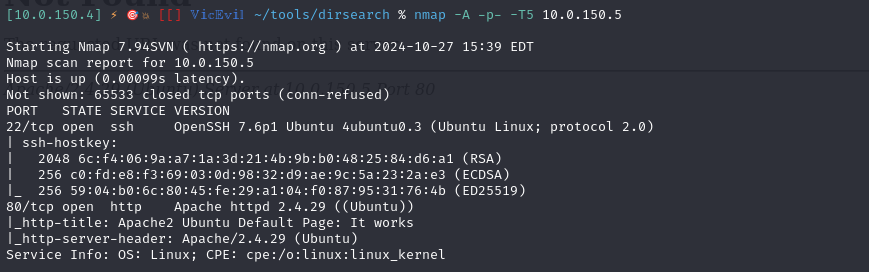


primera pista: CUANTOS, me la llevo a la kali metodo python -wget

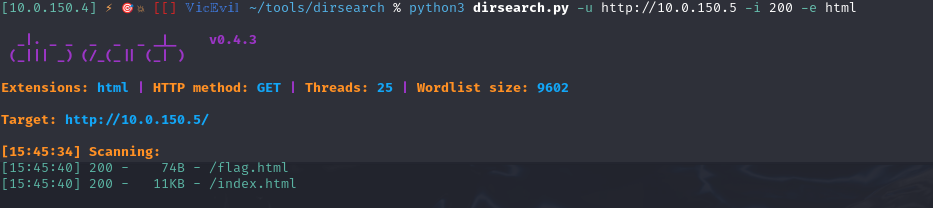




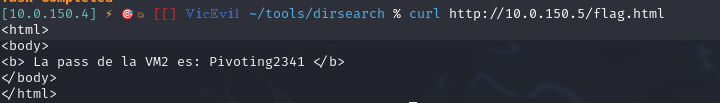
mapeo a PV1

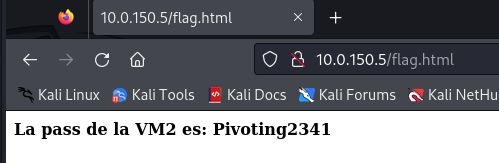


uso dirsearch en la Ip de PV1 por el port 80:

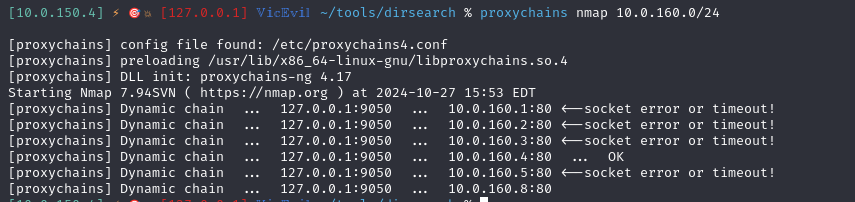


contraseña PV2



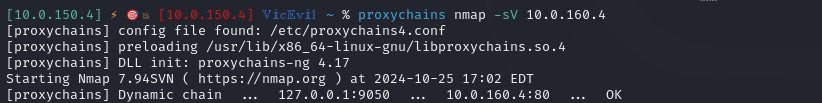


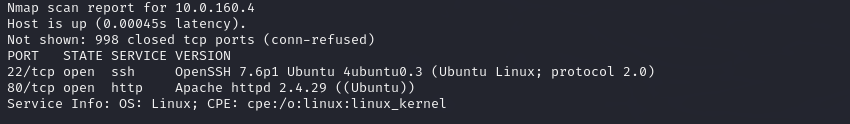
a traves del tunel dinamico

10

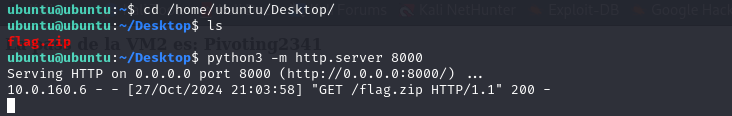
P pivoting 2 10.0.160.4

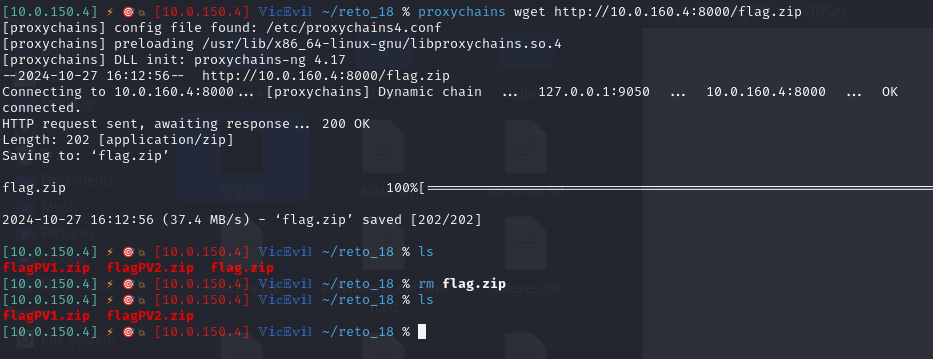
nmap



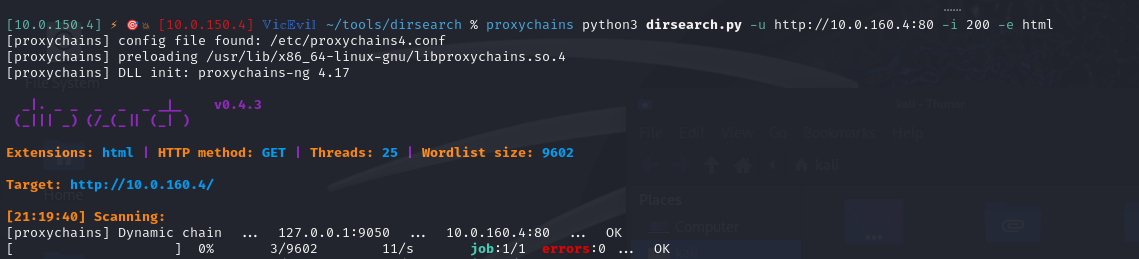


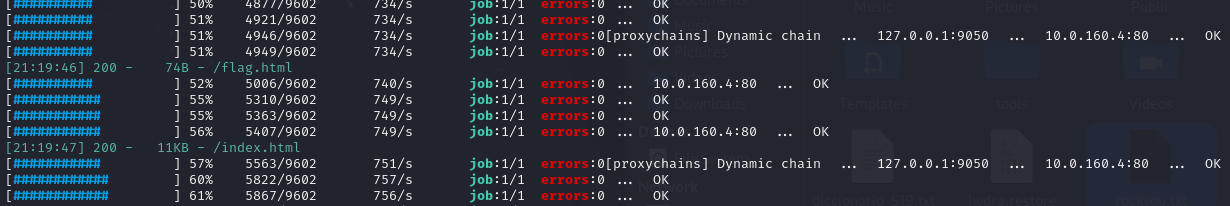
me traigo el flag que esta en la carpeta Desktop



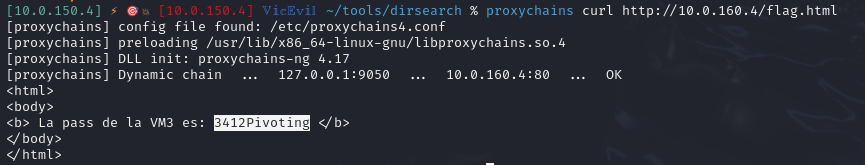


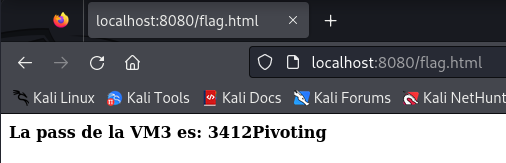
ATACAMOS MEDIANTE DIRSEARCH SIN DICCIONARIO CON LOS FLAG -i 200 -e html



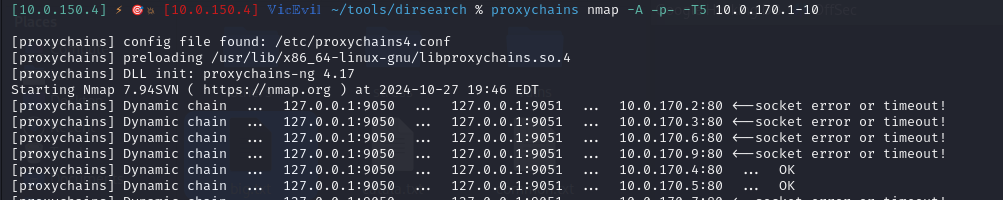


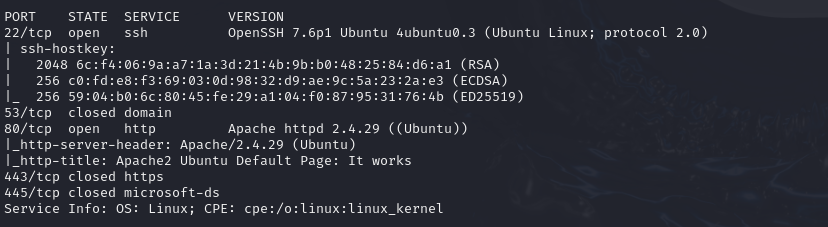
CONSEGUMOS LA PASS DE LA PIVOTING 3



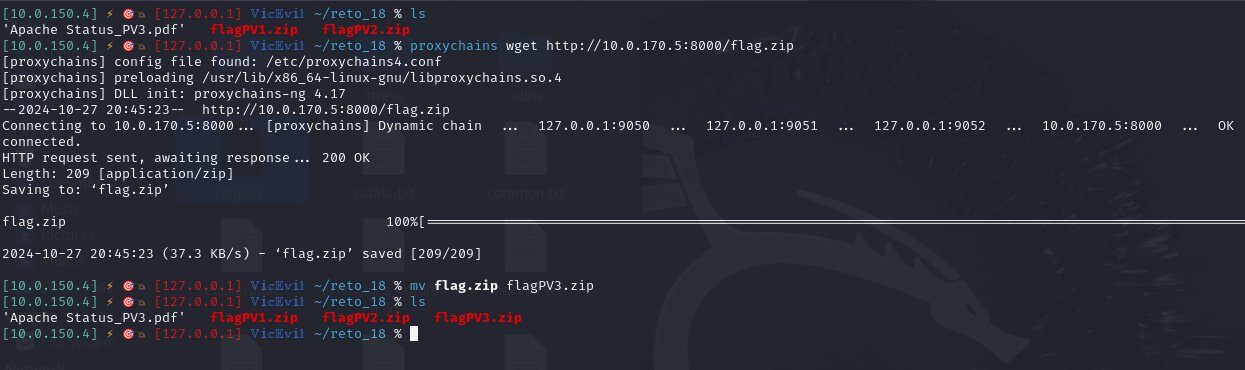


donne tengo abierto el tunel dinamico en la pv1 ejecuto otro nuevo Tunel dinamico a la PV2 por el puerto 9051 del proxychains, procediendo a escanear des kali con nmap para localizae la IP de la PV3= 10.0.170.5.

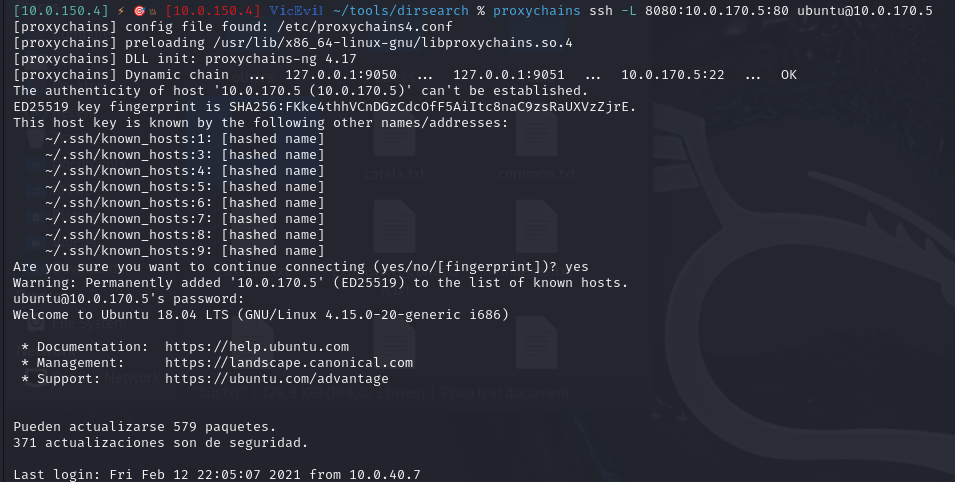




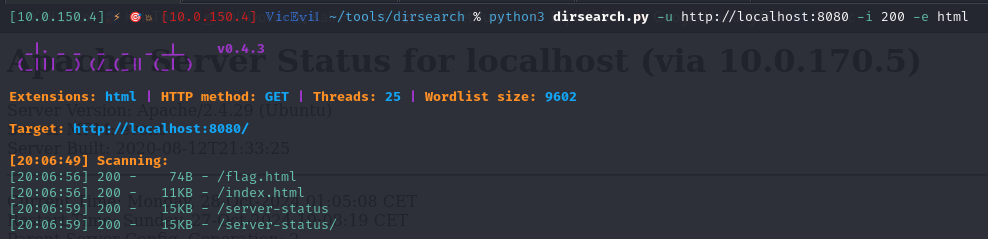
con la Ip y la contraseña se procede a sucooexion por shh para inspeccionarla encontrado un flag.zip el cual es trasladado por el metodo python -wget a la kali



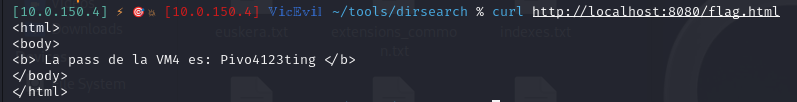
Creo un tunel local para poder ver el servicio del puerto 80 en la kali

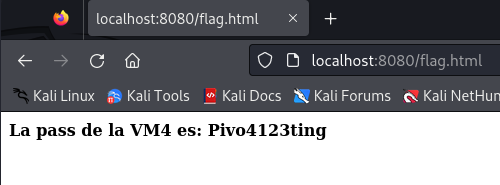


y tras atacarlo con dirsearch

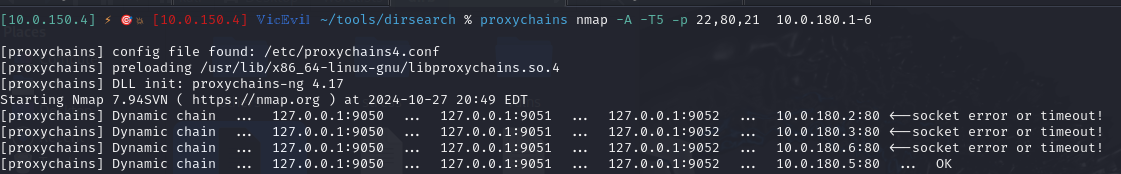


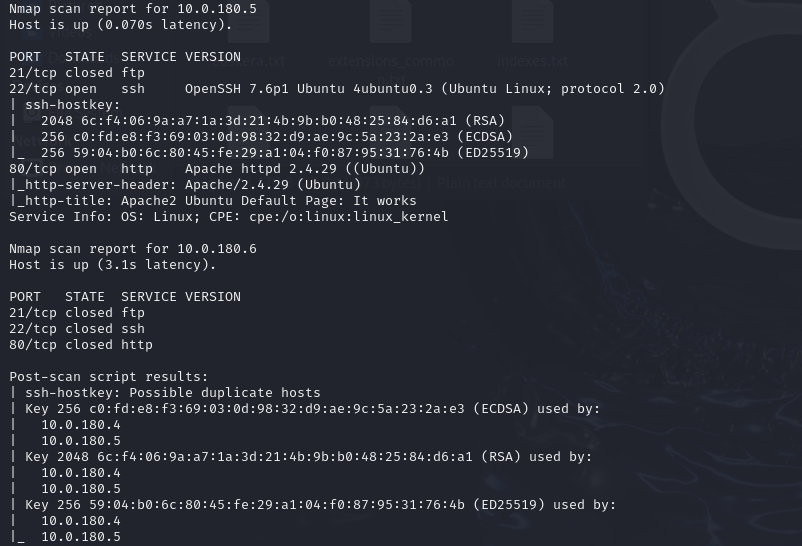
resulyanbo



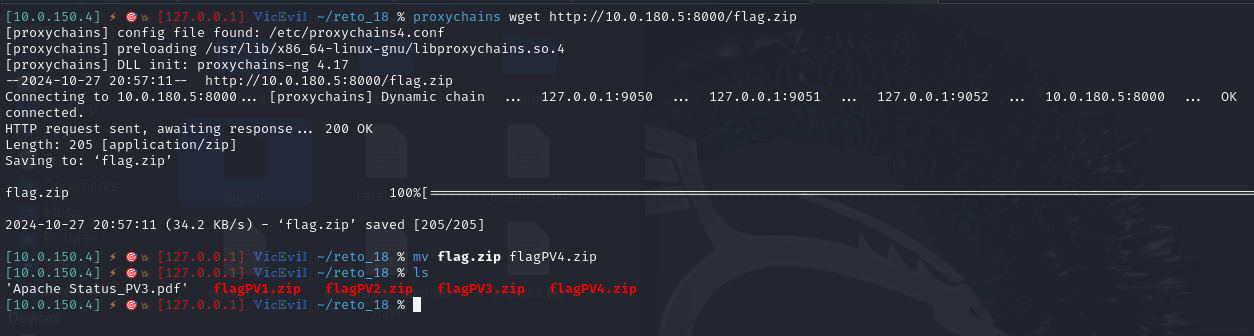


escaneo de nuevo con map, no sin antes haber concatenado detras del ultimo tunel dinamico un tecer tunel dinamico a travesd e PV3 por el puerto de proxychains 9052:

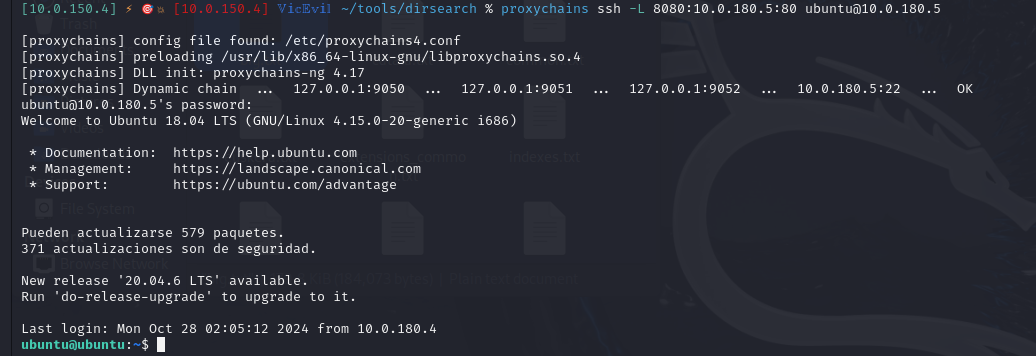


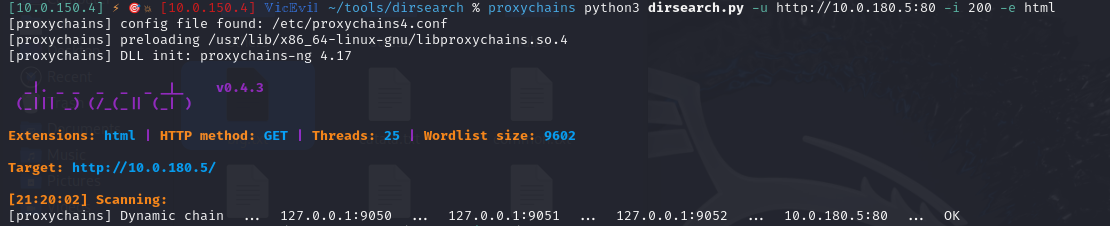
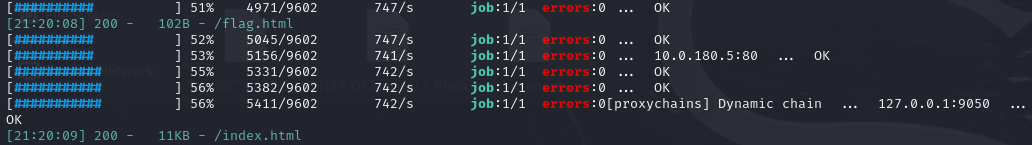


se proce a conexion via ssh con la Ip PV4 con proxysaihn, y una vez conectado en el escritorio encontramos la 4 flag, la cual, es llevada a la kali mediante el metodo python-wget

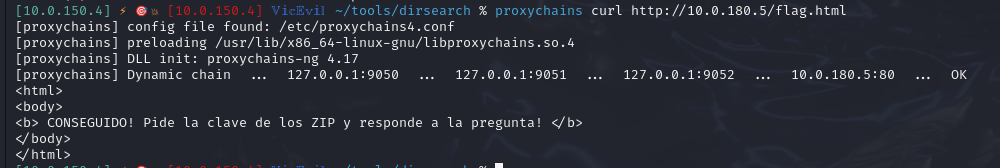


finalmente, para ver el contenido del puerto 80, abro un tunel local con la IP de la PV4:

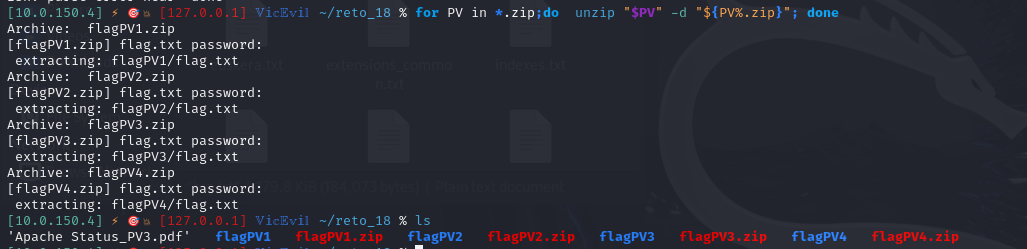


Le hago un dirsearch  
  
  


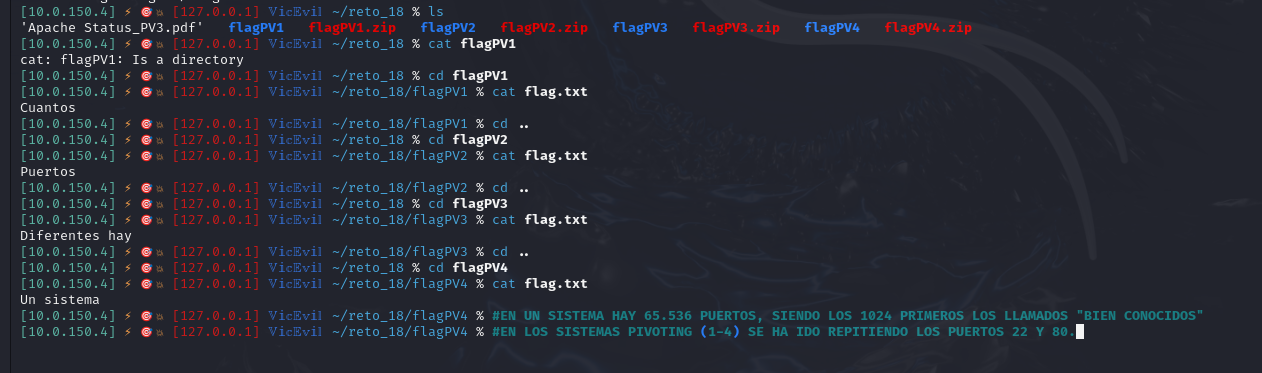
le hago un crul al flag:



Ahora voy a la capreta de mi kali reto \_18 donde he almacenado todos los flags de las Pviotings, realziando primeramente una descoimprension de los archivos.zip



LECTURA Y RESPUESTA



LA PREGUNTA ES: ¿Cuántos puertos diferentes hay en un sistema?

En un sistema, existen 65,536 puertos en total, numerados del 0 al 65,535. Estos se dividen en tres rangos principales:

Puertos Bien Conocidos (Well-Known Ports): Del 0 al 1023

Son puertos reservados para servicios y aplicaciones estándar, como HTTP (80), HTTPS (443), FTP (21), SSH (22), entre otros.

Puertos Registrados: Del 1024 al 49,151

Estos puertos son comúnmente asignados a aplicaciones o servicios específicos, aunque no están estrictamente reservados. Muchos servicios que no tienen puertos bien conocidos suelen usar puertos en este rango.

Puertos Dinámicos o Privados: Del 49,152 al 65,535

Estos puertos son utilizados para conexiones temporales y suelen ser asignados dinámicamente por el sistema operativo para conexiones cliente (por ejemplo, al navegar por Internet o realizar conexiones de red).

Cada puerto puede ser asignado a un servicio o aplicación, y muchos sistemas operativos gestionan los puertos dinámicamente para permitir múltiples conexiones simultáneas.

### Explicación del Flujo de Tráfico

1. **Kali** -> **PV1** (SOCKS en 9050 -red 10.0.150.0/24 y 10.0.160.0/24)
2. **PV1** -> **PV2** (SOCKS en 9051- red 10.0.160.0/24 y 10.0.170.0/24)
3. **PV2** -> **PV3** (SOCKS en 9052 -red 10.0.170.0/24 y 10.0.180.0/24)
4. PV4 -> red 10.0.180.0/24