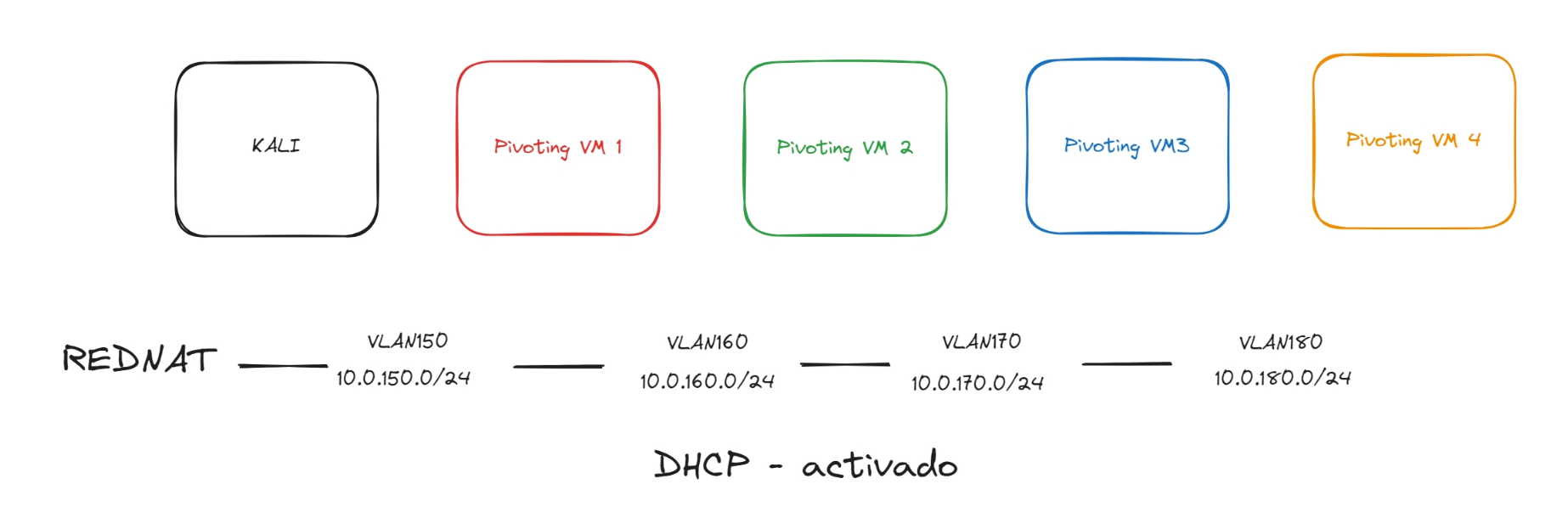


**SPRINGO 18**

**TEAM CHALLENGE**

**RETO SSH - PIVOTING**

Para la realización de este Team Challenge, se han conectado 5 maquinas virtuales a la red como se muestra en la imagen:



Para llevar a cabo la conexión de las máquinas, así como para conseguir las distintas credenciales de acceso a cada una de las máquinas y los archivos *“flag.zip”* para poder conseguir responder a la pregunta final que se formula en este Team Challenge, se han realizado las siguientes gestiones:

1. Se procede a un escaneo mediante la herramienta “arp-scan” desde la máquina Kali para conocer la IP de la maquina *“Pivoting VM 1”* (PV1, en adelante):

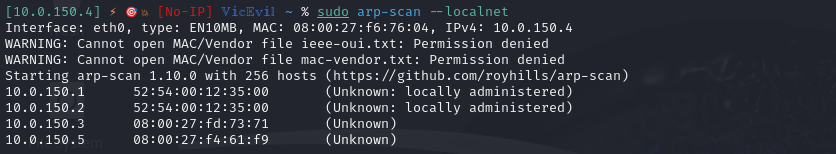


Imagen 1.- escaner de IPs en la misma red, siendo la **PV1: 10.0.150.5**

1. - Se conecta por el protocolo SSH (Secure Shell) a la maquina PV1, dado que conocemos el usuario y contraseña: “ubuntu”, estableciendo un túnel dinámico por el puerto 9050, redirigiendo el tráfico de manera segura a través de un servidor intermediario, permitiendo el acceso a recursos de otra red, como si fuera un proxy.

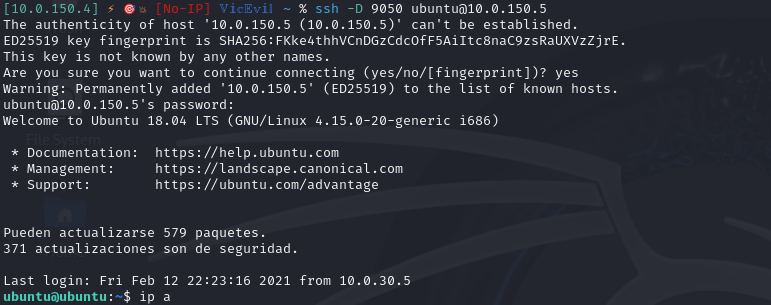


Imagen 2.- establecimiento túnel remoto a través de la PV1, para poder conseguir acceder a otro rango de red

1. Se visualiza las IPs asignadas a la maquina PV1; 10.0.150.5 y 10.0.160.6, siendo esta ultima interfaz de red la que conectará con la nueva máquina *“pivoting VM 2”* (PV2, en adelante)

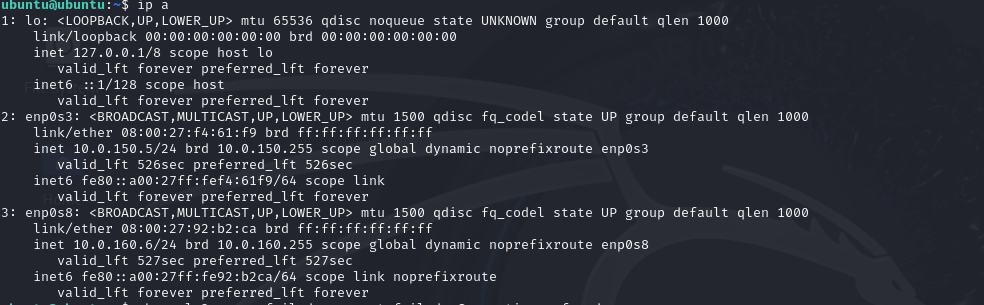


Imagen 3.- resultado de ejecutar el comando IP a de la máquina Linux PV1

1. Se inspecciona los archivos en el interior de la maquina PV1, encontrando en el escritorio de la misma, el primer archivo “flag.zip”, el cual el transferido a la Kali, usando el método “servidor python -wget”.

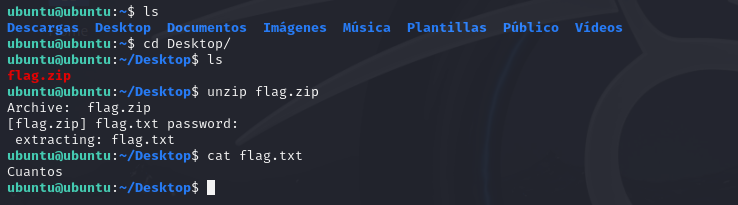




Imagen 4.- Se observa la ruta del primer archivo “flag.zip”, así como la trasferencia hacia Kali

1. Se escanea mediante la herramienta *“Nmap”* todos los puertos y servicios disponibles de la máquina PV1, encontrando dos puertos abiertos (**22 y 80)** con los servicios openSSH 7.6p1 y **Apache** 2.4.49, respectivamente.

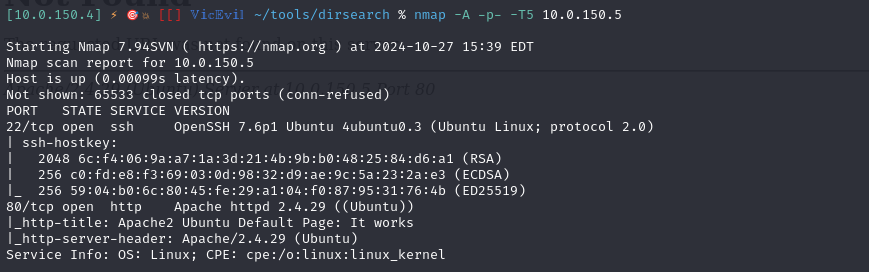


Imagen 5.- Resultado de la ejecución del comando “Nmap” con sus respectivos parámetros de la PV1

1. Al comprobar que hay servicio web por el puerto 80 de la PV1, se procede a un escaneo con la herramienta ***“dirsearch”*** para encontrar directorios y archivos ocultos en el servidor web, encontrando un directorio llamado “flag.html”, el cual contiene la información con la **contraseña de la PV2**.

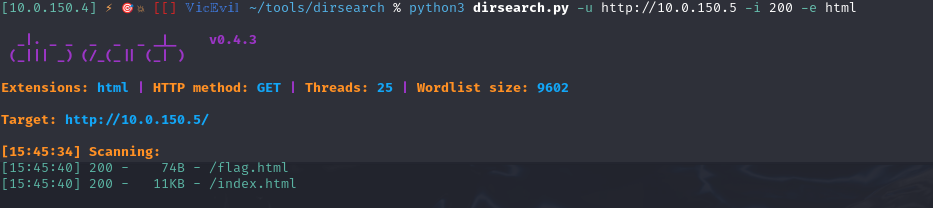
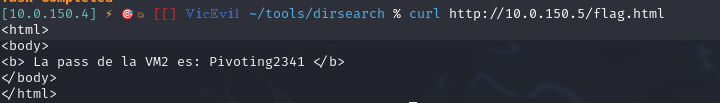


Imagen 6.- resultado de ejecutar la herramienta “dirsearch” sobre el servidor web de PV1



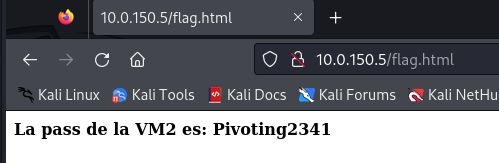


Imagen 7.- Contenido del directorio encontrado “/flag.html” con la contraseña de la PV2.

1. Mediante la herramienta **Proxychains,** la cual, permite el enrutamiento del tráfico de red a través de diferentes proxies en serie (como HTTP, SOCKS4, SOCKS5), consiguiendo ocultar la dirección IP del usuario, mejorar la privacidad y, en algunos casos, eludir restricciones de red. En nuestro caso, hemos usado sólo el **socks4** por el puerto **9050**, permitiendo un **enmascaramiento de la IP**, y de esta forma poder ejecutar diferentes herramientas y llegar a redes mas lejanas o con diferente rango de IP, como en nuestro caso, ejecutamos “***Nmap***” sobre el rango de red 10.0.160/24, aprovechando el túnel dinámico que tenemos abierto desde Kali hasta el final de la PV1, con lo cual, podemos escanear todos los hosts activos que se encuentren en dicho rango de IP, **localizando la IP de la “pivoting VM 2”.**

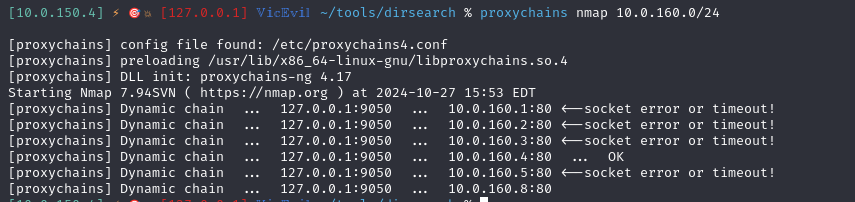
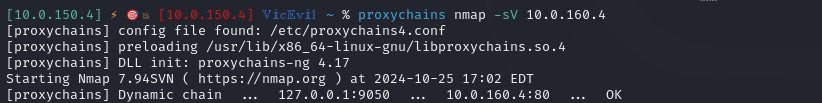


Imagen 8.- Ejecución de la herramienta Nmap . a través de Proxychains y el túnel dinámico que tenemos abierto

1. Se escanea mediante la herramienta***“Nmap”****,* usando las ventajas y servicios que proporciona **Proxychains** y el túnel dinámico aperturado en PV1**,** todos los puertos y servicios disponibles de la máquina PV2, encontrando, dos puertos abiertos (**22 y 80)** con los servicios openSSH 7.6p1 y **Apache** 2.4.29, respectivamente.



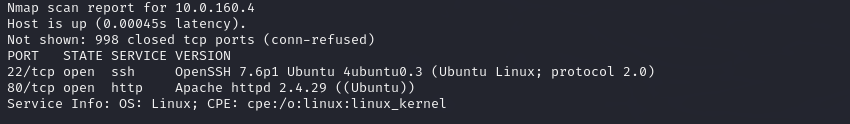
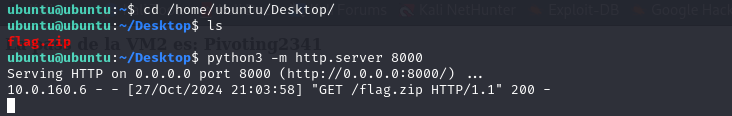


Imagen 9.- Ejecución de Nmap a través de Proxychains para conocer los servicios y puertos abiertos de la PV2

1. Se procede a la **conexión mediante SSH a la PV2**, una vez conseguidas la IP, la contraseña y sabiendo que el puerto 22 esta abierto, inspeccionado los archivos del sistema en busca del **segundo “flag.zip”,** siendo encontrado también en el escritorio de PV2, siendo transferido a la Kali mediante el método *“server python\_wget”*



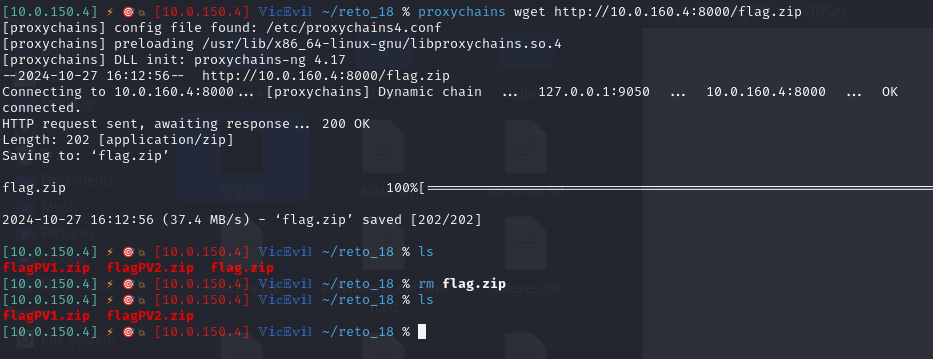
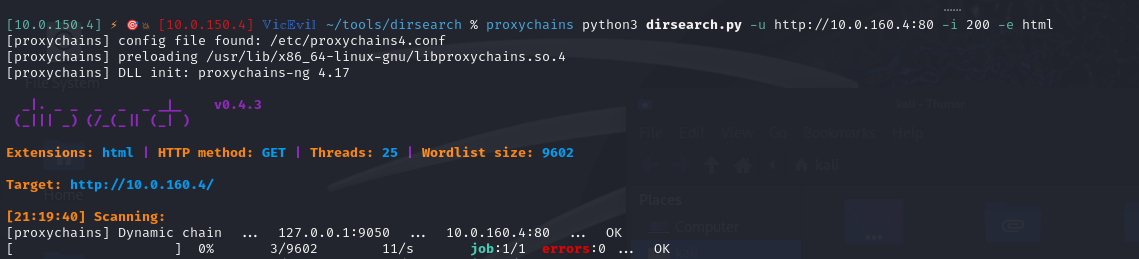


Imagen 10.- Transferencia segundo flag hacia la Kali con el método server python -wget

1. Utilizando nuevamente Proxychains, utilizamos la herramienta **dirsearch** sobre el **servidor web de la PV2,** comos e ha comprobado anteriormente mediante Nmap, encontrando otro directorio ***“/flag.html”.***



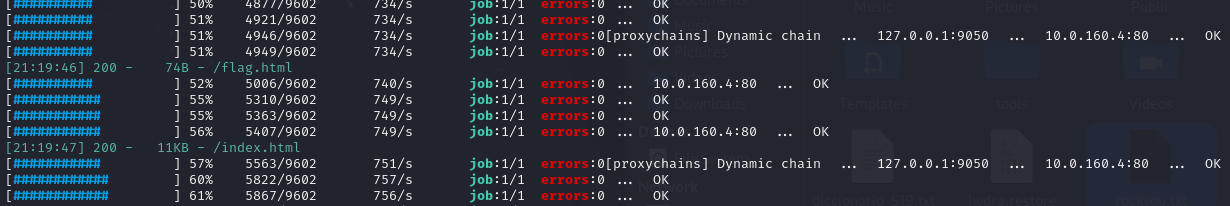
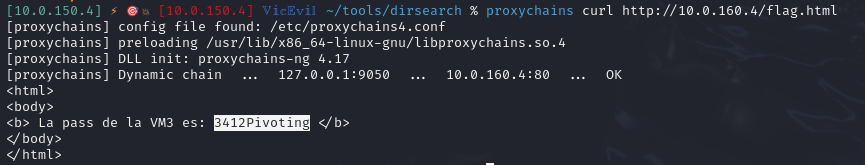


Imagen 11.- Uso de dirsearch a través de Proxychains, consiguiendo el directorio /flag.html

1. Se procede a consultar el directorio encontrado en el punto anterior, aportando información con la **contraseña de la maquina “pivoting VM 3**(PV3, en adelante)



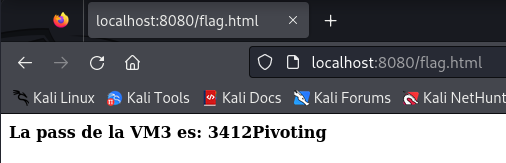
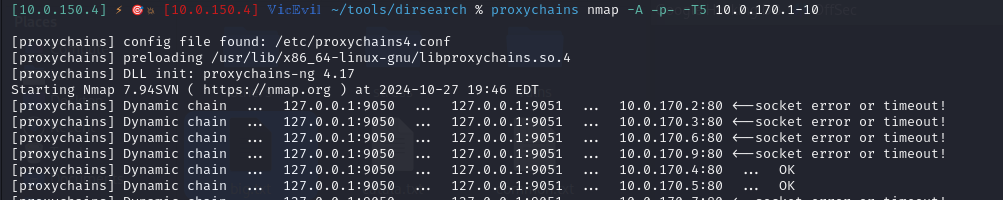


Imagen 12.- Contraseña de acceso a la maquina PV3

1. Una vez llegados a este punto, necesitamos obtener un nuevo túnel dinámico que vaya desde la PV1 hasta le final de la PV2 y que conecte con el que ya teníamos abierto entre Kali y PV1.

Para construir el nuevo túnel, en la terminal donde tenemos abierto el primer túnel dinámico, es decir en la PV1, y usando las técnicas de ssh-tunneling, ejecutaremos el **nuevo túnel dinámico, utilizando la IP de PV2**, no sin antes haber modificado el archivo de configuración en la ruta ***“/etc/proxychains.conf”***, agregando una nueva instrucción: ***“socks4 127.0.0.1 9051”***, todo con la finalidad de poder llegar a la PV3.

1. Se procede a realizar un escaneo **Nmap** mediante proxychains, que como se puede observar ***enlaza el socks 9050 y 9051***, resultando que la IP de la **PV3 es la 10.0.170.5**, ya que la 10.0.170.4, pertenece a la segunda interfaz de red de PV2. Ademas muestra que tiene abiertos los puertos **22 y 80**, con los mismo servicios que las anteriores máquinas (SSH y Apache)



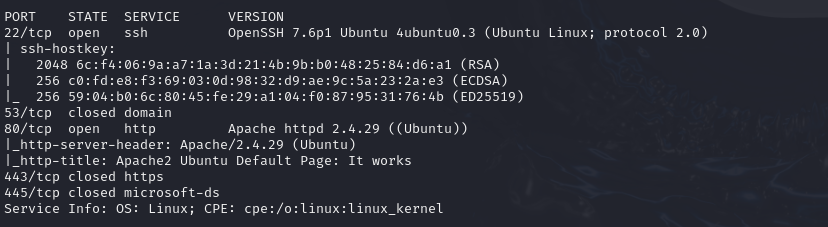
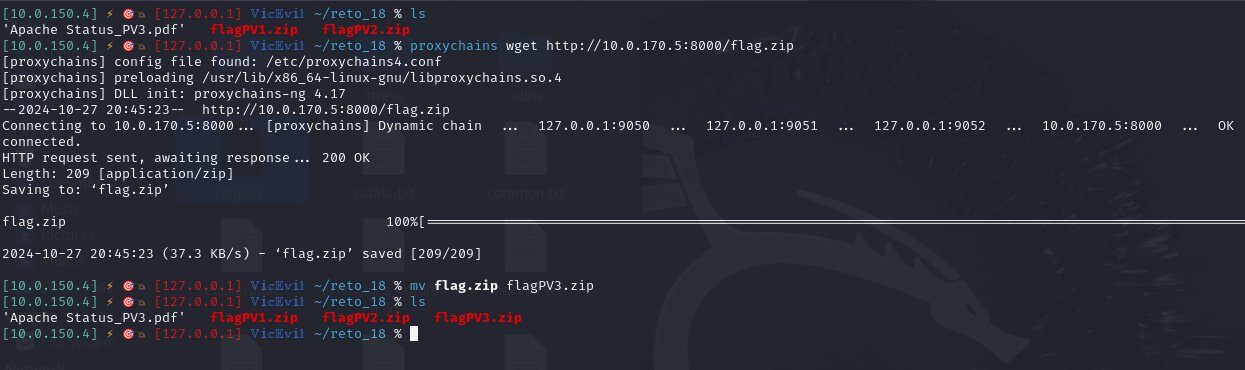


Imagen 13.- Ejecución de Nmap a través de los dos túneles establecidos para alcanzar PV3

1. Se procede a la **conexión mediante SSH a la PV3**, una vez conseguidas la IP, la contraseña y sabiendo que el puerto 22 esta abierto, inspeccionado los archivos del sistema en busca del **tercer archivo “flag.zip”,** siendo encontrado también en el escritorio de PV2, siendo transferido a la Kali mediante el método *“server python\_wget”*



1. Por cambiar la la manera de conseguir acceso al puerto 80, se crea un túnel local entre la PV3 y la Kali, mediante la conexión por SSH a la máquina PV3.

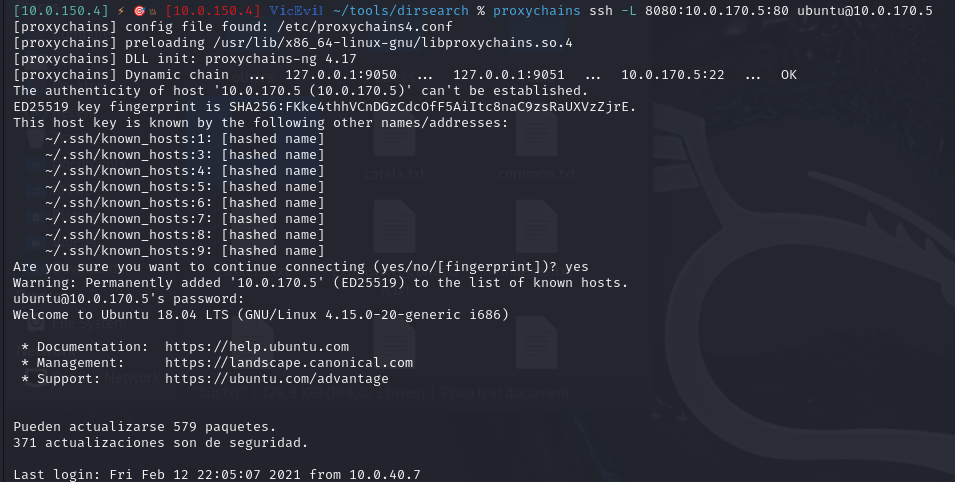
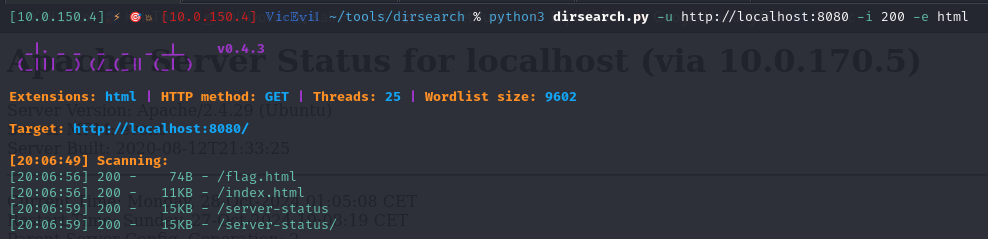
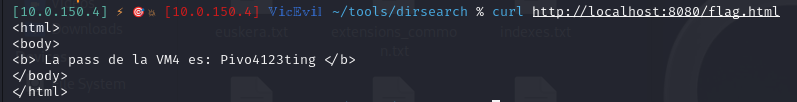


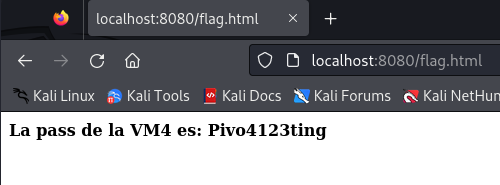
Imagen 14.- Ejecución del túnel local entre PV3 y Kali

1. Se usa la herramienta **dirsearch** sobre el **servidor web de la PV3,** encontrando el **tercer directorio *“/flag.html”.*** En este caso **no** ha hecho falta usar la herramienta **Proxychains**, debido q que hemos establecido un túnel local entre ambas maquinas, **redirigiendo** todo el **puerto 80** de la PV3 al puerto **8080** de nuestra maquina kali, es decir, **nuestro hosts**.

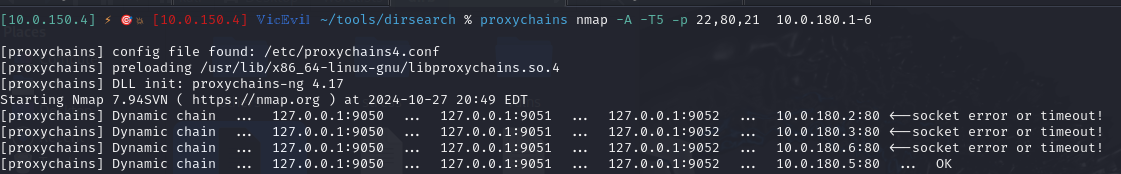


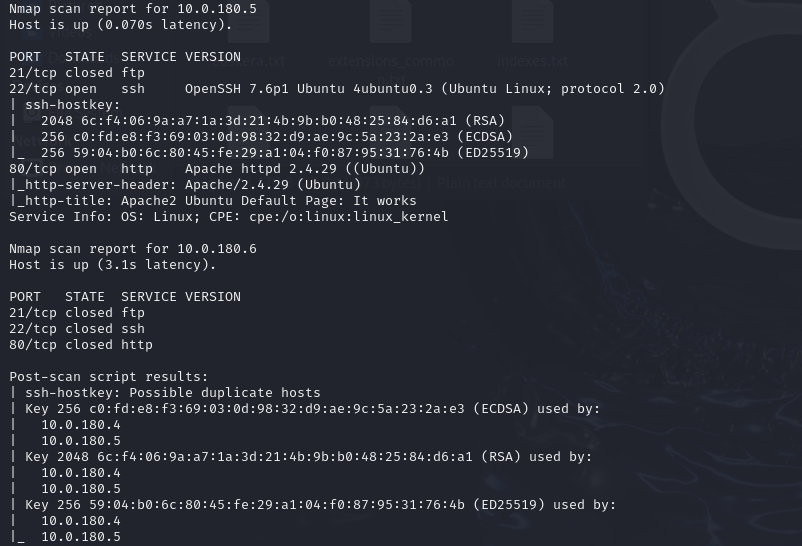
1. Se procede a consultar el directorio encontrado en el punto anterior, aportando información con la **contraseña de la maquina “pivoting VM 4**(PV4, en adelante).



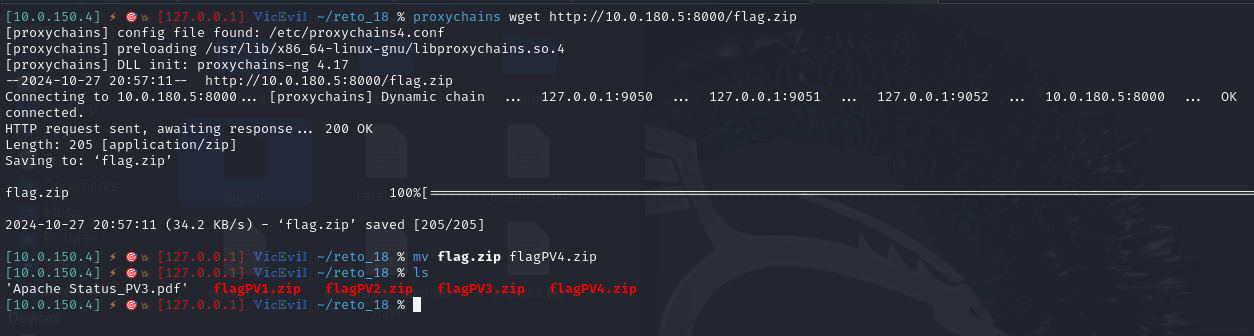


1. Para continuar hacia la ultima máquina, se construye un nuevo túnel, en la terminal donde tenemos abiertos los dos túneles dinámicos, es decir en la PV1 y PV2, ejecutando el **tercer nuevo túnel dinámico,** sobre el ultimo incorporado (PV2), **usando la IP de PV3**, no sin antes haber modificado el archivo de configuración en la ruta ***“/etc/proxychains.conf”***, agregando una nueva instrucción: ***“socks4 127.0.0.1 9052”***, todo con la finalidad de poder llegar a la PV4.
2. Se continua con la ejecución de **Nmap** a través de la cadena de proxies (socks4 9050,9051 y 9052), establecidos en los túneles dinámicos creados al efecto, resultando que la **IP de PV4 es 10.0.180.5**, teniendo abiertos los **puerto 22 y 80**, como todas las máquinas anteriores.





1. Se procede a la **conexión mediante SSH a la PV4**, una vez conseguidas la IP, la contraseña y sabiendo que el puerto 22 esta abierto, inspeccionado los archivos del sistema en busca del **cuarto archivo “flag.zip”,** siendo encontrado también en el escritorio de PV4, transferido a la Kali mediante el método *“server python\_wget”*



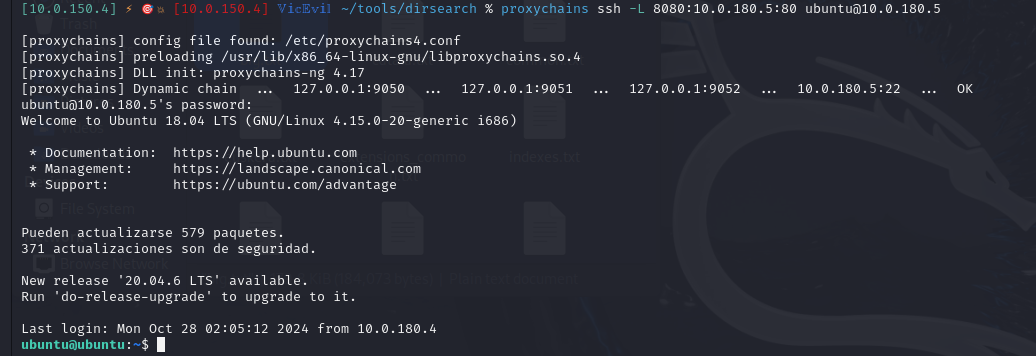
1. Se procede a ver el contenido del **servidor web de la PV4**, se apertura un **túnel local** entre la **Kali y PV4** , a través de la conexión SSH de la IP de la PV4, como se ha explicado anteriormente, teniendo el siguiente **Flujo de Tráfico:**

Kali -> PV1 (SOCKS en 9050 -red 10.0.150.0/24 y 10.0.160.0/24)

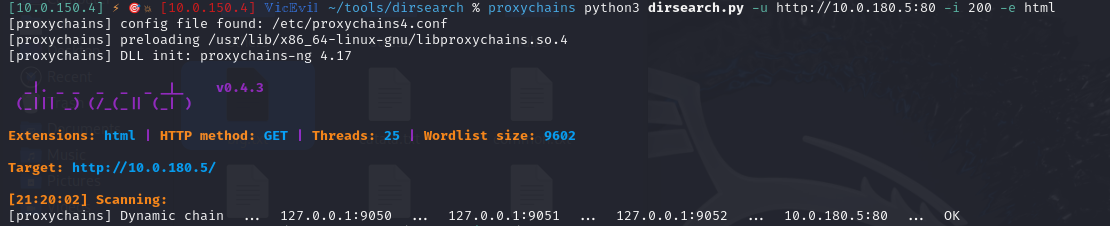
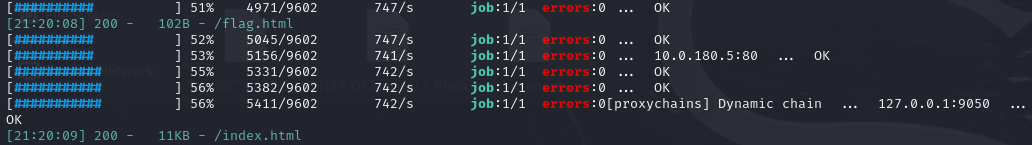
PV1 -> PV2 (SOCKS en 9051- red 10.0.160.0/24 y 10.0.170.0/24)

PV2 -> PV3 (SOCKS en 9052 -red 10.0.170.0/24 y 10.0.180.0/24)

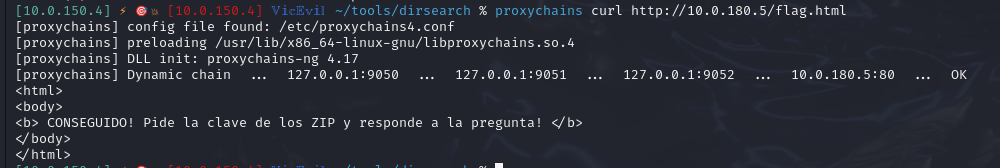
PV4 -> red 10.0.180.0/24



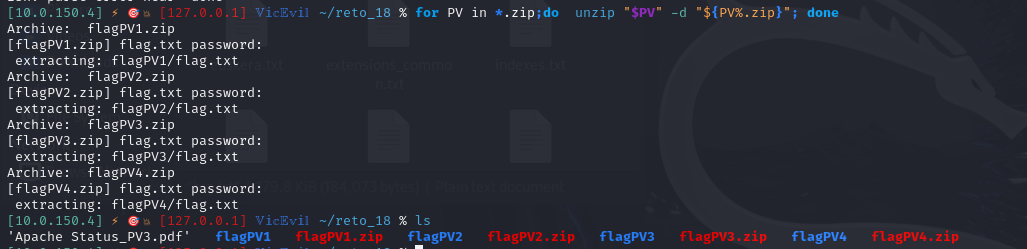
1. Se usa la herramienta **dirsearch** sobre el **servidor web de la PV4,** encontrando el **cuarto directorio *“/flag.html”.*** En este caso **no** ha hecho falta usar la herramienta **Proxychains**, como se ha explicado anteriormente.

1. Se procede a consultar el directorio encontrado en el punto anterior, aportando información sobre la **consecución del reto**, solicitando **responder a la pregunta** que están en los **archivos “flag.zip”** que se ha ido transfiriendo hacia la Kali.



1. Una vez en nuestra máquina Kali, abrimos el directorio donde se ha ido almacenando los distintos archivos flag.zip, ejecutando en un **bucle “for”** para automatizar el la descompresión de los archivos y, como todos tiene el mismo nombre, que se vaya guardando en carpetas diferentes.



1. Finalmente, se procede a la lectura de los diferentes archivos de texto, siendo la pregunta:  **¿Cuántos puertos diferentes hay en un sistema?**

**--** En un sistema, **existen 65,536 puertos en total,** numerados del 0 al 65,535, los cuales, se dividen en tres rangos principales:

- Puertos Bien Conocidos (Well-Known Ports)(0 - 1023)

- Puertos Registrados (1024- 49,151)

- Puertos Dinámicos o Privados (49,152- 65,535)

**--** En relación a los **sistemas explotados**, los **únicos puertos** **abiertos** han sido el **22 y el 80**, que pertenecen a los puertos bien conocidos.

