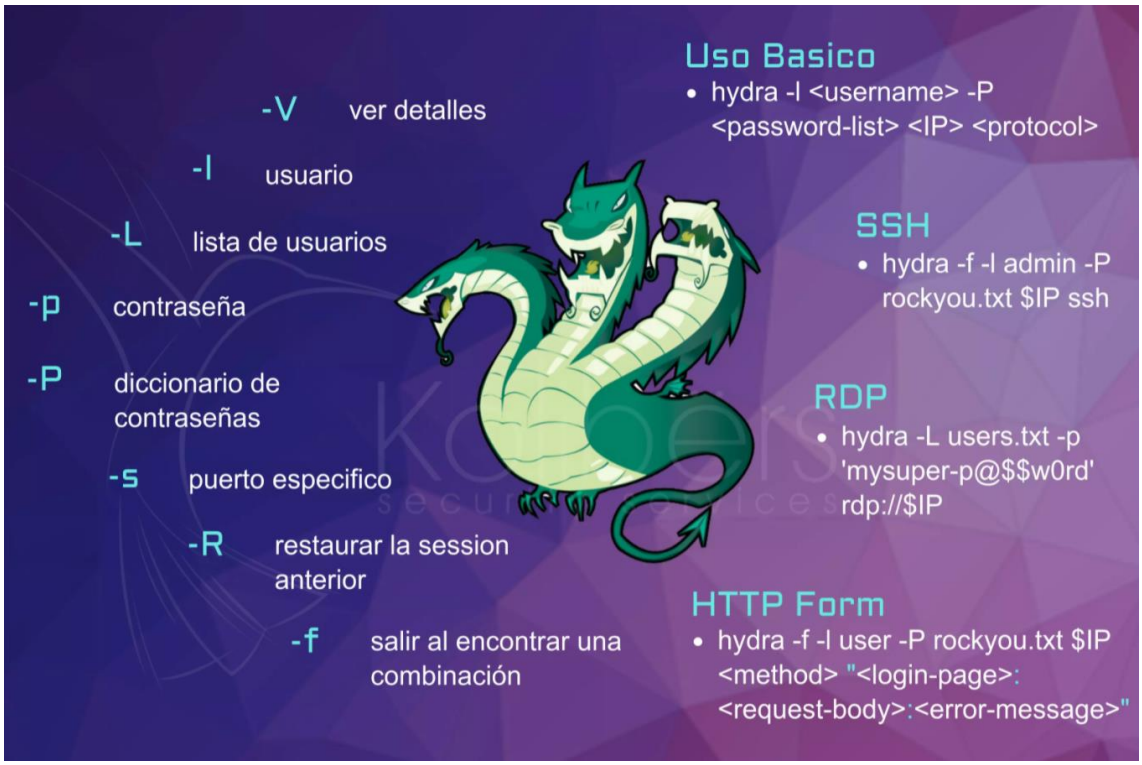
Hydra – Fuerza bruta



Hydra es una herramienta de auditoría de inicio de sesión que trabaja con múltiples tareas en paralelo, soporta una gran variedad de protocolos. Es muy rápido y flexible, y los nuevos módulos son fáciles de agregar. Esta herramienta permite a los investigadores y consultores de seguridad mostrar lo fácil que sería obtener acceso no autorizado a un sistema de forma remota.

ATAQUE SSH

Hydra puede ser una herramienta realmente sencilla y efectiva, pero también cuenta con algunos parámetros interesantes que valen la pena investigar. Para realizar ataques por diccionarios a protocolos comunes usaremos la siguiente sintaxis.

Sintaxis básica:

hydra -l o -L <usuario, lista> -p, -P <contraseña o diccionario> <dirección IP> <protocolo>

-l: especificamos el nombre del usuario

-P: ingresamos el diccionario a utilizar

-e nsr: esta opción nos permite ingresar una contraseña vacía (n), el nombre

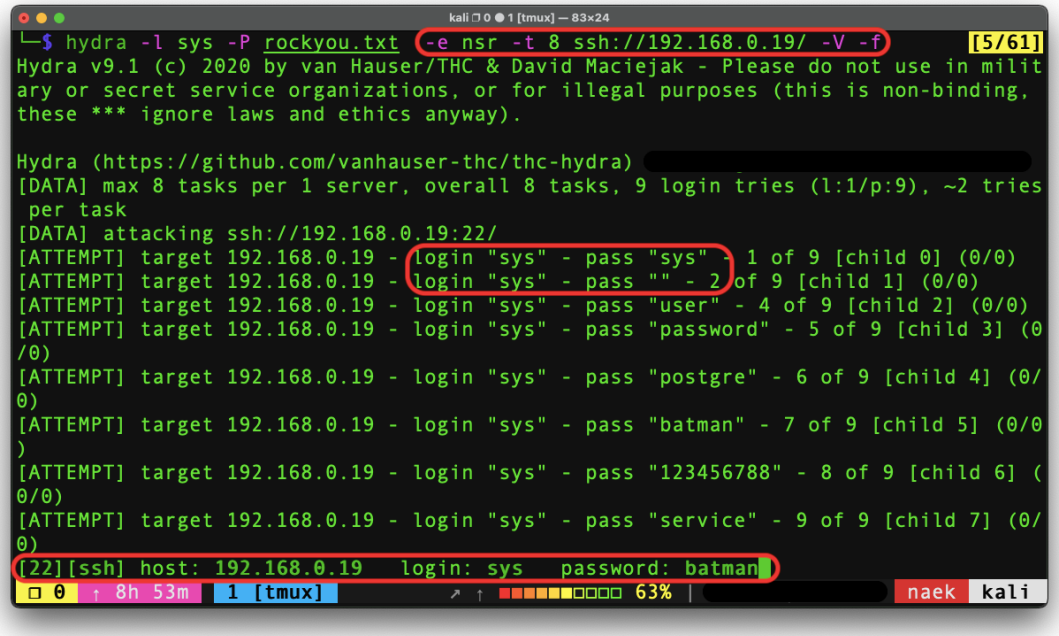
del usuario como contraseña (s), y el mismo usuario invirtiendo las letras (r)

-t: número de tareas en paralelo

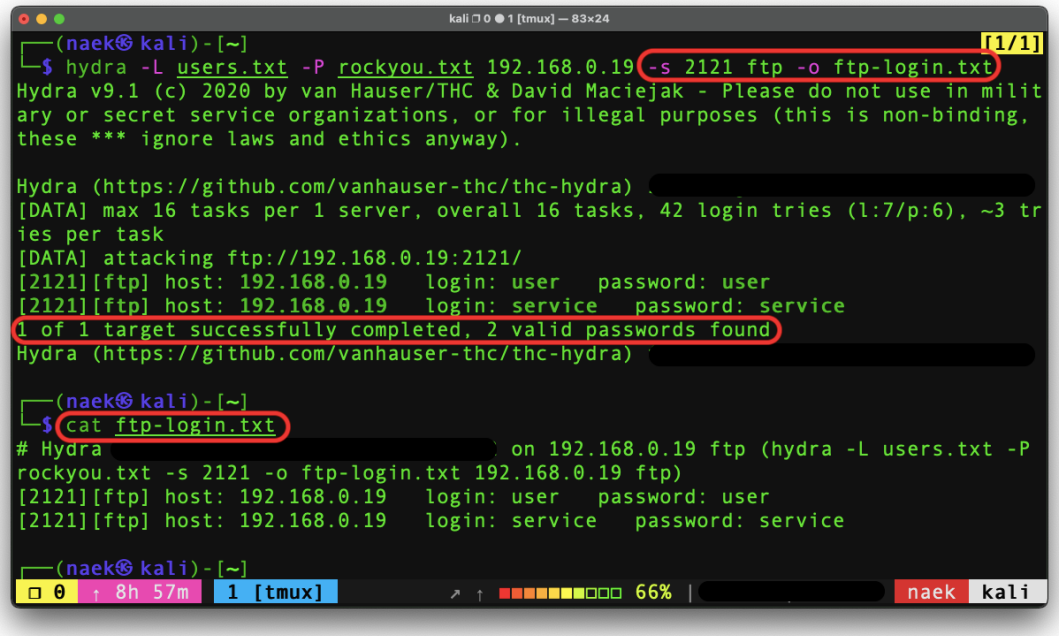
ssh: especificamos el protocolo

-V: usamos el modo detallado

-f: termina los procesos si ha encontrado una combinación válida



ATAQUE FTP



-L: ingresamos la lista de usuarios a utilizar

-P: usamos el mismo diccionario de contraseñas

IP: especificamos la dirección IP

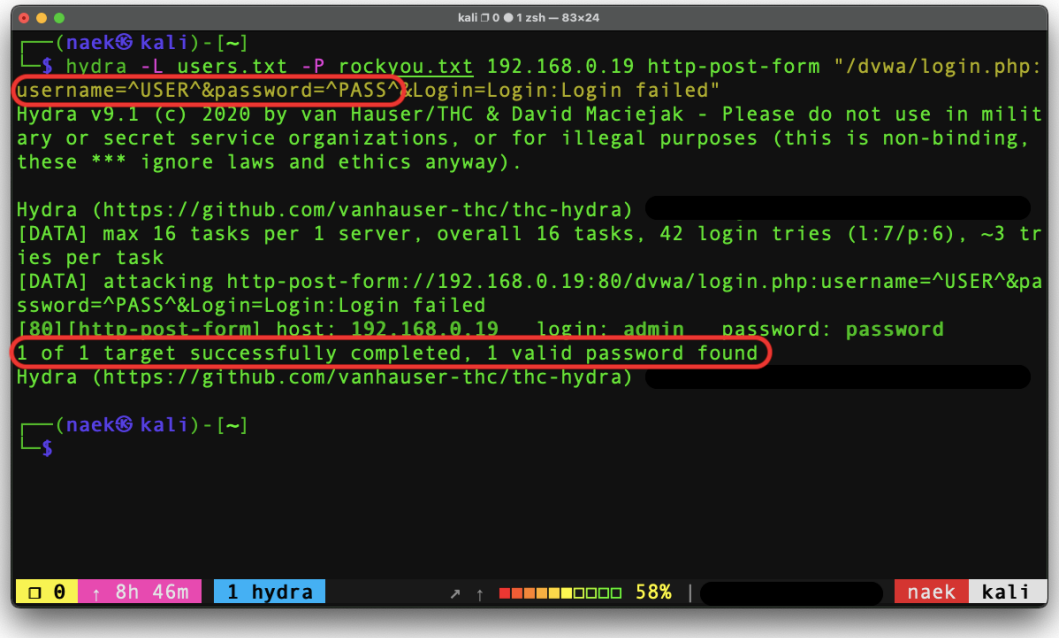
ftp: protocolo a utilizar

-s: número de puerto especifico

-o: guardamos los resultados del ataque

ATAQUE A UN FORMULARIO WEB

- Usuario o lista de usuarios.
- Contraseña o diccionario de contraseñas.
- Dirección IP.
- Método de consulta (Get-Post). (Lo capturamos con burp)
- Página de inicio de sesión.
- Cuerpo de la solicitud.
- Mensaje de error de inicio de sesión.



Hacer el número 4 de fuerza bruta de esta página: ATTACK.SAMSCLASS.INFO