COMANDOS TALLER DISCOVERY

Ejecutar el docker con las herramientas:

En la carpeta en la que tengamos el Dockerfile:

docker build . -t discovery
docker run -it discovery

Para apple silicon:
docker build . -t hola --platform=linux/amd64

Domain utils:

ping example.com
nslookup example.com
dig example.com
whois example.com

Subdomains Finder

Importante estar en la carpeta de Sublist3r:

python3 sublist3r.py -d example.com

Routes Finder

wfuzz -w /SecLists/Discovery/Web-Content/directory-list-2.3-small.txt https://example.com/FUZZ
wfuzz --hc 404 -w /SecLists/Discovery/Web-Content/directory-list-2.3-small.txt https://example.com/FUZZ

Netcat

netcat IP port

Nmap

nmap ip
-p-
-p port
-sS y -sV
-oG -oV

Nuclei

cd root/go/bin
./nuclei -u URL -t list_templates
-debug