

### Reconocimiento DNS

**nslookup** ip o dominio realiza la traduccion de nombre a ip y viceversa

**dig** ip o dominio obtener informacion sobre los servidores de nombres, direcciones de host, puertas de enlace

**whois** ip o dominio obtener informacion de cualquier nombre de dominio del mundo

**tracert** ip o dominio lista los nodos atravesados para llegar al destino

### Comandos de descubrimiento NMAP

Escaneo de ping nmap -sP [objetivo]

Sin ping nmap -PN [objetivo]

TCP SYN Ping nmap -PS [objetivo]

TCP ACK ping nmap -PA [objetivo]

UDP ping nmap -PU [objetivo]

SCTP Init Ping nmap -PY [objetivo]

ICMP echo ping nmap -PE [objetivo]

ICMP Timestampmap -PP ping nmap -PP [objetivo]

ICMP addressmap -PM mask ping nmap -PM [objetivo]

IP protocol ping nmap -PO [objetivo]

ARP ping nmap -PR [objetivo]

### Herramientas SMB

listar recursos compartidos en un host específico smbmap -H [objetivo]

con autenticacion smbmap -H [objetivo] -u [usuario] -p [contrasena]

enumerar usuarios smbmap -H [objetivo] -u [usuario] -p [contrasena] -e

listar recursos compartidos smbclient -L //SERVER -N

### Webs de reconocimiento pasivo

**dumpster.com** descubrimiento de servidores en base al dominio

**shodan.io** motor de busqueda de dispositivos de red

**phonebook.cz** lista dominios y correos asociados a un dominio principal

**hunter.io** buscador de direcciones de mail

**verifyemailaddress.org** verificador de direcciones de email

**emailchecker.net** verificador de direcciones de email

**dashed.com** credenciales y brechas de seguridad

### Deteccion de versiones con NMAP

Sistema operativo nmap -O [objetivo]

Intentar adivinar el sistema operativo nmap -O --osscan-guess [objetivo]

Version de los servicios nmap -sV [objetivo]

Troubleshooting de version de servicios nmap -sV --version-trace [objetivo]

Escaneo RCP nmap -sR [objetivo]

### Tecnicas de evasion de firewall NMAP

Fragmentacion de paquetes nmap -f [objetivo]

Especificar el MTU nbmap -mtu [MTU] [objetivo]

Usar un decoy nmap -D RND [numero] [objetivo]

Escaneo zombie nmap -sl [zombie] [objetivo]

Especificacion manual de puerto nmap --source-port [port] [target]

Spoofing de MAC nmap --spooof-mac [mac] [objetivo]

### Herramientas de reconocimiento

Clearbit connect extension de chrome para la busqueda de emails

Wapalyzer extension de firefox para el analisis web

CTRF (github) programa de busqueda de subdominios basado en transparencia de certificados

Motores de busqueda Google, firefox etc..

### Comandos basicos de hydra

ataque de fuerza bruta a ssh hydra -l usuario -P /ruta/a/lista\_de\_contraseñas.txt ssh://ip\_del\_objetivo

ataque de fuerza bruta a ftp hydra -l usuario -P /ruta/a/lista\_de\_contraseñas.txt ftp://ip\_del\_objetivo

ataque con lista de usuarios hydra -L /ruta/a/lista\_de\_usuarios.txt -P /ruta/a/lista\_de\_contraseñas.txt



By Davomeist

[cheatography.com/davomeist/](https://cheatography.com/davomeist/)

Not published yet.

Last updated 15th October, 2024.

Page 1 of 2.

Sponsored by [ApolloPad.com](https://apollopod.com)

Everyone has a novel in them. Finish Yours!

<https://apollopod.com>

### Comandos basicos de hydra (cont)

ataque con conexiones concurrentes `hydra -l usuario -P /ruta/a/lista_de_contraseñas.txt -t 4`

ataque con timeout `hydra -l usuario -P /ruta/a/lista_de_contraseñas.txt -s 5`

### Uso basico de gobuster

busqueda de subdirectorios `gobuster dir -u http://ip_de_objetivo -w /ruta/a/lista_de_palabras.txt`

enumeracion de archivos por directorio `gobuster dir -u http://ip_de_objetivo -w /ruta/a/lista_de_palabras.txt -x php,html`

enumeracion de subdominios `obuster dns -d dominio.com -w /ruta/a/lista_de_subdominios.txt`

filtrar por codigo de estado http `gobuster dir -u http://ip_de_objetivo -w /ruta/a/lista_de_palabras.txt -s "200,204,301,302"`

escaneo recursivo `gobuster dir -u http://ip_de_objetivo -w /ruta/a/lista_de_palabras.txt -r`

con uso de proxy `gobuster dir -u http://ip_de_objetivo -w /ruta/a/lista_de_palabras.txt -p http://127.0.0.1:8080`

### Uso basico de gobuster

busqueda de subdirectorios `gobuster dir -u http://ip_de_objetivo -w /ruta/a/lista_de_palabras.txt`

enumeracion de archivos por directorio `gobuster dir -u http://ip_de_objetivo -w /ruta/a/lista_de_palabras.txt -x php,html`

enumeracion de subdominios `obuster dns -d dominio.com -w /ruta/a/lista_de_subdominios.txt`

filtrar por codigo de estado http `gobuster dir -u http://ip_de_objetivo -w /ruta/a/lista_de_palabras.txt -s "200,204,301,302"`

escaneo recursivo `gobuster dir -u http://ip_de_objetivo -w /ruta/a/lista_de_palabras.txt -r`

con uso de proxy `gobuster dir -u http://ip_de_objetivo -w /ruta/a/lista_de_palabras.txt -p http://127.0.0.1:8080`

C

By **Davomeist**  
[cheatography.com/davomeist/](https://cheatography.com/davomeist/)

Not published yet.  
Last updated 15th October, 2024.  
Page 2 of 2.

Sponsored by **ApolloPad.com**  
Everyone has a novel in them. Finish Yours!  
<https://apollopad.com>