EPICODE

Progetto Alessandro Moscetti 02/11

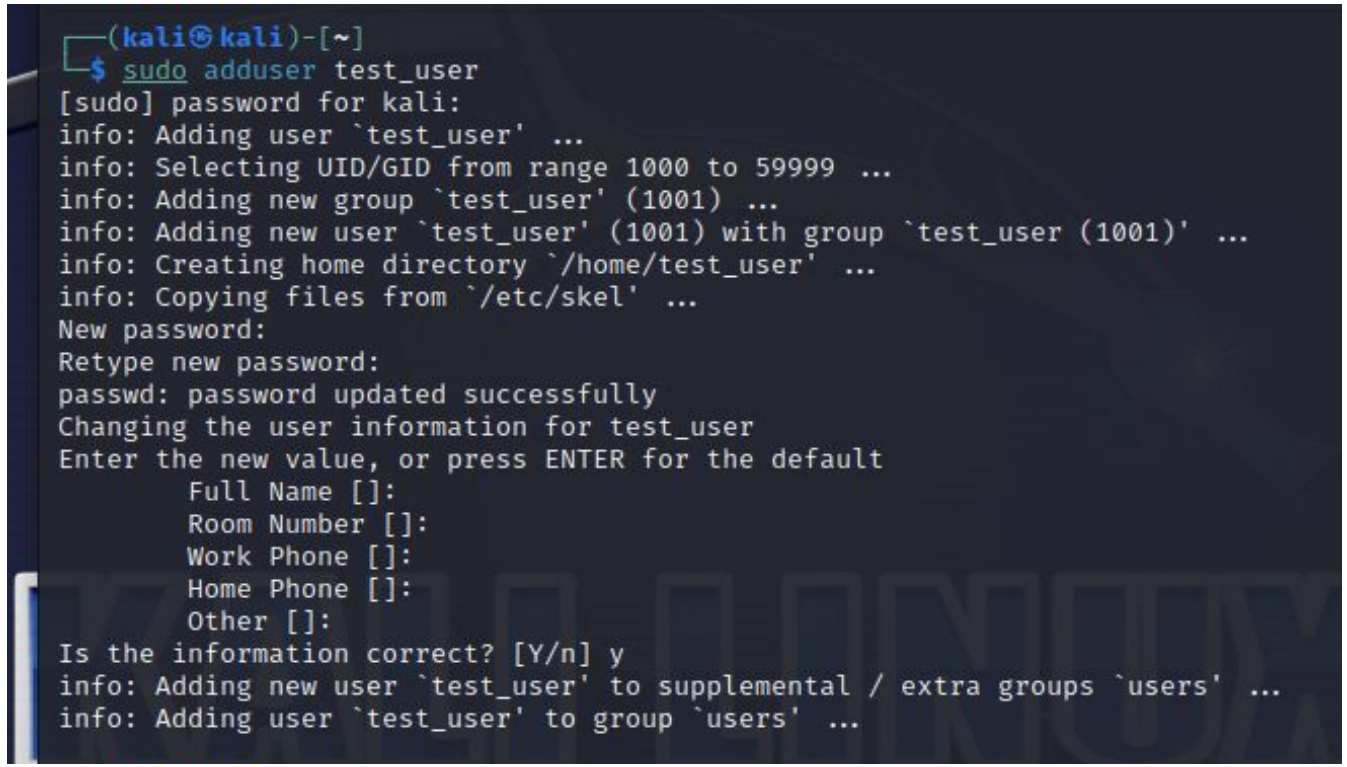
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 940 not upgraded.
Need to get 431 MB of archives.
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]
Fetched 431 MB in 54s (7944 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 399700 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) ...
```

1

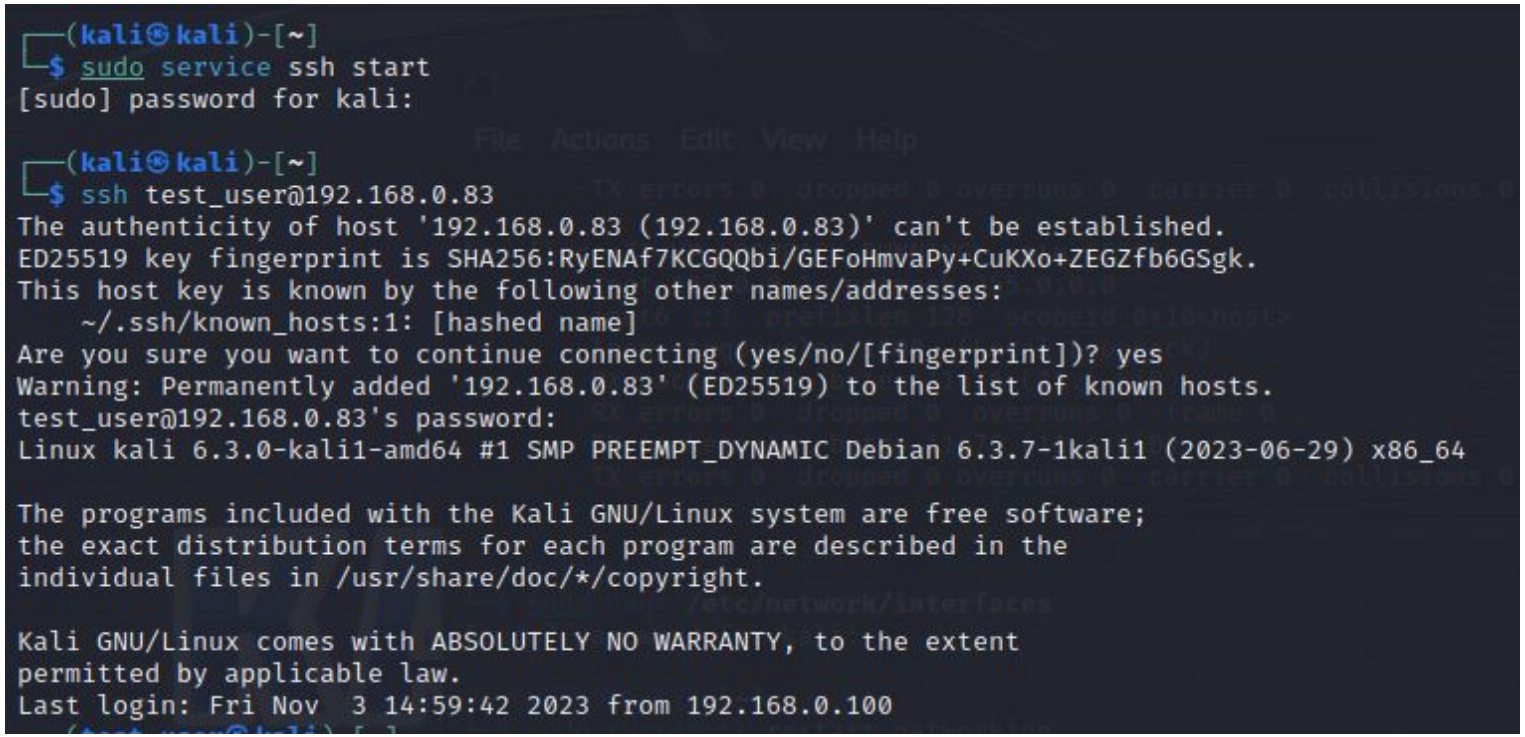
Download liste username e password ‘seclists’ (fig.1).
Installazione servizio ftp Kali (fig. 2).

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
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 940 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 (149 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 405253 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) ...
```

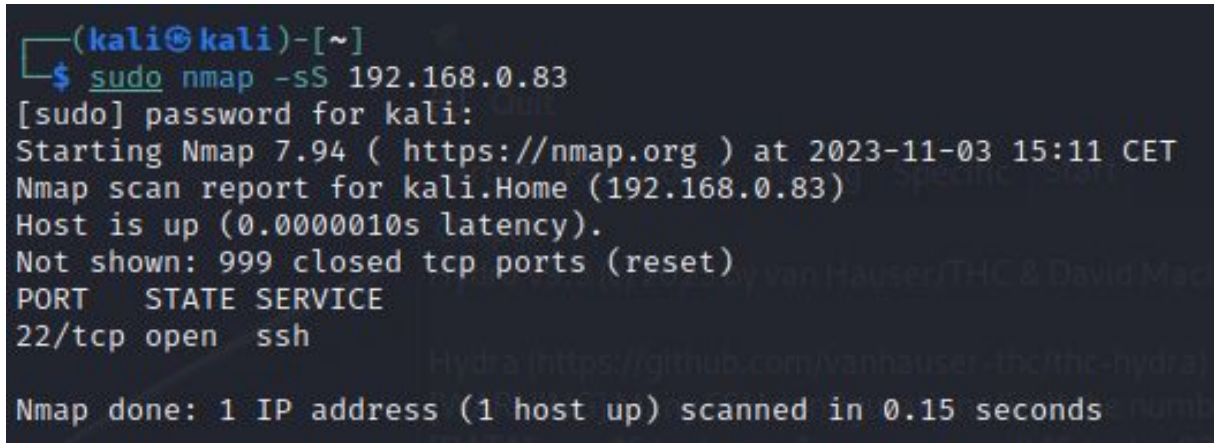
2



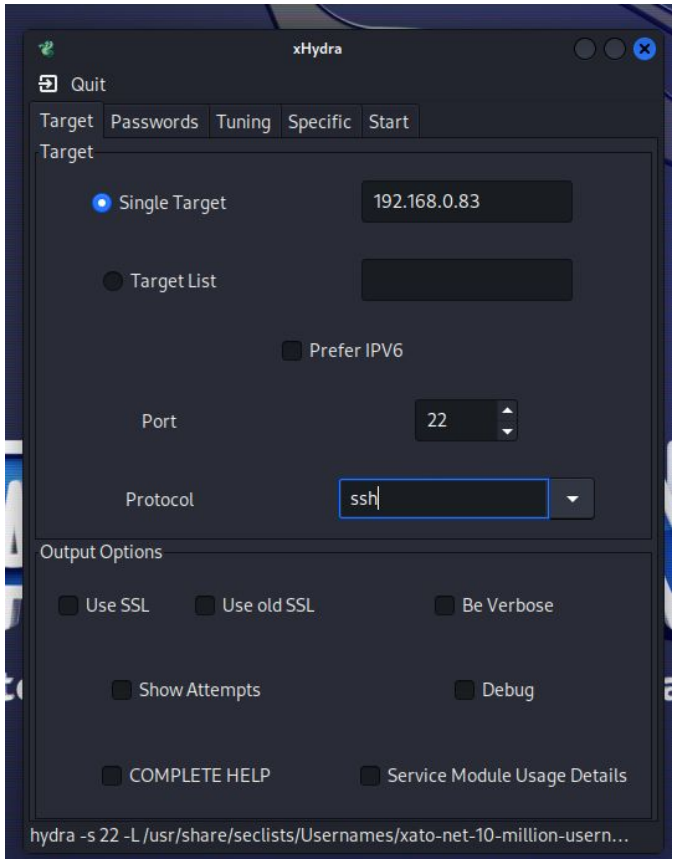
Creazione utente ‘test_user’ su Kali.



Avvio servizio ssh e test connessione nuovo utente sul servizio.

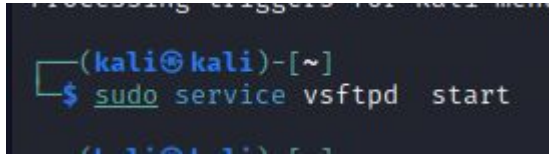


Scansione con nmap per conferma che il servizio sia effettivamente attivo.




```
[DATA] attacking ssh://192.168.0.83:22/
[22][ssh] host: 192.168.0.83   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
```

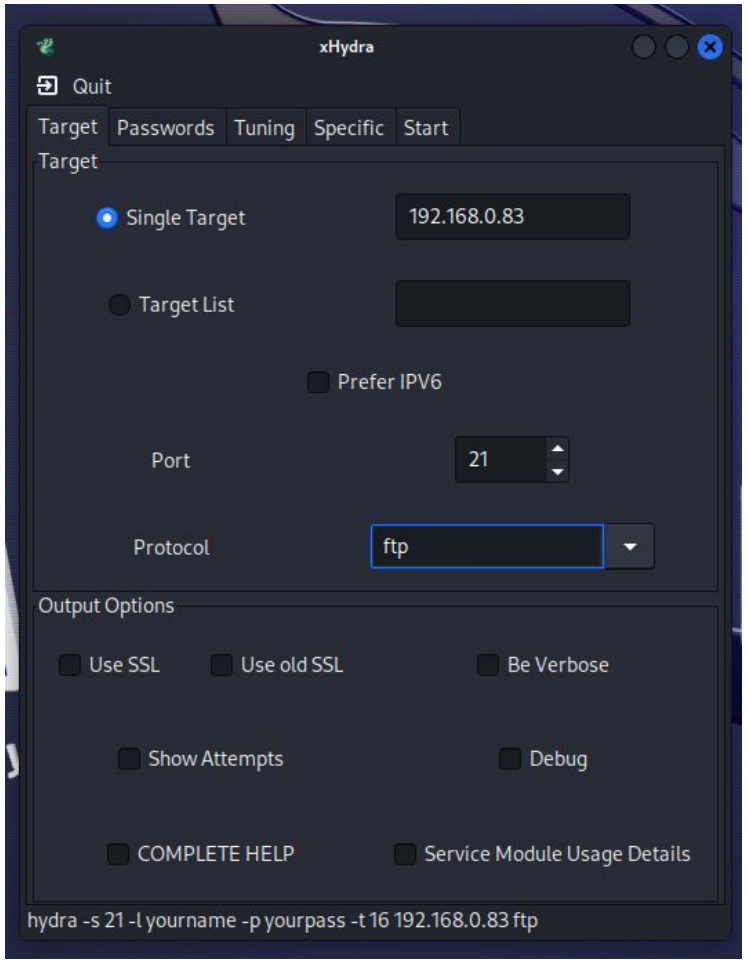
Cracking con Hydra sul servizio ssh di Kali.



1

2

Nella fig. 1 startiamo il servizio ftp precedentemente installato.
Nella fig. 2 avviamo una nuova scansione per verificare l'effettivo avvio del servizio e in seguito test di connessione del nuovo utente sul servizio.



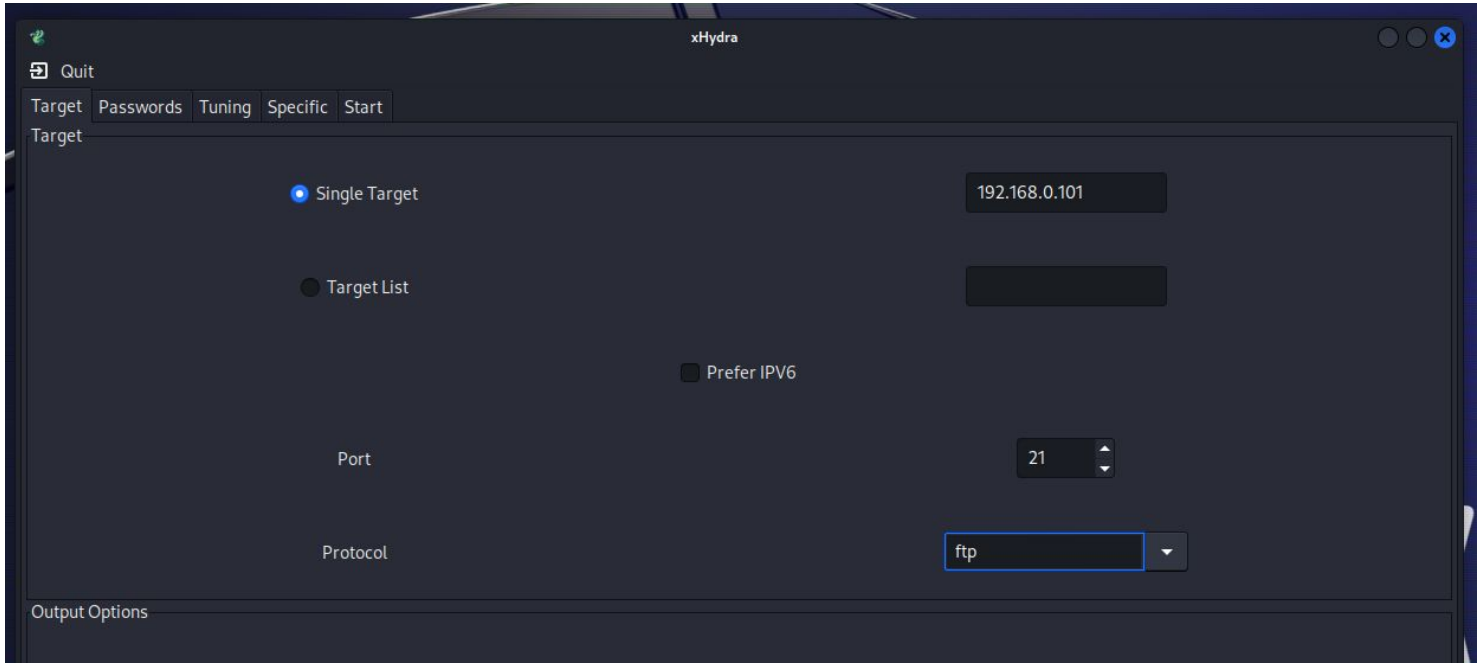

```
[DATA] attacking ftp://192.168.0.83:21/
[21][ftp] host: 192.168.0.83   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
```

Cracking con Hydra sul servizio ftp di Kali.

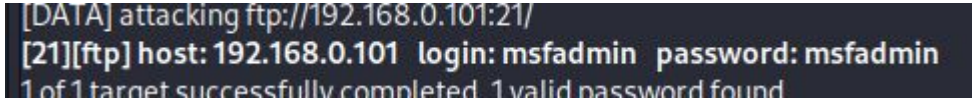
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.0.101
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-03 15:25 CET
Nmap scan report for 192.168.0.101
Host is up (0.00038s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  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
513/tcp  open  login
514/tcp  open  shell
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:E6:33:5F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
```

Scansione sulla macchina Metasploitable per visualizzare i servizi attivi.



Cracking con Hydra sul servizio ftp di Metasploitable.



Grazie per l’attenzione.