Arrow :Isınma

İlk öncelikle açık portları bulmamamızı istemiş nmap ile tarama yapıyoruz .1 tane 23 portu açık.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -sC -O -Pn 172.20.7.50
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 13:03 EDT
Nmap scan report for 172.20.7.50
Host is up (0.087s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/sub
mit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/9%OT=23%CT=1%CU=35906%PV=Y%DS=2%DC=I%G=Y%TM=6706
OS:B765%P=x86_64-pc-linux-gnu)SEQ(SP=FC%GCD=1%ISR=10C%TI=Z%CI=Z%TS=A)SEQ(SP
OS:=FC%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=FC%GCD=2%ISR=10C%TI=Z%CI=Z%
OS:II=I%TS=A)OPS(O1=M509ST11NW7%O2=M509ST11NW7%O3=M509NNT11NW7%O4=M509ST11N
OS:W7%O5=M509ST11NW7%O6=M509ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE8
OS:8%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M509NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40
OS:%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=
OS:%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%
OS:W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=
OS:)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%
OS:DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.08 seconds
```

Açık çalışan servisin adı tcp olduğunu görüyoruz.

```
PORT   STATE SERVICE VERSION
23/tcp open  telnet  Linux telnetd
```

Telnet servise açık olduğu için buradan Telnet ile bağlantı kurup giriş yaptıktan sonra hostname komutunu çalıştırarak sistemin adını öğrenebiliriz.

```
┌──(root㉿kali)-[/home/kali]
└─# telnet 172.20.7.50

Trying 172.20.7.50 ...
Connected to 172.20.7.50.
Escape character is '^]'.
Hey you, you're trying to connect to me.
You should always try default credentials like root:root

it's just beginning *_*
arrow login: root
Password:
Linux arrow 5.10.0-26-amd64 #1 SMP Debian 5.10.197-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@arrow:~# hostname
arrow
root@arrow:~#
```

Hostname adını arrow bulduk. Bağlantı sırasında verilen ipucu ("you should always try default credentials like root") varsayılan kullanıcı adı ve şifreyi denemeniz gerektiğini belirtiyor. Genellikle, varsayılan kimlik bilgileri şu şekilde olabilir:

- **Kullanıcı adı**: root
- **Şifre**: root

Telnet'e bağlandığınızda çalışma dizini konumununuz root dur.