

File Hunter: Isınma

```
(root@kali)-[/home/kali]
# nmap -sS -sV -O -T4 172.20.3.149

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-09 13:46 EDT
Nmap scan report for 172.20.3.149
Host is up (0.12s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=10/9%OT=21%CT=1%CU=39807%PV=Y%DS=2%DC=I%G=Y%TM=6706
OS:C193%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=107%TI=Z%CI=Z%TS=A)SEQ(S
OS:P=103%GCD=1%ISR=107%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M509ST11NW7%O2=M509ST11NW
OS:7%O3=M509NNT11NW7%O4=M509ST11NW7%O5=M509ST11NW7%O6=M509ST11)WIN(W1=FE88%
OS:W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M509N
OS:NSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=
OS:Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=A
OS:R%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=4
OS:0%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=
OS:G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Host: Welcome

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 34.65 seconds
```

Nmap ile port taraması yapıyoruz ve hangi portlar açık olduğunu buluyoruz. 21 tcp portu açık olarak görüyoruz.

FTP'nin açılımı nedir? File transfer protocol olarak yazıyoruz.

```
(root@kali)-[/home/kali]
# ftp 172.20.3.149
Connected to 172.20.3.149.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.3.149:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Ftp ip adresi le bağlanılıyor. FTP' ye Anonymous kullanıcı adı ile bağlanıyoruz.

Hangi komut FTP sunucusunda hangi komutları kullanabileceğimizi gösterir?

```
(root@kali)-[/home/kali]
# ftp 172.20.3.149
Connected to 172.20.3.149.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.3.149:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

!                epsv6          mget             preserve         sendport
$                exit            mkdir            progress         set
account          features       mls              prompt           site
append           fget          mlsl             proxy            size
ascii            form          mlst             put              sndbuf
bell             ftp           mode             pwd              status
binary           gate          modtime          quit             struct
bye              get           more             quote            sunique
case             glob          mput             rate             system
cd               hash          mreget           rcvbuf           tenex
cdup             help          msend            recv             throttle
chmod            idle          newer            reget            trace
close            image         nlist            remopts          type
cr               lcd           nmap             rename            umask
debug            less          ntrans           reset             unset
delete           lpage         open             restart           usage
dir              lpwd          page             rhelp            user
```

Help komutu ile bakıyoruz.

FTP sunucusundaki dosyanın adı nedir?

```
ftp> ls
229 Entering Extended Passive Mode (|||20276|)
150 Here comes the directory listing.
-rw-r--r--  1 ftp      ftp          25 Sep 08  2023 userlist
226 Directory send OK.
ftp>
```

Dosyanın adının userlist olduğunu görüyoruz.

Bir FTP sunucusundan dosya indirmek için kullanabileceğimiz komut nedir?

Get komutunu kullanıyoruz.

Dosyada hangi kullanıcıların bilgileri vardır?

```
ftp> less userlist
jack:hackviser
root:root
ftp> █
```

Jack ve root kullanıcılarının bilgileri bulunuyor.