

## FILE HUNTER WRITE-UP

Bu yazımda sizlere Hackviser platformunda Warmups kısmında bulunan File Hunter senaryosunun çözümünü anlatacağım.

**SORU 1:** Hangi port(lar) açıktır?

Nmap taraması yaparak bunu öğrenebiliriz.

```
(root@kali)~[/home/kali]
# nmap -A -Pn 172.20.5.21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-06 13:45 +03
Nmap scan report for 172.20.5.21
Host is up (0.075s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-r--r-- 1 ftp      ftp      25 Sep 08 2023 userlist
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:10.8.9.164
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 3
|     vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
```

Burada **21** (FTP) portunun açık olduğunu buluyoruz.

**SORU 2:** FTP'nin açılımını soruyor?

File Transfer Protocol

**SORU 3:** FTP'ye hangi kullanıcı adı ile bağlandınız?

```
Connected to 172.20.5.21.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.5.21:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30204|)
150 Here comes the directory listing.
-rw-r--r-- 1 ftp      ftp      25 Sep 08 2023 userlist
226 Directory send OK.
ftp> █
```

Burada bize "Welcome to anonymous" dediği için ben anonymous ismini denedim ve bağlanmakta başarılı oldum. Bazen çok basit düşünmek gerekir 😊

**SORU 4:** Hangi komut FTP sunucusunda hangi komutları kullanabileceğimizi gösterir?

Burada Linux bilgilerime dayanarak cevapladım. Genelde çoğu tool -h veya help komutu ile bize bu bilgileri verir. İpucuna baktığımda(cevap yazma kısmında 4 harfli olduğunu bizlere gösteriyor.) cevabın **help** olduğunu bulduk.

```
ftp> help
Commands may be abbreviated.  Commands are:

!            edit            lpage          nlist          rcvbuf          struct
$            epsv           lpwd           nmap           recv           sunique
account      epsv4           ls             ntrans         reget           system
append       epsv6           macdef         open           remopts         tenex
ascii        exit            mdelete        page           rename          throttle
bell         features        mdir           passive        reset           trace
binary       fget           mget           pdir           restart         type
bye          form           mkdir          pls            rhelp           umask
case         ftp            mls            pmlsd          rmdir           unset
cd           gate           mlst           preserve       rstatus         usage
cdup         get            mlsd           progress       runique         user
chmod        glob           mode           prompt         send            verbose
close        hash           modtime        proxy          sendport        xferbuf
cr           help           more           put            set             ?
debug        idle           mput           pwd            site
delete       image          mreget         quit           size
dir          lcd            msend          quote          sndbuf
disconnect   less           newer          rate           status

ftp>
```

**SORU 5:** FTP sunucusundaki dosyanın adı nedir?

Dosya listelemek için "ls" komutunu kullanıyoruz.

```
ftp> ls
229 Entering Extended Passive Mode (|||23217|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp        25 Sep 08  2023 userlist
226 Directory send OK.
```

Burada dosyanın isminin **userlist** olduğunu buluyoruz.

**SORU 6:** Bir FTP sunucusundan dosya indirmek için kullanabileceğimiz komut nedir?

Biz FTP ile bağlantı kurduğumuz bir makineden dosya indirmek için **GET** komutunu kullanırız.

```
226 Directory send OK.
ftp> help get
get          receive file
ftp>
```

**SORU 7:** Dosyada hangi kullanıcıların bilgileri vardır?

```
ftp> get userlist
local: userlist remote: userlist
229 Entering Extended Passive Mode (|||55977|)
150 Opening BINARY mode data connection for userlist (25 bytes).
100% |*****| 25 595.46 KiB/s 00:00 ETA
226 Transfer complete.
25 bytes received in 00:00 (0.32 KiB/s)
```

Get komutunu kullanarak dosyayı indiriyorum.

Cat: Bu komut bize istediğimiz dosyanın içindekileri görüntülememizi sağlıyor.

Ama cat komutu ftp ile bağlantı kurduğumuz makinede çalışmadı. Çünkü bu bir Linux terminal komutudur.

Ana makineye indirdiğimiz userlist dosyamızı cat komutu ile okumaya çalışıyoruz.

```
(root@kali)-[/home/kali]  
# cat userlist  
jack:hackviser  
root:root
```

Burada cevabın **jack**, **root** olduğunu görüyoruz.