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.

```
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--
                         ftp
               1 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

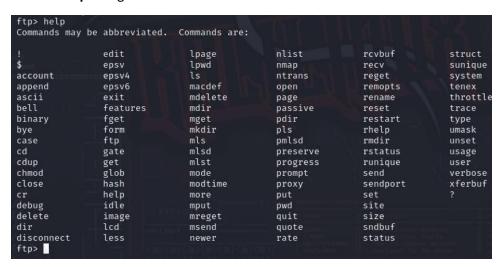
226 Directory send OK.

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.



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
ftn>
```

SORU 7: Dosyada hangi kullanıcıların bilgileri vardır?

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.