

File Hunter Write-up

FTP Nedir?

FTP (File Transfer Protocol), internet üzerinden dosya aktarımı yapmak için kullanılan bir ağ protokolüdür. 1971 yılında geliştirilen bu protokol, kullanıcıların sunuculara dosya yüklemesine veya sunuculardan dosya indirmesine olanak tanır. FTP özellikle web sitelerinin yönetimi ve veri paylaşımı için oldukça kullanışlıdır.

FTP, genellikle iki temel bileşenden oluşur: bir FTP sunucusu ve bir FTP istemcisi. FTP sunucusu, dosyaların saklandığı ve dış dünyaya sunulduğu merkezi bir bilgisayardır. FTP istemcisi ise, kullanıcıların FTP sunucusuna bağlanıp dosya aktarımı yapmalarını sağlayan yazılımdır. Kullanıcılar, genellikle bir kullanıcı adı ve şifre kullanarak FTP sunucusuna bağlanır, ancak bazı sunucular **anonim erişime** de izin verebilir.

FTP, kullanım kolaylığı ve geniş uyumluluğu nedeniyle popülerliğini korumaktadır. Ancak, FTP'nin şifrelenmemiş bir protokol olması, veri güvenliği açısından bazı riskler taşır. Bu nedenle, hassas verilerin aktarımı için genellikle güvenli bir alternatif olan SFTP (SSH File Transfer Protocol) veya FTPS (FTP Secure) tercih edilir.

Bir FTP sunucusuna bağlanmak için aşağıdaki komut dizisi kullanılır.

```
ftp <SERVER-IP-ADDRESS> -P <PORT-NUMBER>
```

Not: Eğer FTP servisi varsayılan olarak 21 portunu kullanıyorsa bağlanırken port numarası belirtmemize gerek yoktur.



```
root@hackerbox:~# ftp 10.0.0.88
Connected to 10.0.0.88.
220 (vsFTPd 3.0.3)
Name (10.0.0.88:hacker): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Yukarıdaki örnekte bir FTP sunucusuna **anonymous** olarak nasıl bağlanabileceğimizi gördük.

Bir FTP sunucusuna bağlandıktan sonra çalıştırabileceğimiz komutları görmek için **help** komutunu kullanırız. Aşağıda bazı önemli komutları görebilirsiniz.

```
help : Çalıştırılacak komutları gösterir ve komutlar hakkında bilgi verir.
```

```
get : Bir dosya indirmek için kullanılır.
```

```
dir : Uzaktaki dizinin içeriğini listeler.
```

```
bye : FTP oturumunu sonlandırın ve çıkın.
```

Bilgi Toplama

Hedef makinemize yönelik port taraması gerçekleştirelim.

Görev 1

Servislerin versiyon bilgilerini de öğrenmek için nmap komutumuza **-sV** parametresini ekliyoruz.

```
root@hackerbox:~# nmap -sV 172.20.24.150
Starting Nmap 7.80 ( https://nmap.org ) at 2023-11-17 11:50 CST
Nmap scan report for 172.20.24.150
Host is up (0.0014s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.8 or later
MAC Address: 52:54:00:E7:28:8B (QEMU virtual NIC)
Service Info: Host: Welcome

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.99 seconds
```

Görev 2

Bu yazının başlarında da anlatıldığı gibi FTP'nin açılımı **File Transfer Protocol**'dür.

Sisteme Erişim

Hedef makinemize FTP ile bağlanmayı deneyelim.

```
root@hackerbox:~# ftp 172.20.24.150
Connected to 172.20.24.150.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.24.150:root):
```

Görev 3

FTP'ye bağlanmaya çalışırken, henüz kullanıcı adı ve parola girmeden bir hoş geldin mesajı görüyoruz. Bu mesajdan da anladığımız üzere FTP servisine **anonymous** olarak bağlanmayı deneyelim.

```
root@hackerbox:~# ftp 172.20.24.150
Connected to 172.20.24.150.
220 Welcome to anonymous Hackviser FTP service.
Name (172.20.24.150:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Evet anonymous olarak sunucuya başarılı bir şekilde bağlandık.

Anonim FTP erişimi, kullanıcı adı ve şifre gerektirmeden herkesin sunucudaki belirli dosyalara erişmesine olanak tanır. Bu, genellikle açık kaynak yazılımların, halka açık verilerin veya büyük dosyaların dağıtımı için kullanılır.

Bir FTP sunucusuna anonim olarak bağlanmak için, FTP client aracılığıyla sunucu adresine bağlanılır ve genellikle kullanıcı adı kısmına "anonymous" yazılıp, şifre kısmı boş bırakılır. Bağlantı kurulduktan sonra, kullanıcılar sunucudaki dosyaları görüntüleyebilir ve indirebilirler.

Anonim FTP, kolay erişilebilirliği ile bilgi paylaşımını kolaylaştırır. Ancak güvenlik açısından sunucu sahiplerinin de erişilebilir içeriği dikkatle yönetmeleri gerekir.

Görev 4

Çalıştırabileceğimiz komutları görüntülemek için **help** komutunu yazıyoruz.

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

!      dir      mdelete  qc       site
$      disconnect mdir     sendport size
account exit      mget     put      status
append form      mkdir    pwd      struct
ascii  get       mls      quit     system
bell   glob      mode     quote    sunique
binary hash      modtime  recv     tenex
bye     help      mput     reget    tick
case    idle     newer    rstatus  trace
cd      image    nmap     rhelp    type
cdup    ipany     nlist    rename   user
chmod   ipv4      ntrans   reset    umask
close   ipv6      open     restart  verbose
cr      lcd     prompt   rmdir    ?
delete  ls        passive  runique
debug   macdef   proxy    send
```

Görev 5

Bağlandığımız FTP sunucusundaki dosyaları görüntülemek için **ls** komutunu çalıştıralım.

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp          25 Sep 08 08:07 userlist
226 Directory send OK.
```

Görev 6

Komut listesi içerisinde gördüğümüz **get** komutunu dosyaları indirmek için kullanabiliriz.



```
ftp> help get
get          receive file
```

Görev 7

FTP sunucusunda bulunan **userlist** adlı dosyayı **get** komutu ile indirip FTP bağlantısını kapatabiliriz. Ardından **cat** komutu ile dosyanın içeriğini okumamız yeterli.



```
ftp> get userlist
local: userlist remote: userlist
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for userlist (25 bytes).
226 Transfer complete.
25 bytes received in 0.00 secs (121.4630 kB/s)
ftp> bye
221 Goodbye.
root@hackerbox:~# cat userlist
jack:hackviser
root:root
```

-

Tebrikler 🎉

✨ Bu ısınma makinesindeki tüm görevleri başarıyla tamamladınız.