FTP ve Güvenlik Duvarları

FTP Protokolü

FTP, sık kullanılan protokoller(HTTP, SMTP, DNS vs) arasında en sorunlu protokoldür. Diğer protokoller tek bir TCP/UDP portu üzerinden çalışırken FTP birden fazla ve dinamik portlarla çalışır. (IRC'deki veri transferi ve iletisim portu gibi). Bu portlardan biri "Command port" diğeri DATA port olarak adlandırılır.

Command portu üzerinden ftp iletişimine ait gerekli temel bilgiler aktarılır. Temel bilgiler; ftp sunucuya gönderilecek kullanıcı adı ve parola bilgileri, ftp sunucuya hangi porttan bağlanılacağı, hangi ftp çeşidinin kullanılacağı gibi bilgiler olabilir.

Data portu ise veri transferi amaçlı kullanılır.

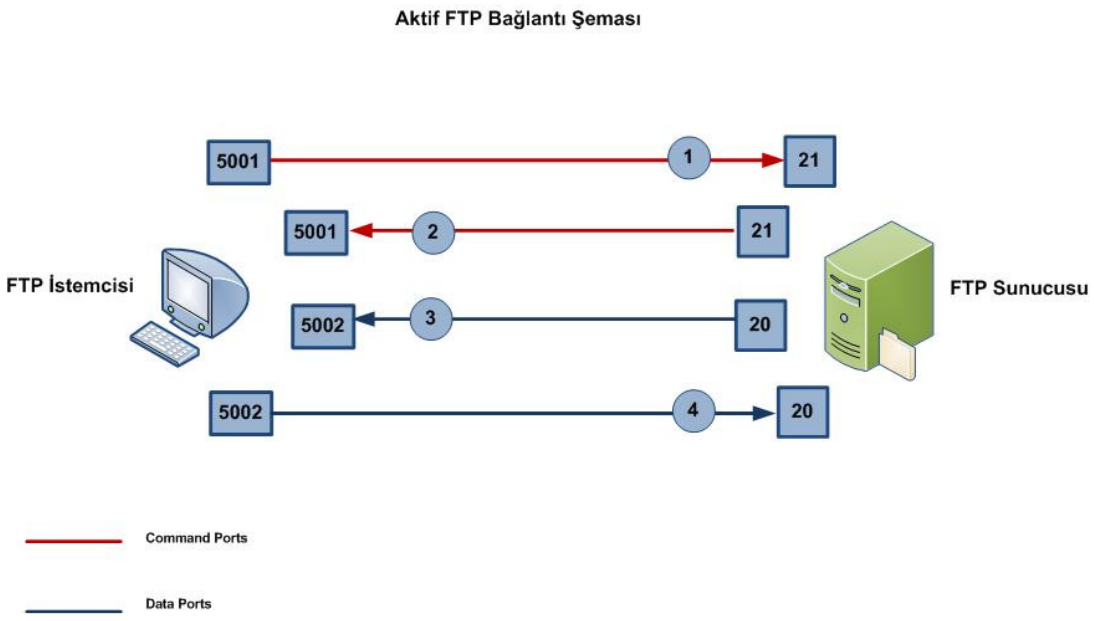
FTP Çeşitleri

FTP iki çeşittir: pasif ve aktif FTP. Her ikisininde farklı amaçlı kullanımları mevcuttur. Hangi FTP çeşidinin kullanılacağı ftp istemcisi tarafından belirlenir.

Aktif FTP

Bu FTP çeşidinde istemci aktif rol alır. Bilinenin aksine orjinal ftp aktif ftpdir fakat günümüz internet altyapısında çeşitli sorunlara yol açtığı için pasif ftp daha fazla tercih edilmektedir. Aktif ftp de çıkan sorunlar pasif ftpnin geliştirilmesini sağlamıştır.

Adım adım Aktif FTP;



1)istemci FTP sunucuya Command portundan(21) bağlanır.

2)FTP sunucu gerekli karşılama mesajı ve kullanıcı adı sorgulamasını gönderir.
-istemci gerekli erişim bilgilerini girer.
-Sunucu erişimi bilgilerini kontrol ederek istemciye yanıt döner.
Eğer erişim bilgileri doğru ise istemciye ftp komut satırı açılır.

Burada istemci veri transferi yapmak istediğinde(ls komutunun çalıştırılması da veri transferi gerçekleştirir)3. adıma geçilir.

-İstemci kendi tarafında 1024'den büyük bir port açar ve bunu PORT komutu ile FTP sunucuya bildirir.

3)FTP sunucusu , istemcinin bildirdiği port numarasından bağlantı kurar ve gerekli aktarım işlemleri başlar.

4) İstemci Onay mesaji gönderir.

Örnek Aktif FTP bağlantısı

```
# ftp -A -d 192.168.100.27
Connected to 192.168.100.27.
220 (vsFTPd 2.0.3)
Name (192.168.100.27:root): huzeyfe
---> USER huzeyfe
331 Please specify the password.
Password:
---> PASS XXXX
230 Login successful.
---> SYST
215 UNIX Type: L8
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
---> EPRT |1|192.168.100.27|58518|
200 EPRT command successful. Consider using EPSV.
---> LIST
150 Here comes the directory listing.
```

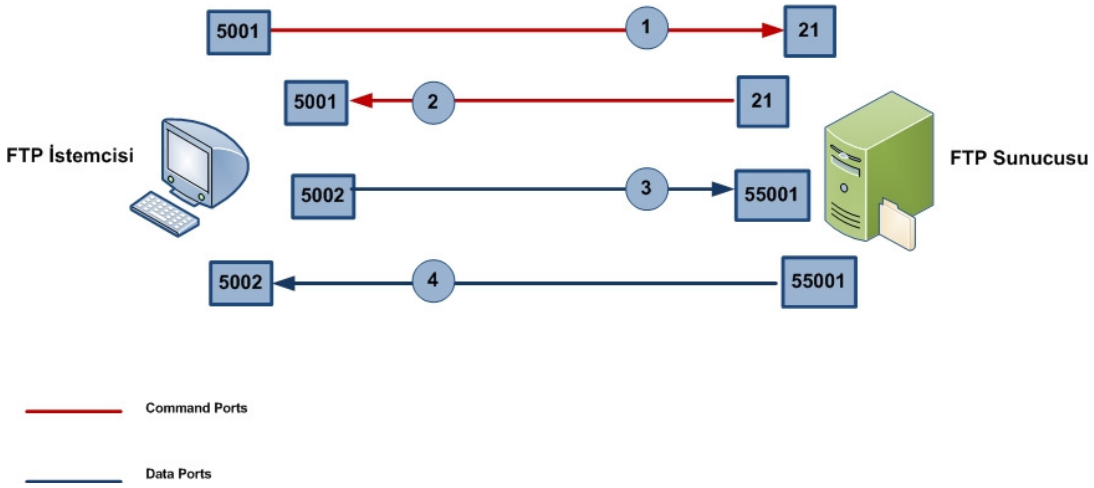
Aktif FTP bağlantısının Sniffer(Wireshark) çıktısı

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.25	193.140.100.100	TCP	1933 > ftp [SYN] Seq=0 Len=0 MSS=1460
2	0.018576	193.140.100.100	192.168.2.25	TCP	ftp > 1933 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452
3	0.018592	192.168.2.25	193.140.100.100	TCP	1933 > ftp [ACK] Seq=1 Ack=1 Win=60480 [TCP CHECKSUM INCORRECT] Len=0
4	0.042998	193.140.100.100	192.168.2.25	FTP	Response: 220 linux.org.tr FTP yansisi
5	0.233337	192.168.2.25	193.140.100.100	TCP	1933 > ftp [ACK] Seq=1 Ack=31 Win=60450 [TCP CHECKSUM INCORRECT] Len=0
6	1.845505	192.168.2.25	193.140.100.100	FTP	Request: USER ftp
7	1.862332	193.140.100.100	192.168.2.25	FTP	Response: 331 Please specify the password.
8	1.983454	192.168.2.25	193.140.100.100	TCP	1933 > ftp [ACK] Seq=11 Ack=65 Win=60416 [TCP CHECKSUM INCORRECT] Len=0
9	3.251032	192.168.2.25	193.140.100.100	FTP	Request: PASS anon
10	3.269880	193.140.100.100	192.168.2.25	FTP	Response: 230 Login successful.
11	3.405688	192.168.2.25	193.140.100.100	TCP	1933 > ftp [ACK] Seq=22 Ack=88 Win=60393 [TCP CHECKSUM INCORRECT] Len=0
12	13.330639	192.168.2.25	193.140.100.100	FTP	Request: PORT 192,168,2,25,7,143
13	13.349912	193.140.100.100	192.168.2.25	FTP	Response: 200 PORT command successful. Consider using PASV.
14	13.350882	192.168.2.25	193.140.100.100	FTP	Request: NLST
15	13.368457	193.140.100.100	192.168.2.25	TCP	ftp-data > 1935 [SYN] Seq=0 Len=0 MSS=1452 WS=3 TSV=4096339253 TSER=0
16	13.368484	192.168.2.25	193.140.100.100	TCP	1935 > ftp-data [SYN, ACK] Seq=0 Ack=1 Win=60480 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
17	13.388065	193.140.100.100	192.168.2.25	TCP	ftp-data > 1935 [ACK] Seq=1 Ack=1 Win=66240 Len=0 TSV=4096339273 TSER=0
18	13.389043	193.140.100.100	192.168.2.25	FTP	Response: 150 Here comes the directory listing.
19	13.393287	193.140.100.100	192.168.2.25	FTP-DATA	FTP Data: 378 bytes
20	13.394164	193.140.100.100	192.168.2.25	TCP	ftp-data > 1935 [FIN, ACK] Seq=379 Ack=1 Win=66240 Len=0 TSV=4096339273 TSER=0
21	13.394176	192.168.2.25	193.140.100.100	TCP	1935 > ftp-data [ACK] Seq=1 Ack=380 Win=60102 Len=0 TSV=132041 TSER=4096339273
22	13.398324	192.168.2.25	193.140.100.100	TCP	1935 > ftp-data [FIN, ACK] Seq=1 Ack=380 Win=60102 Len=0 TSV=132041 TSER=4096339273
23	13.412246	193.140.100.100	192.168.2.25	FTP	Response: 226 Directory send OK.
24	13.412269	192.168.2.25	193.140.100.100	TCP	1933 > ftp [ACK] Seq=53 Ack=202 Win=60279 [TCP CHECKSUM INCORRECT] Len=0
25	13.416607	193.140.100.100	192.168.2.25	TCP	ftp-data > 1935 [ACK] Seq=380 Ack=2 Win=66232 Len=0 TSV=4096339301 TSER=132041

Pasif FTP

Pasif FTP, günümüz internet dünyasında kullanılan güvenlik duvarı, nat cihazları gibi trafikte değişiklik yapan sistemlerden kaynaklanan ftp problemlerini sunucu tarafında halledebilmek için çıkarılmıuş FTP çeşididir. Pasif FTP de istemci pasif roldedir, sunucu aktif roldedir.

Pasif FTP Bağlantı Şeması



Adım adım Pasif FTP:

1)istemci FTP sunucuya Command portundan(21) bağlanır.

2)FTP sunucu gerekli karşılama mesajı ve kullanıcı adı sorgulamasını gönderir.

-istemci gerekli erişim bilgilerini girer.

-Sunucu erişimi bilgilerini kontrol ederek istemciye yanıt döner. Eğer erişim bilgileri doğru ise istemci

-FTP istemcisi PASV komutu aracılığı ile sunucudan ek port açmasını bekler. Sunucu yapılandırma dosyasında belirtilen port aralığından bir port açarak bunu istemciye belirtir

3)FTP istemcisi , sunucudan gelen bu porta bağlanarak veri alışverişini başlatır

4)İstemci onay mesajı yollar

Örnek Pasif FTP bağlantısı

```
# ftp  -d 192.168.100.27
Connected to 192.168.100.27.
220 (vsFTPd 2.0.3)
Name (192.168.100.27:root): huzeyfe
---> USER huzeyfe
331 Please specify the password.
Password:
---> PASS XXXX
230 Login successful.
---> SYST
215 UNIX Type: L8
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
---> EPSV
229 Entering Extended Passive Mode (|||35330|)
---> LIST
150 Here comes the directory listing.
```

Pasif FTP bağlantısının Sniffer(Wireshark) çıktısı

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.2.25	87.51.34.132	TCP	1929 > ftp [SYN] Seq=0 Len=0 MSS=1460
2	0.295302	87.51.34.132	192.168.2.25	TCP	ftp > 1929 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452
3	0.295362	192.168.2.25	87.51.34.132	TCP	1929 > ftp [ACK] Seq=1 Ack=1 Win=60480 [TCP CHECKSUM INCORRECT] Len=0
4	0.737723	87.51.34.132	192.168.2.25	FTP	Response: 220 ftp.beastie.tdk.net FTP server (Version 6.00LS) ready.
5	0.738121	192.168.2.25	87.51.34.132	FTP	Request: USER anonymous
6	0.899371	87.51.34.132	192.168.2.25	FTP	Response: 331 Guest login ok, send your email address as password.
7	0.899539	192.168.2.25	87.51.34.132	FTP	Request: PASS mozilla@example.com
8	1.192982	87.51.34.132	192.168.2.25	FTP	Response: 230 Guest login ok, access restrictions apply.
9	1.193174	192.168.2.25	87.51.34.132	FTP	Request: SYST
10	1.409623	87.51.34.132	192.168.2.25	FTP	Response: 215 UNIX Type: L8 Version: BSD-199506
11	1.409798	192.168.2.25	87.51.34.132	FTP	Request: PWD
12	1.657851	87.51.34.132	192.168.2.25	FTP	Response: 257 "/" is current directory.
13	1.658031	192.168.2.25	87.51.34.132	FTP	Request: TYPE I
14	1.887282	87.51.34.132	192.168.2.25	FTP	Response: 200 Type set to I.
15	1.887457	192.168.2.25	87.51.34.132	FTP	Request: PASV
16	2.043888	87.51.34.132	192.168.2.25	FTP	Response: 227 Entering Passive Mode (87,51,34,132,230,35)
17	2.044157	192.168.2.25	87.51.34.132	FTP	Request: SIZE /
18	2.044318	192.168.2.25	87.51.34.132	TCP	1930 > 58915 [SYN] Seq=0 Len=0 MSS=1460
19	2.302096	87.51.34.132	192.168.2.25	FTP	Response: 550 /: not a plain file.
20	2.302281	192.168.2.25	87.51.34.132	FTP	Request: MDTM /
21	2.303292	87.51.34.132	192.168.2.25	TCP	58915 > 1930 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452
22	2.303310	192.168.2.25	87.51.34.132	TCP	1930 > 58915 [ACK] Seq=1 Ack=1 Win=60480 [TCP CHECKSUM INCORRECT] Len=0
23	2.474597	87.51.34.132	192.168.2.25	FTP	Response: 550 /: not a plain file.
24	2.474772	192.168.2.25	87.51.34.132	FTP	Request: RETR /
25	2.667775	87.51.34.132	192.168.2.25	FTP	Response: 550 /: not a plain file.
26	2.667957	192.168.2.25	87.51.34.132	FTP	Request: PASV
27	2.974166	87.51.34.132	192.168.2.25	FTP	Response: 227 Entering Passive Mode (87,51,34,132,204,56)
28	2.974385	192.168.2.25	87.51.34.132	TCP	1930 > 58915 [FIN, ACK] Seq=1 Ack=1 Win=60480 [TCP CHECKSUM INCORRECT] Len=0
29	2.974516	192.168.2.25	87.51.34.132	FTP	Request: CWD /

Güvenlik Duvarlarında Yaşanabilecek FTP Sorunları

Zaman zaman arkadaşlarınızın FTP ye bağlanıyorum ama ls çektiğimde bağlantı kopuyor ya da öylesine bekliyor dediğine şahit olmuşsunuzdur. Bu gibi istenmeyen durumlar FTP'nin karmaşık yapısı ve Firewall'ların protokolden anlamamasından kaynaklanır.

Bir Firewall'da HTTP bağlantısını açmak için sadece 80. portu açmanız yeterlidir fakat FTP için 21. portu açmak yetmez.

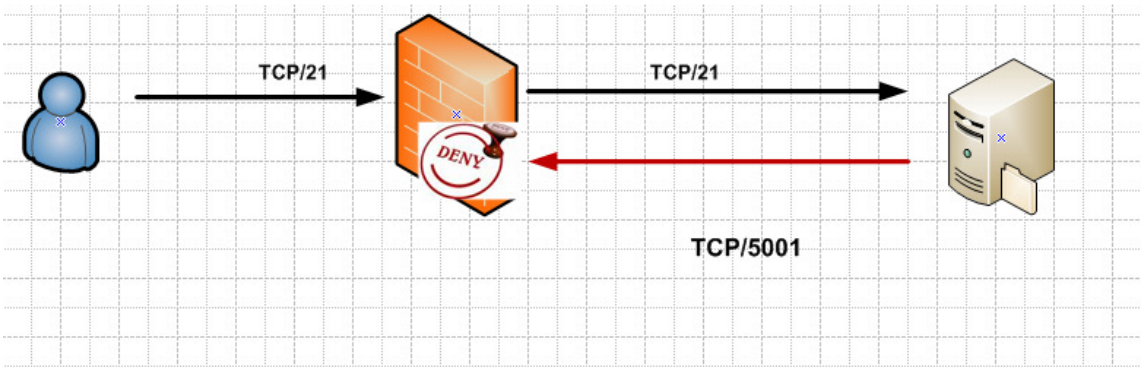
Bunun sebebi FTP'nin komutların gidip geldiği ve verinin aktığı port olmak üzere iki farklı port üzerinden çalışmasıdır. İlk port sabit ve bellidir:21. port fakat veri bağlantısının gerçekleştiği port olan diğer port kullanılacak ftp çeşidine (Aktif FTP veya PAsif FTP) göre değişir ve eğer firewall FTP protokolünden anlamıyorsa genelde sorun yaşanır.

Yeni nesil Firewall'larda bu sıkıntı büyük ölçüde giderilmiş olsa da ara ara eksik yapılandırmalardan aynı hataların yaşandığını görüyoruz.

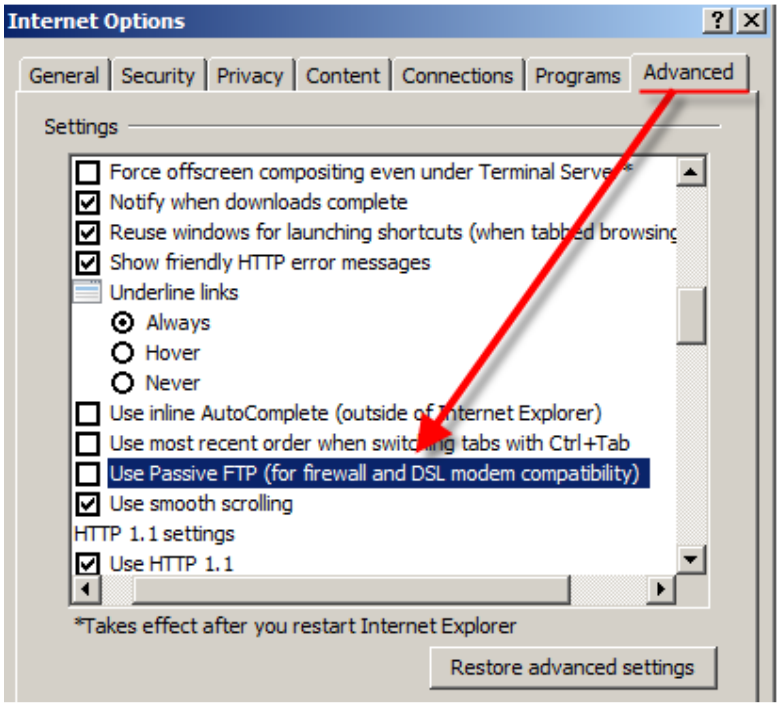
Linux Iptables'da ftp problemini aşmak için mod ip_conntrack_ftp modülünün sisteme yüklenmesi gerekir. OpenBSD Packet Filter ise bu tip aykırı protokoller için en uygun yapı olan proxy mantığını kullanır. FTP için ftp-proxy, upnp için upnp proxy, sip için sip-proxy vs.

Aktif FTP ve Güvenlik Duvarı

FTP istemcinin önünde bir Firewall varsa istemci kendi tarafında port açsa bile bu porta izin Firewall tarafından verilmeyeceği için problem yaşanacaktır.

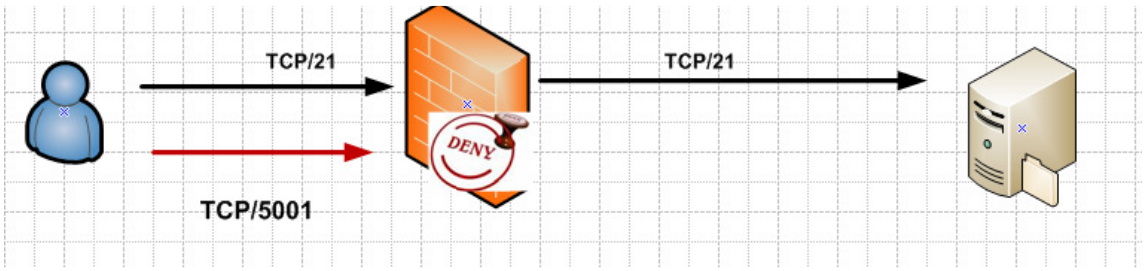


Internet Explorer varsayılan durumda Aktif FTP yapmaya çalışır. Pasif FTP yapmaya zorlamak için aşağıdaki adımlar takip edilmelidir;



Pasif FTP ve Güvenlik Duvarı

Pasif FTP de ftp sunucu ek port açsa bile önünde bir firewall varsa Firewalldan o porta erişim izni verilmesi gerekir.



Kaynaklar:

[1] http://slacksite.com/other/ftp.html
[2] http://blog.lifeoverip.net/2009/01/19/openbsd-packet-filter-yuk-dengelemede-ftp-kullanimi/
[3] http://www.kalamazoolinux.org/presentations/20010417/conntrack.html