

RE: FTP Proxy

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2004-01/0504.html>

From: David Gillett (gillettdavid_at_fhda.edu)

Date: 01/30/04

To: "'Fernando Gont'" <fernando@gont.com.ar>, "'pablo gietz'" <pablo.gietz@nuevobersa.com.ar>
Date: Fri, 30 Jan 2004 10:33:02 -0800

Gack! You're right about the server specifying the port — I had misremembered that bit, and it led me to try to make almost the right point, but from the wrong side of the session.

Let's consider again the client side. My users don't just want to get to a single specific outside FTP server. Potentially, they could want to get to every public FTP server in the world, and maybe a few that aren't public, but which they individually or we, as an organization, have been granted access to.

Again, if I have a stateful firewall with FTP awareness, properly configured, I don't care whether the clients are active or passive.

What if I don't, for whatever reason, have such a device? (Perhaps we're millions of dollars in the red, and our funding source is also in the red by Billions....) To allow my users to use PASV mode to a vast array of external FTP servers, I have to allow them to make outbound connections on any arbitrary port. (At this point, it no longer matters whether the client or the server picks the port number — *I* don't get any say.)

There is a traditional view that the role of perimeter security is to keep bad traffic out, and that all traffic originating from inside is good/trusted/etc. This wasn't too unreasonable before about 1995, when many users could be assumed to know every piece of software on their machines, and to be responsible for its network traffic.

We don't live in that world any more. The vast majority of users haven't a clue what's legitimately on their box, let alone what bits of malware/spyware/etc have surreptitiously installed themselves. You *have* to do egress filtering for your local network to be a good citizen of the Internet.

And allowing PASV mode means you can't do that with a simple packet filter. If I disallow PASV mode, I can at least limit the inbound data connections to servers sourcing from port 20, which is admittedly a hole, but will suffice against most script kiddies, etc. It's (IMHO) a much smaller hole than allowing arbitrary internally-originated streams out.

SecurityFocus BASICS: RE: FTP Proxy

[Some simple-minded NAT boxes may only be able to create mappings for outbound connections, in which case PASV is the only option. That **might** be Pablo's situation — or with his multiple perimeters to cross, there's a chance that one permits only PASV and another only non-PASV. Ouch....]

If I'm going to offer a publicly-accessible FTP server, I really want to put it behind a stateful firewall with FTP awareness, so I don't care whether clients are active or passive. My firewall will see the PORT commands and do the Right Thing. If I can't properly firewall it, my choices are to either block PASV access, or hope the server software allows us to configure some restrictions on the data ports and duke it out with the server admin to enact them.

I think it's pretty obvious that the Right Solution is a good firewall (which also requires symmetric border routing, so the firewall sees both sides of every session — also not always available, unfortunately). But if you can't do that, PASV mode is not **automatically** the best compromise available.

My hot button isn't really about PASV per se, but about the too-frequent knee-jerk suggestion that it is the answer to every FTP network security question. Fernando, I may have read a little more of that into your initial response than you intended, and if so then I apologize.

David Gillett

> -----Original Message-----
> From: Fernando Gont [mailto:fernando@gont.com.ar]
> Sent: Friday, January 30, 2004 9:23 AM
> To: gillettdavid@fhda.edu; 'pablo gietz'
> Cc: security-basics@securityfocus.com
> Subject: RE: FTP Proxy
>
>
> At 08:29 30/01/2004 -0800, David Gillett wrote:
>
>> > This requires more processing in the firewall, though.
>> > Because the PORT command must be "patched" in the stream, it
>> > may be the
>> > case that the firewall not only needs to recalculate TCP's
>> > checksum, but
>> > may have to "recalculate" the sequence numbers, too. (The
>> > "patched" PORT
>> > command might be longer or shorter than the original one).
>> Who said anything about PATCHING the PORT commands?
>
> Sorry, I got hang thinking in the NAT.
>
>
>> > It's probably more easy to configure the FTP server to use
>> > some specified

RE: FTP Proxy

SecurityFocus BASICS: RE: FTP Proxy

> > > port range (and thus allow incoming connections on only those
> > > ports) than
> > > configure **all** the clients that want to access your FTP site
> > > in a similar way.
> > *BUT that's not how PASV FTP works! In PASV, the *CLIENT* picks a
> > random port number, and sends the server a PORT command
> > that says "I'm
> > about to connect to your port XXX, please bend over and drop your
> > pants." The server doesn't get to say "Please only use ports
> > YYY–ZZZ."*
>
> *That's not the way PASV FTP works!*
>
> *For passive FTP transfers, the client issues a *PASV*
> command. The server
> replies with an IP:port where it will listen for the client
> connection. And
> the client will connect to that IP:port, which has been
> specified by the
> *server*.*
>
> *In active transfers, the client sends a *PORT* command
> telling the server
> on which IP:port it will listen for incoming connections. And
> the server
> will connect to that IP:port, which has been specified by the
> *client*.*
>
> *Section 3.3 of RFC 959 says:*
>
> *" Negotiating Non–Default Data Ports: The User–PI may specify a
> non–default user side data port with the PORT command. The
> User–PI may request the server side to identify a non–default
> server side data port with the PASV command. "*
>
> *Also from RFC 959:*
>
> *" PASSIVE (PASV)
> This command requests the server–DTP to "listen"
> on a data
> port (which is not its default data port) and to
> wait for a
> connection rather than initiate one upon receipt of a
> transfer command. The response to this command
> includes the
> host and port address this server is listening on.
> "*
>
> *and also*
>
> *" DATA PORT (PORT)*

RE: FTP Proxy

SecurityFocus BASICS: RE: FTP Proxy

>
> *The argument is a HOST-PORT specification for*
> *the data port*
> *to be used in data connection. There are*
> *defaults for both*
> *the user and server data ports, and under normal*
> *circumstances this command and its reply are not*
> *needed. If*
> *this command is used, the argument is the*
> *concatenation of a*
> *32-bit internet host address and a 16-bit TCP*
> *port address.*
> *This address information is broken into 8-bit*
> *fields and the*
> *value of each field is transmitted as a decimal*
> *number (in*
> *character string representation). The fields*
> *are separated*
> *by commas. A port command would be:*
>
> *PORT h1,h2,h3,h4,p1,p2*
>
> *where h1 is the high order 8 bits of the internet host*
> *address.*
> "
>
> *As you see, in active transfer, the client *chooses* on which*
> *IP:port it*
> *will accept connections. In passive transfers, the server*
> **chooses* on*
> *which port it will accept incoming connections.*
>
>
> > *BTW, the FTP server was external to his organization, so...*
> > *why should *him* take the risk?*
> > *If I run an FTP server, must I assume *all* of the risk? If so,*
> > *I'm going to get really picky about who I trust to connect to it...*
>
> *Unless you expect that all clients be configured to use*
> *passive transfers, yes.*
>
> *Anyway, I don't think it's that risky....*
>
>
> --
> *Fernando Gont*
> *e-mail: fernando@gont.com.ar || fgont@acm.org*
>
>

SecurityFocus BASICS: RE: FTP Proxy

Ethical Hacking at InfoSec Institute. Mention this ad and get \$720 off any course! All of our class sizes are guaranteed to be 10 students or less.

We provide Ethical Hacking, Advanced Ethical Hacking, Intrusion Prevention, and many other technical hands on courses.

Visit us at <http://www.infosecinstitute.com/securityfocus> to get \$720 off any course!
