

RE: FTP Window of opportunity?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-03/0163.html>

From: Stevenson, John G (*JGStevenson_at_pier1.com*)

Date: 03/24/04

Date: Wed, 24 Mar 2004 11:57:10 -0600

To: "Jerry Shenk" <jshenk@decommunications.com>, <pen-test@securityfocus.com>

Kind of off-topic, although I'd love for Carolyn to sniff the traffic and report back, just for our on satisfaction. Anyway, on to my question: Is this "intentional response" by the raptor firewall really a good thing? Does it allow the connections to pass 'to' the server or does it seemingly accept the connections and drop them once the response is sent to the attacker? Just curious...

John

-----Original Message-----

From: Jerry Shenk [mailto:jshenk@decommunications.com]

Sent: Tuesday, March 23, 2004 9:37 PM

To: pen-test@securityfocus.com

Subject: RE: FTP Window of opportunity?

I'd use a sniffer to log monitor what actual packets are being received from the "ftp server" to see what scanner is right. It would seem to me that ISS should be getting something back if it's claiming that the port is open. You could run a sniffing in the path of the traffic between the scanning machine and the ftp server and set it to only log the traffic between that pair.

It seems quite normal to get results back from an automated tool that conflict with something else. Then the pen tester needs to dig a little deeper and analyze what actually happened.

BTW, some firewalls (Raptor at least) intentionally respond to all kinds of crazy traffic. It seems that they intentionally try to confuse an attacker (or pen tester;) by allowing connections to ports that aren't really open.

-----Original Message-----

From: C Ryll [mailto:carolynryll@hotmail.com]

Sent: Tuesday, March 23, 2004 4:50 PM

To: pen-test@securityfocus.com

Subject: FTP Window of opportunity?

SecurityFocus Penetration: RE: FTP Window of opportunity?

I recently assessed a system in which I already know its configuration (and have full legal rights to). FTP is purposefully not running, as well as blocked by the firewall.

When I scan with ISS, the FTP port shows up. When I use NMap, it does not show FTP's port.

Because of the discrepancy, I tried to manually FTP into the system. It actually said "Connected...", hung for about 10 seconds, and then said "Connection Terminated."

(As a baseline, telnet's port is also blocked by the firewall, and does not show up in scans – essentially, results for telnet are as expected).

With ISS, I'm assuming that it saw "Connected..." and showed me that port.

My guess would be that NMap waited around to try something else, but saw

"Connection Terminated" and didn't list it.

However, as I said previously, seeing that it actually says "Connected", and then hangs for about 10 seconds before terminating:

- 1). Can I use this behavior to my advantage somehow? If yes, how?
- 2). Is there a known explanation to this?

The firewall is the Internet Connection firewall, and I am curious if it requires the ftp port inadvertently for its functioning when checking the incoming packets...

While I can make some changes to the system (like shutting off certain services and shutting off the firewall), I cannot modify it such that I can try another firewall or anything else like that.

Any help is greatly appreciated.
Carolyn.

All the action. All the drama. Get NCAA hoops coverage at MSN Sports by ESPN. <http://msn.espn.go.com/index.html?partnersite=espn>

You're a pen tester, but is google.com still your R&D team?
Now you can get trustworthy commercial-grade exploits and the latest techniques from a world-class research group.
www.coresecurity.com/promos/sf_ept1

RE: FTP Window of opportunity?

SecurityFocus Penetration: RE: FTP Window of opportunity?

You're a pen tester, but is google.com still your R&D team?
Now you can get trustworthy commercial-grade exploits and the latest
techniques from a world-class research group.
www.coresecurity.com/promos/sf_ept1

You're a pen tester, but is google.com still your R&D team?
Now you can get trustworthy commercial-grade exploits and the latest
techniques from a world-class research group.
www.coresecurity.com/promos/sf_ept1
