

RE: Bypassing Personal Firewalls

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-02/0270.html>

From: Oliver Lavery (oliver.lavery@sympatico.ca)

Date: 02/22/03

From: "Oliver Lavery" <oliver.lavery@sympatico.ca>
To: "'Drew Copley'" <dcopley@eeeye.com>, <bugtraq@securityfocus.com>
Date: Fri, 21 Feb 2003 18:22:59 -0500

>(Sidenote: a number of previous apps used to test PFWs or Application
Firewalls --
><http://www.pcflank.com/art21.htm>)

Yes, these are great tests. Most PFWs block them all now.

>There are a number of ways to do this, you use the more popular method of
openprocess and
>writeprocess memory. However, there is a limit to the number of api calls
which implement this.
>Ultimately, this kind of code needs to be blocked, first, at the NT API
level... Such blocking
>should use the same method as blocking the network calls, ie, "Do you want
to allow this
>application to ..."

Yes. Before we go prompting users ever time someone calls
CreateFile, though, there are much simpler measures. One of them would make
OpenProcess require a privilege of some sort (see below).

>Most commonly, this would be used with writeprocess memory.
>Createremotethread would need to be blocked in this manner.
Postremotethreadmessage.
>PostThreadMessage. Are some of the more dangerous calls, in this context.

You'll notice that all of these calls require a handle returned by
OpenProcess (hProcess in my code).

>After that, you are probably talking about having to do somesort of
signature analysis at the
>binary level.

MD5 of the binary memory image! This is probably feasible, but good
god it would resource intensive.

>OpenProcess does require seDebugPrivileges, I believe.

SecurityFocus Bugtraq: RE: Bypassing Personal Firewalls

No, and this is very much the point. According to MS docs:
SeDebugPrivilege:
Determines which users can attach a debugger to any process. This privilege provides powerful access to sensitive and critical operating system components.

This only prevents users from using OpenProcess on system processes (winlogon.exe etc.). There need to be tighter restrictions on the use of OpenProcess.

Cheers,
~ol