

## Re: XP Personal Firewall

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-08/0042.html>

---

**From:** Mike Arnold ([mike@midkaemia.fsnet.co.uk](mailto:mike@midkaemia.fsnet.co.uk))

**Date:** 08/17/02

From: Mike Arnold <[mike@midkaemia.fsnet.co.uk](mailto:mike@midkaemia.fsnet.co.uk)>

To: "Jeremy Junginger" <[jjunginger@interactcommerce.com](mailto:jjunginger@interactcommerce.com)>, <[pen-test@securityfocus.com](mailto:pen-test@securityfocus.com)>

Date: Sat, 17 Aug 2002 02:17:30 +0100

On Thursday 15 Aug 2002 5:50 pm, Jeremy Junginger wrote:

- > *I've come across a few XP hosts that are trying to be sneaky with the*
- > *"Internet Firewall" feature enabled. I've seen responses from NMAP SYN*
- > *and ACK scanning while seeing next to nothing on Nessus. Also, I am*
- > *unable to uncover any additional information about the hosts and*
- > *available services. Do you have any tips on beating the XP "firewall?"*
- > *Perhaps there is a post in the archives.*

nmap and nessus are basically 2 different tools classes. Nmap tells you which ports are open, but no info on what software is available – you would have to banner the port for that. The report generated by nmap maps ports-> services using the information in the /etc/services file (on RH linux anyway) and not from a banner grab if I remember correctly!

Nessus is a vulnerability scanner and does banner the ports, etc. provided the appropriate plugins are enabled. In your case where you want the services running, usernames, etc. then you are looking for specific ports to be open using the nmap scanner, these being port 135 (lists DCE services) and ports 137/139 (NetBios – usernames, domain SIDs and other useful stuff). If those ports aren't open then you won't be able to get that information easily, even with nessus. Nessus will only report on ports that are open – after all, there are few vulnerabilities for closed ports.

Without netbios ports open nessus won't be able to connect on a "null" session to provide you with that information, and even with NetBios open a registry hack will prevent "null" sessions anyway. If these are malicious machines then in all likelihood they have closed off any means of obtaining useful information from them since that would prevent them from operating in stealth mode. Of course they could be very clever and simply return you a series of dummy responses leaving you to hack account "xyz" that never existed; or trying connecting to share "abc" that doesn't exist either!

At the end of the day, the firewall is there to block this kind of intrusion. From what I know and have read, the XP firewall is pretty good at doing it (please correct me if I'm wrong). Most exploits of systems running firewalls

## SecurityFocus Penetration: Re: XP Personal Firewall

of this nature target applications exposed on other ports such as instant messaging or Universal PnP or a web server (yum), and of course the ubiquitous dumb user (—please click here —) exploit!

Since you should only be doing this on boxes you "own" anyway (in the "It's my machine 'cos I've paid for it sense", not the "I OwnZ u" sense), wouldn't it just be easier to physically locate the machines and use other techniques to interrogate them or the users?

On a final note, they now know you are coming as well since you have already performed a very "loud" network scan of them using nessus. So if they are malicious machines, chances are there will be some surprises in store for you when you get to the boxes and successfully logon! Provided they haven't just setup a couple of drone machines that they don't care about of course!

Great fun isn't it?

> *-Jeremy*

Mike

--

"In their capacity as a tool, computers will be but a ripple on the surface of our culture. In their capacity as intellectual challenge, they are without precedent in the cultural history of mankind."  
Edsger Wybe Dijkstra on Computers

---

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

---

- **Previous message:** [Earl Sammons: "RE: Digital UNIX 5.60 recurses"](#)
- **In reply to:** [Jeremy Junginger: "XP Personal Firewall"](#)
- **Next in thread:** [Mike Arnold: "Re: XP Personal Firewall"](#)
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)