5.6.1

Testing Your Host Firewall

Version 1

March 2005

Laboratory Overview

Objective

At the end of this lab students will be able to test a host firewall for common vulnerabilities.

Information for Laboratory

A. Students will test a host without a firewall for network access vulnerabilities.
B. Students will repeat vulnerability testing with an active host firewall.

Student Preparation

The student will have completed requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

Be sure that your computer has internet access and that at least one firewall program is available. The Microsoft firewall included with SP2 is acceptable.

Estimated Completion Time

20 Minutes

Vulnerability Testing

You have all the tools in place, installed and up to date with the latest patches. Installed on the host computer is a virus protection package, an adware/ spyware program, your browser is suitably configured, and of course you have the firewall in place. That means you're completely protected, right?

It's true that in such a case due care has been taken to assure reasonable precaution. Yet it is naïve to suppose that one is blithely in a state of invulnerability. One telecommunications worker put it this way, "If you don't test it, it won't work." Another retorted, "If you do test it, maybe it will work." The first sentiment realizes that if you don't test a system or product, points of failure will never be discovered. The second statement affirms that testing can never be exhaustive.

Information assurance specialists and IT mangers should all be from Missouri, and all should be pessimists of a sort, aware that a failure or successful attack can occur at any time.

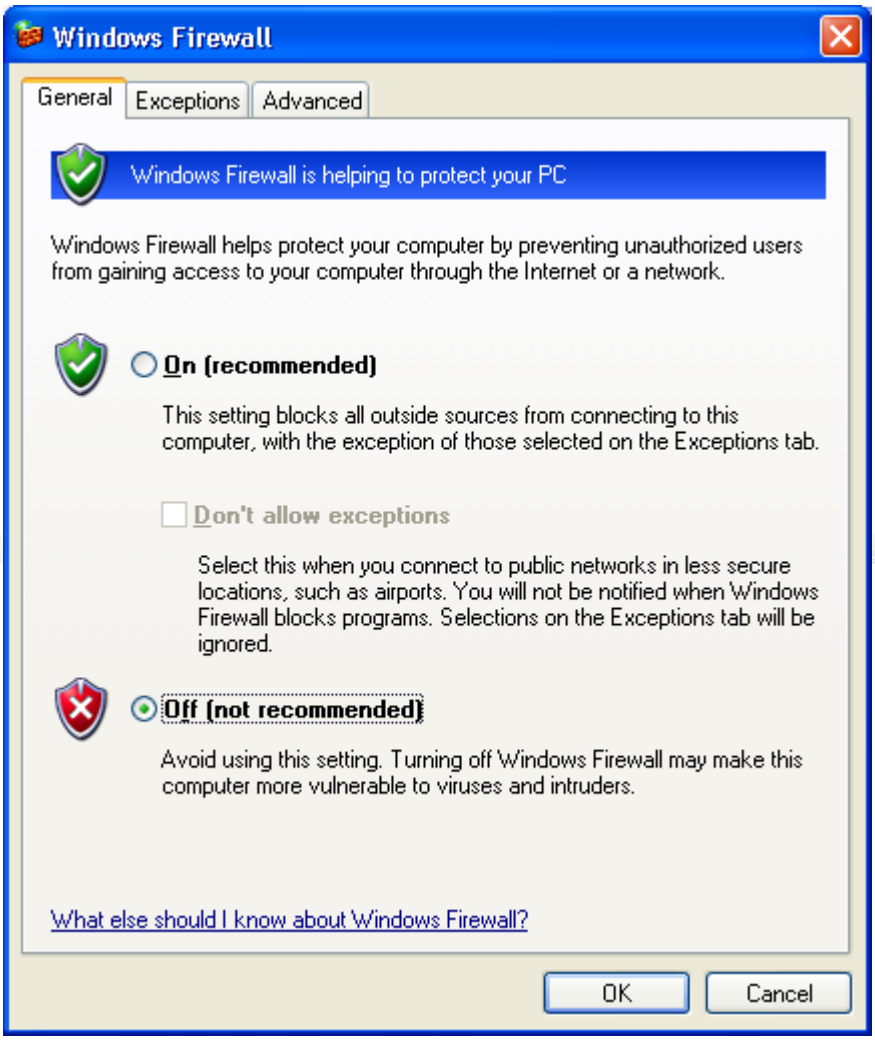
Shields Up!!

A host firewall test cannot be run locally. Of interest is how the host responds to internet communications, and what potential vulnerabilities exist as viewed externally.

This is the purpose of Shields Up!!, an internet based tool provided for free by Gibson Research Corporation. Steve Gibson is a recognized expert in the field and has done a great service by providing Shields Up!! and other free tools.

Step I:
Configure the lab host computer so that a local firewall is not running. Don't worry, the school owns the computer.

If you are using the Windows Firewall included with Windows XP SP2, go to the control panel and select Windows Security Center, and then select Windows Firewall. Turn the Windows Firewall off.



Step 2:
Browse to the home page of Gibson Research Corporation,

www.grc.com

There is a plethora of information available that can be assimilated later. For now, navigate to Shields Up!! which is under Hot Spots. Be sure to read the important points prior to proceeding to the Shields Up!! page.

From the Shields Up!! page, the following tests can be performed:

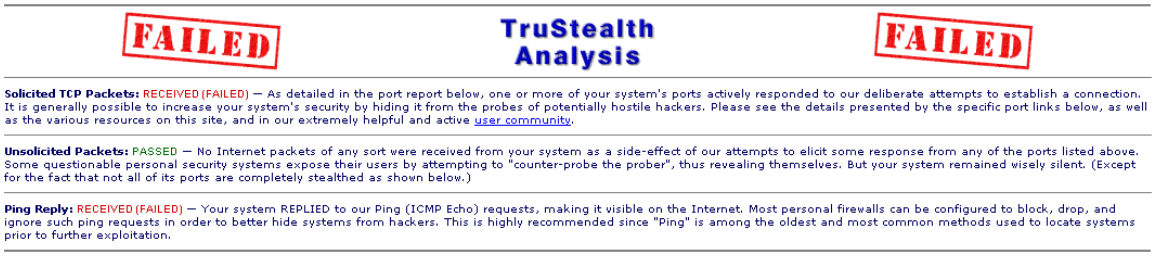
File Sharing
Common Ports
All Service Ports

Messenger Spam
Browser Headers
User Specified Custom Port Probe

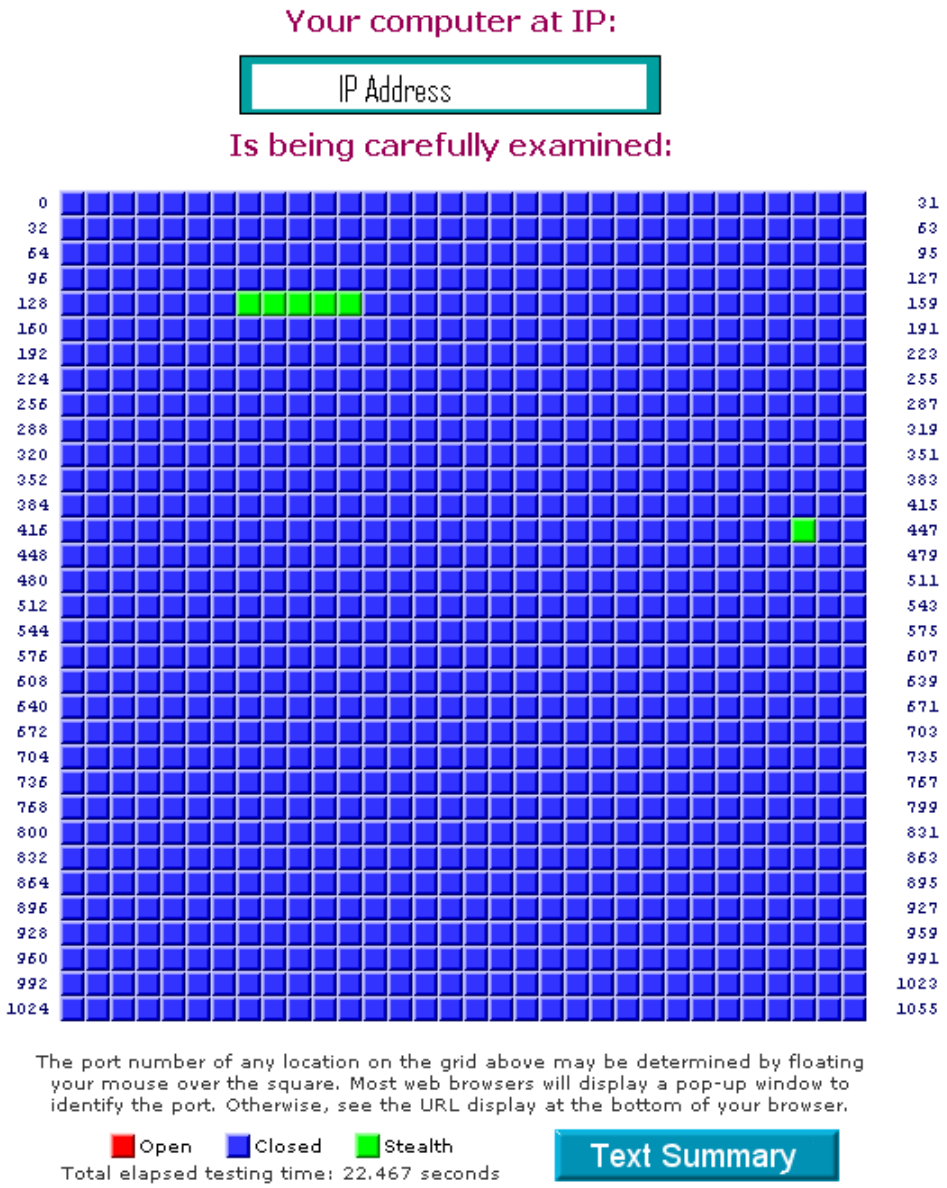
You can also Lookup Specific Port Information.

Begin by testing File Sharing, which will test port 139 and NetBIOS activity. Document your results.

Step 3:
Continue by testing Common Ports. Results might look like the following:



Be sure to study the detailed listing following the summary. Now that we have tested common ports, continue by testing All Service Ports.

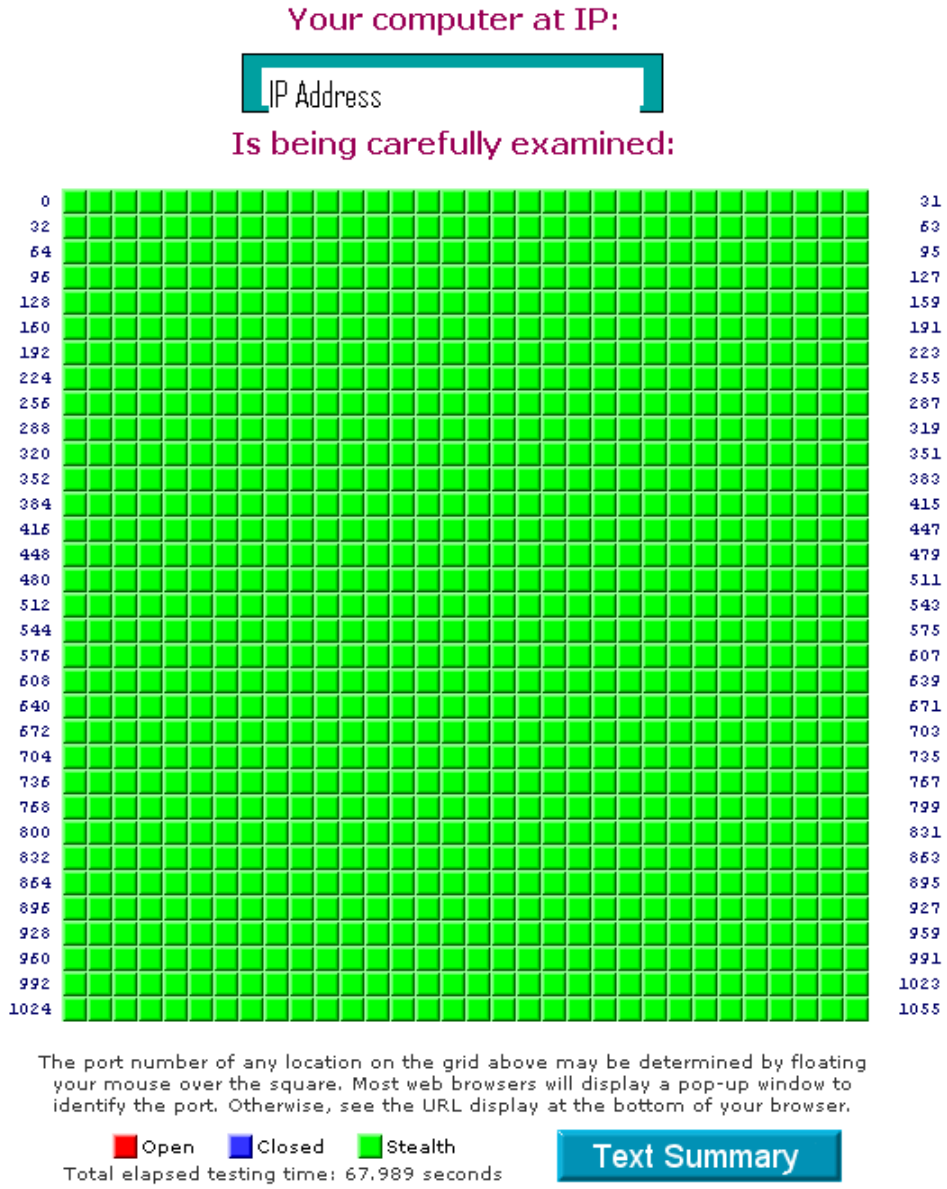


Continue using Shields Up!! by testing Messenger Spam and Browser Headers. Be sure to test the cookie feature of the Browser Header test.

Step 4:
Go back to the Microsoft Security Center and activate the Microsoft Firewall. Then repeat the Shields Up!! test suite.

With the Microsoft Firewall active, all common ports are now in stealth mode. In fact, on further testing All Service Ports, it will be found that all service ports are in stealth mode when the Microsoft

Firewall is active. Shields Up!! might still declare failure only by registering a valid ping reply.



Analysis

1) Discuss the usefulness of the Shields Up!! tool for both home and business use.

2) What broader implications do you conclude regarding testing of a network rather than just a host?

3) What is the difference between a port being closed versus stealth mode?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

If You Want To Learn More

Use the Lookup Specific Port Information to learn more about network services. As an example, find out about port 443, reputed to be one of the more problematic ports.

Explore more information at the home page of Gibson Research Corporation. Be sure to see the video about his excellent SpinRite product.

Appendix

This lab was completed using Microsoft Windows XP Professional SP2 and the associated Microsoft Firewall.