Network Services Thwarts Spammers by Scanning for Vulnerabilities

UFIT
2046 NE Waldo Rd, Suite 2100
Gainesville Florida  32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
Table of Contents

Network Services Thwarts Spammers by Scanning for Vulnerabilities .........................3
Network Services Thwarts Spammers by Scanning for Vulnerabilities

Seeking out vulnerabilities in the ufl.edu network has become a mission for some at NERDC.

As part of keeping the ufl.edu domain safe from hackers, Network Services scans campus PCs and servers to find chinks in the armor that could be exploited to send spam or, worse, compromise data or hosts.

Computers are "scanned" by sending data packets to various "ports" on each computer, and observing the computer's response. Ports are the numbers included with each Internet packet that specify which (or what type) of program is to process that packet. A computer has a port "open" if it is running software which responds to packets addressed to that port. While often useful, and sometimes even necessary, open ports present "windows of opportunity." If they are vulnerable, or become so, hackers can attack them and hi-jack those ports for their own purposes.

"We're scanning ports because it takes less energy and you will sustain less damage if you fix things that you know are broken before they are attacked. If you have a large population of anything, something's going to be broken. The server's administrators might be busy or they might have installed the software five years ago and it's been running fine. They may be too busy to pay attention to bug reports. Things drift," said Marcus Morgan, network coordinator of Network Services.

A year ago, there were enough vulnerabilities and hackers/spammers taking advantage of them that any mail originating from ufl.edu (UF's mailing address, for all practical purposes) was blocked from many servers and other service providers. The university, in effect, was "blacklisted" from sending out any mail. This prompted Network Services to start a pro-active approach against hackers and spammers taking advantage of servers on the ufl.edu domain. The security team at NERDC has been scanning ports since then.

A port scan done by the group tells them which ports are open and being used for network activity (such as File Transfer Protocol, telnet, or Web servers) and what software is being run on the other end. Using that information, they can determine which may be vulnerable to attack. After running additional tests, the group works with the computer's administrators to help make the box a less likely target.

"For scanning we use an automated process against an address space. Our tests are very specific and we publicize what we're going to do before we do it. We post to the net-managers list and tell them when we're starting and what we're going to do, so that if they have detection software running, they'll know it's just us," said Morgan.

Using this approach, Network Services has reduced the number of possible "chinks in the armor" from 277 down to fewer than 10.

Morgan wants network managers on the ufl.edu domain to know that many times when people scan ports, these scans are meant to be a good offensive move against hackers. While some of the tools used may be the same as those in a hackers' software toolkit, the end results are a reporting of where vulnerabilities may be and what the owners can do to fix them.

"What we're doing is not invasive. We're trying to detect the presence of servers and the
software running on them. We're not trying to exploit vulnerabilities that are there," he said.

"It's an ongoing process. I'd have a coronary if we ran a scan and didn't find something."

**Your Comments are Welcome**

We welcome your comments and suggestions on this and all UFIT documentation. Please send your comments to:

**UF Information Technology**

**UFIT**

2046 NE Waldo Rd, Suite 2100
Gainesville Florida  32609-8942
(352) 392.2061
<editor@cns.ufl.edu>