CNS /Update Newsletter Feature

I&R: A Day in the Life of a Network Security Administrator

CNS Document ID: u021002a
Last Updated: 11/8/02

UF Information Technology

UFIT

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

I&R: A Day in the Life of a Network Security Administrator ........................................3
The attacks are silent, except to those on the prowl for them. Quiet probes seeking weaknesses and exploits are the signs of the quarry sought by Network Security Coordinator Kathy Bergsma and the OIT Network Services security team.

Bergsma detailed a day in the life of a security administrator to the September 6 meeting of the NERDC Instruction and Research User's Group.

"One of the first things I do each day is check my e-mail for complaints sent to abuse@ufl.edu. Generally there are several messages; many of which are false positives," said Bergsma.

She and her staff also sift through other complaints. There are spam complaints to which all they can do is respond with an educational message about how the sender can combat the spam. If there are complaints about spam that originated from UF computers, the security team resolves the problem.

After looking through e-mail, they turn their attention to the IDS (Intrusion Detection System) logs. IDS detects suspicious activity on the routers that could mean someone is launching a hack attack. The Intrusion Detection System has been in place since right before the Year 2000 rollover. In the IDS logs, hacker activities -- such as attempts to gain command line access on a Web ports -- show up. It also searches for hack patterns that would indicate password cracking.

"People are trying every day to compromise the ufl.edu domain. Sometimes it's just for bragging rights. Sometimes, it's more," Bergsma said.

UF recognized the security problem with .edu domains many years ago and was one of the first universities to start building a security team and security infrastructure.

When they are finished checking e-mail and security logs, they turn their attention to prevention. This includes contacting network administrators who have vulnerable computers on the network.

Training is another aspect of prevention. Yearly, UF holds a daylong event focusing on computing security, ITSA (Information Technology Security Awareness) Day. ITSA Day this year was held on September 25, 2002. For more information about the event, please see http://www.itsa.ufl.edu.

Bergsma also discussed UF's contract with Foundstone to provide a network security training workshop on NetBIOS vulnerabilities, which was held in July. On November 6, the Foundstone training continues with a seminar about "Web Hacking." The seminars are sponsored by the UF Provost's office and are free to UF employees. For more information about the upcoming Foundstone seminar, please see http://net-services.ufl.edu/security and click on General Info. Select Foundstone seminar from the list.

Bergsma said her days also include meeting with the Network Security Policy Committee, which gathers monthly to keep security policies updated.
At the end of the day, there's always more "hacktivity" to track down, but through educating network administrators, prevention at the router-level, and other security measures, the Security Team makes sure our wired campus is as secure as possible.

Your Comments are Welcome

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

UFIT Information Technology

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