CNS /Update Newsletter Feature

Security Team Safeguards
UF/NERDC Networks

CNS Document ID: u001111a
Last Updated: 11/01/2000

UF Information Technology

UFIT

2046 NE Waldo Rd, Suite 2100
Gainesville Florida  32609-8942
(352) 392.2061
<editor@cns.ufl.edu>
Security Team Safeguards UF/NERDC Networks

Knowledge is power. Increasingly, as computing and information technology become more important in our lives, we find that, like knowledge, so too information is power. It is probably safe to say that nearly every person in the developed world has experienced important changes and improvements in his or her life due to the explosion in information technology. NERDC is privileged to be at the forefront of the "Information Technology Revolution," providing Internet connectivity to the UF campus and other groups, and managing the UF Intranet. However, the same technologies responsible for so many wonderful and useful changes in our society also expose us to new threats and vulnerabilities. As we become increasingly dependent on the free and fast flow of information for everything from our medical and financial records to casual correspondence, so too are we endangered by any threat which compromises that information, or our ability to access it. Just as "power corrupts," information technology lends itself to being abused by the unscrupulous and malicious.

As an important part of its role in providing information and network services, NERDC is also responsible for ensuring the stability and security of those services, guarding against threats both mischievous and malicious.

To meet this responsibility, NERDC has established a Network Security team which works with the system managers of the various colleges, departments, and other groups we serve, as well as end users. The Network Security team helps by educating the individuals responsible for each system about potential threats and "best practices" security measures which should be taken to guard against those threats. They also provide tools to test for vulnerabilities, and assistance in recovery and damage control when a security compromise does occur. In addition to its role in assisting the system managers and users, the team also employs a variety of tools which continually evaluate the overall "health" of the networks it serves. These tools provide alerts whenever conditions suggest that an attack or other compromise is in progress, watching not only for characteristic malicious data packets, but also for patterns which might suggest that normal-seeming packets (such as regular e-mail) are being used as a vehicle for an attack (such as was the case with the "Melissa" or "ILOVEYOU" incidents). These alerts are then reviewed by a Network Security team member to determine what action is needed (if any).

For this story, we spoke with Kathy Bergsma, Network Security Coordinator.

Q: What is "Network Security?"

A: Essentially, network security can be viewed as "risk assessment": understand the assets that you are protecting, the threats against them, and the cost of protecting them. This involves both vulnerability assessment and "attack signature" detection.

Q: Why do we need network security?

A: As part of our role in providing service to UF, we are required by the U.S. Family Educational Right To Privacy Act (a.k.a. the "Buckley Amendment") to protect student records; both to preserve them, and to prevent unauthorized access. Another federal law, the Health Insurance Portability and Accountability Act (HIPAA), has established requirements for privacy and security of individually identifiable medical patient information-rules which specify security standards for the patient medical records used by the Health Science Center and Shands HealthCare.
It is also essential to prevent disruption of services to our users, and to prevent our systems from being used as the source of a security incident. The world-wide interconnectedness of information networks is such that any "compromised" system can be used to launch an attack which can threaten any other system anywhere on the global Internet--or even the functionality of the entire Internet.

Q: What is the scope of NERDC's primary responsibility in this area?

A: In general that includes anything that goes through our Internet connection, which serves the UF campus, FCLA, Health Science Center, Shands HealthCare and IFAS traffic across the state.

Q: What changes have there been in NERDC's network security functions over the past year?

A: I guess the biggest change would be the tools that we use. We now use more sophisticated tools for attack-signature detection. We are continually updating our capabilities to include the best current set of tools for signature detection (recognition of characteristic "signatures" of known attacks), and the latest network scanner technology to locate vulnerabilities, hopefully before the "hacker community" does.

Q: What are some significant events which occurred in the realm of network security during the past year?

A: The rise of "distributed denial of service" attacks is probably the biggest event during this past year. As bandwidth increases, hackers have found new means to deny service. They launch attacks from many (possibly hundreds, some claim thousands) hosts against a single host or domain. Many tools are available to hackers for this purpose.

On the "prevention side" of the equation, we've made tremendous progress at limiting the number of open SMTP relays on campus to help reduce the volume of "spam" that flows through the UF network. We've also improved Domain Name Service (DNS) security in recent months.

Q: How do we usually find out about a security breach?

A: Our network hardware creates logs, which we watch for "attack signatures" and other signs of suspicious activity. In addition, we receive abuse complaints from system managers and users, which alert us to potential problems. NERDC Operations is available 24-7 to handle incoming or outgoing abuse complaints, and the Operations staff will then contact the Network Security team, if necessary.

Q: What sort of spot-checks or intermittent monitoring is done?

A: We do vulnerability assessments of various networks within UF as requested, or as indicated by the Intrusion Detection System and its detection of attacks.

Q: What sort of actions do we take when we become aware of a breach (or potential breach)?

A: A compromised host is immediately disconnected from the network, and the network administrator or department head for the unit responsible for the machine is contacted. We attempt to determine the method of compromise. The host is not allowed to be reconnected to the network until it is rebuilt.
Q: To what degree do we try to be "up-to-the-minute" on implementing defenses against new exploits?

A: We maintain current tools and skills on all fronts.

Q: How can regular users help?

A: Use strong passwords, practice safe e-mail, and maintain current virus protection. Read and understand the Acceptable Use Policy (see "Security Resources" on previous page).

Q: How can subnet managers help?

A: Observe best practices (see "Security Resources" on previous page).

Q: What message do you want to send to our readers about net security, and NERDC's role?

A: Cooperation with all concerned. We're here to help improve security.

Security Resources

Both system managers and end-users can play an important role in safeguarding our shared information networks against attacks and other forms of abuse. The resources below are a good place to start learning how to play your part in this important, cooperative effort. ITSA Day, held annually in the Fall term http://www.itsa.ufl.edu


Internet Security Policy http://www.cio.ufl.edu/inetsec.htm

E-mail net-services@ufl.edu [mailto:net-services@ufl.edu] to request a network vulnerability assessment. E-mail abuse@ufl.edu [mailto:abuse@ufl.edu] to report an abuse complaint.

Your Comments are Welcome

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

UFIT

UFIT

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