A(n Extended) Campus Information Security Conversation

Wherein the chair of the Department of Molecular Gerontology (MG) at a large university <bigu.edu> phones the university's Information Security Officer (ISO)

By **Dan Updegrove**

The text of this skit was used to open the EDUCAUSE Security System Taskforce meeting held at EDUCAUSE 2001 in Indianapolis. It is available online at http://wnt.utexas.edu/~danu/security-skit.html.

MG: Hello, is this the Information Security Office? Our departmental server here in Molecular Gerontology is running very slowly, and students and faculty are complaining to me daily that they can't get their work done. As you may know, Joe Smith, the wizard grad student who architected our network and ran the server so expertly, left last year, and the new student we've assigned, Bill Jones, can't seem to diagnose the problem.

ISO: We'll send Susan Gonzales, one of our information security analysts, over to have a look right away. Can you have Bill meet her to review the problems?

MG: Well, actually, Bill is in Europe on a research project, but Mary, our departmental business manager, can unlock the door of the computer room.

A few hours later...

ISO: This is the Information Security Officer. May I speak with the Chair, please?

MG: Speaking. Thanks for getting back to me. Since we talked, I've had three more complaints. Have you been able to resolve the problem?

ISO: Well, Susan's work was hampered by not having access to the system logs and the administrator password that Bill could have provided, but she was able to make a preliminary diagnosis.

MG: Great! How soon before we're back to business as usual?

ISO: Well, that's hard to say. Based on observation of Mary's logging, Susan noted that the version of the operating system is two years old and so has not had several recent security patches installed. Susan also reported that servers running this version of the OS have been the target of attacks around the Internet recently, including several on campus. These attacks follow a common pattern, exploiting a well-known vulnerability in the "sendmail" program to gain root access.

MG: What exactly does "root access" mean?

ISO: You can think of root access as having complete control of the system, including all programs installed, all user accounts, and all user data.

MG: But what does this root access have to do with poor performance of the server?

ISO: Well, it could be several things: one or more rogue processes running, perhaps a password sniffer, an open FTP, or an IRC bot. Also, it appears there's nearly no disk space left on the system, which could indicate that one of these rogue programs is malfunctioning or perhaps uses substantial disk storage as part of its operation.

MG: How soon can Susan clean this up and get us back to work?

ISO: Too soon to tell. Partially it depends on whether we can reach Bill to get the root password.

MG: Can't you just call the computer vendor and ask them for emergency help?

ISO: Well, that's a bit awkward, since the version of the OS you're running is no longer supported by the vendor. Moreover, Mary advised us that your systems are not under a maintenance contract. I will ask Susan if she can stay late this evening to explore this further.

MG: Thanks. Please keep me informed. Here's my home number. I'll have Mary try to track down Bill.

Later that evening...

ISO: Good news and bad news: Good news is that we didn't need Bill to obtain root access. The root password was set to "gerontology," which Susan guessed after several tries. The bad news is that you do indeed have a root penetration on your hands, and the cracker installed a sniffer on your Ethernet interface. The reason you're out of disk space is that the sniffer's log file has gotten enormous because it's been running for about ten weeks.

MG: Well, I'm glad the password was easy to guess!

ISO: Frankly, if it was easy for Susan to guess, it may have been the way that root access was obtained by the cracker.

MG: I see what you mean. Now what exactly is a sniffer?

ISO: It's a program that monitors traffic on the Ethernet interface, looking for character strings that appear to correspond to login IDs and passwords. These combinations are logged, and, from time to time, the cracker harvests the data for future use. Apparently he or she got careless and forgot to delete the log file.

MG: Well, now that Susan has done her job so expertly, let's have her delete the log file, change the root password, and get everyone back to work. What a relief!

ISO: Unfortunately, it's not that easy. We can't be sure that the cracker didn't install a backdoor program to obtain root access, so we'll have to take the server off the network, reinstall the operating system and all the security patches to the OS, and reinstall the application programs and their security patches. Then, since all the user passwords are compromised, we'll have to have all users change their passwords, not only for this server, but all other systems they log into, here and at other universities.

MG: How long will this take?

ISO: Best guess would be three days for the server work. The password changes could be done in parallel.

MG: That's out of the question! We have students preparing for mid-terms and a major proposal due to NSF next week. We'll just have to put up with the slowness until these deadlines are past. Then we'll get people to change their passwords and get Bill to fix the server.

ISO: Sorry, we can't allow a compromised system to remain on the network. We'll have to disconnect you from the campus network this evening.

MG: You can't be serious! You say it's been compromised for ten weeks. What's the risk of its remaining on the network for another week or two, until the academic crunch is passed? There are no sensitive university data on that server anyway, only e-mail and some doctoral research.

ISO: The risks are actually quite high: Data on the server could be deleted or altered, e-mail could be sent in the name of any of your users, or the system could be used as a launching point for attacks on computers here or elsewhere.

MG: Launching point for attacks? That sounds pretty far-fetched.

ISO: Actually, computers at Stanford and UCSB were used last year to launch so-called "denial of service" attacks on several key commercial sites, such as eBay and Amazon.com.

MG: We can't function for a day without e-mail!

ISO: Well, that's comparatively easy: Our central e-mail server is preprogrammed to provide e-mail for all faculty, staff, and students. For some reason, however, your department has elected to run its own e-mail server. We can activate accounts for all your folks by 9:30 tomorrow morning.

MG: Thanks, but will they all have the proper address, of "firstname@molgero.bigu.edu"?

ISO: Sorry, you'll have to settle for "firstlast@bigu.edu," which is our standard format.

MG: But we've always been "molgero.bigu.edu." It's this sort of inflexibility that led us to run our own server in the first place.

ISO: Well, perhaps we can address this issue after we get your server back on the air. Now, what account should Susan's overtime be charged to?

MG: This is outrageous! You take us off the network and then charge us to help us get back on?

ISO: Well, perhaps we wouldn't be faced with such extreme measures if your department hadn't elected to run its own server without professional administration. Or if it hadn't ignored three messages from this office alerting you to the server security vulnerability. Or if it had attended our quarterly information security update meetings. We much prefer to engage proactively rather than in crisis mode. Now, what was that account number again?

MG: Mary will provide the account number in the morning, and I'll be calling the provost as well. With all the indirect cost recovery this department generates, I can't believe the central administration lets us be exposed to such risks!

Dan Updegrove (updegrove@mail.utexas.edu) is Vice President for Information Technology at the University of Texas at Austin.

The Computer and Network Security Task Force

In July 2000, EDUCAUSE created the Computer and Network Security Task Force, which works closely with Internet2 and federal agencies to ensure development of a thoughtful and measured response to the demand for better security. For information about how to join the task force or participate in its discussions, please visit <http://www.educause.edu/security/>.