Security Technology Training 101

A look inside a class that gives executives insight on hackers

By JACLYNE BADAL
May 14, 2007; Page R8

To stop a computer hacker, it might help to think like one.

With that in mind, more than a half-dozen information-technology executives gathered in San Diego last month to try out the techniques commonly used by attackers of corporate computer systems.

Run by the SANS Institute, a computer-security training and research group in Bethesda, Md., the $9,995 course consisted of six days of lectures and exercises designed to teach executives how to scan for a network's entry points, exploit systems, set up back doors for re-entry and remain undetected.

A familiarity with hacker techniques not only helps IT managers guard against potential attacks, it also allows them to speak the language of their security staffs, giving the bosses the ability to ask smarter questions and filter out fluff answers. As companies confront a growing number of security threats, it is the people who sign off on computer security, not their staffs, who often are held responsible if something goes wrong.

"In the real world, you get no 'E' for effort," says class instructor Eric Cole, a security consultant at Secure Anchor Consulting in Reston, Va. "You either get an 'A' or an 'F.'"

Reports of vulnerabilities -- weaknesses in computer systems or software that could be exploited -- are on the rise. The CERT Coordination Center, part of the federally funded Software Engineering Institute at Carnegie Mellon University in Pittsburgh, recorded 2,176 vulnerability reports in the first quarter of this year alone, compared with 2,437 in all of 2001.

IT's Navy Seals

Most of the nine participants in last month's maiden "Hacking for Managers" class at the SANS 2007 conference weren't willing to be identified. They wanted to remain anonymous to keep their companies' security tactics secret and refrain from tempting hackers.
Attendees are given laptops loaded with software designed to find and exploit vulnerabilities in computer systems, such as Core Impact from Core Security Technologies in Boston, and common hacker tools like Pwdump2, used to steal password codes, John the Ripper, used for code cracking, and Netcat, sometimes used to maintain access to a system through a virtual "back door."

The class starts with the grim reminder that even the savviest security teams are likely to encounter problems, or "incidents." Incident handlers are the Navy Seals of the IT world, and SANS advises managers to select handlers based on their ability to work as part of a team and stay calm under pressure.

Dr. Cole, the instructor, tells managers that incident-handling procedures should be up to date and in one place. Too often, checklists and procedures are scattered in multiple files or are too numerous to be useful. If a manager, or his staff, can't say for sure how well-prepared a company is to handle an incident, trouble could be brewing, he says.

**ABCs of Hacking**

After the introduction, Dr. Cole walks students through the five steps of hacking.

The first lesson is basic reconnaissance, the electronic equivalent of casing the joint before burglarizing it. He explains how hackers can use Internet search engines to gather publicly available company data, such as executive names and the style for email, and employ sites such as www.InterNIC.net to get information on domain names. It is child's play for many of the executives, who bemoan spending a morning using Google to mine information.

But step two, scanning, grabs their attention. Dr. Cole says many clients gripe that employees use company networks to set up wireless Internet-access points without permission. Bad idea, he says, because hackers can exploit these connections to gain entry to company computers. To stop misguided employees, Dr. Cole teaches executives how to use a program called NetStumbler to help detect wireless local area networks. The tool, similar to the wireless scanners built into many laptops, detects signals being emitted at the wireless access points.

Experimenting with the program, Dwane Knott, a security officer for Newlink Global Engineering Corp., a government contractor in Alexandria, Va., finds more than 35 wireless access points in the vicinity of the classroom. "This is really cool," Mr. Knott says, as he walks outside to see how many more he can find.

Part two of the scanning lesson focuses on limiting the information people can get from the Internet. When hackers are scanning, they are looking for open ports -
"firewalking," a tactic in which a hacker uses a firewall's error messages -- often sent back to users -- to determine what type of traffic gets through.

Dr. Cole recommends configuring a firewall to basically be silent. "No matter what it does, [a firewall] should give no feedback," he says. And if a company is using an intrusion-detection system, or IDS, to detect malicious traffic a firewall might miss, the IDS should know what type of traffic the firewall wants to block. Dr. Cole urges the executives to ask their staffs if the IDS has the same rules as the firewall.

**Attacks Made 'Easy'**

In step three, the executives learn how hackers can exploit a computer system once they know the machine's Internet address. For this exercise, the executives try the Core Impact software, which allows a user to steal information from a target computer with a few clicks of the mouse.

The managers watch as Dr. Cole hacks into a nearby computer. He captures a snapshot of the target computer's screen by selecting that command from a list of options and using his mouse to drag the command onto an image of the victimized computer, much like someone would move a Microsoft Word document from a computer desktop to its Recycle Bin.

The students practice the same moves on their own computers. Craig Johnson, a principal at consulting firm Netxygen Corp. in Anaheim, Calif., and an IT manager at a Southern California technology company, calls the tool the most alarming part of the series. "It really upset me," says Mr. Johnson, one of two executives willing to be identified.

IT managers can use a program like Core Impact to monitor their security staffs, Dr. Cole says. A manager could run the program and ask staffers a few days later if they had seen anything suspicious. A negative answer would serve as a warning that staffers either aren't watching the event logs that track network activity or are watching the wrong ones, he says.

Dr. Cole warns managers, however, that they should get written company approval before using something like Core Impact, because certain uses of the program may break the law. "Just because it's easy doesn't mean it's legal," he says.

Students move on to stealing password hashes, or codes, with Pwdump2 and cracking codes with John the Ripper. A password based on a common dictionary word can be cracked in seconds and is a security sin akin to using the same password for everything.

**Watching the Back Door**

After working with the hacker tools, the executives are introduced to step four: maintaining access. They learn their way around Netcat, a tool sometimes used by hackers to establish a back-door connection to a
computer system. They receive a lecture on ways that hackers sneak information out without anyone knowing. A sophisticated firewall may do an excellent job of preventing bad traffic from getting in, but it may pay little attention to traffic going out. Knowing this, a hacker may set up access so the victimized computer is contacting the hacker.

"What concerns me in my professional practice is all the stuff that's going outbound that we're not paying attention to," says Jonathan Ham, a security consultant in Missoula, Mont., who provided computer support to the attendees and added to Dr. Cole's lectures.

Dr. Cole urges the managers to periodically ask staff about incoming and outgoing traffic. They should have an idea of what is normal, so they can spot abnormalities. If they don't have ready answers, a closer look at monitoring practices may be warranted, he says.

The fifth and final hacking lesson addresses "covering your tracks." The best advice for catching someone who has taken control of a system and is operating under cover is to pay attention to the little things, the instructors say. At this stage, hackers aren't making obvious mistakes and are mainly caught when a staffer follows up on activities that are slightly out of the ordinary.

Mr. Ham's favorite example involves a system administrator who looks for open ports, where information passes into and out of a network. A good hacker can manipulate the system, so that an administrator doing an internal search wouldn't see all of the open ports. But the ruse has limits. If the employee examined the network from the Internet, using a program called a port scanner, he would discover the deception.

The class ends with a day of practice. Students play a virtual game of capture the flag that takes them through the steps of hacking and allows them to use the items in their hacker toolkit.

Netxygen's Mr. Johnson says that on the day he returned to the office, he put the hacking lessons to use. Impressed by how easy it was to crack codes, he established policies requiring passwords to contain numbers and be a certain length. He is in the process of dividing the company's network into parts, so that if a hacker does succeed in breaking in, he won't have unlimited access.

And, of course, he wowed his staffers. Mr. Johnson told employees to pick any computer in the office, and he was able to hack into it within moments. "The demonstration was a slap in the face to them," Mr. Johnson says. "I can guarantee you everyone is more security conscious."

--Ms. Badal is a staff reporter of The Wall Street Journal in South Brunswick, N.J.

Write to Jaclyne Badal at jaclyne.badal@wsj.com

URL for this article:
http://online.wsj.com/article/SB117873747421897504.html

Hyperlinks in this Article:
(1) http://online.wsj.com/page/2_1300.html
(2) http://online.wsj.com/article/SB117873739494197490.html
(3) http://online.wsj.com/article/SB117873749878997506.html
(4) http://online.wsj.com/page/2_1300.html
(5) http://www.InterNIC.net
(6) mailto:jaclyne.badal@wsj.com