The Knowledge Bank™
only from S.R. Snodgrass
"Your Key to a Wealth of Information"
SNODGRASS
Certified Public Accountants and Consultants
www.srsnodgrass.com

As seen in the
June 2008 Issue of
Community Banker

MISSION IMPOSSIBLE?

BY JEREMY BURRIS, CISA, MCP, LPT, CPTS, CEH, ECSA

Consider if your financial institution's information systems are as secure as you think.

"Your mission—should you choose to accept it—is to breach an impenetrable security barrier." It wasn't Tom Cruise foiling a nuclear terrorist, but a recent demonstration of the vulnerability of even the most seemingly secure data. The mission was assigned by a bank that felt its security was impenetrable, but wanted to test it. Good thing. Like Tom Cruise, our Penetration Tester got inside without breaking a sweat.

The Mission

This institution felt it had superior physical security and a great security-awareness training program to educate employees about the dangers of a "hackers." Additionally, policies and procedures noted that only three employees had access to the disaster recovery servers located within the basement of one of the remote branches. The mission posed to the Penetration Tester by the client was to enter the disaster recovery room where the servers were located and "steal" data from those servers.

The Penetration Tester began his mission at a local hotel, where he attempted to breach the servers by connecting to one of the bank's external IP addresses, which handles email. The bank correctly felt confident that their e-mail system was set up not to allow e-mail relaying (spoofing). However, some hotel networks route traffic differently and create their own relays of e-mails.

Using the hotel's system, the Penetration Tester sent a spoofed e-mail—supposedly from the vice president of information technology at this bank—to the branch manager of the remote location that housed the disaster recovery room. The e-mail informed the branch manager that an auditor was helping him do some work on the disaster recovery servers in the basement and should be allowed access to that room.

The Penetration Tester then proceeded to the remote branch. After verifying that the branch manager had received the e-mail from the vice president of information technology, the tester explained that he needed access to the secure room for 30 minutes and that his work on the servers would not disrupt the business. The branch manager asked to verify identification. Although his business card and driver's license were real, they could easily have been fakes.

The tester was asked to sign the log, which he did willingly with such sloppy handwriting that it was barely legible. He was then escorted to the room where the disaster recovery servers were located. Once inside the room, the tester told the branch manager that he would come find him when the work was done. The branch manager then left the tester alone in this room and closed the door behind him. Part one of the mission was a success. The tester was now inside a room that policies and procedures noted only three staff members were allowed to access.

The next part of the mission was to "steal" the data. The tester observed that all servers were located in a rack

This newsletter is intended to provide timely, accurate, and authoritative information on the subject matter herein. Due to the general nature of this newsletter, the information contained herein should not be acted upon without professional advice related to your specific situation.

mount with the front of the cabinets secure, and they were approximately three feet away from the wall where the communications equipment resided. The tester could not locate a hidden key to the cabinet, but he noticed that the backs of the cabinets were left completely open, allowing access from the rear of the cabinets to all of the servers.

The Penetration Tester then identified one of the active directory servers within the cabinet and placed a bootable Linux distribution CD into the CD drive of this server. Then, he rebooted into a Linux environment. While the server was rebooting, the tester placed a USB thumb drive into the back of the server. Upon booting into Linux successfully, the penetration tester entered five commands and saved the entire SAM database (housing every active directory password on the network) to his thumb drive. The CD and thumb drive were then ejected, and the server was rebooted back into Windows.

The Penetration Tester now had what he needed and thanked the branch manager for his time. He then went back to an office location and used a password-cracking tool on the stolen SAM file (and syskey file) to crack passwords on the domain. He obtained an administrative password on the network in less than one minute (despite password settings on the network being within current industry standards) and used that log-in account and password to create his own administrative account. The Penetration Tester would now have been able to log on to any of the active directory servers and "steal" any of the data residing on it. Part two of the test was successful.

The entire process (including travel time) took less than one hour, and the on-site portion at the disaster recovery site took less than ten minutes, once he was inside the room. Rather than stealing data, the Penetration Tester described controls to management that could be put in place to prevent a breach in the future.

Lessons Learned

Our mission, and many similar missions we have conducted, demonstrates the two biggest security risks that account for some 75 percent of information leaks: inadequate physical security and lack of security awareness among personnel.

1. **Physical security:** Even if servers are located in a room behind a keypad lock, make sure they are further secured. As demonstrated, a securable locking cabinet to house servers isn't enough. The cabinet itself must be fully secured (even in the back).

2. **Personnel:** Employees should be taught not to trust e-mails when they deal with sensitive information or access to sensitive areas. All e-mails should be followed up with a phone call to senders to verify their identity and the content of the e-mail. Employees should be trained to escort all vendors to secured areas of the bank and not to leave them unattended, no matter how trusted the vendor.

Information security is essential to financial institutions for both compliance and reputation reasons. If a hacker were to breach your network and steal non-public customer information to the extent that the bank must report it to local authorities, the news media would quickly jump on the story. Breaches of security are a black mark on an institution's reputation. Regulators and customers would naturally feel uneasy about the safety of their money and information.

About the Author

Jeremy Burris is a Senior Technology Services Consultant at S.R. Snodgrass, A.C. Jeremy's areas of expertise include Network Attack and Penetration and other IT security-related audits for financial institutions and private companies. Snodgrass is best known for our expertise in the financial services industry, where we currently serve over 175 financial institutions on a national scale. Accordingly, we have extensive industry business experience and sound working relationships with all of the regulatory agencies. Examples of that experience are displayed on our Web site's *Knowledge Bank* at www.srsnodgrass.com, where you can view several articles and video presentations on banking-related topics, including a live Attack and Penetration demo.

This newsletter is intended to provide timely, accurate, and authoritative information on the subject matter herein. Due to the general nature of this newsletter, the information contained herein should not be acted upon without professional advice related to your specific situation.