

Special points of interest:

- How Secure Is Your Network?
- Free Internet Security Test
- Upcoming Events

How Secure Is Your Network?

**By Chris Schroeder
Manager, Technical Audits
Canaudit, Inc.**

How secure is your network? This is a question I ask people when they attend one of my classes. I usually get one of two answers: 1) We are secure; or 2) We know we are not secure and have decided that we cannot afford security. Now decide which category you fit into. Odds are you fit into one of them.

For starters, Canaudit has performed many penetration tests over the years. We have never once failed to “own” the network. This includes those clients that believed they were secure. The fact is, there is no such thing as a secure network — just well managed ones. A well-managed network can limit the damage that can be done by an intruder by segmenting the network, having hard-to-guess passwords on all accounts, and all system security patches up-to-date. Unfortunately,

(Continued on page 2)

Free Internet Audit

Pay full price for any of Canaudit’s 5-day classes taking place in January or March and get a free internet audit.

The Internet Attack includes an initial “blind” penetration attempt from the Internet conducted by the Canaudit Remote Penetration Team. We will identify the Internet connections that can be found from public sources without specific knowledge. We will then launch an Internet attack. The tools used include, but are not limited to, Port scanners, Telnet, FTP, Sam Spade, Nessus, CIS, custom written scripts, or other proprietary tools.

The Internet Audit:

- Exploit weaknesses using safe techniques to harvest files.
- Test the web server to ensure a hacker does not have the ability to modify the web site using known techniques from the Internet.
- Test the firewall. We will not perform denial of service or distributed denial of service attacks.
- Provide the client with a list of machines that were audited.
- Prepare an audit report segment describing the exploits that succeeded in penetrating the client’s network; samples of data harvested.
- We will prepare a report identifying the issues arising from the penetration audit along with suggested actions to mitigate the risks.

Turn to page 5 for more information on qualifying classes, visit our website, canaudit.com, or contact Kristie Tryk in our Marketing Department at (805) 583-3723 or via e-mail at kristie@canaudit.com.

I have never seen a network that had all three of these basic housekeeping issues in place.

Most articles about network security go into detail about this operating system or that application, but they never address the basics. How much does it cost to ensure all accounts on the network have hard-to-guess passwords? Most people believe security equates to dollars, yet in reality, if basic security principles are put into place most networks would be much more secure at little or no cost.

Before we get into some of the basic security principles, we need to discuss how intruders get into your network. There are four primary avenues of approach: Internet, physical access, modems and wireless LANs.

Access from the Internet

Management has become wise lately and has put resources toward securing the network from attacks originating from the Internet. It is not as easy to break into a network from the Internet today as it was two years ago, yet we still find those organizations that have not gotten with the program. Typically, the most common mistakes organizations make are having misconfigured firewalls in production. Such misconfigured firewalls allow many services to be accessible from the Internet, such as NetBIOS, Telnet and SNMP (Simple Network Management Protocol).

Virtual Private Networks (VPNs) are becoming very popular nowadays, yet many organizations are not properly securing them. Organizations are using default installations and values, and only require UserIDs and Passwords to log onto the network. Secondary authentication, such as secure tokens, should certainly be considered for use with VPNs. Is your UserID on the network the same as your email address? If so, then all we need to do is guess your password.

“Typically, the most common mistakes organizations make are having misconfigured firewalls in production.”

How secure are your organization's Internet facing routers and switches? Can we attempt to log onto them from the Internet and reconfigure them? Do these devices have Simple Network Management Protocol (SNMP) enabled? Do you know? The hackers do.

Modem Access

Of all of the companies Canaudit has audited in the past, we were unsuccessful in gaining access via modems only three times. This should be a warning to you. Organizations are still using modems in an insecure way and will continue to until either an incident or proper testing and securing occur. The majority of the modems we penetrate are using default UserID's and passwords. When was the last time your organization used a product like PhoneSweep to scan for modems? It is important to perform a war-dial on a regular basis to identify the modems on your network. It is especially important to find the modems you do not know you have. If at all possible, place all modems in a modem pool behind a firewall that requires the users to authenticate before gaining access onto the network. Again we are discussing secondary authentication techniques as we did with VPNs

Wireless

The latest wave in technology is Wireless LAN's (WLANs). Many organizations have been implementing WLANs without regard to the security risk they pose to the network. During my travels around the world, I have been conducting a study to see how many WLANs I could find — and how many of those are using encryption. I have found that 73% of the Wireless Networks are not using standard wireless encryption to help secure their networks.

If your organization has a WLAN, and you are not taking extra security precautions, then unauthorized access to the internal network is immanent. Your organization might as well get rid of your firewalls and security systems, because an improperly secured WLAN can bypass these measures.

Physical Access

The majority of attacks on the Internal network occur from within the network, either from disgruntled employees, contractors, or people that just walk in off the street. I always hear people saying that the internal network is a trusted environment, but does this mean we need to give away the whole farm? Do you really believe the internal network is a trusted environment? In 2001, 65% of the successful attacks originated from within the internal network.

On a scale of 1 –10, how would you rate your organizations network security? Does the possibility exist that someone could walk into your company under false pretences and start hacking away? Could this person place a wireless access point behind a network printer? Does your organization have any remote offices that are not as secure as the corporate headquarters? If you answered yes to any on these questions, then your organizations network is at risk of an outsider gaining access to the internal network. Of course not all attacks are from people you don't know, some attacks are from trusted employees or contractors.

Why do so many organizations believe they are secure? For one thing, they are told by the system administrators they are. But how do the administrators know? Many of you may be thinking, well it obvious, the administrators administrate the system, thus would know whether or not it is secure. But think about this, an administrator's job is to keep the system up and giving access, meanwhile IS security's job is to keep people out and limiting access. How can the person who is giving access be expected to limit access? The answer is simple, they can't. Yet many organizations expect the administrators to do just that, and unfortunately it is not working. The proper way to ensure that security is in place at your corporation is to have a separate security team whose job is to research new vulnerabilities and to test the network for those vulnerabilities.

Basic Security Principles

Many people think that in order to break into networks hackers use black magic and have a special "mojo" that gives them this ability. In reality, most attacks are easily accomplished by using simple, free, widely available tools.

In the majority of the penetration audits I perform, I use only basic network tools such as: Port Scanners, Sniffers, Netbios Tools, Password Crackers and tools that comes with window, such as: FTP, Telnet, Finger, TFTP, Ping & Trace route.

It is not very often that I need to use more sophisticated techniques like a man-in-the-middle attack, or buffer and integer over-flows. Commonly, systems are easily penetrated because basic security principles (housekeeping) are not in place.

If your organization implements basic security principles, then the network would be headed in the right direction and would force me to earn my money when I perform a penetration audit on your organization's network.

Companies often rely on a security packages for creating a secure network environment. Unfortunately, this is not the case. You cannot purchase basic security (housekeeping) from a vendor; security comes from your own people. Most of the recommendations I give our clients after an audit do not require the spending of a lot of money, although it may require time. Use the resources you already have. In fact, you may be surprised to find out how much security related knowledge your organization already has in house.

The following is a list of what I consider as basic security principles:

1. Using hard-to-guess, non-dictionary passwords on every account on every system;
2. All applicable security patches are tested and implemented.
3. Ensuring default passwords are changed.
4. Segmenting the network.
5. Enforcing the corporate password policy.
6. Turning off unneeded services. (finger, exec, login, shell, echo, Chargen and telnet.)
7. Using SSH instead of Telnet.

(Continued on page 4)

A consistent complaint I hear is that, while auditors and system administrators address network security related issues with management, their issue fall on deaf ears. Until, that is, an outside firm conducts their tests and identifies many of the same issues. These auditors and system administrators then may ask themselves, why should we waste their time addressing these issues if no one is going to listen to them? As you can see, this can cause degradation of security and issue reporting by the very people who know about the security related problems.

“Using basic and widely available tools, hackers can own most networks.”

A way of gaining loyalty is to train audit and system administrator staff. Send them to classes that help them to perform their job better, with security in mind. Many organizations are cutting back on their training budget. I feel this is a mistake. A well-trained employee is an asset for any company, and regular classes will ensure they are kept up-to-date with rapidly changing technology. While teaching Canaudit's The Ultimate Network Penetration Course, a 5-day hands-on class that teaches the techniques we use to perform our penetration audits, I have found many of the students that have been to this class have found that they have a renewed interest in their job and go back to work rejuvenated ready to fight off the hackers!

Back to my original question: How secure is your network? Using basic and widely available tools, hackers can own most networks. So, how much would it cost to make it secure? You do not need to run right out and purchase the latest, greatest and most expensive, security package. The most cost effective security is simply to implement good house-keeping measures and to keep security staff well trained.

Chris Schroeder
Manager, Technical Audits and Security Services
Canaudit, Inc.

2003 Canaudit, Inc.

If you found this article interesting, please forward it to your colleagues or professional associates. As always, I look forward to receiving your comments. Please e-mail me at chris@canaudit.com.

Chris, a former U.S. Marine, has unique insight when performing security audits. He has performed many forensic audits and has been studying the legalities of the new Patriot Act. Along with Canaudit President, Gordon Smith, Chris has written a physical security guide available at the Canaudit website www.Canaudit.com.

Canaudit, Inc.

P.O. Box 2110
Simi Valley, CA 93062

Phone: (805) 583-3723
Fax: (805) 582-2676

Audits:
Email: gordon@canaudit.com
Email: chris@canaudit.com

Seminars:
Email: kristie@canaudit.com



UPCOMING EVENTS

Professional Development Seminars

Build your technical audit skills and keep up-to-date by attending any of our upcoming 2-day professional development workshops. Our instructors excel in explaining new techniques in terms participants can easily understand.

At Canaudit, we believe in the control self-assessment process. Therefore, most of our auditing courses contain a complete set of COSO-compliant checklists.

Professional Development Week

****Register by March 3rd and Save up to \$100****

Washington, DC area:

- **Control & Security of Oracle** - April 14-15
- **Control & Security of UNIX** - April 14-15
- **I.S. Auditing: The First Step** - April 14-15
- **Understanding & Preventing Electronic Fraud** - April 16-17
- **Control & Security of PeopleSoft** - April 16-17

The Ultimate Network Penetration Class—\$2,495

This five-day, "Hands-on" class is designed for those security officers, IT auditors and administrators who want to learn how to penetration test their organization's network. This class, taught by two members of the Canaudit "Strike Force", will teach you how to attack your network from the Internet, Intranet and dial-up modems.

- Los Angeles, CA area - January 27-31 (Last chance to register.)*
- Los Angeles, CA area - June 2-6 (Register by **April 25th** and save \$200.)

The IT Audit & Security Boot Camp—\$2,295

This five-day, "hands-on" technical audit course is designed for new IT Auditors, financial or integrated auditors making the transition to IT auditing, and existing IT auditors who need to refresh their skills. This intensive session combines over ten days of training and fourteen hundred pages of material into a one-week technical audit and security boot camp.

- Los Angeles, CA area - January 27-31 (Last chance to register.)*
- Chicago, IL area - March 3-7 (Register by **January 24th** and save \$200.)*

* Registrants in these classes who pay full price will receive a Free Internet Audit. See page 1 for more details or contact Kristie Tryk either at (805) 583-3723 or via email, kristie@canaudit.com.