

The Canaudit Perspective

Volume 4, Issue 4
April 2003

Special points of interest:

- How Do You Know You've Been Hacked?
- [The Canaudit Internet Security Program](#)
- [Upcoming Events](#)
- [Canaudit Perspective Special](#)

How Do You Know You've Been Hacked?

By Chris Schroeder
Senior Manager Technical Audit & Security Services
Canaudit, Inc.

Occasionally you read in the papers or on security web sites about a site that has been hacked, have you ever wondered how they knew? How would you know if your network got hacked? Try going to www.zone-h.com and look at how many sites have been hacked for the current day, or better yet, do a search to see if your site is listed in their database. I know of only four ways you would know that you got hacked:

IDS

While everyone knows installing an intrusion detection system on your network is a necessity, not everyone realizes that simple installation is not enough. The problem is not necessarily with the products, but rather in the implementation itself. Many people falsely believe once an IDS is installed, they will automatically know when their network is under attack.

In order to get the full benefit of any IDS, you must commit the personnel necessary to properly monitor your system and respond to any incidents reported. These staff members must also be properly trained to understand the difference between the false positives most systems provide and an actual alert. Many people decide to "tweak" their intrusion detection system to reduce the numerous false positives received rather than receive and investigate every alert. Unfortunately, this "tweaking" of the IDS often

eliminates so many alerts an intruder can attack your network without ever setting off an alarm. Additionally, many attacks will not be detected by some forms of IDS.

Many organizations have IDS but are not using it as effectively as possible. Network sensors are often placed in high traffic areas in order to capture the most data. Unfortunately, IDS does not look at every packet on the network. While your system is busy looking at a packet to determine if it is an attack, several others may go by unchecked. The more traffic on that portion of the network, the less accurate the results.

One of the most important steps in properly implementing any intrusion detection system is having an intrusion response procedure. If your security team identifies an attacker on your network, they must know the proper course of action and react in an organized manner. These procedures should outline exactly which actions to perform and whom to notify.

Log Files

By reviewing IDS log files it can be easy to spot the telltale signs of an unwelcome intruder. Unfortunately, at many of the organizations I have audited, log files do not get reviewed often enough, if at all. In fact, I find quite often log files do not get reviewed unless the company is being attacked. The fact is, log files are only evidence an intruder has already been on your system and by the time you review the logs, it's already too late.

Another problem with just reviewing log files is many people only log activities on the servers and do not have logging enabled on the workstations. When I perform a penetration audit, I usually attack the workstations first. On almost every audit, I have found workstation security is not a priority, and if present at all, can easily be breached. Once I have gained access to the local workstations, I can easily use that access to discover which accounts exist on the network, steal the password files and crack them. I can then authenticate to the servers using these cracked passwords without a single failed logon attempt. Using this scenario you wouldn't see any unusual activity without having logging enabled at the workstation level.

Luck

Every once in a while, we all get lucky. At times this means you may notice an intruder during an attack or realize an account on your system doesn't belong. Either way, many people have been caught because someone got lucky and saw something they were not looking for.

I let you know

Now consider this, if you don't have IDS, you don't review your log files on a regular basis and you're not that lucky, then the only way you will know you got hacked, is if I

tell you. There are several ways I could let you know. I could crash your system, which you may take notice of, or I could delete your customer database, or I just call you up on the phone and say "I just took a copy of your customer database, which has your customers Social Security Numbers and I want \$50,000 or I will post it on the Internet". Many people would say that this is a pretty easy way to get caught, and that is what I originally thought, but I have seen corporations pay these people the money. Paying this ransom is cheaper than the public relations nightmare that could result in the attacker posting the information.

So what does all of this mean? Well, if you don't have IDS, I don't let you know I was there, you're not that lucky and you don't review your logs, then I guess you will never know that you were hacked. It is important that everyone in your organization contribute to network security, from the cleaning crew all the way up to the CEO.

2003 Canaudit, Inc.

As always, the comments and opinions in this article are mine and mine only. I invite you to email me your remarks and promise to respond personally to all of them. 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 on the Canaudit website, www.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 or 5-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

******Last Chance to Register. Class starts in less than 2 weeks******

Washington, DC area:

Control & Security of Oracle - April 14-15, 2003

Control & Security of UNIX - April 14-15, 2003

I.S. Auditing: The First Step - April 14-15, 2003

Control & Security of PeopleSoft - April 16-17, 2003

The Ultimate Network Penetration Class **

****Look below for information on how you can attend this class for \$995 less than our regular rate.**

******Last Chance to Register by the Early Registration Deadline and Save up to \$200******

- Los Angeles, CA area – June 2-6, 2003 (Early Registration Deadline – **April 25, 2003**)

IT Audit & Security Boot Camp

- Washington, DC area – July 21-25, 2003 (Early Registration Deadline – **June 13, 2003**)

Professional Development Week

Los Angeles, CA area: (Early Registration Deadline – **July 3, 2003)**

Control & Security of Electronic Fraud – August 11-12, 2003

Control & Security of Telecommunication Networks - August 11-12, 2003

Control & Security of Web Applications - August 11-12, 2003

Cyber Terrorism & Electronic Espionage - August 13-14, 2003

Computer Forensics for Security & Audit Professionals - August 13-14, 2003

Control & Security of Wireless Networks - August 13-14, 2003

For more information, a course outline or to register, please visit our website, www.canaudit.com or call (805) 583-3723.

Canaudit Perspective Special

Canaudit is offering a special rate of **\$1,500** to the next 10 people who register to attend our June Ultimate Network Penetration Class. Registration and payment must be received by April 25th. (Registration Code #CPS042503)

The Canaudit Internet Security Program

By Gloriana Hunter
Marketing Analyst, Audit & Security Services
Canaudit, Inc.

Recent headline news has reminded us that the risk of hackers taking over your Internet remains a real threat. Security conscience auditors and IT/IS professionals know that the best offense is a good defense. This is why we are introducing the Canaudit Internet Security Program.

If you are planning an Internet security review this year, Canaudit would like to have the opportunity to respond to your Request for Proposal. With over 18 years experience in security and IT auditing, our reviews are more detailed than most regulatory standards require. We will test your Internet using safe and sane tools, many of which are similar to the tools that hackers use. Each report is custom written for you, and provides a prioritized and systematic technical plan of how you can cost-effectively manage vulnerabilities. In addition, Canaudit provides ongoing free email and telephone consultation to assist you in implementing the changes listed in the report.

The Canaudit Internet Security Program focuses on control and security of your organization's Internet, internal and extranet connections. Our process is ideal for periodic testing to identify technical security flaws that hackers often compromise. The program starts in the remote Canaudit Lab and includes an initial "blind" penetration attempt from the Internet by the Canaudit Penetration Team. Additionally, Canaudit can visit your organization's network to perform an on-site portion of the audit. During this phase, we will audit and review configuration and implementation of all Extranet and Internet connections and devices. We will also perform a limited review of the client's wireless connections (if present) to determine if the Internet connection is exposed to unauthorized wireless access and usage.

Canaudit has proudly performed Internet Security Reviews for Fortune 1000, international and mid-market firms in a wide array of industries, including banking, distribution, federal, state and local government, financial services, health care, insurance, logistics, manufacturing, nonprofit, telecommunications, transportation, utilities, and more.

For more information on the Canaudit Internet Security Program, please contact Gordon Smith (Gordon@canaudit.com) or Chris Schroeder (chris@canaudit.com) at (805) 583-3723.

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