

The Canaudit Perspective

Volume 4, Issue 2
February 2003

Special points of interest:

- Preparing the Corporation for War and Retaliation
- Canaudit's "The Value of Membership Program"
- Upcoming Events

Preparing the Corporation for War and Retaliation

By Gordon Smith
President
Canaudit, Inc.

As many of you know, I like to use the Canaudit Perspective to provide my take on current audit and security issues. In this issue, I am very concerned that our clients are not prepared for the upcoming war with Iraq, the continuing war against terrorism, and actions by sympathizers. It does not matter whether you are for the war or against it. Your organization may be a target in either case. Therefore, in this issue, I am going to discuss several security risks facing many organizations and then offer a blueprint for quickly shoring up your security prior to the outbreak of hostilities.

I have been warning of the threat of cyber terrorism for 4 years now. Whether you agree with my opinions on cyber terrorism or not, this is not the time for debate. It is now time to ensure our networks and facilities are secure and that our employees are protected. In my November article, [Business Recovery Following Major Disruptions](#), I described some groundbreaking techniques for disaster preparation, mitigation and recovery. In last month's issue, Chris Schroeder wrote an article entitled [How Secure is your Network?](#) Both of these articles provided information about preparing for normal security threats. Hopefully, the articles were passed to senior management and remediation measures are in the process of being implemented. If not, I suggest you download them now and distribute them to those who need to understand the risk and authorize the required changes.

In this issue, I want to point out a simple yet effective method to breach the network, penetrate web mail and obtain an unauthorized access card to a secure facility. Then I will present an audit or security review plan to do a whirlwind, yet thorough security review or audit to identify the most critical IT risks so they can be resolved within several weeks. I will also provide you with a link to our network audit checklist at the end of the article. You can use this to do a quick network review to identify the risks.

The first item, web mail penetration and the ability to breach VPN security was identified at several client sites recently. Many security analysts and auditors are aware that there is a port 80 "feature" that can enable a hacker to download the configuration file of some Cisco devices. We have used this successfully on multiple clients over the last few months. This "feature" is quite simple to execute. First, run Solar Winds or another scanner to identify Cisco devices with port 80 open, then bring up your web browser and enter the following URL: http://ENTER_IP_ADDRESS_HERE/level/16/exec/show/config. Simply insert the IP address of the intended target where indicated. Hit enter and, if the "feature" is activated, a copy of the configuration will be downloaded to your browser.

Look for the passwords and the password types. If the device is poorly secured, the enable secret function will not be implemented and you can use an excel macro to decrypt the required passwords. If the device is better secured, the MD5 encryption will be in place. It may take several days or even a few weeks to crack the password. Since these passwords are rarely changed, the time to crack

the password may not be a factor. Whether it takes an hour or a month, the result is the same, you gain administrative access to the device.

Now, onto the next step. Several of our clients were using Cisco devices as part of a VPN implementation. This is an excellent solution, provided you follow the instructions and advice of Cisco. For whatever reason, some of our clients created other accounts on the devices that bypassed the VPN security (access tokens, certificates, etc.) so that the network administrators could login directly from the Internet. We can only assume that they wanted this access in case the VPN or security mechanisms failed and they needed to get into the network from the internet. Whatever the reason, when these accounts exist, and if the port 80 "feature" is active, it is a simple matter for a hacker to grab the accounts and passwords then crack them to gain access to the internal network.

Here is an example which has been altered to protect confidential information:

```
version 12.1
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service linenumber
!
hostname XXXXXXXX
!
boot system flash XXXXXX-9.E.bin
no logging console
aaa new-model
aaa authentication login default local
aaa authorization exec default local
enable secret 5 $1$FED1$IKGRGLhVgHXe/iK0
!
username letmein privilege 15 password 7 ****Encrypted value was here
username IMAHACKER privilege 15 password 7 ****encrypted value was here
*****Edited to end of config listing*****
```

In the above example we were able to crack the passwords instantly, using an excel macro available at the downloads section of our website at <http://www.canaudit.com/Downloads/downloads.htm>.

Notice that the account name and encrypted password are clearly visible. To make matters worse, in one case, the administrator's Cisco account and password was the same as his domain administrator's account and password. Once we had the Cisco device, we also owned the primary domain controller. We then breached the network and harvested all of the user passwords and cracked them. This not only gave us access to their files within the network, but it gave us access to their email.

In another case, our mandate was to perform a penetration study including social engineering at several of the client's locations. In our penetration audit, we lifted the encrypted passwords from the Primary Domain controller and cracked them. This proved very useful as the client provided internet web mail to their staff who authenticate to the mail server via the Internet using these accounts and passwords. With the password files in hand, we were able to view employee email from the Internet, create emails from their accounts and send them without having to resort to "spoofing".

We used the account of a senior executive to send an email to the facilities coordinator. In the email we requested that two people be given access cards for all areas of the facility as they were conducting a special study. We sent the email from the executive's account, copying in a project leader. Then we removed the email from the executive's and the project leader's mail folders (including the sent folder and the deleted items folders). When the facilities coordinator replied to the executive, we were watching for the reply and deleted it before the executive could read it.

We phoned the facilities administrator a few moments before we arrived at the facility to ensure that our cards were ready. When we arrived, the facilities administrator gave us the cards. We had free and complete access to the facility, in spite of several layers of controls. While some might say we just

got lucky, this is not the first time we compromised security cards, nor will it be the last. Managers and staff often get complacent due to the controls they have installed, assuming these controls work. Al Queda, Saddam or just your local laptop thief or electronic espionage agent could use these techniques to defeat your security. They could place wireless cameras, bug phones and meeting rooms, or insert a wireless access point so the cyber terrorists can access the data from a van in the parking lot.

Let's recap here quickly. These types of security events are often caused by network administrators who feel they do not need to use the same VPN controls as normal users. Maybe they are concerned about access when the VPN is down; maybe they are worried that they could lose their access token or digital certificate. Whatever the reason, cyber terrorists are ready, willing and able to exploit the administrator's back door.

Since the port 80 feature is so easy to use, it is the first item on a hacker or cyber terrorists work plan. Therefore check all of your Cisco devices for the port 80 feature. At a minimum, turn it off from the Internet side of your network. Preferably turning off this feature or securing it throughout the network. Next, make sure that all emailed, faxed or even paper requests for access cards or devices are authenticated by means other than email. This includes calling or visiting the authorizing authority. Faxes or secure, encrypted email with public / private keys may also be an alternative. Then, you must test the control on a regular surprise basis. The frequency of the test depends on the specific threat risk for your organization; however it should be performed at least quarterly.

IDENTIFY YOUR RISKS / IMPLEMENT CONTROLS

Let's move on to the next topic. Several of our clients have asked us to prepare a security / review audit plan for the current global situation. As always, I believe that the network is the first line of defense. For many of our clients, network security is more important than physical security because they have a large network that spans the globe and makes extensive use of the Internet to link with trading partners, customers and agents. Once the network is breached, physical security may also be breached as in the example I previously mentioned.

The network audit should include several components. The first is an external and internal penetration audit or vulnerability assessment. If you are using a consultant for this audit, the audit should not be performed solely from a consultant's lab, but should include an onsite visit by the consultant to check the internal network, wireless links and to transfer skills to your staff. The external internet security test and the modem test can be conducted from the consultant's lab. Detection of wireless network connections, video or audio surveillance and wire taps should also be conducted during the onsite visitation depending on the nature of the business you are in and the severity of the risk.

This penetration / vulnerability assessment will identify the total risk to your organization from a network standpoint and also from a server and device security perspective. If the network is breached, then servers and devices can be attacked. Network security weaknesses and server security issues can be identified, prioritized and then rectified. Many of the items uncovered by this review will be easy to correct. Some can be corrected in a matter of minutes, others will take several months. Additional funding and staffing may be necessary to implement the proper level of security for your organization.

Once the penetration study or vulnerability assessment is complete, the network audit is next on my list. For best results, couple this with a physical security review. The network audit looks at business continuance from a carrier, internal and trading partner standpoint. There is also a contract review to ensure the right to audit, the terms and conditions are reasonable, and protection of your network and data is included along with remedies should the contract be breached.

The physical security component ensures that the facilities, network rooms, closets, and data center are properly protected. This component can include attempts to defeat physical security and social engineering to test the human component of your security structure. Once this is complete we move onto network device and circuit review, followed by server and trading partner security.

To make it easier for you to perform this review, I am making our Network Audit and Security checklists available on the Canaudit web site. (<http://www.canaudit.com/FTPRoot/Guide.pdf>) This

material is copyrighted and has evolved over my 27 years of auditing networks. After downloading the checklist file, email Gloriana@Canaudit.com, provide your name, address, phone and email address and Gloriana will send you the password to decrypt it. This file will only be on the web site until April 1, 2003. So please download it quickly. (You may forward this article to your associates so that they can download the checklists and register as well.)

The network audit and security review should be followed by operating system reviews of the various operating systems in use at your organization. We normally prioritize these audits based on the results of the penetration and network audits we performed, fixing the most vulnerable first. Don't forget to include network device configuration and IOS's in this audit segment.

For best economies of scale, you should include an audit of the most critical databases with the operating system reviews. This will avoid the finger pointing that often occurs. (When you audit the database sometimes the database administrators say the controls are in the operating systems. When you audit the operating systems, the system administrators may say the controls are in the database). Avoid the grief and audit them both at the same time. Backup and recovery, remote archiving, offsite data storage and general business continuance plans should also be reviewed as part of the network audit, or as part of a separate physical security audit.

A word of caution. When doing a war drive with some participants in our recent IT Audit and Security Boot Camp, we observed a major offsite records storage company van that was left unattended for at least 20 minutes. We toyed with the idea of having it towed away as it was in a no parking zone. Imagine how the clients would feel if the truck with their vital records and essential backup data was towed away!!!! The lesson to be learned here is not just to look at the offsite storage facility, but also do the additional testing to ensure that your vital records are secured in-transit and that procedures are in place. You may need to follow the truck to watch the stops it makes, whether the vehicle is attended at all times and determine if the vehicle is left unlocked at any time.

In another case, a "phony" courier picked up the offsite materials prior to the arrival of the real courier. This is a great trick to get copies of most of your critical data which has worked before and will work again if you are not careful. Remember, many of our clients who physically transfer data offsite are exposed to this specific social engineering threat. The solution is to use remote archiving if possible. If not, ensure that proper file transfer procedures are in place.

While there are other reviews that would be part of a full security or audit cycle, I believe that the above items are an essential part of war or terrorist preparation programs. In addition to this, you may want to rethink your organization's evacuation plans in the event of a disaster. Many of our clients limit this to doing a fire drill once a year. In a previous article, I provided a new and somewhat revolutionary approach to disaster containment, evacuation and recovery. This article is also available on the articles and publications section of our web site.

I do not want to use the current international situation as a marketing ploy, nor do I respect others who would do so. If you can do the audits and security reviews yourself, then get started now. Don't wait until the threat warning moves from orange to red. It will be too late then and your staff may want to be home with their families if a true disaster strikes. If you do not have the skills to perform these reviews, then select a qualified consultant to perform those items you cannot do yourself. If you are looking for a consultant, then we would like to be considered along with our competitors. Another way to get the information necessary to perform these war preparation audits is to attend our IT Audit & Security Boot Camp. The next class is in the Chicago area March 3-7; there are still some seats left as I write this news letter.

It is essential that all of our companies, governments, organizations and businesses build a strong security cocoon and revise their business continuance plans. We have to prepare for the worst case scenario, even though the worst case may not occur. I hope with all of my heart that this current state of affairs ends up like the Y2K threat which was prevented by good preplanning and responsible action by our leaders, businesses and governments. We all have to work together to ensure that our society, our organizations, our people and our jobs are protected.

In closing, let me say that Churchill warned of the Nazi risk in 1933. No one listened. Just before Pearl Harbor, messages were received that indicated that an attack was imminent, but no one listened.

Immediately prior to 9/11 there were warnings of terrorist activity, but we were not concerned. The oceans have always protected us. If anyone said on September 10th that a group of terrorists would use box openers to commandeer planes to crash into buildings, some of us would have questioned their sanity. In the process of gearing up for war, we are angering many nations and individuals. It is only a matter of time until we are attacked again, but this time, we will be ready if we heed the warnings. Our physical security will be in place. Our information networks, the lifeblood of our economy, will be protected, and most importantly, our people will be protected. This will not happen by accident. Each and every one of us will have to do our part. Let's work together to ensure the security of our nation and our people.

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.

Gordon Smith / President, Canaudit, Inc.

2002 Canaudit, Inc.

In addition to his work in the field of auditing as President of Canaudit, Gordon enjoys writing articles for several trade journals including the ***Canaudit Perspective*** and is currently finishing work on his second book, "***Control and Security of E-Commerce***," which will be published shortly by John Wiley and Sons. Gordon can be contacted at Gordon@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.

The IT Audit & Security Boot Camp

- Chicago, IL area – March 3-7, 2003 (**Last Change to Register**)

Professional Development Week

******Last Chance to Register by the Early Registration Deadline and Save up to \$150******

Washington, DC area: (Early Registration Deadline – March 7, 2003)

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

Understanding & Preventing Electronic Fraud - April 16-17, 2003

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

The Ultimate Network Penetration Class

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

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

Canaudit Announces our Value of Membership Program

We are proud to introduce our new Value of Membership program. We pride ourselves on the consistent high level of support we have provided to the audit community during the 18 years we have been in business. Our Value of Membership program is directed at increasing our level of support for local IIA, ISACA, ISSA and AGA chapters nationwide. We are offering the following benefits to all members of local chapters who hold a 2-day Canaudit training seminar this year:

- Discounted rates to all Canaudit 5-day hands-on public courses during the same chapter year in which the 2-day chapter seminar is held. (Total discount of \$750)
- A \$5,000 discount on a Network or Penetration Audit booked with Canaudit during the same chapter year in which the 2-day seminar is booked.

Any chapter members who wish to utilize these discounts, please contact your local chapter for your discount code. This discount code must be presented when registering for a 5-day class or at time of requesting an audit proposal.

If your local chapter is planning a 2-day seminar and you would like to know more about the benefits of our Value of Membership program, please contact Kristie in our Marketing Department at (805) 583-3723 or via email, Kristie@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