

Canaudit Perspective

January 2007
Volume 8, Issue 1

TOPICS OF INTEREST:

- Active Directory and the Windows environment are often poorly configured
- Oracle database issues increased significantly
- Email and VPNs were not properly protected
- Network devices remain an issue
- UNIX / Linux machines need to be secured
- The mainframe can be attacked
- Conclusion

GREATEST IT AUDIT & SECURITY RISKS OF 2006



GORDON SMITH
Canaudit President

In this annual IT audit and security update to my clients, I want to point out the issues we identified in our technical audits over the last year. It is surprising to find that many of the risks from the previous year have not been remediated. One would think that after several years of Sarbanes-Oxley (SOX) audit work, networks would be more secure. We

can see improvements in documenting financial control as well as servers that host financial systems. Unfortunately, we have noticed no overall improvement in information security.

During our closing meetings for our audits and security reviews, I am often asked how the results could be so dismal given that the client is SOX compliant. The answer is simple: SOX assesses the overall management and financial control structure. Security on the SOX-related servers is usually good, as these servers are thoroughly audited and any issues identified are quickly remediated. Unfortunately, the over-emphasis on SOX means there are less resources available to identify and secure flaws on other servers and databases. These non-SOX machines may be vulnerable to attack due to missing patches, poor configuration, and other serious issues and well-known exploits. By taking advantage of these machines, in all but one of our audits last year we gained complete access to the Windows domains and Active Directory. Once this access was gained, we were able to compromise a number of machines that were SOX related.

Keep in mind that a single security flaw can topple the entire Windows environment. Cross-over accounts (accounts that have the same password in multiple environments) between the Active Directory, UNIX, mainframe or other devices enable these machines to be compromised, leading to a potential security domino effect. In this article I will focus on some of the key issues we identified and offer some advice on how to better secure the IT environment. Let us start with the Windows environment, as it remains the most poorly secured of all of the environments we audit.

ACTIVE DIRECTORY AND THE WINDOWS ENVIRONMENT ARE OFTEN POORLY CONFIGURED

My first concern is Active Directory implementation. This Microsoft product can be well controlled if the vendor's recommendations are followed. After a failure to properly implement patches and security updates, the biggest issue, in my opinion, is the failure to eliminate the LanMan password. This has been around since before the implementation of Windows NT. It stores passwords in upper case only and the password is split into two seven character passwords, which makes it easier to crack. Using RainbowCrack, a password cracking tool, we can crack any LanMan password that is up to 14 characters in length in less than 30 minutes. We strongly suggest that the LanMan password be eliminated, as it is no longer required for Windows 2000, XP or Server 2003. Once we capture the local password file on one machine, often a poorly secured workstation, it is a simple matter to crack passwords needed to get onto other machines.

At some of our clients, account lockout is not activated or it is poorly implemented. We often find the lockout policy set to five attempts in 15 minutes and the account is locked out for 15 minutes. In some organizations, we

find that the account lockout policy is not activated at all or is implemented on a haphazard basis. We believe that account lockout should be implemented on all domains, servers and workstations. We suggest a setting of three bad passwords in 500 minutes and the account is locked until unlocked by an administrator.

Another issue we commonly identify is a failure to place a password on the sa account on Microsoft SQL servers. In most environments, we find several servers running Microsoft SQL Server with the default blank password or a password of 'password' or 'sa'. Hackers have scripts or tools that can quickly identify susceptible machines then gain system administrative rights. In a few seconds, the password file can be downloaded. Thirty minutes later we will have any crossover accounts we need to gain access to other machines or domain. A cross-over account is an account we use to go from one machine to another. The account and password are the same. If we are really lucky, a cross-over account from one machine will give us access to other domains.

To speed our audits, we wrote a program to automate scanning for the sa account. We can test up to 5,000 machines in about an hour using our tool. If we have a tool, it must be assumed that the hackers have one as well. A single occurrence of a poorly secured sa account can and has given us administrative access to the domain. At several clients, this was the only weakness we found that would give us administrative rights. I strongly suggest that all machines in your environment be checked for poorly secured sa accounts.

Another issue is the continued use of the free version of VNC to enable administrators to service machines. The VNC password can be captured and decrypted instantly once access is gained to a machine. Then, using VNC, we may gain access up to the administrator level by using the password we cracked. We suggest that VNC be replaced with secure implementations of Radmin or PCAnywhere. There are some secure versions of VNC that can be used, just ensure that they use encryption and require both an account name and password.

Once administrative access is gained to a Windows machine, we can often use a tool called lsadump2 to dump the LSA secrets. Here we often find unencrypted passwords for privileged accounts that are used to run Windows services.

A tool called CacheDump can also be used to dump the contents of the domain cache. The cache exists so that users can log onto their system when they are traveling (i.e. laptop) or when the domain controller is down

(preventing them from logging onto the domain). Once retrieved, the passwords must be cracked. By default, the last ten accounts and passwords are stored in the cache. We suggest that this be reduced to two to lower the risk that an administrator-empowered account and password could be gleaned from the cache.

Service accounts continue to be a serious issue. Some, such as the Blackberry (bberry), Exchange admin (exchadmin) and other similar ones give us administrative access. They often have well-known default values and, as such, make the machines vulnerable to attack. Missing patches, particularly the NetAPI32, the Plug and Play (UPnP) and the DCOM exploits give an attacker instantaneous administrator access. Most of our clients have corrected the DCOM vulnerability; however the other vulnerabilities remain a serious issue. We had many other issues in the Windows environment. If you would like further information on these issues, call or e-mail me.

ORACLE DATABASE ISSUES INCREASED SIGNIFICANTLY

This year we found a significant increase in poorly secured Oracle databases. Our new OraScan software automated the penetration and vulnerability assessment process. As a result, we were able to test Oracle security issues without increasing the cost of the audit. The key factor we identified was a poorly secured listener port. By connecting to the listener port that is not password protected, we can obtain a list of Oracle databases running on the affected database server and safely test for known default username/password combinations. It is not uncommon during this audit segment to identify over 20 accounts across several databases with default passwords, some of which are Database Administrator (DBA) empowered. This simple exploit can also be accomplished using OScanner, which is free software from Cqure.net (http://www.cqure.net/wp/?page_id=3). In addition to known accounts with default passwords, many Oracle accounts have simplistic passwords that also facilitate access to the affected database. We usually find several accounts with a password equal to the account name and the "ORACLE" account with one of several defaults or variations of a known default.

We use our own proprietary scripts to audit Oracle parameters and settings. We found a significant number of Oracle issues that are present at most of our clients. One significant issue we often identify is the inclusion of DBA-empowered accounts and passwords in SQL scripts (programs). Since many of these scripts are world readable (anyone on the system can read them) the

passwords are accessible to anyone who gains access to the system. Developer access to production databases was quite common, violating basic separation of duties. We also found that those who know the root password often have Oracle DBA access due to operating system authentication. This is also a very poor separation of duties.

Basic Oracle security, such as account lockout for multiple unsuccessful login attempts, the requirement to change passwords, and the implementation of critical auditing features, are generally not in place. Unsuccessful login attempts are not being monitored or monitored very infrequently. Another issue, which occurs less frequently, is programs and scripts that are world writable. Anyone who gains access to the system could then modify these scripts and programs to create an account or perform some other nefarious function. The next time the script or program executes (with DBA rights), the Trojan embedded in the program executes, possibly creating a backdoor into the database.

We found significant issues with excessive or unnecessary database links and poorly secured database links. Database links can be used to facilitate integration of databases and can result in unauthorized disclosure of confidential information. A key audit task that is often forgotten is the controls over database links. All unnecessary links should be disabled.

Lastly, we found that critical Oracle patches are not installed. The usual reason is the fear that vendor application software will not function properly if the patch is applied. The failure to implement an automated testing facility, such as Mercury TestDirector (<http://www.mercury.com/us/products/quality-center/testdirector/features.html>), means that Oracle patches for complex applications cannot be easily tested. This may be the true cause of poor patch management. If there is a test facility that can ensure that the Oracle patches work on the affected applications, then implementing patches is not only safer, but it is often easier. Based on the issues we identified in 2006, I strongly suggest that our clients schedule audits of critical Oracle databases and applications this year.

E-MAIL AND VPNS WERE NOT PROPERLY PROTECTED

2006 was also the year we focused on e-mail. Executives and key personal using Blackberries and similar devices are linked 24 hours a day. Our audit results indicate that e-mail is often poorly secured. The greatest weakness is the poorly secured Windows environment that often hosts e-mail. The e-mail servers are usually connected to

Active Directory. Once the domain administrator accounts are compromised, everyone's e-mail can be accessed. A hacker can even send and receive mail from another user's account. There are several controls that need to be implemented. The first is to remove exchange administrator access from as many administrator accounts as possible. Next, two-factor authentication (described below) should be required for e-mail access. If this is considered too expensive, then those with sensitive access, such as system and database administrators, executives, lawyers, auditors and Human Resources staff should use two-factor authentication. Another common issue was the use of the default Blackberry password on the domain. This gives an unauthorized person the ability to access e-mail and to disable devices at will. Imagine the impact of the CEO and CFO's Blackberries being disabled during a hostile takeover attempt!

We are also concerned by poorly secured Virtual Private Networks (VPNs) that are often used to remotely connect to the network for e-mail and other network activities. I am a true believer that working remotely is essential. During the last year, we noticed that many organizations do not use two-factor authentication to properly validate a user before granting them access to the internal network or to e-mail. We urge our clients to use tokens, digital certificates or biometrics in addition to accounts and passwords for authentication. The cost of these technologies is dropping, as the risk of not using them is rising. In 2007, I would make two-factor authentication a very high priority if it is not already in place. I would also ensure that those with administrative access to operating systems, databases, network devices and e-mail use two-factor authentication.

A few of the VPNS we audited permitted vendors and some users to bypass two-factor authentication. An auditor or security professional has to be very careful about the questions asked during audits and reviews. If the question is "Is two factor authentication used?" the answer may be yes. Make sure you ask for a list of all accounts that bypass two-factor authentication. This should include vendors who require remote access to the internal network to service their software and employees who need temporary access because they lost or misplaced their token.

The vendor issue is more complicated than most of our clients realize. Often the vendors do not want a token as they cannot identify which person will be on call when your organization has a problem. I also contend that they may want to use off-shore technicians to provide assistance to save on their maintenance costs. By using a secondary password instead of a token, the vendor has the

option of using an in-country resource at any one of their support sites, or they can use an off-shore resource. I have several concerns with this. The first is that the password is passed around and may be used for unauthorized access. This risk increases when the vendor outsources their maintenance and support to another overseas firm. To counter this, I strongly suggest a single-use password be set up for every service activity. The password expires when the service person logs off. If they need to come back in, they need to obtain a new secondary password.

My other concern is that the vendors only need to access the machines that they service. Many VPN configurations let them into the network with no limitations on the machines they can access or any time constraints on their access. As a result, they can enter the network and freely roam. The potential exists for the vendor's staff or subcontractors to extract information from machines outside their area of responsibility, download confidential data or perform malicious activities. I urge our clients to limit the network scope to only the machines and applications the vendor services and to restrict their logon time to a reasonable timeframe, say two hours. If they need more time, they must contact your organization for an extension. I also believe that all of their actions should be logged and the logs monitored so that if issues arise, the logs can be used to document the vendor activity.

It is a good practice to disable lost tokens immediately. If an employee forgets their token and is issued a secondary password, it should be for a single day. It is best to assume that a forgotten token has been lost. Ensure it is disabled as part of the process of creating the secondary password. When the employee returns with the token, it can be reactivated. One last thing on tokens – make sure that a security alert is generated any time a lost token is reactivated.

NETWORK DEVICES REMAIN AN ISSUE

In the last year, network devices had many of the same issues and some new ones. Community strings (passwords for network devices) are often set to the default value of “public” or “private”. “Public” community strings can enable an unauthorized user to view information on the device. A “private” community string can enable an unauthorized user to change the configuration of the device, create a pathway out to or in from the Internet or program a backdoor account into the device so that they can have access if the community string is changed.

Another older issue is unnecessary services active or ports running. Only the required services and ports should be active. Again last year, we encountered several clients who had TCP port 80 open on some of their Cisco devices that were not patched. As a result, we were able to connect to the devices without authentication with the ability to alter the configuration of the device or simply download the configuration. Cisco issued a patch for this several years ago so it is not a Cisco issue. Make sure that these devices are patched and that TCP port 80, which should not need to be open, is closed.

Other clear-text services, such as Telnet, File Transfer Protocol (FTP) as well as HTTP and SNMP transmit data unencrypted. This includes accounts and passwords as well as the data that is passing through the network and possibly the Internet. This makes it easy for an unauthorized person or software program to sniff the passwords and data off the network. Once sniffed, they may be used to gain access to the devices.

My last concern with network devices is the failure to segment the network using simple filters available on most routers and switches. Network segmentation greatly limits the damage that can be done should the network be breached. Segmentation can also be used to protect legacy machines which can be placed behind an internal firewall or filtered network device. If the issues with a legacy machine or application cannot be remediated, then it should be isolated. Network devices are ideal for performing this function.

We identified the need for further controls over Simple Network Management Protocol (SNMP) this year. Since SNMP provides information about the device to those who can connect to the device with read or write capability, we strongly suggest that there be an access control list for inbound SNMP requests. If a user or device is not on the list, access will not be granted. It is important to ensure network devices are properly secured, as disruption of the network can lead to a complete loss of connectivity, preventing users and trading partners from performing critical business transactions.

UNIX / LINUX MACHINES NEED TO BE SECURED

UNIX and Linux machines remain prone to poor security implementation. The finger service or the expand (EXPN) and verify (VRFY) SMTP commands, if active, enable accounts to be enumerated. This is a boon to an unauthorized user, as passwords are often equal to the account name and occasionally are blank. Last year we had several clients with blank passwords on root or root-

empowered accounts. This is highly unusual and came as quite a surprise to our team members. Once onto a machine with a poorly secured account, an unauthorized user can take advantage of vulnerabilities to escalate their capabilities, often to the root level.

The most successful exploit remains trust relationships. Once a user, (authorized or unauthorized) is logged onto the computer, they can use trust relationships to connect to another machine without authentication. Once they are connected they will have rights at least equal to their rights on the first machine and may be able to escalate up to the root level. In the last year, we noted several organizations that had trust relationships set to “+ +”. This means that any user can log on without authentication from any UNIX or Linux machine. Once on the machine, they may have up-to-root access. The double plus sign is highly unusual. If your organization has vendor-installed and supported UNIX machines, ensure the .rhost and host.equiv file entries are scrutinized. That said, all trust relationships should be eradicated as they are extremely high risk and there is a high likelihood of a security event. Since both risk and likelihood of occurrence is high, this should be an immediate fix.

Some of our clients find that legacy software issues prevent them from removing trust. In cases like this, we suggest that they isolate the machines behind an internal firewall (if the issue cannot be remediated, isolate the machine). Another alternate technique is to use a combination of Secure Shell (SSH) and TCP Wrappers. TCP Wrappers place access controls on services to limit who can connect; SSH ensures the connection is encrypted.

A failure to properly patch machines was also an issue in the last year. Various versions of Linux and Sun OS had issues. In the case of Sun, the two critical issues are the Sadmin exploit and the Integer Overflow exploit. Sun’s recommended security enhancements for these issues have been around for over two years, yet, we still find clients who have Sun machines that have not been patched. In the Linux environment, organizations with multiple versions of Linux from different vendors often

have a difficult time keeping up with patches. We suggest that patches be applied on a very regular basis.

THE MAINFRAME CAN BE ATTACKED

Our mainframe clients use RACF, ACF2 or Top Secret to secure the environment. A common flaw we identified in the last year was a failure to implement monitoring of failed logons or account lockout on the FTP service. A smart attacker who gains access to the Windows environment will harvest and crack the passwords. They will then use brute force against the FTP port using the Windows accounts with cracked passwords. If FTP failed logons are not monitored, the attack will go unnoticed. At one recent client, we brute-forced the mainframe using over 12,000 accounts with cracked Windows passwords. This took about an hour and gave our team three passwords we could use to logon. One account gave us OPERATIONS and AUDIT capability (the keys to the kingdom). The comment at the exit interview was that we got lucky. Out of 12,000 accounts, only one gave us significant access. Our response was that it only takes one. Needless to say, this vulnerability was corrected immediately. To detect brute-force attacks, make sure that FTP logons are monitored and that a high-level alert is sent to the security analyst when there are more than 25 failed logons to the FTP port in five minutes. With a brute-force attack, there is not much time to detect the issue before a valid account might be compromised.

CONCLUSION

I trust that the items I discussed in this article will help you in several ways. Many of our clients feel that their security is much worse than other organizations because the majority of the above flaws exist in their organization. Well, they shouldn’t feel too bad. Most organizations suffer from many or all of the above issues. If you have not had a major security event, then count your blessings. If you have, you already know how serious these issues are. In either case, 2007 should be the year that these issues are corrected.

The opinions expressed in this article are mine and mine alone. I look forward to receiving your comment and questions by email (Gordon@canaudit.com and talking to you personally about the issues in this article or any other IT audit or security-related issue).

SIGNIFICANT PRICE REDUCTIONS TO CLIENTS WHO WANT TO QUANTIFY THEIR IT AUDIT EXPOSURE

My professional staff and I are very concerned about the lack of controls in the American IT environment. We want to ensure that price is not a barrier to identifying your organization's risks and exposures. With that in mind, I have created a double-pronged approach to kick off the remediation efforts. The first is spreading the knowledge of the risks through our Professional Development Weeks. To accomplish this **we are offering a two-for-one offer on all of our public courses throughout 2007.** To qualify, you must register and pay by January 31, 2007. Please visit www.canaudit.com or e-mail Brenna@canaudit.com. Register soon to ensure that there is still space in the classes you wish to attend.

Our next offer is one that is quite exceptional. We are willing to reduce our fees by up to 25% on audits performed before March 31, 2007. The table below lists the specific services and the associated fees. The fee does not include travel and other expenses, but we always try to keep these costs low.

Audit	Normal Fee	Discounted Fee
Full Penetration Test	\$55,000 - \$75,000	\$44,000 - \$60,000
IT Security Baseline	\$55,000 - \$65,000	\$42,500 - \$50,000
Network Vulnerability Assessment	\$45,000 - \$55,000	\$35,000 - \$43,000
Oracle Database Audit <i>(up to 5 databases)</i>	\$25,000	\$20,000
Windows Vulnerability Assessment <i>(up to 5000 machines)</i>	\$30,000	\$22,500
UNIX/Linux Audit	\$20,000	\$17,000
Internet Penetration Test	\$17,500 - \$25,000	\$15,000 - \$22,000

If you are interested in any of the above audits, please e-mail me or my senior staff (Gordon@canaudit.com, Tamra@canaudit.com, Chris@canaudit.com). You can also phone 805-583-3723 and ask for Tamra Savage Jones, Senior Account Executive who will be pleased to assist.

PROFESSIONAL DEVELOPMENT

Canaudit also provides quality seminars to local chapters and major corporations. These seminars include technical information system audit classes aimed at everyone from an introductory level up to management. With a list of over 30 courses to choose from, we are sure to have a course that will meet your individual needs. In addition to chapter and private seminars, Canaudit also holds public courses. Upcoming public courses are posted on the website, www.canaudit.com.

Upcoming Public Courses:

<u>Allentown, PA</u> March 5-9, 2007	The IT Audit & Security Boot Camp	<i>HANDS ON</i>
<u>Philadelphia, PA</u> May 7 - 11, 2007	The Ultimate Network Penetration Class	<i>HANDS ON</i>
May 7 - 8, 2007	Control & Security of Windows 2003	
May 7 - 8, 2007	Control & Security of UNIX	
May 9 - 10, 2007	Control & Security of Web Applications	
May 9 - 10, 2007	Control & Security of Oracle	
May 11, 2007	Control & Security of Microsoft SQL Server	<i>NEW</i>
<u>Bloomington, MN</u> June 11 - 15, 2007	The Ultimate Network Penetration Class	<i>HANDS ON</i>
June 11 - 13, 2007	Automating Technical Auditing	<i>HANDS ON</i>
June 11 - 12, 2007	Control & Security of Windows 2003	
June 13, 2007	Control & Security of Microsoft SQL Server	<i>NEW</i>
June 14 - 15, 2007	Control & Security of UNIX	
June 14 - 15, 2007	Control & Security of PeopleSoft	
<u>Farmington Hills, MI</u> October 15-19, 2007	The IT Audit & Security Boot Camp	<i>HANDS ON</i>
October 15-19, 2007	The Ultimate Network Penetration Class	<i>HANDS ON</i>
<u>Simi Valley, CA</u> December 3 - 7, 2007	The IT Audit & Security Boot Camp	<i>HANDS ON</i>
December 3 - 5, 2007	Automating Technical Auditing	<i>HANDS ON</i>
December 6 - 7, 2007	Control & Security of Windows 2003	

Registration for a Canaudit public seminar can be performed online at www.canaudit.com. For additional information or interest in hosting a Canaudit seminar, please email Brenna@canaudit.com or call (805) 583-3723.
