

DATA MINING: HOW HACKERS STEAL SENSITIVE ELECTRONIC INFORMATION



Since my very successful presentation on data mining personal information at a recent conference, I have had several people contact me to convert the presentation into an article. This edition of the Canaudit Perspective presents the main items in the presentation in written form. Obviously the live, hands-on demonstrations cannot be

presented here, but the techniques can certainly be explained. At the conference, we offered a significant discount for performing a Canaudit IT Security Baseline or a Network Penetration Test. At the end of this article, I will provide details of the significant discount off our normal price for a basic 360-Degree IT Security Baseline. Now onto the article:

There are six main objectives of this article that coincide with the six processes the hackers use to gain access to and copy sensitive electronic information. These are as follows:

- How to hackers gain access to the network?
- How do hackers avoid detection, even if there is an Intrusion Detection System or Intrusion Prevention System implemented?
- How do hackers identify or catalog the machines in the environment?
- How do hackers identify and target sensitive data?
- How do hackers compromise databases and take sensitive data?
- How do they implement a firewall breach so they can return at will from the Internet?

GAINING ACCESS TO THE NETWORK

Most organizations have public areas. As many of you know from my classes, breaching physical security is relatively easy. A few days of observation usually give me the ability to exploit flaws in the organization. Often times I just walk in, find an empty desk, conference room, or office and plug in. If I am asked any questions, I just say that I am an auditor. In every case where I have used this technique, I have been left alone to work. At each location, I have been able to identify a workspace, set up a computer, and start working on defeating the network security. Physical security is very difficult to implement in many organizations, as often parts of a facility, district, or regional office are open to the public. It is up to the employees to be aware of unusual activity and report it. Awareness training and a well established hotline for security events are a must.

Another access point is poorly secured wireless networks. During many of our audits we have sat in the parking lot and gained access to the wireless network and the internal network. Unencrypted and poorly secured wireless is still an issue at some organizations. Certain industries, such as hospitals, are worse than other industries and organizations as some have not identified wireless as a risk and have not taken the necessary steps to secure it.

While the internal network at an organization may be secured, it is often possible for an insider to set up an unauthorized wireless network. The equipment can be purchased from Best Buy for \$40, plugged into the network, and be used by anyone within broadcast range. It is critical that regular wireless sweeps be conducted to identify rogue and poorly secured wireless networks.

Hackers may also be able to compromise the Virtual Private Network (VPN) that may connect both external and internal users to the network. This results primarily from poorly secured network devices, the use of default accounts and passwords, and the failure to use two-factor authentication (RSA SecurID or other mechanisms). If the VPN is "hacked" from the Internet, the hackers may have a high-speed

connection to the internal network. Poor controls over webmail may provide hackers the leverage to gain access through the VPN. It is best to provide SecurID tokens or other two-factor authentication to secure the webmail application. Once these devices have been purchased for use on webmail or for external connection through the VPN to the internal network, why not go one step father? Use the tokens for access to the internal network where possible.

We have some clients who have successfully implemented two-factor authentication. There are always concerns that tokens will impede the ability of users to log in, particularly in an emergency. By selecting the correct methodologies and working with staff, these hurdles can and have been overcome.

The last major entry point is poorly secured trading partners that connect to the network. Often these partners have networks that connect to other organizations. This makes understanding all of the access points to the network very difficult indeed. This risk could be compounded if the trading partner does not meet or exceed your organization's security standard. If the partners' network is compromised by hackers, then it may be possible for the hackers to view and possibly migrate their attack your network. Compounding this risk, trading partners often connect to many other trading partners. A hacker can take advantage of a poorly secured trading partner network and may be able to compromise several organizations networks from the same breached partner network. Some of our clients have mitigated this risk by requiring partners to meet the minimum standard before connecting to the organization's network. If they cannot meet or exceed the standard, they cannot connect their network to the network. Instead they come in with a secure Virtual Private Network connection, with very little or no access to the internal network.

HOW HACKERS AVOID DETECTION

For many organizations, an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS) is considered a luxury that the organization cannot afford. As a result, they have no ability to detect a hacking attack during the early stages, isolate the activity, and investigate the incident. Without an IDS, the scale is dramatically tipped toward the hacker. Without an IDS or IPS, there is very little defense against even a novice hacker attack. Experienced hackers will be able to gain access to the network, identify personal information and trade secrets, and capture a copy of it within one to three hours. In an unprotected network, our teams often have complete administrative access to the Active Directory and the Windows domains within an hour.

If a network does have an IDS, a knowledgeable hacker has several techniques they can use to avoid detection. The first is to avoid broad network scanning. Most IDS's pick up multi-port scanning as a serious threat. To avoid scanning, a hacker can use the "net view" command from a command prompt. This command, when directed against a domain, provides the hacker with a list of all of the machines connected to the domain. Using this list, they do not have to scan the network. Instead, they can launch a low-level attack against these machines, identify the poorly secured machines, and gain administrative right to those machines. We teach auditors and security staff to use the same tools at our IT Audit and Security Boot Camp. The best way to secure the network is to test it with the same tools that the bad guys use and then implement the required security.

Hackers defeat an IPS by masquerading as devices that are normally excluded from IPS monitoring. These include printers, video conferencing devices, and Voice over IP (VoIP) systems. These types of systems are excluded as they normally create a large volume of false positives or alarms. These false alarms result in investigations that divert security staff from directing their efforts to real attacks. Our philosophy is to properly configure the IPS so that the false alarms are minimized. Management needs to recognize that this will take a significant manual effort by the security folks, so it must be staffed and funded properly.

Clearly, a properly configured IPS or IDS is an essential component in a security package. They work in conjunction with other controls to ensure the early detection and investigation of hacking attempts.

CATALOGING THE ENVIRONMENT, IDENTIFYING TARGETS

There are many ways to document or catalog the network. In our normal network audits, we use tools that work quickly, but are easily detectable. Hackers, on the other hand, want to remain undetected as long as possible. Once they have connected to the network, there are several approaches they can use to avoid detection. The first is to use a simple scanner such as Solar Winds IP Browser. Most IDS's are configured to ignore simple network management protocol (SNMP) scans as many network management tools use this service. Using Solar Winds, many of the devices in the network can be identified. Naming conventions for machines may reveal the nature of the information on the machine. A machine with a name of Psoft most likely hosts the PeopleSoft application. Other names we often see are Lawson, McKesson, and Cerner. Once the machines are identified, it is a simple matter to determine if known exploits have been patched.

In some organizations, patches are often not applied due to concerns about the impact on the application. As a result, we can normally get onto these unpatched systems and harvest sensitive files. One of the easiest files to harvest is the database backup file. Whether the database is Oracle, DB2, or Sybase, the backup files are generally world readable. This means that anyone who can get onto the system can capture a copy of the backup. It is a simple matter for the hacker to import the backup into a database on one of their own systems. They now have a fully accessible copy of all of the data in the database.

There are two lessons here. The first is to ensure that all machines are properly patched. If there is some uncertainty that a critical application will run after the patch is implemented, then take an image of the machine and load it onto a test server. Then apply the patch, and run full testing of the application. If it continues to perform well, then the patch will likely not cause any harm. Take another image of the production system, and then apply the patches to production during a low-volume period, such as over night. If the machine fails, restore from the image and resume normal operations. Machines that absolutely cannot be patched should be isolated behind an internal firewall so that hackers cannot access them. If you cannot remediate an issue, then isolate it on a protected network segment.

The second lesson is that backups should not be world readable. Modify the backup procedure so that any time a backup is created, the file permissions on the backup file restrict access to only a few people. These people would be the ones who would restore an application after a process interruption or failure.

Another way to quickly find databases is to use a scanner such as SuperScan and set it to only scan for specific ports. The Oracle listener port is TCP port 1521. By setting the scanner to only locate the listener, the attacker can minimize the likelihood of being detected, while quickly identifying the Oracle databases. Our audits reveal that most Oracle databases have default accounts and passwords that can give an attacker database administrator-type access. Once they are able to get onto the database, they can extract additional passwords from the UserData table and crack them with Cain or another free Oracle password cracker. With database Administrator (DBA) access it is easy to extract the PHI or customer financial data from the databases.

Many of our clients are now using Microsoft SQL (MS/SQL) database applications. Again using SuperScan or a similar scanner, scan for TCP port 1433. MS/SQL databases that are poorly secured are simple to compromise. Simplistic passwords on DBA-empowered accounts, such as 'sa' with a password or 'sa' or 'admin' with a password of 'admin', give the attacker DBA-type access in a few minutes. Once they have DBA access, they can use a simple query to take sensitive data. They can also gain local system access to the server which may lead to the compromise of the entire Active Directory and the domains within it.

The quickest way to data mine confidential information is to go directly to the databases. Hackers do not bother scanning the entire network. Instead, they identify the machines hosting databases, directly connect to the databases, and take the data.

BUILDING AN INFORMATION SUPERHIGHWAY THROUGH YOUR FIREWALL

Once a hacker gains access to the internal network, they like to be able to come back at will. The best way to do this is to place a copy of LogMeIn software (free from www.logmein.com) on a windows machine within the network. Once this software is installed, a hacker can pass through the firewall and gain high-speed access to the internal network. I have written about this in several of my articles and demonstrated it in several of my classes. I will not pontificate any further on these inside-out, outside-in exploits. Just remember that software such as LogMeIn, GoToMyPC and RemotelyAnywhere can create openings in the firewall that can be compromised by hackers.

CONCLUSION

Most organizations in general are a target for data miners due to the lack of a properly configured Intrusion Detection System, failure to apply patches, and the use of simplistic passwords. Once in, a hacker can easily glean personal information and confidential business data. A full IT Security Baseline is required to identify flaws for remediation. Periodic baseline checkup need to be performed to measure and quantify improvements to create metrics that senior executives can understand and evaluate. Follow-up baseline scans can also identify additional risks since the first baseline was performed.

The opinions expressed in this article are mine and mine alone. I look forward to receiving your comments and questions. You can email me at Gordon@canaudit.com If you would like to receive articles like this in the future directly, please opt-in to our distribution list on the Canaudit website.

SPECIAL PRICING OFFER

At Canaudit, we are committed to improving information security. We are aware that there are budget issues that make it difficult to afford a complete IT Security Baseline. Our full IT Security Baseline typically costs \$65,000 plus expenses. To demonstrate our commitment to healthcare security, we are offering our **basic** Internal Network Security Baseline to organizations for \$30,000 plus expenses. This work must be performed between December 2008 and February 2009. The following prices apply to this offer:

Basic Internal Network Security Baseline	\$30,000 + expenses
Wireless Test	\$5,000 + expenses
Internet Test	\$15,000 + expenses
Internet Test w/ Web Application Security Audit	\$22,500 + expenses

To qualify for the discount the contract must be signed by December 15, 2008. The work must be started before February 28, 2009. Please contact Gordon@canaudit.com or Tamra@canaudit.com for more information.

Canaudit is also offering to all healthcare organizations 50% off the IT Audit and Security Boot Camp in Simi Valley, CA (December 8-12, 2008). To receive this discount, please use the code CP2008 when registering.

AUDIT & SECURITY SERVICES

Canaudit specializes in a variety of information system and technology audits, ranging from periodic network penetration testing to full network and operating system security review. Our tailored audits provide an objective, disciplined, and in-depth analysis to evaluate and improve the effectiveness of risk management, control and security within your organization's technological environment.

For interest in Canaudit to perform an IT audit for your organization, please email Gordon@canaudit.com or Tamra@canaudit.com, or call (805) 583-3723.

PROFESSIONAL DEVELOPMENT

Canaudit 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 20 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>Farmington Hills, MI</u> October 20-23, 2008 October 22-23, 2008	Hands-On: Performing an IT Audit and Security Baseline Control and Security of PeopleSoft	<i>NEW</i>
<u>Simi Valley, CA</u> December 8-12, 2008 December 9-10, 2008 December 11-12, 2008	Hands-On: IT Audit and Security Boot Camp Control and Security of Web Applications Computer Forensics for Security and Audit Professionals	
<u>Albuquerque, NM</u> January 12-15, 2009 January 12-13, 2009 January 14-15, 2009	Hands-On: Performing an IT Audit and Security Baseline Control and Security of Oracle Control and Security of Enterprise Wide E-Commerce	<i>NEW</i>

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.