

# The Canaudit Perspective

June 2004  
Volume 5, Issue 6

## *Modems: Your Network's Weakest Link*



***Cisco Pix Firewall 535: \$29,995. ISS Proventia G1000F Intrusion Prevention System: \$36,995. Chief Information Officer's salary: \$483,245 (well at least it should be). The look on the bosses face when he learns the network security systems have been defeated by a \$10.50 modem: Priceless.***

As ridiculous as this may sound, bypassing a million dollars worth of Firewalls, IDS, IPS and any other network perimeter defense mechanisms, with a \$10.50 modem is not such an unlikely scenario. Modem security is one of the most overlooked exposures facing corporate network security, like an open window to the network. I often associate network security to that of the security of a house. This may sound familiar to those who have attended any of the Canaudit security courses. Picture it: you secure your house with top-of-the-line locks and redundant security systems. You have cellular and analog connections to the monitoring station, laser light beams, thermal motion detectors and the big tough body guard by the front door. You deplete an unbridled budget to secure the obvious entry points – the front door, the back door, the garage, even the chimney. Your house is so secure the tooth fairy could not get in without the local SWAT team showing up. Santa Clause will not come within 10 miles because of the pit bulls that want to chase him all the way back to the North Pole. While all this is going on, someone left the proverbial back window open, allowing your house to be an easy target for thieves. Your house, much like your organization's network, is only as secure as the weakest point of entry. Organizations using the latest in network perimeter defense technology can still fall victim to an improperly secured modem.

If your organization is not conducting a periodic war-dial or modem security audit, then you have to ask yourself one question... "Do you feel lucky? Well, do ya?" Since more and more organizations are adopting preemptive approaches to information system security, it is absolutely imperative that modem security be considered, tested, controlled and monitored. It is a very simple procedure to install a modem on a PC plugged into the network without notifying or obtaining permission from the appropriate IT security personnel. If unauthorized modems are not regularly identified, there could easily be a rogue modem serving as an entry point for hackers into the network. Periodic war-dialing will help your organization identify, analyze, and control the security risk inherent with the use of unauthorized modems.

The first step to controlling modem security is to identify the phone numbers modems are residing on. There may already be a pre-existing list of known modems within the walls of your organization. It may or may not be accurate, and chances are it is outdated. A good starting point is to create a list of all phone numbers that will be subjected to a modem war dial. From experience, finding out what phone numbers belong to an organization is, hands down, the most difficult part of conducting a war dial. The accuracy of the initial phone number list directly correlates with the accuracy of the war-dial results. So take time in this portion of the war-dial to identify and include in your list as many numbers belonging to your organization as possible. Personally, I am never content with all the numbers I have obtained. There always seem to be more, somewhere. Some good places to start with finding organizational phone numbers are with the PBX operator, the accounts payable department (phone bills) and the organizational telephone directory. You can also take a walk through the wiring closets and data center, as there are always seems to be phone numbers written on the demarcation panel. Contacting the phone company to request a list of all circuits that terminate in your facilities is also a useful technique. Just remember, great care must be taken to not include any numbers outside your organizational assets, as penetrating a phone circuit that is not your property may likely be a crime, even if such access was unintentional.

A war-dialer, also commonly called a demon dialer or modem sweeper, is a software product that dials a given list or range of phone numbers and then records the response. Specifically, the software is looking for a response it can identify as a modem by listening for a handshake tone. Those phone numbers responding with a handshake tones may be modems and could possibly be entry points into a computer, telecommunications system, or network. Those numbers that respond may also be telemetry devices, fax machines or perhaps a tone response, which may allow for unauthorized access to the organizations long distance access service. Each number identified as having a modem, fax etc. or tone response must be carefully documented and followed up on. Some of the more feature-rich commercial war-dialers have built-in mechanisms for identifying and logging, which I have found very useful and timesaving.

When setting up your war-dial, take into consideration the hours you will be dialing. You do not want to dial during production hours, if at all possible, to avoid disrupting employees. Also, consideration to phone numbers in different time zones should be made. Be sure to ask about any internal emergency numbers your organization may have and be sure to exclude those, along with any 911 numbers from your lists. One final note: determine how much time you have until voice mail starts recording and cut your maximum call length about two to four seconds short of that time period. You do not want to fill up the message system's memory with blank messages and cause important messages to be missed.

Once a modem has been identified by the war-dialer, you should connect to it manually using Microsoft's Hyper Terminal, or my preferred application, Procomm Plus from Symantec. Procomm Plus has some great scripting and logging features which are invaluable in documenting and automating your quest for more access. You will still have to be adaptive and flexible in your techniques for manually connecting and testing modems, based on the type of connection protocol, by using the appropriate client for the protocol being tested. It may not always be possible to detect what type of modem you have found. If the host modem is expecting communications from a proprietary client or application protocol, you may be out of luck. Some war-dialing software comes with the ability to automatically detect the type of modem it has identified, such as Sandstorm's PhoneSweep. I strongly encourage you to connect to each modem manually and take note of the modem's response and whether or not it allows unlimited authentication attempts. If not, how many authentication attempts can be made before the modem drops the line?

Another item to take note in your testing process is the information displayed in the welcome banner. Information that may help an attacker, such as OS type or version, should not be displayed. Identify and take note of the warning banner on systems. You will want to enhance modem system banners to ensure the connecting user has been advised that they "MAY BE MONITORED," and that unauthorized use is prohibited and will be prosecuted. I bolded "may be monitored," because unless the connection is actively being monitored at all times, you may run into some legal problems if the banner reads "are being monitored." For exact wording of such banners, the legal department should be consulted.

Do some research on the Internet for default accounts and passwords for the specific type of application or modem being tested. You will likely be surprised with what you find. There are many default account and password lists available to clever "googlers" for specific devices. Also, be sure to check the vendor's web site for any support documentation that may contain default account and password information. Try authenticating to the modem with the defaults and any educated guesses. In some cases, you may not need a password at all and will be dropped right in. Be extremely careful to not lock out any accounts, as this will never help your purpose. A good rule of thumb is to not attempt more than two password guesses for any one account, unless absolutely certain there is no account lockout.

Intruder detection for modems? What a concept! I wish I had thought of it first, but the clever folks at Sandstorm beat me to it. Sandtrap is a product designed to detect war-dialing, mimic a juicy modem target, log everything, and send alerts to the required staff. If you already have it, then you have likely been detected at this point in your modem audit. If you do not have this software, your attack will likely go unnoticed.

It is possible that your failed authentication attempts are being logged. If they are, the important question is: Are these logs being reviewed? This needs to be researched for each identified modem. I suggest that after three bad password attempts, the circuit should be dropped, forcing the user or attacker in this case (you) to redial. Additionally, three failed logon attempts and the account is disabled should be considered on all systems, even those without modems. I have come across many modems on systems that allow unlimited authentication attempts with no circuit drop or locking out of accounts. Even if I were to ftp or telnet to the same machine from the network, I would be locking out accounts left and right and having to reconnect every three to five guesses. Unlimited authentication attempts via modem connections present a HUGE RISK to any network or system allowing them. In such cases, an attacker – or in this case you – can script username/password guessing attacks to run automated and quickly.

Phonesweep is capable of password-guessing attacks and is extremely effective against modems with unlimited authentication. I often use the scripting feature of Procomm Plus, called Aspect, to launch account/password guessing attacks. Aspect scripts can easily be created (you do not have to be a programmer) to attempt password-guessing attacks. Aspect is similar to Expect, a tool used to automate user input. Either tool you use, the fact remains the same: three bad authentication attempts and a circuit drop can slow down an automated password guessing attack against a modem.

After you are comfortable that enough testing has been done for each identified modem, start investigating the modems within your organization. For each identified modem, it should be decided whether or not the modem is required for day-to-day operations and by whom it was approved. Some other good information to be documented about each and every identified modem includes the following: the purpose, authentication mechanisms, level of access to the network, physical location and who has been given access to the modem. Each modem should be tested and reviewed internally at this point to ensure it is properly secured and all default accounts and passwords have been changed. Ensure only authorized accounts requiring modem access are enabled and any default accounts or those no longer requiring access are disabled. Pay particular attention to accounts used by employees who are no longer with the organization, as well as temporary accounts used to grant vendor access that may have been forgotten about. This is also a good point during the process to ensure all passwords used to access any modem either meet or exceed organizational password policy standards. Do not forget, we touched on this earlier; you will want to determine what logging, if any, occurred during your modem attacks. Find out who reviews failed access logs and how often this is being done, if at all.

Speaking of policies, I am a major advocate of policies and documentation; however, that is a whole different article. Sometime during the modem security audit, you will want to find out if your organization has a formal modem security policy. Perhaps modem security is covered on your organization's remote access policy. Either way, there is no better time than the present to review the modem security policy and make updates if required. Remember that policies are worthless if they are not known to all employees and strictly enforced. Ensure everyone has read and understands the newly updated modem security policy. This is, of course, assuming that your organization has some sort of formal modem security policy, right? Well, they will now.

Canaudit has performed countless network security audits and penetration tests, which often include a war dial. Our penetration team gains access through modems approximately 8 out of 10 audits. Most of the time we gain access to modems using blank, default, or easy-to-guess account/password combinations on modems the organization did not even know about. If we are not successful with default account and password strings, we will try to gain access to modems using an account and password gleaned from the internal network test to simulate an attack with information a disgruntled or previous employee could easily obtain. In many cases, some of the modems we identify are not authorized by the organization and IT Security did not even know they existed. We often find modems used and installed by third-party vendors so they can access the systems they support when the need calls for such access. Ensure you do not let this occur without being contacted first by the vendor.

Vendors often have more access to the internal network than they require for servicing and supporting their systems. In cases involving third-party modems for vendor access, the modem should be unplugged, prompting a phone call from the vendor when they need access. This access should be documented and monitored and disconnected when no longer required.

There are many different war-dialing products available to perform such a test. Freeware tools include Toneloc and THC-Scan. There are also highly functional Commercial war-dialer products, such as Phonesweep, Modemscan and Telesweep. Note: you do get what you pay for on these products. Freeware has limited capabilities and is often DOS based. On the other hand, Sandstorm's easy-to-use GUI PhoneSweep includes robust multi-modem scanning, identification of over 470 systems, username and password checking, and customizable reporting.

Modem security must be made a priority in information system security. The significant risk is not only associated or limited to blind war-dialing attacks from the outside, but with attacks using internal knowledge as well, either from disgruntled or previous employees. I can not emphasize enough the importance of knowing what modems your organization has, as well as the controls, or lack thereof, to mitigate the inherent risk they create. Since modems are not the obvious avenue of attack on a network, they are often excluded from information system security programs. Any unnecessary or unauthorized modems should be removed and disabled. For the remaining authorized modems (you know those modems IT and the third-party vendors swear they can not live without), a feasibility study should be performed to see if they can be replaced with either a well-controlled virtual private network, concentrated into a modem pool, secured using call-back techniques or RSA authentication, and my personal favorite - unplugged until it is required, then unplugged again. In closing, it is imperative that these modems are identified, documented, and secured. Do not let your company's network perimeter defense systems be defeated by a \$10.50 modem.

If you require any assistance on conducting an authorized and legal war-dial for your organization or would rather have an experienced team from Canaudit conduct a formal modem security audit, please contact our main office at (805) 583-3723 or email me at [tamra@canaudit.com](mailto:tamra@canaudit.com). Additionally, I always appreciate feedback and comments from anyone willing to provide it.

Tamra Savage  
Senior Technical Audit & Security Specialist



1376 Erringer Road, Simi Valley, CA, 93065  
Telephone: (805) 583-3723 – Fax: (805) 582-2676 – Web site: [www.canaudit.com](http://www.canaudit.com)