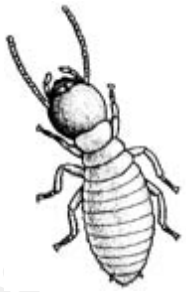
Global Information Assurance Certification Paper

Wayde R. York
GSEC Practical Assignment
Version 1.2c

Weakening The Infrastructure From Within

A house, freshly painted, looking new and shiny, has the appearance of a well-kept abode. From the outside, any who see it would likely think, "here is a homeowner who knows how to keep their place in top shape." A network, be it an Intranet, Extranet or simple Local Area Network (LAN) with properly arrayed firewalls, firewalls and intrusion detection devices may also give the appearance of a well-kept abode. Again, from the outside, protection appears daunting. However, in both cases, appearances can be deceiving.

The subterranean termite lives by ingesting cellulose fibers, usually from wood products. Termites eat their way through wood from the inside, leaving little evidence of their presence from an outside view. Based on normal feeding activity, termites take 3 to 8 years to cause appreciable damage. According to the University of Nebraska-Linclon under ideal conditions, a termite colony of 60,000 workers may consume a one-foot length of 2" x 4" pine in four to five months. Those ideal conditions include high humidity within the "eating area" that is created by the termites bringing mud into the wood chambers they have opened while ingesting the cellulose fibers.



According to Orkin, termites cause more damage to homes in U.S. than storms and fire combined. Therefore, that shiny, freshly painted home that may look like it is in great shape could be in the process of being eaten from the inside out, ultimately causing substantial, and usually surprising harm. In short, the home's infrastructure has been compromised.

The good-looking network with its array of externally faced protection may also have termites of a sort chipping away at the network from the inside. According to a recent survey of 359 companies by the FBI and the Computer Security Institute (CSI), in the year 2000, 38% of the threats to a network came from within the network. During this same survey, remote dial-in accounted for another 22% of attack sources. Combined, that means that of all the attacks a network is likely to encounter, nearly 60% will come from sources other than the Internet, i.e. insiders. Of the sources of attack against an organization's web server, two facts stand out; in 2000, 81% came from disgruntled employees and less than half of these attacks were ever reported to either corporate or law enforcement authorities.

By not stopping and not reporting attacks against networks, we are not only creating a larger target on our topology, but an organization is actually "bringing

in the mud," by making the environment more comfortable for the insider threats to do their deeds.

Provided the 2" x 4" board that termites can consume in 4 to 5 months is not a supporting beam of a home, the cost of that piece of wood is minimal. However, companies, reporting a loss, lost more than $50 million last year as a result of unauthorized insider access and abuse of IT systems.

What does an insider threat look like? Here are two examples from an U.S. Army publication titled, The Insider Threat To Information Systems:

> A Management Information Systems (MIS) professional at a military facility learns she is going to be downsized. She decides to encrypt large parts of the organization's database and hold it hostage. She contacts the systems administrator responsible for the database and offers to decode the data for $10,000 in "severance pay" and a promise of no prosecution. He agrees to her terms before consulting with proper authorities. Prosecutors reviewing the case determine that the administrator's deal precludes them from pursuing charges.
>
> An engineer at an energy processing plant becomes angry with his new supervisor, a non-technical administrator. The engineer's wife is terminally ill, and he is on probation after a series of angry and disruptive episodes at work. After he is sent home, the engineering staff discovers that he has made a series of idiosyncratic modifications to plant controls and safety systems. In response to being confronted about these changes, the engineer decides to withhold the password, threatening the productivity and safety of the plant.

A timely example of insider threat can be seen in recent headlines. Robert Hanssen, a former high-level FBI agent is currently charged with spying for Russia. However, this case has an interesting Information Technology (IT) twist. Dan Verton of Computerworld reported on February 21, 2000 in an article titled FBI Spy Case Highlights Insider Threat to Corporate Data:

> "According to a 100-page affidavit filed in the U.S. District Court in Alexandria, Va., Hanssen used his access to the FBI's Electronic Case File system, which contains classified information about ongoing FBI investigations, to check whether the FBI had been alerted to his activities. Although Hanssen and his Russian handlers relied heavily on traditional spying methods, such as "dead drops" for exchanging packages anonymously, the case is being touted by the FBI and IT security experts as a harsh lesson in the growing threat to corporate data by insiders.
>
> "In short, the trusted insider betrayed his trust without detection," said Freeh during a press conference yesterday. "He constantly checked FBI records for signs that he and the drop sites he was using were being

> investigated." Freeh has since ordered that a special panel be formed to review all FBI processes and systems and to study the issue of insider abuse."

While the allegations in the Hanssen case do not show the classic "insider-hacker" profile, these allegations are a sobering reminder of what a trusted member of an organization can do. While it is unlikely that the type of insider activities Mr. Hanssen is alleged to have committed can be prevented or stopped, the insider threat to a connected organization can be significantly mitigated through a strong policy and correctly focused detection program.

Policy

Every good security effort depends upon relevant and current policy. Combating the insider threat is no exception. System-use policies which govern what a user can and cannot do with the organization's IT asset should be designed to clearly articulate restrictions and enforcement measures. In order to mitigate the insider threat, system-use policies may include the following prohibitions:

- Port scanning on the network
- Assigning share drives without passwords
- Enabling ftp servers on their systems
- Operating modems in any mode other than a "no auto answer" mode
- Excessive use of the ICMP Ping application
- Possession or use of password cracking tools
- Usage of unauthorized remote control tools

Additionally, the policy should address privacy rights while using organizational systems. The more specific the policy is the more latitude network security professionals will have in enforcing these policies.

Most employees will never run afoul of policies such as those seen above. In fact, most employees may not understand how to run afoul of these policies. However, the "curious" user who may start off innocently by downloading a remote control tool such as Back Orifice or SubSeven to "see what it does," can easily turn into a malicious user or cause unintentional harm. Having these policies in place will allow enforcement and punishment.

Should an organization create policies to penalize the curious? Take SubSeven, for example, as a program that a curious user may download and install. Once installed, SubSeven's GUI user-interface allows the user to easily monitor a victim's keystrokes, take screen shots, eavesdrop through the computer's microphone, control the mouse pointer, read and write files, and sniff traffic off the victim's local network. These types of events may be harmful enough, if confidential information was compromised or the victim system's information was lost.

But wait, there's more… a SubSeven server can also be programmed to announce itself over ICQ or Internet Relay Chat (IRC), and groups of servers can be remotely controlled by someone else as one. This may well occur without the knowledge of the curious but unskilled "experimenter." Suddenly, the program becomes useful for launching distributed denial of service attacks (DDoS), in which loosely connected systems are simultaneously commanded to flood a single site with an overwhelming volume of traffic. The potential liability of the organization, whose hosts were used, even unwittingly, is untested. But no organization wants to be the first to face such a lawsuit.

Detection

Now the policy is in place, all users have signed and acknowledged their understanding and intention to adhere to the policy. How will an organization know when violations are occurring? The concept of "Defense In Depth" speaks to providing multiple layers of protection, so that an intruder must traverse a number of layers, like peeling an onion, to get to the goal. Firewalls, routers with access control lists and certain ports blocked and Intrusion Detection Systems (IDS) are typical components of a "Defense In Depth." The problem with this defensive posture is that typically all resources are arrayed to keep the outsider from coming in. With no protection within the inner core of the network layers, the threatening insider is free to roam about and do practically anything. Also, should an outsider penetrate the layers of an organizations defense and gain control of an inside host, that compromise could open a long-term door in the organization's information infrastructure.

Lately, the developer of Back Orifice has released a new "tool" called SMBRelay. This application exploits a design flaw in the SMB (Server Message Block) protocol on Win NT/2K machines, enabling an attacker to hijack the connection between the client and the server. SMBRelay also collects the NT LAN Manager password hashes transmitted and writes them to hashes.txt in a format usable by L0phtcrack for ease of cracking. This application is easily downloaded and in the user-friendly style of other offerings from The Cult of the Dead Cow, it is easy for the novice to use. Its ease of use makes it a program that can be very dangerous in the hands of an insider. Insiders can easily guess most network usernames, since usernames are typically standardized throughout the organization. Add a cracked password, and you have the potential of an inside user using the Vice President's username and password to view salary files, highly sensitive data and the like.

There are a number of measures that can be implemented to protect the inside of the infrastructure from infestation. Among these measures are:

- The installation of a network-based IDS that looks into the network, vs. outside
- Network scanning by the network or security administrator

- Monitoring traffic flow to determine potential malicious activity
- Configuring organizational email systems to block Trojan horse carriers
- Configuring and updating anti virus software to detect and eradicate unauthorized remote control applications

Each of these items is discussed below.

THE INSTALLATION OF A NETWORK-BASED IDS THAT LOOKS INTO THE NETWORK, VS. OUTSIDE.

Implementation of an IDS that looks into the network will provide 24/7 monitoring of traffic and immediately detect the use of known hacker tools and exploits. In a Microsoft environment, copious amounts of NetBios and NetBeui traffic may cause false alarms in some IDS. The good news is that most current IDS's have the capability to tune attack profiles to the "normal" operation of the network it is protecting. Naturally, an organization would want to locate the IDS on the inside of the firewall-protected perimeter.

There are a number of products on the market that can monitor application layer activity, TCP/IP and Microsoft protocols, are configured to match network traffic to attack patterns, and will notify the administrator via pager, email, console and other devices. Among these are: (in no particular order)

- Cisco's **Secure Intrusion Detection System** (formerly Net Ranger)
- Internet Security System's **Real Secure**
- Symantec's **NetProwler**

When evaluating IDS products, pay close attention that the system under consideration adequately covers the protocols used within the network. When monitoring applications it is useful to note the use of tools that should not necessarily be in use, such as an ftp server. And finally, an IDS that not only employs attack pattern matching but also provides updates to those patterns as new exploits arise will keep the detection process (nearly) up to speed with the development and download of new hacker tools.

An organization operating with an extremely limited budget may find SNORT useful. SNORT is a free IDS, which may be found at http://www.snort.org. SNORT has three primary uses. It can be used as a straight packet sniffer like tcpdump, a packet logger, or as a network intrusion detection system. SNORT operates on a number of UNIX and LINUX distributions, and even claims to operate on WIN32 and MAC OS – based systems.

NETWORK SCANNING BY THE NETWORK OR SECURITY ADMINISTRATOR

Network administrators scanning their network for a network interface device operating in promiscuous mode is another method of detecting potential threats.

Promiscuous mode is where a node on a network accepts all packets, regardless of their destination address, instead of only the packets addressed to that node. This mode permits passive capturing of packets, some of which will contain passwords and other interesting data. If a network interface device operating in the promiscuous mode is coupled with a program to select specific packet types, then the network could be said to have been invaded with silent termites chewing away at the infrastructure.

The typical user workstation should not have this mode set. One tool that can be employed to ferret out packet sniffing promiscuous mode network cards is AntiSniff by Security Software Technologies Inc. AntiSniff works by running a number of non-intrusive tests, in three different modes, which can determine whether or not a remote computer is listening in on all network communications. Executing this tool, or others like it, on a routine basis will enable the administrator to keep track of which devices on the network have a legitimate reason to operate in promiscuous mode, and which ones may be a threat.

MONITORING TRAFFIC FLOW TO DETERMINE POTENTIAL MALICIOUS ACTIVITY

Monitoring traffic flow with tools such as tcpdump (or SNORT) can provide clues to unauthorized activity emanating from the inside of the enterprise. Both applications can be set to look at specific protocols, or all traffic. Monitoring traffic flow also provides an opportunity to baseline the network activity and become familiar with what is "normal" on a particular network.

CONFIGURING ORGANIZATIONAL EMAIL SYSTEMS TO BLOCK TROJAN HORSE CARRIERS

Organizational email systems can be configured to prohibit executables or other types of files known to carry malicious payloads from being sent or received. A number of large organizations have started this practice. It may seem intrusive to not allow any .exe files to flow across the organizational email system, but it also is a good way to prevent **an** insider from sending Trojan horses to other users in an attempt to take over their hosts. The remote control tool Back Orifice was once distributed within a "Whackamole" program executable. When the user received this program in email, they would need only to double click on the cute sounding executable to not only play the game, but to install Back Orifice server on their system, making it a slave to an unknown master.

CONFIGURING AND UPDATING ANTI VIRUS SOFTWARE TO DETECT AND ERADICATE UNAUTHORIZED REMOTE CONTROL APPLICATIONS

Finally, a method of detection which should be standard operating procedure on any system is the installation and continuous update of an anti virus program. Current anti virus programs from major vendors such as McAffee VirusScan and Computer Associates InnoculateIT detect the presence of many known Trojans and remote control tools such as the Back Orifice and Sub Seven servers. As a

last line of defense, these programs can protect unwary users who may be targeted as remote control hosts. The key is to continuously update the anti virus signature files to ensure adequate protection against the latest variant of malicious code.

To achieve termite control for long periods of time, termiticides must be applied as a continuous chemical barrier in the soil and adjacent to the foundation, to prevent termite travel from their nest in the soil to the wood in the house. Failing this, reinfestation by termites traveling through untreated gaps is practically a given.

Unlike the scenario to use termiticides to keep termites outside the area they wish to invade, defending an organizations network from the inside needs to focus on keeping the insider threat inside, and rendering them harmless. Failing this, the insider with malicious intent is permitted to travel around unprotected network segments, wreaking havoc.

List of References

1. Shripat T. Kamble, Extension Specialist, Pesticide Impact Assessment, "Termites" Cooperative Extension, Institute of Argriculture and Natural Resources, University of Nebrasks-Lincoln,
Electronic version issued October 1995
URL: http://www.ianr.unl.edu/pubs/Insects/g1062.htm#evidence (3/20/01)

2. Orkin Corporation "Orkin Bug Guide"
URL: http://www.orkin.com
(4/12/01)

3. Eric D. Shaw, Ph.D., Keven G. Ruby, M.A. and Jerrold M. Post, M.D. Political Psychology Associates, Ltd. "The Insider Threat To Information Systems" Reprinted from *Security Awareness Bulletin* No. 2-98, published by Department of Defense Security Institute, September 1998
URL: http://www.smdc.army.mil/SecurityGuide/treason/Infosys.htm#1. (3/20/01)

4. Verton, Dan, "FBI Spy Case Highlights Insider Threat to Corporate Data" Computerworld, February 21, 2000
URL:
http://www.computerworld.com/cwi/story/0,1199,NAV47_STO58062,00.html
(4/15/01)

5. Computer Security Institute, "2001 Computer Crime and Security Survey" March 12, 2001