Global Information Assurance Certification Paper

SANS Security Essentials GSEC Practical Assignment
Version 1.2f

Information Technology Department Network Security Briefing
Thad Nobuhara
December 27, 2001

When I started my career in Information Technology (too many years ago to mention), the corporate network at the company I was working for consisted of private leased lines to other cities within the United States. There was a single production mainframe computer that basically only had two types of devices that it communicated with, dumb terminals and printers. Security was straightforward, physically protecting the mainframe computer and peripherals was the most important item.

Today it's a totally different story. The Corporate Network at our company consists of communications to our field offices, employee home offices, 3rd party offices, and employee mobile (dialup and broadband) offices running a virtual private network (VPN) over a public network (the Internet). We also communicate with other 3rd party organizations over various Frame Relay (semi-public) networks. The devices connected to our network are no longer just dumb terminals and printers. For example, we also have servers, routers, switches, VPN gateways, firewalls, desktops and notebooks. In terms of security, the most dangerous of these devices are the notebook computers. Our road warriors connect their notebook computers to the Corporate Network directly, their home network, hotel networks, and in a substantial number of cases they connect to various customer networks. Additionally, wherever our Corporate Network touches another network, whether it is a home office, mobile office, or 3rd party network, there is a security concern caused not only by the remote network, but also by computers and networks that are attached to that remote network.

Because like most organizations, we use the Internet as a communications vehicle, we now have to protect each and every connection to the Internet from potential attacks. For the main office and field offices, a high level of security can be achieved since these connections are static and are actively maintained by the Information Technology (IT) Department. For 3rd party offices, a medium to high level of security can be achieved since most organizations take network security as an important aspect of their job. However, they may not have the proper level of funding to maintain a high level of security. It is important to note that every connection that the 3rd party offices utilize to the Internet is a potential security breach, and therefore the security of our network can be affected. As for employee home offices, the range is from low level to a high level of security. For the employee that follows the standards and guidelines and properly use our recommended security products (such as virus software, hardware firewall, software firewall), high security can be achieved. There will always be employees that do not follow the standards and guidelines, and we must recognize this and be prepared for this security issue. That is why it is important to automate the

maintenance of whatever security mechanisms are in place. Currently this is not completely possible, and even when it can be done, there are still security issues. One example is although our virus software automatically distributes virus updates, what if an employee is never connected long enough to receive the latest update and becomes infected from a customer network? Another concern is that it is quite simple for an employee to take their notebook computer and connect to a friend's or hotel's unprotected network, allow the notebook's personal firewall to accept traffic from the local subnet, and access our company network. As mentioned before, the danger whenever you connect to an unknown network is that it may already be compromised, and the notebook computer can be compromised, and next our Corporate Network can be compromised.

Intrusion Detection Systems (IDS) are another tool in defending against attacks. IDS plays a role in addressing not only external attacks, but internal attacks as well. Although IDS plays an important part in the security of our network, it is outside of the scope of this briefing, and will not be discussed in any detail.

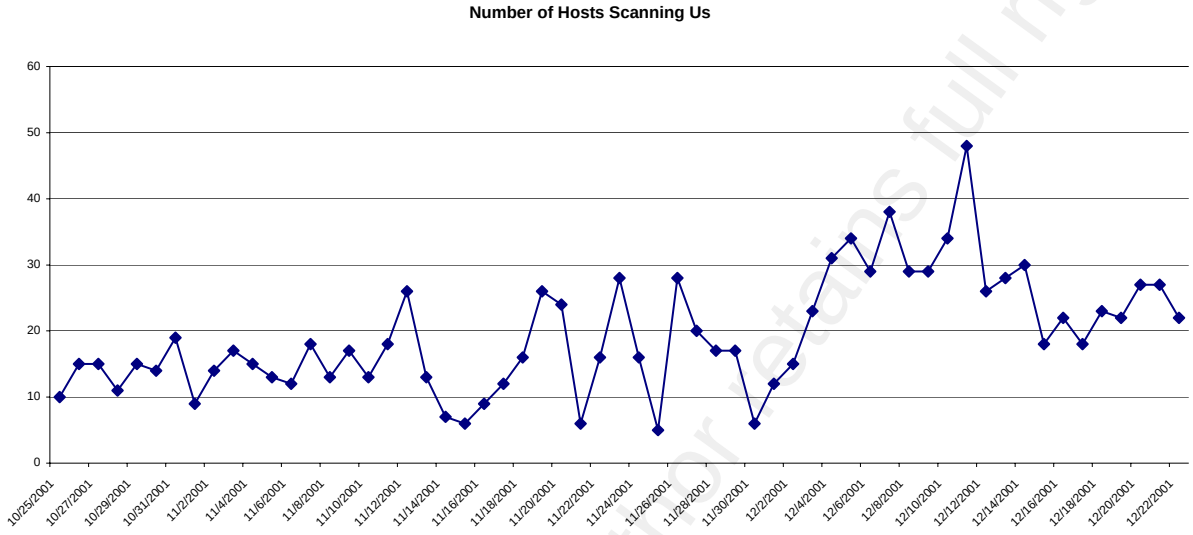
A Frame Relay connection to 3rd party network is generally highly secured. The major providers do an excellent job in limiting access to only the network a customer should have access to. However, since it is a connection to another network, there is a concern on the security relationship that the 3rd party has with other companies and the Internet.

In the case of our company, we have over 500 notebook computers that access the Corporate Network from various connection environments. These computers are taken from the office to the home, to a hotel in various states, and some are even taken to different countries. The employee requires Corporate Network access from all of these locations. In order to meet the communications requirements, the Internet is used as a transportation vehicle. Now with always on broadband access from almost anywhere, our network extends to many locations. This gives the hackers a target rich environment.

In the FBI/CSI 2001 Computer Crime and Security Survey, it cites that 85% of the respondents detected computer security breaches within the last twelve months. The most frequent point of attack was their Internet connection (70%). This number was only 59% as reported in the year 2000. Also, 64 percent of the respondents reported that they experienced unauthorized use of computer systems within the last 12 months, and 11 percent stated that they did not know if there was unauthorized use within the last 12 months.

As an experiment to highlight whether unknown hosts are looking at our Internet connection, I placed a personal computer running a popular personal firewall software on the outside DMZ of one of our T1 connections we utilize. Please note that the only other device on this connection is a VPN gateway. Also note that both devices on this

subnet are not listed in any external DNS, and therefore the unknown hosts that scanned this network only found the host by scanning, and not by first identifying the host by using their DNS name.



First of all, shortly after placing this computer on the DMZ, the scanning began. As you can see, the number of hosts that are scanning the test system is continuous and increasing. Over the period of the 59 days that this experiment was run, there were scans from 733 unique IP addresses, which averages to almost 13 a day. There is no reason for anyone to scan the test host other than for potential hacking. This limited experiment shows that there are people scanning the Internet for hosts that respond. This is one of the first steps in hacking.

One of the questions that I repeatedly get asked is that we have nothing of real value, and therefore why would a hacker want access to our network. The experiment shows that there are persons that scan for IP address of any hosts that respond. These people did not first look for us based on our domain name. It is easier to scan by blocks of IP addresses looking for hosts, than to look for domains to scan (unless that you are specifically going after a certain organization). It doesn't matter why a hacker wants access, it is more than likely that they want access to any network. If a hacker gains access to a host, they can attempt to gain control of other hosts (whether they are PCs or Servers). Once they have control and even if we have nothing of value, they can use that computing resource to attack others in the world. This could have liability issues for our company.

As stated previously, a goal of a hacker is to obtain control of or compromise one or more computers/networks. They will use the easiest method available to them. In our network the starting point is any host that is directly attached to the Internet. This could be our e-mail server, web servers, VPN gateways, firewalls, and employee computers directly connected to the Internet for the purpose of VPN access. Employee computers are often overlooked, however, with the substantial increase in always on

broadband connections, they become just as important as the traditional network devices. It is extremely important to maintain the patch level of all of the equipment. This includes the operating system and applications loaded on the network device. This is not as straight forward as you would think. Patches are being released by vendors sometimes too quickly. The patch may not close the security hole, the patch may open up a previous closed security hole, and the patch may even cause the device to no longer function. Also you must utilize firewalls to restrict access to only the TCP/IP ports that are required for the network device to perform its function. But of course, this puts another device on the network for attack. Applications and Services must be investigated as to whether they need to be running on the computer. If there are files that are not required, remove them, even documentation files can contain information that a hacker can use. System defaults need to be modified. This includes the administrator id and the default location of directories. Test the hardening process by trying to penetrate the server. Finally, create a checklist as to what steps you took in hardening this application so that it can be repeated and refined over time.

Hackers know that the weakest link in security is the employee, and they try to exploit this in order to obtain any information that will help them find a vulnerability to exploit. This could be through social engineering to obtain userid, password, and other information. This information maybe as simple as the phone number for the help desk, going through trash (called dumpster diving) to look for any information, and scanning newsgroups and other web sites looking for e-mail addresses. This information is used to identify personnel that work at a particular company, their function at the company, and identify products that are used by the company (for example firewall vendors, virus detection vendors). For example, with this information the hacker can look for specific vulnerabilities of the products being used at the company, or they can try to get userid/password information by pretending to be an employee. The best way is to defend against this is to educate the employee not to reveal any information, and to instruct IT personnel not to use their company e-mail address or company name when dealing with newsgroups.

There are so many tools readily available for the hacker. There are multiple sites, with all kinds of information. Here is one example of some of the categories and descriptions for Microsoft Windows. I just did a search on the Internet and was able to locate a web site that lists this type of information.

Category	Description
FLOODERS	Crash computers and networks by sending huge amounts of information to them.
NUKERS	OOB nukers, multi-port nukers, etc. This tools crash computers and networks.
TROJANS	These tools give you full access to the victim's computer if they have a server running.
CRACKING	From password crackers, dial account rippers, bios

	crackers, etc, to password generators, wordlists, etc.
ICQ	ICQ related stuff... Password stealers, ICQ crashers, etc.
NT HACKING	Programs used to hack NT systems.
CRYPTOGRAPHY	Programs concerning cryptography
PHREAKING	War dialers, tone dialers, multi-frequency dialers, cellular phones related stuff, etc.
KEYLOGGERS	Lots of Windows keyloggers. They record every keystroke in one text file.
MAILBOMBERS	This Programs send lots of e-mails to the victim. Some anonymously, others not.
MULTI-TASK	Each of these programs does multiple things. For example, a program can make some Dos attacks, and include a port scanner.
PATCHES	Some files to protect your OS against different exploits or attacks.
PORTING & NETWORK SCANNERS	These programs can scan remote computers for open ports, known exploits, cgi´s, etc. They can also listen for incoming connections, block certain ports, etc.
NEEDED FILES	Dll´s and ocx files needed by other programs to run.
SNIFFERS	These tools let you monitor and analyze all the traffic that goes through an Ethernet card. They can be used to detect bugs or making an attack plan.
SPOOFERS	Programs that let you hide or change you real ip, identd on ftp and irc sessions, etc. As for DOS programs, UNIX tools are much more effective.
CARDING	Programs that let you fake or counterfeit different credit cards numbers
OTHER TOOLS	Other programs not included in any of the other sections. Pagers, hex editors, etc

Hackers are getting smarter. Each day there seems to be a new vulnerability discovered in some piece of equipment. Hackers are getting younger. An example is the Goner worm. It was written and distributed by four teenagers (ages 15-16). Hacking is getting easier. There are web sites that will teach you how to hack. Like I mentioned before, the tools are easy to obtain. Hackers are expanding their horizons. No longer are hackers attacking mainly servers and desktops, there have been attacks on routers, printers and even cell phones. I am strongly convinced that no matter what device you have, there is someone writing a piece of code to attack it.

What are the steps that need to be accomplished to defend against this? Securing our network, which is also training the employee in addition to devices, can be broken down into four phases.

1. Identification
2. Preparation
3. Monitor
4. Response

These phases continually repeat from Identification through Response. In addition, some phases repeat within themselves, such as Preparation. What I mean is that once you feel that you have prepared to prevent an attack, after a certain period of time, probably measured in hours, you need to re-investigate and re-prepare to ward off any new attack techniques. Security is never ending. It requires vigilance on an hourly basis. You need to have a certain level of regard for hackers and consider them as members of a huge organization, not just as individuals. The members range from newbies (entry level) and script kiddies to the elite. We need to be prepared for all of the members. Don't kid yourself, they can all do damage. And the damage doesn't have to be intrusive, it could just disrupt communications to a server that the affects our employees or customers.

Before we can protect our assets, we must first identify the assets in order to determine our vulnerability. It is important that not only the technical aspects are investigated, but also the social aspects as well. The business continuity plan will identify the risks that our company is willing to take regarding data, resource availability, etc. With this knowledge we will have the first steps in the risk assessment. The next step is to determine if the current physical security of the network is sufficient. All of the computing hardware, from the servers to the networking equipment and even to some critical desktops should be reviewed. Additionally, the inventory of this equipment must be kept up to date, and the patch levels maintained and documented. I believe that continuous documentation is the most important step in the identification phase. If we do not know what equipment we have and what patch levels are on the equipment, we can not be on top of protecting that equipment. Another important consideration is the personnel requirement. We must identify and maintain a certain level of personnel and skill sets at all times to properly handle any attack.

Like a lot of things in life, it is better to take preparatory steps regarding an event, rather than to spend your time dealing with the fallout caused by the event. In terms of security, this is extremely important. The best way to deal with preparation is in training. Every employee needs to understand that it is up to them to assist in the protection of the corporate assets. The IT staff needs to be educated on the additional security responsibilities that they have. They must understand that they have a master key to a lot of the corporate resources, and they must keep security in the forefront

when dealing with anyone, whether it is another IT member, employee or outside vendor.

We must document the network, and understand the heartbeat of the network (baseline). A network sniffer will provide valuable information. With this information we will be able to become aware if something looks out of the ordinary. Intrusion Detection Systems will help in identifying whether you are under attack or not. These systems will help in reducing the volume of data that is collected (for example in log files). However, you must spend the time each day in reviewing what the IDS has detected and see if things you know of were not detected.

Other things that can be done to prepare are to put in place a system to identify if others are doing any sort of sniffing of the network. This would be a trigger that unauthorized activity is occurring. Additionally, authentication systems need to be reviewed and improved. How is a lost or stolen notebook reported to the IT Department? This needs to be specifically identified so that the appropriate action is taken.

So what do we do if we have an attack? The proper response is that we need to isolate the device from the production network. This means that it needs to be removed. The last thing you want is for this system to spread the attack to another server, or even worse another server not at our company. We will need to quickly identify the problem, and find a fix (whether it is from the vendor, or just a workaround that was created in-house). Then you need to confirm that none of the similar equipment has been attacked. Once that happens, you can do more extensive research into the original attack. Again, the goal here is to fix the problem and return the device into service to minimize downtime. Whatever the solution is, make sure that the information is disseminated to the rest of the team, and the Help Desk is notified if employees need to be warned of this type of attack. Make sure you document what was discovered and use this information to assist in preventing future attacks, and also in your request for funding of other security projects. But the last thing is what not to do. You should not try to attack the perpetrator. The owner of the host that attacked you was probably not the attacker, the host was compromised, and acted as a zombie in the attack. Even if you were able to properly identify the hacker, you do not want to attack the hacker, because they will treat it as a challenge, and they have a lot more time on their hands to strike back. The correct process would be to follow the approved plan for attack resolution outlined by the company.

In conclusion, the corporate network over the years has gone from a simple and controlled environment, to an extremely complex environment, and now to a hostile environment. This is largely due to all corporations having one or more connections to the Internet. We can no longer rely on ignorance as one level of security. We must maintain an active role in protecting not only our Internet exposed devices, but also all devices on the corporate network, including employee personal computing devices.

This can no longer be the sole responsibility of the Information Technology Department. It requires employee involvement at all levels and by even employees that do not have access to computer. In order to protect all corporate assets, we must educate the employee to prevent them from being a victim of social engineering. Another danger today is that everyone with a computer and an Internet connection considers themselves an expert. They make configuration changes, download patches, and upgrade software without the proper considerations, never mind standards and licensing issues. If this person is an employee, you have a potential problem. If this person is a non-employee that exchanges electronic information or just on a common network with an employee, you have another potential problem.

We must also put in place detection systems to expose attacks when they happen. This is not limited to the devices at the fixed sites, but also the notebook computers. We need to monitor e-mail servers to look for sudden bursts of activity that may reveal an attack or even a hoax attack or a hoax response. There must be a written policy that addresses break-ins and the required action. We also need to have systems in place to record everything, and quickly escalate to upper management in the event of a break-in. We also need to continuously review the processes and refine them over time.

Business continuity becomes even more important to our organization in this environment. If a hacker succeeds in disrupting our business (whether it is done directly or the use of a virus or worm), a quick recovery is the only solution to reduce lost productivity and financial loss.

Because of our links to 3rd party organizations, the corporation needs to investigate risk management. The major question is that how does our corporation respond to attacks that are launched coming from and to 3rd party organizations.

We must be relentless in regards to security. The weakest link may have a significant detrimental impact to our organization. It may even put us out of business.

Finally, if you're scared now, wait until tomorrow … then you'll really know what scared is.

Bibliography

Coffee, Peter (2001) 5 Steps to Enterprise Security – Step 1: Assessment, eWeek Labs, www.eweek.com/article/0,3658,s%253D25132%2526a%253D17878,00.asp, November 14, 2001.

Coffee, Peter (2001) 5 Steps to Enterprise Security – Step 5: Vigilance, eWeek Labs, www.eweek.com/article/0,3658,s%253D25132%2526a%253D19720,00.asp, December 10, 2001.

Computer Security Institute (2001) Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar, *Computer Security Institute Press Release*, www.gocsi.com/prelea/000321.html, March 12, 2001.

Computer Security Institute (2001) 2001 CSI/FBI Computer Crime and Security Survey, *Computer Security Issues and Trends*, Vol. VII, No. 1.

Crume, Jeff (2000) *Inside Internet Security What Hackers Don't Want You To Know*. Addison-Wesley. ISBN: 0-201-67516-1.

Dyck, Timothy (2001) 5 Steps to Enterprise Security – Step 2: Prevention, eWeek Labs, www.eweek.com/article/0,3658,s%253D25132%2526a%253D18257,00.asp, November 12, 2001.

Infosyssec (2001) Hacking – How it's done & Tutorials, Infosyssec, www.infosyssec.net/infosyssec/hackhow1.htm, December 1, 2001

Infosyssec (2000) The Best of the Best Hacking Download Sections on the Net, Infosyssec, www.infosyssec.net/infosyssec/tools2.htm, April 21, 2000

McCarthy, Linda (1998) *Intranet Security Stories From The Trenches*. Sun Microsystems Press. ISBN: 0-13-894759-7.

Perera, Rick (2001) Brief: Israeli youths admit to creating 'Goner' worm, Computerworld, www.computerworld.com/cwi/story/0,1199,NAV47_STO66492,00.html, December 10, 2001.

Rapoza, Jim (2001) 5 Steps to Enterprise Security – Step 4: Response, eWeek Labs, www.eweek.com/article/0,3658,s%253D25132%2526a%253D19366,00.asp, December 3, 2001.

Sturdevant, Cameron (2001) 5 Steps to Enterprise Security – Step 3: Detection, eWeek Labs, www.eweek.com/article/0,3658,s%253D25132%2526a%253D18957,00.asp, November 26, 2001.

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS