GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Charles Coffey
October 3, 2001
SANS Security Essentials
GSEC Practical Assignment
Version 1.2f

Information Warfare – It's Everybody's Battle

There's a war going on, and it's all about your computer. If it's not about your computer, then it's about mine, and I don't like it…

Major companies and government agencies have been fighting a vicious battle for years to defend their automated information systems. A constant bombardment by viruses and hackers, combined with headline grabbing accounts of spies and espionage, have led to the upsizing of computer security departments all over the globe. As the Plant Computer Security Officer and Incident Coordinator for a three-letter government agency, I have seen the attacks, and have personally cleaned up the damage caused by a variety and multitude of those attacks. Granted most of my clean-ups are from viruses, but the threat of intrusions and account compromises is always present.

Cisco Systems has long been the leader in networking for the Internet. Cisco Systems says:

> *"When you connect your private network to the Internet, you are physically connecting your network to more than 50,000 unknown networks and all their users. Although such connections open the door to many useful applications and provide great opportunities for information sharing, most private networks contain some information that should not be shared with outside users on the Internet. In addition, not all Internet users are involved in lawful activities".*

As the attackers crash against our defenses, the Computer Security Group at my company is working side-by-side with other computer security professionals and government agencies to build a network of organizations to collect information on the attacks, analyze the data, and distribute the findings. For security professionals the information gathered is priceless in bolstering our defenses.

One of these organizations, the Computer Security Institute, conducts a yearly Computer Crime and Security Survey. The findings are staggering; they receive "*responses from 538 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities".* The one statistic that jumped out at me was:

> *"For the fourth year in a row, more respondents (70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%). Indeed, the rise in those citing their Internet connections as a frequent point of attack rose from 59% in 2000 to 70% in 2001".*

© SANS Institute 2000 - 2005 Author retains full rights.

Groups such as CIAC (Computer Incident Advisory Capability) and SANS (System Administration, Networking, and Security) publish frequent warnings on cyber attacks and known vulnerabilities. These groups define the known problems and often provide patches and resources to plug the gaps in our networks.

What is the motivation of these attackers?

Carnegie Mellon University operates the Software Engineering Institute, a federally funded research and development center. The Software Engineering Institute studies Internet security vulnerabilities through an organization called the CERT Coordination Center (CERT/CC). In an article on "Security of the Internet" the CERT team wrote:

> *"It is difficult to characterize the people who cause incidents. An intruder may be an adolescent who is curious about what he or she can do on the Internet, a college student who has created a new software tool, an individual seeking personal gain, or a paid "spy" seeking information for the economic advantage of a corporation or foreign country. An incident may also be caused by a disgruntled former employee or a consultant who gained network information while working with a company. An intruder may seek entertainment, intellectual challenge, a sense of power, political attention, or financial gain".*

There are many methods of attack. Certain tools can be used to access what's on your computer, while others blindly damage any computer they can. The attacker can be halfway around the world or working in the next cubicle. The method used depends on the objective, and it doesn't always have to be with "Mission Impossible" technology.

I'd like to focus on two incidents. The first highlights an external attack, and the second highlights an internal attack, both are Account Compromise type situations.

Scenario 1

The IT management at *Company ABC* does not define a policy for Instant Messaging because several vice presidents use ICQ instant messaging to keep in touch with friends and associates at different sites. Therefore, if the executives of the company can use ICQ, so can the rank and file employee. It is discouraged, but most employees know it is allowed.

During a day of conducting routine computer assessments, a Computer Security Officer and I made an unannounced visit to a well-known supervisor's office. We politely requested to do an assessment of his computer, and the supervisor readily agreed. As I inspected the computer, my associate conducted an Assessment Interview with the supervisor. First, she verified the information we have on file concerning the user, location information, and hardware and network configuration. After that she started asking our standard assessment questions:

1. Is your computer training current? Including yearly awareness training? Do you understand the training? The replies were all yes.

© SANS Institute 2000 - 2005 Author retains full rights.

2. Are you aware of the computer security requirements for your system (e.g., password protection, screen saver, banner message)? The replies were all yes.

It is important to note here that the computer displays a clear message banner that warns the user the computer belongs to the Federal Government, it is for official work purposes only, it's use is monitored, and there is no expectation of privacy associated with it's use. It states that any information gathered can be shared with any law enforcement agency the company deems necessary. When you logon you agree to the terms on the banner.

3. If required, are media and hardware properly marked? The replies were yes.
4. Are adequate controls in place to protect information (administrative, physical, personnel)? The replies were all yes.
5. Do you maintain current virus software, and do you perform checks on all new disks or files? The replies were yes.
6. Do you the system owner have a software inventory available for review? The reply was yes.
7. Are backups created and maintained for the system? The reply was yes.
8. Is the system clear of fraud, waste, and abuse? The reply was yes.

As the user replied to the questions, I noticed several freeware programs in the computer's directory structure, such as streaming media and music players, search bots, and ICQ.

ICQ was running and the user had been chatting, using the companies Internet connection. A closer look at the ICQ folder revealed a folder called "Downloads". This folder was divided up into sub-folders according to female screennames, and each of those folder contained jpeg format pictures. I opened the graphic file viewer Irfanview, version 3.33. This viewer will run from the floppy drive. I opened three of the jpegs found in the first folder. The first two were photographs of a female adult, the user said he did not know her personally, but chatted with her occasionally. The third picture was a pornographic act featuring the female.

I minimized the picture and asked if he had seen that picture before, and he replied yes he had. I asked if he had saved that picture to his hard drive, he replied no he did not. He stated that the lady had sent him the pictures, and he didn't realize when she sent them that one would be pornography. He also said he did not realize that the pictures would be saved on his hard drive.

I asked if he felt the other folders contained similar files? He said that other people had sent him "dirty pictures" using ICQ, and that he had viewed them. So yes, he figured there probably were more pictures in the other folders.

My initial assessment was: This is an Incident.

I disconnected the Ethernet cable from the computer and informed the user that I was beginning an inquiry into this incident, and informed him we would appreciate his full cooperation. He agreed, and asked what would happen next.

© SANS Institute 2000 - 2005 Author retains full rights.

I told him the procedure was to discreetly inform his supervisor that an inquiry was in progress, and that I would have to lock his office until I could move his computer to a security area. I told him this was an inquiry on behalf of the company, and it was not a criminal investigation. I told him that I could not and would not share any information concerning the inquiry with his co-workers or supervisor, but other managers would be involved. I told him I would notify my supervisor, the Information Systems Security Site Manager, and I would also inform the manager for Internal Auditing.

The Internal Auditing manager informed the user that the *Company ABC* has a policy against waste, fraud and abuse, which is what he felt this incident involved. He was told that if he cooperates fully with the inquiry, and no law has been broken, he could be given a second chance. (The *Company ABC* has a policy that gives first offenders a "Final Written Notice", but if caught violating company policy after that, he could be terminated). It was the manager of Internal Audit's personal policy not to "send the employee home with the weight of the world on his shoulders".

I assigned the incident a unique number, and started an Incident Data Sheet to record all aspects of the inquiry.

Back at the lab:

1. I made a copy of the hard drive using a program called Ghost.exe. This is the best practice when dealing with an incident; you can inspect the drive contents thoroughly without compromising the integrity of the original drives information. If you find evidence on the copy, that a company policy or even a law has been broken, the original drive can be submitted as not tampered with evidence.
2. I tagged and stored the original hard drive in a locked vault. This is best practice because you need to have a clear "chain of custody" if evidence is found on the copy.
3. I gathered information such as what network resources the user had access to.
4. I noted how many drives, on what servers, the user actually had mapped. Those drives would have to be searched.
5. I checked to see if he shared access to his hard drive with anyone. He had not.
6. I checked to see if he had personal e-mail folders in Outlook. He did, and it was located on the hard drive. No delegates shared any of his e-mail on Outlook.
7. I did an inspection of the contents of the copied disk. In the ICQ folder I found chat log files that showed the user was very active on the chat scene with many people, mostly women, and the chat sessions were all personal, social, mostly with strangers, and mostly attempts to have erotic sessions with women. It was also obvious the user knew he was receiving pornography during his chat sessions. The user had received a lot of porn pictures, dirty jokes, electronic games and greeting cards.
8. I found several cases of Adware running, such as Whagent.exe, Qttask.exe, and Wnap.exe. I call them Adware, while others call them Spyware. These are programs that load with other software and collect information to send back to the parent company.

   Gilles Lalonde is with a Computer Security Company called Infoforce, Gilles says:

© SANS Institute 2000 - 2005 Author retains full rights.

"I find the use of Spyware a despicable action. ***"Spyware"*** *is ANY SOFTWARE which employs a user's Internet connection, without their knowledge or explicit permission, to collect information. That these information be personally identifiable or not is of no avail. ".*

In these trying times I don't think any IT manager would want a back-channel "information" paths open.

9. I found a zipped file in an ICQ downloads subfolder. I unzipped the file called BDDancer.zip and found four files that unzipped along with a file called Birthday Dancer. The greeting card file containing a cute animated dancer. The other four files were Starrcmd.exe, see32.dll, wsys.exe, and wsys.dll. Starrcmd.exe was a Spyware program from a site called www.iopus.com. Luckily for my user, the person who zipped the files didn't know how to direct one the files to the needed directory to operate. It wasn't configured correctly and wasn't functioning. The e-mail tab inside Starrcmd.exe had been configured for an e-mail account provided by a well-known web portal. The target e-mail address was plain-text, but the password was encrypted. After visiting the Iopus site I found they had a freeware program that recovers passwords. It worked well. The user had transferred the zipped file that contained the Spyware several times to other users at the facility, thinking it was just a Birthday greeting card. The originator of the file was working for a different company at a nearby facility.
10. I contacted my counterpart at *Company DEF* and set up a meeting to discuss starting an inquiry from their end.
11. I tested the Starrcmd.exe program, and when it is configured properly it works well. It has in an invisible mode, it uses Port 25 to e-mail keystroke logs and screenshots, and it can encrypt the data. The Starrcmd.exe is the control panel for the program, and is not required for the stealth monitor (wsys.exe) to operate. Loaded correctly this program could have gone unnoticed for months.
12. As a result of the incident, *Company ABC* realized they had to change their polices against Instant Messaging, downloading of streaming music or radio broadcasts, and web surfing to sites that are not work related. The company's entire firewall policy was reviewed and updated, and implemented. Particular to this incident, all SMTP traffic on Port 25 was blocked at the firewall.
13. I made a final report to management, then labeled and stored the evidence in a secure vault. I closed the Incident.
14. The employee was given a second chance.

Scenario 2

At my facility a much wider range of employees access computers now, than in years past. Security Guards, maintenance personnel, custodians, mechanics and groundskeepers use computers to access Building Directories, Material Safety Data Sheets, Inventory Control, Timekeeping, and Benefits Information. At the same time, what had been a large manufacturing

© SANS Institute 2000 - 2005 Author retains full rights.

plant managed by one company has been converted to an industrial park. The parent company is now in charge of integrating dozens of small companies into the cleanup and re-industrialization of the site. This means the plant infrastructure, including network resources have to be shared. The smaller companies, trying to operate on tight budgets, have a large turnover in their workforce. Add these factors up and it means that more people, on whom very little background information is available, have access to our information systems.

Facts:

1. The group doing our Internet monitoring saw some suspicious traffic going to a computer in a remote part of the plant.
2. The report contained the Domain Name and IP address of the offending machine, plus a listing of the ports used and the sites visited along with the date and times.
3. The computer was register to Ms. Ima Surfer. (the name changed for privacy reasons).

My initial assessment was: This is an Incident.

1. I analyzed the report and determined the activity lasted several hours, late at night, and it appeared to all happen on one computer. The only port involved was port 80, HTTP traffic.
2. I gathered additional information such as who was the registered owner of the computer; location of the computer; who the supervisor for the group that occupied the area where the computer was located; the users network access; and the network configuration information of the computer.
3. I categorized it as a waste, fraud and abuse case, and a potential Account Compromise case. I notified the Information Systems Security Site Manager, who sent me on to the Manager of Internal Auditing.
4. The Internal Audits Manager told me that since neither the computer owner nor the computer had access to classified information, we should monitor things for a few days and establish a pattern of activity.
5. I assigned the incident a unique number, and started an Incident Data Sheet to record all aspects of the inquiry.
6. Four workdays later the Internal Audits Manager, a Computer Security Officer and I visited the area supervisor. We were informed that the owner of the computer worked only the day shift and that nobody else used any part of the area at night. Even the janitors worked the day shift.
7. I introduced myself to the computer owner and informed her that I suspected someone was using her computer at night and asked if I could perform an assessment on it. She readily agreed, and as I inspected the computer, my associate did an Assessment Interview with her. A few people recognized us as computer security officers and were hovering in the hallway trying to listen. We politely informed them we needed a little privacy and they went back to their offices.
8. We determined she was the owner, it was the correct computer, the cache files did contain pornography, and the dates and times in the browser history log matched our records. There was no boot-up password configured. You could cancel past the (Windows 95)

© SANS Institute 2000 - 2005 Author retains full rights.

logon screen and gain default access, which included browser access to the Internet. The inner office door was left open at night and Ima had occasional found used sandwich bags and candy wrappers in her trashcan some mornings when she arrived at work.

9. We inspected all of the computers in the area to make sure no other computers were involved, and they weren't. *This also took the pressure off Ima by not singling her out.*
10. We took Ima's computer for evidence and had it replaced. We also asked the workers in the area not to discuss our visit with anyone, and all agreed.
11. Protective measures were implemented in the area. We requested that the occupants begin locking the inner office doors at night. We had boot passwords installed. We had the registry in the Windows 95 computers configured to not bypass the logon screen. This is done by modifying the registry entry [HKEY_LOCAL_MACHINE\Network\Logon] to logonvalidated"= 10 00 00 00.
12. Because there is very limited access to that area of the plant at night, we concluded it was a security guard doing the surfing. Nobody volunteered to confront an armed porn surfer (who knew they could lose their job if caught), so we decided to share the evidence with the Guard Department and let them handle it.
13. I copied the original computer's hard drive using a program called Ghost.exe, and did a thorough inspection on the copied disk. I found nothing unusual.
14. I labeled and stored the evidence in a secure vault.
15. The surfing stopped at the remote site, and porn traffic began showing up at a computer in Guard Headquarters. I started another Inquiry for that.
16. A week later a security guard resigned after being questioned by his supervision on an unrelated issue. The Guard Department said all evidence had pointed to this person. The porn surfing stopped.
17. I made a final report to management, and closed the Incident.

Conclusion

The methods of attack and defense outlined here are important because they remind us of the need to safeguard our data. Protection against Account Compromises depends on the user making good decisions at the source.

These scenarios contained only the potential for a serious Account Compromise, but in the first scenario an attempt was made. Stealth programs that use normal communication channels are some of the biggest threats to our information.

When the supervisor distributed the Birthday Dancer program to his friends at the facility, it could have opened the door for many Account Compromises. Those compromises would have been from an inside, trusted source.

Dorothy E. Denning said in her book, Information Warfare and Security:

> *"Insiders - employees and others in trusted positions within or with an organization - are generally regarded as the greatest threat to an organization's information resources. This is not surprising, as they also have the greatest access to information*

© SANS Institute 2000 - 2005 Author retains full rights.

within the organization. They could exploit information resources for personal gain or sabotage computer systems for revenge. They could unintentionally reveal secrets to contractors, partners, customers, visitors, or outsides requesting information."

Was the second scenario any less a threat because the guard only used the computer to visit pornography sites? NO.

The more the security guard surfed to porn sites, the more vulnerable the information was on the computer he was using. Many porn sites display a welcome banner that asks – *Do you want to see Naked Women?* If you click YES a Phone Dialer program is loaded into your computer and shortcuts are placed on your Desktop, Start Menu, and in the Directory Structure. Delete these links and reboot, and they reappear. Often these files are loaded into System Files to reload themselves. The site can modify your browser's Home Page, and links can be placed in your browser's Bookmarks. If these sites can do this much when you click YES, why couldn't they do the same things when you click NO, or when you click the famous ANY button. And couldn't they download any piece of devious software they want to? Sure they can.

The best defense against any attack is regularly assessing your vulnerabilities, develop effective measures that build layers of protection, secure management approval, and implement the plan. Follow that up with user training, periodic user awareness training and interaction with computer security professionals and organizations.

References

1. http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/security.pdf, Security Technologies, Chapter 47, Internetworking Technology Overview, June 1999.

2. http://www.gocsi.com/prelea/000321.html, "2001 Computer Crime and Security Survey".

3. http://www.cert.org/encyc_article/tocencyc.html, Security of the Internet, Published in The Froehlich/Kent Encyclopedia of Telecommunications vol. 15. 1997, pp. 231-255. Authors: THOMAS A. LONGSTAFF, JAMES T. ELLIS, SHAWN V. HERNAN, HOWARD F. LIPSON, ROBERT D. MCMILLAN, LINDA HUTZ PESANTE, DEREK SIMMEL.

4. http://www.infoforce.qc.ca/spyware/, Gilles Lalonde, Infoforce.

5. Information Warfare and Security, Dorothy E. Denning.

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS