Global Information Assurance Certification Paper

Option #1 Illustrate an Incident
GIAC Advanced Incident Handling and Hacker Exploits
Practical Assignment for SANS GIAC examination

January 16, 2005

John Adamczak

""

Table of Contents

Introduction

The information you are about to read relates to a large financial company that was in the early stages of developing an information security effort. Therefore this company did not have intrusion detection systems completely implemented. Their information security effort consisted of three distinct disciplines that were evolving simultaniously. The three disciplines were:

- Developing and strengthening policies and standards;
- Creating a Security Awareness Program; and
- Implementing procedures to monitor and report compliance with the policies and standards.

Sr. Management for this company endorsed and supported the information security effort, however they were sometimes tentative about purchasing information security software since the "total cost of ownership" associated with implementing and maintaining these products is high. As a result, the information security department had to "encourage/sell" the purchase of information security software at every opportunity. In addition, Sr. Management believed that the major information security threats came from outside of the company – external hackers. Therefore the information security department also had to "educate/inform" Sr. Management about how a majority of the computer hackers are people who are granted access to a computer system (insiders).

This document contains a scenario where a violation to the company's policies and standards lead to the detection of unauthorized access by an employee into another employee's desktop computer and information. It also tells about how this situation was used to "sell" the implementation of information security software and educate the Company's Sr. Management. The names and dates were changed to sanitize this information.

Executive Summary

On February 2, 2001 we identified a violation to our company's policies and standards that lead to the detection of unauthorized access by an employee. This is not an unusual occurance as stated in the following CSI/FBI survey.

Based on responses from 643 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the findings of the "2000 Computer Crime and Security Survey" confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting…….(it is also important to note that)….Seventy-one percent of respondents detected unauthorized access by insiders. ….. **2000 CSI/FBI Computer Crime and Security Survey,"**

Problem

A company employee, with a high level of access privileges, inappropriately used these privileges to surf and downloaded games, harassing and pornographic information from nonbusiness related Internet sites. The employee sent this information to other individuals inside and outside the company. They also downloaded several hacker related tools found on the Internet.

Our company received several viruses as a result of this employee's computer behavior. These viruses were identified and innoculated without harming our company's network and information. We had appropriate virus protection installed and regularly updated this virus protection.

However we were not as fortunate when it came to the hacker tools. The hacker related software that was downloaded from the Internet included keyboard monitoring, wipe software programs and computer software that would allow the user to increase their access privileges on the companies computer systems.

Keyboard monitoring programs are only used for two purposes:

- To determine if someone is using you computer when you are not around the computer; or
- To gather information entered into another persons computer[1].

Wipe programs are used to permanently destroy any deleted evidence that may exist on a computer after it has been erased.

Finally, computer software that would allow the user to increase their access privileges on the companies computer systems allows an individual to preform functions or get information that they normally should not access.

Summary

Eventhough we were very fortunate to have a good virus infrastructure designed and implemented to prevent the viruses from harming our systems, this and

[1] For example, a person, if they have appropriate access, could load this program on another individual's computer and get the individual's user identifications and passwords using this software application.

similar situation do expose our company to potential legal descrimination[2], harrassment[3], offensive content[4], defamation and libel[5], copyright and other intellectual property infringement liability[6], information leaks[7], malicious virus attacks, lose of sensitive/confidential information and hacker attacks.

Recommendation

We must become more proactive and reactive by implementing proper information security software to identify these type of inappropriate behavior. Below is a list of the proactive and reactive procedures and software we need to implement to reduce these exposures:

1. Intrusion Detection Systems since it helps to:
    - Detect unauthorized use of information and Information systems
    - Continuously monitor authorized users actions
    - Notify us when unauthorized users attempt to access or use Company's information resources
2. E-mail and Web surfing monitoring since they help to decrease:
    - The Company's legal risk from sexual harassment or discrimination litigation and the bad publicity associated with these legal cases
    - Loss of confidential company data and intellectual property
    - Inappropriate use of technical assets

---

2 A Federal court in New York has allowed a class-action discrimination suit based on racist e-mail. The defendant is a large Wall Street brokerage firm and the plaintiffs are seeking $60 million in damages. (Owens and Huttons v. Morgan Stanley & Co., Inc. Case No 96 Civ 9747)

3 Chevron settled a sexual harassment lawsuit for $2.2 million over e-mail postings such as:"25 reasons why beer is better than women." (Jerry Adler, Newsweek, "When E-mail Bites Back," Nov 23, 1998)

4 The New York Times dismissed 23 employees at an administrative center for violating the company's e-mail policy regarding "offensive or disruptive messages, including photographs, graphics and audio materials." (Staff Writer, NYTimes, December 1, 1999)

5 An insurance company was sued for circulating an e-mail that accused an employee of using here corporate credit card to defraud the company. (Meloff v. New York Life Insurance Co. 51 F.3d372 (2nd Cir. 1992)

6 *Time*, August 14, 2000 — "In 1995 Chevron Corp. paid 2.2 million to four female employees who asserted that they had been sexually harassed because of jokes sent through the company network. For abuses to end, snooping proponents argue, monitoring must take place." http://www.time.com/time/magazine/articles/0,3266,52098,00.html

7 Employee E-Mail Leaks Company Secrets--April 21, 2000 --
As if corporate computer security managers didn't have enough to worry about from disgruntled former employees, a new study finds a marked increase in the number of employees who acknowledge receiving confidential information via e-mail from employees at other companies. http://www.computeruser.com/news/00/04/21/news3.html

Description of the 6 stages of incident handling

Preparation:

The company had policies and standards established and communicated them in the following manner:

Policies and standards:

A General and Electronic Communications Security Standards that stated:

> … Files containing inappropriate material are not to be stored in or brought into the Company's computing environment. ***(General Security Standard)***
>
> …….. Employees are to use the electronic communication resources provided by the Company in a proper, ethical manner….
>
> Sending or downloading threatening, obscene, defamatory or offensive messages to others or from the Internet is not permitted. ***(Electronic Communications Security standards)***

Security Awareness Program:

- These standards were communicated to the employees :
  - During orientation
  - Through Information Security Seminars and meetings
  - As a link on the Information Security Web Site
  - As a posted warning banner when an employee logged onto the systems

> Access is given to this electronic network and its resources (collectively, the "Network") for use by Company employees and authorized Company clients. Access by any other person(s) is prohibited and unauthorized. Company reserves the right to access and review all information in the Network at anytime and without any prior notification. Any review of information in the Network will be to protect confidential information, prevent theft or abuse of the Network, to monitor workflow and productivity or for other legitimate business purposes. Personal software, including screensavers, may not be installed onto the Network or any other Company computer equipment. Your use of the Network acknowledges your understanding of and your agreement to adhere to the "Company policies and standards", found in the employees handbook.

Detection:

The information security department first became aware of the potential problem when the employee's supervisor told them that a number of viruses were reported on the employee's machine by the company's anti-virus software.

After talking with the supervisor it was determined that the employee's:

- Work performance decreased significantly over the last two months
- Attitude recently had changed as a result of not receiving an offer for an internal job posting that they felt they should have received.

The information security department also determined that this employee had administration access to the Company's Windows NT workstations and domains.

Incident Response Toolkit

The incident response toolkit consisted of :

- a Dell Inspiron 3800 laptop with a 20GB1 Ultra ATA hard drive and removable floppy and CD drives
- CD-Rom burner
- Software
  - Nmap
  - Internet Security Scanner
- Administrator passwords to every system -- Passwords are kept in sealed, signed, and labeled KeySure boxes
- Corporate phonebook

Containment

After the Information Security Department's (ISD) interview with the employee's supervisor, they determined the information security department needed to gather additional information to determine if a security event(s)[8] had occurred and if this event(s) would lead to an incident[9].

[8] An "event" is any observable occurrence in a system and/or network. Examples of events include: the system boot sequence, a system crash, and packet flooding within a network *(SANS Network Security 2000 – Sunday, October 15,2000 Track 4 handbook --page 5)*

[9] The term "incident" refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such and event. Examples of incidents include: unauthorized us of system privileges, and

Here are the steps the ISD took:

1. They determined and verified which desktop(s) the individual could physically access and what the individual's access privileges were on those and other machines.
2. They searched the Primary Domain Controller (PDC) to determine what was available.
3. They used the SMS installation logs to determine what software was installed on the employees machine and on the machines the individual recently worked on. They also determined what software was updated recently on those machines.
4. A backup image of the individual's system was made using Symantec Norton Ghost software[10]
5. They remotely logged onto the user's primary desktop computer to identify the log files the ISD would use for forensics.

Their investigation determined that the following logs and audit trails were available. In addition the ISD identified the following information was contained in the logs and audit trails.

- Internet history
  - Found over 400 questionable sites visited in the last few months
- Cookie cache
  - Found 6 URLs with suggestive language in the URL
- "Recent" documents used
  - Found a lot of .jpegs and .gif files with suggestive titles
- Favorites
  - Did not find any questionable favorite bookmarks

---

execution of malicious code that destroys data. Incident implies harm, or the attempt to harm. *(SANS Network Security 2000 – Sunday, October 15,2000 Track 4 handbook—page 4)*

[10] At this location, nightly incremental backups of the Windows machines are done using Computer Associates ARCserve products. Employee's PCs are backed up incrementally throughout the week, with full backups done Friday evening starting at 11:00pm.

No problems were encountered while backing up the employee's PC using Symantec Norton Ghost (Ghost information is available in the **appendix**), nor were there any problems encountered restoring files using ARCserve.

- Collected files for the default user and the specific user profile
- Desktop Windows NT Event Viewer

Realizing that the ISD could only do a limited review and might create suspection remotely logging onto the employee's desktop, they decided to ghost[11] the hard drive of the individual's machine to a secured server for additional review. The ISD also captured the current IP address for the desktop.

After analyzing the logs and audit trails the ISD were able to determine that the person's desktop was being used to surf non-business related sites (pornography and harrassment), download games and hacker software.

The ISD now believed that several security events occurred.

Their next goal was to determine if any security incidents occurred. The ISD attempted to accomplish this goal by:

- checking the registry for typed URLs (hkey_local_machine(or users)/software/microsoft/IE/typedURLs) (This would show intent)
- checking the hard drive to determine if the games and hacker software were installed on the desktop computer

They found:

- several inappropriate URLs and access to a free ISP in the employees registry key;
- that the individual used a dial-up free ISP account; (This would allow the individual to go around several of the company's websurfing controls since the individual's machine had a modem attached.)

They then

- Run ISS (Internet Security Scanner) and NMAP against the machine to look for evidence of active/listening trojans
- Checked the task manager / processes for evidence of any questionable processes running
- Checked the recycle bin
- Checked for additional drives

During the analysis performed for this phase the ISD determined or resubstanciated that:

- Several games were installed on the machine

[11] See the appendix for detailed information

- A free ISP's software was installed and functional
- No trojans were running on the machine
- Only company authorized dial-up accounts could be used
- A keyboard monitor was installed and functional
- Files containing the user identifications and passwords were resident on the individual's machine.

Since the keyboard monitor (KM) was installed and functional on the employee's machine, The ISD wanted to determine if it was loaded on any other machines in the company. They uses SMS (Systems Management Server) to help identify which machines had the KM installed. They found that the KM was installed and functional on one other machine --the employee's supervisor machine. Since the KM was just load on the individual's and their supervisor's machine at the end of the individual's last shift, the ISD felt pretty comfortable that they clearly identified the individual's intent for distribution and installion of hacker software.

At this point the ISD felt that they had enough evidence to determine that a security incident had occurred. The ISD based their conclusion on the fact that the employee violated the Company's policies and standards, used their access privileges inappropriately to install software on their and others desktops and appeared to have the intent to to gather and use another user's account privileges.

The ISD then used SMS (Systems Management Server) to determine if any other the machines had the keyboard moniter installed on them. This scan did not identify any additional machines.

The ISD then removed the employee's and the supervisor's Hewlett Parkard Vectra VL P3309 Desktop model, Intel Celeron 700 MHz, 64 MD SDRAM , 10 GB hard drive CD-ROM, 48XIDE from the network and disconnect its 3com US robotics 56k modem. The hard drives from the machines were then placed in "Personal and Confidential" envelops, sealed and labeled with the employee's name, date, and desktop computer number. The "Personal and Confidential" envelops were then locked in a safe that has limited access. Only two individuals from the ISD have keys to the safe.

The ISD updated the company's virus signatures for the e-mail, application, file and print servers and desktop computers and kicked off a company wide virus scan during non-business hours later the same day.

Eradication and Recovery

The ISD placed a new hard drive in the employee's desktop workstation and their supervisor's machines. They also reformatted and installed a fresh image (ghosted) on the supervisor's hard drive. In addition, as a precaution, the ISD

reimaged all of the desktops located it the employee's department. They also forced all of the user's in the department and company to change their password during their next log in.

Follow-up/Lessions learned

On the positive side, the ISD contained the problem in a timely manner. They discussed the computer incident response process and determined that it should be improved to be more effective in future incidents. Also during these discussions, it was determined that the company needed to educate management to quickly spot disgruntled employees and provide them with quick incident response processes to communicate this information to the appropriate personnel. In addition, a committee was created to review and improve the security breach escalation process. Some of the suggestions from the committee included:

- An operations handbook needs to be created that contains:
  - Staffing information - contacts, telephone numbers, FAX numbers, pager numbers
  - Hotline Use - numbers, on-call lists
  - Constituency Communications - procedures for receiving and sending information
  - Incident Reports - incident identification forms, incident survey forms, incident containment forms, and incident eradication forms
  - Computer Equipment – administration policies, configurations, procedures
  - Administrative Procedures – expense reports, travel, security clearances
  - Contacts within investigative agencies
  - Dealing with media – press reports, clearance process
  - Vendor Contacts

Security escalation procedures needed to be clearly documented and communicated to all the computer area.

The incident response toolkit needed to include:

- operating system documentation
- additional security assessment and forensic software (e.g., The Canaudit, Inc., NT Security Forensic toolkit)

Selected members from the ISD and computer areas needed to attend forensic training.

Processes and software needed to be implemented to monitor and report compliance with the policies and standards, such as automated real-time intrusion detection, web surfing and e-mail content monitoring software

Assessment and Containment

During the IDS's review of the event, they verified that the user brought several viruses into the company in a very short period of time. Below you will find information related to some of the viruses and hacker tools brought into the company. You will also see excerpts for some of the logs they reviewed to determine what the employee was doing.

PC-4248:

08/22/2000 7:11AM clubs.yahoo.com/clubs/cuminoraroundwomenshair

08/24/2000 clubs.yahoo.com/clubs/amateurfacialcumshotfanclub

08/24/2000 clubs.yahoo.com/clubs/abi3gal4u

08/24/2000 clubs.yahoo.com/clubs/femalestrapons

08/24/2000 clubs.yahoo.com/clubs/straponsex

08/24/2000 clubs.yahoo.com/clubs/trickponysstraponconnection

08/24/2000 clubs.yahoo.com/clubs/straponformales

08/24/2000 2:21PM clubs.yahoo.com/clubs/theworldofstraponladies

08/25/2000 11:23AMclubs.yahoo.com/clubs/straponloversofrussia

08/25/2000 clubs.yahoo.com/clubs/straponsexzone

10/13/2000 1:43PM clubs.yahoo.com/clubs/acockhungryslutwife

10/13/2000 clubs.yahoo.com/clubs/childhoodfacesitting

10/13/2000 clubs.yahoo.com/clubs/controlledsex

10/13/2000 clubs.yahoo.com/clubs/cumsluttracyanne

10/13/2000 clubs.yahoo.com/clubs/dirtyblonde29slutpics

10/13/2000 clubs.yahoo.com/clubs/drunkassyounggirlsareus

10/13/2000 clubs.yahoo.com/clubs/drunkhornywomenwantyou

10/13/2000 1:52PM clubs.yahoo.com/clubs/lilutheultimatelolita

10/13/2000 2:01PM clubs.yahoo.com/clubs/primproperwifeturnedslut

10/13/2000 2:08PM clubs.yahoo.com/clubs/realdrunkgirls

PC-3148:

10/26/2000 1:13PM clubs.yahoo.com/clubs/shaggysslutwife

10/26/2000 1:14PM clubs.yahoo.com/clubs/primproperwifeturnedslut

10/26/2000 1:16PM clubs.yahoo.com/clubs/girlsforcinggirlstosuckcock

12/6/2000 2:05:42 PM NAV Alert Error Information 33306
COMPANY\USER PC-4138 Virus Detection Event

Item: File

Name:C:\TEMP\kristy.mpeg.exe

Virus: Backdoor.SubSeven

Domain: COMPANY

System: PC-4138

User: USER

Action: Access to the file was denied.

12/6/2000 2:05:41 PM NAV Alert Error Information 33306
COMPANY\USER PC-4138 Virus Detection Event

Item: File

Name:C:\TEMP\kristy.mpeg.exe

Virus: Backdoor.SubSeven

Domain: COMPANY

System: PC-4138

User: USER

Action: Unable to repair this file.

11/20/2000 12:44:55 PM NAV Alert Error Information 33306
COMPANY\USER PC-4138 Virus Detection Event

Item: File

Name:C:\WINNT\Profiles\USER\Temporary Internet Files\Content.IE5\HYXMQ8F1\preeteenhc.jpg[1].exe

Virus: W32.Navidad

Domain: COMPANY

System: PC-4138

User: USER

Action: Access to the file was denied.

11/20/2000 12:44:55 PM NAV Alert Error Information 33306
COMPANY\USER PC-4138 Virus Detection Event

Item: File

Name:C:\WINNT\Profiles\USER\Temporary Internet Files\Content.IE5\HYXMQ8F1\preeteenhc.jpg[1].exe

Virus: W32.Navidad

Domain: COMPANY

System: PC-4138

User: USER

Action: Unable to repair this file.

5/1/2000 4:05:55 AM NAV Alert Error Information 33306
COMPANY\USER PC-4138 Virus Detection Event

Item: File

Name:C:\WINNT\Profiles\USER\Temporary Internet Files\Content.IE5\6GE57TCD\Pretty%20Park[1].exe

Virus: W32.PrettyPark.D.Worm

Domain: COMPANY

System: PC-4138

User: USER

Action: Access to the file was denied.

5/1/2000 4:05:55 AM NAV Alert Error Information 33306
COMPANY\USER PC-4138 Virus Detection Event

Item: File

Name:C:\WINNT\Profiles\USER\Temporary Internet Files\Content.IE5\6GE57TCD\Pretty%20Park[1].exe

Virus: W32.PrettyPark.D.Worm

Domain: COMPANY

System: PC-4138

User: USER

Action: Unable to repair this file.

2/17/2000 1:15:00 PM NAV Alert Error Information 33306
COMPANY\USER PC-4138 Virus Detection Event

Item: File

Name:C:\Program Files\Agent\Happy99.exe

Virus: Happy99.Worm

Domain: COMPANY

System: PC-4138

User: USER

Action: Access to the file was denied.

SCREEN SHOTS CUT OUT

Chain of Custody

As noted above, the employee's hard drive was removed from the desktop computer, labeled and stored in a secured area with limited access. The envelop used to store the hard drive was sealed and signed by the information security manager. His signature was placed across the seal on the envelop to deter tampering (opening) with the envelop.

All of the log files were copied. The original hard drive and copy were hashed using MD5. PGP version 5 was used to digitally sign the MD5 sums for the log files. These MD5 sums were also written in a log associated with the case and physically signed by the information security manager and the staff performing the investigation.

All screen prints, taken during the investigation, were printed. Copies of the screen prints were also placed on a floppy disk. This floppy was encrypted and digitally signed by the information security manager and the staff performing the investigation. This information was locked in a physically secure area with limited access.

Appendix

CD-ROM IMAGE DOWNLOAD PROCEDURES

********** DO NOT USE THIS CD DIRECTLY **********

IT MUST BE USED WITH THE IMAGE LOAD BOOT FLOPPY !!!

****

Files Included on CD-ROM:

* Corporate "C" Baseline Image (CBASE-G.GHO)
* Norton Ghost ver 5.1C (GHOST.EXE)
* Download Procedures (README.TXT)

GHOST.EXE has been included on the CD-ROM for

Emergency Purposes ONLY, when the Server is not available.

How To Create an Image Loader Boot Floppy:

1.) Login to FIINTIMG1\SYSVOL\Images\Setup.DSK

2.) Run the batch file MAKEDISK.BAT <or> type: MAKEDISK drv

Where "drv" is the floppy disk drive

that you want to copy the PC setup image to

Windows NT V4.0
Image Preparation Check List
Prior to Ghosting

Please use this checklist as a guide to tasks that need to be performed prior to creating a copy of an NT image using Ghost or any other disk duplication method.

These items are necessary when preparing a "clean" image for distribution:

- ☐ Clear the Internet Explorer history and cache.
- ☐ Verify that the Exchange/Outlook profile is not defined and no user account created.
- ☐ Clear the "Run" Command line and recently used list by emptying the following key: **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU**
- ☐ Set the Video Adapter type back to Standard VGA.
- ☐ Remove 32 bit test data sources (using 32 bit ODBC Administrator)
- ☐ Remove 16 bit test data sources (using 16 bit ODBC Administrator).
- ☐ Delete all files in the TEMP directory.

- ☐ Delete log files from the **C:\Desktop_Support\LOGS** folder.
- ☐ Delete files from the "Recently used" folder under default user. Make sure the "Documents" folder on the Start Menu bar is empty.
- ☐ Copy the profile used for building the PC to the "Default User" profile.
- ☐ Delete extraneous user profiles (e.g. NTBUILD, NTBUILD-Test, DSCadmin, etc.)
- ☐ Run Event Viewer and check the Event Logs for any unexpected errors.
- ☐ Clear the Event Logs (System, Security, and Application)
- ☐ Empty the Recycle Bin.

These Items MUST be done prior to ghosting ANY image:

- ☐ Delete **`C:\SMS.INI`** and **`C:\SMS.NEW`** – note this is a "hidden" file.
  Note: DO NOT delete the `C:\MS` folder!
- ☐ Run User Manager and remove test and extraneous accounts from the Administrators group.
- ☐ Delete all local drive mappings.
- ☐ Run Disk Administrator and verify that no errors occur and everything "looks" OK.
- ☐ Run REGEDT32 and delete the key **`HKEY_Local_Machine\System\DISK`**
- ☐ Run the Norton Anti-Virus Live Update
- ☐ Perform a Virus Scan.
- ☐ Set the Computer Name to **`PC-0000`**
  (For Baseline Images the computer name is set to PC-BASE-C-rev (e.g. PC-BASE-C-G)).
- ☐ Disconnect from the Domain and join the **`AIS`** workgroup.
- ☐ Delete the network adapter from the Network Control Panel.

When Ghosting:

- **DO NOT copy images to or from the image server from the production network between the hours of 8:00AM to 5:00PM.** Ghosting is permitted in the 7th floor lab at any time.
- Select Maximum Compression.
- Save the image to the appropriate folder on the image server, as follows:
  Baseline Images: \\FIINTIMG1\SYSVOL\IMAGES
  Old Dept. Images: \\FIINTIMG1\SYSVOL\ARCHIVE\Dept_Img
  Old Baselines: \\FIINTIMG1\SYSVOL\ARCHIVE\BaseLines
  Wrks Backup: \\FIINTIMG1\SYSVOL\BACKUP
- Be sure to follow the standard procedures for restoring images.
- Contact Desktop Integration Services (XXX) 288-XXXX if you have any questions.