Global Information Assurance Certification Paper

Windows Forensic How-to: Incident Response Plan for Abuse of Corporate Assets

Joseph Burke

GSEC Assignment 1.4b
February 26, 2003

Contents:

1. Introduction:

I will be explaining the process involved with extracting forensic evidence from a Windows 2000 based machine to prove abuse of a corporate asset. The types of abuse I will discuss include installation of unauthorized software, unauthorized Internet usage, and possession of unauthorized files. I will also discuss ways to discover and track this abuse.

This practical assignment will not be a focused technical discussion on technology alone; it will also include policy, corporate process, risk analysis and other aspects to provide a larger more complete picture of what an investigation entails.

2. Defining what qualifies as abuse using written policy:

An important step in creating a corporate policy for the acceptable use of corporate assets is to create a policy that has received buy-in from executive level staff. A policy that has backing from executive staff ensures that the policy is enforceable across the entire organization. It would also be a good idea to work with your direct manager or supervisor when creating the policy, so that you can have their support when submitting a draft to upper management for approval.

Keep in mind while writing a policy that it is easier to define acceptable use rather than unacceptable use. Also, the systems and applications you use at your corporation today may not be what is in use tomorrow. Therefore it would be wise to broadly define what is considered unacceptable, rather than mention specific technologies and problems of the present time. A basic summary of unacceptable use should include actions that would cause the corporation harm or lost productivity.

The underlying spirit of your policy should be that company owned assets

including Desktop PCs, Laptops, and Handheld devices are for business use only.

Finally, make sure that the policies are stored in a location such as an internal corporate website or network location that all employees can access. Policies are only useful when people actually read them, and have the opportunity to follow them. Having the policies in a convenient and accessible location also allows you to quickly and easily point employees to the policies they need to read, or reference.

3. Detecting Abuse:
There are many methods for detecting abuse of assets, and I have detailed some of the methods in this section. Chances are that many of the methods discussed can be accomplished without purchasing any additional solutions or products.

a. Observations from the help desk - The help desk deals with many different machines and users on a daily basis. During their daily experiences, the help desk may encounter suspicious files or computer activity that could be reported for further investigation. It is important to create a standard procedure for your help desk to follow when reporting possible abuse of assets. A standard procedure will decrease the chances that the incident is mishandled. Any action on, or discussion of the repercussions of asset abuse should be channeled through the suspect's manager, HR contact or other entity deemed appropriate for this purpose. The information technology department should avoid confrontation with the suspect.

b. Virus outbreak monitoring tools - Can be used as a starting point to find the source of infected machines. Depending on the product used, these reports can be drilled into to discover the machine names and folder paths where the viruses reside. The folder paths and files revealed may indicate the installation of unauthorized software or trojan horse programs.

c. Firewall logs - If you have a default-deny (AKA default rule) firewall policy, or have a list of chosen denied outbound ports, the firewall log can be a good source to locate client machines to investigate. Worms, trojan horse programs, file sharing programs and others can be discovered from your firewall logs assuming auditing is enabled, and someone is monitoring the logs.

d. Web filter logs - Can provide reporting data on users that visit questionable sites. This could be used as another lead to a possible investigation.

e. Intrusion Detection Systems (IDS) - Today's worms and malware can sometimes resemble the pattern of a live attacker, and as such are detectable by Intrusion Detection Systems. This occurs because a worm uses the same exploits and vulnerabilities to propagate as a human attacker could use. Therefore Intrusion Detection Systems are another possible way of tracking

worms and malware back to an internal system that may have been abused. There is also of course the ability of an Intrusion Detection System to track internal systems that are attacking using a live operator to coordinate the attacks.

d. Gathering additional information:
After you have identified the source of suspicious activity, you may be able to gather additional information using the following:

-Port scan tools such as nmap or superscan can be used to find open ports that may indicate unauthorized software is running on a remote machine. Make sure you have permission from the appropriate personnel before conducting any scans.

-Windows administrative shares like C$ may be accessible to you, given your job responsibility for Information Security. Through these shares you can search a target machine's disk drive using Windows explorer.

-Systems management and monitoring tools like Microsoft Systems Management Server, or Aelita Enterprise Directory Reporter can search your enterprise systems for specific software or files, and create a detailed report on the machines you are interested in.

Gathering additional information beforehand can save you time and resources by qualifying valid targets without initiating a full investigation. If you require permission to investigate, the extra data gathered can be used to strengthen your case and recommendations.

Always remember that "The difference between a security administrator/auditor and a hacker is permission." (SANS Institute, p.3-30)
Make sure you've covered yourself by getting permission to perform your investigation before you begin. Also be sure to stay within the bounds of your own network and systems when probing to avoid activity against other entities that may perceive your actions as an attack. Lastly, it would be a good idea to have the right to investigate included in your job description and responsibilities. As a rule, you should keep someone other than yourself aware of your investigative activities, preferably your manager or supervisor.

4. Collecting and handling of the suspect's equipment
For the purposes of investigation, the best way to avoid tampering of evidence from the PC you wish to investigate would be to take the machine from the user immediately without any notice. This method of confiscation may work fine for the FBI, but is of course unacceptable in a business environment, and would be likely to result in negative consequences for you and your department.

For the purposes of a more acceptable retrieval procedure, discussing the issue with the user's supervisor before retrieving any equipment is a good idea. You

may not want to inform the suspect that you are confiscating the machine for suspicious activity. You may wish to use a valid non-security related reason when taking the machine for examination to decrease the chance that the suspect will delete evidence before submitting the machine to your department. From previous sections of this practical you have seen that virus and worm activity can be used as a starting point for investigation. Requesting retrieval of the laptop for the purpose of cleaning and investigating a possible virus can often reduce the odds of the user challenging your motives. It might pay to be selective with the information you provide, but dishonesty is not a recommended approach. Be sure you can provide a replacement PC before taking the suspects machine to avoid downtime and lost productivity for the employee. Whether it is at the server or the client, availability is an important aspect of security, and it also tends to be the most publicly visible. Make sure that your replacement PC is fully functional and contains all hardware and software necessary for the suspect to perform their job responsibilities.

If you have the time, you may wish to implement some evidence control procedures. These procedures could include having someone monitor your actions, or work with you on the machine at all times to avoid claims of tampering while you are examining a machine. You could also keep a written log of all actions performed on the machine and arrange for someone other than you or your assistant to store both the log and the PC.

5. Forensic tools

All the utilities described in this section are free except for Ghost. Always virus scan and carefully read the license agreement for any file you download from the Internet. If possible, always configure your tools to run from the CD instead of the target machine's hard disk to avoid overwriting deleted data or infecting your tools with a virus.

a. Ghost - Used to create images of the hard disk to be examined. Although not the best or most sophisticated technology for hard disk data capturing, it is a cost effective method for creating a copy of the disk you are working on.
Where to find it: Norton/Symantec, licensed purchase

b. Disk Investigator - A graphical based program that reads deleted sectors and can search through deleted information. This tool is useful for searching the hard drive for deleted files such as mp3, jpg, mpg etc. You can then reconstruct your evidence of abuse one deleted sector at a time.
Aside from searching for file extension names, another good search string is to enter the suspect's userid. A windows 2000 userid is prefixed to every cookie that is generated from an Internet Explorer session. The text following the @ symbol is typically the domain address from the site issuing the cookie. From this you can get an idea of where a user has been browsing on the web, even if they deleted their cache, history and cookies.
Where to find it: http://www.theabsolute.net/sware/dskinv.html

c. Partinfo - A command line based tool that displays partition information. Windows 2000 may not correctly display non-Windows partition types. This tool can be used to find partitions that are hidden from Windows. Although this paper is focused on Windows 2000, it should be noted that there are other file systems such as Linux that are capable of supporting Windows files.
Where to find it: ftp://ftp.powerquest.com/pub/utilities/

d. Vision - A graphical based TCP/IP port mapper, process viewer, and more. Can be used to display all running processes and any associated TCP/IP connections. Vision will also display running services, and device drivers. This program is useful for gathering information on running programs for the purpose of making them easier to identify.
Where to find it: http://www.foundstone.com/knowledge/proddesc/vision.html

e. Nmap for Windows - A command line based port scanner, derived from a Unix program of the same name. Used to find open ports on a target machine. Nmap features stealth scanning options to decrease the chance of your probe being detected.
Where to find it: http://www.eeye.com/html/research/tools/nmapnt.html

f. Superscan port scanner - A graphical based port scanner. Very easy to use, and capable of scanning a range of IP addresses. Used to find open ports on a target machine.
Where to find it: http://www.foundstone.com/knowledge/scanning.html

g. A list of port number assignments - This list can be used with superscan or nmap to correlate port numbers to applications. This is a very exhaustive list, and includes many instances of programs you wouldn't want running on your corporate network such as Doom, Quake, KaZaA etc. If you can't find the port you're looking for on the iana's list, you can probably find more information through Internet searches. Remember that matching port numbers to applications is not always accurate.
Where to find it: http://www.iana.org/assignments/port-numbers

h. Regedt32 - A graphical based registry editor. Can be used to export selected parts of the registry as text files for future reference.
Where to find it: Included with Windows 2000

i. PSInfo - A command line based tool that displays build, processor, root dir, and other system information. Output from this utility can easily be piped to a file for future reference.
http://www.sysinternals.com/ntw2k/freeware/psinfo.shtml

j. nbtstat - A command line based tool that can be used to find the current logged on user based on a hostname. ex: nbtstat -a <host>

Where to find it: Included with Windows 2000

k. enum - Can be used to find group information, user information, and more from a remote or local machine. Knowing which groups or users are present on a machine may help you figure out what software is installed or other information about the system you're examining. Another useful feature of enum is it's ability to find active file shares.
http://razor.bindview.com/tools/desc/enum_readme.html

l. Gdisk - Used to clean the machine via low-level formatting before it is redistributed. I typically use "gdisk 1 /DISKWIPE /DOD" which is supposed to format to Department of Defense standards.
Where to find it: Packaged with Norton/Symantec Ghost or free version at: http://www.drd.dyndns.org/gdisk.html

6. Basic procedure
This section serves as a template to follow in addition to the specific items you may have been tasked with examining. The procedure should be followed in the order it is presented. It would be helpful to familiarize yourself with your company's standard operating system build and application configuration, so that abnormalities can be more easily identified.

a. Make a ghost image before starting the examination:
<Syntax> Ghost.exe -afile=ghost.err -fro -id -z9 -ws -autoname -split=649
(Restore using Ghost.exe -fnf)
It would be wise to consult with your legal department and/or record retention policy before archiving any evidence related to your investigation. Any evidence that is archived should be compressed and encrypted. As an extra layer of security, the files can be hashed using MD5 or other hashing algorithm to ensure their integrity has been preserved during storage.

b. Check for abnormal or hidden partitions using partinfo.
To use partinfo.exe, you must first create an MS-DOS boot disk and copy partinfo.exe to that disk. After using the bootdisk to boot the machine, type "partinfo > partinfo.txt" to run the program and save the output as a text file which will contain the partition information.

c. Check Cookies from all profiles and check for deleted cookies using Disk Investigator searching by userid. (Note malware sites, and sites pertinent to your investigation)
Select 'Tools' -> 'Search Disk' from the main menu to locate the files you're looking for.

d. Check SAM for abnormal groups and userids using the enum program (Or use the Computer Management MMC console)

To get group information, type: "enum -G <ipaddress>"
To get user information, type: "enum -U <ipaddress>"

e. Check for abnormal processes and TCP/IP connections using the Vision Utility. (Make note of any malware or copyrighted material found.)
To use the Vision utility, open the program and use the TCP/IP Portmapper and Processes tab from the left hand menu. From the processes screen, you can get more information about each running process by clicking the "+" symbol to the left of each process name.

f. Search hard disks for copyrighted material and malware. Common file extensions to search for include:
.nfo - This file extension is often included with pirated software and contains information regarding the piracy group that cracked and distributed the associated program.
.mp* - mp3, mpeg, and mpg are popular media file extensions for audio and video.
.wma - A popular audio file extension
.jp* - jpeg, and jpg is a popular image format, especially for pictures stored on the Internet because of it's compression features.

g. Run "dir /s /ah /ogen c:\ > dirdumphidden.txt" and "dir /s /ogen c:\ > dirdump.txt" and store the text files for later analysis. This can be used as a reference for items found in the previous 2 steps. Dirdumphidden.txt holds a list of hidden files on c:\, while dirdump.txt holds a list of all non-hidden files on c:\. Both lists are arranged in an organized and easy to read format.

h. Run "psinfo > sysinfo.txt" and store for later analysis. This dumps Internet Explorer, Service Pack, RAM, Processor, build date timestamp, and other information into a text file.

i. Helpful tips:
*The registry can be exported using regedit if needed, and Regedt32 can export selected parts of the registry as text files for reference.

*Internet search engines and MS TechNet are helpful for determining what the files you find are used for.

*Keep in mind that the most frequent user of the machine is not always the perpetrator of the abuse. Be sure to dig deep enough in your examination to uncover all possible users of the machine.

7. Meeting with management to discuss findings
a. Preparing for your presentation:
Take your notes from the investigation and compile them into a formal presentation. Be sure to tailor the presentation to your audience, and simplify

technical concepts if necessary. If you simplify your presentation, be sure that you have your notes containing the technical details of your investigation handy in case there are questions.

Use graphs, illustrations and screenshots to help convey your message, but edit the graphics when necessary to remove any sensitive information.

b. Discussing risk analysis and mitigation:
List the unauthorized software and files present then review the associated risks and issues.
The word mitigation, which means to alleviate or lessen, is frequently used in the information security field in regards to risk or vulnerability. The basic strategy for improving the security of your computing environment is to identify the risks, analyze the risks discovered to determine the full implications, and then create a plan to mitigate the risk. Your goal will be to convince management to eliminate as much risk as possible.

"Remember that risk to an enterprise can never be totally eliminated - that would mean ceasing operations. Risk mitigation means finding out what level of risk the enterprise can safely tolerate and still continue to function effectively" (Krutz, Vines, p.15).

c. Examples of risks to discuss:
-Intellectual Property Violations (Installing unlicensed software, illegally distributing or receiving copyrighted software, music, movies etc) puts your company in danger of legal litigation and lawsuits. Intellectual property lawsuits are getting alot of attention in 2003. The RIAA and MPAA are targeting music and movie piracy violators for legal action in record numbers. Trade groups such as the RIAA have also issued public statements to Fortune 1000 companies urging them to take a pro-active approach to prevent intellectual property violations perpetrated by their employees or else face legal consequences.

-Unauthorized programs may contain exploits and vulnerabilities that can affect other systems or the operating system itself. Unauthorized programs can raise help desk costs, damage valuable data, or facilitate the theft of valuable information.

-Chat programs like AIM, and MSN Messenger along with gaming websites like www.zone.msn.com, and games.yahoo.com waste productivity and can be used as a vector for viruses or malware. As instant messaging becomes more popular in both home and work environments, it becomes more attractive for virus and worm writers to use instant messaging and websites to spread their malicious code.

-Webmail allows users to download files while bypassing your corporate email gateway's defenses. These files could be infected with viruses or malware.

There is also a risk that unprotected webmail may be used to send and receive corporate data by users that do not understand the risks.

-Files downloaded from P2P sharing programs may contain viruses that bypass web and email anti-virus filters. Another risk presented by P2P programs is the ability to accept mapped drive letters and share your private corporate file server with the world.

-Spyware/Adware programs that are built in to free or shareware software can introduce a number of problems including: Interference with network access, frequent pop-up advertisements, and vulnerabilities that can allow system compromise. There is an abundance of programs available that can be downloaded for free from the internet, and most users are unaware that they have installed spyware when using them.

d. Wrapping up:
Present your best determination of the cause for the risks and issues present. Be careful when the evidence points to a particular user as the cause, and make use of the word "appears" or "seems" instead of an affirmative when necessary. You should also avoid personally attacking anyone, and keep your report as emotion free as possible.

8. Preventing future abuses, and other opportunities
a. In closing your presentation of the investigation, you should recommend a few options to mitigate the current risks and issues, and also suggest ways to prevent abuses in the future.

b. Be sure to retrieve all important files, and low-level format the machine when you are done with your examination. A good low-level format decreases the risk that the next person to use the machine will be able to access any unauthorized programs or files.

c. Education opportunities exist in almost any situation, and there are many different educational programs available to meet your needs. There is also an abundance of information available online that could assist you with educating your users.
The US government has issued several education campaigns to help educate users on information security topics at no cost, and can be found online at the following websites:
http://www.isalliance.org/resources/papers/ISAhomeuser.pdf
http://www.ftc.gov/bcp/conline/edcams/infosecurity/index.html

d. Firewall rules can be used to block the port numbers used by p2p programs, games, worms, chat clients, trojan horse viruses etc. Implementing good firewall rules not only protects you from outside sources that are attempting to penetrate and damage your systems, but it also prevents your systems from attacking other

companies. Creating a good firewall ruleset can reduce your liability in the event that another company is attacked by your systems by showing you exercised due care in limiting the potential for outbound attacks from your company.

e. Web proxy rules can be used to block webmail sites, p2p utility download sites, malware sites, hacker sites etc. Products such as surfcontrol, smartfilter, and websense can be used to filter what is permitted to be viewed on your company's PC's while they are connected through your corporate network to the world wide web.

f. Policies and procedures can be put in place to scan each workstation for unauthorized software using SMS or other client scanning tools. The reports generated by systems management utilities can be compiled and searched for the keywords of your choice on a periodic basis to detect unauthorized programs and files.

g. The examples of abuse from the incident can be used as leverage to purchase spyware/adware removal utilities or other solutions to help mitigate the risks discovered by your investigation.

h. The examples from the incident can be used as leverage to use Windows 2000 group policy to lock down the workstation. Using group policy to restrict what your machines can be used for not only makes is more difficult to abuse corporate assets, but it can also create a larger trail of evidence to follow. For example, one way to bypass restrictions on your corporate computer would be to log on as the local administrator. There are many sites on the Internet that show you how to change the local administrator password without knowing the previous password or having administrator rights on the PC. However, changing the local administrator password makes it obvious that the PC has been compromised because it is no longer using the password set by the unit that manages desktop PC's.

References:

a. Wood, Charles Cresson, CISSP, CISA. Information Security Policies Made Easy, Version 9. San Deigo: PentaSafe Security Technologies, Inc., 2002. Ch 8, Appendix G.

b. Krutz, Ronald L., Russell Dean Vines. The CISSP Prep Guide. New York: John Wiley & Sons, Inc., 2001.

c. Kruse, Warren., Heiser, Jay. Computer Forensics, Incident Response Essentials. New York: Addison-Wesley, 2002. 197 - 212.

d. SANS Institute. SANS Security Essentials I: Networking Concepts., 2002. 3-30.

e. Webb, Bill. "The Trouble with Spyware & Advertising-Supported Software" URL: <http://www.cexx.org/problem.htm> (24 Feb. 2003)

f. PestPatrol Inc. "About Spyware: What Products Incorporate Spyware?" 29 Dec 2000. URL: <http://www.safersite.com/Support/About/About_Products_Incorporating_Spyware.asp> (24 Feb. 2003)

g. SecurityGlobal.net LLC. "Gator Plugin for Microsoft Internet Explorer Lets Remote Users Install Arbitrary Software on the User's Host" 20 Feb 2002. URL: <http://securitytracker.com/alerts/2002/Feb/1003611.html> (24 Feb. 2003)

h. Dalton, Curtis. "Special Report -- Preventing Corporate Network Abuse Gets Personal." 5 Feb 2001. URL: <http://www.networkmagazine.com/article/NMG20010126S0003/1> (24 Feb. 2003)

i. Techweb News. "Hollywood Warns Fortune 1000: Don't Copy -- Or Else." 14 Feb 2003. URL: <http://www.internetwk.com/breakingNews/showArticle.jhtml?articleID=6900077> (24 Feb. 2003)

j. National Institute of Standards and Technology. "Training and Education." 4 Feb 2003. URL: <http://csrc.nist.gov/ATE/te_full.html#government> (24 Feb. 2003)

k. Daniel Petri Ltd. "Forgot the Administrator's password?" 29 Jan 2003. URL: <http://www.petri.co.il/forgot_administrator_password.htm> (24 Feb. 2003)

l. Purdue University. "Digging For Worms, Fishing For Answers" 2002. URL: <http://www.acsac.org/2002/papers/68.pdf> (26 Feb. 2003)