Global Information Assurance Certification Paper

Defending Against Misuse of Forensic Analysis Tools on Windows Systems

Michael Christiansen
GIAC GSEC
v1.4b, Option 1

January 11th, 2004

Abstract

Data stored on network file servers is usually well safeguarded from users stealing that data. But what about when that secured data is copied to a user's workstation? Often there are no locked doors to keep employees from accessing a machine which is not their own. Many users are in the habit of copying files locally to work with before placing them back on the hardened file server you have secured behind closed doors. This is especially true for engineers work with huge documents that will not run efficiently from the network. Who is to say a user cannot walk up to a machine in HR or Finance at 8pm, after the department has gone home? They are then free to boot the machine to a forensics CD, plug in a USB hard disk or memory card, and copy everything, even password files! The thief can now obtain that 60MB CAD drawing, or even a spreadsheet of employees' confidential information.

Think you are safe using file permissions on NTFS? Think again. Unless you are using good encryption, you are at risk. Administrators need to secure the data which lives on the machines in the workplace. In this document, I will provide a guideline for protecting your precious data from prying eyes. Also, security/network administrators need to understand the forensic analysis tools that are wonderful for all us good guys, are also available (for free) to anyone. Understanding how these tools work is critical to securing data not protected by physical security methods. While it is feasible any system a user has physical access to is breakable, there are methods to securing the data to such a degree that it is very difficult to obtain without the use of enormous computing power. Hopefully, by the time the data is cracked, months, or years will need to have passed, and the information will be of much less value.

Scope

This document assumes the reader is moderately skilled in a corporate Microsoft Windows production environment as well as some basic UNIX/Linux knowledge. Client operating systems will include:

- Microsoft Windows 2000 & XP
- Modern versions of Linux (as it pertains to the forensics tools used)

This document will also assume a base knowledge of security in the basic Microsoft file systems: FAT, FAT32, & NTFS.

Background of Forensics & Tools

Computer Forensics

The purpose computer forensic software was created to allow investigators to acquire data from a system, as to leave that system in its original, untouched state. Investigators should include either administrative staff from your company, a third party security professional, or a government forensics expert. Typically, the investigator will image the target drive, and then analyze the image separately, leaving the original exactly as it was. Finally, the investigator will report their findings to the appropriate authorities. This process usually requires the investigator have complete physical access to the target media. In essence, the investigator is getting an untainted copy of the data from which to begin her research. (R1)

Tools

Today, forensics tools are abundant to say the least. These tools range from very powerful, free and useful tools to very expensive (and often more user friendly) ones. This section will discuss some of the more popular tools and how they work and allow investigators to acquire data.

F.I.R.E. (Forensic and Incident Response Environment) was created by William Salusky of DMZ Services, Inc. It is an excellent, Linux-based, forensics tool. Available for free download at http://fire.dmzs.com, it employs tons of powerful data acquisition and analysis tools. F.I.R.E. boots from your CD reader and is practically a full version of Linux complete with anti-virus, web browsing, and file/network utilities galore. Some of the features in F.I.R.E. are:

- Data collection and imaging
- Recover data from lost partitions
- Security tools: Nessus, Nmap, whisker, hping2, hunt, Ethereal, Snort, tcpdump, ettercap, dsniff, airsnort (there are many more)
- Runs on a x86 system and can read any Windows volume including NTFS
- Can mount external USB drives to copy/image data to
- Leaves no trace to access of files residing on a Windows volume

F.I.R.E. boots to an X-Windows environment or can be operated from a text based command-line interface. It should be noted that learning and using F.I.R.E. requires a basic knowledge or Linux and its commands. (R2)

Another forensics software company is Paraben. Paraben is a complete line of corporate level forensics tools, which is able to analyze even more types of computer storage methods. In addition to hard drive imaging/copying tools, Paraben has the ability to look into deleted files on a hard disk, email databases such as Exchange, and even PDAs. Paraben's tools are not free, and range from

around $160 - $400 per tool set. These tools provide an easy to use Graphical User Interface (GUI) and are intended for professional and law enforcement use. (R3)

Paraben's software is less of a "hardcore hacker" tool, and allows the user to work on a much higher level than F.I.R.E. This could be attractive to anyone that wants to steal data, but is not a full fledged computer guru. Like F.I.R.E., Paraben's toolkit is way too extensive to list. The point of mentioning this type of software is to inform the system administrator that anyone can be an attacker, not just that "know it all" you've got you eye on.

The Problem

The Hacker

In order to understand why someone would want to steal data, or do anything illegal, we must understand the mindset of the thief, i.e. hacker. While people hack for many different reasons: curiosity, to exploit vulnerability, terrorism. We will focus on a certain category of hacker. The hacker this paper deals with is the one that wants to steals industrial information, secrets and/or intellectual property. This group represents the minority of most hackers, but is also the most devastating towards a company's business investments. (R4)

Physical Access

Physical access is something we cannot protect on every workstation or laptop in the building. It would not make sense for every user to have a personal office that only themselves, plus support personnel, had access to. Securing every workstation with the same physical security as the file or email server is not financially practical. It would require too much management, and too much equipment.

Most companies may have a segregated access by door locks to parts of the building, but for the most part they are wide open to anyone that can get in. This is all that the attacker needs to compromise an unsecured system: the ability to walk up to a machine and touch it. The most practical action is for the attacker to boot the machine with a forensics tool and collect information.

By allowing physical access, most intrusion detection systems are completely useless. The most an administrator could know is that a system was rebooted. That usually would not cause any suspicion in a Windows environment. People reboot their computers all the time due to program crashes, patches, to free memory, etc. Windows aside, reasons that a system was rebooted could even include a power failure/disruption or a clumsy janitor kicking the cord loose.

The Attack

Now let's cover the worst case scenario: what happens when the "investigator" is a thief, using one of these (or a host of other) forensics tools? To avoid detection, malicious users can use a tool, such as F.I.R.E., to image a hard disk drive to his USB hard disk drive or USB memory card. Any Unencrypted data on either a laptop system, or a desktop, is immediately readable. Paraben's toolkit also boasts a very easy to use password decryption utility. This utility can be used to find the passwords to the Windows operating system, Microsoft Office documents, WinZip, Adobe Acrobat, Lotus Notes, and many, many other popular applications. It really makes you think twice about how secure you data really is!

File permissions on an NTFS volume mean nothing to Linux. NTFS permissions only apply to Microsoft Windows operating systems. Once the attacker has your data in his private possession, what will guard you against him exploiting everything he can? The next section will discuss how you can defend your data.

Solutions

For starters, there is no one solution or technique for defending against attackers that use forensics tools. We must practice defense-in-depth. According to the SANS Institute, defense-in-depth is "the need to be certain that if one countermeasure fails, there are more behind it." Attackers will have many different methods to compromise a system ranging from social engineering to brute force encryption cracking. All layers of defense in our strategy must be implemented with equal vigilance, or we run the risk of compromise. (R5)

This section will discuss methods to keep sensitive Windows workstations secure. As a rule, laptops should be given extra attention since they are more susceptible to loss and theft. Educating your users will also play a vital role as they have the ability to deliver to anyone the data they work with, or have access to. Next this paper will discuss some methods the administrator can use to "harden" user's workstations and laptops. The topics will include enforcing a strong password policy, BIOS protection, and file/folder encryption. Implemented properly, these defense techniques should provide a fortress of a machine that will provide a stiff wall between the hacker and your data.

Employee Education

The first line of defense is to educate users on why a security policy exists. They need to understand intellectual property can keep a company alive, and you are there to help them protect themselves from being a target. Trust needs to be developed between the IT department and its users. Without trust, users *will* find ways to weaken their systems. Even the most complex password, and the most

encrypted data, is worthless if a user writes their password on a post-it® note next to their machine.

Begin employee education by starting with your (and you should have one) security policy. Make this policy internally public and encourage users to review it. Provide a method for users to access the policy anytime by means of a file server, intranet website, database, or a document control system. When a user has a question, it is always nice to be able to refer them to something that has been signed by executive management. Let the users know that you are all aiming towards a common goal, and that the success of your company is dependent upon your security policy. The more the user knows about the importance of security, the more secure her system, and your company data, will be.

Strong Passwords by Policy

In a Microsoft Windows 2000 Active Directory environment, password policy is highly customizable. The default configuration for domain password policy is at best weak. To begin setting up a password policy for your domain open Start>Programs>Administrative Tools>Domain Security Policy from a Domain Controller. On the left side of the window, expand Security Setting, then Account Policies. The following settings should be present: Password Policy, Account Lockout Policy, and Kerberos Policy. This will set the policy at the root of the domain of the server you are using. Be aware that it will be possible later to define polices in sub-containers that can override your settings, unless you check the option to not allow overrides.

Below is a list of settings to create a strong password policy: (R6)

Object:	**Default Value**	**Strong Value (minimum)**
Enforce password history:	1 password remembered	10 passwords remembered
Maximum password age	42 days	30 days
Minimum password age	0 days	7 days
Minimum password length	0 characters	8 characters
Complexity requirements	Disabled	Enabled (see below)
Reversible encryption	Disabled	Enabled (see below)

Complexity requirements give the administrator the ability to force the user to use hard to guess passwords. Complex passwords will only allow users to create passwords that meet the guidelines you specify. There are 4 basic options that should be enabled that will be required for every password created on a domain computer:

- Upper case letters
- Lower case letters
- Numbers
- Special characters (e.g.: $,#, or punctuation characters such as ? or !).

In addition to these settings, the administrator should not allow users to create passwords that contain any part of the username, or users' full name.

The “store password using reversible encryption for all users in the domain” option should also be enabled, but is of little relevance to a system compromised with forensics tools. This setting enables CHAP and is a preventative measure to network sniffing.

The second piece of a good password policy is the Lockout Policy. This should be set for any windows domain, to protect password guessing. However, the context of protecting a system that is compromised, the attacker does not apply to the lockout policy. Before implementing a password policy, it is recommended that the administrator download and run the Microsoft Baseline Security Analyzer available at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsahome.asp.

The object of having a strong password policy to ensure that the local hashes saved on a user’s computer are safe. Once an attacker has obtained a local copy of the password file, it is only a matter of time before the system can be cracked. By having a strong password, we ensure that the password will not be compromised (in a reasonable amount of time) by even a lengthy brute force crack.

It should also be noted that an alternative to a strong password, is a smartcard. These devices contain very strong or even changing passwords. The use of a smartcard, while creating more cost and administration than password policy, is certainly worth a look for protecting the most critical of data. A good starting point for deploying smartcards in a Windows 2000 environment is available from Microsoft at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/smrtcard/smrtcdcb/default.asp.

BOIS Protection

To create another layer of protection, users should protect their laptops and desktops from allowing an attacker to boot to a device other than the hard disk. Almost all modern computers have a Basic Input/Output System (BIOS) that can be configured to secure its configuration. Since it is usually not possible to enforce a BIOS password by policy, it is a good idea to have a manual management system for them. For example, the administrator could configure the BIOS password to be the same for each department, and then keep a secure spreadsheet with those passwords. The passwords should be complex as outlined in the previous section. These passwords should not be given to users, as that could potentially compromise multiple systems.

Some BIOS programs allow for two passwords. One for booting the device, and one for modifying the BIOS settings. From a usability perspective, it is ideal to setup the BIOS so that it boots to the hard disk that contains the operating system first. Other boot options should be disabled. Then, the administrator only sets the system to require a password for editing the BIOS (not booting the system). (R7)

Again, this is not 100% protection from someone booting your computer to their forensics tool. Most motherboards have a switch or jumper that can reset such passwords. While this requires more effort on the attacker's part (especially for a laptop), it is possible. Also, if the attacker can physically remove the drive, it can be inserted into another system, bypassing the BIOS password. To tackle this challenge, some vendors have a hard disk based BIOS password. Hard disk passwords should be used on laptops because they run a higher risk of the entire system being stolen or lost. As before, hard disk passwords are not foolproof and can be bypassed by a user with the right skills and tools.

By default in Windows, a strong BIOS password will not protect your data from hibernation mode on laptops. Hibernation mode in Windows allows the system to save power by dumping the contents of its memory to disk and shutting down power. This mode should be password protected in Windows (by default it is not). Otherwise, when a system leaves hibernation mode, no password is required to return to use. As a preferred alternative, use stand-by mode. Stand-By mode will also save power, but for a shorter period of time. If the system will be off for an extended period of time, shut it down. This is cleaner for the operating system. By using stand-by mode, you require the user to enter their password for re-entry into the system. Using stand-by mode is faster than using hibernation. However, stand-by mode requires a tiny amount of power consumption and will usually last 48-72 hours, whereas hibernation mode can last weeks.

Encryption

Using file encryption builds a major wall for forensics tools. The idea is to use encryption that is so hard to decrypt, it is not feasible to do so in a reasonable amount of time. There are two major options for file encryption in a Windows 2000/XP client environment. They are the built-in file encryption for Windows, and PGP. Each of these options has pros and cons that we will discuss in the following sections.

Windows 2000/XP native encryption

Microsoft has built an Encrypting File System (EFS) right into its Windows 2000 and XP operating systems. Since Windows 2000 SP2, Windows has used 168-bit 3DES encryption algorithms to protect files. Users must be using the NTFS (not the FAT or FAT32) to enable EFS. One of the greatest benefits to using EFS files is that it is transparent to the user. Simply add the appropriate attribute to a folder, and all subfolders and files can be set to automatically use strong

encryption. Opening such files happens on the fly as files are used. Aside from the folders that contain personal/sensitive data that should be encrypted, it is also good practice to encrypt any files used by the email program to store local email. In Microsoft Outlook, these are the .ost and .pst files that reside in a user's profile. Otherwise, you could be offering any sensitive email you may have stored on your hard disk.

EFS can be implemented in a corporate environment using a Public Key Infrastructure (PKI) that allows administrators to hold a copy of all keys & certificates in the unlikely event that a user local key becomes unavailable. The keys are stored on a server which creates certificates for users to obtain. EFS can also be implemented on a stand-alone system using self-signed certificates generated by the operating system.

Users must remember the built in Windows EFS is only as strong as the password they have created for logging into the system. If an attacker can obtain the user's password, all file encryption is transparent to them as well. For this reason, it might be worthwhile to use a passphrase, as opposed to a password, for Windows login on a system using EFS. This can provide more robust security which comes closer to the stronger (and much more cumbersome from an end-user's perspective) PGP.

PGP

Pretty Good Privacy (PGP) is the de facto standard for file encryption software. The free version of PGP (available from www.pgp.com) allows file encryption options galore, but is limited to encrypting files only on a stand alone system. There is a commercial version of PGP which allows encrypting and digitally signed email as well. This version also provides key management for a corporate infrastructure. PGP Corporate is not free, and license fees apply.

PGP has options for setting key size (strength) and offers many proven encryption algorithms. Although PGP provides one of the strongest file encryptions available, it comes at a price. That price is usability. Technical users usually do not have a problem with the extra burden of management in PGP; however, the director of HR is probably not a computer guru and will prefer to use a transparent solution.

In the personal version of PGP, where no key management system is in place, it is possible for a user to completely lock himself out from the encrypted data. A good, strong, and easy to remember passphrase should be selected by the user. (R8)

Summary

Figures have stated over 75% of *successful* attacks are from inside the firewall (usually hands on & on site!). Forensics software has the ability to do some

amazing work for those we trust, however, we need to defend our data from the attacker using these powerful tools. It is all too easy for an attacker to gain physical access to a workstation that resides outside the server room and compromise data stored locally. For this reason, it is important to practice defense-in-depth at the individual system level.

We start by educating the user about how protection is vital to the company's survival. Keeping anyone from obtaining a password is arguably the most vital step. When the attacker has the password to a system, it is a free for all on anything that user has access to. BIOS passwords can help prevent the use of bootable forensics tools by not allowing a system to boot to a device other than the hard disk. BIOS passwords are certainly not very safe as hard disks can be removed and imaged. Also, most motherboards have a BIOS password reset that can be used to clear the BIOS password. Our last layer of defense is file encryption. If the user has managed to obtain an image of the hard disk, sensitive files will be very difficult to crack if good encryption techniques have been practiced.

References:

(R1) Limongelli, Victor. “Statement of EnCase Software Compliance Under Section 508.” 05/21/2003. URL: http://www.guidancesoftware.com/corporate/downloads/508Compliance.pdf (11/11/2003).

(R2) Loss, Dirk. “F.I.R.E. - Frequently Asked Questions.” Revision 2. URL: http://fire.dmzs.com/?section=faq. (11/11/2003).

(R3) Paraben Computer Forensics Software. “Product Listing.” URL: http://www.paraben-forensics.com/products.html. (11/24/2003).

(R4) Kremen, Stanley. “Apprehending The Computer Hacker: The Collection and Use of Evidence.” URL: http://www.shk-dplc.com/cfo/articles/hack.htm. (11/24/2003).

(R5) Cole, Eric; Fossen, Jason; Northcutt, Stephen; Pomeranz, Hal. SANS Security Essentials with CISSP Volume 1. “Vunerability Scanning”. USA: SANS Press, 4/1/2003. 700.

(R6) Johansson, Jesper. “Windows 2000 Security Harding Guide. Version 1.2. 5/15/2003. URL: http://www.microsoft.com/downloads/details.aspx?familyid=15E83186-A2C8-4C8F-A9D0-A0201F639A56&displaylang=en. (11/25/2003).

(R7) searchWin2000.com Definitions. “BIOS.” 11/18/2003. URL: http://searchwin2000.techtarget.com/sDefinition/0,,sid1_gci213814,00.html. (12/2/2003).

(R8) Hoel, Jeremy. “PGP For Everyday Use”. URL: http://www.sans.org/rr/papers/index.php?id=887. (12/09/2003)

Last Updated: October 22nd, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive