Computer Forensics: Introduction to Incident Response and Investigation of Windows NT/2000

Norman Haase

Computer Forensics: Introduction to Incident Response and Investigation of Windows NT/2000

Norman Haase

December 4, 2001

Introduction

The purpose of this paper is to be an introduction to computer forensics. Computer forensics is a newly emerged and developing field which can be described as the study of digital evidence resulting from an incident. It involves collection and analysis of digital data within an investigative process. Other important steps include incident preparation, detection and recovery. All these procedures should be documented and conducted according to a standard methodology (Mandia & Prosise, 2001; McMillan, 2000). After introducing some important incident response considerations I will focus on a strategies for dealing with compromised Windows NT/2000. My hope is that this paper might be of some assistance in handling your own incidents and investigations. This paper is about investigating Windows hosts and conducting an analysis in order to promote growth and learning as opposed to a "how-to" guide to gather legal evidence in view of criminal prosecution.

I've chosen to focus on Windows NT/2000 because "a recent study said that 90 per cent of business information worldwide is stored in Office documents, Word and Excel files residing on Windows NT/2000 servers" (Armstrong, 2001). Therefore Windows presence within many corporate and government environments it is essential that one be familiar with procedures and challenges encountered by a forensic analysis.

Incident Response Essentials

Computer Forensics: incident response essentials provides a skeleton methodology which it summarizes as the three A's of digital forensics which apply to Windows incidents as well as other OS platforms: (Kruse & Heiser, 2002).

1. Acquire the evidence without altering or damaging the original.
2. Authenticate that your recovered evidence is the same as the originally seized data.
3. Analyze the data without modifying it.

Standard Methodology

"A standard methodology will provide for the protection of evidence and some common steps that should be followed in the investigation process" (McMillan, 2000). The standard methodology should encompass the following "activities/procedures for securing a suspected computer incident scene [and include] shutting the down the computer, labeling the evidence,

providing chain of custody documentation, documenting the evidence and transporting the evidence" (Grace, 2001). The methodology should also apply to evidence handling, authentication and storage.

In order to implement procedures in a timely manner an organization should have an incident response team already in place. Each member of the team should have access to the same documentation and capable of performing each of the steps assigned to a particular phase. All members of the team should be intimately familiar with each procedure and cross-trained to assume another phase if someone on the team is unavailable or complications arise. Often times when an incident occurs not enough time has been put into refining and documenting an organizations response procedure and this can create chaos during a response. Another aspect that is often overlooked is the need for incident response drills to test its true functionality of the documentation so it can be revised accordingly. The incident response team also needs to rehearse anytime the incident response procedures are changed. The organization should mandate at least one mock incident response training session per year for the team.

Preparation

Probably the easiest Windows incident to respond to is the one that has not occurred yet. Therefore, it is necessary to evaluate and strengthen Windows host and network based security to provide protection from attacks. Particular attention should be paid to the configuration of domain controllers since they are centers for authentication, services and data. Some specific measures that you should take will include: installing the latest service packs available on all Windows hosts, installing security hotfixes which are not included in the latest service packs, update installed applications with the latest vendor patches, consult supplemental windows security resources such as www.ntbugtraq.com or www.ntsecurity.net and others. Enable or increase audit logging on domain controllers as well as event logging for all hosts, backup all critical data and export a copy to a secure location off site, disable any unnecessary services and block or filter access to ports at the host level especially on domain controllers, record cryptographic checksums of critical system files and take every opportunity to educate users on general host based security guidelines such as choosing good passwords, reporting unusual activity or events without investigating to the appropriate contact and the dangers of users installing certain software which may threaten the integrity of the of the network itself.

Windows network based security improvements will include installing and configuring firewalls, installing and tuning an Intrusion Detection System (IDS), topology adjustments to allow for effective monitoring, encrypting network traffic and effective router access control lists (Mandia & Prosise).

Investigating Windows NT/2000

A necessary component of any system investigation is a standard assortment of software tools that will provide information about the current state of the host or network you are examining. The toolkit that you build yourself or purchase as a suite from forensics supplier should contain

everything you need to duplicate, analyze system files and data stored on the disk. There will often be times where one needs to be able to circumvent encryption, crack passwords, monitor traffic and sniff data off a host or network and your toolkit should contain appropriate programs. Those organizations seeking a packaged forensic tool suite for Windows NT and 2000 could obtain one from New Technologies www.forensics-intl.com. Another vendor offering tools and online training can be found at www.cftco.com. However, this paper uses free tools when possible to enable anyone to build a custom toolkit, burn it to CD and copy specific frequently used ones to floppy disks.

Some tools that can be considered for Windows NT/2000 include:

- Byte Back and Norton Ghost used for creating disk clones.
- tcpdump and WinDump: used to capture network traffic for analysis.
- Nmapnt: an NT/2000 version of the original Nmap used for scanning ports and services on local or remote hosts.
- L0pht's Antisniff: used for detecting sniffers.
- L0phtcrack: an NT password cracking utility.
- pwdump: used for dumping password hashes locally or remotely on NT systems.
- Foundstone's Forensic toolkit: contains an assortment of utilities for examining visible and hidden files on an NTFS partition.
- Netcat: is a multi-purpose "TCP/IP Swiss Army knife".
- DumpSec: utility produces a list of shares locally and remotely.
- NTFS DOS: allows one to mount an NTFS file system locally from a DOS prompt for read/write.
- PGP: provides high-encryption for securing entire disks or individual files.

A more exhaustive list of tools can be found in Hacking Exposed.

Acquiring Data

There are several steps to be considered initially when gathering information on a compromised Windows NT/2000 machine. The first is collecting volatile data. However, you might encounter obstacles which need to be dealt with beforehand such as "continued presence of [the] intruder on the system, possible "booby traps", impact of system compromise on continued operations [and] involvement of law enforcement" (Romig, 2001). Volatile data can be defined as active information temporarily reflecting the machines current state including registers, caches, physical and virtual memory, network connections, shares, running processes, disks, floppy, tape, CD/ROM and printing activity. Before one begins collecting volatile data there are a few guidelines to follow:

- Avoid tools that use a GUI interface. Command line tools are best here.
- Use safe and tested tools you know that work.
- Create two or three floppy disks containing your volatile collection tools and write-protect them.
- Generate a checksum and validation for each of your tools and store it safely within your toolkit.

Some of the tools recommended for the collection of volatile data are:

- Srvcheck.exe: A NTRK utility that displays the shares locally or remotely.
- Kill.exe: A Windows 2K Support tool for terminating a selected task or process.
- Rasusers.exe: A NTRK utility that lists all user accounts on a domain or server that have been granted permission to dial in to the network.
- Dumpel.exe: A NTRK utility to create an ASCII copy of the Event Viewer Logs.
- Filemon: A monitoring tool that displays all file system activity in real time.
- Regmon: A monitoring tool that displays all registry activity in real time.
- Tokenmon: A monitoring tool that displays logons, logoff, privilege usage and impersonation.
- Handle: A tool that displays what files are open by which processes and more.
- ListDLLs: A tool that lists all DLLs that are currently loaded, including where they are loaded, version numbers and the full path names of the loaded modules.
- Process Explorer: A tool that displays open files, object processes, registry keys, DLLs and owners of object processes.
- MD5sum: A tool that generates the checksum of a file and provides verification.
- Fport: A tool that maps application processes to the ports they listen on.
- TCPView: A tool that shows the endpoints of all open TCP and UDP connections.
- Cmd.exe: The command prompt for Win NT/2000.

When one begins the volatile data collection record your general findings in a notebook along with the time and date. Use a tape recorder for more detailed information. Try to run your tools from your floppies or CD so as not to interact with the system anymore than necessary. This will help to establish that your data gathering is accurate. Keep in mind, however that the system you are working on could have a rootkit installed compromising it at the kernel level. Therefore any information that is gained from the system *must* be considered suspect, but should still be recorded. Rootkits often times include trojaned versions of system commands or programs that circumvent standard system processes and functions. For example, the registry may be altered, and/or processes, files and registry keys hidden, calls redirected to Trojan functions, false information generated and malicious code executed (Scambray, McClure & Kurtz).

System Quarantine

After this initial data collection phase has been completed the decisions to unplug the machine from the network and power it off must be considered. Usually best judgment is acquired both through intuition and experience, but there are potential positive and negative to each case. This is because "understanding cause and effect are absolutely crucial – any opponent has lots of opportunities to change or subvert your machine" (Farmer & Venema). This could be an argument in itself for shutting the machine off which would eliminate this risk. On the other hand "destroying or modifying data to hide evidence can leave significant marks as well – sometimes more telling than if they had left the system alone" (Farmer & Venema). Most of the decision here should be based on the confidence level and extent of initial information gathering and documentation. If one believes that the systems activities are a threat to the network then

unplug the machine from the network. This will isolate the host, but if the determination is made that the system was not compromised by an internal source then much bigger and more serious issues exist. If the machine is absolutely critical and cannot be powered down then a workaround will need to be followed probably involving a substitute system. A suspected machine or one under investigation should *never* be rebooted, but shutdown cleanly through the OS. Most systems that undergo additional investigation or disk imaging should be powered off unless the drive in some instances is a hot swappable non-system disk only containing data. If not one risks corrupting various levels of system data that will create obstacles in further analysis. As a rule, powering the machine off after *all* "volatile" information has been acquired maybe considered less risky for host and/or network environments. Any plans that involve using a Windows NT/2000 system recently involved in an incident for any purposes prior to forensic analysis should be avoided.

Authentication

Gaining access to the Windows NT/2000 operating system initially prompts for a username and password. This applies to the local host and to one that participates in a domain or workgroup. There are a few methods for achieving this and some of these may be carried out earlier in the investigation. Developing a detailed understanding of the Windows NT/2000 security environment with a dash of imagination will help greatly here.

- Boot the system to DOS via floppy, mount the NTFS volume with NTFS DOS and copy the SAM database to floppy and use a program like L0phtcrack to crack the passwords hashes.
- Boot the system to DOS and delete the SAM file.
- Access the registry and make changes that allow one to circumvent the normal authentication process. (Use this method as a last resort only)

There exists a host of other methods for gaining access to various Windows NT/2000 resources, but for an initial test drive of the cloned disk under analysis the issue of login always presents itself.

Software applications have there own password considerations. The more you know about the software applications security features the more you will be able to work around them. There are many free and low-cost tools to help access many protected software application data, files and documents and some important guidelines to keep in mind when conducting this work.

- Does the software application encrypt the password, if so can the hash be extracted?
- Is the password stored in more than one location?
- Does a plaintext copy exist and if so where does it reside?
- What are the most effective attacks to use, brute force, dictionary, plaintext or distributed.
- Is there any information you have already that will allow you to make educated guesses and get access quickly?
- Compressed files that have been password protected and which no plaintext copy is stored will take longer to crack

- Passwords longer than eight characters in length that have been encrypted usually take longer to crack. This is especially true in the case of strong password character selection is encountered.

Analysis

Forensic duplication is the process of creating a copy (or clone) of the hard disk on the compromised system. Then one will be able to conduct a complete in-depth analysis of the disk contents without jeopardizing the original. Here the entire disk will be duplicated including all partitions regardless of whether or not data resides on a particular partition or sector. This involves removing the disk from the system and hooking it up to a dedicated workstation equipped with a laptop hard disk adapter, large capacity IDE and SCSI hard drives and plenty of memory. This workstation will have cloning software installed like Byte Back or Norton Ghost that will allow disk-to-disk copying. One might have a portable unit to create the initial copy during a response and make a duplicate on an in-house station It is highly recommended that you create a second copy of the disk image that can be stored and used in the event complications arise and a fresh copy is needed. After disk clones are created the actual process of analyzing the image begins. This process must be conducted in a controlled system environment away from workstation system files or processes that may corrupt the image under analysis. For added insurance this could be accomplished on a forensic workstation running Windows 9x or Linux.

There are a number of areas on the disk that might contain data and must be examined:

- Files: Data associated with system data and software applications.
- Slack space: The space between the end of data and the end of a block of the file system which may contain fragmented or deleted data
- Swap file: A hidden windows system file named pagefile.sys that is used for virtual memory.
- Unallocated clusters: Blocks that are not currently used by a file.
- Unused partitions: Space that is allocated and formatted, but does not appear to contain any data.
- Hidden partitions: Hidden space that might contain unallocated space that may also deliberately hide data.

Additionally, the boot tracks may contain elusive data usually not visible or accessible to the operating system and most disk utilities (Kruse & Heiser).

While one is examining the hard drive record the size, make and model. Make sure that all the partitions and unallocated space add up to the capacity of the disk. This may provide some early hints regarding the presence of hidden partitions, data, and other file systems. One simple tool used for viewing the partition table of hard disks is the old DOS FDISK utility that will provide a general picture of the structure. If you prefer PartitionMagic contains a program to view partition tables. However, since NT/2000 supports FAT, FAT32 and NTFS one will need to mount the NTFS volume read-only offline. This can be accomplished by the NTFS DOS utility which will also allow you to search anywhere on the mounted volume for anything of interest without risk to the file system. Another tool that is valuable for conducting other low-level disk investigations

is a good hex editor. One freeware hex editor XVI32 provides many features including text string searches, runs as a single .exe file and fits on a floppy. Hex editors will be useful for examining slack space, unallocated space, files, boot tracks, unallocated, hex string searches and character conversions.

Usually as an investigation progresses through stages the focal points for analysis gradually shift from bits and bytes to use of the disk clone in a live machine for further study. This stage introduces the frequently encountered issues of passwords, encryption and hidden data that are used to secure the operating system itself, and obscure applications, documents, files and sometimes an entire partition or disk. There are additional tools, techniques and procedures one can follow to help overcome each of these obstacles.

Hidden Data Objects

There are numerous ways data can be hidden throughout a Windows NT/2000 system and literally dozens of places. One method that is employed involves the use of Windows NTFS file streams that allow one to attach hidden data including executables, directories, scripts, documents and other data objects to visible files. One tool that can detect the existence of files hidden in file streams is sfind, which is included in the Foundstone Forensic Toolkit. Other files can be renamed, extensions changed, or file attributes manually changed to hide them. Hidden files could conceal sniffers, backdoors into the system, trojaned programs including rootkits, malicious code or viruses (Scambray, McClure & Kurtz).

Conclusion

Windows NT/2000 is deployed globally and the Microsoft Office Suite ranks among one of the most widely used software packages by corporate and government entities it is critical for a network administrator to be familiar with securing and protecting data present on Windows NT/2000 servers (Armstrong, 2001). In this paper, we reviewed some options on how to investigate a compromised system. Forensics is an extensive process that is time consuming and resource costly. These costs may be judged too high by some, but what would be most costly in the long run? To use the adequate resources in order to strengthen the network or to follow a laissez-faire policy hoping that the incident was an isolated event without detrimental consequences to an organization.

References

Sources cited in text:

Armstrong, Illena. "Windows vs. Linux: Taking Security Seriously." 2001. http://www.securityfocus.com/library/3446 (2 November 2001).

Farmer, Dan and Venema, Wietse. "Forensic Computer Analysis: An Introduction." Dr. Dobb's Journal. September, 2000. http://www.ddj.com/documents/s=881/ddj0009f/0009f.htm (1 November 2001).

Grace, Scott. "Computer Incident Response and Computer Forensics Overview." March 2001. http://www.sans.org/infosecFAQ/incident/IRCF.htm

Kruse, Warren G. and Jay G. Heiser. Computer Forensics: incident response essentials. Indianapolis: Addison-Wesley, 2002.

Mandia, Kevin and Chris Prosise. Incident Response: Investigating Computer Crime. Berkeley: McGraw-Hill, 2001.

McMillian, Jim. "Importance of a Standard Methodology in Computer Forensics." May 2000. http://www.sans.org/infosecFAQ/incident/methodology.htm

Romig, Steve. "Forensic Computer Investigations." October 2001. http://www.net.ohio-state.edu/security/talks/2001-10_forensic-computer-investigations/6up-pdf/ (2 November 2001)

Scambray, Joel, Stuart McClure, and George Kurtz. Hacking Exposed: Network Security Secrets and Solutions. Berkeley: Osborne/McGraw-Hill, 2001.