Global Information Assurance Certification Paper

Daeman Stewart
GSEC Practical Version 1.4b
Date submitted: April 12, 2004
Option 1 – Research on Topics in Information Security

Introduction to Incident Handling – A guide to safer computing within a Windows Environment

1.0 Executive Summary

The goal of this paper is to provide readers with a fundamental understanding of how to handle some of the most common threats in a Microsoft Windows environment. Because of the critical number of threats targeting windows systems, it has become more important than ever to be well-educated on this topic. By providing examples of common threats and defining the steps and tools required to handle them, my intention is that the reader will use this work as a reference guide for handling incidents of their own. This practical should prove to be most useful for home users and system administrators of local area networks (LAN) who may lack proper computer security skills. This paper will focus on two of the most common information security incidents, viruses and compromised systems.

2.0 Introduction

Computers running Microsoft Windows operating systems are vulnerable to a variety of different attacks- the most common being viruses and compromised systems. Both are capable of delivering malicious payloads and causing damage ranging from lost or corrupted data to theft of personal and financial information. Incident handling, therefore, is core essential knowledge for anyone who wants to use and maintain his or her computer safely and securely. Incident handling is the process of responding to and handling attacks. Handling is, of course, the procedures implemented for restoring a computer or network to its' pre-attack status. Having a clearly defined and documented Incident Handling procedure in place will strategically ensure that any incident you encounter is handled efficiently.

With the popular use of P2P (peer-to-peer) networks like Kazaa, Gnutella and Limewire, many people have become accustomed to downloading files from unknown sources. This poses a great risk to your system because it is virtually impossible to be certain of the integrity of the source file and the true contents of what you're downloading. Some viruses specifically target P2P networks, copying themselves to the users shared folder.

Whereas the most security conscious practice is one of abstaining from downloading files from unknown sources. Realistically a balance of common sense, following best practices and using the tools that are available to prevent attacks is the soundest advice. Being extra vigilant when downloading files from P2P networks, web sites, or emails is good practice. Be aware that malicious programs are often disguised as legitimate files such as songs, documents, and screensavers…

There are many methods used to secure computers, networks, and informational assets. They include the use of widely available software and hardware tools as well as commonly known suggested best practices such as using secure passwords and performing regularly scheduled backups of all your important data.

3.0 General Introduction – 6 Steps

This section will introduce each of the steps used to Handle Incidents. They are based on the Sans Institutes' "Incident Handling 6 Steps" [1] and include: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. These six steps will be the building blocks for the rest of this paper.

3.1 Step 1: Preparation

Having a systematic process in place for dealing with incidents will help limit damage caused by an attack. For this reason, I consider preparation the most crucially important of all six steps. Performing back-ups, software updates, and making use of available security tools can help secure your computer and the data within it.

Patching bugs and vulnerabilities is a must because they exist in all software. This includes all software that you run on your system(s), updating anti-virus software definitions and performing Windows updates as often as needed.

Using secure (hard to guess) passwords is a major contributor in limiting access to sensitive data. Using a minimum of "8 characters" is highly recommended [6]. Choose a mix of numbers, letters (upper & lower case), and symbols. Never write your password on paper or use dictionary words. Both can result in unauthorized access.

3.2 Step 2: Identification

There are many signs that might indicate an incident has already occurred. Anti-virus software reporting that a virus has been detected is one, others signs can

include poor system performance, system reboots, and unexplained events such as new user accounts. Another good method (requiring more advanced knowledge) is checking your system logs for anomalous (abnormal) activity. Microsoft Windows has an Event Viewer tool that can log suspicious activity/events much like an (IDS) Intrusion Detection System.

3.3 Step 3: Containment

Once you've identified that an incident has occurred, the next procedure is containment. If the computer in question is on a network, physically disconnecting it from the network is sufficient. If you're in a stand-alone environment (single computer), making sure you're not online (connected to the internet) is the most effective method of containment. In the case of a virus infection, keeping the system offline will ensure that the virus doesn't propagate (spread) to other systems. If the system has been compromised or hacked, keeping it offline will restrict remote access to it.

3.4 Step 4: Eradication

Eradication is the process of identifying the cause or weak point that allowed for the attack to occur in the first place. It will also aid you to avoid future attacks. This is not always the easiest thing to determine but when possible it can prove to be very useful. Often, back tracking your recent activities may prove helpful. Did you recently download an email attachment or a file from an untrusted source? If not, there may be a vulnerability on your system that was exploited. Make sure all your software has been updated with the most recent patches available.

3.5 Step 5: Recovery

The recovery phase includes restoring any files or programs that may have been corrupted by the incident. In the case of corrupted files, using the most recent backup of the files in question is often the best you can do. Before restoring any files, use your anti-virus software to scan them. This will ensure that you do not restore any files that are infected. If program files were infected, try uninstalling and then re-installing the software.

3.6 Step 6: Lessons learned

The lessons learned phase consists of analyzing both the attack and how you handled it. This phase of pausing and assessing can sometimes be undervalued and therefore overlooked but, in my opinion, it should always be followed. It will

help improve your computer's protection as well as improve your incident handling skills.

4.0 Handling Viruses

In the first three months of 2004 we've already experienced higher volumes of virus activity than in all of 2003 combined [7]. The recent batch of viruses - MyDoom, Beagle and NetSky, and their increasing number of variants are mainly to blame for these rising statistics.

A virus is a program that replicates and infects files and programs by attaching or inserting itself to other file(s). Most viruses simply replicate themselves but many contain malicious payloads, which means they can cause irreparable damage by corrupting or deleting important data.

True viruses require human assistance to infect other machines. A person can, for example, deliberately or not, infect another machine by transferring infected data from one machine to another via floppy disk or Writable CD.

A 'Worm' refers to a program that self propagates to other machines and network shares. Shares are resources such as files or applications that are made available (or shared) on a network. Mass mailing worms propagate via email and often arrive as attachments with legitimate looking file names. They search for email addresses on the infected systems hard drive and then email copies to all the addresses they find. The process continues once a new system is infected. In order to infect, most mass mailing worms require that you open an attachment but some others like Bubbleboy or the more recent Beagle.N are capable of executing simply by being previewed in programs like Microsoft Outlook.

Once a virus is released into the wild there are often modified versions released called Variants. These variants are often more dangerous then the originals like in the case of NetSky.D which reached "Category 4" [4], Symantec's Severe Risk Level. User-friendly tools capable of modifying viruses are widely available and often require minimal technical skills to use.

Be very careful when handling your email. Infected emails can come from both known and unknown sources. I recommend configuring your anti-virus software to scan all your emails. If you're attempting to determine if an attachment is safe or not, performing a web search on the attachment name can often provide important insight.

4.1 Step 1: Preparation

"February 2004 was the worst month in computing history for viruses" [3], As

such, having Anti-Virus software is very highly recommended security protection. Anti-Virus solutions are reasonably priced at around $50 (USD), a well-invested price to pay to protect your system. Having anti-virus software is not enough however. Keeping your anti-virus software updated is equally as important as it will help detect the most recent viruses. Most anti-virus vendors provide (automatic) live update features that can notify you when updates are available.

Another important update to perform on a regular basis is Microsoft's Windows Update. These updates will provide patches for your version of Windows and will correct issues ranging from performance bugs to major security vulnerabilities. Critical updates are most important and are "automatically selected" [5] by Microsoft's Windows Update service. You can access windows update from the start menu or by visiting http://www.microsoft.com/windowsupdate.

Back up your data! With the current cost of a CD-Writer (burner) being around $50 (USD) and Writable CD's (CDR's) costing about $1/CD (USD), it's never been easier to back up large amounts of data in such an easy and cost effective way.

4.2 Step 2: Identification

Early identification is important and can reduce the amount of potential damage caused by today's viruses. Having your virus definitions up to date, performing full system scans, and routinely scanning for both incoming and outgoing emails will help in early detection. Once the virus has been identified, containment is the next procedure.

4.3 Step 3: Containment

Disconnecting network access (Internet or Local Area Network) is of vital importance. This will prevent the virus from propagating to other systems. Un-plugging your network cables (modem or Network) and removing wireless access cards will be sufficient for that purpose, but will not stop a virus from infecting other files within the system. The process of Eradication should be dealt with as promptly as possible.

4.4 Step 4: Eradication

Eradicating viruses consists of removing the virus and all infected files from the system. Most anti-virus solutions can delete viruses and restore the infected files to their original state. Specific virus removal tools are often made available by Anti Virus Vendors. In cases where a virus cannot be successfully removed, formatting your system may be your only recourse.

Determining how the system became infected is an additional task that should be performed. It will help you avoid being re-infected.

4.5 Step 5: Recovery

The Recovery step is effectively implemented by replacing infected files with known good (clean) copies of the files or programs from Backups or Original CDs. I firmly recommend scanning any files before restoring them on the system. The last thing you want to do is restore a file that is infected! Once you've restored your system, it's time to validate it. Run a full system scan and perform any available updates before re-connecting it back on to the network/internet.

4.6 Step 6: Lessons learned

Mindfully and systematically taking the time to reflect on how you handled the incident and determining how the computer became infected will help improve your personal skills with the incident handling process. Avoidance of future infections is another prized lesson to take from striving for handling excellence.

5.0 Compromised Systems

System attacks exist mainly because of buggy code in software and in operating systems. Buggy code can often result in critical security flaws or vulnerabilities. When these vulnerabilities are detected, vendors are normally given a reasonable time frame in which they must produce a patch. Once a patch is available it's up to the user to download and apply it. Many won't know that the vulnerability or patch even exists and so will remain un-patched. This leaves them vulnerable to possible attacks. Exploit tools are specially crafted to exploit known vulnerabilities and can often result in someone gaining full access to your system, just as if they were sitting at your computer.

"Most hackers fall into the "script kiddie" category. These hackers will try to cause havoc and mischief on the Internet, as a game or a way of striking out anonymously" [11]. They use prefabricated hacker tools and are normally not very technical individuals. More dangerous are the Agenda hackers who have actual expertise and purposes for their hacking activities. These purposes can range from politically motivated attacks to industrial spies attempting to obtain proprietary information.

Often a hacker will use a compromised system as a launch pad for directing attacks towards other systems. This makes it much harder to determine an attacker's identity by creating a degree of separation between the attacker and his intended target(s).

Checking for patches for any software you may have installed is highly recommended. Resources like the Sans Institutes Top 20 Internet security threats and Security focus' BugTraq list are great resources for keeping up to date on vulnerabilities and patch information.
(http://www.sans.org/top20 - http://www.securityfocus.org/archive/1)

I will now explain some common methods of attack that can result in unauthorized access of your computer(s).

A **Trojan Horse** is a destructive program that masquerades as a benign application" [9]. They are often disguised as legitimate programs like screensaver, games, and popular media files. One of the most common examples is a Product called Back Orifice 2K. The tool is be distributed for legitimate security purposes but can also be also be used to take full control of another system. By using the Client interface, someone can control a system (running the server version) as if he/she were physically at the targeted computer. Trojans are hard to detect as they normally run in stealth mode.

A **BufferOverflow** is a very common security flaw. "The buffer overflow bug is caused by a typical mistake of not double-checking input, and allowing large input (like a login name of a thousand characters) "overflow" into some other region of memory, causing a crash or a break-in" [10]. Such an attack can often result with someone gaining full privileges or what is called "Root Access" on the target machine.

5.1 Step 1: Preparation

There are a several tools that can help prepare you for potential attacks. A first line of defense is often a Firewall. It is used to control access to and from your computer or network. Personal Firewalls such as Zone Alarm are applications that you run locally on a computer, they are usually simple to install and configure. Microsoft Windows XP comes with a basic internet firewall which can be enabled through the Network Icon in the control panel.

IDS (Intrusion Detection systems) such as Internet Security Systems' BlackIce can detect suspicious activity based on known signatures (or patterns of activity). BlackIce keeps logs of your computers events and includes a severity rating and explanation for each event. Microsoft's Event Viewer displays logs of Application,Security, and System events and is accessible from the Administrative Tools section of the control panel.

A Vulnerability scanner is another very useful tool, it helps avoid potential attacks by scaning systems for known vulnerabilities. After scanning, they generate reports detailing any vulnerabilities detected and rate them based on their

severity. You can then use this information to obtain and install the necessary updates and patches. On the down side, this sort of tool is also used for reconaissance purposes by hackers. Knowing what vulnerabilities a system has is an important factor in determining what method of attack to use on a target machine.

As always, regular scheduled back-ups of all important data is crucial in limiting the potential damages of any type of attack.

5.2 Step 2: Identification

The use of Firewalls, Anti-Trojan tools, and IDS's will increase your chances of detecting an intrusion. Random checks for determining what processes are running on your computer can also help detect unauthorized applications that may be running without your knowledge. Running processes can be viewed through the Task Manager tool in Microsoft Windows (Ctrl-Alt-Del and selecting the Task Manager).

5.3 Step 3: Containment

Containing the attack consists of isolating the system. Prevent remote access to the compromised system by disconnecting network access (network cables / wireless cards). It is also important to restrict physical access to the machine until it has been eradicated.

5.4 Step 4: Eradication

The Eradication process consists of removing the attack tool or patching the vulnerability or point of entry that allowed for the attack to take place. Anti-Virus software may detect some Trojans but in cases where it doesn't, Trojan Horse detection tools are available and very useful. A common one named "A Squared" is available in a free or paid version. If no Trojan Horse was found, then determining what vulnerability allowed the attack is necessary. It will help avoid falling victim to the same attack. Vulnerability scanners can help determine what vulnerabilities may have been used to exploit your system. Formatting the system, re-installing and updating all software is sometimes the easiest option.

5.5 Step 5: Recovery

If you were successful in the Eradication step and were able to determine the root cause or point of entry that the attack occurred, then formatting may not be required. Restore any files that may have been deleted or corrupted by the attack

by scanning them first and then copying them back to your system. Before going back online or re-connecting the system to the network, make sure your system is ready by scanning it for viruses and Trojans, and performing updates to your software and operating system.

5.6 Step 6: Lessons learned

Taking the extra time to reflect on how the incident was handled will help improve your process the next time around.

6.0 Conclusion

Becoming educated about the various threats faced by Windows systems is the first step to safer computing. Implementing tools such as Firewalls, Anti-Virus Software and performing updates for both your applications and Operating systems will greatly increase your system's overall level of protection.

Being prepared and having the necessary tools and processes in place for dealing with Incidents is a must, but won't avoid all attacks. Multiple vulnerabilities are detected everyday, according to the Cert Coordination Center "3,784 vulnerabilities were reported in 2003" [8]. Staying up to date on issues ranging from technology news, vulnerability lists, software updates and adhering to best practices is strongly recommended.

In conclusion, I want to firmly stress the importance of backing up your data. You can have every tool that exists on the market for preventing attacks but you'll never be 100% secure. Performing regularly scheduled backups of all your important data is the only way to ensure that you can successfully recover from an attack. Thoroughly following all six of the steps of the Incident Handling process is also essential. Often the last step (lessons learned) is not followed through because the system is usually back online and running fine again. Yet, on a final note, mindful reflection of your procedural experience while Incident handling is the only lasting way to continually improve on your incident handling skills. Having a documented process on hand ahead of time will enable you to confidently and properly handle your next Incident with success.

"Only through careful administration and protective measures can we secure our information and resources." [2]

Works Cited

[1] SANS Security Essentials II : Network Security "Incident Handling Foundations." 2002 - Section 1.2.4 (4-9)

[2] Rubin, Aviel D. White-Hat Security Arsenal – "Tackling the threats" (forward by William R. Cheswick) June 2001

[3] Ruiz, Yolanda. "This has been the most active period in the history of computer viruses" - Panda Software. March 1, 2004 http://www.pandasoftware.com/about/press/viewNews.aspx?noticia=4806&ver=21&pagina=&numprod=&entorno=

[4] Symantec Security Response "W32.Netsky.D@mm" - Symantec Corporation. March 12, 2004 http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.d@mm.html

[5] Microsoft Windows Update – "About Windows Update" - Microsoft Corporation http://v4.windowsupdate.microsoft.com/en/default.asp

[6] SANS Security Essentials II : Network Security Overview "Access Control Management." 2002 - Section 1.2.3 (3-37)

[7] Clark, Jack. "The virus avalanche" - BugWatch. March 17, 2004 http://www.vnunet.com/News/1153550

[8] Cert.org – "CERT/CC Statistics 1988-2003" - Vulnerabilities reported http://www.cert.org/stats/#vulnerabilities

[9] Webopedia.com. Trojan Horse - November 24, 2003 http://www.webopedia.com/TERM/T/Trojan_horse.html

[10] Buffer Overflow Description - Internet Security Sytems (ISS) http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/buffer_overflow/default.htm

[11] McAfee.com. "Who are Hackers? Where do they come from and why are they called hackers?" E-Security News http://dispatch.mcafee.com/esecuritynews/jan2002/firewallforum.asp

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor