Use offense to inform defense.
Find flaws before the bad guys do.

Marietta E. Kirby
Advanced Incident Handling Practical
"Your First Primary Incident Handler Case"

My first incident as a Computer Incident Response Primary Incident Handler came when I was still very new to incident handling. I had been previously working with Cisco Net Ranger and ISS Real Secure Intrusion Detection systems for my employer and was transferred into the Computer Incident Response Team. My background is Novell systems administration, so I had the basics of TCP/IP, various vulnerabilities, (ports, Trojans, etc.) down to an art, but handling an actual incident in real time was going to be a challenge. Needless to say, I was nervous. The company I work for is a very large worldwide company with 24/7 operations and an incident could happen at any time, on any day. Hopefully, I would be prepared.

Once I was first transferred, my responsibility was to analyze incident reports from offices all over the world. In this capacity, I would be able to disseminate information from log files and incident reports into a master incident database for tracking purposes. This was the first step in my education to becoming an incident handler. It allowed me the opportunity to dissect the log files for many different types of probes and exploits on various operating platforms in a real time basis as they were reported to the CIRT. Seeing these log files every day, though, could not prepare me for the panic which would ensue from the office which had their web server hacked. It was at this point that the critical stages of incident handling really came into play.

The six stages of an incident are preparation, identification, containment, eradication, recovery and follow-up. The following paragraphs describe my first incident through each phase of incident handling.

Preparation. This is the stage where you are preparing for the event of an incident. In this stage you should be preparing your "jump bag". This is the kit of tools, which you will need to adequately assess and evaluate the incident. Some items which should be required to be included would be forensic software, fresh back up media, CD's with binaries, Windows Resource Kit, a laptop with dual OS, your call list and phone book, cell phone and a small tape recorder or other note taking device.

In my role as a "call center" type of Incident Handler, I felt it was imperative to have a working library of documents ready to assist the victim sites with their situations. I worked on gathering together information on recovering from root compromises, Windows NT recovery, as well as developing various sets of instructions with step-by-step recovery methods to send to the victim sites.

After gathering this information, I proceeded to put together my call list for law enforcement, my chain of command, fellow incident handlers and company personnel. I also garnered a list of operating systems and the website locations for the hot fixes. Such as the link for Microsoft is: http://www.microsoft.com/ntserver/nts/downloads/default.asp#RecommendedUpdates. These updates occur frequently and having access to them quickly would be required to assess if a victim system was up to date on their patches. I also gathered information from the Computer Incident Response Team at Carnegie Mellon University at www.cert.org as well as SANS at www.sans.org both sites carry a wealth of information.

Identification. This phase consists of the actual identification of an incident. In this phase, the primary incident handler should be identified. The incident handler will be the person in charge of this particular incident. They will be looking for indications and warnings, flushing out the intelligence information from users and systems administrators. Then fusing the information together to make an educated guess as to the whether or not an event is actually an incident.

Most of the information involving an incident comes from the system administrators and end users. You should be carefully documenting all the interviews and evidence that you gather. Some bits and pieces of information in and of itself may not be significant, but in a whole case scenario, the puzzle will start to come together. Documentation is very important should the case go to trial. It will also help you to assess the situation after the fact when you are putting together your final report on the incident. This is the time to begin your evidence gathering, being careful not to delete or overwrite any files.

Communications play a key role in this stage, too. You should begin to contact the appropriate people. Keeping a low key, calm presence is important in maintaining control of the situation.

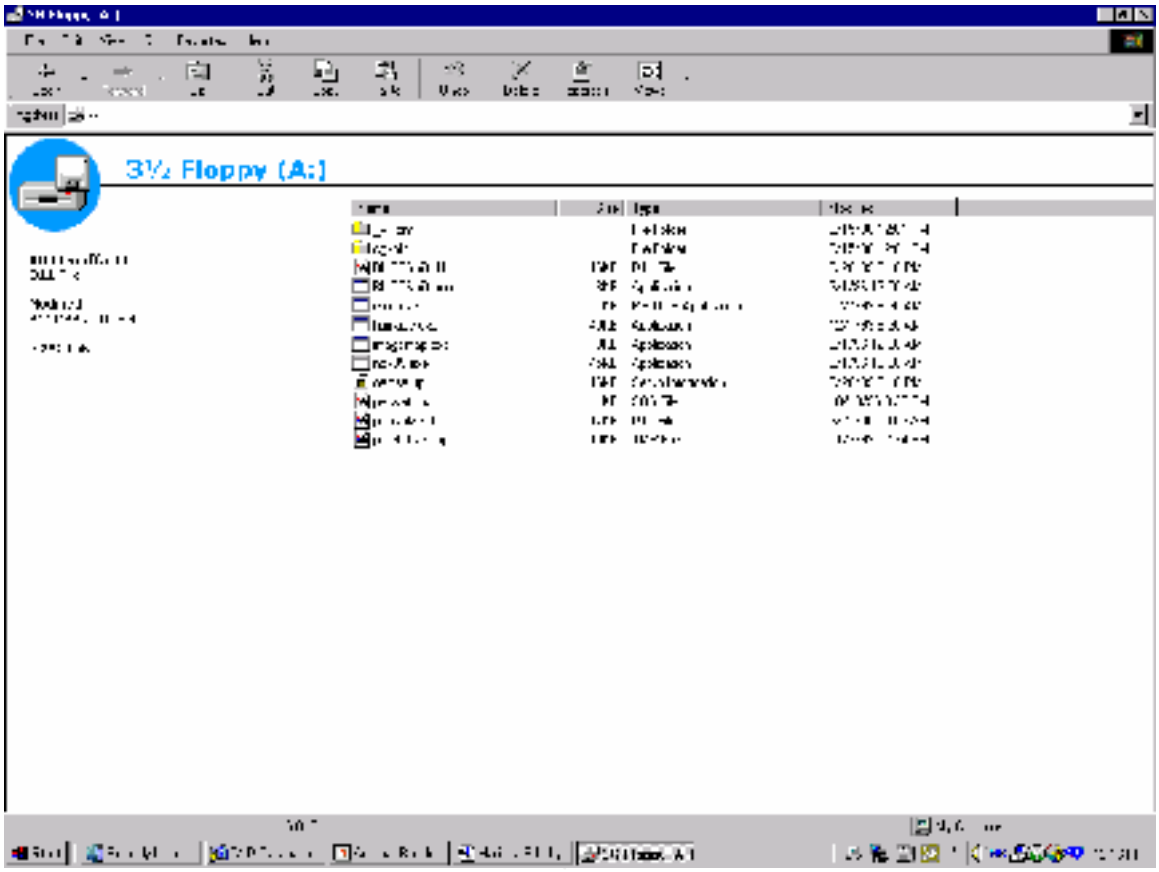
On May 31, 2000, I received a telephone call from the system administrator of one of our websites located in Florida. When Mr. Administrator was initiating his morning assessment of his network. His anti-virus software Net Shield, advised him that a file, patch.0xe.tmp, had the Netbus.svr virus. Considering the recent publicity involved with the “love bug” virus program, Mr. Administrator was very upset. He had assessed his own situation, and called to inform me that his entire network was infected with the Netbus virus and his anti-virus software could not clean it.

After trying to calm this system administrator down, I continued to garner the more information from him. I got his job title, who he reported to and his phone number. From there I moved on to the type of operating system he employed, which happened to be a Windows NT Server. Are you running IIS and/or Frontpage? He informed me that he was running both; I informed him that there were various vulnerabilities in these programs and we would discuss that

situation later. I asked him if the site was up or down? He said that he had taken it offline, afraid of infecting his entire network with this virus. Excellent move, because if it was a virus, it was isolated, or if it was a hack, the box was unavailable to the attacker for further manipulation. I then asked him for the version of the software and the service pack number he was running and he didn't know offhand. I asked him if he had paper handy, then asked him to make a list of some additional information I was going to need from him. I needed him to find out for sure the version number and service pack he was running on his Windows NT Server.

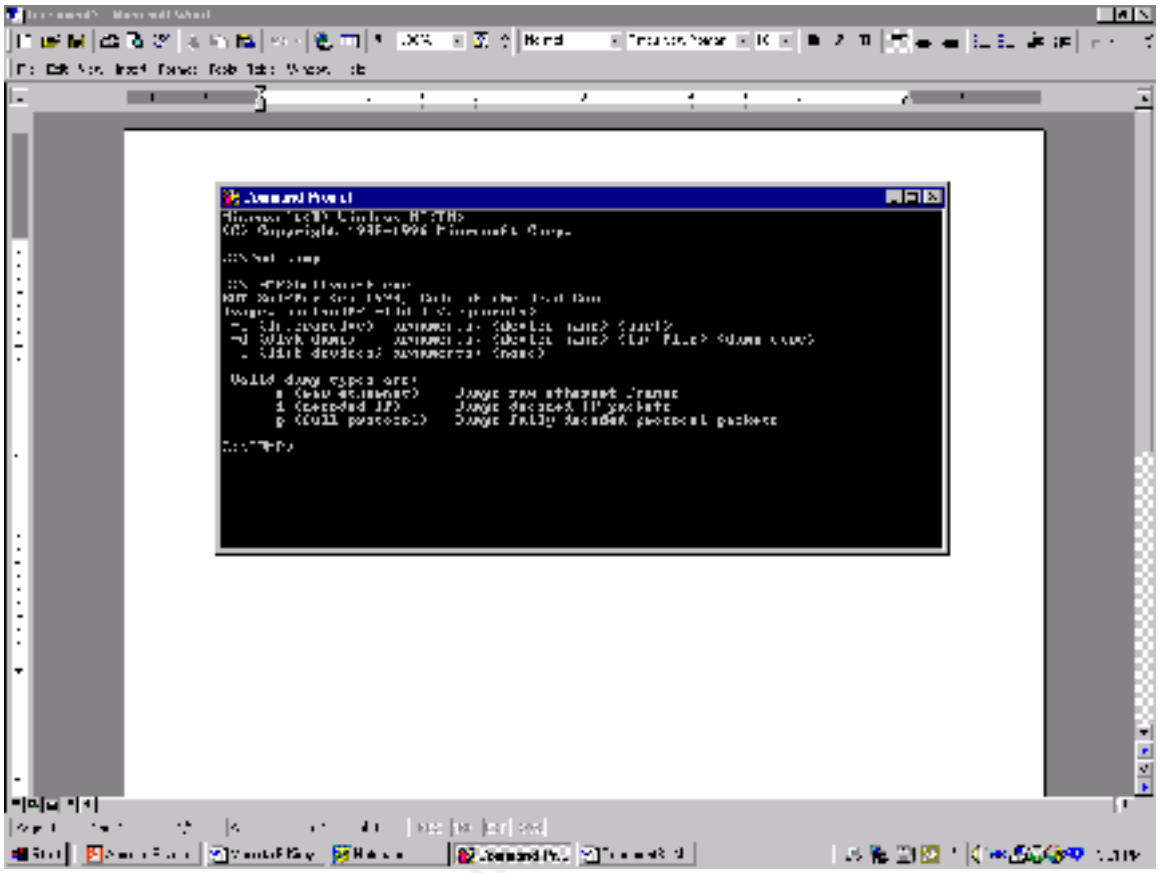
Next, I asked him if he had made any changes to his system or any files on the system. He had not, and I breathed a sigh of relief. My next question was to inquire as to the mission of the system. This question is very important. Number one, because his had told me that his system was already offline, and number two, I wanted to know who is going to be calling my boss demanding his system to be put back online. I was informed that the box was a web server used for the Personnel department. Prospective employees searched the website for job listings and used the site to forward their resumes for consideration. He did not consider the box to be mission essential. I then continued to document information concerning the ip address and domain name of the server that had been compromised and what additional services, if any were running on the machine.

My next question was to ask if there were any other clues that he saw when he looked in his file directories. He stated that his NT Event Log Detail had been popping up error messages that stated, *"The script started from the URL '/cgi-bin/ncx99.exe' with parameters" has not responded within the configured timeout period. The HTTP server is terminating the script."* I suggested that we look for that particular directory. The following is a screen capture replica of the contents of the cgi_bin.



As you can see, there are various files listed. The most significant clue was buttsniff.exe and buttsniff.d11, but we can also see that the executable file that was hanging on the NT Event logger was also in this directory. These files, in his system were modified on May 30, 2000 at approximately 6:15 pm. Okay, we have an incident. Mr. Administrator, you have Trojan programs loaded on your machine. Let's proceed to the next step of the incident handling process.

First a little background on the Trojan program BUTTSniffer, which was installed on this system. It is a packet sniffer and network monitor. It works as a standalone executable, and as plug in for Back Orifice. It features TCP Connection monitoring, full and split screen access, text and hexadecimal views, password sniffing with a full phrase catcher built in. The latest version currently supports HTTP basic authentication, FTP, and Telnet logins. Packet filtering and firewall style filtering lists are a nice feature and you can exclude and/or include ranges of IP addresses and ports. The program can be started on any of the system's network interfaces. Multiple instances of BUTTSniffer can be run at the same time and it has an interactive mode. It also spawns a port that you can telnet to, and displays an easy to use vt100 menu based user interface for remote sniffer access. The problem is, it could have been loaded locally. But was it? The following is a screen capture of the BUTTsniff.exe executed at the command prompt with the various arguments available.



Containment. In this phase, you should be deploying an on-site team to survey the situation. In my organization, we have a core incident handling team that covers incidents in our company from a centralized location. Our law enforcement personnel handle the majority of our on-site work. They are based out of our office and have field representatives to handle most locations, which we may have occasioned to utilize. Therefore, I placed a telephone call to our internal team and informed them of the situation. It is their responsibility to assign an agent to the incident. They gave me the name and telephone number of the agent who would be in charge of this case. I informed my victim site of this information and told him that this agent would be contacting him to ensure the security of the site and the evidence.

In conjunction with informing law enforcement, my number one goal in this phase is to secure the area. Granted, it is not very easy to do over the phone, but we have a strict policy of evidence gathering. Getting the system off of the network to protect your data should be paramount, if at all possible. The attacker could

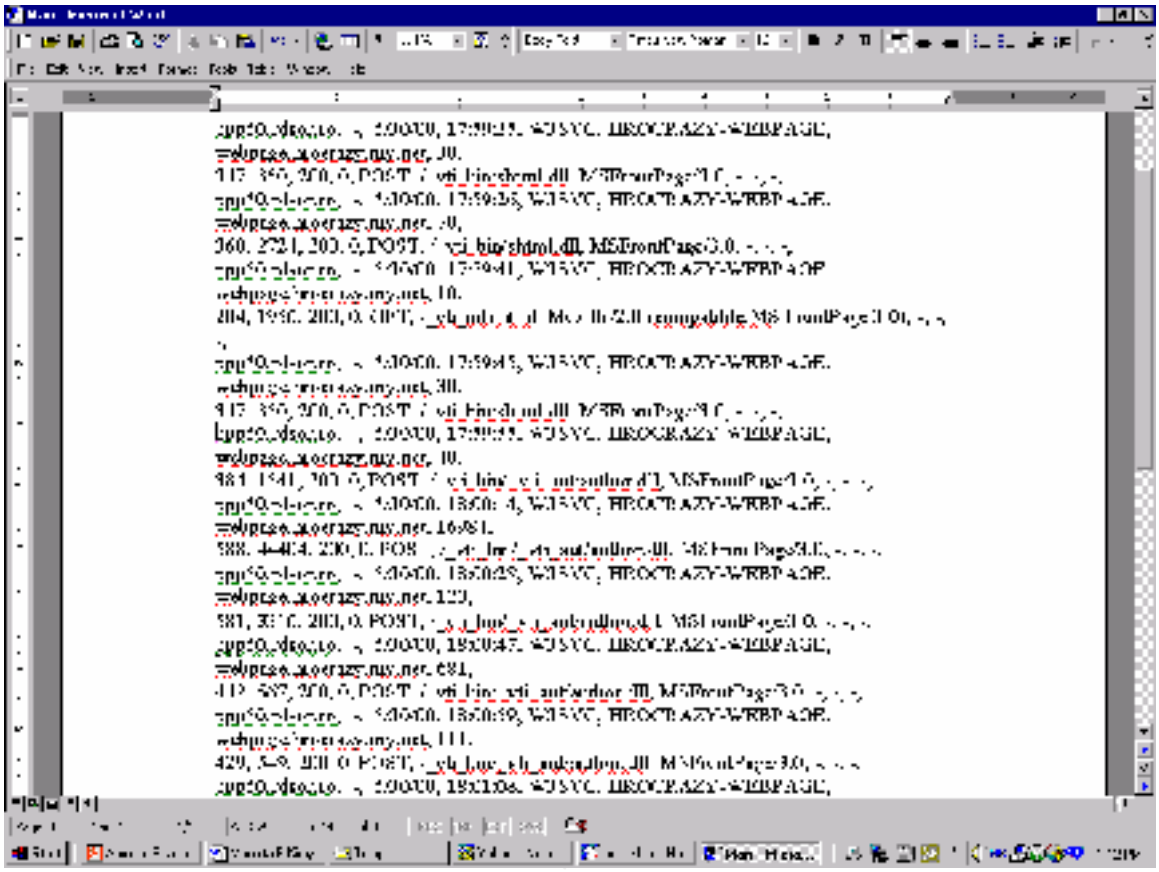
possibly still be in your system; this action effectually denies his access to your system.

At this point a zero level back up is required. If it is at all possible, in our organization, we take the original hard drive into evidence. This is accomplished by having the hard drive removed, placed into an evidence bag, signed and dated with the time recorded. The bag is sealed and placed in a locked and secured location. We use evidence custody documents, which record every movement of the hard drive. From person to person, even from person to facility, even if it is a file cabinet. Each movement of the evidence is signed and dated with the time recorded. This ensures the safe keeping of the evidence.

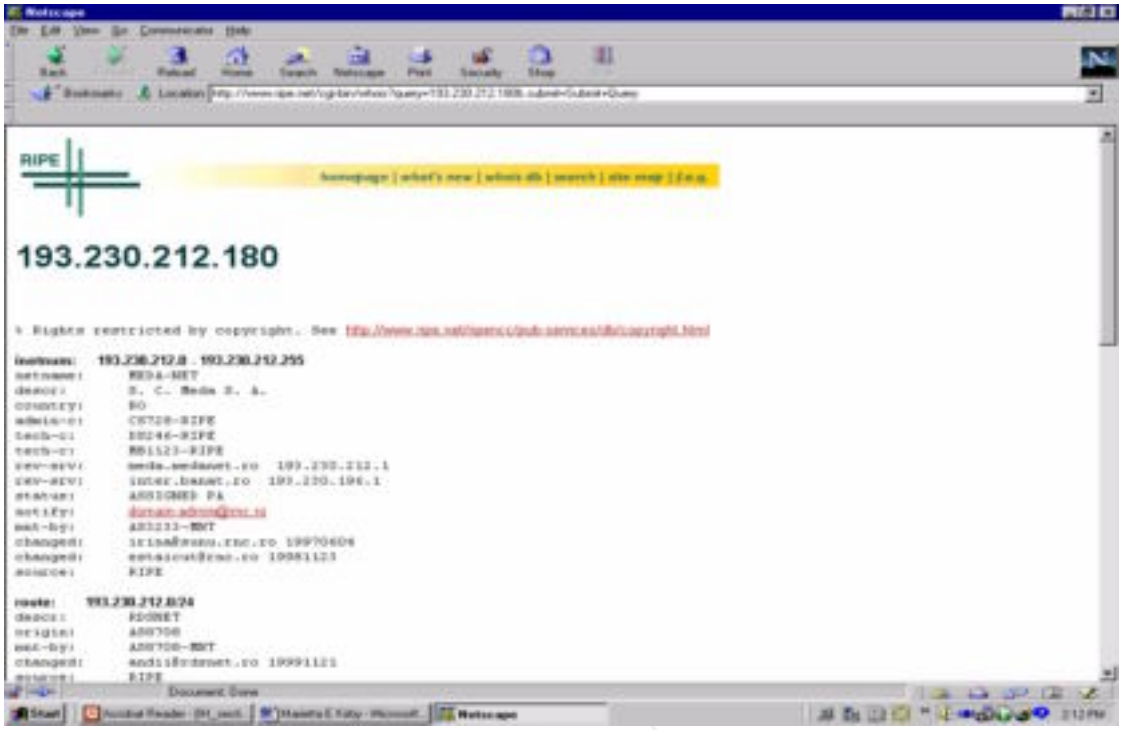
I forwarded Mr. Administrator a current copy of our published policy on web page security. This documentation includes information on the Microsoft IIS Vulnerability, and the Microsoft FrontPage Vulnerability. This information and research that he needs to do will keep him busy while we wait for law enforcement to get to his location.

Our next step is to acquire log files and other sources of information. It is imperative that you know the operating system with which you are working. It is especially important for our organization, as we are handling the event over the telephone and we employ all types operating platforms in our company. We need to be able to describe the exact log files we will be requiring, as well as providing the path to them. Of course this information varies with operating systems, and you should be prepared to disseminate this information to the victim site.

Since I suspected the Microsoft FrontPage vulnerability had been exploited, I requested a copy of the server log files. When I receive these log files, I usually convert them to a Microsoft Word document and do a search for POST commands. A copy of the log files follows:

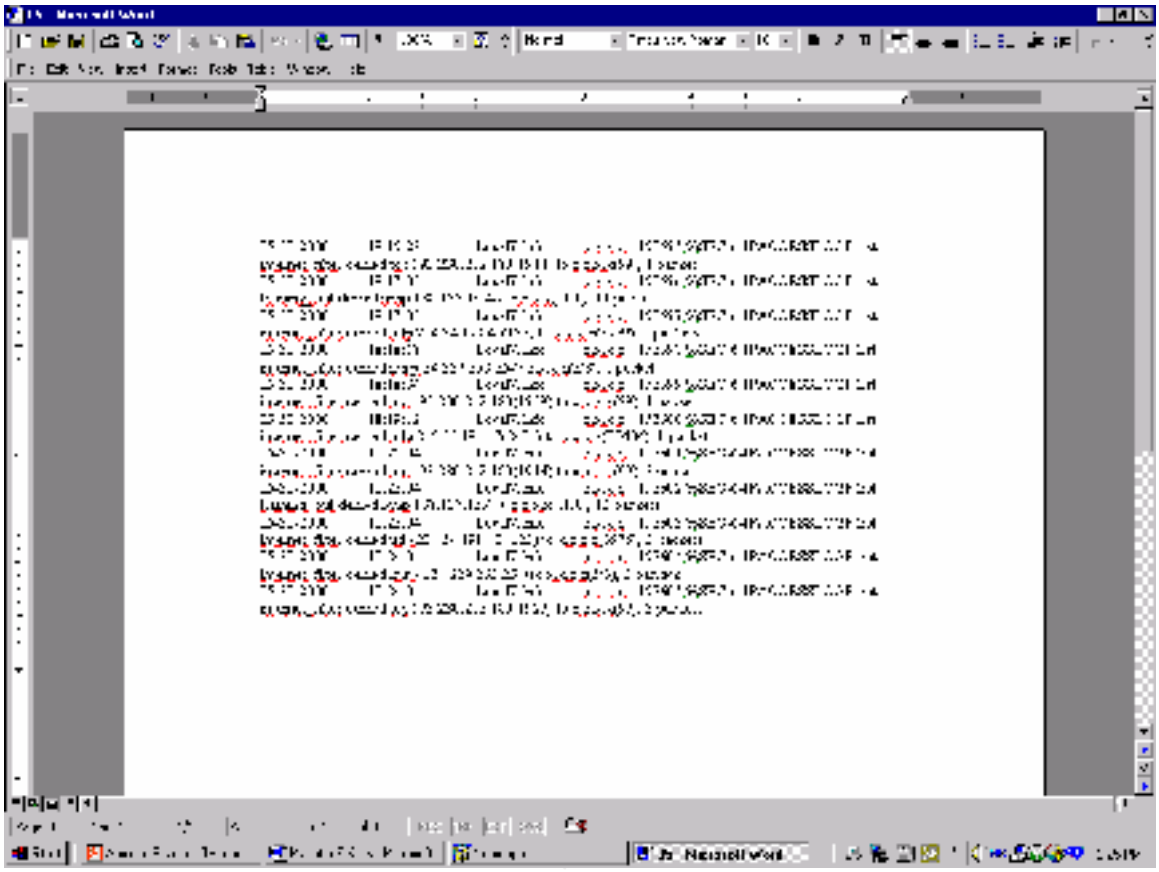


Looking at the post data, I was able to find the domain name of the attacker. This attacker has a domain name of ppp50.rdsor.ro. Doing an nslookup, I was able to obtain the ip address of 203.230.212.180. Which resolves in ripe as Meda Net out of Romania. The ripe whois interface follows giving contact information for this Internet service provider, etc. Keep in mind, I am at a different location from the victim site, therefore, my lookups do not affect the hacker looking at the victim box. I quickly passed this information to our law enforcement agent in the field.



Since it appears now that I have verified a foreign attack. There are various cracker/hacker groups operating from Romania. They are usually not malicious and only wish to share their political views with the world. Although, not usually malicious they are intent on defacing web pages. Now, I want to get the server connection logs. Performing a search of the connection logs, I was able to correlate the timing in which the attacker was logged into the box. The time of the file modifications, the time of the POST transactions and the connection information all would assist me in determining the method of attack. From the directory listings and the log files, I was able to tell which files the attacker was able to modify.

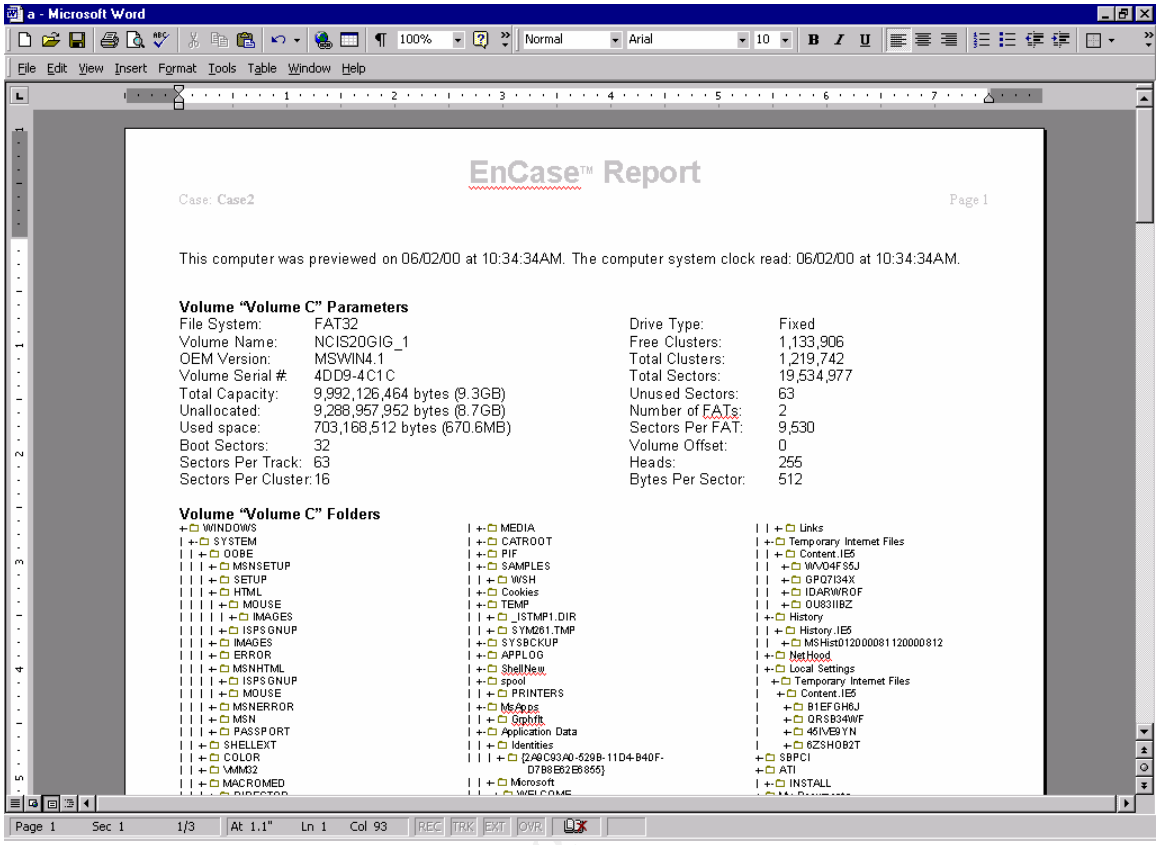
From the connection logs which follow, I was able to determine that the attacker was able to connect on port 99, which is a hidden Trojan port. Since the Trojan program that was placed on the server contains a password sniffer, we discussed a having the victim site perform a password change operation.



Eradication

In this phase of incident handling, you must determine the cause and symptoms of an incident using information gathered during the identification phase. Determine how to improve your defenses with firewalls; router filters, moving the system to a new name and ip address. Perform vulnerability assessments on the system before you place it back on line. Our company uses ISS Internet Scanner for our vulnerability assessments. After you assess your system, make sure to take the steps necessary to patch your vulnerabilities.

Our law enforcement uses a specialized software package call Encase to analyze the hard drive. This is a forensic program with various safeguards to protect the data, as well as hashing to prove the integrity of the system. A screen capture of a sample system follows.



Recovery. Our policy is to have the site reload the operating system from good media. Patch the security holes, and then replace the data files from backup prior to the incident, if a date can be ascertained. Once the system has been restored, verify that the operation was a success and the system is back to normal condition. Then decide when to restore normal operations. After resuming normal activity, continue to monitor for backdoors, which may have escaped detection.

Since the hard drive was removed for evidence purposes. The system administrator had to install a new hard drive. Then he had to reload the Windows NT Server from original media, install Service Pack 6. Load the fixes for the Microsoft IIS and FrontPage vulnerabilities.

As a matter of policy, we conduct an "On-line survey" of the victimized system. This provides information concerning the system vulnerabilities. Our company uses ISS Internet Scanner. We provide them with a list of services running on their system and the ports and services we feel they should disable.

Follow-up. This is the time to write up your report concerning this incident. Use all your notes and follow the guidelines provided by your CIRT. Encourage all

affected parties to review the draft, attempt to reach an agreement because it may make a difference in your case, should it reach trial. Provide an executive summary to management.

The lessons learned discussions from this incident included call tree problems, vulnerability updates which should have been installed, and call notification trees. Our lessons learned included the following:

A. *Notification Tree:* Obviously communications is absolutely paramount in this process, however the time required keeping all concerned updated can become time consuming. Recommend the formulation and implementation of a notification tree.

B. *Collateral information*: While processing open incidents, the Intrusion Detection Department was able to provide a list of IP addresses conducting suspicious activity: This activity could and/or may have been directly involved with the incident reports.

C. *Vulnerability Updates:* It is becoming increasingly noticeable that patches that are readily available are not being loaded. We need to develop a system of checks and balances concerning system administrator's responsibilities to their managers. The problem is that upper management is usually not technically aware enough to know what questions to ask. Therefore, we suggest developing a quarterly "hot topics" list, which addresses the agenda which management can use to assist in information security.

Executive Summary

On May 31, 2000, Mr. System Administrator began his normal morning duties, when he was advised by Net Shield, anti-virus software, that a file called patch.0xe.tmp was infected with the netbus.svr virus. The anti-virus software was unable to clean the file and advised him to check the registry of hrocrazy.my.net. Mr. Administrator disconnected the system from the network and placed a telephone call to CIRT team. The incident handler on your case was able to ascertain that a Trojan program was installed on the subject system.

The vulnerability used to exploit subject system is a widely know vulnerability and patches are available although not installed on the system. The system has now been updated and is back in service. Suggest considering a firewall installation to further secure the subject system.

Last Updated: July 22nd, 2018

Upcoming SANS Penetration Testing

SANS Pen Test Berlin 2018	Berlin, Germany	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS vLive - SEC560: Network Penetration Testing and Ethical Hacking	SEC560 - 201807,	Jul 24, 2018 - Aug 30, 2018	vLive
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
San Antonio 2018 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
Security Awareness Summit & Training 2018	Charleston, SC	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
Mentor Session - AW SEC560	Austin, TX	Aug 08, 2018 - Oct 10, 2018	Mentor
Northern Virginia- Alexandria 2018 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
SANS Northern Virginia- Alexandria 2018	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS New York City Summer 2018	New York City, NY	Aug 13, 2018 - Aug 18, 2018	Live Event
Northern Virginia- Alexandria 2018 - SEC542: Web App Penetration Testing and Ethical Hacking	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
SANS Krakow 2018	Krakow, Poland	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Chicago 2018	Chicago, IL	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, Czech Republic	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
Mentor Session - SEC504	Cincinnati, OH	Aug 21, 2018 - Oct 02, 2018	Mentor
Mentor Session - SEC542	Denver, CO	Aug 23, 2018 - Oct 25, 2018	Mentor
SANS San Francisco Summer 2018	San Francisco, CA	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, India	Aug 27, 2018 - Sep 01, 2018	Live Event
Mentor Session AW - SEC504	New York, NY	Aug 27, 2018 - Sep 17, 2018	Mentor
SANS Copenhagen August 2018	Copenhagen, Denmark	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Wellington 2018	Wellington, New Zealand	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FL	Sep 04, 2018 - Sep 09, 2018	Live Event
Mentor Session AW - SEC560	Chantilly, VA	Sep 05, 2018 - Sep 12, 2018	Mentor
Threat Hunting & Incident Response Summit & Training 2018	New Orleans, LA	Sep 06, 2018 - Sep 13, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MD	Sep 08, 2018 - Sep 15, 2018	Live Event
Threat Hunting & IR Summit - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	New Orleans, LA	Sep 08, 2018 - Sep 13, 2018	vLive
Community SANS Toronto SEC504	Toronto, ON	Sep 10, 2018 - Sep 15, 2018	Community SANS
SANS Alaska Summit & Training 2018	Anchorage, AK	Sep 10, 2018 - Sep 15, 2018	Live Event