Incident Report for GCIH
Network Security 2000, in Monterey, CA, October 2000
Scott White
November 22, 2000

Option 1 – Illustrate an Incident

1. Executive Summary

The information in this report documents an incident that occurred the third week of February 2000. Since our organization has never had an incident response policy, no procedure was in place for the handling of this incident. It prompted my initiation into security training. I have been put in charge of handling security for our organization, which held the belief that a firewall was sufficient for all problems. This event changed that idea, and has prompted my pursuit of incident handling to prepare for future incidents as they may occur. I intend to illustrate our incident, and how it should have been handled based on the material covered during the Incident Handling session held in Monterey, CA.

During the week starting February 14, our help desk received calls about lost files from our network drives. As the week progressed the number of calls escalated. With the distribution of calls from many unrelated departments, we became concerned that something had happened on a larger scale than any specific user error might have accounted for.

We noticed that all the files missing had been "deleted" on that Monday from the date of the last valid backups for the missing files. They had also disappeared from an organization wide shared network drive. As calls continued to come in, we found that the engineering department had lost files from their shared drives accessible only to their department, making us believe that the problem had originated in that area. I interviewed the employees in that department and on Thursday, one employee admitted to trying to run an executable attachment to an email he had received from a friend working in another department. The timestamps of several of the missing files coincided closely with the time he had executed this program. We removed his machine from the network, and began to track down who had sent him the message.

From the header file and mail logs the message appeared to come from another machine on our network. On calling the owner of this machine, we discovered that that individual had been out of the office for a 2-week period during which this incident occurred. Upon investigating the machine itself, the event logs show that during this time, the machine had not been running. Further research showed that the userid that was used as the sender had been out of service for over a year prior to its use. It was presumed at this point that the address and userid used to commit this incident had been spoofed, and the network logs were the next in line to be checked. While this was going on, the user's pc was placed on a test network, to see if it was safe for the network. Upon booting up, no problems were discovered, except the absence of any Word, Access, or Excel files on the system. The executable in question was copied to a floppy, and another test machine was

infected with the executable to observe from start to finish what appeared to happen. We do not currently run any host based intrusion detection software, but are looking to evaluate several products at this time. The only noticed change was the deletion of all Word, Excel, and Access related files from the new test system. With no way of telling if this system was further infected, both systems were nuked. The user had kept all critical files on the network drives to allow for full backups of the information to be run. His machine was reinstalled after a full wipe of the previous info, reconfigured, and returned to the owner. No repeat occurrences have happened.

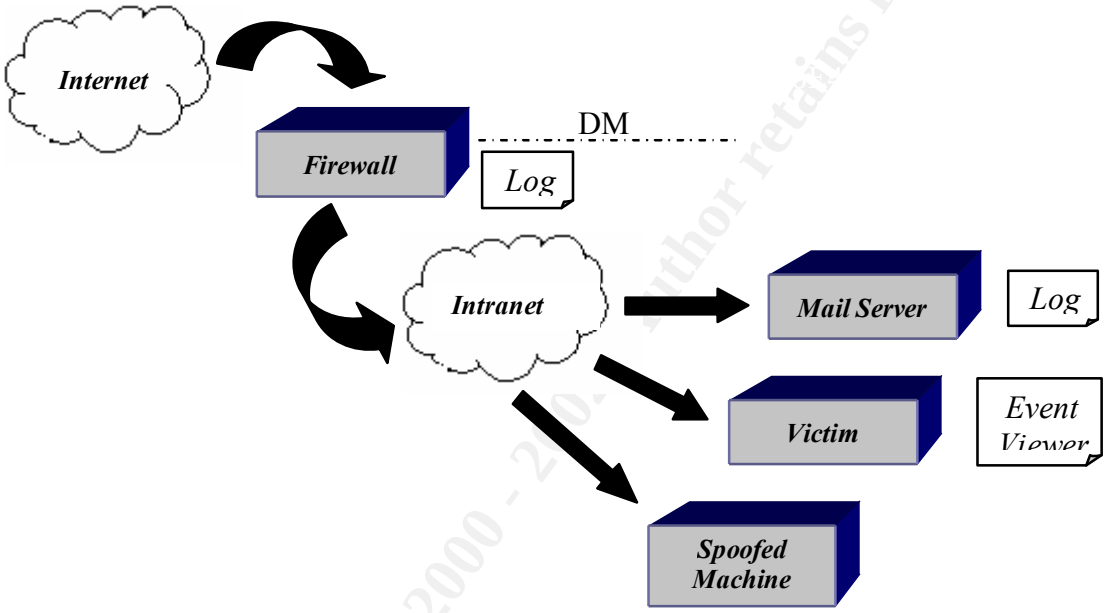

Figure 1. Illustration of network setup at the time of incident.

Six Stages of Incident Handling

The six stages of incident handling are preparation, identification, containment, eradiation, recovery and lessons learned. A short description of each step follows.

1. PREPARATION. Preparation involves prior planning on how to respond to incidents. It involves answering questions of policy, contact persons, data protection, tools needed to meet the requirements for incident handling, i.e. backup software, safe binaries, and proper system documentation when an incident occurs.

2. IDENTIFICATION. Identification begins as the detection of disparities and unauthorized changes to systems and networks. The detection can arise from review of network traffic, system logs, and from help desk logs. Having a user inform you of problems can prevent unnoticed problems from escalating. The determination of the severity of the incident arises from this detection and the following investigation. To identify an incident requires that the event is found to be abnormal, and not related to normal activity. Once the full extent of the incident is known, the notification of appropriate parties, and remaining steps in the incident handling process can begin.

3. CONTAINMENT. Containment as it states is an effort to minimize the damage that could result from the incident. It often will require that the compromised system is removed from use, unless it is believed that greater good can come from further observation of the attackers actions.

4. ERADICATION. Eradication is composed of steps taken to remove the attackers presence from your network. Further steps that can be enacted to prevent new attempts should be enacted at this point.

5. RECOVERY. Recovery is taken after the incident is understood, and the vulnerabilities that led to it are rectified. At this point, affected systems are rebuilt, and backups restored to allow for normal operation to continue.

6. FOLLOW-UP. Follow-up is used to enact procedures that are discovered through post incident meetings that will improve the handling of events in the future.

2. Preparation

A comprehensive list of steps to follow during the preparation stage of incident handling is as follows:

- Establish policy and post warning banners
- Develop management support for an incident handling capability
- Select incident handling team members and organize a team
- Develop an emergency communications plan
- Provide easy reporting facilities
- Conduct training for team members
- Establish guidelines for interdepartmental cooperation
- Pay particular attention to relationships with system administrators and network managers
- Develop interfaces to law enforcement agencies and other computer incident response teams

In our organization, none of these steps had been fully implemented. The concepts that come with incident handling were unknown to us. In the following section I will attempt to show how we handled our situation in relation to the prescribed steps.

Preparation is the first stage of incident handling. The first item on the preparation checklist is policy. We have a standing written policy that is required reading and must be agreed upon by all new employees in our organization. This policy states proper use of computer resources, and imposes that no privacy is to be expected on organization computers. Currently no warning banner exists on our systems, but a draft of a warning banner has been prepared and is waiting approval from our legal support. Other policies at the time of the incident required the placement and maintenance of a perimeter firewall to protect our internal network from external sources.

Our situation at this time does not allow for the creation of a true incident handling team. We do not have enough employees to man a complete incident handling team, so our organization had to rely upon the main administrators for specific systems to serve as point of contact in handling the incidents in relation to their systems. A list of work, home, and other personal numbers is kept in several locations throughout the organization.

Data in this organization is being maintained and backed up on a nightly basis. We test this data occasionally by restoring files to systems and verifying their validity.

Presently we are creating a jump bag. The need for which only became apparent since my attendance of the SANS advanced incident handling course. When completed this bag should include CDs with binaries, Windows resource kits, a small hub, forensic software, binary backup software i.e. ghost, a call list, cell phone with extra batteries, small tape recorder, and a laptop with dual operating systems.

Steps needing further implementation based on the information provided by the advanced incident-handling course are:

- Evaluate the need for secure encrypted communications. Our site doesn't normally rely on email communications, but should any outside communications be demanded, the need requires looking into.
- Establish an easy reporting system to make the gathering of information and documentation quick and efficient.
- Develop guidelines that will govern interdepartmental communications and cooperation.
- Contacting and developing relationships with law enforcement agencies and computer incident response teams will only help in future incidents.
- A network intrusion detection system has been added since this incident, and a host based intrusion detection system is being evaluated for future use.
- Finally new corporate anti-virus software has been distributed to all systems within the organization and is running weekly updates on the dat files.

3. Identification

A comprehensive list of steps to follow during the preparation stage of incident handling is as follows:

- Assign a person to be responsible for the incident
- Determine whether or not an event is actually an incident
- Be careful to maintain provable chain of custody
- Coordinate with the people who provide your network service (ISP)
- Notify appropriate officials

In the following section I will attempt to show how we handled our situation in relation to the prescribed steps.

Identification began after calls to the help desk began to show a pattern of missing or deleted files from the network drives. These calls started coming in late on February 14th 2000. As the week progressed, a pattern to the problem emerged. The problem displayed itself as a general deletion of all MS Word, Excel, and Access files on the network drive shared across the entire organization. By Thursday of this week, calls had begun to show that files located on the Engineering shared drive had also been deleted. Since no other department lost any information, this narrowed the problem down to the Engineering department because of their read and write privileges on this particular drive.

As the individual assigned to investigate the incident, I interviewed the department head to gain an image of problems that his group had during this week. After talking with several of his people, one user, user0, admitted to having received an email from a coworker, user1, earlier in the week with an executable attachment. He ran the program several times but didn't think anything was happening, so he figured it was just corrupt. I checked user0's email and event logs, and determined when he received the message and executed the attachment. His execution of the program coincided with the deletion of files from his system and the network. So I had found who had started the problem, but not where it came from. Our current virus-protection at the time did not detect the program as a known virus. Upon investigating user1, we found that he had not sent the message. The userid that generated the message had not been used for several years, and did not exist on the main UNIX or NT servers.

We use a static DNS host file, and we were able to determine the sender's IP address. From looking at the headers of the email in question, the message appeared to have been sent from a pc located in our health department. With the location of the suspected pc found, a trip to the health department was made. The owner of the pc had been on vacation for 2 weeks during which this incident had occurred. After checking the system's event log, and mail clients setup, it was determined that this machine had not been turned on during the event and could not be the source of the incident.

The final step in our identification was to check the firewall logs and try to determine if any spoofing had come from outside our network, but learned that the present network administrator had a policy of deleting logs after two days. Leaving us at a dead-end in

our pursuit of the true source of the malicious code. After interviewing our firewall administrator, we learned that address spoofing is blocked from outside sources leading us to believe that the attacker was internal, and had used an address that he determined was not currently being used on our network. This helped eliminate the importance of the firewall logs in reference to this particular incident. However, the logs are now being kept, and backed up on a more regular schedule. The guilty party apparently had knowledge of internal relationships between user0 and user1, userid structure used within our organization, and how to "spoof" a userid and IP address for our network. At this point we knew of no other options that we could use in the pursuit of the attacker.

Steps needing further implementation based on the information provided by the advanced incident-handling course are:

- Maintenance of a provable chain of custody. Our organization having never been involved in an investigation did not have the procedure in place to properly handle evidence.
- Coordination with our ISP. In this case the attack appeared to come from within so the assistance of the ISP would not be required, but in future cases this avenue needs to be pursued.

4. Containment

A comprehensive list of steps to follow during the preparation stage of incident handling is as follows:

- Deploy the on-site team to survey the situation
- Keep a low profile
- Avoid, if possible, potentially compromised code
- Backup the system
- Determine the risk of continuing operation
- Continue to consult with system owners

- Change passwords

In the remainder of this section I will show how we handled our situation in relation to the prescribed steps and what steps need work.

Since we do not have a team, I was assigned the responsibility to investigate this incident. Containment began once it was determined that user0's pc had been the source of the file deletions. Our first step was to remove this machine from the network. The owner had kept his major files on the network drives, which are backed up regularly, but his local files had been lost to the malicious program. A test network was established and a test machine was setup with the same configuration as user0's pc, leaving user0's pc untouched while the extent of his problem could be determined. A copy of the malicious

program was executed on the test system and changes to the system were documented. The only changes noticed at that time were the deletion of the related MS Word, Excel, and Access files. Being new to the security aspect of working with computers, we did not possess proper software to correctly identify all possible changes to the system at the time of this incident. With our concern for something that could be missed in our quick check of the system it was decided that the system should be rebuilt from the ground up.

The steps that should be taken in this situation differ from those we performed. A complete binary backup of the PC in question should have been made, and from these copies the testing of the system should have taken place. The original system hard drive should be stored and labeled in the event that it is needed as evidence. From this copy the event logs could be obtained and reviewed. Also more complete documents needed to be kept. As a final step in our containment, the local administrator passwords were changed for the "infected" machine as well as those in the same section of the network.

5. Eradication

A comprehensive list of steps to follow during the preparation stage of incident handling is as follows:

- Determine cause and symptoms of the incident
- Improve defenses
- Perform vulnerability analysis
- Remove the cause of the incident
- Locate the most recent backup

With the source of the incident found, eradication could begin. From the investigation at this point, there did not appear to be a great compromise in our network and firewall. We decided that the existing policy of not running email attachments from people that are not known to you would have prevented this incident from affecting the larger user community. Our NT desktop group is responsible for recovering the operating system and configuring the system to return damaged systems to production. This process uses a complete wipe of the existing system and restoring the software from a disk image that has been built and configured clean of any possible corruption. Our UNIX system administrator was contacted and asked to restore all missing files from our victim, user0, and once restored, we verified the data. The last step for this system was to ensure that a good copy of our anti-virus software was installed on his system, and that his department was made current with respect to this software. This effectively removed the program from our network, and all effects from this system. Had the trail been clearer, or with more experience, we believe that the attacker might have been caught.

To improve our defenses, a network intrusion detection system was installed. The firewall rules have been reviewed, and the firewall software has been upgraded, and all current patches have been installed. Also in this case, a reminder memo was sent to all

users restating the policy that no attachments should be trusted from people that you either do not know, or have not solicited mail from.

In this stage of incident handling, several more steps could be imposed to prevent any future incidents:

- Perform vulnerability analysis on our network to find possible holes in network configuration.
- Perform system vulnerability analysis.

Using commercial products, or one of the several free tools available can satisfy these steps. However the commercial products can be very expensive. If this is an issue, one of the free tools like nmap can be used.

6. Recovery

A comprehensive list of steps to follow during the preparation stage of incident handling is as follows:

- Restore the system
- Validate the system
- Decide when to restore operations
- Monitor the systems

After reinstalling the users system from the disk image used for the engineering department, I installed all the current patches and service packs. Then I verified that user0 was able to connect to the network. At this point, user0 was required to install and configure his CAD software. With this finished, I verified that user0 could access his network drives, and that his files had indeed been restored from our tape back up system. I had the user0 change his local passwords, and changed his network passwords on the appropriate systems to prevent any possible use of a compromised password from his system.

With user0's system restored, I asked him to keep an eye out for any new attempts on his system. User0 has agreed to inform our department of any new attacks. This time, we lost very little data. The only loss we suffered were a few locally stored files that should have been stored to our network drive as is standard policy.

7. Follow Up and Lessons Learned

- **Follow Up**

With our lack of a true incident handling team at the time of this incident, a follow up meeting was not performed. Had we been able to field this team, we would have used this meeting to establish that all suggested changes to policy were made, and all patches and upgrades were performed sooner. The follow up report would also have been filed so that we could give a comprehensive description of what happened and what steps we took to correct this problem to prevent any reoccurrences.

- **Lessons Learned**

  This was the first true incident that has occurred at our organization that was recognized as an incident. Others may have occurred, but were not realized at the time. The belief before this incident was that our firewall was all the external security we needed. We now know that this attitude isn't sufficient in today's complex environments, and steps are being taken to shore up the existing security and add new components as they are evaluated and needed. The following list shows the changes that were deemed immediately necessary after our incident:

  - Ultimately better procedures and policies need to be put in place. Several of these were modified after the event.
  - System logs are kept for longer periods of time, and backed up when disk space becomes an issue, thus allowing investigation of events that happened past the time threshold being maintained.
  - Better training for all people involved in incidents is a must. This has prompted my personal attendance of the SANS training seminars during the past year. We plan to have more people receive appropriate training once the responsibilities are ironed out, and budgets will allow.

8. For at least one operating system involved in the incident, show the process used to assess and contain, including screen shots and operating system commands. In this section you should describe your jump kit, and all the tools that you used.

The compromised system was a NT 4.0 workstation running service pack 5. The owner had local administrator rights, but no administrator privileges on the NT domain. At the time of this incident, we did not have procedures in place to accommodate the collection of notes, and their importance in reference to an investigation was not understood. Without note taking, no screen shots were collected. We did not use the system that had been compromised, but took a clean pc set up with the same software as the compromised system and evaluated the effects of the malicious program on it.

A test network was setup with the test machine attached, and a pc running netmon to observe and capture any suspicious traffic. Netmon is a standard program included with MS SMS 2.0 and its client pieces. By using a client installation, the tool was available, and network traffic could then be monitored.

A copy of the malicious program was executed on the test system, and changes to the system were noted. At the time we performed this test, we used the system's own search utility to find all files that were modified during the test execution of the program. Today, I would have used sysdiff binary from a cd-rom on the system and checked for changes that were made by the malicious program.

If the compromised system had served a more administrative role, and was not used as a simple workstation, then more dramatic steps would have been required.

As stated at the beginning of this report, no jump bag existed at the time of this incident. In fact until I had taken this course, there was no knowledge of an incident handling team, or the steps suggested to prepare, assess, contain, or generally handle any similar problems.

9. For at least one operating system involved in the incident describe in detail the process used to back up the system. This should include descriptions of the hardware, commands, and any problems that you ran into.

In our organization, the written computer use policy states that all personal data can be stored on local machines, but any pertinent data related to business is to be stored on network drives that are regularly backed up. The victim in this case had successfully followed procedure and only lost one file that he had not pushed to the network before he executed the malicious program. With nothing remaining on the system, the decision was made to reformat the system from the ground up. Our procedure for backing up data is to keep important files on our network drives. On a nightly basis, a scheduled backup of the network drives takes place. This is maintained by a backup server, and kept on a tape library with redundant connections, drives, and power supplies for high availability. Since no compromised files were identified, no new backups were deemed necessary.

With what I have learned during this course, a binary back up should have been performed once the compromised system was identified. We now use Symantec's ghost product to create and restore disk images needed for all system rebuilds. This product allows us to create binary backups. Once a binary copy had been created, the original disk should be stored in a Ziploc bag with an index card stating what was in the bag, and signed off on by the head incident handler.

10. Describe in detail the chain of custody procedures used, any affirmations, and a listing of all evidence.

With no incident handling procedures in place, the correct steps were not followed. In an established organization, a chain of custody is needed to ensure the validity of evidence. Backups, copies of notes, and other evidence need to be signed off on and witnessed at critical points in the investigation.

References:

Computer Security Incident Handling Step by Step, A Survival Guide for Computer Security Incident Handling, Stephen Northcutt.

SANS Incident Handling Step-by-Step and Computer Crime Investigation, Eric Cole, Book 4.1, Track 4, Incident Handling and Hacker Exploits.

Last Updated: July 22nd, 2017

Upcoming SANS Penetration Testing

Security Awareness Summit & Training 2017	Nashville, TN	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
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 Hyderabad 2017	Hyderabad, India	Aug 07, 2017 - Aug 12, 2017	Live Event
Mentor Session - SEC542	Des Moines, IA	Aug 14, 2017 - Sep 13, 2017	Mentor
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC560: Network Penetration Testing and Ethical Hacking	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Memphis SEC504	Memphis, TN	Aug 21, 2017 - Aug 26, 2017	Community SANS
Mentor Session AW - SEC504	Milwaukee, WI	Aug 23, 2017 - Sep 29, 2017	Mentor
Mentor Session AW - SEC504	New York, NY	Aug 24, 2017 - Sep 08, 2017	Mentor
Mentor Session - SEC504	Denver, CO	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits and Incident Handling	SEC504 - 201709,	Sep 05, 2017 - Oct 12, 2017	vLive
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, Ireland	Sep 11, 2017 - Sep 16, 2017	Live Event
Mentor AW - SEC504	Santa Clara, CA	Sep 11, 2017 - Sep 22, 2017	Mentor
Community SANS Columbia SEC560	Columbia, MD	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Toronto SEC542	Toronto, ON	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC560	Dallas, TX	Sep 13, 2017 - Nov 15, 2017	Mentor
Community SANS Madrid SEC560 (in Spanish)	Madrid, Spain	Sep 18, 2017 - Sep 23, 2017	Community SANS
Mentor Session - SEC504	Arlington, VA	Sep 20, 2017 - Nov 01, 2017	Mentor
Mentor Session - SEC560	Manchester, NH	Sep 21, 2017 - Nov 02, 2017	Mentor
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event