Global Information Assurance Certification Paper

GIAC Advanced Incident Handling and Hacker Exploits

GCIH Practical Assignment

Version 1.5c

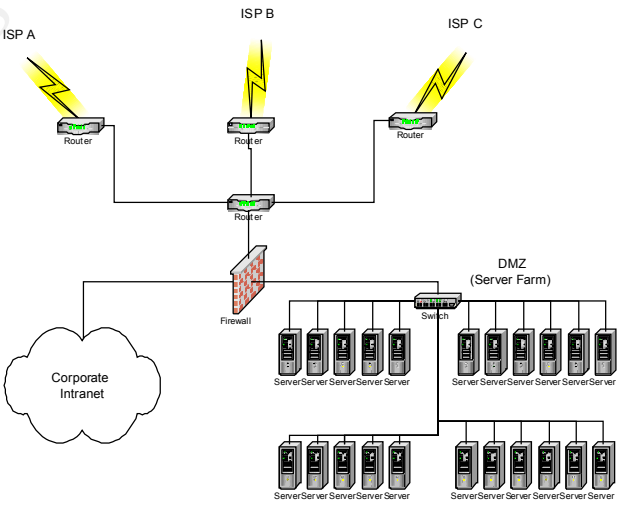
Illustration of Web Site Defacement Incident

Written by Jeff Cummings
Attended: Baltimore SANS 2001
Date Submitted: January 16, 2005

On May 8, 2001 a company's website was hacked. The incident proved to be a blessing in disguise to a company unprepared. The company's web site was compromised and it's web page replaced with a vulgar message. Although the website was not a revenue generating site, it was a direct interface to customers for information exchange. Viewed after the alteration, it would have proven to be very offensive to the company's customers. Luckily, the web defacement was identified before anyone outside the company had an opportunity to view the page. That was the good news; the bad news is the company was not prepared to fully react to the intrusion. The company did not have an incident response plan in effect to guide the recovery process. Although the plan was not in place, the servers involved were returned to service with little effect on the company's business. As a result of the incident, tasking, funding, and a high priority for an incident response plan was issued from the company's upper management. This paper will discuss the incident, the recovery, and the preparation for future attacks.

The first evidence of the attack was discovered by one of the business group members who maintain the site. She had logged on the site at about 09:00 am to gather some information and found the site had been hacked and displayed a vulgar reference to the U.S. Government. The group member immediately contacted her superior and the group leader. They verified the defacement and called the Corporate Information Systems (CIS) staff to report the incident at 09:30 am. The three team members then scanned the server for files changed since the last know correct configuration. They drafted a list of the files that had changed to help determine scope of the incident. The CIS staff member arrived and disconnected the affected server from the network at 09:45 to eliminate any further viewing of the site. The CIS staff immediately began the incident response procedure. The only problem was there was no defined, documented incident response procedure, so they did their best.

The CIS team set up a "war room" to facilitate the investigation. It was an empty cubicle in the server room, but served the purpose. The location had limited access and enough area to facilitate a team operation. A network diagram was printed and hung on the wall to allow the investigation team to understand the path taken by the hacker to get to the server. That diagram is show below. Conveniently, the server room and most of the people required to work the incident were all in the same location.



The listing of the files affected, as determined by the business group's initial assessment, was also listed on the wall for the team. That list is shown below. All 8 files had been altered on May 8, 2001 at approximately 10:29 pm. That meant the page was altered and online for 11 hours and 15 minutes before discovery.

c:\index.htm
c:\default.htm
c:\Inetpub\index.htm
c:\Inetpub\default.htm
c:\Inetpub\ftproot\index.htm
c:\Inetpub\ftproot\default.htm
c:\Inetpub\iissamples\index.htm
c:\Inetpub\iissamples\default.htm

While the war room was being assembled, the team was being called. It was now about 10:15 am. Although there was no formal list of personnel to call, a team was assembled. The initial local team consisted of the web page designer, the local CIS operations manager, a member of the business group, and an Information Security Engineer from the Information Assurance (IA) Group. I was the Information Security Engineer chosen to work the problem. Typically, our IA group is involved in assessing security solutions for customers. Incident response has not been our charter, but we are aware of the basic procedures to follow and have extensive experience with network intrusions.

After asking several questions on the phone, I assembled my bag of tricks to include my laptop computer with CDRW drive, a box of blank disks (both floppy and CD), a hub, several ethernet cables, and a notebook. The software at my disposal was primarily for vulnerability assessments and penetration analysis, but I did have Ghost enterprise on my hard drive for just such an occasion. I also had AGNetTools and Sam Spade, both collections of utilities for tasks such as whois, name and DNS lookups, ping and ping scans, etc. PGP was installed on my machine to encrypt the data as it was recorded. PKZip is another tool that is standard to the load of my machine; it has come in handy more than once. My last tool of mention was my browser. A web browser is invaluable as a research tool when searching for information on specific exploits and defaced web sites. When I had gathered my equipment, I informed my manager of the situation and left for the war room.

When I arrived at the makeshift war room at 10:30, my first goal was to determine the scope of the incident and the approach to handle the incident. Were any other servers hacked? What was running on the servers? How critical are the affected servers? Is the goal to contain, clean, and deny access or to monitor and gather information? My secondary goal was to document the effort properly. All the members were provided a notebook with which to document their actions. The team was instructed to document everything they did or observed. These notebooks would later be collected for evidence.

When I asked if any other servers had been modified, I was a little shocked to hear that no one had checked the other servers. There are more than 20 web servers in the area, yet only one had been checked. I surveyed the room and made a list of all the servers' web addresses. I plugged in my computer to the network and began to browse to all of the servers. I found three

additional servers that had the same vulgar message displayed. I noted all the servers affected and reported my findings to the team. The owners of the servers were contacted and informed that their servers would be taken offline immediately. They all concurred and sent a representative down to support the team. All the affected servers were disconnected from the network. When the representatives arrived they were asked what was running on their server and how critical the servers being online was to the company. All of the servers were deemed non-critical, but significant. The loss of the servers would not deny revenue, but could affect the customer's impression of the company's capability to host a web server. The CIS staff had already determined the goal was to contain, clean, and deny access. The servers would be not monitored for further access.

At this time, about 10:45, all the servers affected had been taken offline. It was time to make a backup of the servers for further investigation. I asked the CIS rep to log on to one of the servers to ensure a clean shutdown, but found that he had no access to the server. This was a disturbing revelation; CIS staff did not have direct access to the servers. I asked the web developer to log on to the original hacked server and shut down the server. I began to make an image of each of the servers to my local disk on my laptop. The servers were rebooted, and the disk imaging was initiated via a DOS based boot disk to preclude any modification of the existing evidence on the hacked machine. The process used for the making the backups is described in Appendix A. My drive had about 15 GB of free space and a PGPDisk of 10 GB. The image files could be gigabytes in size, but the space available should accommodate the image files produced. The original image files for the first server, with no compression, were a total of 3.16 GB in size, much too large to fit on a CD. Once the image file was completed, I marked it "read only" and zipped the data into a file of only 334 MB. The resulting zipped file was marked "read only" and copied to a CDR for archival. This would provide a permanent, non-editable, copy of the data. The disk was labeled, with a permanent marker, with the time, date, server name, my name, and "Compromised Server".

A small problem occurred when the first backup as initiated. When using the Symantec Ghost software in the Multicast mode, an incorrect choice was made when building the client boot disk. Two options for the specific NIC used, were presented: 3COM 3C90X NDIS and 3COM 3C90X Packet. My first choice of the Packet version failed. Another network boot disk was made with the NDIS version of the NIC drivers and it worked flawlessly. The resulting backup images could then be viewed with the Ghost Explorer program. The program allows full browsing of the file system as well as the option to open and read the files. While the backup of the server continued, the team assessed other areas of concern.

The CIS person contacted his staff to determine if there were any indicators of the attack in the firewall or router logs. The firewall logs did not indicate any odd behavior, and the router logs were non-existent. The log server for the routers had been taken offline for maintenance just days before and all of the routers had not been reconfigured to point to the temporary log server. The evidence of this attack would not include the router logs. The firewall ruleset allowed only HTTP and HTTPS traffic on port 80 and 443 to enter the DMZ through the firewall. Evidently, the attack had not been an elaborate attempt, but rather a random attempt with a specific exploit. The firewall logs were also reviewed and did not indicate an attempted

port scan or other suspicious activity at the time of the incident. The attack must have come in via http, a protocol that could not be blocked if web traffic was to continue.

The next step was to verify the path taken from the attacker to the web servers. The local CIS representative made the appropriate calls to his staff and determined that the attack had passed through one of the company's 3 Internet Service Providers (ISP). The only path to the servers was through a border router, a local router, and a firewall to finally arrive in the company network's Demilitarized Zone (DMZ). Unfortunately, since the router log server was down during the incident, no data was available to identify which ISP the attack came through. This was disturbing news as well; there were no records of access to the entire site for the last several days.

The backups had not completed, so I started researching the hack on the net. I searched for information on the attack on the www.cert.org website. I found the exact message that had been placed on the hacked servers listed on the following URL: *http://www.cert.org/advisories/CA-2001-11.html*. At this point, the attack appears to be the result of a self-propagating malicious code worm referred to as sadmind/IIS Worm. The site listed impacts and solutions to the problem. The worm targets machines running Windows NT and serving the web content via Microsoft Internet Information Service (IIS) version 4.0. Our servers were also running that configuration. The advisory indicated the solution to the Windows NT/ISS portion of the exploit was to install the following patch from Microsoft described at the following site: http://www.microsoft.com/technet/security/bulletin/MS00-078.asp.

The advisory from the CERT listed a sample log file from an attacked IIS server. To verify our server had the same entries, I opened the Ghost Explorer application and reviewed the log file (c:\winnt\system32\logfiles\W3svc1\ex010508.log) on the **image** of the compromised server. The file is listed below (note that the IP address has been changed to protect the guilty).

```
#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 2001-05-08 22:27:09
#Fields: time c-ip cs-method cs-uri-stem sc-status
22:27:09 1.2.3.4 GET /scripts/../../winnt/system32/cmd.exe 200
22:27:09 1.2.3.4 GET /scripts/../../winnt/system32/cmd.exe 200
22:27:09 1.2.3.4 GET /scripts/../../winnt/system32/cmd.exe 502
22:27:11 1.2.3.4 GET /scripts/root.exe 502
22:27:11 1.2.3.4 GET /scripts/root.exe 502
22:27:11 1.2.3.4 GET /scripts/root.exe 502
22:27:14 1.2.3.4 GET /scripts/root.exe 502
22:27:14 1.2.3.4 GET /scripts/../../winnt/system32/cmd.exe 502
22:27:14 1.2.3.4 GET /scripts/root.exe 502
22:27:16 1.2.3.4 GET /scripts/root.exe 502
22:27:16 1.2.3.4 GET /scripts/root.exe 502
22:27:16 1.2.3.4 GET /scripts/root.exe 502
22:27:19 1.2.3.4 GET /scripts/../../winnt/system32/cmd.exe 502
22:27:19 1.2.3.4 GET /scripts/root.exe 502
22:27:19 1.2.3.4 GET /scripts/root.exe 502
22:27:22 1.2.3.4 GET /scripts/root.exe 502
22:27:22 1.2.3.4 GET /scripts/root.exe 502
```

```
22:27:22 1.2.3.4 GET /scripts/../../winnt/system32/cmd.exe 502
22:27:24 1.2.3.4 GET /scripts/root.exe 502
22:27:24 1.2.3.4 GET /scripts/root.exe 502
22:27:24 1.2.3.4 GET /scripts/root.exe 502
22:27:27 1.2.3.4 GET /scripts/root.exe 502
22:27:27 1.2.3.4 GET /scripts/../../winnt/system32/cmd.exe 502
22:27:27 1.2.3.4 GET /scripts/root.exe 502
22:27:29 1.2.3.4 GET /scripts/root.exe 502
22:27:29 1.2.3.4 GET /scripts/root.exe 502
22:27:29 1.2.3.4 GET /scripts/root.exe 502
22:27:32 1.2.3.4 GET /scripts/../../winnt/system32/cmd.exe 200
22:27:32 1.2.3.4 GET /scripts/../../winnt/system32/cmd.exe 502
22:27:32 1.2.3.4 GET /scripts/root.exe 502
22:27:35 1.2.3.4 GET /scripts/root.exe 502
22:27:35 1.2.3.4 GET /scripts/root.exe 502
22:27:35 1.2.3.4 GET /scripts/root.exe 502
22:27:37 1.2.3.4 GET /scripts/../../winnt/system32/cmd.exe 502
22:27:37 1.2.3.4 GET /scripts/root.exe 502
22:27:37 1.2.3.4 GET /scripts/root.exe 502
22:27:40 1.2.3.4 GET /scripts/root.exe 502
22:27:40 1.2.3.4 GET /scripts/root.exe 502
22:27:40 1.2.3.4 GET /scripts/../../winnt/system32/cmd.exe 502
22:27:42 1.2.3.4 GET /scripts/root.exe 502
22:27:42 1.2.3.4 GET /scripts/root.exe 502
22:27:42 1.2.3.4 GET /scripts/root.exe 502
22:27:45 1.2.3.4 GET /scripts/root.exe 502
22:27:45 1.2.3.4 GET /Default.htm 200
```

The items listed in the logs match the description in the advisory, a good indicator that we are on the right track. The system logs on the machines were reviewed as well. They did not supply any information to indicate further external exploitation. This was partly due to the fact that the auditing on the server had not been set up to audit anything more that logins. Finally, I verified that the latest patch on the operating system was service pack 4 and ISS was straight out of the box. No updates had been made. This confirmed that the operating system service pack was not up to date, and the IIS install had not been patched.

While I had the image opened, I looked further to verify the data. I looked for each of the files listed by the business group as being changed. I found the each of them set off my virus detection software. The Backdoor.Sadmind.Dr virus was listed as the offending virus. This further verified that the attack was the sadmind/ISS worm. Furthermore, I found more copies of the infected files. There were four files affected: default.asp, default.htm, index.asp, and index.htm. These four files were found in each of the following folders and had all were edited at the time of the incident (10:29-10:30).

```
c:\
c:\Inetpub\
c:\Inetpub\ftproot\
c:\Inetpub\iissamples\
c:\Inetpub\mail\
c:\Inetpub\mailroot\
c:\Inetpub\scripts\
```

c:\Inetpub\wwwroot\
c:\Inetpub\wwwroot\images
c:\Inetpub\wwwroot\cgi-bin
c:\Inetpub\wwwroot_private

The original list of modified files had now been verified and several files added to the list. Another issue was brought to the forefront with this discovery. There was no virus protection software running on the server. This is a major issue for an online asset. This would be presented again in the final report.

The next step was to determine the originator of the attack. I used the whois command within the Sam Spade program to determine the address (found in the ISS logs, 1.2.3.4 in this example) was registered to a site in Brazil. An example of the results can be found in appendix B. I have used the SANS site as an example to further protect the guilty parties. I then initiated a telnet sessions through a series of secured servers to the offending site. The multiple sessions were an attempt to protect my identity. The prompt returned indicated a host at the target address was a Unix server running Solaris System V Release 4.0. The resulting prompt (modified to protect the guilty) is shown below.

Trying 1.2.3.4...
Connected to hacked.brazil.com (1.2.3.4).
UNIX(r) System V Release 4.0 (Name of Server)
login:

This tracks with the CERT's advisory, which indicated the attack is launched from a compromised Solaris host. Using a tool called Visual Route, I made a final verification. I used the trial version found at http://www.visualware.com/visualroute/livedemo.html to further protect my identity. The product both visually and textually displays every hop taken to get to an IP address. It provides the IP address and geographical location of every hop taken to the target host. The trace is launched from the Visualware site and therefore does not contain any IP information from our company. The result of the program confirmed a path to Brazil. This server may be the point of origin, or just another victim of the attack. A greater effort would be required to determine the status of the site, for now we will just note the data in our notebook. At this point, I felt there was sufficient evidence that the compromise was the result of the sadmind/IIS Worm exploit.

I returned to the team and presented my preliminary results at about 11:30. The team agreed that the websites had apparently fallen prey to the sadmind/IIS worm. The CERT advisory states "The sadmind/IIS worm exploits a vulnerability in Solaris systems and subsequently installs software to attack Microsoft IIS web servers. In addition, it includes a component to propagate itself automatically to other vulnerable Solaris systems." [1] This fact led us to a scan of the company's Solaris servers in search of a compromised machine. The CIS representative tasked his staff to access the Solaris servers on the network for signs of

[1] Carnegie Mellon Software Engineering Institute, CERT Coordination Center. (2001). CERT Advisory CA-2001-11 sadmind/IIS Worm. Retrieved May 9, 2001 from the World Wide Web: *http://www.cert.org/advisories/CA-2001-11.html*

compromise. About 45 minutes later, it was confirmed that none of the Solaris systems had been modified.

As the backups continued, the next task of the team was to assess the damage, and determine any steps to be taken. At this point two of the four servers had been confirmed to have the same indicators of the attack. The web page defaced, the same files changed, and the same attacker listed in the IIS logs. The original web pages had been overwritten and must be restored. A query of the business groups indicated that no reports from users had been received at this point, so we assumed our company's image was still intact.

The offending IP address of the Solaris machine was then restricted at each of the border routers at 11:45. If the address attempted another attack, the offender would be blocked and a notice e-mailed to all of the team members.

Just before noon, a conference call was made with the incident team, the head of CIS, and the company's vice president. All parties were brought up to speed with the current state of the investigation. The vice president was very concerned that the company's image and directed the team to consider the findings to be company proprietary and not to release anything outside the response team. Further, he instructed us to do nothing that may associate the company's name with being hacked. His direction was to preserver the evidence, get the servers back online immediately, and keep him informed. The team must now review the next step to take in the investigation. A common step when discovering a compromised machine is to report it to the Computer Emergency Response Center (CERT) and possibly the ISP from which the hack traversed and/or originated. The vice president negated both these actions. He did not want a story in the paper about our servers being hacked. Our attention must now be placed on restoring the servers and returning the websites to operational status. That is where the day took a turn for the worse.

By 13:00, images of all four hacked servers had been backed up and stored offline. I accessed each of the recent backups to verify they were all readable. I then quickly scanned the remaining two server images to verify the same evidence existed. Each of the servers had the same files modified at approximately the same time. I checked the NT log files and found no evidence of auditing. The date on the files was over a year old. When I was convinced I had good backups, I informed the team that we could continue with the restorations phase. We could now proceed with the reconstruction of the machines. The request was made to the team to provide the backups. Two of the four representatives responded with "What backups? CIS does the backups." CIS indicated they could not run backups on machines not under their control. Bottom line, no recent backups existed. They would have to re-create those two servers from scratch. The other two groups had backups of their data and immediately began reformatting their machines and building a clean installation.

The owners of the two servers without backups returned to their group to determine how to rebuild their servers. The two groups with backups would restore their web server data on a clean install of the operating system and IIS web server program. When the backups were restored, I quickly verified that the server did not contain the modified web page documents. Both machines received the latest service pack from Microsoft (currently version 6a), and all

recommended patches for ISS as recommended by the vendor at the following location: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/iischk.asp.

Before any machines could be placed back into service, the CIS staff would perform a standard security configuration checklist on the server. This would ensure that the server was properly patched and configured for secure operation in the company's DMZ.

The CIS group has been fighting a long running battle over the control of corporate assets. Many of the business groups have web server that are managed by members of their own team. The problem is that they are not all aware of standard security and disaster recovery practices. The CIS group is very concerned about unsecured servers being placed into operation on their network without being secured. Maintenance and backup of the servers should be performed by the CIS group who control the area and are working right by the servers. Finally, the CIS staff should have access to all machines placed in the DMZ. If CIS had been given access to the servers, an emergency such as this could have been minimized. It turns out that there is a company policy in place to provide web server support and requirements for corporate assets added to the network. All the systems currently online had not been reviewed at the time of the incident.

The CIS team reviewed the configuration of the two machines, made several configuration changes and placed them both back into service. By 16:30, the first two servers had been restored on online again. The other servers took several more days to totally rebuild. They were patched, secured, and configured by the CIS staff before finally going back online.

The team assembled at the end of the day to close out the incident and review the day. Copies were made of all the logs, floppies, and CDs. The originals were placed in a sealed package, labeled, and placed into a safe just in case further action were required. That concluded the pleasant part of the review. Now it was time to reflect on our lack of an incident handling plan. Having no formal plan was an obvious detriment to the handling of this incident. A meeting was planned later that week to discuss the incident and how we could respond better.

Finally, another conference call was made with the incident team, the head of CIS, and the company's vice president. The day's actions were briefed and the current status presented. Simply put, we were very luck this time. Four servers were exploited and their websites hacked. The attack was appeared to be a scripted exploit with a specific target of IIS servers. The attacker used only one exploit. No effort was made to hide the tracks of the aggressor. Minimal damage was incurred by the company, since the sites were not revenue producing or heavily used by the customers. An effort to further track the perpetrator was negated by the management at this point. There was just not enough loss to justify the pursuance of the investigation. The company cut it's losses and moved on with the business. There was no evidence that any customers viewed the modified web content. Another small blessing. The recovery of the servers was now 50% complete with two servers back on line. The remaining two servers are expected to be online soon. The lack of an incident plan was discussed and direction was provided to the members of the team that an incident response policy, plan, and review process must be drafted, approved, and placed into affect.

The incident handling plan was not only poor. It was not-existent. Although I was scheduled to attend the SANS course on incident handling in several weeks, that provided little help to me during the meeting. For the sake of this paper, I will break down our shortcoming into the six-phase process recommended by SANS.

The first phase, ***preparation***, was obviously poorly performed. The policy was not in place at the time of the incident. Although the company's CIS team had made great strides and had many improvements, to include intrusion detection, on their recommendation list, they had not been implemented when they were needed. The machines exploited were not secured nor kept up to date with updates and patches. No formal approach or team had been devised or approved. When the attack occurred, there were no formal guidelines for the team to assemble, who to inform, or what actions to take or not take. The disaster recovery plan was obviously lacking since half of the machines did not even have a backup or a procedure to make one. Although there were no formal alliances between the business groups, the CIS group, and the Information Assurance group, the team came together and worked very well together to recover from the incident. This may not be the norm in many companies. Finally, a training effort should have been implemented to educate both the investigation team, the CIS staff, and the users on the network. This education would include safe practices for operating networked devices and what to do if you think an intrusion has occurred.

Several key sources of information were not available to evaluate the incident that should have been online and operational when the event occurred. The primary problem was the lack of logs. There were no logs available for the routers or the web servers. The routers had been configured to collect audit information. In fact the standard operating procedure was to log all the router logs to a central server for ease of auditing. The problem during this incident was that the log server had been taken offline for maintenance and all the routers had not been rerouted to the new server. This negated a critical data point in the investigation.

The auditing of the NT based web servers had also failed to be configured. The only logging on the web servers was the ISS auditing within the application. Although these ISS logs provided critical information in the investigation, more data would have led to a more complete evaluation of he incident. As a result the audit logs on the systems were blank. No useful information could be acquired from the logs. Another key source of information was not available for this investigation.

The backup procedures for the servers were not in force at the time of the incident. This is just not acceptable for a public online data source. Two of the four servers compromised had a backup of the data, and the two did not. Of the two with the backups, each used a different product. Both of the selected products differed from the company standard of Veritas Backup Exec. Since each of the servers was supported by a different group, the backups were also managed, or not, by the individual groups. The current implementation is a disaster waiting to happen.

Lastly, none of the servers was running any type of virus software. If there had been an application scanning for malicious code, a warning may have alerted someone to take action

sooner. This was not the case. We would recommend the addition of antivirus software on each of the servers to the management.

The second phase, ***identification***, was much better performed by the company's recently assembled incident response team. The team was immediately formed after the first indication of an incident. A single person, myself, was the one looked to for guidance during the incident. I did not have authority to proceed without other approval, but there was only one person guiding the effort. The first thing we did as a team was verify that it was indeed an incident and begin protecting the chain of custody of the evidence. Although we did not track down the perpetrator, the evidence is still available for further investigation if necessary. Access to that evidence was limited to members of the team and all documents and disks were immediately placed in a safe upon conclusion of the investigation. The network staff was directly involved in the effort from the first call from the person who discovered the incident. Most important in this incident was the communication between company officials. Communication was initiated immediately and continued throughout the effort.

The third phase, ***containment***, was the best performed of the phases. An onsite team was on the scene within 30 minutes of the initial report. Access to the affected machines was immediately denied by disconnecting the servers from the network until a backup was completed. The first access to the machine was to shut down the machine after they had been fully backed up. The backup process was well defined and started immediately. Extreme care was taken to not directly contact the attacking IP address to prevent any further actions by the perpetrator. After information was gathered, a team decision was made to not continue the forensics or any public or legal actions. This consensus was made with the team, the system owners, and the vice president of the company.

The fourth phase, ***eradication***, was only partially successful. The cause of the incident was determined quite quickly and the defenses heightened. The access lists on the border routers were altered to deny access to the attacking IP address. An abbreviated vulnerability analysis was performed on the machine that immediately indicated the cause of the exploitation. After the cause was found, the team analyzed other potential servers that may have been affected by the worm. We found 3 additional targets of the worm during the process. That portion of the effort was successful, unlike the task of finding the system backups. All the machines were rebuild, patched, secured, and tested before returning to the network. This step, specifically adding the patch to the IIS program, eradicated the vulnerability that allows the exploit to be successful.

The fifth phase, ***recovery***, was performed quite well by the business groups and the CIS team. Once the backups issues noted above were overcome, the team prepared the servers based on the company standards. The servers affected had net been previously made compliant. All the machines were restored and a clean backup made by the CIS team using Veritas Backup Exec before they were put back online. This would now be a standard procedure to be performed by the CIS team for ALL servers in the DMZ. Prior to the backups, the systems passed a rigorous checklist to ensure that the machine was properly configured and secured. This checklist included auditing, permissions, and access controls for both the OS and the ISS application. Antivirus software was also added to each of the servers. The software was

configured to send an alert to the CIS staff if any activity occurred. Additionally, the software was configured to update itself daily from a local server.

The failed router logging issue was also resolved and a more robust logging solution was placed into operation just days after the incident. Now all logs are directed to a central server for storage and auditing. In the future, much more data will be available if another incident should occur.

The sixth and final phase, ***follow-up***, is ongoing. An executive summary was written and shared with appropriate employees in the company. More importantly, the lack of a plan was brought to the attention of the top level management as well as the potential for greater damage in the future if a plan is not developed. The top management recognized the importance of the plan and has provided funding and manpower to resolve this shortfall. The task of establishing a complete incident handling plan was given to the Information Assurance group within the company. The plan to be created will include policy, process, education, software, and hardware, all in a published document that will be available to all appropriate staff. Furthermore, the chosen staff will all be required to attend intensive training on the plan and its implementation.

The CIS staff had been researching a solution for intrusion detection and enterprise monitoring for the network prior to this incident. As a result of the recent events, the priority of these efforts was raised to critical and approval to procure the products was authorized. Within a month, the company should have both capabilities online and functioning.

A potential nightmare was overcome and a great deal of good has come from this particular incident. Although many mistakes were made and shortfalls noted, the resolve of the incident will lead the company to a more highly protected infrastructure. The positive attitude and professional response kept throughout the effort led to the direct tasking for a formal fully funded incident handling process.

Appendix A

Symantec Ghost Multicast Server Instructions

The following procedures detail the process to remotely backup a remote disk or partition to a central server. The procedures are written assuming a complete install of Symantec's Ghost Enterprise Edition has been installed on the computer used as the Multicast server. The process has three major steps:

1. Create a Ghost Boot Disk
2. Configure the Multicast Server to receive a backup image
3. Initiate an image copy from the remote computer

The process must be performed in the correct order or failures will occur.

STEP 1:

The first step is to prepare a boot disk for the target computer that will be backed up. This disk will be used to boot the computer, load the network drivers, and run the software. This provides a method of backup that is non-intrusive to the current operating system loaded on the machine. The only downfall of this process is a reboot is required. The process requires knowledge of the network interface card (NIC) used in the target. Follow the following steps to create the Ghost Network Boot Disk.

1. Start the Ghost Boot Wizard (Start\Programs\Symantec Ghost\Ghost Boot Wizard)
2. Choose the Network Boot Disk option
3. Choose the appropriate NIC driver to install
4. Choose the Symantec Ghost option
5. Choose the appropriate option to acquire an IP address
    a. DHCP will assign the IP address
    b. The IP settings will be statically defined
6. Select the appropriate floppy drive label (A:)
7. Select the number of copies
8. Select Quick format
9. When format is complete the software will load onto the disk.

The Ghost Network Boot disk is now ready to take to the target machine.

STEP 2:

The second step prepares the multicast server to receive the request for an image to be stored on the server. The server must be located on the same network segment as the client. This is one of the reasons a hub and a set of cables come in very handy on an incident response. Connect the server to the network segment and establish connectivity. When connectivity has been achieved, follow the following steps to prepare the multicast server for operation:

1. Start the multicast session (Start\Programs\Symantec Ghost\Multicast Server)
2. Type a session name (This name must be entered into the client portion in step 3)
3. Choose "Dump from Client" to receive a file from a client
4. Choose a filename for the session to be backed up. This should be descriptive and related to the machine you are backing up. I chose to place the files on a PGP encrypted disk on my local computer. Note: the encrypted disk must be mounted before the process begins or failure will occur.
5. Choose the "Disk" option to copy the entire disk
6. Configure the Logging options
    a. Choose "File\Options
    b. Choose Log Level = All (to fully document the imaging of the disk. This will take up some disk space, but will provide details for further analysis.
    c. Choose Log File to be some descriptive name, and place it in the same directory as the image files.
7. Click the "Accept Clients"

The server is now ready for the image to be transmitted)

STEP 3

This step is performed on the machine from which the image will be originated.

1. Insert Ghost Network Boot disk into target machine and reboot
2. System boots, acquires an IP address, and loads Ghost software
3. Choose the Multicasting option
4. Insert the session name entered in Step 2
5. Choose the drive to image from the listing
6. Choose the "High" compression option for the image
7. Choose "Yes" to continue with the image creation
8. The image will be compressed and backed up to the multicast server
9. When process has completed, exit the program
10. Remove the floppy from the drive
11. Reboot if appropriate.

An image of the entire disk is located on the multicast server. The resulting image file may be quite large, but will compress dramatically with an application such as PKZip. The resulting zipped file can then be copied to a CDR media for storage.

Appendix B

Sample output from Sam Spade software:

whois -h whois.networksolutions.com sans.org ...

Registrant:
The SANS Institute (SANS-DOM)
15235 Roller Coaster Rd.
Colorado Springs, CO 80921
US

Domain Name: SANS.ORG

Administrative Contact:
Paller, Alan (AP160) alanpaller@AOL.COM
Escal
4610 Tournay Road
Bethesda, MD 20816
301-229-1062
Technical Contact:
Polk, Jeff (JP232) polk@DELOS.COM
Delos Enterprises
15235 Roller Coaster Rd.
Colorado Springs, CO 80921
US
719-481-6541 719-481-6551
Billing Contact:
Paller, Marsha (MP1458) mmpaller@AOL.COM
The SANS Institute
4610 Tournay Road
Bethesda, MD 20816
301-951-0102

Record last updated on 19-Jul-2000.
Record expires on 05-Aug-2009.
Record created on 04-Aug-1995.
Database last updated on 16-Jul-2001 21:03:00 EDT.

Domain servers in listed order:

SERVER1.SANS.ORG 167.216.133.33
NS.BSDI.COM 206.196.44.241
DELOS.COM 192.65.171.1

List of References

Carnegie Mellon Software Engineering Institute, CERT Coordination Center. (2001). CERT Advisory CA-2001-11 sadmind/IIS Worm. Retrieved May 9, 2001 from the World Wide Web: ***http://www.cert.org/advisories/CA-2001-11.html***

Microsoft Corporation. (2000). Microsoft Internet Information Server 4.0 Security Checklist. Retrieved 9 May, 2001 from the World Wide Web: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/iischk.asp

Microsoft Corporation. (2001). Microsoft Security Bulletin (MS00-078), Patch Available for "Web Server Folder Traversal" Vulnerability. Retrieved May 9, 2001 from the World Wide Web: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms00-078.asp

Northcutt, Stephen. Computer Security Incident Handling Step by Step, A Survival Guide for Computer Incident Handling. The SANS Institute, 1998.

Visualware, Inc. (2001). VisualRoute Server – Live Demo. Accessed May 9, 2001 from the World Wide Web: http://www.visualware.com/visualroute/livedemo.html