Global Information Assurance Certification Paper

IIS Unicode Exploit Illustration

I. Introduction

In today's fast moving, "gotta have it now" world, where would we be without the internet, or more specifically the web? So much of our daily lives at home, work and school have become ever more dependent on the web and all it has to offer including things like email, streaming video, streaming audio, Napster, newsgroups, on line shopping, etc. Most, if not all of these applications are served up from a web server that could be hosted from just about anywhere in the world. As a whole we have become accustomed to delays in loading or downloading from certain web sited depending on the time of the day or just say, "I'll go back later when the other half of the world goes home". For the most part we wouldn't think twice, but what if you went to a web site with the intent of conducting business and instead of getting a welcome screen with all the things you intended to buy, you got a dark and sinister web page spewing antigovernment or racial slurs accompanied with some blatantly offensive adjectives? Well, I don't know about you, but I would question the security of any personal information may have already given them not to mention any information transmitted to them via their web site and would probably do business elsewhere.

One of the most popular web server products in use today is Microsoft's IIS (Internet Information Server). IIS 4 is available for the Windows NT 4 platform in the form of Option Pack 4 while IIS 5 is integrated into Windows 2000 and fully enabled using a default installation. Because of its dominant presence in the world of HTTP, it is routinely target for any vulnerability. The most prevalent exploit being used today is known as the IIS Unicode Exploit. Although this vulnerability is easily fixed, many system administrators simply don't take the time to routinely apply patches to their systems. This exploit allows an attacker to run programs on the web server to replace default homepages with that of their own, or potentially take a wide range of destructive actions against it.

II. Executive Summary

Institutional Structure:

The name of the organization used for the purpose of this paper will be referred to simply as the *institution*.

The ITS Department at the *institution* is responsible for all day-to-day computer system, network (LAN and WAN), and video (CATV) services and operations and user support. Only the groups pertaining to this particular incident will be mentioned.

- User Support/Help Desk – The "trenches" or front line support for ALL users. software, trains users, and resolves user issues.

- Network/Computer Operations – This includes system and network administrators, the network manager and the lead incident handler. At the *institution*, one person in most instances shares these responsibilities.

III. The 6 Stages of The Incident Handling Process

The compass and roadmap for proper incident handling are:

Preparation – In a nutshell, this step includes 10 general sub categories, policies, people involved, data, software/hardware, communication methods, supplies needed, means of transportation, space, power and environmental controls and documentation.

Identification – At this step we need to determine weather or not the situation is an incident or an event. If necessary, appropriate personnel are notified, every piece of evidence is identified access to the evidence is controlled.

Containment – If an incident has been declared, this is the step in which the threshold is crossed and the system(s) involved are modified. All parties involved should be notified including the ISP. A good backup of the affected system(s) should be made before disconnecting from the network and a copy of the backup should be safely stored. A mirrored disk would provide an excellent means of a backup.

Eradication –The specific cause of the incident should be identified, and any vulnerability corrected. System and network vulnerability testing analysis should be performed to verify these "loopholes" were corrected.

Recovery – The goal of the previous 4 steps is to get the affected system(s) back into production status. If possible, the compromised systems should be prepared to resume production status by using a base-lined, clean system that has been installed from scratch (this is preferred), but not always possible. Thus a restore from a recent backup prior to the incident will suffice. Although some data may be lost, this is better than loosing all of your data.

Follow Up – This is the final step that occurs after the calm has been restored and the involved parties have had some time to rest. Input from all parties involved in the incident comment and make recommendations on how things were unveiled and handled so they may be better prepared if they come across a similar incident.

A. Preparation

At the *institution*, a formal incident handling team wasn't heard of until very recently (within the past year). Administrators and a large majority of the IT staff seemed to turn a blind check to the reality that several incidents had occurred and would continue until a

total disaster occurred. Although several of the incidents were due to mischievous users (insiders) some were the result of a computer virus and users on the Internet. The results caused from these incidents were continually blamed on faulty hardware or an incompetent system administrator. The past several months have been a turning point for the *institution*, as education and first hand involvement have opened many eyes. It's good to see that some of the policies put in place at work are being carried over to users private practices at home.

Employee Awareness and Training

When an employee arrives for work on their first day, they are required to read, initial and sign the institutions policy on proper use on the institutional computer systems and network. These guidelines include what the *institution* considers abuse, along with the possible actions that may be taken if they choose to abuse their privileges. This must be completed before they are granted any access to the network. Within 3 months of their start date, a formal 2-hour class is held for all new employees and anyone else wishing to attend for a refresher (if seats are available). Even though the servers are adequately covered for antiviral infection and are backed up nightly, users must be trained on similar procedures for maintaining copies of their important documents and acceptable antiviral maintenance practices. Often times a real-time demonstration drives the point home.

Warning Banners

Upon logging onto any server locally, this warning banner is displayed.

NOTICE TO USERS

This is a College owned computer system and is the property of the *institution*. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning. Warning banners are present at all system logins on all systems.

In addition, all users are presented with a warning banner, in addition to informational data such as the date, time and workstation they are logged on from. This is accomplished via their logon script. They are required to press a key to clear the message. This forces them to do it and perform some action to make it go away. Their banner reads as follows:

NOTICE TO USERS

Use of this system constitutes consent to security monitoring and testing. All activity is logged with the date, time, your host name and IP address.

Due to the sheer diversity exposure to continuous change, individual workstations do not present a warning banner, at least not at this time.

Institutional approach to incident handling

Only staff members whose duties are directly related to core system and network support are authorized to take extreme actions to contain an incident, to include shutting down suspected systems and core network boxes. It has been my experience that too many cooks cause more chaos and convolute an incident by conducting heroics.

In the event that ANY system or network device shutdown occurs for security reasons, personnel responsible for those systems and their immediate supervisor are to be notified immediately. Only after the lead incident handler or executive director have the authority to request the system(s) be brought back on-line again and/or place back into production if such a shutdown occurs.

Users at the *institution* have been instructed to report a suspected incident to the helpdesk as soon as they become aware of it. This puts all calls into a central office where they are logged by date, time, username, their location and the circumstances surrounding their suspicions. This can give the incident handling team a road map of how things may have played out as well as a pattern of vulnerability. Users can also use this as a central point to stay abreast of the situation. This gives the user a feeling that their needs are being seen to and they're not being shut out.

If an incident is reported, the helpdesk is required to immediately notify a member of the incident handling team so the process of determination can begin ASAP. Heroism is STRONGLY discouraged and may be treated administratively if the circumstances warrant it. Again we want to keep untrained and unqualified personnel from contaminating possible evidence or invoking further damage.

The system and network manager is responsible for monitoring his own logs of events and reporting suspicious activity as needed. This person is our best friend as he knows the systems better than anyone and will more often than not be the direct target and alerted before users start calling the helpdesk.

Incident Handling Team

The *institutions* incident handling team, although still in its infancies, is formed from a lead response team which responds to most calls and are skilled in many facets of system and network engineering as well as incident handling, an secondary response team which is made up of appropriate our more technically proficient support staff (mainly helpdesk personnel), and system admins.

The Lead Response Team includes one security person trained and skilled in incident handling and a database admin skilled in database and programming languages from both the ITS department.

The Secondary Response Team is formed of the appropriate system administrators and Help Desk staff, as required.

If an incident has been declared, the *institutions* network center has been designated at the command post because it is secure, close to essential facilities like food, drink, bathroom, and is equipped with several means of communication. All essential personnel can be reached by cell phone or pager.

Jump Bags

Both teams are, for the most part, teams are primarily in fixed locations, and therefore do not carry jump bags per se'. We do have an isolated network located in the network center that may be used to test systems off the production network and can serve as a supply of spare switches, hubs and even a router. If need be, the isolated network can be connected to the production network. We always keep several spare UPS on hand (in various sizes) not necessarily for the onset of an incident but they are available if they are needed. The network center is supplied with about 40 minutes of backup power and is also backed by a natural gas powered generator, which kicks in within 10 seconds of a power failure. All software is stored in a secure cabinet in the helpdesk area if they are needed.

Key members on both teams members carry a cell phone and a pager at all times. All cell phones are capable of sending and receiving text messages as well as standard numeric and alphanumeric pages.

B. Identification

On Saturday, May 12, 2001, the default web site of the *institutions* web server was attacked and the default web pages replaced and infected with a Solaris backdoor virus. Fortunately the default web site was not used and the immediate impact on the user community was minimal. The following is an excerpt from the incident report as well as screen shots of what was left behind.

05 MAY 2001

1910 The Unicode exploit was launched against the mail server.

1912 Attacker tftp's an executable file "root.exe" to /inetpub/wwwroot/_vti_bin.

1912 Attacker begins replacing default.htm, default.asp, index.htm and index.asp files in the following directories:

c:\inetpub	c:\inetpub\wwwroot
c:\inetpub\mail	c:\inetpub\wwwroot\\images
c:\inetpub\mailroot	c:\inetpub\wwwroot_private
c:\inetpub\iissamples	c:\inetpub\scripts
c:\inetpub\wwwroot\cgi-bin	c:\inetpub\ftproot

1914 Attacker left the site. A total of 36 files had been added or replaced.

1935 System Administrator discovers the incident and contacts a member of the lead incident response team.

Over weekends the helpdesk is only staffed from 9:00AM – 5:00PM, so there was nobody else on hand to notify. The helpdesk manager was notified and on call staff were asked to report to work to handle any phone calls regarding this incident.

The remainder of the lead incident response team was summoned to work and the secondary incident response personnel were notified that they might also be called in to help with user support and damage control.

1950 Helpdesk messages are checked, and discovered that the first call came in at 1943.

1952 System administrator and the lead incident handler start reviewing security logs to determine the time of the incident as well as the extent.

2025 The decision is made by the lead incident handler to take the web server off-line. It was determined that disconnecting the system did not pose any risk of data contamination, to keep people off the contaminated site.

2028 The security logs indicated that the extent of the damage was limited to the Inetpub directory on the C:\ drive, which was mirrored. 1 drive was removed, bagged, identified and sealed.

2042 System administrator runs "netstat –an" from a command prompt and redirects its out put to a text file (ports.txt) to ensure that there are no unusual ports opened.

2048 System administrator and lead incident handler compare the results with documentation gathered after the last system changes.

2105 It is determined that all ports open on the server are legitimate.

2110 A virus scan of all partitions is started using Norton Antivirus 2000.

2133 Virus scan completed and it is discovered that all 36 of the files deposited with the attacker are infected with the Backdoor.Sadman.Dr virus.

A quick on the Symantec McAfee web sites aligned with what we saw on the affected system:

"Backdoor.Sadmind attempts to spread on systems that have unpatched versions of Solaris installed by using a buffer overflow exploit on a program named Sadmind. Backdoor.Sadmind uses TCP port 600 on the Solaris computer to listen. Two directories are created:

/dev/cub
/dev/cuc

These directories contain a list of compromised computers and the tools used by Backdoor.Sadmind. Several scripts will also be running on the Solaris computers such as sadmin.sh and uniattack.sh.

Backdoor.Sadmind also victimizes systems that have unpatched versions of Microsoft IIS. It replaces the default Web page file so that the Web server displays the new Web pages instead of the default pages. These pages contain profane remarks against the government, and the text:

PoizonBOx"

The next step was to check Microsoft's web site for a description of the vulnerability. The site is: http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

At this point the team felt as though they had a handle of what had happened, how it happened and what to clean up. To this point, the help desk had answered and returned over 200 phone calls. For the most part users were polite and understanding, and had expressed their appreciation for the quick initial response and long hours.

This was only the first significant incident the *institution* had ever responded to since the induction of an incident response team, so tensions were high, hearts were pounding and the fear of God struck the disbelievers. The one thing that was missing, was the finger pointing. This showed me the mutual trust and respect for the members of the department.

C. Containment

Upon shutting off access to the web server, the project of notifying users and responding to calls was under way. It wasn't until after reviewing the log files that we were sure that the damage had been contained to the directory containing the default web site. What we were unsure of it what other types of payload the deposited files may have contained. For example, when an unsuspecting user opened it, did any code run on their computer or were any other scripts called that caused damage to the affected system itself.

The *institution* in mostly comprised of a switched internetwork, although some building have a few pieces of shared media. The core of the network is completely switched and divided into 19 VLANs to allow for segmentation and refined manageability. This allows the network manager the option of filtering or disconnecting depending on the circumstances. The decision was made to unplug and remain completely detached was made until the full affects of the incident were known.

Although this completely disabled access to the web site, all other services remained up and the danger of propagating further infection was eliminated.

In this specific incident, the decision to take the server completely off-line was made to avoid the embarrassment of the vulgar language presented on the tainted web pages, and

to prevent the potential use of destructive code embedded in the page(s) themselves. We came to a unanimous decision that attaching the server to the "isolated" network and launching the pages was too risky in itself and based on the information we attained from Symantec and Microsoft, we felt that any danger had been contained.

D. Eradication

In this incident, all data files that had changed since the last known good backup were replaced from backup. Due to the detail outlined in the security logs, we focused primarily on the C:\Inetpub directory. Because all of the .htm and .asp files that had been planted on the server were infected with the Backdoor.Sadmind virus, a thorough virus scan of all partitions was conducted as well. Even though we knew that sadmind was used to exploit the Solaris box that was used to attach the *institutions* server and didn't do any damage to the NT system, the fact that another backdoor or other malicious code could have been planted was a real concern.

This exploit uses a known issue with the way in which IIS handles Unicode sent to it as part of a URL. It relies solely on the lack of keeping systems up to date and patched.

Microsoft had posted a hot-fix for this very vulnerability in August of 2000, but it had never been applied to this system. This is a very common oversight by many system administrators, although far be it from an acceptable excuse. In today's world of connectivity, no longer can patches and upgrades take a back seat in order to avoid down time. The threat(s) are a reality, as this incident serves as case and point.

E. Recovery

05 MAY 2001

2205 All original files were replaced from a known good backup.

2230 Full scan using Norton Antivirus was performed on all partitions to ensure no viruses were left behind.

2330 All NT hot-fix patches since service pack 6a were applied.

06 MAY 2001

0020 All IIS hot-fix patches since the release of Service pack 6a were applied.

0140 A netstat –an was run to ensure that all ports open for listening were legitimate.

0230 A meeting involving all lead and secondary incident handlers was held to discuss weather the system should be put back into production.

0300 The system was placed back into service, all members retired for the remainder of the weekend.

11 May 2001

1000 A wrap up meeting was conducted with all individuals involved in the incident. The system was declared stable and clean. The incident declared resolved.

F. Follow Up / Lessons Learned

Upon conclusion of the incident summary, the following conclusions were drawn.

- **Systems weren't up to date with patches.**

While all system administrators are reminded monthly to check their vendors web sites for patches, this had fallen between the cracks because things had been going smoothly.

The ITS department as a whole had taken a beating in the past when they announced downtimes for various activities, and started to avoid doing the right thing in order to avoid some of the negativity from the user community

- **Keep the restore machine in the network center**.

A technician from the helpdesk needed a PC to use so he could test some software and the restore machine was given to him to use. Not only was this person out of the area, so was the PC. Nobody knew where he had taken it. After 1,5 hours of searching, we ended up commandeering a computer from a lab. Not only was this time wasted, it added to the frustration of spending a Saturday at work not knowing how bad things were going to be.

- **User awareness had to be heightened.**

One of the main factors in the system involved not being kept up to date, was the sys admins fear of repercussion from Senior Administration and the user community for taking systems down on a monthly basis. What I had found work for some of the people in the ITS department was a live demonstration showing how a simple mistake can cost you your data. Users tend to have the "it can't happen to me" attitude.

Recommendations:

- The *Institution* should regularly schedule downtime on a predetermined routine so that systems can be maintained properly. This requires Senior administration to fully support this recommendation, and would take that pressure off the system admins.
- Security awareness training should be conducted on a regular basis starting with

the ITS department. This training should also be made available to the user community and possibly put on-line in the form of streaming video. Again, live demonstrations seem to drive the point home.

- Equipment designated for evidence collecting or incident handling should be held just for that . Under no circumstances should any of that equipment be taken from the network center unless it is being used in the investigation of an incident.

IV. Assessment Details

Unicode exploit definition:

The primary sources used to understand what had happened were Microsoft, Cert and Sun Microsystems. Below are snippets of information that proved most useful during the identification phase.

- **Microsoft**

"A canonicalization error can, under certain conditions, cause IIS 4.0 or 5.0 to apply incorrect permissions to certain types of files. If an affected file residing in a folder with restrictive permissions were requested via a particular type of malformed URL, the permissions actually used would be those of a folder in the file's parentage chain, but not those of the folder the file actually resides in. If the ancestor folder's permissions were more permissive than those of the correct folder, the malicious user would gain additional privileges to the affected file."

-AND-

"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."

- **CERT**

"Based on preliminary analysis, 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. It will add "+ +" to the .rhosts file in the root user's home directory.

Finally, it will modify the index.html on the host Solaris system after compromising 2,000 IIS systems. After successfully compromising the Solaris systems, it uses a seven-month-old vulnerability to compromise the IIS systems.

Solaris systems compromised by this worm are being used to scan and compromise other Solaris and IIS systems. IIS systems compromised by this worm can suffer modified web content.

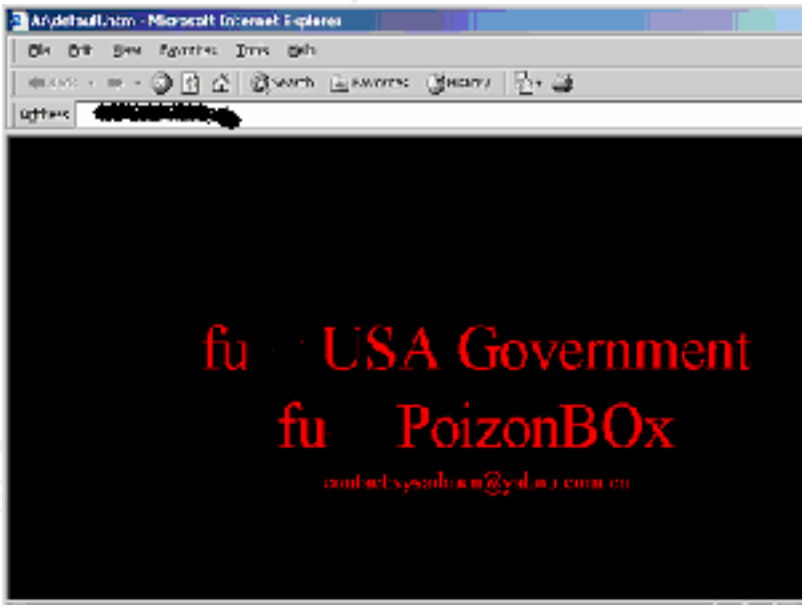
Intruders can use the vulnerabilities exploited by this worm to execute arbitrary code with root privileges on vulnerable Solaris systems, and arbitrary commands with the privileges of the IUSR_*machinename* account on vulnerable Windows systems. "

· **Sun Microsystems**

"The sadmind program is installed by default on SunOS 5.7, 5.6, 5.5.1, and 5.5. In SunOS 5.4 and 5.3, sadmind may be installed if the Solstice AdminSuite packages are installed. The sadmind program is installed in /usr/sbin. The program can be used to perform distributed system administration operations remotely. A buffer overflow vulnerability has been discovered in sadmind which may be exploited by a remote attacker to execute arbitrary instructions and gain root access."

Defaced Web Pages

This is a screen shot of the web pages left behind by the attacker. The "adjectives" used to describe the government have been altered to avoid offending any readers.



All of the .asp and .htm files left behind were also infected with the Backdoor.Sadmind.Dr virus. None of these files were executed from the server. We used a standalone PC to open them to attain screen shots, then re-ghosted the hard drive when through.

Security Logs

Upon close examination of the security logs it became very clear as to what the attacker had done. Below are a few of the entries recorded. Because the screen shots don't show all of the details, I dumped them into Excel so you can see the details of an entire event.

Event Type:	Success Audit		
Event Source:	Security		
Event Category:	Detailed Tracking		
Event ID:	592		
Date:		5/5/2001	
Time:		7:12:52 PM	
User:		NT AUTHORITY\SYSTEM	
Computer:	-------		
Description:			
A new process has been created:			
	New Process ID:	2160080192	
	Image File Name:	root.exe	
	Creator Process ID:	2193296320	
	User Name:	SYSTEM	
	Domain:		NT AUTHORITY
	Logon ID:		(0x0,0x3E7)

Time:		7:12:52 PM
User:		-------\IUSR_--------
Computer:	----------	
Description:		
Object Open:		
	Object Server:	Security
	Object Type:	File
	Object Name:	C:\Inetpub\wwwroot\index.asp
	New Handle ID:	-
	Operation ID:	{0,2371512584}
	Process ID:	2160080192
	Primary User Name:	IUSR_-------
	Primary Domain:	-------
	Primary Logon ID:	(0x0,0x8CD754DA)
	Client User Name:	-
	Client Domain:	-
	Client Logon ID:	-
	Accesses	
		SYNCHRONIZE
		WriteData (or AddFile)
		AppendData (or AddSubdirectory or CreatePipeInstance)
		WriteEA
		ReadAttributes
		WriteAttributes

Event Type:	Success Audit		
Event Source:	Security		
Event Category:	Detailed Tracking		
Event ID:	592		
Date:		5/5/2001	
Time:		7:12:55 PM	
User:		NT AUTHORITY\SYSTEM	
Computer:	-------		
Description:			
A new process has been created:			
	New Process ID:	2160003488	
	Image File Name:	root.exe	
	Creator Process ID:	2193296320	
	User Name:	SYSTEM	
	Domain:		NT AUTHORITY
	Logon ID:		(0x0,0x3E7)

Event Type:	Failure Audit		
Event Source:	Security		
Event Category:	Object Access		
Event ID:	560		
Date:		5/5/2001	
Time:		7:12:55 PM	
User:		-------\IUSR_-------	
Computer:	-------		
Description:			
	Object Server:	Security	
	Object Type:	File	
	Object Name:	C:\Inetpub\wwwroot\index.htm	
	New Handle ID:	-	
	Operation ID:	{0,2371513281}	
	Process ID:	2160003488	
	Primary User Name:	IUSR_-------	
	Primary Domain:	-------	
	Primary Logon ID:	(0x0,0x8CD754DA)	
	Client User Name:	-	
	Client Domain:	-	
	Client Logon ID:	-	
	Accesses		READ_CONTROL
		SYNCHRONIZE	
		WriteData (or AddFile)	
		AppendData (or AddSubdirectory or CreatePipeInstance)	
		WriteEA	
		ReadAttributes	

The IIS event log provides information that indicates when someone has tried to exploit the vulnerability. The information located in these logs confirmed what we saw in the security logs.

All we did was search the event log for a successful GET involving an URL that has the string "/../" anywhere in it.

Virus San Results

Before making any attempts to manipulate any data on the server, a complete system viral scan was performed using Norton Antivirus 2001. The definition files were checked to ensure they were the most recent before starting. Below is a snippet of the generated report (the system name has been sanitized for this report)

Date: 5/5/01, Time: 21:12:12, ------- on -------
The file
C:\inetpub\default.htm
is infected with the Backdoor.Sadmind.Dr virus.
Access to the file was denied.

Date: 5/5/01, Time: 21:12:46, ------- on -------
The file
C:\inetpub\default.htm
is infected with the Backdoor.Sadmind.Dr virus.
Access to the file was denied.

Date: 5/5/01, Time: 21:19:10, ------- on -------
The file
C:\inetpub\default.asp
is infected with the Backdoor.Sadmind.Dr virus.
Unable to delete this file.

Date: 5/5/01, Time: 21:19:14, ------- on -------
The file
C:\inetpub\default.htm
is infected with the Backdoor.Sadmind.Dr virus.
Unable to delete this file.

These files were deleted manually upon completion of the scan through the Norton console, thus ensuring that all traces were eradicated.

Stand Alone Network

Located in the office of the *institutions* network manager, is a stand-alone test network. This small but useful network server in various capacities besides incident handling and can be if necessary, connected to the production network. This network is used to test and configure new equipment, test new technologies for performance in a production environment, personnel training and troubleshooting. This “special” network is comprised of the following equipment:

- 1 - 3Com CoreBuilder 9000 (Ethernet fabric) with L3 and L2 capabilities
- 1 - 3Com switch 3300

- 1 - 3Com SSII PS40
- 1 - Cisco 2514 router
- 4 - Media converters (2 - fiber to 10BaseT, 2 - AUI to 10BaseT)
- Servers and laptops are available in the office and aren't permanently designated to this network. One of the servers contains a DAT drive and one contains a DLT drive to accommodate restores.
- Software – a complete library of all software deployed on campus is available in the Helpdesk area in a locked cabinet. Copies of network specific software (sniffer, IDS, Vulnerability scanners, backup software, etc.) are located in the network managers office.

The only item we used in the handling of this incident was a recovery server, so that we could do a file compare from the last good backup.

V. System Backups

It is important that file system backups are performed regularly on all production servers, at least 5 days per week (typically Monday through Friday). At the *institution*, all production servers are backed up daily with the exception of BDC's and secondary DNS servers. If nee be, they can be reinstalled from the original CD's and synchronized with their primary. A full backup is performed on all servers Monday through Friday and are on a 4 week rotation (basically a monthly rotation)

Backup Equipment

NT servers are backed up with 2 different types of backup software, Replica for NT and ArcServ 2000. NT Backup proved to be very slow and not effective in backing up the OS or open files. Depending on the amount of data being backed up on a particular server, the *institution* uses a mix of 4mm DAT, and DLT7000's.

Mail /Web Server

At the *institution*, the Exchange server is replicated to tape using a product from Stac software called Replica for NT. The software performs a sector-by-sector backup, which ensures that ALL files are backed up every time. While this software inherently provides for simple disaster recovery capability out of the box, if the backups span tapes, the only way to get single files or directories form backup is to do a complete restore (OUCH). This hasn't been an issue because users mailboxes are limited to 20MB, so the entire mail store is only 12GB, and the entire system easily fits onto a single DLT tape.

Backups typically take about 3.5 hours to run.

Recovery

Because the hacker didn't alter any files outside of the inetpub directory that hosted the Default web site, the production site was unaffected and therefore caused no interference

with the production site. A restoration of each partition was performed on a recovery server and compared with the files on the live server.

Once all altered or replaced files were identified, they were deleted and replaced with known good files from backup. The system administrator was then instructed to apply ALL patched released for NT and IIS since the release of SP6a (the currently installed service pack) to ensure all known vulnerabilities were patched.

It was after this that the system was tested and placed back into production. As a precautionary measure, the appropriate system administrators were instructed to do the same thing to their systems so that we could formalize this in their documentation and eliminate the possibility or revisiting this same incident on another system. A member of the LEAD RESPONSE TEAM stayed on hand until this process was completed.

There was no evidence of any other systems being penetrated or compromised.

VI. Evidence

To provide and ensure a means of the collection of evidence in the event of an incident, the lead incident response team has assembled a collection kit. The kit resides in the Security office because it is manned 7x24, is secure and is provisioned with means of backup power and communication.

The *institutions* evidence collection kit contains the following items: plastic and anti-static bags (several sizes of each), 6-black permanent makers, 2-rolls of scotch tape, 2-rolls of 2" masking tape and 1-roll of duct tape, and finally, a copy of the *institutions* policy and guidelines for collecting, handling and storing evidence. All non-static sensitive evidence is collected and placed in plastic bags and all static sensitive materials (like hard drives) are stored in static bags. The bags are then sealed, taped and marked with the time and date, signed by a handler and 1 witness. These items are then placed in a lockup cage in the security office until they are needed. Again, this location is manned 7x24 and the storage event is also logged into dispatch logbook. This further enhances the integrity of the handling if the incident leads to trial.

The incident in this case was one of the mirrored hard drives used for the OS. In the event the *institution* wanted to pursue the person responsible, we had an exact image of the hard drive prior to and attempt to contain or eradicate things. We also included a copy of the last known good backup for thoroughness. Other information was collected, but was not maintained at a level for legal proceedings.

- The *institution* had 9 individuals involved in this incident. All of them we members of the ITS department
- Total downtime for the mail server was about 10.5 hours. Although we weren't aware of this at the beginning, all of the downtime was precautionary, the actual functionality of the server wasn't affected, but the security flaws could have been

devastating. (Did you ever tell your users they lost ALL of their mail, and it would be a few days until the service would be restored?)

VII. Innovations made by the *Institution*

Although the *institution* fell prey to a simple oversight, the lesson learned and innovations made far surpass what other *institutions* larger and smaller are doing or planning to do..

Implementing traffic shaping techniques to the WAN.

Although it does not directly relate to this specific incident, prioritizing traffic to and from the internet can prevent any 1 application from consuming all of your bandwidth. This also provides an excellent means of identifying all types of traffic flowing both in and out of your network. All unidentified types of traffic can be lumped together and managed as a whole if it is being "hidden in the mess".

Keep the network as logically and physically segmented as possible

Time is important when dealing with an incident. The ability to separate a server, servers or an entire segment form the rest of the network in order to stop an attack in progress or to perform testing, containment and eradication is very important. You don't want to take unaffected services off-line or entire segments of users if that is not your intent. This should also allow you the option of connecting the system(s) in question to an isolated network.

The implementation of IDS.

By implementing a well planned and managed IDS system between the WAN and the LAN as well as between the server segment and the rest of the internal network. In the case of the *institution*, many incidents as launched from the inside. This can provide a handler more insight into the incident and act as evidence if it is to be pursued in court. IDS is also used to baseline what may be considered as normal probes and scans.

Regular use of vulnerability scanners against the network and servers.
At the *institution*, as well as many other places, IT folks tend to wear several hats. This can lead to lack of keeping systems up to date and patched as well as the lack of awareness to new vulnerabilities that may be present in their systems. A good vulnerability scanner with its database up to date, can provide the insight needed to prevent the threat of attack. While it is not bullet proof, the harder it is for someone to break in, the more likely they'll move on to the next house. It is better to be proactive than reactive.

References:

Microsoft, Web Server Folder Traversal, October 17, 2000
http://www.microsoft.com/technet/security/bulletin/MS00-078.asp

Microsoft, File Permission Canonicalization, August 10, 2000
http://www.microsoft.com/technet/security/bulletin/ms00-057.asp

CERT, Advisory CA-2001 sadmind/IIS worm, May 10, 2001
http://www.cert.org/advisories/CA-2001-11.html

Sun Microsystems, Bulletin #00191 sadmind, December 29, 1999
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/191&type=0&nav=sec.sba

Stmantec, Backdoor.Sadmind, June 12, 2001
http://www.symantec.com/avcenter/venc/data/sadmind-iis.html