GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Roy Hutchison - roy.hut001
Advanced Incident Handling and Hacker Exploits
GCIH Practical Assignment
Version 1.5c
Current as of March 28, 2000 (amended May 22, 2001)
Option 1-Illustrate an Incident

Title: Unicode exploit of IIS servers and sadmind / IIS worm incident

Executive Summary

"The Company" is an electronic commerce software and services firm that provides custom solutions and off the shelf software integration solutions for its customers. The Company provides end-to-end services from strategy consulting to hosting and applications management. Two of the company's clients Internet application servers were defaced at The Company's East Coast hosting facility at approximately 3 AM EST on May 7, 2001. A client user detected the defacement at approximate 8 AM EST that morning. The Company followed its incident handling procedures for detection, containment, eradication, and recovery. The Company was able to have the afflicted systems back on line by 4:30 PM EST. The major symptoms of the attack were the actual defacement and entries in the IIS server logs. The cause of the exploit was determined initially to be an exploit of the IIS Unicode vulnerability. On May 8th, CERT released an advisory addressing the sadmind / IIS worm. The IIS log fingerprint published in the CERT advisory for the CERT IIS exploit matched that of the compromised systems. The Company implemented improved system build procedures and ISS Scanner to prevent future compromises that arise as a result of improperly patched servers.

Background

The Company builds Internet and electronic commerce applications for commercial and government entities. The primary focus of the company is the development of custom solutions for its clients and provides the option to host the client's electronic commerce application in a hosting facility located on the East or West Coast. The Company has several divisions. Internal Information Technology is supported under the Company's Operations division. The Company also has a service delivery division that includes a hosted services group. The hosting service's facility's Network Operations Center (NOC) is responsible for all aspects of client hosting support. A NOC is located in the East and West Coast hosting facility.

The general architecture of the NOC hosting facility's environment is illustrated in Appendix A, figure 1. The systems that were affected by this incident are referred to as "System A" and "System B". The hosting facilities have two independent Internet connections, redundant power supplies, and a controlled atmosphere. The NOC has a centralized backup system and uses Virtual Local Area Networks (VLANS) for traffic segregation.

Preparation



© SANS Institute 2000 - 2005 Author retains full rights.

The Company has a corporate incident response program that is outlined in its Incident Response Procedure Manual. The manual includes process flows, contact information, and forms for gathering information when handling an incident. The process flows provide guidance to the incident handler and the team as to responsibilities, immediate actions required and supplementary actions required to guide the response team through the incident. The contact information lists the company members that are qualified to be incident managers, corporate management, administrative, and public relations contacts. The forms provide an outline of information required to be gathered during the incident response.

The East Coast NOC follows the corporate procedures and has its own supporting incident handling procedures for use in the hosting facility's operations. The NOC incident handling and response procedures as well as corporate and client contact lists are maintained in the NOC for the shift support personnel to use. The NOC's incident handling policy and procedures include required immediate actions and instructions on who to call first. The Company's management makes decisions to notify law enforcement agencies and is responsible for coordinating client relations. All NOC employees are trained to follow the NOC's incident response procedures as part of their initial employment training and revisions are passed through email. Formal refresher training is held on an as needed basis.

The Incident handling processes and procedures provide a framework for handling incidents including interdivisional reporting requirements. The roles of the administrators, incident handlers, and management leadership teams are outlined. There is an appendix with a decision matrix to assist with decisions regarding Law Enforcement Agencies and how to maintain an evidence trail.

The Company has shifted its approach to handling incidents to minimize expenses by reducing travel costs. During the Identification and Containment phases, the "Incident Manager" and affected Project / Program Manager will make a decision as to whether or not to travel to support the incident. Only in cases of extreme damage will the entire team actually travel to the hosting site.

Jump kits

Members of The Company's staff that work on incidents are encouraged but not required to maintain a jump kit. The author's jump kit contains the following items:

1. Toshiba Tecra 8000 with 128 MB RAM
    2. Two 6 GB hard disks: one with Windows2000 Professional (disk for corporate work) and one with WindowsNT 4 workstation and Redhat Linux 6.2 (dual boot). VMWare with Windows 95 is loaded on the Redhat disk.
    3. 10/100 Ethernet PCMCIA card
    4. Internal modem
    5. IOMega Zip drive
6. Netgear DS104 (Dual speed 4 port hub)
7. Cisco Rollover cable, 9pin, and 25 pin connectors



© SANS Institute 2000 - 2005 Author retains full rights.

8. 7 foot and 25 foot straight through network cable
9. 7 foot crossover cable
10. CDs with WindowsNT 4, SP 6a, NT Option Pack, Resource Kit, Windows2000 server, Solaris 2.6 and 7.0, Linux 6.2
11. Corporate phone list and incident response procedure
12. Reference books from library for the appropriate O/S
13. Notebook, pencils and pens

Members of the incident handling teams routinely monitor mailing lists and other Internet information resources for alerts to vulnerabilities. In the case of one of the systems (a government client), one of the incident team members received a warning from the NIPC on April 26, 2001 regarding the sensitivity of the Chinese to the First week of May. This warning was part of the April 26th SANS Newsbyte:

> "NIPC Warns of Potential for Increased Cyber Attacks:
> The National Infrastructure Protection Center (NIPC) warned US businesses to prepare to defend against increased cyber attacks from China during the first week of May which encompasses May Day, Youth Day, and the anniversary of the accidental NATO bombing of the Chinese embassy in Belgrade"[0]

This warning was forwarded to the NOC manager on May 4th and promulgated to NOC team members via email. The seriousness of a Chinese cyber threat was exacerbated by the emergency landing of a U.S. Navy EP-3E Aries aircraft on Hainan island, China On May 1, 2001.

Identification

The NOC has numerous manual and automated processes for intrusion detection and response. The goal of the monitoring is to ensure that the Company's client sites are available and operating in accordance within the requirements of the established contracts and service level agreements. The goal of the manual processes is to monitor the results of the automated manual processes, identify vulnerabilities that emerge as a result of operating system configurations, and enforce the NOC's change management policy. Other procedures and provide guidance for setting up and maintaining firewall rule sets, supporting administrator remote access, and instructions for the taking and restoring backups.

Automated processes include using network monitoring software to perform the following tasks:

- Monitoring and analysis of user and system activity
- Recognition of activity patterns reflecting known attacks
- Statistical analysis for abnormal activity patterns
- Operating-system audit-trail management
- Tracing user activity from the point of entry to point of exit or impact
- Attack Signature response triggering (email)



© SANS Institute 2000 - 2005 Author retains full rights.

The Company uses ISS Real Secure network modules for network based intrusion detection. Host level intrusion monitoring is not performed unless the client specifically requires it. Firewall and router logs are kept and used for post incident analysis.

Despite the in-place automated monitoring systems, the incident was discovered by a System A client representative who observed the web site defacement during casual Internet surfing on the morning of 07 May, 2001. The defacement is illustrated in appendix A, figure 2 (warning: this figure contains offensive language). The HTML code that generated the page (contained in the .htm, .html, and .asp pages listed in table 1 is (offensive words edited):

> "html><body bgcolor=black><br><br><br><br><br><br><table width=100%><td><p align="center"><font size=7 color=red>f*ck USA Government</font><tr><td><p align="center"><font size=7 color=red>f*ck PoizonBOx<tr><td><p align="center"><font size=4 color=red>contact:sysadmcn@yahoo.com.cn</html>"

The NOC verified that System A was indeed defaced. The NOC began to follow their required immediate actions by notifying the appropriate management personnel and manually checking the status of other client's hosted systems. During the manual checks, it was determined that System B's database server was also compromised as a result of an installation of the web service on that machine. At this point in time, the only facts about the incident that were known were that the servers that were defaced were running Microsoft Internet Information Server (IIS) version 4.0.

Containment

The NOC manager declared the event an incident and directed that a full (and separate from the normal rotational backups) backup be taken of the System A and System B servers. This was accomplished using the NOC's Legato Networker backup system. Fresh tapes were used to create a full file by file backup of the server. These tapes were then removed from the DLT storage device and stored in locked cabinet in the NOC. The Legato GUI client was used to create the backup.

Notifications were made to The Company's management and the IT security group. The clients for System A and System B were also notified. The servers were disconnected from the Internet connected portions of the NOC's network. Temporary web sites for System A and System B were installed that contained the message "this site under construction". The Company's IT Security Engineer became the overall incident team leader and the NOC manager the on site leader. The two made a list of the required incident handling team members consisting of subject matter experts and system support personnel.

Initial surveys of the damage done by the defacements indicated that it was limited to the IIS servers home directories based on log data and quick, preliminary file system surveys. The System A and system B IIS servers supported Internet applications; a secondary impact of the defacement was to deny users of the systems access to their data and application functionality.



© SANS Institute 2000 - 2005 Author retains full rights.

As a result, the NOC manager and incident manager decided to use a virtual response team and did not require travel by all team members. This decision was based on the need to control company costs and on the apparent limited scope of the damage. If the investigation warranted a larger scope investigation or more support, the decision to fly the entire incident team to the NOC would be made. The incident handling team was lead locally by the NOC manager. The Incident Team leader (IT security engineer) worked the issue remotely from the corporate headquarters (not local to the East Coast NOC) and made reports to the Company's operations officer. Information gathering and corrective actions were to be taken by off shift NOC personnel and support staff. Network security consulting services were provided from the service delivery group (author).

The NOC manager made the decision to file a report with the National Infrastructure Protection Center via the online web site at http://www.nipc.gov/. Although a final financial damage report was not yet available, it was estimated to be less than $50,000.

Eradication

Evidence from the incident was copied and reviewed in an effort to diagnose the symptoms, determine, if possible, the cause, and determine what actions are required to resume operations. Logs were also examined from the firewalls and IDS systems to determine if other servers were attacked. The Company's IT security engineer made discreet announcements to corporate office IT managers to look for signs of the attack on other servers that are accessible from the Internet.

The affected servers' home page / web site was replaced with a temporary page that listed it as "under construction". Firewall rules were examined to determine the types of connections permitted. Table 1 lists the firewall policy that drove the rule st in effect for System A and System B.

**Table 1. Firewall policy for System A and System B**

| From | To | Protocol | Policy |
|---|---|---|---|
| Any | System A WWW server | HTTP, HTTPS | Permit |
| System A WWW server | System A application / DB server | ODBC | Permit |
| System A WWW server | Any | Any | Permit |
| System A DB / applications server | Any | Any | Permit |
| Admin Network | System A | PCAnywhere | Permit |
| Admin Network | System A | Networker Backup | Permit |
| Any | System B WWW server | HTTP, HTTPS, FTP | Permit |
| Any | System B DB server | HTTP, HTTPS, FTP | Permit |
| System B WWW server | System B application / DB server | ODBC | Permit |
| System A WWW server | Any | Any | Permit |



© SANS Institute 2000 - 2005 Author retains full rights.

| | | | |
|---|---|---|---|
| System A DB / applications server | Any | Any | Permit |
| Admin Network | System B | PCAnywhere | Permit |
| Admin Network | System B | Networker Backup | Permit |
| Any | System B WWW server | HTTP, HTTPS, FTP | Permit |
| Any | System B DB server | HTTP, HTTPS, FTP | Permit |

Further, the setup of the firewall permitted UDP DNS queries and ICMP implicit rules. The rules show excessive services permitted to connect to System B's Database / application server. Another vulnerability illustrated by the policy is the lack of control over the outbound connections.

There were two major pieces of information that were left behind by the attack: changes in files on the victimized systems and entries in the IIS logs. Firewall and IDS logs did not detect port scans or attempts to access the systems on esoteric ports. The attack was recorded by other IIS servers' logs in the NOC; however, these systems were not defaced successfully.

The following files (Table 2) were found or altered on both System A's and System B's the IIS servers (absolute paths presented are illustrative):

**Table 2. Changed Files**

| File name | Modified | size(bytes) |
|---|---|---|
| D:\inetpub\wwwroot\default.htm | 5/6/2001 3:58 AM | 289 |
| D:\inetpub\wwwroot\index.htm | 5/6/2001 3:58 AM | 289 |
| D:\inetpub\wwwroot\default.asp | 5/6/2001 3:58 AM | 289 |
| D:\inetpub\wwwroot\index.asp | 5/6/2001 3:58 AM | 289 |
| D:\inetpub\scripts\root.exe | 11/18/1999 3:04 PM | 208,144 |
| D:\inetpub\scripts\tftp274 | 3/4/2001 5:37 PM | 0 |

The owners of the files were the IUSR_SYSTEM_A and ISUR_SYSTEM_B for system A and System B, respectfully. The IIS logs of systems A and B (successfully compromised) contained a very distinct footprint (a more complete log excerpt may be found in Appendix B). The source address was a web server with Pro-Chinese content. The time hash on the IIS logs was found to be 4 hours off of the system time.

System A / B IIS logs.

#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 2001-05-06 07:57:27
#Fields: time c-ip cs-method cs-uri-stem sc-status
07:57:27 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 200
07:57:27 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 200



© SANS Institute 2000 - 2005 Author retains full rights.

07:57:29 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:57:30 source.attack.domain GET /scripts/root.exe 502
07:57:30 source.attack.domain GET /scripts/root.exe 502
07:58:41 source.attack.domain GET /scripts/root.exe 502
07:58:44 source.attack.domain GET /Default.htm 200

An exhaustive review of the other web server logs hosted in the NOC facility contained similar logs but with different results; the defaced servers had sc-status of 200 for some of the variant URL requests whereas the unaffected systems returned 403 errors. An example of an unaffected "System C" logs is contained below:
System C IIS logs:

#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 2001-05-07 00:31:43
#Fields: time c-ip cs-method cs-uri-stem sc-status
00:07:43 source.attack.domain GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir 403

Neither System A nor System B were formally baselined (using a program such as TripWire) prior to the attack. File dates and sizes were compared with other systems that had similar software installations to roughly determine the extent of the damage. The NOC administrators would sit side by side and compared the files using a command prompt and dir /p on the c:\winnt, c:\winnt\system32, and c:\inetpub directories. The defaced web server for System A was the portal of System A's web site. The defaced web server for System B was the database server that supported the application. The application installers had left a default installation of IIS running and accessible due to a miscommunication between the installers and the NOC staff.

The first impression was that the systems were defaced by a disgruntled employee that used the open FTP access to upload the modified pages. This was based on the fact that the company had just begun a RIF layoff and that inadequate time had passed to change the passwords on then servers and the exposure of System B to FTP (firewall policy). The firewall logs and FTP server logs did not support this; System A did not have an active FTP service, either. The incident team reviewed the available IIS logs and defaced files and determined that likely mechanism for defacing the IIS servers was the Unicode file traversal exploit[1].

The National Infrastructure Protection Center (NIPC) published several advisories concerning the vulnerability of un-patched IIS servers[2] to the Unicode and other IIS vulnerabilities. NIPC and the Center for Information Security (CIS) released a tool called "patchwork" to help Windows NT / IIS server managers to test their systems[3]. SANS Global Incident Analysis Center also wrote a detailed analysis of a Unicode exploit kit called BackGate[4]. The WinGate / Backgate kits also make use of the Unicode exploit.

"The Unicode Bug" arises from several vulnerabilities in Microsoft Internet Information server. It was first documented in the fall of 2000[5] and Microsoft issued a patch in October, 2000. Unpatched IIS (versions 4 and 5) servers can be exploited if the attacker uses the "double dot



© SANS Institute 2000 - 2005 Author retains full rights.

slash [../]" and the extended Unicode character representations of known or default directory locations[6]. The attacker types a URL (or writes a tool that submits a URL to a web server) of the form:

http://<victim.server.com>/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+<command>+<args>

This would allow the attacker to execute WindowsNT command directives if the file system on the victim system matches the request URL. The Unicode exploit takes advantage of the way that IIS interprets requests in Unicode. Default installations of IIS also leave the IUSR_<computername> account in the "everyone" group. This allows a user to copy the cmd.exe file into the (for example) c:\<webroot>\scripts directory[7]. The attacker can now exploit the server using Unicode to issue commands to the copied file in the \\scripts directory. The Backgate and Wingate toolkits use the copied cmd.exe to deposit exploits through TFTP (trivial file transfer protocol. The only limitation is the permissions of the IUSR_<computername_account>.

IIS web server logs will record the request as illustrated above and in Appendix B; however, unless uri-stem and uri-query are selected, the results will not include the detailed Unicode. In the case of System A and System B, the extended log properties were not set and as a result, the actual attack commands were not known. System C's logging (see above) did have the uri-stem and uri-query properties selected.

For the attack against of System A and System B, the root.exe file had the same characteristics (file size and date) as the cmd.exe file in the c:\winnt\system32\ directory and was the copy in the scripts directory that allowed the attacker to execute their commands remotely. The presence of the tftp274.exe file was also of concern. It left the impression that the web site defacement could have been a decoy and more serious damage could have been done (i.e. depositing a Trojan program or logic bomb) on the system.

Recovery

At 1245 (on May 7th), a teleconference was held to discuss the incident and determine the next steps. The challenge facing the team was to determine what other damage had been done and how to return the sites to operation. The clients for System A and System B wanted their Internet sites restored to operation as soon as possible. The primary issue to be resolved was how to return to operations. There was no evidence to suggest that further attempts were being made to compromise any of the system and the damage seemed limited to the defacement. The unknown factors were the lack of a true comparison to a prior known condition. A clean backup could be used to determine a baseline; however, time a resources did not permit this as the same amount of resources could be used to reload the systems from scratch.

In light of the clients' desires and the unknown nature of the damage done, the decision was made to reformat the system hard disks, reload the servers from operating system up, and recover a backup from May 05, 2001. A separate recovery team of system and project administrators for System A and System B was set up to rebuild and restore the affected systems. Fortunately for



© SANS Institute 2000 - 2005 Author retains full rights.

System B, no transactions were attempted over the weekend (non business hours); as a result, the system could be rebuilt from Saturday's full backup without a risk of losing data.

Timeline

The sequence of events up to this point is as follows:

0815 Client of System A notified the NOC that the web site had been defaced
0820 Problem confirmed, log entry made and escalated to NOC Manager and Firewall Administrator. Survey of all other web sites begun. System B compromise identified by 0845
0845 NOC directed to perform a full back up of the System A and System B servers
0900 Backups initiated
0920 Backups completed
0940 Report of incident made to NIPC
1055 System A and System B temporary web page " Site Under Construction For Routine Maintenance " installed. Distributed logs and system information to virtual incident team
1100 Notified the clients of the current status
1117 NOC manager issued memo to staff regarding confidentiality
1245 Incident response team teleconference / meeting to review situation and determine next steps
1250 Implemented expanded firewall security measures, began rebuild of System A ands System B servers

System A's web server and System B's Database / application server were rebuilt by reloading and patching the operating systems, then recovering clean backups. The procedures for installing and configuring servers as well as the procedures for maintaining operational servers was also changed to make it easier (procedurally) to load vendor (specifically Microsoft) patches that correct vulnerabilities. Changes to the system loading and configuration procedures were made to ensure that the systems were properly patched. IIS was configured to "run in separate memory space". The patchwork.exe utility was run on the rebuilt System A and System B servers to verify that they ere no longer vulnerable to the Unicode exploit. The patchwork tool was also run on all other servers in the NOC data center to ensure that all servers were properly patched.

The NOC made several additional changes to improve the defenses against this type of attack. System B's database server had a very loose rule set that allowed FTP, HTTP, and HTTPS connections from "any" server. This rule set was tightened to allow only HTTPS from a designated server to connect to it via the Internet and for System B's application server to make ODBC calls from behind the firewall. All hosted systems' firewall rule sets were reviewed and changed to minimize the number of servers that permitted connections from "any". Outbound connections from the hosted servers were also severely restricted and an emphasis was placed on logging and alerting to attempts to connect from inside the firewall. Passwords for all hosted systems, routers and devices were changed as a precaution in light of the incident and as a routine procedure in light of the RIF in progress.



© SANS Institute 2000 - 2005 Author retains full rights.

The NOC further purchased licenses for ISS Scanner and began a program to regularly scan all NOC server assets for vulnerabilities. This program was established to identify vulnerabilities before they can be exploited. Once built a server is scanned by ISS is now used to verify that the known vulnerabilities have been removed (from a network perspective) and scans are performed at least weekly to ensure that no servers "fall through the cracks" and are patched.

Follow Up

On Tuesday, an alert from CERT[8] for the sadmind / IIS Worm was published. The IIS component of the signature of the sadmind /IIS worm matched the logs and defacement of the NOC servers exactly. In addition, other the logs for other IIS servers run by The Company's other divisions were picking up attempts to exploit the Unicode vulnerability in a similar fashion. The sadmind / IIS worm exploits vulnerabilities in both Sun Solaris and Windows IIS. The worm exploits a buffer overflow vulnerability in Solaris' remote administration Solstice sadmind. This is a known vulnerability for which Sun released a patch in 1999[9]. The sadmind listens on port 111. Once a vulnerable sun host is located, a payload is deposited. The payload has a component to scan for additional Sun hosts that are vulnerable to the sadmind vulnerability and code to scan for IIS servers that are vulnerable to

The Sun vulnerability added an additional component to the incident. Until this time, only IIS hosts had been seriously looked at. NOC systems administrators reviewed the configuration and logs of all of the Sun hosts in the NOC data center to determine if one of the Solaris machines had been compromised. None of the servers ran the Solstice suite nor had the sadmind daemon running; it was determined that no Solaris machines had been compromised by the Sun component.

A summary report in the format of an email was written to highlight the cost in man hours. Overall, 20 people had spent 4 – 12 hours each in the process of handling this incident. Two client systems were unavailable for 8 working hours and 14 non-working hours. The total cost was estimated to be 186 man-hours (close to $4000) in lost productivity and delays in other project work. It may not have been necessary to expend the resources to completely rebuild the servers given the mild damage caused by the sadmind / IIS worm; however, at the time the details of sadmind / IIS were not known and a conservative recovery was made. To avoid future expenditures in this area, The Company directed its NOC management to investigate tools for baselining systems (such as Axent ESM or Tripwire) so that in the future, a more precise picture of the damage done by a defacement can be done. The backups of System A and System B will be retained for the length of the contract with clients A and B in case they are needed in the future.

The Company's Information Security Engineer made additional warnings to Server Managers and project technical support staff. Despite this, the sadmind / IIS worm eventually infected 20% of The Company's Internet connected IIS servers over the course of the next three days, including a server used for remote email access via Outlook Web Access (OWA). The initial incident identified that in some cases, IIS servers for client systems were not being patched as actively as they should have been; the follow on incidents identified a company wide problem



© SANS Institute 2000 - 2005 Author retains full rights.

that resulted in revised guidance for all Internet facing servers. The Company extended it regular use of IIS Scanner for all Internet facing servers to reduce the possibility that a known exploit could be used against them.

© SANS Institute 2000 - 2005, Author retains full rights.



© SANS Institute 2000 - 2005 Author retains full rights.

Appendix A. Figures

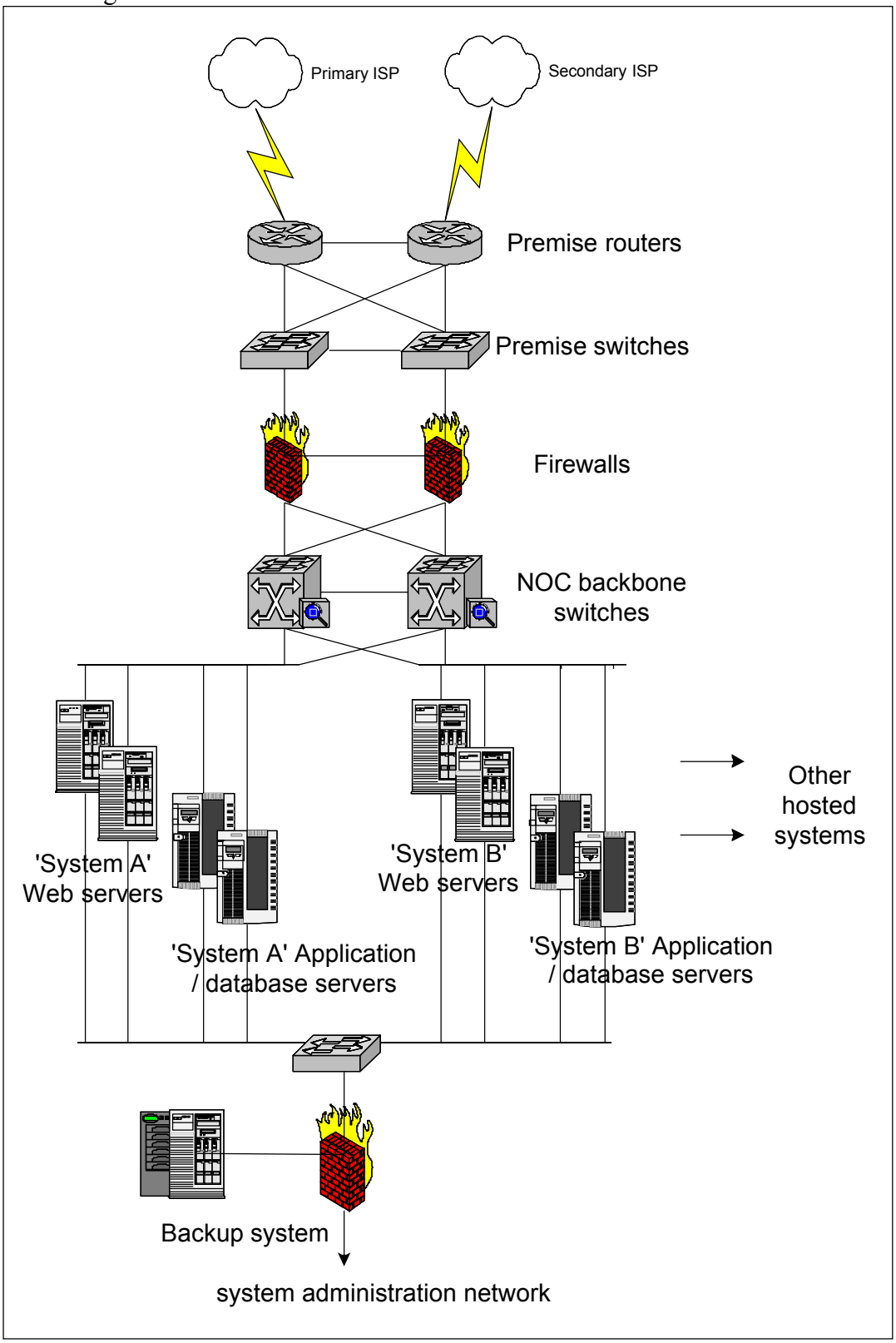
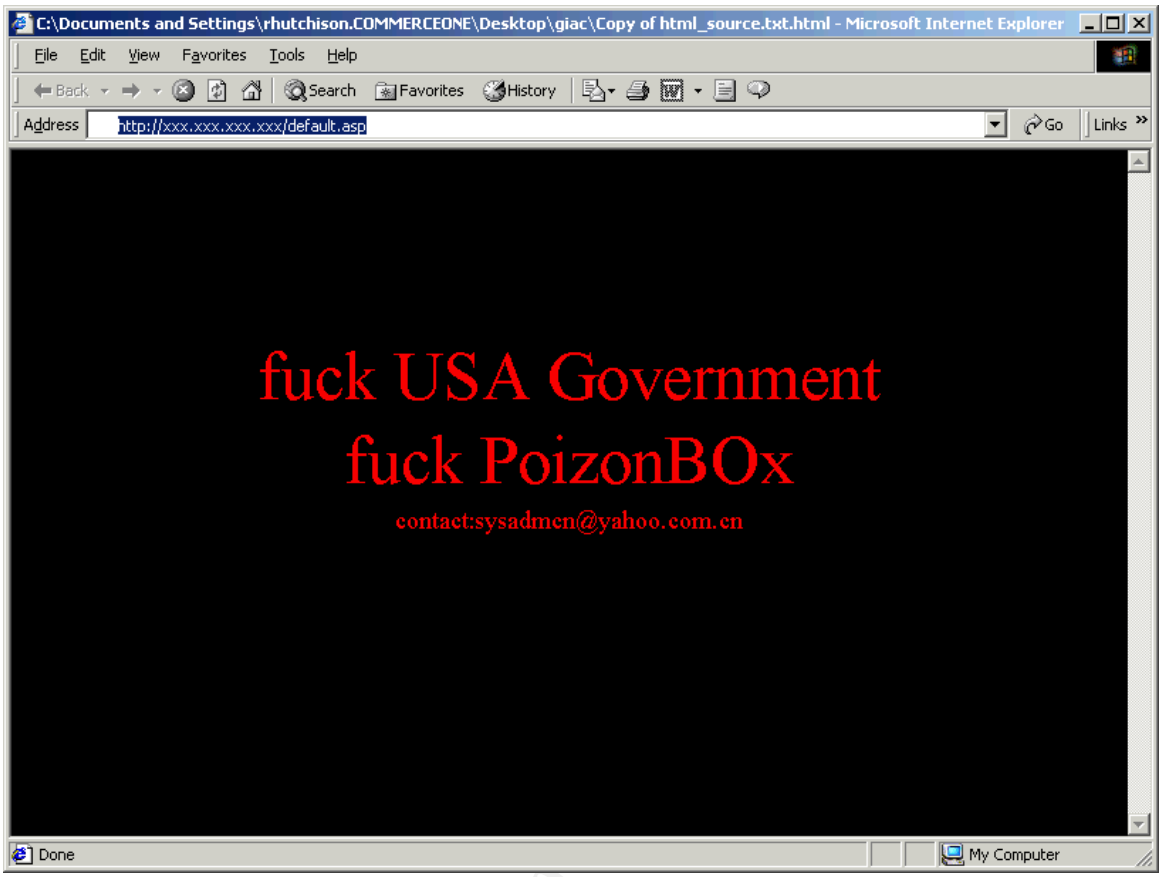



Figure 1. General NOC hosting environment.



© SANS Institute 2000 - 2005 Author retains full rights.




© SANS Institute 2000



© SANS Institute 2000 - 2005 Author retains full rights.

Appendix B. Detailed Excerpts from IIS server logs

System B:
#Software: Microsoft Internet Information Server 4.0
#Version: 1.0
#Date: 2001-05-06 07:57:27
#Fields: time c-ip cs-method cs-uri-stem sc-status
07:57:27 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 200
07:57:27 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 200
07:57:29 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:57:30 source.attack.domain GET /scripts/root.exe 502
07:57:30 source.attack.domain GET /scripts/root.exe 502
07:57:31 source.attack.domain GET /scripts/root.exe 502
07:57:31 source.attack.domain GET /scripts/root.exe 502
07:57:33 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:57:33 source.attack.domain GET /scripts/root.exe 502
07:57:35 source.attack.domain GET /scripts/root.exe 502
07:57:35 source.attack.domain GET /scripts/root.exe 502
07:57:37 source.attack.domain GET /scripts/root.exe 502
07:57:41 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:57:42 source.attack.domain GET /scripts/root.exe 502
07:57:42 source.attack.domain GET /scripts/root.exe 502
07:57:44 source.attack.domain GET /scripts/root.exe 502
07:57:48 source.attack.domain GET /scripts/root.exe 502
07:57:48 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:57:50 source.attack.domain GET /scripts/root.exe 502
07:57:50 source.attack.domain GET /scripts/root.exe 502
07:57:52 source.attack.domain GET /scripts/root.exe 502
07:57:52 source.attack.domain GET /scripts/root.exe 502
07:57:53 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:57:54 source.attack.domain GET /scripts/root.exe 502
07:57:54 source.attack.domain GET /scripts/root.exe 502
07:57:56 source.attack.domain GET /scripts/root.exe 502
07:57:56 source.attack.domain GET /scripts/root.exe 502
07:57:58 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:57:59 source.attack.domain GET /scripts/root.exe 502
07:57:59 source.attack.domain GET /scripts/root.exe 502
07:58:01 source.attack.domain GET /scripts/root.exe 502
07:58:01 source.attack.domain GET /scripts/root.exe 502
07:58:02 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:58:04 source.attack.domain GET /scripts/root.exe 502
07:58:04 source.attack.domain GET /scripts/root.exe 502
07:58:05 source.attack.domain GET /scripts/root.exe 502
07:58:05 source.attack.domain GET /scripts/root.exe 502
07:58:07 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502



© SANS Institute 2000 - 2005 Author retains full rights.

07:58:08 source.attack.domain GET /scripts/root.exe 502
07:58:08 source.attack.domain GET /scripts/root.exe 502
07:58:10 source.attack.domain GET /scripts/root.exe 502
07:58:10 source.attack.domain GET /scripts/root.exe 502
07:58:12 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:58:13 source.attack.domain GET /scripts/root.exe 502
07:58:13 source.attack.domain GET /scripts/root.exe 502
07:58:15 source.attack.domain GET /scripts/root.exe 502
07:58:15 source.attack.domain GET /scripts/root.exe 502
07:58:16 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 200
07:58:16 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:58:18 source.attack.domain GET /scripts/root.exe 502
07:58:18 source.attack.domain GET /scripts/root.exe 502
07:58:20 source.attack.domain GET /scripts/root.exe 502
07:58:20 source.attack.domain GET /scripts/root.exe 502
07:58:22 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:58:23 source.attack.domain GET /scripts/root.exe 502
07:58:23 source.attack.domain GET /scripts/root.exe 502
07:58:24 source.attack.domain GET /scripts/root.exe 502
07:58:24 source.attack.domain GET /scripts/root.exe 502
07:58:26 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:58:30 source.attack.domain GET /scripts/root.exe 502
07:58:30 source.attack.domain GET /scripts/root.exe 502
07:58:32 source.attack.domain GET /scripts/root.exe 502
07:58:32 source.attack.domain GET /scripts/root.exe 502
07:58:34 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:58:35 source.attack.domain GET /scripts/root.exe 502
07:58:35 source.attack.domain GET /scripts/root.exe 502
07:58:37 source.attack.domain GET /scripts/root.exe 502
07:58:37 source.attack.domain GET /scripts/root.exe 502
07:58:39 source.attack.domain GET /scripts/../../winnt/system32/cmd.exe 502
07:58:40 source.attack.domain GET /scripts/root.exe 502
07:58:40 source.attack.domain GET /scripts/root.exe 502
07:58:41 source.attack.domain GET /scripts/root.exe 502
07:58:41 source.attack.domain GET /scripts/root.exe 502
07:58:44 source.attack.domain GET /Default.htm 200

---

Endnotes / References.


[0] http://www.sans.org/newlook/digests/nbarchive.html
[1] http://www.microsoft.com/technet/security/bulletin/MS00-078.asp
[2] http://www.nipc.gov/warnings/advisories/2001/01-003.htm
[3] http://www.cisecurity.org/patchwork.html
[4] Scarborough, Matt, "BackGate Kit Analysis and Defense", http://www.sans.org/y2k/unicode.htm, March 28, 2001




© SANS Institute 2000 - 2005 Author retains full rights.

[5] Ibid.
[6] Bugtrac ID 1806, http://www.securityfocus.com/bid/1806, October 17, 2000
[7] Scarborough, Matt, "BackGate Kit Analysis and Defense", http://www.sans.org/y2k/unicode.htm, March 28, 2001
[8] http://www.cert.org/advisories/CA-2001-11.html
[9] http://www.cert.org/advisories/CA-1999-16.html

© SANS Institute 2000 - 2005, Author retains full rights.



© SANS Institute 2000 - 2005 Author retains full rights.