



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 permitted 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>

SANS GIAC PRACTICAL

FOR CERTIFIED ADVANCED INCIDENT HANDLING (GCIH) CERTIFICATION V 2.1

OPTION 1- EXPLOIT(S) IN ACTION

Hosting Controller Exploit Brings Trouble @ Home

By Brian M. Slater

© SANS Institute 2000-2002, Author retains full rights.

EXECUTIVE SUMMARY.....	3
THE EXPLOIT	4
PROTOCOLS/SERVICES.....	6
HTTP.....	6
TCP.....	6
ASP.....	6
IIS.....	7
THE ATTACK.....	7
NETWORK ARCHITECTURE	7
Open Ports	8
HOW TO USE IT	9
DIAGRAM OF THE ATTACK	11
Initial Attack.....	11
Attack after protection.....	12
Signature of the attack.....	13
Web Server Logs.....	13
Packet Captures.....	13
Intrusion Detection System (IDS)	14
PROTECTION	14
Disabled Parent Paths (Q184717 / Q226474).....	14
Programming Level.....	16
THE INCIDENT HANDLING PROCESS.....	17
PHASE 1 -PREPARATION	17
Policies and Procedures	17
Incident Handling Equipment and Software	17
Intrusion Detection System (IDS)	18
Webserver Logging.....	18
Sygate Logging.....	18
PHASE 2 -IDENTIFICATION	18
PHASE 3 -CONTAINMENT.....	20
Commands Used.....	21
Tracking modifications to the system.....	22
PHASE 4 -ERADICATION	29
Disabled Parent Paths (Q184717 / Q226474).....	29
No website directories on the system partition.....	30
Removing Administrative Tools.....	30
Network	30
PHASE 5 -RECOVERY.....	33
PHASE 6 -FOLLOW UP/LESSONS LEARNED.....	35
LESSONS LEARNED	36
The Forgotten Policy.....	37
Check List Needed.....	37
REFERENCES.....	38
APPENDIX A	39
APPENDIX B	44
APPENDIX C	45
APPENDIX D	47
APPENDIX E	48
APPENDIX F	49

Executive Summary

In January 2002, I was evaluating Hosting Controller, an automated web hosting tool that claimed to make web hosting much more efficient and profitable. The tool seemed to do just as it claimed, making web hosting and site creation in Internet Information Server much easier to perform and maintain.

During the evaluation, I searched the internet for listings of known exploits for Hosting Controller. Unfortunately in minutes, several exploits were found from various security and hacking sites on the Internet. I went back to Hosting Controller's corporate website to check if the exploits were addressed and if there were any patches or solutions, but none were listed and the exploits were not even mentioned.

I decided to start testing the validity of the exploits and possible solutions. A testing environment was established. A Windows 2000 test server was setup with all the latest patches and Hosting Controller installed with the default installation. A network-based Intrusion Detection System (IDS) was installed on the server to monitor the activity of the exploits and to learn more about them.

All of the posted exploits worked as described in the internet postings. There were two major problems. One, the ASP code did not check if the user was already authenticated after the initial logon page. Two, the ASP code allowed transversal of directories and with full permissions.

A slight modification of the code on all of the ASP pages to incorporate an `#include` statement and disabling parent paths prevented both exploits from functioning. Additional measures were taken to strengthen the firewall and to perform routine vulnerability assessments.

A new rule was added to the IDS to detect new attempts using the transversal exploit. In addition, tools, such as Analysis Console for Intrusion Detection (ACID) for easier analysis of the IDS data and Nessus for vulnerability assessments were added to assist in future incident detection.

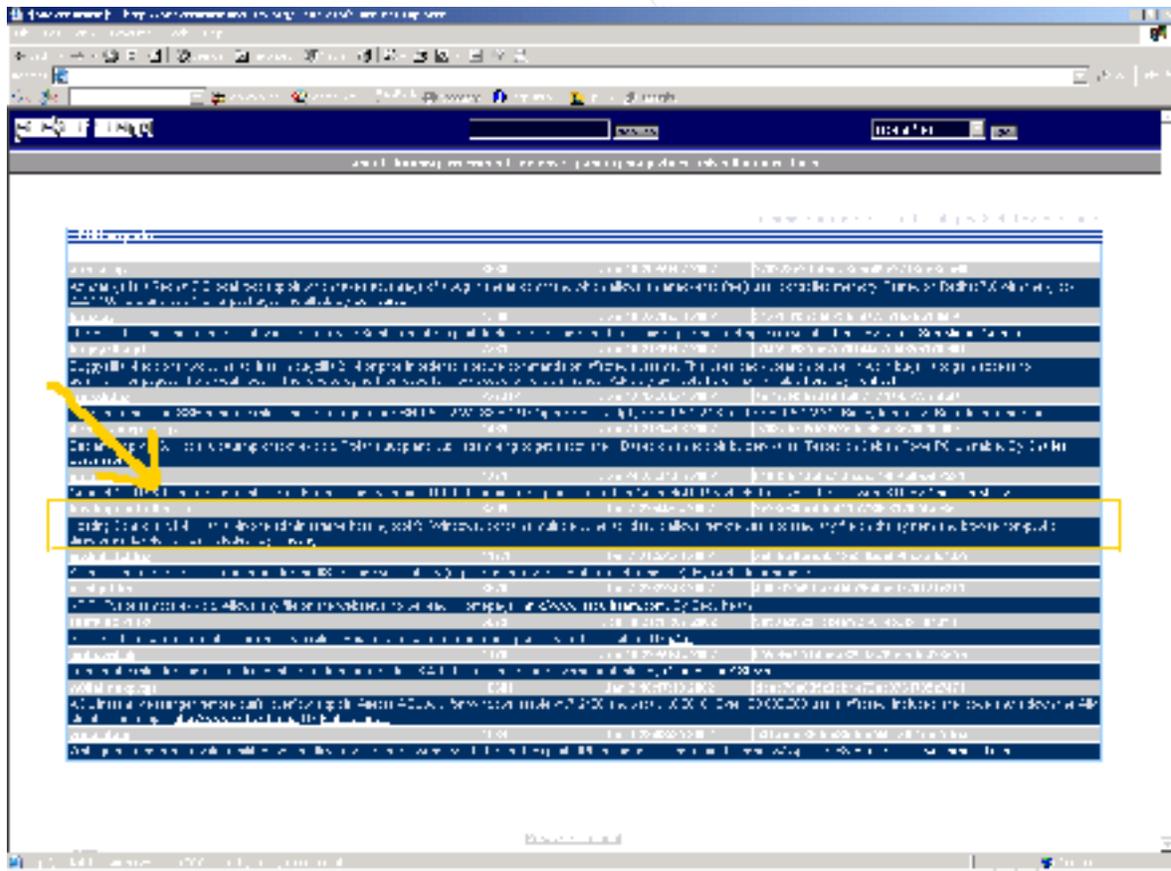
The Exploit

I was evaluating a software package called Hosting Controller. The company's web site made this statement:

Hosting Controller is an add-on to your Windows based hosting server. It automates all hosting tasks and give full control of each website into hands of respective owners without compromising any security. In addition to Microsoft products, the latest version supports most third party products that are commonly used by hosting providers as a standard.¹

The product claimed it did not compromise security, so I decided to install the software on a test server. The test server was not on an isolated network and had an Internet connection.

One of the best ways to see if a program has known exploits is just to search Google for the software title. The search results provided several hits. On the top of the list of the results was a hit for packetstormsecurity.org. This is a good indication that there is a published exploit. The exploit documented showed that Hosting Controller is susceptible to transversal attacks and other exploits.



¹ <http://www.hostingcontroller.com>

The Hosting Controller Exploit affects Windows 2000/NT with Internet Information Servers (IIS) 5.0/4.0 (see Appendix A for all operating systems and versions affected). Hosting Controller is written in Active Server Pages (ASP) with the options of using MS SQL 2000/7, Access, or even Excel to store the data. It also features integration with:

- **FTP Servers:** MS FTP Server, Serv-U FTP Daemon
- **Mail Servers:** IMail Mail Server, Merak Mail Server, VOPMail Mail Server, MailMax, Mail Server, Post.Office
- **DNS Servers:** Microsoft DNS, Bind DNS Server (Bind 4x and 8x), Simple DNS Plus
- **Statistics Servers:** MediaHouse LiveStats Statistics Server, Web Trends Enterprise, Reporting Server, Webtrends Enterprise Suite, WebAlizer Statistics Server¹

The original posting at <http://packetstormsecurity.nl/0201-exploits/hosting.controller.txt> of the Hosting Controller Exploit is summarized below. Hosting Controller has several exploits that one could take advantage of while using Port 80 and built-in ASP files:

1. Dot Dot Slash attack using filemanager.asp – allows attacker to transverse directories.
2. Autosignup/dsp_newhc.asp - allows an attacker to create a new domain name and a new account without logging in as administrator.
3. Poorly written ASP login pages exist that enable anyone to confirm the validity of usernames and crack the password of known users via the brute force method.
4. Browsing Non-public Directories Allowed – allows attackers to browse any file and any directory without authentication.

Hosting Controller is attempting to rewrite the ASP login page to limit the logon attempts in an effort to reduce brute force attacks, but there aren't any application updates/patches to fix browsing non-public directories, auto-signup, or the Dot Dot Slash problem (to date) at the company's web site.

The exploits were posted in news groups and on websites such as:

- Browsing non-public directories, auto-signup, or the Dot Dot Slash Vulnerability
 - <http://packetstormsecurity.nl/0201-exploits/hosting.controller.txt>.
 - <http://groups.google.com/groups?selm=bugtraq/20020105150649.17382.qmail%40web13407.mail.yahoo.com&output=gplain>
 - http://www.iss.net/security_center/static/7823.php
- Login Vulnerability
 - <http://securityfocus.com/archive/1/252645>

¹ <http://www.hostingcontroller.com>

Protocols/Services

HTTP

Short for HyperText Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the commands that came before it. This is the main reason that it is difficult to implement Web sites that react intelligently to user input. This shortcoming of HTTP is being addressed in a number of new technologies, including ActiveX, Java, JavaScript and cookies.

<http://www.webopedia.com/TERM/h/http.html>

TCP

Transmission Control Protocol (TCP) The most common transport layer protocol used on Ethernet and the Internet. It was developed by DARPA.

TCP is built on top of Internet Protocol (IP) and is nearly always seen in the combination TCP/IP (TCP over IP). It adds reliable communication, flow-control, multiplexing and connection-oriented communication. It provides full-duplex, process-to-process connections.

Defined in STD 7, RFC 793. It is connection-oriented and stream-oriented, as opposed to User Datagram Protocol

http://www.webopedia.com/TERM/T/TCP_IP.html

ASP

“Active Server Pages (ASP) is a technology that allows for the programmatic construction of HTML pages just before they are delivered to the browser. ASP is not a language (in the sense that Pascal and C++ are languages) – although it does make use of existing scripting languages such as VBScript or JavaScript. It’s not really an application (in the sense that FrontPage and Word are applications) either. Instead we describe ASP using a rather more ambiguous term, technology. ASP is a technology for building dynamic and interactive web pages.”¹

¹ Beginning Active Server Pages 3.0 David Buser, et.all, Wrox Pred Ltd, Feb 2002.

IIS

Short for *Internet Information Server*, Microsoft's Web server that runs on Windows NT platforms. In fact, IIS comes bundled with Windows NT 4.0. Because IIS is tightly integrated with the operating system, it is relatively easy to administer. However, currently IIS is available only for the Windows NT platform, whereas Netscape's Web servers run on all major platforms, including Windows NT, OS/2 and UNIX.

<http://www.webopedia.com/TERM/I/IIS.html>

CERTs

There were no matching CERTs for this exploit, but it was referenced in the Security Focus Bugtraq database (see appendix A).

BugTraq-3808

<http://online.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3808>

BugTraq-3971

<http://online.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3971>

BugTraq-3811

<http://online.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3811>

Variants of Exploit

None known.

The Attack

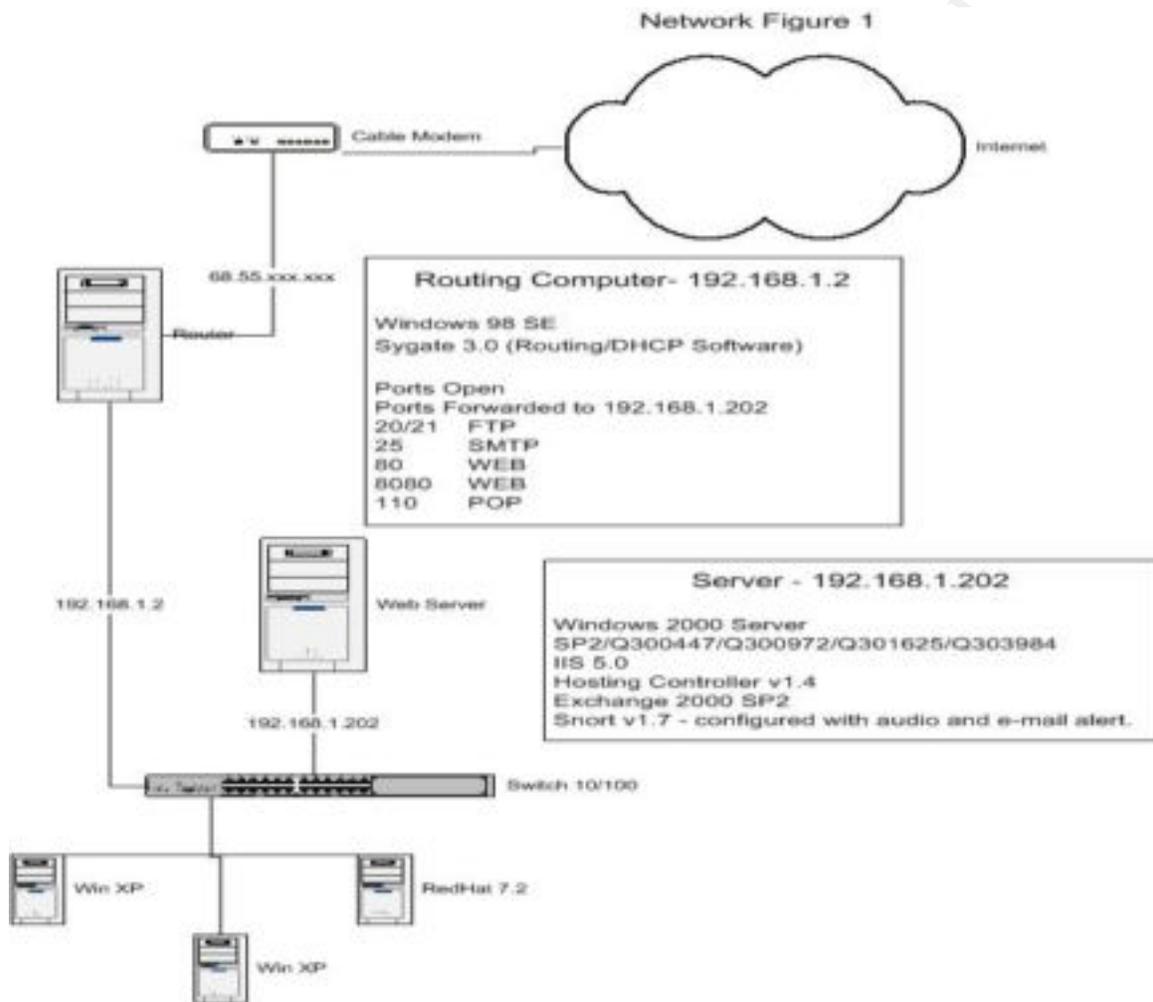
Network Architecture

The testing network consists of 5 computers. The configuration is as follows:

- Windows 2000 Server SP2 w/Q300447/Q300972/Q301625/Q303984
 - IIS 5.0
 - Exchange 2000 SP2
 - Hosting Controller v1.4
 - IDS (Snort) v1.7 – configured with audio and e-mail alert.
- Windows XP Professional – receives e-mail alerts.
- Windows XP Professional
- RedHat Linux v7.2
- Windows 98 SE (router)
 - Sygate v3.0
 - Sygate was configured to forward any requests for ports 20, 21, 25, 80, 110 to the internal Windows 2000 computer running those services.

The network shares a cable modem connection, one IP address, and uses NAT for the internal computers.

The protocols used are TCP/IP and IPX- with TCP/IP as the primary protocol used and IPX required for some of the multi-player entertainment software installed on a few of the workstation computers. For a diagram of the initial layout of the network, refer to the Network Diagram, Figure 1.



Open Ports

The open ports on the Hosting controlling server are:

20 UDP	File Transfer Protocol (FTP)
21 TCP	File Transfer Protocol (FTP)
25 TCP	Simple Mail Transfer Protocol (SMTP)
80 TCP	Hypertext Transfer Protocol (HTTP)
8080 TCP	Hypertext Transfer Protocol (HTTP)
110 TCP	Post Office Protocol (POP)



Clicking on the Hosting Controller's Directories option on the left menu will inform the attacker the File Manager page (filemanager.asp) is what allows web site owners to manage files within the web server directory of \\webpace\resadmin\newaccount\newaccount.com. The filemanager.asp of Hosting Controller is vulnerable to the "Dot Dot slash" bug (../..), which allows the directories to be transversed with a script URL. All transversal attacks use the ".." notation with executable code to "walk up" and "walk down" the directory hierarchy.

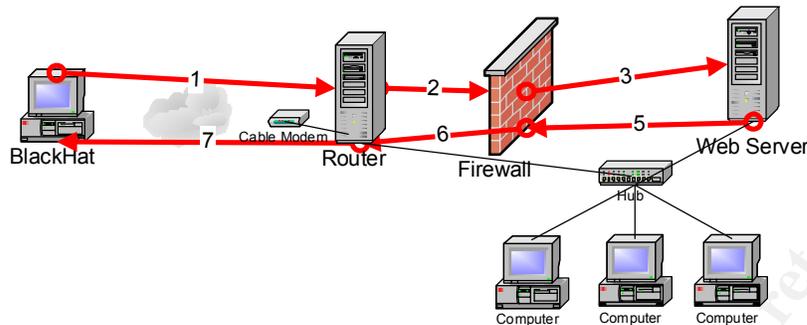
<http://www.eq.com/hc/folders/filemanager.asp&siteindex=testing&sitename=testing.com&OpenPath=C:\webpace\resadmin\testing\testing.com\www\..\..\..\..\>

Using the URL above, the attacker is able to read, delete, rename and upload files anywhere on the hosting server since they are logged in as an administrator (originally only to the site), which the rights are carried with them as they transverse directories. From here the attacker could upload any tools, backdoor, or trojans.

To be less obvious and stealthy, a technique that the attacker could use would be to legitimately set up a website with the hosting company. Then perform the transversal. This way the attacker would not attract any unwanted attention with the unauthorized creation of websites.

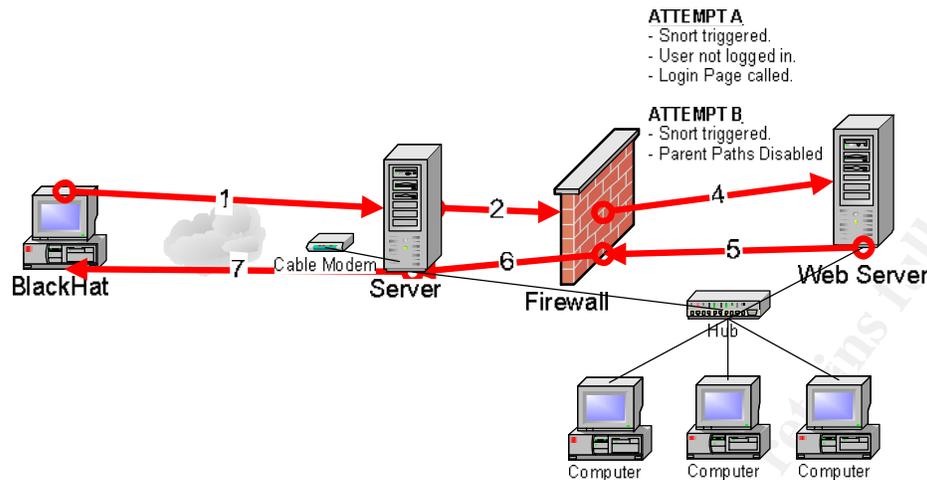
Diagram of the Attack

Initial Attack



- 1) Blackhat system requests dsp_newwebadmin.asp on port 80 to the external IP address.
- 2) Router logs the request and passes the request through the Firewall to the internal IP of the web server.
- 3) The firewall logs the request and lets the request through because port 80 is allowed.
- 4) The web server logs the request. Snort does not log anything since there are no rule matches made. The page allows anonymous access.
- 5) Web server replies to the request and sends through the Firewall.
- 6) Firewall allows the outgoing request.
- 7) Page is sent back to Blackhat.
- 8) Dsp_newwebadmin.asp displays in browser on Blackhat.
- 9) New site information, username, and password are created using dsp_newwebadmin.asp. The same basic flow of 1-8 is used. This information is sent back to the web server and appropriate directories and IIS site creation is processed.
- 10) Blackhat uses new account to log into the new site. Currently, Blackhat only has admin rights to the site.
- 11) The same basic flow of 1-8 is used and Blackhat uses filemanger.asp with the ".." bug to transverse directories and retains admin status in all transversed directories.
- 12) Anything can be done at this point. Files and information can be read. If the Blackhat wants, that person can FTP additional tools to the server. Port 21 is allowed through the firewall. Using the allowed ports and ASP pages, the attacker can successfully compromise the server.

Attack after protection



Attempt A -dsp_newwebadmin.asp

- 1) Blackhat system requests dsp_newwebadmin.asp on port 80 to the external IP address.
- 2) Router logs the request and passes the request through the Firewall to the internal IP of the web server.
- 3) The firewall logs the request and lets the request through because port 80 is allowed.
- 4) The web server logs the request. Snort is triggered with the dsp_newwebadmin.asp rule. Alert is sent to admin. The page does not allow anonymous access and calls the Login Page.
- 5) Web server replies to the request and sends through the Firewall.
- 6) Firewall allows the outgoing request.
- 7) Login Page is sent back to Blackhat.
- 8) Login Page displays in browser on Blackhat.-
- 9) Unsuccessful Attempt.

Attempt B – filemanager.asp “..” transversal attack

- 1) Blackhat gets valid username/password for a site. Logs into website. Gets Management page.
- 2) Uses filemanager.asp with “..” bug to transverse directories.
- 3) Router logs the request and passes the request through the Firewall to the internal IP of the web server.
- 4) The firewall logs the request and lets the request through because port 8080 is allowed.
- 5) The web server logs the request. Snort is triggered with the filemanager.asp rule. Alert is sent to admin. The page cannot be displayed because PARENT PATHS are disabled.
- 6) Web server replies to the request and sends through the Firewall.
- 7) Firewall allows the outgoing request.
- 8) The Page Cannot Be Displayed indicating that “..” cannot be used page is displayed in browser on Blackhat.

Signature of the attack

Attack signatures watch for common transmission related to applications like web and FTP; they look for patterns and identify what applications or type of traffic the pattern matches.

Web Server Logs

The web server logs will show the signature below during the GET command. The log shows a transversal of the directories took place as the `\..\` grows one more in length to go up one more level and that fact that so many `\..\` are in a row.

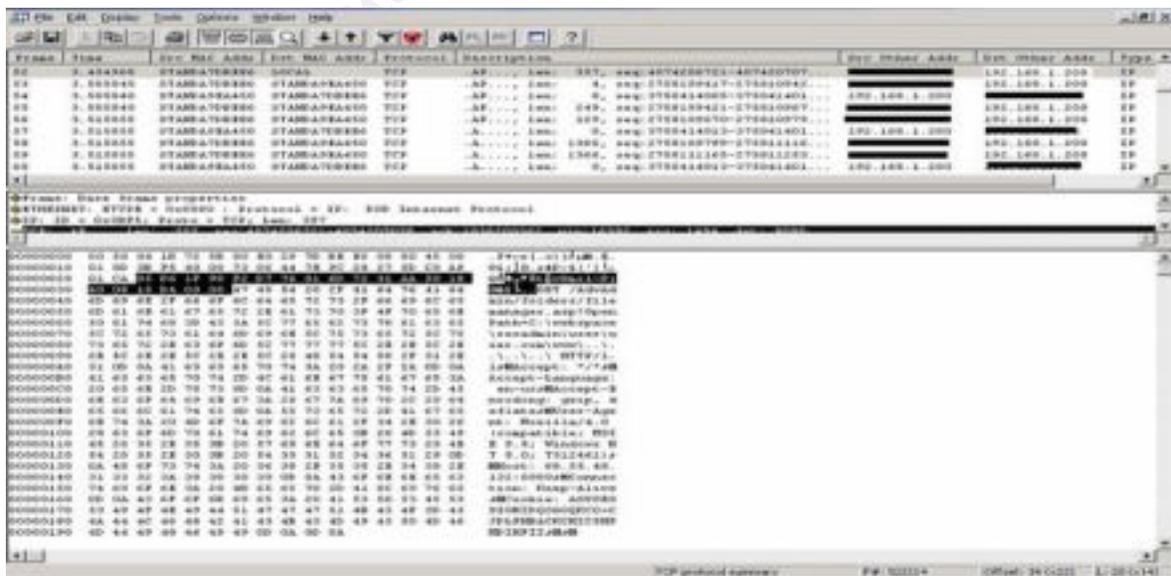
```
2002-01-30 23:39:34 192.168.1.200 - W3SVC1 THESERVER 192.168.1.202 80 GET
/advadmin/images/ren.gif - 304 0 140 527 0 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461)
ASPSESSIONIDGGGQQKBO=CBGNPAJDDGHKDIOGOONKCJLI
http://192.168.1.202/advadmin/folders/filemanager.asp?siteindex=hacked.com&sitename=hacked.com&OpenPath=C:\webpace\resadmin\hacker\hacked.com\www
```

```
2002-01-30 23:40:02 192.168.1.200 - W3SVC1 THESERVER 192.168.1.202 80 GET
/advadmin/folders/filemanager.asp
siteindex=hacked.com&sitename=hacked.com&OpenPath=C:\webpace\resadmin\hacker\hacked.com\
www\..\..\..\..\ 200 0 0 559 10756 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461)
ASPSESSIONIDGGGQQKBO=CBGNPAJDDGHKDIOGOONKCJLI -
```

```
2002-01-30 23:40:58 192.168.1.200 - W3SVC1 THESERVER 192.168.1.202 80 GET
/advadmin/folders/filemanager.asp
siteindex=hacked.com&sitename=hacked.com&OpenPath=C:\webpace\resadmin\hacker\hacked.com\
www\..\..\..\..\..\ 200 0 0 562 44794 HTTP/1.1
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+Q312461)
ASPSESSIONIDGGGQQKBO=CBGNPAJDDGHKDIOGOONKCJLI -
```

Packet Captures

This packet capture is identical to the web server logs showing the attack. It shows the exact same content as the web servers logs do.



Intrusion Detection System (IDS)

Since the attack is very easy to spot in both the web server logs and in packet captures, it was easy to create a rule for SNORT to identify this attack.

SNORT Rule

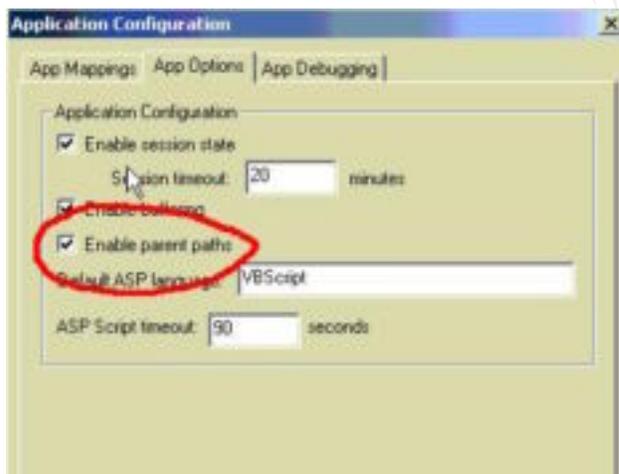
```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 8080 (msg:"Hosting Exploit Transversal Attack"; uricontent:"/filemanager.asp"; content:"\..\");
```

With this rule in place, the IDS was set to alert the administrator by e-mail and audio alert. Once the administrator receives this alert, the web server and other logs could be examined closer to determine if it should be considered an incident.

Protection

Disabled Parent Paths (Q184717 / Q226474)

All transversal attacks use the “..” notation with executable code to “walk up” and “walk down” the directory hierarchy. Disabling the parent path feature is the best countermeasure I found for transversal attacks.

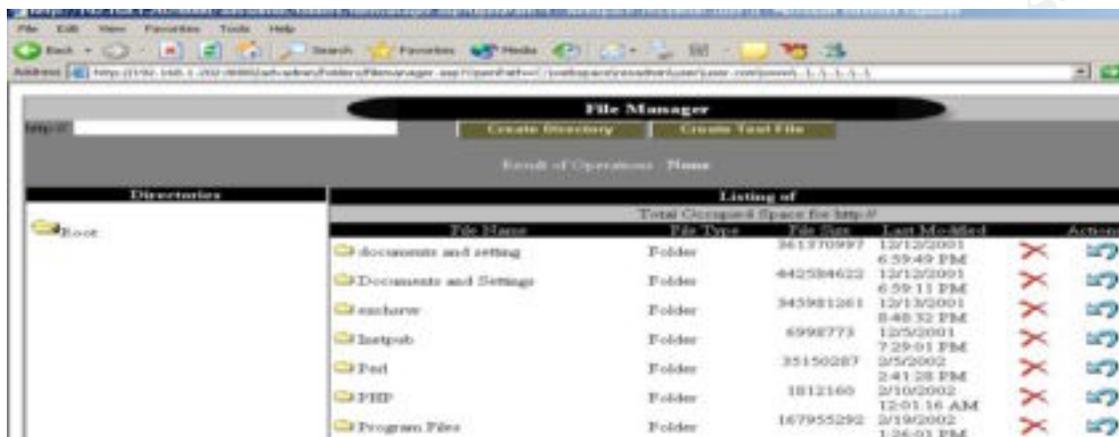


Disabling the parent paths will not affect relative path usage in ASP or HTML. Any relative path to static content will still work. For example ``, a relative path to the images directory will still work.

Disabling parent paths will however break `#include` file statements that are relative. There is a work-a-round for this which is easy to implement. Just move all of your include files into a separate virtual directory and make the change in the include line as follows:

```
<!-- #include file=\"..\file.inc\"--> to <!-- #include virtual=\"/inc/file.inc\"-->
```

Disabling parent paths is the solution for the transversal attack. Before the parent paths were disabled, the transversal attack was successful shown in this snapshot.



After disabling the parent paths on the web server, the first attempt was still successful. The website service was restarted, but the attack was still successful. It wasn't until I rebooted the server, did it give the results I had expected shown in the next screenshot.



The screen shot above shows that disabling parent paths will stop the transversal ability.

Programming Level

All programming languages are susceptible to security holes. Vulnerabilities exist when extensive testing is not performed on each piece of code.

Logon Page

The logon page, Default.asp, is too informative that the user name or password is incorrect. The ASP page response should just be changed to a generic response. For example:

The information entered is not correct. Please check to make sure the information you have entered is correct.

This will help prevent giving out valid user names to use in brute force attacks.

Other pages not checking for logon

The two specific files that do not check if the user is authenticated are:

- Dsp_newwebadmin.asp
By default, this file does not look for authentication from the login script, nor do any of the following files that it calls on. The original code will allow any name to be added for access as long as it is not a duplicate.
- Filemanager.asp
By default, this file does not check for sessions and permissions. If no modifications are made, the command below will work if the upper level directions have proper permissions. The URL is a set of name value pairs in GET format that can be modified to execute additional commands it was not intended to execute from the URL string. If the form only accepts POST, modifications to a client-side copy of the form must be made and submitted from the client.

<http://www.eq.com/hc/folders/filemanager.asp&siteindex=testing&sitename=testing.com&OpenPath=C:\webpace\resadmin\testing\testing.com\www\..\..\..\>

I searched through all the code of the program for how it authenticates and checks permissions. The program has the capability to check if the user is logged in and has the correct permissions, but it is not implemented throughout all the active server pages.

The Default.asp presents a login page and uses Check_Password.asp to verify for a valid username and password. From there it uses an include file under /common/inc_func.asp and to check what group the user belongs to. The check logged in function should be added with an include on each page.

```
<!--#include FILE="common/inc_funcs.asp"-->
```

The Incident Handling Process

PHASE 1 -Preparation

Preparation is the key to effectively avoiding most incidents. Unfortunately, preparation won't stop every incident, but it will go a long way to help minimize damage or even disastrous mistakes on the incident handler's part. There are many aspects of preparation, including policy, communication structure, involvement of appropriate parties, and required supplies – to name a few. The most critical are policy, communication, and appropriate parties. Although having the right supplies and other preparation is necessary, without structured rules, good communication, and people to handle the incident, the other measures are not effective.

Policies and Procedures

The organization is small in people and resources. Since the size of the operation is cannot lend itself to having a dedicated incident handling team, one person has been designated as the incident handler. Having a one person incident handling team is far from optimum, but it is all that can be allocated and afforded. This also does not allow for a chain of custody.

- Designate one person to be the primary incident handler due to the lack of personnel and resources. When more personnel become available, allocate a second in command.
- Create a CD with administrative tools on it. To be used as a trusted source for running programs.
- All modifications to servers are to be logged electronically and hard copy.
- Establish what and what is not to be monitored.
- All testing will be perform on a test network and machine.
- Incident Handling equipment and evidence gathered will be stored securely while not in use

In a larger operation it would be imperative to keep management up-to-date on security issues, especially when there are no incidents. If an organization feels too safe, they may start to get the false impression that their systems are secure and security professionals are no longer required. If an organization feels secure, it is typically due to security professionals working hard on prevention rather than crisis recovery.

Incident Handling Equipment and Software

A laptop was set aside to be dedicated for incident handling. This system used Vmware to accommodate multiple operating systems (See Appendix B)

Intrusion Detection System (IDS)

I needed something to detect attacks to my system. I decided that a network-based IDS would be sufficient to start with. I installed SNORT (<http://www.snort.org>) on the server to monitor its communications.

Webserver Logging

Webserver logging was turned on for all existing sites. The logs were configured for hourly creation.

Sygate Logging

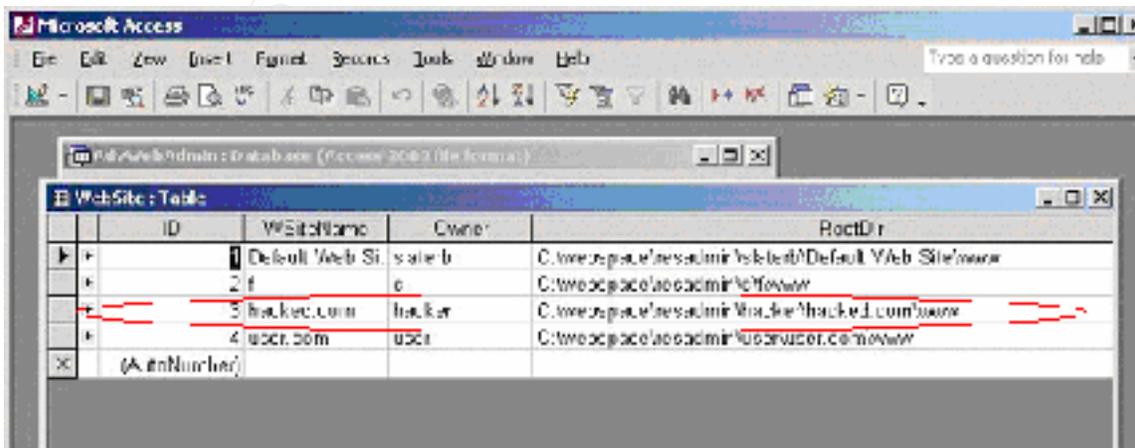
The Sygate software for internet connection sharing was set to log all activity. There was over four gigabytes free on the hard drive to accommodate any size log files.

PHASE 2 -Identification

During a weekly routine manual checkup on the database, new records were found in the database. The records should not have existed. This was classified as an incident when it was confirmed that a new unauthorized website was created. The new website information showed up in several places.

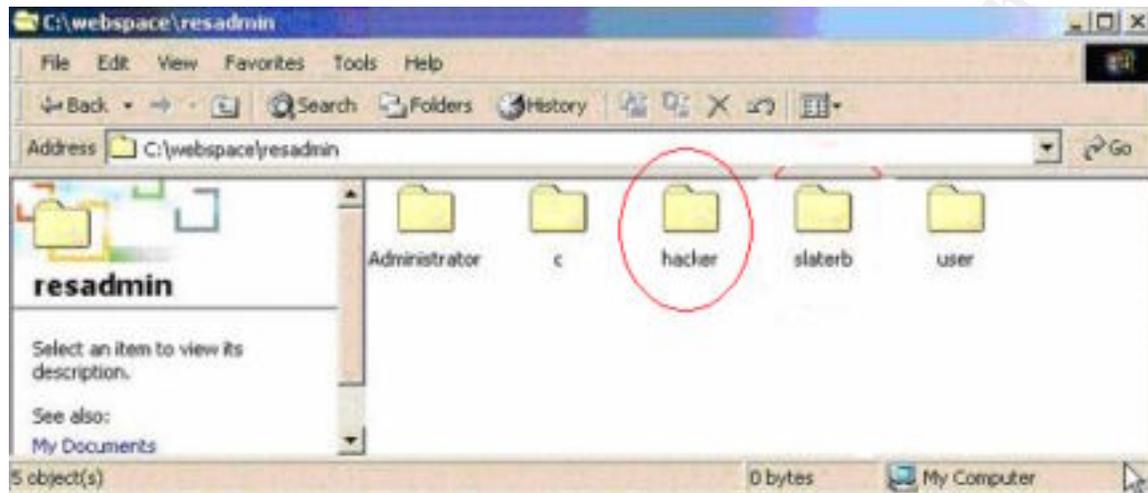
- Internet Information Servers MMC
- Hosting Controllers Database tables
- Directory structure created under the default of %default%\webpace

The IIS website, Hosting Database, and directories will all reflect the same name. So if a website was created called Hacked.com, all of the affected areas would display the same name.



ID	WebSiteName	Owner	RootDir
1	Default Web Site	system	C:\webpace\resadmin\localhost\Default Web Site\www
2	C:\webpace\resadmin\...\www
3	hacked.com	hacker	C:\webpace\resadmin\hacked.com\www
4	uscr.com	uscr	C:\webpace\resadmin\uscruser.com\www

I was able to determine the date and time of the incident and when to start looking for new folders, files, or system changes by the creation dates of the website log folder, created by IIS, and directories. From these timestamps, I was able to narrow down the timeframe and verify this incident for other log files, such as the IDS and firewall logs.



In addition, I keep a hard copy log of changes or updates made on this system. Since this system was compromised, it could not be trusted to display correct information. I cross referenced the hard copy log to rule out the possibility that site was legitimate and this was a false positive.

SNORT comes with a large set of rules. I thought it would show the following alert for this exploit. During testing, this alert did not go off. I needed a new rule.

```
WEB-MISC http directory traversal [**] [Classification: Attempted Information Leak]
[Priority: 3] {TCP} xxx.xxx.xxx.xxx -> xxx.xxx.xxx.xxx
```

The new rule specifically addresses this exploit. The rule proved affective during the testing of the server vulnerability. SNORT is detecting the exploit when the logs display this:

```
02/05-14:55:51.593120 [**] [1:0:0] <\Device\Packet_{1972E2EA-0493-
42DA-B5F0-7B74FBBC164E}> Hosting Exploit [**] {TCP} xxx.xxx.xxx.93:1480
-> 192.168.1.202:8080
```

The SNORT rule that is used:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 8080 (msg:"Hosting Exploit
Transversal Attack"; uricontent:"/filemanager.asp"; content:"\..\");
```

PHASE 3 -Containment

I was close by the machine when the attack occurred, so could react quickly. I started with stopping the web service for the unauthorized web site. This certainly would not stop a second site from being created, but would buy me about 1 minute to check other things and not have to shut down every website on the server.

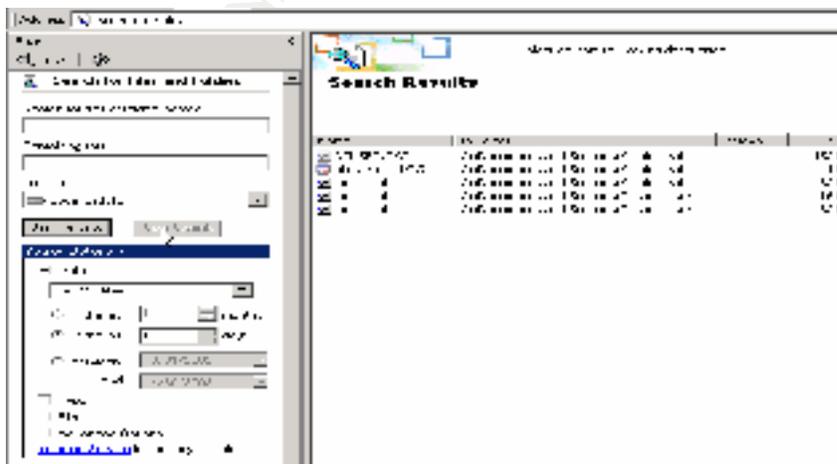
I sent an e-mail message out to the legitimate site owners that a few minute outage was about to occur for maintenance. This would give them the impression that the server was going through a quick maintenance routine rather than alarm them that the server may be compromised.

After the message was sent out, I stop all websites to keep from any additional possible harm. In addition, I went proceeded with disconnecting the network cable to be absolutely sure no more communication could be made.

The FTP logs didn't show any unusual FTP activity during the incident time-frame. The user James is a legitimate user.

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2002-01-15 03:18:12
#Fields: time c-ip cs-method cs-uri-stem sc-status
03:18:40 192.168.1.xxx [2]USER james 331
03:18:40 192.168.1.xxx [2]PASS - 530
03:18:46 192.168.1.xxx [3]USER james 331
03:18:46 192.168.1.xxx [3]PASS - 530
03:18:46 192.168.1.xxx [4]USER james 331
03:18:46 192.168.1.xxx [4]PASS - 530
03:18:46 192.168.1.xxx [5]USER james 331
03:18:46 192.168.1.xxx [5]PASS - 530
```

I made sure that the parent paths were disabled in this site to prevent any more transversals. I used the find files on the computer to see if anything new had been created in the last day. I used the Start>Search> with Search options by date(displayed below).

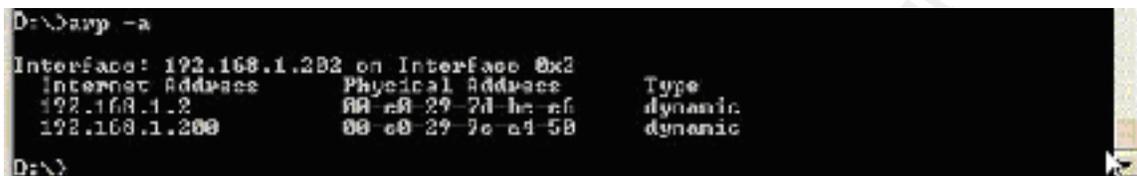


No new files had been updated to the system that weren't normal, but I wanted to make sure I didn't miss anything and proceeded to check a few basic items.

Commands Used

All of the following commands were executed for a trusted CD-ROM on the comprised system.

ARP -A



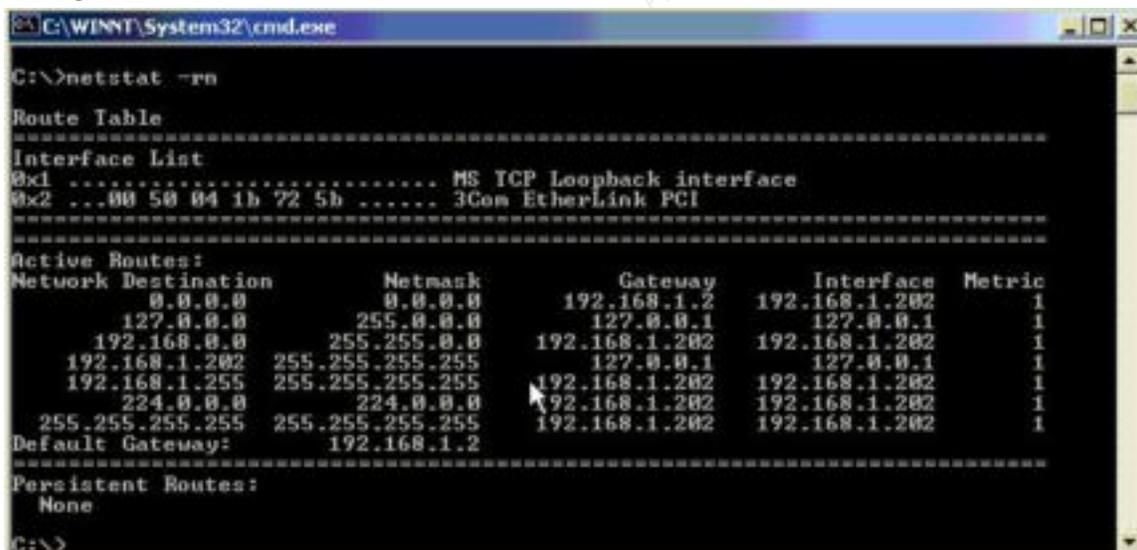
```
D:\>arp -a

Interface: 192.168.1.202 on Interface 0x2
Internet Address      Physical Address      Type
192.168.1.2          00-e0-29-7d-bc-ef    dynamic
192.168.1.200        00-e0-29-7c-e1-58    dynamic

D:\>
```

I checked to make sure there were no unusual ARP table entries. There were no static entries. I checked this several times to make sure there weren't any strange dynamic entries appearing.

NETSTAT -RN



```
C:\WINNT\System32\cmd.exe

C:\>netstat -rn

Route Table
=====
Interface List
=====
0x1 ..... MS TCP Loopback interface
0x2 ...00 50 04 1b 72 5b ..... 3Com EtherLink PCI
=====

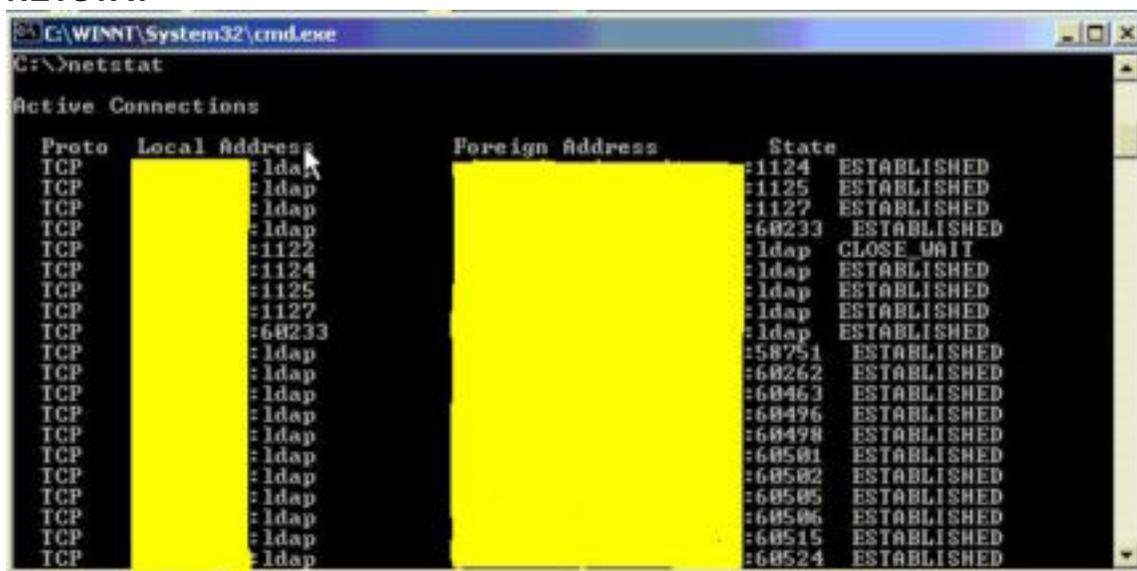
Active Routes:
Network Destination    Netmask          Gateway          Interface        Metric
-----
0.0.0.0                0.0.0.0          192.168.1.2     192.168.1.202    1
127.0.0.0              255.0.0.0        127.0.0.1       127.0.0.1        1
192.168.0.0            255.255.0.0     192.168.1.202   192.168.1.202    1
192.168.1.202         255.255.255.255  127.0.0.1       127.0.0.1        1
192.168.1.255         255.255.255.255  192.168.1.202   192.168.1.202    1
224.0.0.0              224.0.0.0        192.168.1.202   192.168.1.202    1
255.255.255.255       255.255.255.255  192.168.1.202   192.168.1.202    1
Default Gateway:      192.168.1.2

Persistent Routes:
None

C:\>
```

I used the netstat.exe with the -r (display the routing table) and -n (show in numerical form) options. There were no strange entries in the routing table.

NETSTAT



```
C:\WINNT\System32\cmd.exe
C:\>netstat

Active Connections

Proto Local Address Foreign Address State
TCP : :ldap :1124 ESTABLISHED
TCP : :ldap :1125 ESTABLISHED
TCP : :ldap :1127 ESTABLISHED
TCP : :ldap :68233 ESTABLISHED
TCP : :1122 :ldap CLOSE_WAIT
TCP : :1124 :ldap ESTABLISHED
TCP : :1125 :ldap ESTABLISHED
TCP : :1127 :ldap ESTABLISHED
TCP : :68233 :ldap ESTABLISHED
TCP : :ldap :58751 ESTABLISHED
TCP : :ldap :68262 ESTABLISHED
TCP : :ldap :68463 ESTABLISHED
TCP : :ldap :68496 ESTABLISHED
TCP : :ldap :68498 ESTABLISHED
TCP : :ldap :68501 ESTABLISHED
TCP : :ldap :68502 ESTABLISHED
TCP : :ldap :68505 ESTABLISHED
TCP : :ldap :68506 ESTABLISHED
TCP : :ldap :68515 ESTABLISHED
TCP : :ldap :68524 ESTABLISHED
```

The netstat command I thought was most important. It was used to check for any new open ports that should not exist. The routing and the arp tables I think could be detected faster because it could cause network problems or show up with daily trouble shooting. There were no new ports.

Checking for new ports is only half checking your system if you think was compromised. You need to use a tool, such as netcat, to check that each port is responding with the appropriate service. For example, port 23 should respond with a telnet service, not an FTP service. Each port was checked and all services were okay.

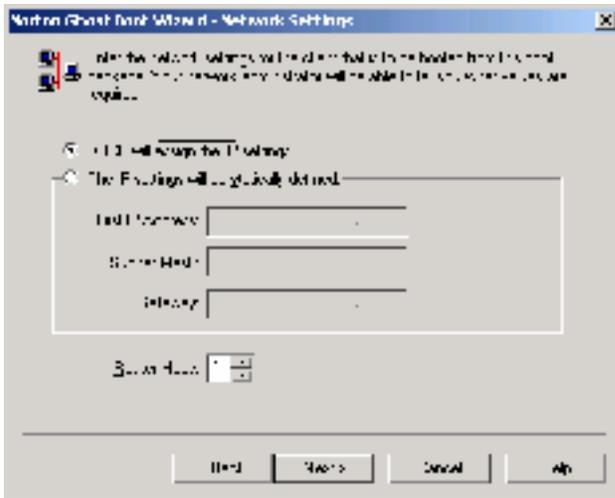
Other systems were checked. I ran the same commands and did not find anything suspicious. In addition, I looked through Sygate's logs and the firewall logs and there was not communication to any other machine during this time.

Tracking modifications to the system

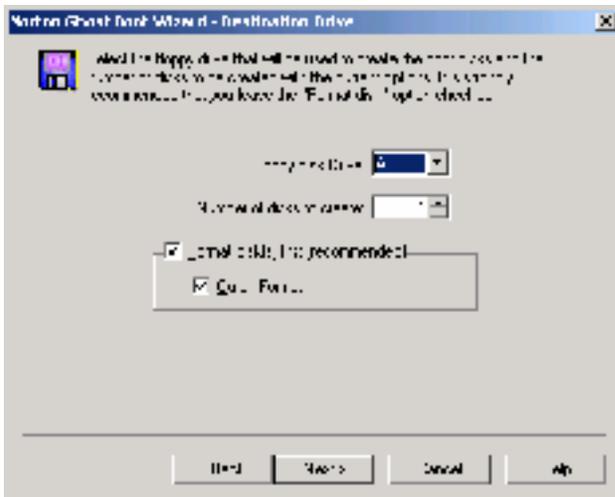
Once I felt confident that the system was secured and contained, I scheduled a time when the server would have low usage to shut the machine down and make an image. It would have been great to be able to make an image of the system while it was still running, but I did not have that capability.

I shut the system down for about 25 minutes and used Norton Ghost to make an image of the system to a trusted laptop computer which was not connected during that attack. The image will be used later to further analyze the system. Going back to take a look at everything a second time may shed new light on the attack that I missed during the incident handling process.

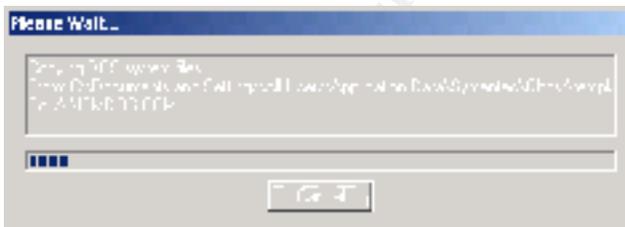
I made my image with Ghost using the Peer-to-Peer Network Book Disk. Simply start the Norton Ghost Boot Wizard to create a floppy disk to boot your system.



Decide if you want Ghost to use DHCP or you want to specify the IP address it will use. If you don't specify the IP address, Ghost will display the IP address it has obtained from the DHCP server.



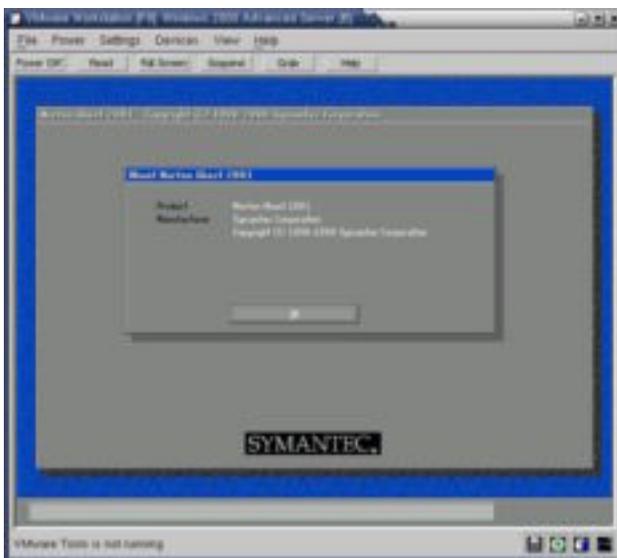
Insert a floppy disk for Ghost to write the necessary files to. You have the option to format a disk if you need.



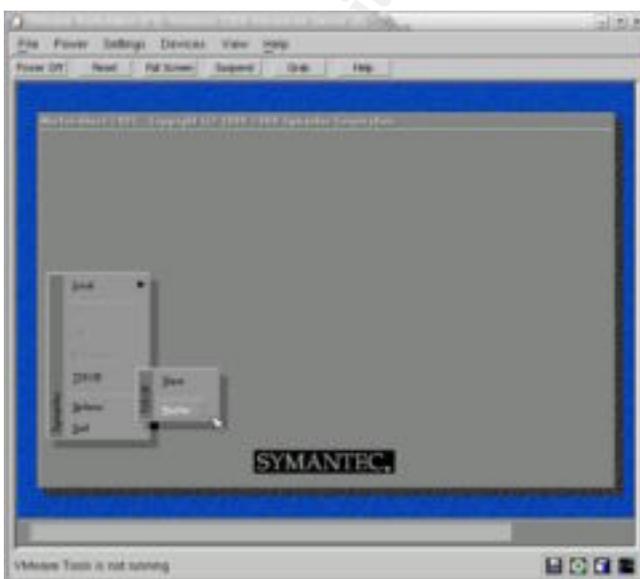
Ghost will create the bootable floppy with the information you provided.



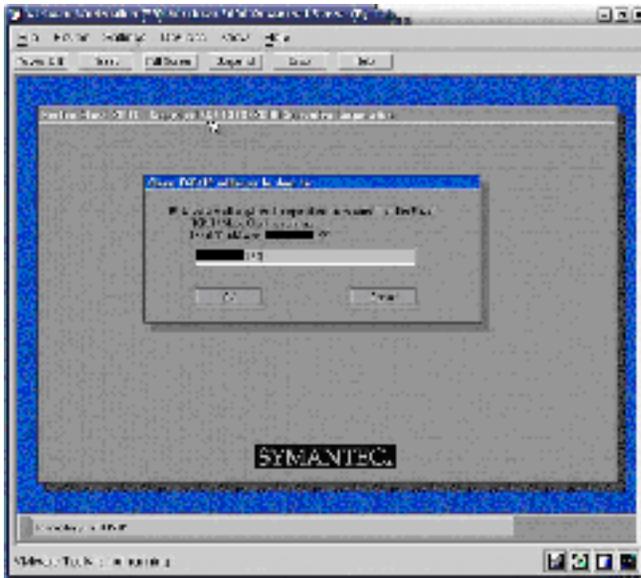
Your boot disk is created. Repeat this process if you need a boot disk for a different network card.



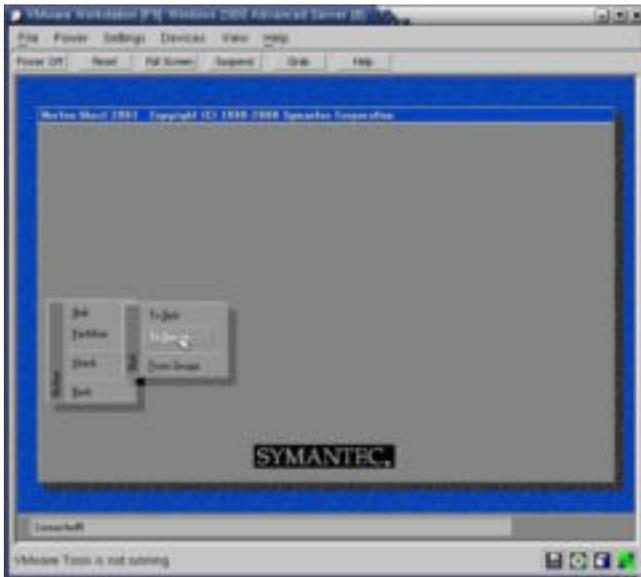
This screen just shot just shows the Ghost has started with the splash screen after the system has boot. Ghost starts automatically.



Use the TCP/IP option and select Master on the computer you want to make the image from. On the computer that will store the image, select Slave. The Slave will display the IP address you need to connect to.

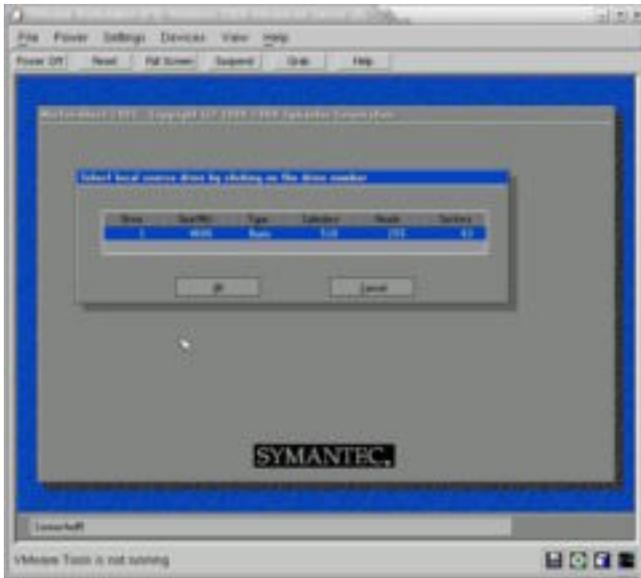


Type the IP of the Slave into the dialog box. The status box at the bottom of the screen will display Connected!! if you are successful.

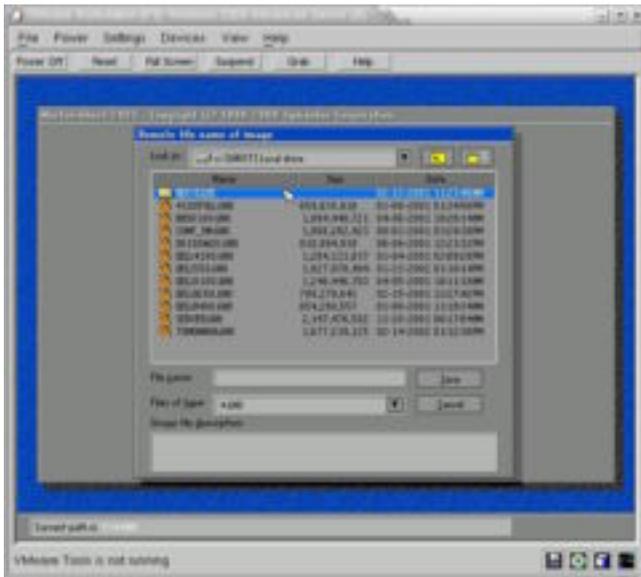


Select the appropriate imaging method. In my case, I selected to image the entire disk. If I had multiple partitions, I could image each partition separately or image the entire disk, which would contain all of the partitions.

© SANS

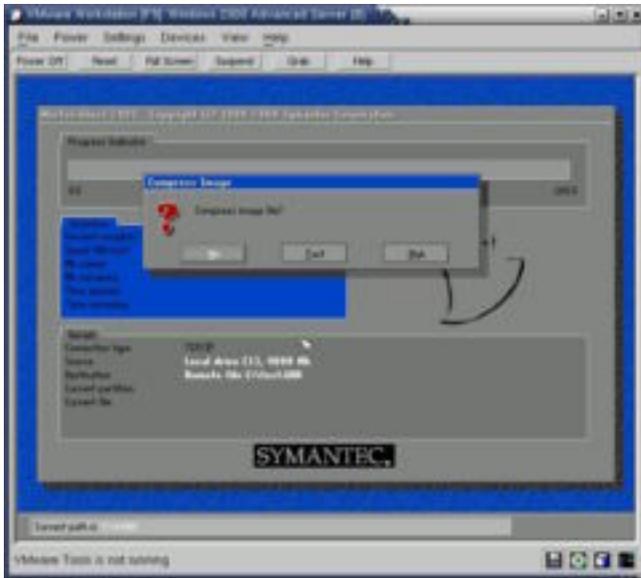


Select the drive or partition you need to image.

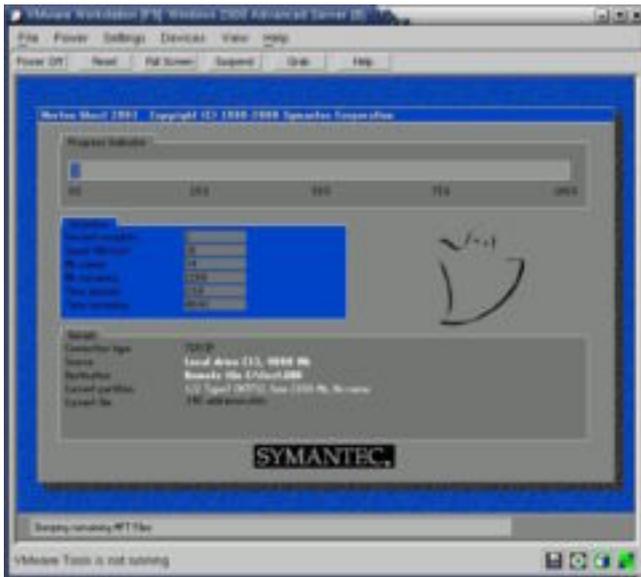


Specify the name of the image and the drive on the remote computer (slave) you want to store it.

© SANS Institute
Author retains full rights.

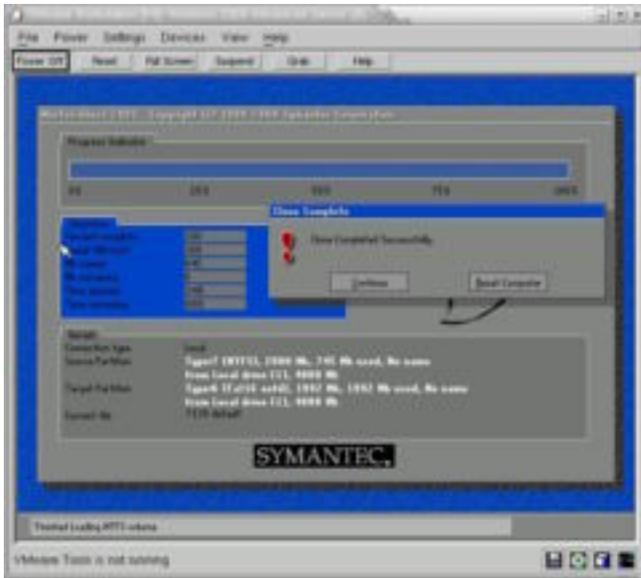


You have the option to compress the image. The higher the compression, the less space the image will take, but the more time it will take to create and restore, if you have the space, don't compress.



Depending on the size of the drive, partition, compress used, ghosting can take anywhere from half hour to three hours. Network activity can affect the speed the image is created over the network. A cross-over cable would minimize network traffic and may speed up the ghosting process.

© SANS



The image creation is complete and ready for any analysis that may be necessary.

PHASE 4 -Eradication

The new Hosting Controller Database, IIS, and the directory entries were deleted after a week's time passed and there was no activity on that site. The reason it was left running was to try to log more attempts to compromise the system and possibly gather additional information about the attacker. Here are the hardening techniques used for securing the system.

Disabled Parent Paths (Q184717 / Q226474)

All transversal attacks use the “..” notation with executable code to “walk up” and “walk down” the directory hierarchy. Disabling the parent path feature is the best countermeasure I found for transversal attacks.



Disabling the parent paths will not affect relative path usage in ASP or HTML. Any relative path to static content will still work. For example ``, a relative path to the images directory will still work.

Disabling parent paths will however break `#include` file statements that are relative. There is a work-a-round for this which is easy to implement. Just move all of your include files into a separate virtual directory and make the change in the include line as follows:

```
<!-- #include file="..\..\file.inc"--> to <!-- #include virtual="/inc/file.inc"-->
```

No website directories on the system partition

It is critical that the operating system and the website directories are not located on the same partition or are on a separate hard drive. In case a transversal attack is successful, the attacker can only transverse up to the root of that partition. By moving all the websites to their own partition or drive, the attacker cannot transverse the operating system directories.

Removing Administrative Tools

I removed all most of the administrative tools from the server and burned them to a CD-ROM. This accomplishes three things.

- 1) If the server is compromise, the attacker will have to upload their own tools.
- 2) If any tools are found on the server, it would be considered an incident, since no tools should be installed.
- 3) If I am using any of these tools, they will be from a trusted source rather than from the server that may have been compromised, along with the tools.

Tools Removed:

ARP.EXE
CMD.EXE
COMMAND.EXE
CSCRIPT.EXE
DEBUG.EXE
DIALER.EXE
EDIT.EXE
FINGER.EXE
[FTP.EXE](#)
HYPERTRM.EXE

IPCONFIG.EXE
MSIEXEC.EXE
NBTSTAT.EXE
NET.EXE
NET1.EXE
NETSTAT.EXE
NSLOOKUP.EXE
PING.EXE
RCP.EXE
RDISK.EXE

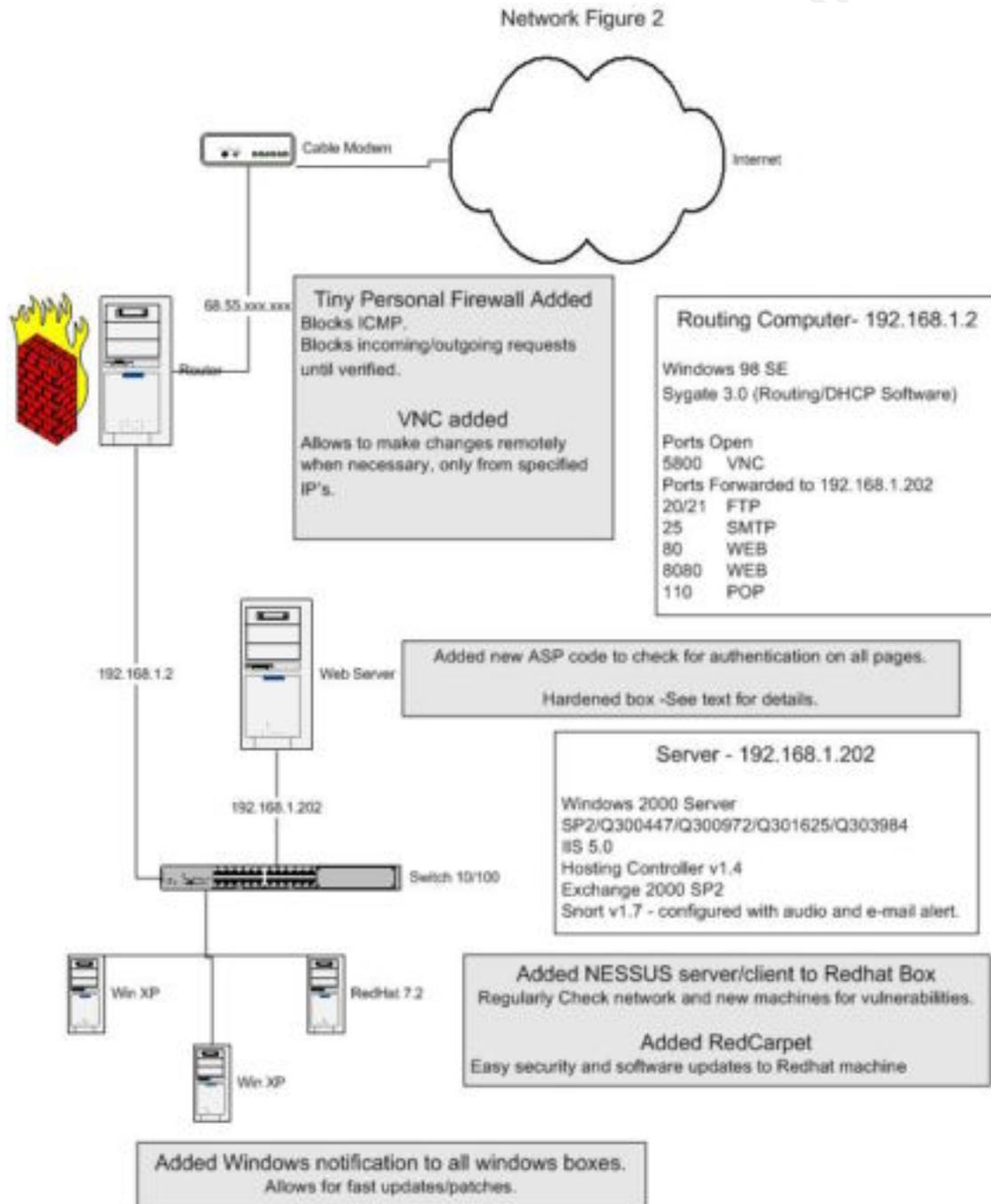
REGEDIT.EXE
REGEDT32.EXE
REGSVR32.EXE
ROUTE.EXE
TELNET.EXE
TFTP.EXE
TRACERT.EXE
WSCRYPT.EXE

Network

The network was improved by using a few free programs that are available for download. The two recommend programs are Tiny Firewall

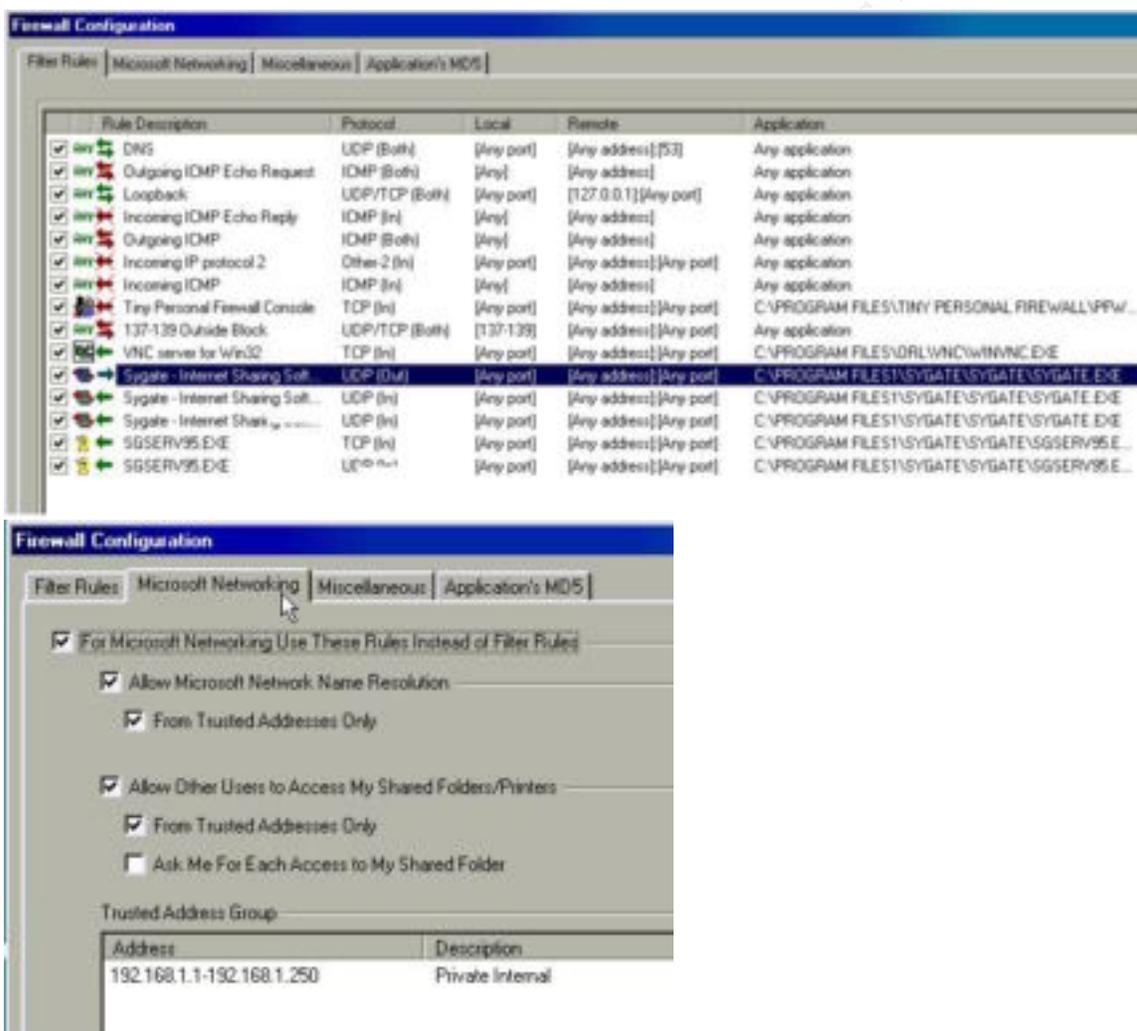
(<http://www.tinysoftware.com>) and Zone Alarm (<http://www.zonelabs.com>). These two programs go a long way in providing protection to your computers by filtering or blocking vulnerable service ports.

The original network configuration in Figure 1 did not have a firewall or any blockage at each system. Figure 2 shows the improved network that includes a firewall at the routing computer and Zone Alarm installed on each internal system for added protection.



The firewall has several rules in place to help reduce attacks. Any port that was not permitted by the firewall, that an attempt was made to connect to, is logged by the firewall. The firewall rules include:

- **ICMP Traffic Blocked (Inbound/Outbound)** - This will help in several ways, but the most important is for automated scanners searching if a system is up and responsive using ping. It will however, reduce options for troubleshooting the network.
- **Incoming Ports allowed** - Incoming ports allowed were restricted to 20/21 (FTP), 25(SMTP), 80(HTTP), 8080(HTTP), and 110 (POP).



As the network traffic becomes more familiar, different rules may need to be applied. The firewall rules were just a preliminary step in establishing an effective rule set.

The firewall does have its limitations. Just because the firewall was installed, doesn't mean that everything is safe. Actually the firewall would have been

useless against the logon page and the transversal attack because it had to let port 80 and 8080 through. However, it will provide added protection to the system and network as a whole.

Zone Alarm will pick up where the firewall left off. Careful not to restrict traffic too much, the firewall just has a few basic rules so far. A better understanding of what applications need to communicate and the ports they use can be accomplished with Zone Alarm.

Every time an application tried to communicate locally or on the internet, Zone Alarm blocked the communication until it was set to one of the three following options:

1. Permitted this once
2. Permitted all the time, which creates a rule
3. Denied this time
4. Denied all the time, which creates a rule

An evaluation of the client computers in a few weeks will give a better idea of what rules need to be changed on the firewall and what is normal network traffic.

I added Virtual Network Computing (VNC) to assist me in remotely managing the servers. This will cut down on down-time associated with traveling if I am not at the same location.

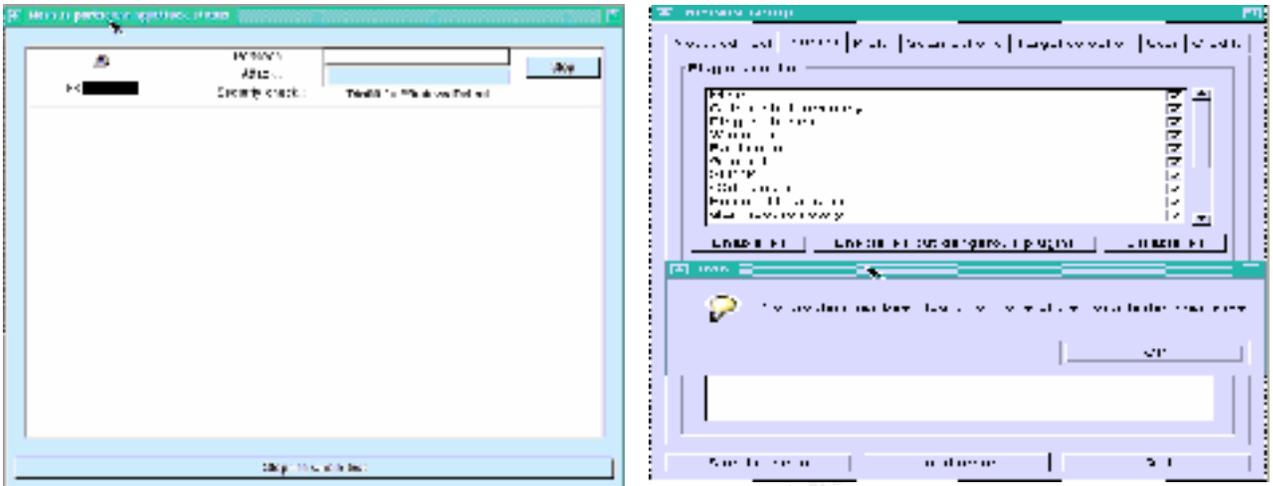
PHASE 5 -Recovery

After the system had been comprised, I kept checking the system manually about every 15 minutes. I was not able to physically sit in front of the machine for next couple of days to watch it's every move, but felt that after hardening the system and adding additional rules to the IDS, that I could afford a little more freedom.

After making an image, using the vulnerability tool Nessus, and verifying that the system was okay, I decided to reconnect it to the network and start all of the services back up. No data need to be restored.

NESSUS added

During the monitoring stage, I also installed and configured the vulnerability scanner, NESSUS, on the incident handling dedicated laptop. This would help identify anything that I may have missed during this incident that made the system vulnerable and will go a long way in preventing future incidents. NESSUS will be used on a weekly routine basis to check for vulnerabilities.



Nessus reports, pictured on the right, it found no problems on the Hosting Controller server. Nessus is making its assessment from the external network. An assessment from the internal network may allow for discovery of vulnerabilities, but these would only pertain to internal computers attacking. My focus at the moment is to secure the server from external attacks. Additional hardening may be applied to the server for internal network communication, but an assessment of usability vs security would need to be completed first. We wouldn't want to secure the server so well internally that it would not be useable by employees.

ACID Added

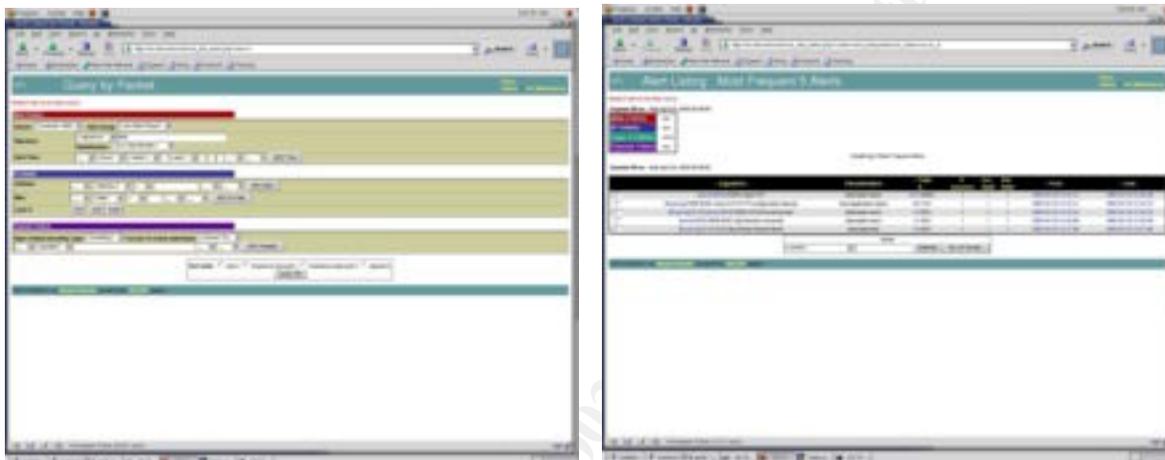
The Analysis Console for Intrusion Databases (ACID) is a PHP-based analysis engine to search and process a database of security events generated by various IDSes, firewalls, and network monitoring tools. The features currently include:

- **Query-builder and search interface** for finding alerts matching on alert meta information (e.g. signature, detection time) as well as the underlying network evidence (e.g. source/destination address, ports, payload, or flags).
- **Packet viewer (decoder)** will graphically display the layer-3 and layer-4 packet information of logged alerts
- **Alert management** by providing constructs to logically group alerts to create incidents (alert groups), deleting the handled alerts or false positives, exporting to email for collaboration, or archiving of alerts to transfer them between alert databases.
- **Chart and statistics generation** based on time, sensor, signature, protocol, IP address, TCP/UDP ports, or classification ¹

¹ <http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html>

Analysis Console for Intrusion Detection was added to better understand the data logged by Snort. ACID uses MySQL to log the data instead of a text file and PHP to format the data for viewing by a standard web browser.

I hope to use ACID to find trends over time and what the common attacks are so that I can better configure my network. Even if the network is secured against the attacks being used, ACID may help identify computer or networks that commonly are being used for attacks.



Pictured on the left is the ACID query builder. You can customize many reports to help organize Snorts data. Pictured on the right is the five most used attacks. This is a good place to start to look for what defenses you need to build that would be the give the most immediate result. Luckily, the top record shows that nmap is being used for reconnaissance, which was generated by my use of Nessus. I know now it would be useful to eliminate records that have the IP address of my vulnerability testing machine so it doesn't clutter the real data.

Setup Guides:

Redhat 7.2/MySQL/ACID

http://www.sfh.net/whites/snort_acid-rpm.html

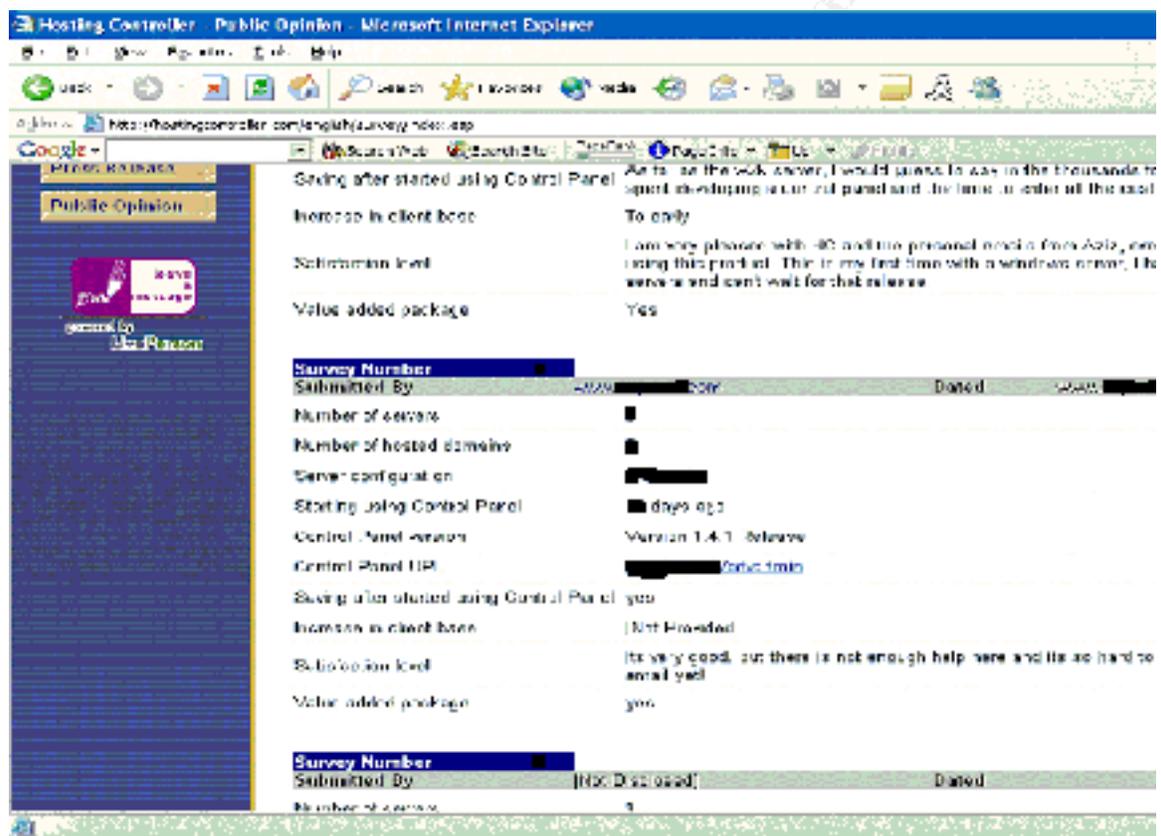
Windows 2000/MySQL/ACID

<http://www.silicondefense.com/techsupport/windows-acid.htm>

PHASE 6 -Follow Up/Lessons Learned

One step that should never be left out is following up. Why go through all the trouble of establishing policies, detecting intrusions, and restoring systems if you are not going to follow up on your systems.

The Hosting Controller Exploit led me to this incident detection. I wanted to add a few things in I found while testing the Hosting Controller package. The company has not addressed the problem at all on their website at the time of this paper. The worst part of all is that the company has a testimonial page that users of the product can post their comments located at <http://hostingcontroller.com/English/survey/index.asp> shown below. In these posts, along with the exploit, no port scanning or recon of any kind is needed. All the information about where the site is located and what directory the control panel is located is all right there! This is an unnecessary field in the survey that adds no value and should be removed. I plan on contacting the company about the potential misuse of this information.



Lessons Learned

The biggest lesson I have learned is never assume you have the complete answer to the incident. Even after you taken the appropriate steps, you should go back over your work several times and if possible, have another person

review what you have done. Assuming you made no mistakes and did a perfect job can be disastrous.

The second most important lesson was that well written policies and procedures greatly improve your chances of success. Too many times writing policies and procedures are put at a lower priority when they need to be one of the first things considered.

There are several other lessons that I learned during this incident:

- Don't get caught in the moment and lose site of handling the incident in methodical manner.
- Don't take attacks as a personal attack. It helps remove illogical emotions from the situation and improve your chances if it becomes a legal matter.
- No matter how many warning, news groups, security alerts, and scary news reports are out there, many systems will go neglected. Most because of ignorance of the user and the fact that most people don't even know they have been compromised.
- Experience, Experience, Experience.

I think most people have the mentality that "It won't happen to me" when most people wouldn't know if it did happen to them.

The Forgotten Policy

One policy that was set, but not adhered to was:

- Test networks and/or machines must be on their own network segment.

Testing exploits need to be performed exclusively in a testing environment. I was jeopardizing other machines by running exploits against the test server on the production network.

There is not set action to take if a policy is broken. It is discretionary, which I believe can lead to many problems. This does make the policies less effective, but at the moment fixing this is on the "back burner".

Check List Needed

For better preparation of incident handling, checklists need to be implemented as a standard. A good checklist to start with for a company can be found at <http://www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp>

Finally, I never fully understood the magnitude of the problem at large and what SAN's efforts can mean against these types of problems globally. This incident alone gives me a better sense of duty to keep up with all the security standards and to know that my neglect could greatly affect others.

References

Hosting Controller. January 14, 2002. <http://www.hostingcontroller.com>

Webopedia, "HTTP". January 15, 2002. <http://www.webopedia.com/TERM/h/http.html>

Webopedia, "TCP/IP". January 15, 2002. http://www.webopedia.com/TERM/T/TCP_IP.html

Beginning Active Server Pages 3.0. David Buser, et.all, Wrox Pred Ltd, Feb 2002.

Webopedia, "IIS". January 15, 2002. <http://www.webopedia.com/TERM/I/IIS.html>

Snort. January 17, 2002. <http://www.snort.org>

Analysis Console for Intrusion Databases, Roman Danyliw, January 15, 2002.
<http://www.andrew.cmu.edu/~rdanyliw/snort/snortacid.html>

"Building a RedHat 7.2 Box to Run Snort and Acid with MySQL", Mark Johnston.
http://www.sfn.net/whites/snort_acid-rpm.html

Windows Documentations for Snort and Acid, April 29, 2002.
<http://www.silicondefense.com/techsupport/windows-acid.htm>

Hosting Controller. January 14, 2002. <http://hostingcontroller.com/English/survey/index.asp>

Company Checklist, Interpol. April 30, 2002.
<http://www.interpol.int/Public/TechnologyCrime/CrimePrev/companyChecklist.asp>

© SANS Institute 2000 - 2002. Author retains full rights.

Appendix A

CERTS

Bugtraq 3803 – No matching CVE

<http://online.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3808>

bugtraq id 3808

object

class Input Validation Error

cve CVE-MAP-NOMATCH

remote Yes

local No

published Jan 05, 2002

updated Jan 07, 2002

vulnerable [Hosting Controller](#) [Hosting Controller 1.4.1](#)

- Microsoft Windows 2000 Advanced Server 0.0
- Microsoft Windows 2000 Advanced Server 0.0SP1
- Microsoft Windows 2000 Advanced Server 0.0SP2
- Microsoft Windows 2000 Server 0.0
- Microsoft Windows 2000 Server 0.0SP1
- Microsoft Windows 2000 Server 0.0SP2
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0SP1
- Microsoft Windows NT Server 4.0SP2
- Microsoft Windows NT Server 4.0SP3
- Microsoft Windows NT Server 4.0SP4
- Microsoft Windows NT Server 4.0SP5
- Microsoft Windows NT Server 4.0SP6
- Microsoft Windows NT Server 4.0SP6a

Discussion-

A vulnerability exists in Hosting Controller which may allow a remote attacker to display arbitrary directories and files.

Reportedly, Hosting Controller is prone to directory traversal attacks. By appending 'filepath=driveletter:\' to a web request, it is possible for an attacker to break out of root and browse the filesystem of the host.

Solution-
None

Bugtraq 3971 – No matching CVE

<http://online.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3971>

bugtraq id 3971

object

class Design Error

cve CVE-MAP-NOMATCH

remote Yes

local No

published Jan 26, 2002

updated Jan 28, 2002

vulnerable **Hosting Controller Hosting Controller 1.1**

- Microsoft Windows 2000 Advanced Server 0.0
- Microsoft Windows 2000 Advanced Server 0.0SP1
- Microsoft Windows 2000 Advanced Server 0.0SP2
- Microsoft Windows 2000 Professional 0.0
- Microsoft Windows 2000 Professional 0.0SP1
- Microsoft Windows 2000 Professional 0.0SP2
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0SP1
- Microsoft Windows NT Server 4.0SP2
- Microsoft Windows NT Server 4.0SP3
- Microsoft Windows NT Server 4.0SP4
- Microsoft Windows NT Server 4.0SP5
- Microsoft Windows NT Server 4.0SP6a

Hosting Controller Hosting Controller 1.3

- Microsoft Windows 2000 Advanced Server 0.0
- Microsoft Windows 2000 Advanced Server 0.0SP1
- Microsoft Windows 2000 Advanced Server 0.0SP2
- Microsoft Windows 2000 Professional 0.0
- Microsoft Windows 2000 Professional 0.0SP1
- Microsoft Windows 2000 Professional 0.0SP2
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0SP1
- Microsoft Windows NT Server 4.0SP2
- Microsoft Windows NT Server 4.0SP3
- Microsoft Windows NT Server 4.0SP4

- Microsoft Windows NT Server 4.0SP5
- Microsoft Windows NT Server 4.0SP6a

Hosting Controller Hosting Controller 1.4b

- Microsoft Windows 2000 Advanced Server 0.0
- Microsoft Windows 2000 Advanced Server 0.0SP1
- Microsoft Windows 2000 Advanced Server 0.0SP2
- Microsoft Windows 2000 Professional 0.0
- Microsoft Windows 2000 Professional 0.0SP1
- Microsoft Windows 2000 Professional 0.0SP2
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0SP1
- Microsoft Windows NT Server 4.0SP2
- Microsoft Windows NT Server 4.0SP3
- Microsoft Windows NT Server 4.0SP4
- Microsoft Windows NT Server 4.0SP5
- Microsoft Windows NT Server 4.0SP6a

Hosting Controller Hosting Controller 1.4

- Microsoft Windows 2000 Advanced Server 0.0
- Microsoft Windows 2000 Advanced Server 0.0SP1
- Microsoft Windows 2000 Advanced Server 0.0SP2
- Microsoft Windows 2000 Professional 0.0
- Microsoft Windows 2000 Professional 0.0SP1
- Microsoft Windows 2000 Professional 0.0SP2
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0SP1
- Microsoft Windows NT Server 4.0SP2
- Microsoft Windows NT Server 4.0SP3
- Microsoft Windows NT Server 4.0SP4
- Microsoft Windows NT Server 4.0SP5
- Microsoft Windows NT Server 4.0SP6a

Hosting Controller Hosting Controller 1.4.1

- Microsoft Windows 2000 Advanced Server 0.0
- Microsoft Windows 2000 Advanced Server 0.0SP1
- Microsoft Windows 2000 Advanced Server 0.0SP2
- Microsoft Windows 2000 Server 0.0
- Microsoft Windows 2000 Server 0.0SP1
- Microsoft Windows 2000 Server 0.0SP2
- Microsoft Windows NT Server 4.0
- Microsoft Windows NT Server 4.0SP1
- Microsoft Windows NT Server 4.0SP2
- Microsoft Windows NT Server 4.0SP3
- Microsoft Windows NT Server 4.0SP4
- Microsoft Windows NT Server 4.0SP5
- Microsoft Windows NT Server 4.0SP6a

Discussion-

Hosting Controller is an application which centralizes all hosting tasks to one interface. Hosting Controller gives every user the required control they need to manage the appropriate web site relevant to them. Hosting Controller runs on Microsoft Windows

systems.

An issue has been discovered in Hosting Controller which may make it easier for remote attackers to brute-force user accounts. When a user enters an invalid username, Hosting Controller gives the following feedback:

"The user name could not be found"

This allows the attacker to determine which usernames are valid. The attacker may then attempt a brute-force attack in an attempt to crack the passwords of valid usernames.

Solution-

Workaround: Use a non-default path for the login page to Hosting Controller.

Bugtraq 3811 – No matching CVE

<http://online.securityfocus.com/cgi-bin/vulns-item.pl?section=info&id=3811>

bugtraq id 3811

object

class Access Validation Error

cve CVE-MAP-NOMATCH

remote Yes

local No

published Jan 07, 2002

updated Jan 08, 2002

vulnerable [Hosting Controller Hosting Controller 1.4.1](#)

- [Microsoft Windows 2000 Advanced Server 0.0](#)
- [Microsoft Windows 2000 Advanced Server 0.0SP1](#)
- [Microsoft Windows 2000 Advanced Server 0.0SP2](#)
- [Microsoft Windows 2000 Server 0.0](#)
- [Microsoft Windows 2000 Server 0.0SP1](#)
- [Microsoft Windows 2000 Server 0.0SP2](#)
- [Microsoft Windows NT Server 4.0](#)
- [Microsoft Windows NT Server 4.0SP1](#)
- [Microsoft Windows NT Server 4.0SP2](#)
- [Microsoft Windows NT Server 4.0SP3](#)
- [Microsoft Windows NT Server 4.0SP4](#)
- [Microsoft Windows NT Server 4.0SP5](#)
- [Microsoft Windows NT Server 4.0SP6](#)
- [Microsoft Windows NT Server 4.0SP6a](#)

Discussion-

Hosting Controller is an application which centralizes all hosting tasks to one interface. Hosting Controller gives every user the required control they need to manage the appropriate web site relevant to them. Hosting Controller runs on Microsoft Windows systems.

Reportedly, an issue exists in Hosting Controller which could enable a user to read, delete and upload arbitrary files to the host.

Due to a flaw in filemanager.asp a user could exploit this issue by attempting to connect to an existing account and specifying '../' character sequences.

Solution-

None

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix B

Incident Handling Laptop

Hardware

- Pentium III 700Mhz
- 512 MB
- 28 GB primary hard drive
- (2) 25 GB removable hard drives
- ZIP 100
- Floppy
- CD-Burner
- 56k Modem
- (2) PCMCIA NICs

Software

Operating Systems

- Red Hat 7.2 – Host Operating System
- Windows 98 SE – Vmware Guest
- Windows NT 4.0 – Vmware Guest
- Windows 2000 – Vmware Guest
- Windows 2000 Server – Vmware Guest
- Windows XP – Vmware Guest
- Red Hat 7.2 – Vmware Guest

Tools- Before incident

- Vmware 3.0
- Port Scanner
- Netcat
- Windows Resource Kits

Tools – added after incident

- Nessus
- Analysis Console for Intrusion Detection (ACID)
- Forensic Toolkit (Foundstone)
- Virtual Network Computing (VNC)

Appendix C

Hosting Controller Exploit

<http://packetstormsecurity.nl/0201-exploits/hosting.controller.txt>

Hi,
Here's my new advisory about Hosting Controller.
Phuong
Hosting Controller - Multiple vulnerabilities
Date: 01/04/2002

Summary

Hosting Controller is an all-in-one administrative hosting tool for Windows. It automates a wide range of hosting tasks and provides control of each hosted site to the respective owners. Hosting Controller is now widely used by hosting providers and can be found at <http://www.hostingcontroller.com>.

Systems Affected: Only the latest version, HostingController 1.4.1, was tested. (Probably all prior versions)

Vulnerability 1 - Browsing Non-public Directories Allowed
Vulnerability 2 - Dot Dot Slash bug and autosignup/dsp_newhc.asp

Impact: An attacker may be able to browse directories not intended to be publically accessible and upload scripts to manipulate files and control administration of sites using the latest version of HostingController.

Vendor contacted.

Details

Vulnerability 1 - Browsing Non-public Directories Allowed

Hosting Controller has a security flaw which allows outside attackers to browse any file and any directory without authentication. Files can't be read, however the second vulnerability (explained below) would allow you to compromise the whole server.

Sample scripts that allow browsing anywhere on the server:

```
http://www.eg.com/hc/stats/statsbrowse.asp?filepath=c:\&Opt=3
http://www.eg.com/hc/serv_u/servubrowse.asp?filepath=c:\&Opt=3
http://www.eg.com/hc/adminsettings/browsedisk.asp?filepath=c:\&Opt=3
http://www.eg.com/hc/adminsettings/browsewebalizerexe.asp?filepath=c:\&Opt=3
http://www.eg.com/hc/SQLServ/sqlbrowse.asp?filepath=c:\&Opt=3
```

The directory "hc" is an example of the path to the HostingController script on the sample domain. The actual "hc" directory name -- such as

"admin" or "hostingcontroller" -- must be discovered for each "eg.com" and replaced in the above URL scripts.

Vulnerability 2 - "Dot Dot Slash" bug and autosignup/dsp_newwebadmin.asp

The dsp_newwebadmin.asp script from Hosting Controller can be executed by using, eg:

http://www.eg.com/hc/autosignup/dsp_newwebadmin.asp

This allows an attacker to create a new domain name and a new account without logging in as administrator. The attacker can then log into HostingController after the new account has been created using the script dsp_newwebadmin.asp.

Once logged in, the attacker can use all HostingController menu options, as owner of the new account. The new domain name you just created, cannot yet be accessed because it needs to be activated by the "resadmin".

To gain control of administration and execute arbitrary code on the hosting server, the attacker need only click on the HostingController's "Directories" option on the left-hand side which will lead to the "File Manager" page allowing and you are only allowed to manage files within <drive>:\webspace\resadmin\youraccount\youraccount.com

But the filemanager.asp of HostingController is also vulnerable to the well-known "dot dot slash" bug `../` allowing directory traversal, via a script URL such as:

<http://www.eg.com/hc/folders/filemanager.asp&siteindex=testing&sitename=testing.com&OpenPath=C:\webspace\resadmin\testing\testing.com\www\..\..\..\..\>

The attacker then is able to read, delete, rename and upload files anywhere on the eg.com server. For example, ntdaddy.asp or cmdasp.asp can be uploaded to active domain names so that the attacker can execute commands via web browser. With a little bit of work, the attacker can also upload nc.exe and called nc.exe from an asp script ... Thereafter, the site is of course toast.

Vendor contacted.

Do You Yahoo!?
Send FREE video emails in Yahoo! Mail!
<http://promo.yahoo.com/videmail/>

Appendix D

Tiny Firewall

Tiny Personal Firewall represents smart, easy-to-use personal security technology that fully protects personal computers against hackers. It is built on the proven WinRoute Pro, ICSA certified security technology. Tiny Personal Firewall is also an integral part in Tiny Software's new Centrally Managed Desktop Security (CMD5) system awarded a contract by the US Air Force to encompass about 500,000 desktop computers. The following descriptions demonstrate the simplicity of use, yet powerful features of Tiny Personal Firewall.

Intrusion Detection

Personal Firewall includes an easy-to-use wizard that detects unknown activity and prompts the user for setup information. After the setup is complete, a new rule is applied to the filter rules list. This option may be disabled.

Application Filter

To protect from Trojan horse and other unauthorized applications, Personal Firewall includes an application filter. The wizard will detect when an application attempts to bind to a port for communication and create a filter rule based on the users input. Users may permit applications manually from the filter rules. Tiny Personal Firewall also provides a database of common applications that use known ports.

MD5 Signature Support

To ensure that Trojan horse applications cannot pose as a trusted application, Tiny Personal Firewall offers the option to check for an MD5 digital signature for trusted applications.

Syslog

Log information can be sent to a central syslog server for reporting purposes. This too will be an integral component of Tiny Software's new centrally managed desktop security system used by the US Air Force.

Trusted Addresses

Users may create filtering rules that apply to user-defined, trusted address groups. Multiple address groups, based on a single IP, a subnet, or range may be created in the "trusted addresses."

Remote/Secure Administration

In addition to login authentication, Tiny Personal Firewall allows for full remote configuration of security policies. This will be an important element for the centrally managed desktop security system as it will allow remote configuration of each user's security policies through a centrally managed console server.

Time Intervals

Filter rules can be arranged so that they are only valid during specific hours.

Tiny Personal Firewall includes many other firewall features and is an ideal security solution for home/business stand-alone and network computers.

Appendix E

Zone Alarm

<http://www.zonealarm.com>

ZoneAlarm version 2.6 automatically blocks known and unknown threats, barricading your computer against outside intrusions and attacks. With millions of users, ZoneAlarm is the most trusted Internet security available. The award-winning ZoneAlarm provides individuals with the easy yet powerful protection they need.

- Stop hackers and dangerous threats—known and unknown
- Instant, out-of-the-box security
- Easy, always-on protection
- Detailed yet easy-to-understand real-time alerts with expert advice from Zone Labs

© SANS Institute 2000 - 2002, Author retains full rights.

Appendix F

NESSUS

<http://www.nessus.org>

The 'Nessus' Project was started in early 1998, and first released in April 1998. At this time, the most complete free security scanner was SATAN, which is clearly outdated, and you could see the emergence of several commercial ones, that were clearly too expensive.

The Nessus Security Scanner is not only another security auditing tool. It is a security auditing as I think it should be - never trust the version number, never trust that a given service is listening on the good port (do all the web servers on earth listen on port 80 ?).

The Nessus Security Scanner is free, open-sourced and wants to be easy to use.

Here are the features of the Nessus Security Scanner :

- **Plug-in architecture.** Each security test is written as an external plugin. This way, you can easily add your own tests without having to read the code of the nessusd engine.
The complete list of the Nessus plugins is [here](#)
- **NASL.** The Nessus Security Scanner includes NASL, (Nessus Attack Scripting Language) a language designed to write security test easily and quickly. (security checks can also be written in C)
- **Up-to-date security vulnerability database.** We mostly focus on the development of security checks for **recent security holes**. Our security checks database is updated on a *daily* basis, and all the newest security checks are available [here](#) and on your FTP servers and mirrors.
- **Client-server architecture.** The Nessus Security Scanner is made up of two parts : a server, which performs the attacks, and a client which is the frontend. You can run the server and the client on different systems. That is, you can audit your whole network from your personal computer, whereas the server performs its attacks from the main frame which is upstairs. There are several clients : one for X11, one for Win32 and one written in Java
- **Can test an unlimited amount of hosts at the same time.** Depending of the power of the station you run the Nessus server onto, you can test two, ten or forty hosts at the same time
- **Smart service recognition.** Nessus does not believe that the target hosts will respect the IANA assigned port numbers. This means that it will recognize a FTP server running on a non-standard port (31337 say), or a web server running on port 8080
- **Multiples services.** Imagine that you run **two** web servers (or more) on your host, one on port 80 and another on port 8080. When it will come to testing their security, **Nessus will test both of them**
- **Tests cooperation.** The security tests performed by Nessus cooperate so that nothing useless is made. If your FTP server does not offer anonymous logins, then anonymous-related security checks will not be performed.
- **Cracker behavior.** Nessus does not believe that version x.y.z of a given software is immune to a security problem. 95% of the security checks will actually perform their job - they'll try to overflow your buffers, relay some mails, and even to crash down your computer !
- **Complete reports :** Nessus will not only tell you what's wrong on your network, but will, most of the time, tell you how to prevent crackers from exploiting the security holes found and will give you the risk level of each problem found (from *Low* to *Very High*)

- **Exportable reports** : The Unix client can export Nessus reports as ASCII text, LaTeX, HTML, "spiffy" HTML (with pies and graphs) and an easy-to-parse file format.
- **Multilingual support**. Nessus can issue reports in English or in French. More languages are to come.
- **Independent developers**. The Nessus developers are independent from the rest of the world, so we will not hide a security vulnerability in the program XYZ because we have a contract with them.
- **Easy-to-reach developers**. You feel that there is a missing feature ? Just contact us [here](#). We reply and implement what makes sense.

© SANS Institute 2000 - 2002, Author retains full rights.