qDefense Penetration Testing
A Subsidiary of Computer Modeling Corp.

Security Report Prepared for XXXXXXXX County/XXX Consulting

Network Range: xxx.xxx.48.192 – xxx.xxx.48.254

Section 1.0: Network Description

The network consists of a variety of hosts accessible from the Internet, each with a different purpose. They are protected by a firewall.

In addition, XXXXXXXX County apparently runs a public web server, www.xxxcounty.com, with IP address yyy.yyy.yyy.yyy. This server is outside the IP range requested, and was therefore not examined.

Section 2.0: Host Analysis

2.1

Host: xxx.xxx.48.193
Name: xxxxxxx-2.yyyy.net
System: Cisco 3640 (Apparently with IOS 11)
Function: Router/Switch
Services Accessible from the Internet:
Telnet tcp/23

The only TCP service on this host accessible from the Internet is telnet, running on tcp port 23. This telnet service uses password authentication, and allows remote configuration of the device. There are two inherent insecurities to the telnet service:

- Passwords in the telnet protocol are sent over the Internet unencrypted. Therefore, if an attacker is able to monitor communications to the host, he will be able to learn the password.
- An attacker may be able to derive the password through "brute force," that is, by having his computer repeatedly connect to the device, and try passwords from a list or dictionary, until the correct one is found. Depending on the speed of his connection, an attacker may be able to try millions of passwords. Therefore, even rare words, or passwords which include both letters and numbers, may possibly be guessed.

It is therefore recommended that, if possible, the telnet service be blocked from the Internet, and that configuration be done only from within the internal network. In any event, it is imperative that a strong password (i.e. not just an English word or name, even with intermixed digits) is used.

A vulnerability leading to denial of service has been discovered with Cisco's telnet software. This was not tested for, since the test could result in a denial of service. Most likely, the host is not vulnerable, since the vulnerability only exists in devices running Cisco IOS version 11.3 or later, while this device seems to be running an earlier version. Contact the vendor for additional information and for a patch (if needed).

Routing protocols, as they are outside of the scope of the audit requested, were not examined.

2.2

Host: xxx.xxx.48.195
Name: smtp.xxxcounty.com
System: Novell NetWare
Function: Mail server
Services Accessible from the Internet:
SMTP tcp/25 GroupWise Internet Agent 5.5.5.1

HTTP tcp/80 NetWare HTTP Stack
POP3 tcp/110 GroupWise POP3 server

The HTTP service indicates that the actual IP address (after NAT) of the host is 172.16.1.22. This information should not be disclosed.

The POP3 service is vulnerable to a buffer overflow attack. When a user attempts to log in using the command APOP, followed by two very long strings, the process crashes. This is do to the application not checking the length of the data before writing it to the allocated memory. An attacker may be able to exploit this to take over the host. As of the time of this writing, there has not been wide spread exploitation of this vulnerability, nor has exploit code been publicized. However, the software should nevertheless be patched immediately. Most likely, the Mercury MTA software for NetWare is being used to provide the POP3 service; contact Pegasus Mail (http://pmail.com) for a fixed version. If another software package is being used, please contact qDefense. See http://www.iss.net/security_center/static/6444.php for more information regarding this vulnerability.

Novell has issued a number of security bulletins and patches regarding GroupWise (see http://www.sans.org/newlook/digests/SAC/netware.htm). Most importantly, they recommend that all users apply the Padlock Update. See http://support.novell.com/padlock for more information.

The SMTP service seems to be configured to permit relaying; that is, to allow an outside party to use the server to send e-mail to another outside party. While this is not a security issue, it should be disabled. See http://www.iss.net/security_center/static/210.php for more information.

2.3

Host: xxx.xxx.48.196
Names: ww2.xxxcounty.com
xxxxxxx-5.yyyy.net
System: Microsoft Windows NT 4.0 Server (Most likely with SP5)
Function: Web Server
Services Accessible from the Internet:
HTTP tcp/80 Microsoft IIS 4.0
HTTPS tcp/443 Microsoft IIS 4.0

The server apparently functions as a web based gateway to the Citrix servers.

The HTTP service indicates that the actual IP address (after NAT) of the host is 172.16.1.27. This information should not be disclosed.

The server has apparently been patched to protect from some of the most commonly exploited IIS vulnerabilities. Nevertheless, it is still, unfortunately, extremely insecure. Significant action must be taken to secure it. Until these actions are taken, the server is a proverbial sitting duck for both human attackers and automated worms and scanners.

Note: Information as to how to eliminate the vulnerabilities discussed herein is included in Appendix B.

List of Vulnerabilities:

2.3.1
The MDAC RDS (Remote Data Service of Microsoft Data Access Components) service is running (http://xxx.xxx.48.196/msadc/msadcs.dll), and is vulnerable to attack. It allows an attacker to execute arbitrary commands on the server (qDefense can perform a demonstration upon request). **It is imperative that this be fixed as soon as possible.**

2.3.2
The IIS Samples are installed. Samples were found in the following directories:

```
/samples
/scripts/samples
/iissamples
/msadc/samples
```

(see Appendix C for a comprehensive list).

Many of the samples are vulnerable to attack, allowing an attacker to execute arbitrary commands on the server or to access restricted files. As per Microsoft's recommendations, samples should NEVER be installed on a production server.

2.3.3
The `//IISADMPWD` virtual directory is installed. It contains files which can be used as proxies for brute force password attacks, or to identify valid users on the system.

2.3.4
FrontPage extensions are installed on the server, at the following URL's:
`http://xxx.xxx.48.196/_vti_inf.html`
`http://xxx.xxx.48.196/_vti_log`
`http://xxx.xxx.48.196/_vti_txt`
`http://xxx.xxx.48.196/_vti_cnf`
`http://xxx.xxx.48.196/_vti_pvt`
`http://xxx.xxx.48.196/_vti_bin/_vti_aut/dvwssr.dll` *
`http://xxx.xxx.48.196/_vti_bin/fpcount.exe`

(see Appendix C)

Many of these extensions have security issues. The URL marked with an asterisk has a major security issue: a possible buffer overflow that allows an attacker to execute arbitrary commands on the server (see http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0260). In general, unless FrontPage is being used, the extensions should be removed.

2.3.5
The `imagemap.exe` program is installed (at URL `http://xxx.xxx.48.196/cgi-bin/imagemap.exe`). Certain versions of this program contain buffer overflows that allow an attacker to execute arbitrary commands on the server. If this program is not being used, it should be removed. Otherwise, contact the vendor for an updated version. Note: imagemap is not a Microsoft product.

Please see Appendix C for a specific list of problem URL's discovered.
Please see Appendix B for recommendations as to how to secure IIS 4.0.

2.4

Host: xxx.xxx.48.197
Names: wts.xxxcounty.com
xxxxxxx-6.yyyy.net
System: Microsoft Windows 2000
Function: Citrix Server
Services Accessible from the Internet:

HTTP	tcp/80	Citrix Web PN Server
Citrix	tcp/1494	Citrix ICA Server (apparently MetaFrame)

No vulnerabilities were discovered.

Some versions of Citrix Servers are vulnerable to denial of service attacks. These vulnerabilities were not tested for, as testing could lead to a denial of service. See the Citrix website (http://knowledgebase.citrix.com/cgi-bin/webcgi.exe?New,KB=CitrixKB,Case=obj(16435)) for more information.

2.5

Host: xxx.xxx.48.205
Name: xxxxxxx-14.yyyy.net

The firewall allows tcp traffic (ports 20, 21, 25, 80, 110, 443, and 1494) to reach this host. However, the host does not have any services accessible; all of the above ports are closed.

2.6

Host: xxx.xxx.48.208
Names: wtsfarm.xxxcounty.com
xxxxxxx-17.yyyy.net
System: Microsoft Windows 2000
Function: Citrix Server
Services Accessible from the Internet:

HTTP	tcp/80	Citrix Web PN Server
Citrix	tcp/1494	Citrix ICA Server (apparently MetaFrame)

No vulnerabilities were discovered.

Some versions of Citrix Servers are vulnerable to denial of service attacks. These vulnerabilities were not tested for, as testing could lead to a denial of service. See the Citrix website (http://knowledgebase.citrix.com/cgi-bin/webcgi.exe?New,KB=CitrixKB,Case=obj(16435)) for more information.

Appendix A: Testing Methodology

Although the details of the methodology employed are proprietary, it consists of five phases:

A.1 Host Detection

Hosts accessible on the network are searched for, using ping sweeps, TCP SYN scans, DNS records, and other methods.

A.2 Host Identification

Once discovered, hosts are analyzed, to determine system, function, and accessible services. Port scanning, OS fingerprinting, DNS records, and other methods are used.

A.3 Vulnerability Identification

The hosts are then checked for any vulnerabilities relevant to their system/services. The methods used to check for vulnerabilities differ with each type of vulnerability.

A.4 Analysis

The analyst reviews the information gathered. If he suspects false positives or false negatives, or notes ambiguities, he may probe further using methods of his discretion.

A.5 Recommendation

The analyst then sorts the information gathered, and draws conclusions. He notes vulnerabilities discovered, and offers recommendations as how to eliminate them.

Appendix B: Recommended Procedure to Secure Microsoft IIS 4.0

B.1 Remove MDAC RDS

> **UNTIL THIS IS DONE, AN ATTACKER MAY EXECUTE ARBITRARY COMMANDS ON THE SERVER (IN ITS CURRENT CONFIGURATION).**
>
> The following is excerpted from the Microsoft IIS 4.0 Security Checklist:
> (http://www.microsoft.com/technet/security/tools/iischk.asp?frame=true#IIS13)
>
> Disable RDS support
>
> This is an extremely important setting.
>
> When incorrectly configured, Remote Data Services can make a server vulnerable to denial of service and arbitrary code execution attacks. You should either remove the capability or restrict its usage using ACLs. Refer to MS98-004, MS99-025 and Q184375 for more info.

B.2 Remove all sample applications

> **MANY OF THE SAMPLE APPLICATIONS CURRENTLY INSTALLED ARE VULNERABLE TO ATTACKS.**
>
> The following is excerpted from the Microsoft IIS 4.0 Security Checklist:
> (http://www.microsoft.com/technet/security/tools/iischk.asp?frame=true#IIS1)
>
> Disable or remove all sample applications
>
> Samples are just that, samples, they are not installed by default and should never be installed on a production server. This includes documentation (the SDK docs include sample code), the Exploration Air sample site and others. Here are the default locations for some of the samples:
>
> IIS: c:\inetpub\iissamples
> IIS SDK: c:\inetpub\iissamples\sdk
> Admin Scripts: c:\inetpub\AdminScripts
> Data access: c:\Program Files\Common Files\System\msadc\Samples

B.3 Install Windows NT 4.0 Service Pack 6a

> This service pack fixes many bugs in IIS that result in insecurities. See
> http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp.

B.4 Install Security Rollup Package (SRP) for Windows NT 4.0

> This fixes 22 additional insecurities in IIS discovered since the release of Service Pack 6a. See
> http://www.microsoft.com/ntserver/nts/downloads/critical/q299444/default.asp.

B.5 Remove the IISADMPWD virtual directory

> The following is excerpted from the Microsoft IIS 4.0 Security Checklist:
> (http://www.microsoft.com/technet/security/tools/iischk.asp?frame=true#IIS15)
>
> Remove the IISADMPWD virtual directory

This directory allows you to reset Windows NT passwords, it is designed primarily for intranet scenarios. It should be removed if this feature is not required or if the server is on the Web. Refer to Q184619 for more info about this functionality.

Note: The above procedures are urgent. Until they are performed, the server is decidely insecure. The following procedures, although not of the same degree of urgency, are recommended to increase security.

B.7 Remove FrontPage extensions, unless they are being used. They have a history of poor security.

B.8 Read up on the Security Bulletins that Microsoft has issued for IIS 4.0. They are available on the Microsoft website:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp?productid=16&servicepackid=0&submit1=go.

B.9 Subscribe to the Microsoft Security Notification Service. This will keep you informed of future security issues discovered in IIS. To subscribe, send an e-mail to securbas@microsoft.com.

B.10 Consider using the IIS Lockdown Tool, freely available from Microsoft (see http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33961).

From the Microsoft promotional literature:
IIS Lockdown Wizard version 2.1 works by turning off unnecessary features, thus reducing attack surface available to attackers. To provide multiple layers of protection against attackers, URLscan, with customized templates for each supported server role, is integrated into the IIS Lockdown Wizard.

B.11 Consider manually removing unused IIS Script Mappings.

The following is excerpted from the Microsoft IIS 4.0 Security Checklist:
(http://www.microsoft.com/technet/security/tools/iischk.asp?frame=true#IIS20)

Remove Unused Script Mappings

IIS is preconfigured to support common filename extensions such as .ASP and .SHTM. When IIS receives a request for a file of one of these types the call is handled by a DLL. If you don't use some of these extensions or functionality you should remove the mappings by open Internet Services Manager then right-clicking the Web server, Properties, Master Properties, WWW Service, Edit, HomeDirectory, Configuration and remove these references:

If you don't use:	Remove this entry:
Web-based Password Reset	.htr
Index Server	.ida
Internet Database Connector (new Web sites don't use this, they use ADO from Active Server Pages)	.idc
Server-side includes	.shtm, .stm, .shtml

B.12 See the Microsoft IIS 4.0 Security Checklist (http://www.microsoft.com/technet/security/tools/iischk.asp) for additional recommendations.

Appendix C: Problem URL's found on host 2.3 (IP Address xxx.xxx.48.196)

Note: Inclusion on this list does necessarily indicate a vulnerability. This appendix is provided only as a reference for the system administrator or a security technician.

This appendix has been deleted from the sample report.