Documentation Forms for Penetration Tests

The reports in this appendix will give you a good idea of what security testers do and how they should present findings to managers and IT personnel. The sample reports show how methodical a security tester must be and emphasize that nothing should be overlooked or assumed to be unimportant. Security testers must consider all factors that might affect the security of a business.

The two reports in this appendix are sample documents shared by ISECOM. Few organizations give examples of documentation for a security test, so these reports will be extremely helpful. Some material in the reports might be beyond the scope of information covered in this book, but remember that you can delve into any areas in which you aren't well versed.

The first sample report is an executive summary usually given to management staff, who typically aren't interested in all the details of a security test. Instead, they want a summary of important areas that they can read over quickly to get the bottom line. For these people, you need to emphasize what problems were found and how they can be fixed. The second sample is the technical report that would most likely be given to IT personnel. This type of report includes details of vulnerabilities and exploits as well as possible solutions for the identified problems.

Clients who hire security professionals to assess their organizations want a report that details what was found and offers recommendations to help protect their resources. Documentation—the task most IT professionals hate—is probably the most important part of a security professional's job. When a team is used to conduct a security test, the person most skilled in report writing should handle creating these reports to management and IT staff.

Testing
Executive Summary

Client Company

Prepared for
John Smith

May 2003

Testing Company. 12456 Main Street Southside, MO 00000
Phone (888) 888-8888 Fax (888) 888-8889
http://www.testingco.com

Testing Company Logo

Table of Contents

Testing Company Logo

Limitations on Disclosure and Use

This document contains sensitive and confidential information concerning vulnerabilities within Client's 193.145.85.0/24 DMZ Network, as well as methods for exploiting these vulnerabilities. Testing Company recommends that special precautions be taken to protect the confidentiality of the information contained in this report. Testing Company has securely retained a copy of the report for future Client reference. All subsequent copies of this report will be delivered by Testing Company to the appropriate Client representative.

While Testing Company is confident that the major security vulnerabilities of the target systems have been identified, there can be no assurance that an assessment of this nature will identify all possible security exposures. Additionally, the findings and recommendations presented in this document are based on the technologies and known threats as of the date of this report. As technologies and risks change over time, the vulnerabilities and the recommendations associated with the Client 193.145.85.0/24 DMZ Network, may also change.

Testing Company Logo

Executive Summary

Testing Overview

In an effort to assess the security of Client's presence on the Internet, Client requested that Testing Company perform Testing service against those systems supporting the Client 193.145.85.0/24 DMZ Network. The purpose of the Testing service was to identify network-level security weaknesses that may be exploited from the Internet.

The Testing service was performed via the Internet from Testing Company's security labs located in Southside, MO between 10-9-2003 and 11-11-2003. All vulnerabilities identified, as well as any security concerns encountered, were communicated to Client contact John Smith throughout the Testing service process.

Testing was limited to the target networks and IP addresses specifically, and did not include any third-party networks or systems that were out of the immediate scope of the project. Furthermore, Testing Company did not perform any Denial of Service (DoS) based attacks against the target systems.

Processes and Techniques

Testing Company's consultants rely on vetted testing practices to determine how susceptible a Client's network is to security exposure. These testing practices have been continuously developed over a period of years and are constantly refined to better represent the threats facing a business's Internet presence.

Testing Company uses various scanning products that have been recognized as industry standards, including Retina by eEye, CANVAS by ImmunitySec, and Nessus by the Security Community. A variety of scanners are used so that the Testing service is not bias to one product and the results are not restricted to the findings of one individual vendor. Testing Company also incorporates what are considered industry standard testing tools into its testing process, such as scanrand, nikto, netcat, and other tools made by security testers for security testers. In addition to using tools that are publicly available, Testing Company's consultants have a variety of testing tools, scripts and processes that have been developed in-house or in conjunction with the Institute for Security and Open Methodologies (ISECOM).

Testing Company implements a multi-phased testing process that is designed to test for all known vulnerabilities, as well as the discovery of unknown vulnerabilities within custom configurations. This multi-phased testing process allows Testing Company to be "self-checking", ensuring that its consultants have thoroughly identified all apparent vulnerabilities.

Testing Company implements separate testing processes for each type of Testing service it offers, including external network testing, internal network testing and web application testing. Each process is specifically designed to target the type of service being performed and implements the best testing practices available.

While performing the Testing service, Testing Company consultants assume the role of an attacker by portraying a "think outside of the box" mindset. This approach allows Testing Company to provide a more accurate representation of the threats an environment is susceptible to. Testing Company uses ISECOM's Open Source Security Testing Methodology Manual (OSSTMM) as the base methodology for all Testing engagements.

Risks

During the security assessment, Testing Company discovered various vulnerabilities and security concerns relating to the 193.145.85.0/24 DMZ Network. It is important to note that the vulnerabilities documented in this report reflect the conditions of the 193.145.85.0/24 DMZ Network at the time of the Testing service and do not necessarily reflect current conditions.

Below is a table highlighting the risks identified during this assessment. Each risk is associated with a Risk Assessment Value that classifies its degree of exposure. For additional details concerning these risks and their associated recommendations, please refer to the appropriate pages of the technical reports.

System	Service	RAV	TR Page
193.145.85.22	Email	Vulnerability – Identified – 1.6	11
193.145.85.43	File Transfer	Weakness – Verified – 1.6	21
	Remote Control	Weakness – Verified – 1.6	21
	Website	Weakness – Verified – 1.6	22
193.145.85.44	Website	Vulnerability – Identified – 1.6	23
193.145.85.58	DNS	Weakness – Verified – 1.6	23
193.145.85.59	DNS	Weakness – Verified – 1.6	24
	DNS	Vulnerability – Identified – 1.6	24
193.145.85.72	Website	Vulnerability – Identified – 1.6	28
	Remote Control	Weakness – Verified – 1.6	28
193.145.85.79	Website	Vulnerability – Identified – 1.6	31

Testing Company Logo

System	Service	RAV	TR Page
193.145.85.90	DNS	Vulnerability – Identified – 1.6	33
	DNS	Weakness – Verified – 1.6	33
193.145.85.91	DNS	Weakness – Verified – 1.6	34
193.145.85.100	File Transfer	Vulnerability – Identified – 1.6	35
193.145.85.150	File Transfer	Vulnerability – Identified – 1.6	36

About Testing Company

Testing Company markets Information Security Protection and Security Education services to large and medium-sized businesses worldwide.

Questions or comments regarding this Testing service, the contents of this report, or Testing Company should be directed to Mike Jones (mike.jones@testingco.com) at (888) 888-8888. Additionally, please visit our website at http://www.testingco.com.

Section
1 Introduction

At the request of Client, Testing Company performed a Testing service of Client's 193.145.85.0/24 DMZ Network. The objective of this Testing service was to determine the overall security of the 193.145.85.0/24 DMZ Network. The security assessment performed was focused on the target systems identified in the Section 1.1. These results are not intended to be an overall assessment of all Client hosts, but only of those systems that fell within the scope of this project.

The Testing service was performed via the Internet from Testing Company's security labs located in Southside, MO between October 9th 2003 and November 11th 2003. All vulnerabilities identified, as well as any security concerns encountered, were communicated to Client employee John Smith throughout the Testing service process.

This testing did not attempt any active Denial of Service (DoS) attacks. In some cases, however, it may be possible to determine if a host is susceptible to a DoS attack without performing the attack itself.

1.1 Target Systems

The following table displays the target systems and networks identified for this network test. Each of the identified systems were tested with all three stages of Testing Company's standard network-level Testing service process (see Section 1.2).

IP Address/Netmask	Host/Network Name	Host/Network Description
193.145.85.0/24	Client DMZ	This is the main DMZ network for Client.
193.145.85.22	mail2.school.mo.us.	Linux 2.4/2.6 (NAT)
193.145.85.23	listserv.school.mo.us.	Windows 2000 SP4, XP SP1
193.145.85.25	Relay.school.mo.us.	NAVGW on NT
193.145.85.28	Sped.school.mo.us.	Mac OS9
193.145.85.29	is.school.mo.us.	Windows NT
193.145.85.33	Clientschools.org.	Mac OS9
193.145.85.36	techctr-backup.school.mo.us.	Microsoft Windows Server 2003 Enterprise Edition, Microsoft Windows 2000 SP3
193.145.85.37	web.school.mo.us.	Windows 2000
193.145.85.38	uxy38.school.mo.us.	Windows 2000

193.145.85.39	193.145.85.39	Mac? (No up ports, only down, Web and Timbuktu)
193.145.85.43	uxy43.school.mo.us.	Polycom Viewstation 512 – Software 7.0.3
193.145.85.44	classrooms.school.mo.us.	Windows
193.145.85.48	uxy48.school.mo.us.	Mac? (No up ports, only down, ftp, web, Frame Maker, Timbuktu)
193.145.85.58	ns1.school.mo.us.	Windows? (no response on any TCP port)
193.145.85.59	ns2.school.mo.us.	Windows? (no response on any TCP port)
193.145.85.68	support.school.mo.us., dap.school.mo.us.	Windows 2000
193.145.85.72	register.school.mo.us.	Windows 2000 (why TS & VNC on same box?)
193.145.85.79	ysystems.com.	Windows 2000
193.145.85.80	uxy80.school.mo.us.	Ridgeway IP Freedom?
193.145.85.90	dns1.Clientschools.org.	Windows? (No response on any TCP port)
193.145.85.91	dns2.Clientschools.org.	Windows? (No response on any TCP port)
193.145.85.100	uxy100.school.mo.us.	Windows 2000
193.145.85.150	web.school.mo.us.	Windows 2000
193.145.85.248	uxy248.school.mo.us.	Mac? (Weird DNS server, not Bind)
193.145.85.251	mail.school.mo.us.	Windows NT 4.0
193.145.84.206	MO.cust-rtr.bigcablemodem.net.	Cisco 801/1720 router running IOS 12.2.8, Cisco router running IOS 12.2(8)T

1.2 Tools & Techniques

For each network-level penetration test, Testing Company follows a robust, peer-reviewed methodology to ensure a complete and accurate security assessment. This documented process includes three individual stages of testing. Each stage utilizes commercial scanners, freely available tools, public resources, and proprietary tools and procedures. Below is a description of each of the stages performed by Testing Company during a network test.

Stage I - Discovery

The first stage of a network-level Testing service is devoted to information gathering and discovery. In this stage, Testing Company will attempt to gather all publicly available information concerning the target environment. This includes:

examining DNS records (both authoritative and non-authoritative), querying various whois servers, utilizing standard network utilities such as ping and traceroute, and analyzing the BGP tables of various backbone Internet routers.

After researching and recording the public information concerning the target environment, Testing Company attempts to map the network architecture of the target systems. This includes attempting to identify any filtering devices, i.e. firewalls or routers, which protect the environment, as well as, recording the various routes to the individual targets. To accomplish this mapping of the target environment, Testing Company used TCP, UDP, and ICMP echo request sweeps, lft, sing, dig, and several other tools designed to perform various queries that flush out live hosts.

Stage II - Enumeration

In the second stage of a network-level Testing service, Testing Company utilizes the information and hosts discovered in Stage I to enumerate specific host configurations and settings. This includes identifying any open TCP and UDP services, detecting, if possible, the software version of the open services and operating systems, and the purpose of the host, i.e. firewall, mail server, DNS server, web server etc. In addition, Testing Company will attempt to ascertain, through experience and research, if the software versions of the services or operating systems are vulnerable to remote exploitation.

To determine the open TCP and UDP ports, Testing Company performs a sweep of all 65,535 TCP ports and attempts protocol specific requests against the most commonly used and exploited UDP ports. Please refer to Appendix A for the complete list of open TCP and UDP services for each target system. Testing Company utilizes several different techniques to identify the software version of the services and operating systems of each target host. These include: OS detection through examination of network packets, system configuration and feedback profiling, and banner grabbing.

During this stage of a network-level Testing service, Testing Company uses various commercial, publicly available, and in-house developed proprietary tools. These include, but are not limited to:

- Retina by eEye

- CANVAS by Immunitysec
- Nessus by Renaud Deraison
- Sing by Alfredo Andres
- Nmap by Fyodor
- Scanrand by Dan Kaminsky

Stage III - Exploitation

The third and final stage of a network-level Testing service is the exploitation phase. In this stage Testing Company will attempt to exploit any vulnerabilities or weaknesses discovered during Stage II. The goal of this stage is to obtain user-level or privileged-level access on the target systems. Typical methods of gaining system-level access include successful brute force attacks or the execution of buffer overflow exploits. If access is obtained, Testing Company will attempt to further penetrate all systems and networks connected to the compromised host. The purpose of this continued penetration is to test the security controls in place to protect confidential assets from compromised systems. Additionally, this test demonstrates the depth of exposure of the target network after one of the hosts has been compromised. Testing Company will immediately alert the appropriate representative if any host is compromised during the Testing service.

Denial-of-Service (DoS)

DoS attacks are special tests designed to determine the susceptibility of a target system or network to unauthorized malicious downtime. Testing Company has accumulated a large database of various DoS programs and methods. These programs range from ICMP DoS attacks, such as smurf, to network flooding DoS attacks, such as SYN Floods. Testing Company does not perform a DoS attack unless specifically requested. In the event that a DoS attack is requested, a time-window will be agreed upon and the DoS attack will only occur during this time period.

1.3 Risk Classification

In Section 2.0 of this document, Testing Company presents all of the vulnerabilities that were discovered during this security assessment. Each of these vulnerabilities has been organized into four different severity classifications: Severe-Risk, Moderate-

Risk, Minimal-Risk, and Security Concerns. Below is a brief definition of each of the four severity categories.

Vulnerability

A flaw inherent in the security mechanism itself or which can be reached through security safeguards that allows for privileged access to the location, people, business processes, and people or remote access to business processes, people, infrastructure, and/or corruption or deletion of data.

A vulnerability may be a metal in a gate which becomes brittle below 0° C, a thumbprint reader which will grant access with rubber fingers, an infrared device that has no authentication mechanism to make configuration changes, or a translation error in a web server which allows for the identification of a bank account holder through an account number.

Weakness

A flaw inherent in the platform or environment of which a security mechanism resides in – a misconfiguration, survivability fault, usability fault, or failure to meet the requirements of the Security Posture. A weakness may be a process which does not save transaction data for the legal time limit as established by regional laws, a door alarm which does not sound if the door is left open for a given amount of time, a firewall which returns ICMP host unreachable messages for internal network systems, a database server that allows unfiltered queries, or an unlocked, unmonitored entrance into a otherwise secured building.

Information Leak

A flaw inherent in the security mechanism itself or which can be reached through security safeguards which allow for privileged access to privileged or sensitive information concerning data, business processes, people, or infrastructure.

An information leak may be a lock with the combination available through audible signs of change within the lock's mechanisms, a router providing SNMP information about the target network, a spreadsheet of executive salaries for a private company, the private mobile telephone number of the marketing staff, or a website with the next review date of an organization's elevators.

Concern

A security issue which may result from not following best practices however does not yet currently exist as a danger.

A concern may be FINGERD running on a server for an organization that has no business need for the FINGER service, a guarded doorway which requires the watchman to leave the door to apprehend a trespasser with no new guard to replace the one who left and maintain a presence at the door, or employees who sit with their monitors and whiteboards viewable from outside the perimeter security.

Unknowns

An unidentifiable or unknown element in the security mechanism itself or which can be reached through security safeguards that currently has no known impact on security as it tends to make no sense or serve any purpose with the limited information the tester has.

An unknown may be an unexpected response possibly from a router in a network that is repeatable and may indicate network problems, an unnatural radio frequency emanating from an area within the secure perimeter however offers no identification or information, or a spreadsheet which contains private data about a competing company.

1.4 Risk Assessment Values

In addition to the risk classifications described above in Section 1.3, Testing Company has associated a Risk Assessment Value for every risk discovered during this security assessment.

	Verified	Identified
Vulnerability	.032	.016
Weakness	.016	0.008
Concern	0.008	0.004
Information Leak	0.004	0.002
Unknown	0.002	0.001

1.5 Use of this Report

The remainder of this document has been organized into the following sections.

Section 2 – Risks & Recommendations

In this section, Testing Company describes the findings and recommendations associated with the 193.145.85.0/24 DMZ Network that was tested during this Testing service. The findings and recommendations have been divided into two different categories: **Vulnerability** & **Weakness.** Risks classified as **Concern, Information Leak** or **Unknown** will be mentioned only in the companion technical document. Please refer to Section 1.3 on page 10 for detailed explanations of these categories.

Section 3 - Concluding Remarks

In this final section, Testing Company presents the concluding remarks concerning the 193.145.85.0/24 DMZ Network. This includes a brief recap of the risks and recommendations, comments on the security of the environment, and a summary of the Testing service.

Appendix A – Open TCP Ports

In Appendix A, Testing Company has supplied Client with the raw output from the port scans performed during the security assessment. The output will highlight the TCP ports currently and historically open on all of the network devices tested during this assessment. Please refer to Section 1.1 for additional details of the target systems for this Testing service.

Testing Company Logo

Section

2 Risks & Recommendations

The Risks & Resolutions section of this document highlights all of the risks and security concerns identified during the assessment of the Client 193.145.85.0/24 DMZ Network. Each risk will have a Risk Assessment Value (see Section 1.4), a list of the vulnerable systems, a discussion, and a recommendation. The discussion is a brief description of how Testing Company was able to identify this particular risk and what affect it has on the security of the system and the rest of the environment, inserting text and screen captures where appropriate. Finally, the recommendation section will contain Testing Company's recommendations for eliminating the respective vulnerability. These recommendations are based on years of information security experience and extensive research.

2.1 Vulnerability

In this section, Testing Company has documented the **Severe-Risk** vulnerabilities associated with the Client 193.145.85.0/24 DMZ Network. **Severe-Risk** vulnerabilities are the most critical findings and may pose a serious, immediate threat to your information assets. All **Severe-Risk** vulnerabilities should be remedied as soon as possible.

2.1.1 Sendmail Buffer Overflows

Relevancy: Identified

Vulnerable Systems: 193.145.85.22

Impact

According to the Fingerprint and the banners shown, this version of Sendmail is vulnerable to many different buffer overflows. There are also a few minor local information leaks with this version. Either way, please consider updating to a newer non-vulnerable version.

CVE : CAN-2002-1337, CVE-2001-1349

Recommendation

Upgrade to Sendmail 8.12.10. (http://www.sendmail.org/)

2.1.2 shtml.dll–Frontpage Extensions 2000 & 2002

Relevancy: Identified

Vulnerable Systems: 193.145.85.44, 193.145.85.72

Impact

Did not validate this, but it seems that this machine is vulnerable to a flaw in the shtml.dll file that can allow a remote attacker the ability to run arbitrary code. This affects both Frontpage Server Extensions 2000 and 2002.

Recommendation

Install the appropriate Microsoft hotfix.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-053.asp

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q329085

See page 28 of the Technical Report for more information.

2.1.3 Bind 9.2.2rc1 Buffer Overflow

Relevancy: Identified

Vulnerable Systems: 193.145.85.59

Impact

This version of bind (based solely on the reported revision number) is known to be vulnerable to a buffer overflow which may allow an attacker to gain a shell on this host or disrupt access to this server (DoS).

Recommendation

If this indeed is a problem, then upgrade to bind 9.2.3 (http://www.isc.org/products/BIND/) or downgrade to the 8.x series. This may not be a problem for you if you're running bind on a windows platform as this specific vulnerability is tied to the GNU DNS resolver library as part of glibc.

2.1.4 Bind 9.2.2rc1 Buffer Overflow

Relevancy: Identified

Vulnerable Systems: 193.145.85.59

Impact

This version of bind (based solely on the reported revision number) is known to be vulnerable to a buffer overflow which may allow an attacker to gain a shell on this host or disrupt access to this server (DoS).

Recommendation

If this indeed is a problem, then upgrade to bind 9.2.3 (http://www.isc.org/products/BIND/) or downgrade to the 8.x series. This may not be a problem for you if you're running bind on a windows platform as this specific vulnerability is tied to the GNU DNS resolver library as part of glibc.

2.1.5 Allaire ColdFusion DoS

Relevancy: Identified

Vulnerable Systems: 193.145.85.79

Impact

Due to a faulty mechanism in the password parsing implementation in authentication requests, it is possible to launch a denial of service attack against Allaire ColdFusion 4.5.1 or previous by inputting a string of over 40 000 characters to the password field in the Administrator login page. CPU utilization could reach up to 100%, bringing the program to halt. The default form for the login page would prevent such an attack. However, a malicious user could download the form locally to their hard drive, modify HTML tag fields, and be able to submit the 40 000 character string to the ColdFusion Server.

Recommendation

Workaround:

Back up all existing data and implement the steps outlined in the following knowledge base article:

http://www.macromedia.com/support/coldfusion/ts/documents/tn17254.htm

http://www.macromedia.com/v1/cfdocs/allaire_support/adminsecurity.htm

2.1.6 Bind 8.2.5-REL Buffer Overflow

Relevancy: Identified

Vulnerable Systems: 193.145.85.90

Impact

Remote shells and DoS.
http://www.securityfocus.com/bid/6160/discussion/
http://xforce.iss.net/xforce/xfdb/10333

When a DNS lookup is requested on a non-existent sub-domain of a valid domain and an OPT resource record with a large UDP payload is attached, the server may fail.

Recommendation

Upgrade to 8.4.1 or 9.2.3

http://www.isc.org/products/BIND/bind8.html

http://www.isc.org/products/BIND/

2.1.7 MS FTP DoS

Relevancy: Identified

Vulnerable Systems: 193.145.85.100

Impact

Based on the version in the banner, it may be possible to crash the ftp server (DoS). This would only be possible after logging in, which would require a valid username/password.

Recommendation

Apply relevant hotfix:

http://www.microsoft.com/technet/security/bulletin/ms02-018.asp

Microsoft Patch Q319733 IIS 5.0

http://download.microsoft.com/download/iis50/Patch/Q319733/NT5/EN-US/Q319733_W2K_SP3_X86_EN.exe

2.1.8 Rumpus FTP DoS

Relevancy: Identified

Vulnerable Systems: 193.145.85.150

Impact

The remote system may be vulnerable to one or more remote buffer overflow attacks.

Recommendation

Contact Rumpus http://www.maxum.com/Rumpus/ for more information.

2.2 Weakness

In this section, Testing Company has documented the **Weakness** risks associated with the Client 193.145.85.0/24 DMZ Network.

2.2.1 FTP Default Password

Relevancy: Verified

Vulnerable Systems: 193.145.85.43

Impact

The FTP server allows logging in as user admin or administrator with any password combination.

Once logged in as an admin level account, you can read files, write files, reboot the device, and update the firmware on the device.

Recommendation

Restrict access to this port at the firewall. Change the admin and administrator passwords.

2.2.2 Telnet Default Password

Relevancy: Verified

Vulnerable Systems: 193.145.85.43

Impact

You can obtain and modify configurations on port 23 and port 24 without being prompted for authentication

Recommendation

Restrict access to these ports at the firewall.

2.2.3 WWW Default Password

Relevancy: Verified

Vulnerable Systems: 193.145.85.43

Impact

Through the admin and administrator accounts on the website you can view and modify the configuration. You can make long distance calls. You can also wipe the logs.

Recommendation

Restrict access to this port at the firewall.

2.2.4 Recursive DNS

Relevancy: Verified

Vulnerable Systems: 193.145.85.58, 193.145.85.59, 193.145.85.90, 193.145.85.91, 193.145.85.248

Impact

This DNS server is allowing recursive queries from the outside. This would allow an attacker to poison the DNS servers local cache. The next victim to request that information may be unknowingly directed to the attackers site.

Recommendation

Disable recursive queries for those outside of the Client IP space.

2.2.5 VNC Enabled

Relevancy: Verified

Vulnerable Systems: 193.145.85.72

Impact

There is a VNC server running on this host. VNC (Virtual Network Computing) allows remote users to control the host machine as though they were physically at the terminal.

VNC is not encrypted in its default form, and authentication is not a part of the Windows standard authentication. There is no username, only a password which can be brute forced.

It's very odd to see VNC and TS running on the same machine, as it's twice the administrative load to properly secure.

Recommendation

Disable VNC.

If you must run VNC, limit access to it with firewall ACL's.

Section

3 Concluding Remarks

This analysis is based on known threats as of the date of this report. Testing Company recommends that the actions suggested for identified risks be applied as quickly as possible.

All in all we found that the current security posture for the systems within the scope was in decent shape from an external point of view. Although, as with most networks we've tested, there is room for improvement. After Client has implemented the changes suggested in this document and the companion technical report, we recommend that Client contact Testing Company for a follow on retest to verify that the suggested changes were made.

Testing Company has appreciated this opportunity to perform the Testing service for Client. We hope that the information contained in these documents is of benefit to your organization. As Client security related needs arise again in the future, it would be our pleasure to serve you again. For more information about our services, please contact our Sales Staff at (888) 888-8888, or visit our website (http://www.testingco.com).

Appendix A: Open TCP Ports

In this appendix, Testing Company has inserted the raw results of the port scans performed against the target systems listed in Section 1.1. For each target host, the list of open TCP ports has been attached. All open ports should be closely examined for their business purpose. Unnecessary open ports should be disabled to avoid any additional vulnerability exposures.

<removed for anonymity>

Testing
Technical Report

Client Company

Prepared for

John Smith

November 12, 2003

Domains xxx.mo.us Clientschools.org ysystems.com Clientonline.com	**Subdomain.Domain.Root** School.mo.us
Principal Services File transfer, Remote administration, Email, Web pages, Database, Video Conferencing, Routing, Unknown, VoIP	**Protocol, Port, Service** FTP, 21, File Transfer Telnet, 23, Remote Administration Telnet, 24, Remote Administration SMTP, 25, Email DNS, 53, Domain Name Service HTTP, 80, Web Timbuktu, 407, Timbuktu HTTP, 591, Filemaker Database
Number of Domains 5	
IP Addresses 193.145.85.1-254, 2193.145.84.206	**IP (types of system)** T1, 1 class C, one boarder GW router.
Gateway Routers 2193.145.84.206	**IP (physical location)** Client Organization 200 Broad Street Richland, MO 00000-0000 US (UNITED STATES)
Number of Visible Systems	20
Primary Operating Systems	OS Name Linux, Windows, Mac OS 9,Windows NT, Windows 2000 (XP?)
Firewall Could not determine	**IP, OS, type** Inline? Could not determine
IDS Could not determine	**IP, OS, type** Could not determine
Web Technologies	**IP** **Technology** 193.145.85.100Microsoft-IIS/5.0 WebLogic Server 8.x 193.145.85.150 Down 11/6/2003 193.145.85.23 Tcl-Webserver/3.4.2 193.145.85.28 WebSTAR/3.0 193.145.85.33 WebSTAR/4.4(SSL) 193.145.85.37 Microsoft-IIS/5.0 193.145.85.44 Says Microsoft-IIS/5.0, might be Microsoft-IIS/4.0 193.145.85.68 Microsoft-IIS/5.0 193.145.85.72 Microsoft-IIS/5.0 ASP.NET 193.145.85.79 Microsoft-IIS/5.0 193.145.85.43 Polycom Viewstation 512 Administrative Web GUI

ISP One primary	**Name, Address, website** MO Internet Services 111 Street St. #5000 City, Mo, 12345 http://www.mointernetservice.net
Test Conditions	**Hops** 10,11,15 **Speed** 120kB/s downloading from websites **Restrictions** Many networking changes throughout testing cycle

Notes

Overall, not bad. There is definitely room for improvement, but we've seen far worse☺. Keep your eye out for anything .8 and higher. The 0.0-0.4 is nit picky, but if you have time, fix those too.

We look forward to working with you again soon. If anything is unclear, please don't hesitate to drop us a line via email or phone.

Testing Team

Document Grinding Assessment

Persons Discovered

person	telephone	e-mail
John xxx		john@School.mo.us
		board @School.mo.us
Lucy xxx	(888) 888-1234	lucy@School.mo.us, lucy_2@School.mo.us
		joe@School.mo.us
Kris xxx		kris @School.mo.us
Susan xxx	(888) 888-2345, (456) 888-XXXX	susan@School.mo.us, susan_2@access.xxx.mo.us
Suey xxx		suey_2@School.mo.us
		pam@School.mo.us
		beth@XXX.us
Scott xxx	(888) 888-3456	scott_2@School.mo.us
John xxx	Ext 4567	john_2@School.mo.us, john @School.mo.us
John xxx	Ext 5678	John_xxx@School.mo.us
Winnona xxx	(888) 888-7890	winnona_xxx@School.mo.us
Joseph xxx	(888) 888-8901	Jo.xxx@School.mo.us
Ariel xxx		ariel_xxx@access.xxx.mo.us
Carl xxx		carl_xxx@access.xxx.mo.us
Kassandra xxx		kassandra.xxx@School.mo.us
Greg xxx		greg_xxx@School.mo.us
Luis xxx	Ext 123	
Fiona xxx	Ext 234	
Charles xxx	Ext 345	
Jessica xxx	Ext 456	
Helpdesks	Ext 222, 333, 444, 555, 666	

External Postings

Link	description
http://www.School.mo.us/directory.html	Who should we call first?
http://groups.google.com/groups?q= 1	Old networking problem
http://www.another.net/cs/pt/view/eg_e/1332	National Board Certification General Meeting
http://www.another.net/cs/pt/view/eg_e/1319	National Board Certification Support Network
http://www.sssss.edu/ed174/resources/information_forms/ informational_handouts/ Info_Bhasha.doc	SUBJECT EXAMINATIONS
http://www.xxxxxxx.com/sgro	Hobby
http://wwwstatic.xxx.org/gems/Mtg.Minutes.htm	BUSINESS AND ADMINISTRATION STEERING COMMITTEE (BASC

http://wwwstatic.xxx.org/gems/Minutes.htm	BUSINESS AND ADMINISTRATION STEERING COMMITTEE (BASC)
www.xxx.org/docs/	Great Technology To Enhance Language Arts
http://www.xxx.org/xxx/lists/rre/Networks	Ancient Post for John

Systems and Technologies	
Technology name	**description or link to information**
Linux	http://www.linux.org – Free operating system
Windows	http://www.microsoft.com – Commercial Operating System
Mac	http://www.apple.com – Commercial Operation System
Polycom Viewstation 512	http://www.polycom.com/products_services/0,1816,pw-4353-4430,00.html – Video Conferencing
WebLogic	http://www.bea.com/framework.jsp?CNT=index.htm&FP=/content/products/server
Tcl-Webserver – Lyris List Manager	http://www.lyris.com/products/listmanager/lm_flyer.pdf
WebStar	http://www.4d.com/products/webstar.html
IIS	http://www.microsoft.com/WindowsServer2003/iis/default.mspx
Elluminate	http://www.elluminate.com/ – Virtual Classroom
WebQuota	http://www.flicks.com/msystems/webquota/ – Advanced Authentication controls
Coldfusion	http://www.macromedia.com/software/coldfusion/
Rumpus	http://www.maxum.com/Rumpus/ – FTPD for the Mac
MacHTTP	http://www.machttp.org/ – the original Web server for Macintosh

E-mail Header
Header Information

```
Return-Path: <>
Received: from mail.School.mo.us ([193.145.85.251] verified)
  by xxx.xxx.net (PicoOS Mailserv SMTP 5.5.5)
  with ESMTP id 670434 for lsl@xxx.com; Fri, 07 Nov 2003 01:20:18 -0800
X-MIMETrack: Itemize by SMTP Server on mail/xxx/CLIENT(Release 5.0.10 |March 22, 2002)
at
 11/07/2003 01:11:54 AM,
            Serialize by Router on mail/xxx/CLIENT(Release 5.0.10 |March 22, 2002) at
 11/07/2003 01:11:54 AM,
            Serialize complete at 11/07/2003 01:11:54 AM
From: Postmaster@School.mo.us
Date: Fri, 7 Nov 2003 01:11:54 -0800
Message-ID: <OFB3D1E476.86C1FD7A-ON88256DD7.0032872A@School.mo.us>
MIME-Version: 1.0
Subject: DELIVERY FAILURE: User xxx (xxx@School.mo.us) not listed in
 public Name & Address Book
To: lsl@xxx.com
Content-Type: multipart/report; report-type=delivery-status;
boundary="==IFJRGLKFGIR419UHRUHIHD"

=-=-=-=-=-=-=-=-=
Return-Path: <lyris-noreply@listserv.School.mo.us>
Received: from listserv.School.mo.us ([193.145.85.23] verified)
  by xxx.xxx.net (PicoOS Mailserv SMTP 5.5.5)
  with SMTP id 670426 for root@xxx.com; Fri, 07 Nov 2003 00:46:21 -0800
Message-Id: <LYRIS0-1068194735--1540-lyris-noreply@listserv.School.mo.us>
X-lyris-type: command-notify
From: "Lyris ListManager" <lyris-noreply@listserv.School.mo.us>
Reply-To: "Lyris ListManager" <lyris-noreply@listserv.School.mo.us>
To: root@xxx.com
Subject: Re: your help request
Date: Fri, 07 Nov 2003 00:45:35 -0800
```

Network Profile

IP ranges to be tested and details of these ranges
193.145.85.1-254 – CLIENT Class C 193.145.84.206 – Border GW Router

Domain information and configurations

user64x248.School.mo.us. 193.145.85.248
Resolved xxx.in-addr.arpa and xxx.in-addr.arpa into Clientonline.com.
This is a very curious name server. It only responds for two IP addresses in this range.
It returns non-authoritive for all lookups (recursive queries allowed) except for other reverse lookups in this IP space.

=-=-=-=-=-=

DNS1.CLIENTSCHOOLS.ORG 193.145.85.90
Bind: 8.2.5-REL

=-=-=-=-=-=

DNS2.CLIENTSCHOOLS.ORG 193.145.85.91
Bind: 9.2.2

=-=-=-=-=-=

NS1.SCHOOL.MO.US 193.145.85.58
Bind: 8.4.1-REL

=-=-=-=-=-=

NS2.SCHOOL.MO.US 193.145.85.59
Bind: 9.2.2rc1

Zone Transfer Highlights

193.145.85.248
None allowed

=-=-=-=-=-=

DNS1.CLIENTSCHOOLS.ORG 193.145.85.90
None allowed

=-=-=-=-=-=

DNS2.CLIENTSCHOOLS.ORG 193.145.85.91
None allowed

=-=-=-=-=-=

NS1.SCHOOL.MO.US 193.145.85.58
None allowed

=-=-=-=-=-=

NS2.SCHOOL.MO.US 193.145.85.59
None allowed

Server List

IP Address/Netmask	Host/Network Name	Host/Network Description
193.145.85.0/24	Client DMZ	This is the main DMZ network for Client.
193.145.85.22	mail2.school.mo.us.	Linux 2.4/2.6 (NAT)
193.145.85.23	listserv.school.mo.us.	Windows 2000 SP4, XP SP1

193.145.85.25	Relay.school.mo.us.	NAVGW on NT
193.145.85.28	Sped.school.mo.us.	Mac OS9
193.145.85.29	is.school.mo.us.	Windows NT
193.145.85.33	Clientschools.org.	Mac OS9
193.145.85.36	techctr-backup.school.mo.us.	Microsoft Windows Server 2003 Enterprise Edition, Microsoft Windows 2000 SP3
193.145.85.37	web.school.mo.us.	Windows 2000
193.145.85.38	user64x38.school.mo.us.	Windows 2000
193.145.85.39	193.145.85.39	Mac? (No up ports, only down, Web and Timbuktu)
193.145.85.43	user64x43.school.mo.us.	Polycom Viewstation 512 – Software 7.0.3
193.145.85.44	classrooms.school.mo.us.	Windows
193.145.85.48	user64x48.school.mo.us.	Mac? (No up ports, only down, ftp, web, Frame Maker, Timbuktu)
193.145.85.58	ns1.school.mo.us.	Windows? (no response on any TCP port)
193.145.85.59	ns2.school.mo.us.	Windows? (no response on any TCP port)
193.145.85.68	support.school.mo.us., dap.school.mo.us.	Windows 2000
193.145.85.72	register.school.mo.us.	Windows 2000 (why TS & VNC on same box?)
193.145.85.79	ysystems.com.	Windows 2000
193.145.85.80	user64x80.school.mo.us.	Ridgeway IP Freedom?
193.145.85.90	dns1.Clientschools.org.	Windows? (No response on any TCP port)
193.145.85.91	dns2.Clientschools.org.	Windows? (No response on any TCP port)
193.145.85.100	user64x100.school.mo.us.	Windows 2000
193.145.85.150	web.school.mo.us.	Windows 2000
193.145.85.248	user64x248.school.mo.us.	Mac? (Weird DNS server, not Bind)
193.145.85.251	mail.school.mo.us.	Windows NT 4.0
193.145.84.206	MO.cust-rtr.bigcablemodem.net.	Cisco 801/1720 router running IOS 12.2.8, Cisco router running IOS 12.2(8)T

Document Grinding

Primary Contacts	John Smith	
Method of Contact	**Phone** (888) 888-8888	**Email** John_Smith@School.mo.us

Organizational Information	
Business Name	Client Company
Business Address	200 Broad Street Richland, MO 00000-0000 US (UNITED STATES)
Business Telephone	(888) 888-8888
Business Fax	(888) 888-8889
Line of Business	Customer services

IP Information	
Domain Names	School.mo.us xxx.mo.us Clientschools.org ysystems.com Clientonline.com

Network Blocks	209.76.0.0/14
Network Block Owner	MO Cable Internet Services
Records Created	1997-04-29
Records Last Updated	2001-09-26

Email Information	
Email Server Addresses	5 relay.School.mo.us. 10 mail.School.mo.us. 20 infoserv.School.mo.us. 20 listserv.School.mo.us. 25 mail2.School.mo.us. 25 newsletter.School.mo.us.
Email Server Types	relay.School.mo.us. Norton Antivirus GW? mail.School.mo.us. Lotus Domino Release 5.0.10-6.0.1CF1 infoserv.School.mo.us. <Dead>? listserv.School.mo.us. MailShield (Lyris Email) mail2.School.mo.us. Sendmail 8.11.6/8.11.6 - 8.12.2-8.12.5? newsletter.School.mo.us. <Dead>?
Email Clients	Notes
Email System	Lotus Domino/Notes
Email Address Standard	Firstname.lastname@domain Firstname_lastname@domain FirstinitialLastname@domain
E-mail Footer	None
Encryption / Standard	None
Bounced mails	The linux email server doesn't bounce email, nor does it forward them. The main mail server (relay) sends all email after processing it to the main lotus notes server (mail). That machine will bounce email back. The listserv also bounces email back.

Web Information	
Website Address	193.145.85.23 listserv.School.mo.us. 193.145.85.28 sped.School.mo.us. 193.145.85.33 www.Clientschools.org. 193.145.85.37 tegrityweb.School.mo.us. 193.145.85.43 user64x43.School.mo.us. 193.145.85.44 classrooms.School.mo.us. 193.145.85.68 ctap.School.mo.us. 193.145.85.72 register.School.mo.us. 193.145.85.79 www.ysystems.com.

Web Server Type	193.145.85.23 Tcl-Webserver/3.4.2 193.145.85.28 WebSTAR/3.0 193.145.85.33 WebSTAR/4.4(SSL) 193.145.85.37 Microsoft-IIS/5.0 193.145.85.44 Says Microsoft-IIS/5.0, might be Microsoft-IIS/4.0 193.145.85.68 Microsoft-IIS/5.0 193.145.85.72 Microsoft-IIS/5.0 ASP.NET 193.145.85.79 Microsoft-IIS/5.0 193.145.85.100 Microsoft-IIS/5.0 WebLogic Server 8.x 193.145.85.150 Down 11/6/2003 193.145.85.43 Polycom Viewstation 512 Administrative Web GUI
Server Locations	Client Company 200 Broad Street Richland, MO 00000-0000 US (UNITED STATES)
Technologies Used	Asp, Coldfusion, Frontpage, Weblogic
Encryption standards	None in use
Web-Enabled Languages	Java

Name Services	
Primary (Authoritative) Name Server	ns1.School.mo.us.
Secondary	ns2.School.mo.us.
Additional Name Servers	193.145.85.248 DNS1.CLIENTSCHOOLS.ORG DNS2.CLIENTSCHOOLS.ORG

Firewall Information	
Firewall Address	Unknown
Firewall Type	Inline Pix FW?
IDS system	Unknown

Routing Information	
Router Addresses	2193.145.84.206
Router Types	Cisco
Router Capabilities	

Server Information

IP Address	domain name
193.145.85.22	mail2.School.mo.us.

Hop	Port	Protocol	Service	Service Details
11	25	SMTP	Sendmail 8.12.2-8.12.5	25 on priority (tied for last)

Banner(s):

Port	Protocol	Banner
11	SMTP	220 mail2.School.mo.us ESMTP Sendmail 8.11.6/8.11.6; Fri, 7 Nov 2003 07:18:34 -0800

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
AF224E1E D58A928A EEF2CEF3 D2CC66FE ED5DAF25 EEFB4754
IPID Sequence Generation
Incremental
Uptime
337 hours (or just over 14 days)

Concern or Vulnerability
Vulnerability – Identified – 1.6 According to the Fingerprint and the banners shown, this version of Sendmail is vulnerable to many different buffer overflows. There are also a few minor local information leaks with this version. Either way, please consider updating to a newer non-vulnerable version. CVE : CAN-2002-1337, CVE-2001-1349
Example
For example, if you had working exploit code (see http://packetstormsecurity.nl/), you could in theory obtain remote root access to the box.
Solution
Upgrade to Sendmail 8.12.10. (http://www.sendmail.org/)

Concern or Vulnerability
Information Leak – Verified – .4 Based on the current configuration it is possible to enumerate local system accounts.
Example
Telnet to 193.145.85.22 on port 25 220 mail2.School.mo.us ESMTP Sendmail 8.11.6/8.11.6; Fri, 7 Nov 2003 07:32:17 -0800 helo foo 250 mail2.School.mo.us Hello xxx.xxx.net [193.145.84.43], pleased to meet you mail from: test@test.com 250 2.1.0 test@test.com... Sender ok rcpt to: rooot@mail2.School.mo.us 550 5.1.1 rooot@mail2.School.mo.us... User unknown rcpt to: root@mail2.School.mo.us 250 2.1.5 root@mail2.School.mo.us... Recipient ok
Solution

Create a "Catch all" virtual user table. See http://www.sendmail.org/virtual-hosting.html for more information.

Concern or Vulnerability
Information Leak – Verified – .4 When you connect to 193.145.85.22 on TCP port 25, 193.145.85.22 send a tcp syn packet to your host on tcp port 113. This allows for "passive" OS fingerprinting.
Example
telnet 193.145.85.22 25 =-=-=-=-=-= 193.145.85.22:2632 - Linux 2.4/2.6 (NAT!) (up: 338 hrs) -> 193.145.84.43:113 (distance 11, link: GPRS or FreeS/WAN)
Solution
Disable the IdentD check in sendmail. See the online sendmail documentation at http://www.sendmail.org

Concern or Vulnerability
Information Leak – Verified – .4 This system allows for Information Leakage. We are able to obtain system information remotely, such as uptime, etc.
Example
nmap –P0 -O 193.145.85.22 -p25 (see http://groups.google.com/groups?q=ICMP+linux+uptime+netcraft&hl=en&lr=&ie=UTF-8&oe=UTF-8&selm=4yUY5.4218%24TU6.379536%40ptah.visi.com&rnum=1 and http://www.insecure.org/nmap/ for more information)
Solution
Because this test relies on the characteristics of the packets rather than any data inside the packet, it's subject to failure if there is a firewall or filtering router in between the server and the outside world.

IP Address	**domain name**
193.145.85.23	listserv.School.mo.us.

Hop	**Port**	**Protocol**	**Service**	**Service Details**
11	25	SMTP	Lyris ListManager	MailShield SMTP server for ListManager software http://www.lyris.com/products/listmanager/
11	80	HTTP	Lyris Webserver	Web interface to Lyris ListManager software

Banner(s):

Port	**Protocol**	**Banner**
25	SMTP	220 listserv.School.mo.us ESMTP Lyris ListManager service ready
80	HTTP	Tcl-Webserver/3.4.2 September 3, 2002

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
649CCE60 5A901405 85077E1A 73995316 3C77D84D 36CFECAF
IPID Sequence Generation
Incremental
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
Weakness – Identified – .8 Allows for brute force login attempts
Example
http://listserv.School.mo.us/
Solution
Consult with 4D and implement attempt lockouts thresholds.

Concern or Vulnerability
Information Leak – Verified – .4 Remote users are able to get the statistics for the web interface. This will help them know which URL's are most commonly accessed.
Example
http://193.145.85.23/status/
Solution
Reconfigure Lyris ListServ to disallow access to that directory

Concern or Vulnerability
Information Leak – Verified – .4 Bounced messages make the server connect to attackers machine. The "passive" fingerprinting methods used in tools such as p0f (http://www.stearns.org/p0f/) are far more accurate than in "active" fingerprinting tools such as nmap, xprobe2, etc. If you can get the mail server to bounce email to an IP of your choice, you can use "passive" fingerprinting to map the OS.
Example

xxx.xxx:~/jobs/Client/Phase 2/Nameserver# nc 193.145.85.23 25
220 listserv.School.mo.us ESMTP Lyris ListManager service ready
helo foo
250 listserv.School.mo.us Hello foo [193.145.84.43], pleased to meet you
mail from: test@193.145.84.43
250 < test@193.145.84.43>... Sender ok
rcpt to: lyris@listserv.School.mo.us
250 < lyris@listserv.School.mo.us>... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Subject: help me
1
2
3
.
2
50 518 Message accepted for delivery.

=-=-=-=-=-=
193.145.85.23:14362 - Windows 2000 SP4, XP SP1 -> 193.145.84.43:25 (distance 11, link: GPRS or FreeS/WAN)

Solution
This is a nit-picky vulnerability. The business justifications to allow a bounce message might outweigh the need to block bounces

IP Address	**domain name**
193.145.85.25	relay.School.mo.us.

Hop	**Port**	**Protocol**	**Service**	**Service Details**
11	25	SMTP	Norton Antivirus Gateway	This service scrubs email before passing it to the Lotus Notes server

Banner(s):

Port	**Protocol**	**Banner**
25	SMTP	220 relay.School.mo.us SMTP; Fri, 07 Nov 2003 07:15:58 -0800

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
DAC37A60 A3293DCC B9510BBC FAE67E91 B54288AE B1F479CA
IPID Sequence Generation
Broken little-endian incremental
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
No concerns currently
Example
n/a
Solution

IP Address	domain name
193.145.85.28	sped.School.mo.us.

Hop	Port	Protocol	Service	Service Details
11	80	HTTP	WebSTAR Webserver	Simple webserver

Banner(s):

Port	Protocol	Banner
80	HTTP	WebSTAR/3.0 ID/59734

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
98574FDC AE31A86A 52B32D3A 4C50D1AB 9B547615 48E0F13F
IPID Sequence Generation
Broken little-endian incremental
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
Weakness – Identified – .8 The admin and log protected areas are protected with basic authentication with no apparent lock out feature. This means that given enough time, these accounts will be brute forced.
Example
Get a copy of http://www.hoobie.net/brutus/ and throw it at this server. http://193.145.85.28/pi_admin.admin http://sped.School.mo.us/webstar.log http://sped.School.mo.us/logs/webstar.log Go take a walk ☺.
Solution
Contact 4D for a solution.

IP Address	domain name
193.145.85.29	is.School.mo.us

Hop	Port	Protocol	Service	Service Details
11	80	HTTP	IIS Webserver	IS "Internal" Server?

Banner(s):

Port	Protocol	Banner
80	HTTP	Microsoft-IIS/4.0

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
5C66B382 935A476A 7B3DD619 76365366 8E0EC76E 55C8DF4B
IPID Sequence Generation
Incremental
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
Weakness – Identified – .8 This allows an attacker to be able to bruteforce login and password attempts to the Front Page Extension Authoring interface. With enough time an attacker could potentially access the authoring portion of Front Page and deface your website.
Example
http://is.School.mo.us/_vti_bin/_vti_aut/author.dll
Solution
Consider disallowing public access to this url.

IP Address	**domain name**
193.145.85.33	www.Clientschools.org. School.mo.us. Clientschools.org. www.School.mo.us.

Hop	**Port**	**Protocol**	**Service**	**Service Details**
11	21	FTP	File transfer	Mac ftp
11	80	HTTP	Website	Mac webserver
11	591	HTTP	FileMaker Pro	File Maker Pro webserver
11	1417	Timbuktu	Remote Administration	Closed
11	1418	Timbuktu	Remote Administration	Closed
11	1419	Timbuktu	Remote Administration	Closed
11	1420	Timbuktu	Remote Administration	Closed
11	8080	HTTP	Web Cache Proxy	Closed

Banner(s):

Port	**Protocol**	**Banner**
21	FTP	220-Welcome to the CLIENT Web server 220 Service ready for new user
80	HTTP	WebSTAR/4.4(SSL) ID/73202
591	HTTP	FileMakerPro/4.0

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
F7F9CA69 715FCCF E00C6489 17DFCACC B8DB4507 C260272D
IPID Sequence Generation
Busy server or unknown class
Uptime
Up since Tue Nov 4 03:36:05 2003

Concerns and Vulnerabilities:

Concern or Vulnerability
Weakness – Identified – .8 The admin and log protected areas are protected with basic authentication with no apparent lock out feature. This means that given enough time, these accounts will be brute forced.
Example

Get a copy of http://www.hoobie.net/brutus/ and throw it at this server. http://193.145.85.33/pi_admin.admin Go take a walk ☺.
Solution
Contact 4D for a solution.

Concern or Vulnerability
Concern – Verified – .8 This url gives up information about the internal IP scheme (10.94.1.75)
Example
http://www.School.mo.us/docushare/
Solution
Fix this link on the server.

Concern or Vulnerability
Concern – Verified – .8 There are "closed" ports. Because everything else is filtered (firewalled), to see a closed port means that the firewall allows those connections through even though the OS isn't listening for any connections
Example
Send a syn packet to 193.145.85.33 on port 1417. You'll get a tcp rst back showing that the port is closed. If it were open you would get a syn ack. If it were filtered (firewalled) you would get nothing back.
Solution
Update your firewall to filter those ports.

Concern or Vulnerability
Concern – Verified – .8 You are allowing FTP sessions. The username, password, and all data sent over FTP are not encrypted by the protocol.
Example
Open up a packet analyzer (Like Ethereal http://www.ethereal.com/) and collect the data as you transfer files to 193.145.85.33 over ftp.
Solution
Migrate to sftp or scp (part of the SSH suite).

Concern or Vulnerability
Information Leak – Verified – .4 The FileMakerPro access is currently showing demo databases. These don't seem to have any business justifiable reason to be on there.
Example
http://193.145.85.33:591/
Solution
Remove the demo content, or restrict access to this port all together.

IP Address	**domain name**
193.145.85.36	Techctr-backup.School.mo.us.

Hop	**Port**	**Protocol**	**Service**	**Service Details**
11	3389	RDP	Remote admin.	Microsoft Remote Desktop Protocol for Terminal Server

Banner(s):

Port	Protocol	Banner
3389	RDP	

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
DAD4274A 55703E9 A9E993C2 1B6BAB5A 9FFA4E40 103C1B4A
IPID Sequence Generation
Incremental
Uptime
Not Available

Concerns and Vulnerabilities:

Concern or Vulnerability
Concern – Verified – .8 There is a Terminal Services remote desktop server running on this host. TS/RDP allows remote users to control the host machine as though they were physically at the terminal. The username and password can be brute forced.
Example
http://www.microsoft.com/windowsxp/pro/downloads/rdClientdl.asp http://www.hammerofgod.com/download/tsgrinder-2.03.zip
Solution
Disable Terminal Services if you don't need it. If you must run Terminal Services, limit access to it with firewall ACL's.

IP Address	domain name
193.145.85.37	tegrityweb.School.mo.us.

Hop	Port	Protocol	Service	Service Details
11	80	http	Website	No site comes up.
11	1417	Timbuktu	Remote Admin	Should be filtered
11	1418	Timbuktu	Remote Admin	Closed
11	1419	Timbuktu	Remote Admin	Closed
11	1420	Timbuktu	Remote Admin	Closed

Banner(s):

Port	Protocol	Banner
80	HTTP	Microsoft-IIS/5.0
1417	Timbuktu	

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
7567D129 CD0DBB5F 74F788B8 902ED12B 8A28CD62 B7D562CD
IPID Sequence Generation
Incremental

Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
Concern – Verified – .8 There are "closed" ports. Because everything else is filtered (firewalled), to see a closed port means that the firewall allows those connections through even though the OS isn't listening for any connections
Example
Send a syn packet to 193.145.85.37 on port 1418. You'll get a tcp rst back showing that the port is closed. If it were open you would get a syn ack. If it were filtered (firewalled) you would get nothing back.
Solution
Update your firewall to filter those ports.

Concern or Vulnerability
Concern – Identified – .4 If you make a Timbuktu remote administrative shell open to the world it can be brute forced.
Example
Play with http://www.macanalysis.com/download.php3
Solution
All remote administrator shells should be limited either via Firewall rule-sets or via VPN's.

Concern or Vulnerability
Concern – Identified – .4 Another brute force opportunity.
Example
http://tegrityweb.School.mo.us./printers
Solution
Consider restricting access to this URL

Concern or Vulnerability
Unknown – Verified – .2 If there is not supposed to be a website on this server why have that port open?
Example
http://193.145.85.37/ comes up with error 403 Forbidden
Solution
Put up a website, or filter this port at the firewall.

IP Address	domain name
193.145.85.38	user64x38.School.mo.us.

Hop	Port	Protocol	Service	Service Details
11	21	FTP	File transfer	Non-encrypted, non-anonymous

Banner(s):

Port	Protocol	Banner
21	FTP	220 TEGRITYWEB Microsoft FTP Service (Version 5.0).

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
5C0B4F6B 9E02BC10 D86853DB 85FA0380 7ABBF049 B3E281EE

IPID Sequence Generation
Busy server or unknown class
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
Concern – Verified – .8 You are allowing FTP sessions. The username, password, and all data sent over FTP are not encrypted by the protocol.
Example
Open up a packet analyzer (Like Ethereal http://www.ethereal.com/) and collect the data as you transfer files to 193.145.85.38 over ftp.
Solution
Migrate to sftp or scp (part of the SSH suite).

IP Address	**domain name**
193.145.85.43	user64x43.School.mo.us.

Hop	**Port**	**Protocol**	**Service**	**Service Details**
15	21	FTP	File Transfer	Non-anonymous, non-encrypted
15	23	TELNET	Remote Administration	Non-encrypted, non-authenticated
15	24	TELNET	Remote Administration	Non-encrypted, non-authenticated
15	80	HTTP	Remote Administration Website	Non-encrypted, null password for admin and administrator
15	1720	NetMeeting	Chat, collaboration	Not-filtered
15	5001	UNKNOWN	Video Conferencing	UNKNOWN
15	5003	UNKNOWN	Video Conferencing	UNKNOWN
15	5004	UNKNOWN	Video Conferencing	UNKNOWN
15	All others	n/a	n/a	Closed

Banner(s):

Port	**Protocol**	**Banner**
21	FTP	220 FTP Server, type ‘quote help’ for help

23	TELNET	Hi, my name is : Client company Here is what I know about myself: Serial Number: 001573 Brand: Polycom Software Version: Release 7.0.3 - 21 Aug 2001 Model: VS Network Interface: ISDN_QUAD_BRI MP Enabled: No H323 Enabled: Yes IP Address: 193.145.85.43 Time In Last Call: 0:01:44 Total Time In Calls: 190:48:52 Total Calls: 924 Switch Type: NI-1 Country Code: 1 Area Code: 714 Client company Client company ISDN 1 a is: 4444063 SPID 1 a is: 71444440630101 ISDN 1 b is: 4441327 SPID 1 b is: 71444413270101 ISDN 2 a is: 4444960 SPID 2 a is: 71444449600101 ISDN 2 b is: 4441463 SPID 2 b is: 71444414630101 ISDN 3 a is: 4444066 SPID 3 a is: 71444440660101 ISDN 3 b is: 4441721 SPID 3 b is: 71444417210101
24	TELNET	Hi, my name is : Client company Here is what I know about myself: Serial Number: 001573 Brand: Polycom Software Version: Release 7.0.3 - 21 Aug 2001 Model: VS Network Interface: ISDN_QUAD_BRI MP Enabled: No H323 Enabled: Yes IP Address: 193.145.85.43 Time In Last Call: 0:01:44 Total Time In Calls: 190:48:52 Total Calls: 924 Switch Type: NI-1 Country Code: 1 Area Code: 714 ISDN 1 a is: 4444063 SPID 1 a is: 71444440630101 ISDN 1 b is: 4441327 SPID 1 b is: 71444413270101 ISDN 2 a is: 4444960 SPID 2 a is: 71444449600101 ISDN 2 b is: 4441463 SPID 2 b is: 71444414630101 ISDN 3 a is: 4444066 SPID 3 a is: 71444440660101 ISDN 3 b is: 4441721 SPID 3 b is: 71444417210101

80	HTTP	Viavideo-Web
1720	NetMeeting	
5001	UNKNOWN	
5003	UNKNOWN	
5004	UNKNOWN	

Concerns and Vulnerabilities:

Concern or Vulnerability
Weakness – Verified – 1.6 The FTP server allows logging in as user admin or administrator with any password combination. Once logged in as an admin level account, you can read files, write files, reboot the device, and update the firmware on the device.
Example
Connected to 193.145.85.43. 220 FTP Server, type 'quote help' for help Name (193.145.85.43:root): admin 331 User name okay, need password. Password: 230 User logged in, proceed. Remote system type is UNIX. ftp> quote help 214- Usage from FTP ls - directory listing bin - set image mode for put get filename - read file from ffs put filename - write file to ffs del filename - delete file in ffs quote swup - set software update mode quote boot - reboot 214 end of help
Solution
Restrict access to this port at the firewall. Change the admin and administrator passwords.

Concern or Vulnerability
Weakness – Verified – 1.6 You can obtain and modify configurations on port 23 and port 24 without being prompted for authentication
Example
telnet 193.145.85.43 23 Or telnet 193.145.85.43 24
Solution
Restrict access to these ports at the firewall.

Concern or Vulnerability
Weakness – Verified – 1.6 Through the admin and administrator accounts on the website you can view and modify the configuration. You can make long distance calls. You can also wipe the logs.
Example
Visit http://193.145.85.43/a_adminindex.htm Login: admin Password:
Solution

Restrict access to this port at the firewall. Change the admin and administrator account passwords.

Concern or Vulnerability
Concern – Verified – .8 Anyone can establish a netmeeting connection to 193.145.85.43:1720
Example
Open Netmeeting. Connect to 193.145.85.43
Solution
Restrict access to this port.

Concern or Vulnerability
Concern – Verified – .8 You are allowing FTP sessions. The username, password, and all data sent over FTP are not encrypted by the protocol.
Example
Open up a packet analyzer (Like Ethereal http://www.ethereal.com/) and collect the data as you transfer files to 193.145.85.43 over ftp.
Solution
Migrate to sftp or scp (part of the SSH suite).

Concern or Vulnerability
Unknown – Identified – .1 Not sure what ports 5001, 5003, and 5004 are used for. Find out and determine if they need to be world accessible.
Example
Visit http://www.polycom.com/products_services/0,1816,pw-4353-4430,00.html Grab the documentation files.
Solution
Restrict access to this port.

IP Address	**domain name**
193.145.85.44	Classrooms.School.mo.us.

Hop	**Port**	**Protocol**	**Service**	**Service Details**
11	80	http	Website	Allows students to navigate to the virtual classrooms
11	2187	JINX	Virtual Classroom	Java based
11	2188	JINX	Virtual Classroom	Java based

Banner(s):

Port	**Protocol**	**Banner**
80	HTTP	Microsoft-IIS/5.0
2187	JINX	400 Goodbye
2188	JINX	400 Goodbye

TCP Sequencing:

TCP Sequence Prediction
Class=truly random

TCP ISN Seq. Numbers
F379BDC7 E52C7DD1 381FEC4C 21BBD424 2AF4241D DD83F25C
IPID Sequence Generation
Incremental
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
Vulnerability – Identified – 1.6 Did not validate this, but it seems that this machine is vulnerable to a flaw in the shtml.dll file that can allow a remote attacker the ability to run arbitrary code. This affects both Frontpage Server Extensions 2000 and 2002.
Example
Solution
Install the appropriate Microsoft hotfix. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-053.asp http://support.microsoft.com/default.aspx?scid=kb;en-us;Q329085

Concern or Vulnerability
Concern – Identified – .4 The authentication over port 2187-2188 are not encrypted.
Example
Open up a packet analyzer (Like Ethereal http://www.ethereal.com/) and collect the data as you authenticate to 193.145.85.44 over the Java interface.
Solution
Contact Elluminate – http://www.elluminate.com/

IP Address	**domain name**
193.145.85.58	ns1.School.mo.us.

Hop	**Port**	**Protocol**	**Service**	**Service Details**
11	53(UDP)	DNS	Domain Name Service	Primary nameserver for School.mo.us domain.

Banner(s):

Port	**Protocol**	**Banner**
53	DNS	8.4.1-REL

Concerns and Vulnerabilities:

Concern or Vulnerability
Weakness – Verified – 1.6 This DNS server is allowing recursive queries from the outside. This would allow an attacker to poison the DNS servers local cache. The next victim to request that information may be unknowingly directed to the attackers site.
Example
http://www.giac.org/practical/gsec/Doug_Sax_GSEC.pdf http://www.cert.org/advisories/CA-1997-22.html
Solution
Disable recursive queries for those outside of the CLIENT IP space.

IP Address	**Domain name**

193.145.85.59	ns2.School.mo.us.

Hop	Port	Protocol	Service	Service Details
11	53(UDP)	DNS	Domain Name Service	Secondary nameserver for School.mo.us domain.

Banner(s):

Port	Protocol	Banner
53	DNS	9.2.2rc1

Concerns and Vulnerabilities:

Concern or Vulnerability
Weakness – Verified – 1.6 This DNS server is allowing recursive queries from the outside. This would allow an attacker to poison the DNS servers local cache. The next victim to request that information may be unknowingly directed to the attackers site.
Example
http://www.giac.org/practical/gsec/Doug_Sax_GSEC.pdf http://www.cert.org/advisories/CA-1997-22.html
Solution
Disable recursive queries for those outside of the CLIENT IP space.

Concern or Vulnerability
Vulnerability – Identified – 1.6 This version of bind (based solely on the reported revision number) is known to be vulnerable to a buffer overflow which may allow an attacker to gain a shell on this host or disrupt access to this server (DoS).
Example
http://www.cert.org/advisories/CA-2002-19.html http://cert.uni-stuttgart.de/archive/bugtraq/2003/03/msg00075.html http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0684
Solution
If this indeed is a problem, then upgrade to bind 9.2.3 (http://www.isc.org/products/BIND/) or downgrade to the 8.x series. This may not be a problem for you if you're running bind on a windows platform as this specific vulnerability is tied to the GNU DNS resolver library as part of glibc.

IP Address	domain name
193.145.85.68	ctap.School.mo.us. support.School.mo.us.

Hop	Port	Protocol	Service	Service Details
11	21	FTP	File Transfer	Non-anonymous
11	21	HTTP	Website	Getting Results
11	1417	Timbuktu	Remote Admin	Closed
11	1418	Timbuktu	Remote Admin	Closed
11	1419	Timbuktu	Remote Admin	Closed
11	1420	Timbuktu	Remote Admin	Closed

Banner(s):

Port	Protocol	Banner
21	FTP	220 vtserver Microsoft FTP Service (Version 5.0).
80	HTTP	Server: Microsoft-IIS/5.0 Content-Location: http://193.145.85.68/index.htm WebQuota Version 5.0f2: 8864247000 WebQuota Version 5.0f2: 8864247000 Date: Tue, 11 Nov 2003 05:28:48 GMT Content-Type: text/html Accept-Ranges: bytes Last-Modified: Thu, 21 Aug 2003 01:03:05 GMT ETag: "448d6efa7f67c31:89c" Content-Length: 5765

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
46ADBCA0 A9F8B4C 326D4CBD 1D10968B E636BC3B D1E76F71
IPID Sequence Generation
Incremental
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
Concern – Verified – .8 You are allowing FTP sessions. The username, password, and all data sent over FTP are not encrypted by the protocol.
Example
Open up a packet analyzer (Like Ethereal http://www.ethereal.com/) and collect the data as you transfer files to 193.145.85.68 over ftp.
Solution
Migrate to sftp or scp (part of the SSH suite).

Concern or Vulnerability
Weakness – Identified – .8 Internet Printing (IPP) is enabled, and there are other signs that show that ISAPI extensions are enabled. The system appears to be patched, but you could save yourself the headache of people trying to exploit things by disabling those features all together.
Example
http://193.145.85.68/NULL.printer
Solution
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-023.asp http://www.securityfocus.com/bid/2674

Concern or Vulnerability
Concern – Identified – .4 This webserver is configured to support the TRACE method. Attackers may abuse HTTP TRACE functionality to gain access to information in HTTP headers such as cookies and authentication data. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method
Example
http://www.kb.cert.org/vuls/id/867593 http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf

Solution
Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. The default configurations of Urlscan 2.5 (both baseline and SRP) only permit GET and HEAD methods.

Concern or Vulnerability
Information Leak – Verified – .4 It's possible to get the Coldfusion debug information from this server by calling for any cfm file (whether or not it exists) and appending ?mode=debug
Example
http://193.145.85.68/xxxxxx.cfm?mode=debug
Solution
As taken from http://www.macromedia.com/support/coldfusion/ts/documents/tn17642.htm 1. Go into Debugging IPs in the ColdFusion Administrator. 2. Go to the box that states: Restrict debug output to selected IP addresses. 3. Enter only one IP Address - 127.0.0.1. 4. Click Add. 5. Click Apply. 6. Restart ColdFusion.

Concern or Vulnerability
Information Leak – Verified – .4 Certain DOS reserved filenames, such as NUL or PRN, can cause Coldfusion to display the path to the web root directory in an error message.
Example
http://193.145.85.68/nul..cfm
Solution
Two solutions are available to prevent IIS from passing DOS reserved filenames to ColdFusion for processing. 1. Install and configure the Microsoft URLScan Security Tool 2. Change IIS properties to check that files exist See http://www.macromedia.com/v1/handlers/index.cfm?ID=22906 for more details.

Concern or Vulnerability
Information Leak – Verified – .4 Coldfusion 4.0-5.0 reveal file system paths of .cfm or .dbm files when the request contains invalid DOS devices.
Example
http://193.145.85.68/nul.dbm http://193.145.85.68/nul.cfm
Solution
Two solutions are available to prevent IIS from passing DOS reserved filenames to ColdFusion for processing. 1. Install and configure the Microsoft URLScan Security Tool 2. Change IIS properties to check that files exist See http://www.macromedia.com/v1/handlers/index.cfm?ID=22906 for more details.

Concern or Vulnerability
Information Leak – Verified – .4 Coldfusion 4.0-5.0 reveal file system paths of .cfm or .dbm files when the request contains invalid DOS devices.
Example

http://193.145.85.68/nul.dbm
http://193.145.85.68/nul.cfm

Solution

Two solutions are available to prevent IIS from passing DOS reserved filenames to ColdFusion for processing.

1. Install and configure the Microsoft URLScan Security Tool
2. Change IIS properties to check that files exist

See http://www.macromedia.com/v1/handlers/index.cfm?ID=22906 for more details.

Concern or Vulnerability

Concern – Identified – .4

It appears this system has WebDAV enabled. If this feature isn't being used, consider disabling it.

Example

```
OPTIONS * HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Tue, 11 Nov 2003 17:05:26 GMT
Content-Length: 0
Accept-Ranges: bytes
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL,
PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL,
PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Cache-Control: private
```

Solution

To disable WebDAV on IIS 5.0:
Create a DWORD registry value called "DisableWebDAV" in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters key, and set it to 1.

IP Address	domain name
193.145.85.72	register.School.mo.us

Hop	Port	Protocol	Service	Service Details
11	21	FTP	File Transfer	Allows anonymous ftp
11	80	HTTP	Website	"Under construction"
11	3389	RDP	Remote admin.	Microsoft Remote Desktop Protocol for Terminal Server http://www.microsoft.com/windowsxp/pro/downloads/rdClientdl.asp
11	5632	Status for PC Anywhere	http://www.symantec.com	Closed
11	5800	VNC	Remote admin.	http://www.uk.research.att.com/vnc - why RDP and VNC? Version RFB 003.003
11	5900	VNC	Remote admin.	http://www.uk.research.att.com/vnc why RDP and VNC? Version RFB 003.003

Banner(s):

Port	Protocol	Banner
21	FTP	220 register Microsoft FTP Service (Version 5.0)
80	HTTP	Microsoft-IIS/5.0
3389	RDP	Windows 2000 Server
5800	VNC	<APPLET CODE=vncviewer.class ARCHIVE=vncviewer.jar WIDTH=800 HEIGHT=632>

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
A95DAFD6 801268D2 91FD17E8 A1B56489 69E3E14C B3A64BA4
IPID Sequence Generation
Busy server or unknown class
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
Vulnerability – Identified – 1.6 A flaw in the shtml.dll file can allow a remote attacker the ability to run arbitrary code. This affects both Frontpage Server Extensions 2000 and 2002. The IIS server appears to have the .SHTML ISAPI filter mapped. At least one remote vulnerability has been discovered for the .SHTML filter. This is detailed in Microsoft Advisory MS02-018 and results in a denial of service access to the web server. It is recommended that even if you have patched this vulnerability that;you unmap the .SHTML extension, and any other unused ISAPI extensions if they are not required for the operation of your site. An attacker may use this flaw to prevent the remote service from working properly (DoS).
Example
Could not find working exploit code. This system may or may not be vulnerable to the issue.
Solution
Install patch: http://download.microsoft.com/download/FrontPage2002/fpse1002/1/W98NT42KMeXP/EN-US/fpse1002.exe Also see: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0692 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-053.asp http://www.microsoft.com/technet/security/bulletin/ms02-018.asp http://support.microsoft.com/default.aspx?scid=kb;en-us;Q329085 Also consider unmapping the shtml/shtm isapi filters. To unmap the .shtml extension: 1.Open Internet Services Manager. 2.Right-click the Web server choose Properties from the context menu. 3.Master Properties 4.Select WWW Service -> Edit -> HomeDirectory -> Configuration ;and remove the reference to .shtml/shtm and sht from the list.

Concern or Vulnerability

Weakness – Verified – 1.6 There is a VNC server running on this host. VNC (Virtual Network Computing) allows remote users to control the host machine as though they were physically at the terminal. VNC is not encrypted in its default form, and authentication is not a part of the Windows standard authentication. There is no username, only a password which can be brute forced. It's very odd to see VNC and TS running on the same machine, as it's twice the administrative load to properly secure.
Example
http://193.145.85.72:5800/ or download VNC Client from http://www.realvnc.com/ http://www.phenoelit.de/vncrack/
Solution
Disable VNC. If you must run VNC, limit access to it with firewall ACL's.

Concern or Vulnerability
Concern – Verified – .8 More brute force opportunities. Also worth noting I was able to create a student account and register for classes.
Example
http://register.School.mo.us/dev_supervisors.asp http://register.School.mo.us/dev_instructors.asp?action=login&caller=&routine=
Solution
Consider restricting public access to these URLs.

Concern or Vulnerability
Concern – Verified – .8 There is a Terminal Services remote desktop server running on this host. TS/RDP allows remote users to control the host machine as though they were physically at the terminal. The username and password can be brute forced. It's very odd to see VNC and TS running on the same machine.
Example
http://www.microsoft.com/windowsxp/pro/downloads/rdClientdl.asp http://www.hammerofgod.com/download/tsgrinder-2.03.zip
Solution
Disable Terminal Services if you don't need it. If you must run Terminal Services, limit access to it with firewall ACL's.

Concern or Vulnerability
Concern – Verified – .8 You are allowing FTP sessions. The username, password, and all data sent over FTP are not encrypted by the protocol. This system also allows for anonymous FTP access, although no write/mkdir permissions were enabled, and there were no files available to download.
Example

Open up a packet analyzer (Like Ethereal http://www.ethereal.com/) and collect the data as you transfer files to 193.145.85.72 over ftp.
Solution
Migrate to sftp or scp (part of the SSH suite).

Concern or Vulnerability
Weakness – Identified – .8 /xxxxx.htw - Server may be vulnerable to a Webhits.dll arbitrary file retrieval.
Example
Could not verify, and this is an old vulnerability. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-006.asp
Solution
Ensure Q252463i, Q252463a or Q251170 are installed installed. See http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-006.asp for more information.

Concern or Vulnerability
Concern – Identified – .4 It appears this system has WebDAV enabled. If this feature isn't being used, consider disabling it.
Example
OPTIONS * HTTP/1.0 HTTP/1.1 200 OK Server: Microsoft-IIS/5.0 Date: Tue, 11 Nov 2003 20:15:47 GMT Content-Length: 0 Accept-Ranges: bytes DASL: <DAV:sql> DAV: 1, 2 Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH Cache-Control: private
Solution
To disable WebDAV on IIS 5.0: Create a DWORD registry value called "DisableWebDAV" in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters key, and set it to 1.

Concern or Vulnerability
Concern – Identified – .4 This webserver is configured to support the TRACE method. Attackers may abuse HTTP TRACE functionality to gain access to information in HTTP headers such as cookies and authentication data. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method
Example
http://www.kb.cert.org/vuls/id/867593 http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf
Solution
Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. The default configurations of Urlscan 2.5 (both baseline and SRP) only permit GET and HEAD methods.

Concern or Vulnerability
Information Leak – Identified – .2 SQL injection is a technique for exploiting web applications that use Client-supplied data in SQL queries without stripping illegal characters first. This vulnerability can allow people to extract sensitive information from the server's database, and possibly even execute arbitrary commands.
Example
http://register.School.mo.us/events/DayView.asp?daterequest=10/6/2003&day=char%4039%41%2b%40SELECT
Solution
Contact Mediablend (www.Mediablend.com) for assistance in fixing the script.

Concern or Vulnerability
Information Leak – Identified – .2 SQL injection is a technique for exploiting web applications that use Client-supplied data in SQL queries without stripping illegal characters first. This vulnerability can allow people to extract sensitive information from the server's database, and possibly even execute arbitrary commands.
Example
http://register.School.mo.us/events/DayView.asp?daterequest=10/6/2003&day='http://register.School.mo.us/events/DayView.asp?daterequest=10/6/2003&day='
Solution
Contact Mediablend (www.Mediablend.com) for assistance in fixing the script.

IP Address	domain name
193.145.85.79	ysystems.com.

Hop	Port	Protocol	Service	Service Details
11	21	FTP	File Transfer	
11	80	HTTP	Website	Virtual Training
11	407	Timbuktu	Control port	Closed
11	1417	Timbuktu	Remote admin.	Timbuktu
11	1418	Timbuktu	Remote admin.	Closed
11	1419	Timbuktu	Remote admin.	Closed
11	1420	Timbuktu	Remote admin.	Closed

Banner(s):

Port	Protocol	Banner
21	FTP	
80	HTTP	Microsoft-IIS/5.0
3389	RDP	Windows 2000 Server
5800	VNC	<APPLET CODE=vncviewer.class ARCHIVE=vncviewer.jar WIDTH=800 HEIGHT=632>

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
A95DAFD6 801268D2 91FD17E8 A1B56489 69E3E14C B3A64BA4
IPID Sequence Generation
Busy server or unknown class
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability

Vulnerability – Identified – 1.6 Due to a faulty mechanism in the password parsing implementation in authentication requests, it is possible to launch a denial of service attack against Allaire ColdFusion 4.5.1 or previous by inputting a string of over 40 000 characters to the password field in the Administrator login page. CPU utilization could reach up to 100%, bringing the program to halt. The default form for the login page would prevent such an attack. However, a malicious user could download the form locally to their hard drive, modify HTML tag fields, and be able to submit the 40 000 character string to the ColdFusion Server. Restarting the application would be required in order to regain normal functionality. You appear to be running Coldfusion 4.5. This administrative login screen can also be brute forced.
Example
The Administrator login page can be typically accessed via: http://193.145.85.79/cfide/administrator/index.cfm Modify the field size and POST action in the HTML tags to allow for the input of a character string consisting of over 40 000 characters. Also play with Brutus (http://www.hoobie.net/brutus/)
Solution
Workaround: Back up all existing data and implement the steps outlined in the following knowledge base article: http://www.macromedia.com/support/coldfusion/ts/documents/tn17254.htm http://www.macromedia.com/v1/cfdocs/allaire_support/adminsecurity.htm

Concern or Vulnerability
Information Leak – Verified – .4 Several Coldfusion default directories are available. This can in some cases divulge exact versions of installed code.
Example
http://193.145.85.79/cfide/administrator/include/ http://193.145.85.79/CFIDE/administrator/docs/ http://193.145.85.79/CFIDE/administrator/images/
Solution
Ensure Q252463i, Q252463a or Q251170 are installed installed. See http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-006.asp for more information.

Concern or Vulnerability
Concern – Identified – .4 Another brute force availability.
Example
http://www.ysystems.com/youthsystems/admin/
Solution
Consider disallowing public access to this url.

Concern or Vulnerability
Concern – Identified – .4 It appears this system has WebDAV enabled. If this feature isn't being used, consider disabling it.
Example

OPTIONS * HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 12 Nov 2003 02:41:30 GMT
IISExport: This web site was exported using IIS Export v3.0
Content-Length: 0
Accept-Ranges: bytes
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Cache-Control: private

Solution

To disable WebDAV on IIS 5.0:
Create a DWORD registry value called "DisableWebDAV" in the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters key, and set it to 1.

Concern or Vulnerability

Concern – Identified – .4

This webserver is configured to support the TRACE method.
Attackers may abuse HTTP TRACE functionality to gain access to information in HTTP headers such as cookies and authentication data. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method

Example

http://www.kb.cert.org/vuls/id/867593
http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf

Solution

Use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. The default configurations of Urlscan 2.5 (both baseline and SRP) only permit GET and HEAD methods.

IP Address	Domain name
193.145.85.90	dns1.Clientschools.org

Hop	Port	Protocol	Service	Service Details
11	53(UDP)	DNS	Domain Name Service	Primary nameserver for Clientschools.org Bind on Windows

Banner(s):

Port	Protocol	Banner
53(UDP)	DNS	8.2.5-REL

Concerns and Vulnerabilities:

Concern or Vulnerability

Vulnerability – Identified – 1.6

There are several major vulnerabilities based on this version information.

Example

Remote shells and DoS. http://www.securityfocus.com/bid/6160/discussion/ http://xforce.iss.net/xforce/xfdb/10333 When a DNS lookup is requested on a non-existent sub-domain of a valid domain and an OPT resource record with a large UDP payload is attached, the server may fail.
Solution
Upgrade to 8.4.1 or 9.2.3 http://www.isc.org/products/BIND/bind8.html http://www.isc.org/products/BIND/

Concern or Vulnerability
Weakness – Verified – 1.6 This DNS server is allowing recursive queries from the outside. This would allow an attacker to poison the DNS servers local cache. The next victim to request that information may be unknowingly directed to the attackers site.
Example
http://www.giac.org/practical/gsec/Doug_Sax_GSEC.pdf http://www.cert.org/advisories/CA-1997-22.html
Solution
Disable recursive queries for those outside of the CLIENT IP space.

IP Address	domain name
193.145.85.91	Dns2.Clientschools.org.

Hop	Port	Protocol	Service	Service Details
11	53(UDP)	DNS	Domain name service	Secondary nameserver for Clientschools.org Bind on windows

Banner(s):

Port	Protocol	Banner
11	DNS	9.2.2

Concerns and Vulnerabilities:

Concern or Vulnerability
Weakness – Verified – 1.6 This DNS server is allowing recursive queries from the outside. This would allow an attacker to poison the DNS servers local cache. The next victim to request that information may be unknowingly directed to the attackers site.
Example
http://www.giac.org/practical/gsec/Doug_Sax_GSEC.pdf http://www.cert.org/advisories/CA-1997-22.html
Solution
Disable recursive queries for those outside of the CLIENT IP space.

Concern or Vulnerability
Information: There is a newer 9.2.x tree available
Example
n/a
Solution
Upgrade to 9.2.3 http://www.isc.org/products/BIND/

IP Address	domain name
193.145.85.100	user64x100.School.mo.us. www.Clientschools.org

Hop	Port	Protocol	Service	Service Details
11	21	FTP	File Transfer	www.Clientschools.org ftp site
11	80	HTTP	Website	www.Clientschools.org

Banner(s):

Port	Protocol	Banner
21	FTP	220 webserver Microsoft FTP Service (Version 5.0).
80	HTTP	Microsoft-IIS/5.0

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
D0546289 B64E6218 E1BE3211 CE884108 C369C71F DB1C99BB
IPID Sequence Generation
Incremental
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
Vulnerability – Identified – 1.6 Based on the version in the banner, it may be possible to crash the ftp server (DoS). This would only be possible after logging in, which would require a valid username/password.
Example
An example request that can cause the crash: STAT ?*<240 x X> More information can be found here: http://www.securiteam.com/windowsntfocus/5XP0H206VM.html
Solution
Apply relevant hotfix: http://www.microsoft.com/technet/security/bulletin/ms02-018.asp Microsoft Patch Q319733 IIS 5.0 http://download.microsoft.com/download/iis50/Patch/Q319733/NT5/EN-US/Q319733_W2K_SP3_X86_EN.exe

Concern or Vulnerability
Weakness – Identified – .8 This allows an attacker to be able to bruteforce login and password attempts to the Front Page Extension Authoring interface. With enough time an attacker could potentially access the authoring portion of Front Page and deface your website.
Example
http://www.Clientschools.org/_vti_bin/_vti_aut/author.dll/admin.dll/
Solution
Consider disallowing public access to this url.

Concern or Vulnerability

Concern – Verified – .8 You are allowing FTP sessions. The username, password, and all data sent over FTP are not encrypted by the protocol.
Example
Open up a packet analyzer (Like Ethereal http://www.ethereal.com/) and collect the data as you transfer files to 193.145.85.100 over ftp.
Solution
Migrate to sftp or scp (part of the SSH suite).

IP Address	domain name
193.145.85.150	web.School.mo.us

Hop	Port	Protocol	Service	Service Details
11	21	FTP	File Transfer	
11	80	HTTP	Website	

Banner(s):

Port	Protocol	Banner
21	FTP	220-Welcome to Rumpus! 220 Service ready for new user
80	HTTP	MACHTTP/2.5

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
A9CF4368 A3F03E63 B550E91E 994FFD63 AE3BC539 DE745F1B
IPID Sequence Generation
Broken little-endian incremental
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
Vulnerability – Identified – 1.6 The remote system may be vulnerable to one or more remote buffer overflow attacks.
Example
Using automated FTP vulnerability "fuzzers" you can look for patterns of past weaknesses. This ftpd exhibited potential weaknesses for exploitation.
Solution
Contact Rumpus http://www.maxum.com/Rumpus/ for more information.

Concern or Vulnerability
Concern – Verified – .8 You are allowing FTP sessions. The username, password, and all data sent over FTP are not encrypted by the protocol.
Example
Open up a packet analyzer (Like Ethereal http://www.ethereal.com/) and collect the data as you transfer files to 193.145.85.150 over ftp.
Solution
Migrate to sftp or scp (part of the SSH suite).

IP Address	Domain name
193.145.85.248	user64x248.School.mo.us.

Hop	Port	Protocol	Service	Service Details
11	53(UDP)	DNS	Domain Name Service	Not sure what function this one is serving.

Concerns and Vulnerabilities:

Concern or Vulnerability
Weakness – Verified – 1.6 This DNS server is allowing recursive queries from the outside. This would allow an attacker to poison the DNS servers local cache. The next victim to request that information may be unknowingly directed to the attackers site.
Example
http://www.giac.org/practical/gsec/Doug_Sax_GSEC.pdf http://www.cert.org/advisories/CA-1997-22.html
Solution
Turn off DNS services on this machine or disable recursive queries for those outside of the CLIENT IP space.

IP Address	Domain name
193.145.85.251	mail.School.mo.us

Hop	Port	Protocol	Service	Service Details
11	25	SMTP	Email	This is the secondary email server for the CLIENT domains.
11	1352	NRPC	Notes Configuration	

Banner(s):

Port	Protocol	Banner
25	SMTP	220 MAIL.SCHOOL.MO.US ESMTP SERVICE (LOTUS DOMINO RELEASE 5.0.10) READY AT THU, 6 NOV 2003 21:25:13 -0800
1352	NRPC	(CN=mail/OU=KalmusC/O=CLIENT)

TCP Sequencing:

TCP Sequence Prediction
Class=truly random
TCP ISN Seq. Numbers
27AABDDC 96B10C65 6442E324 7E05B2F0 54C9418F 56CA30F7
IPID Sequence Generation
Incremental
Uptime
Not available

Concerns and Vulnerabilities:

Concern or Vulnerability
Information Leak – Verified – .4 There is no need for port 1352 to be open to the world. This simply gives up more information about the site than needed.
Example
n/a
Solution
Update the FW rulesets to disallow access to port 1352.