

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Auditing an Apache for Windows Web Server: An Auditor's Perspective

Tony Yao
GSNA Practical Assignment
Version 2.1
June 2003

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Abstract 3

1. Research in Audit, Measurement Practice and Control 4

1.1. Introduction 4
1.2. Purpose and scop e of audit..... 5
1.3. Risks to the system 6
1.4. Current state of practice 10

2. Create an Audit Checklist 11

2.1. Base OS..... 11
2.2. Antivirus 12
2.3. Apache Installation and Basic Configuration 14
2.4. User Account and Group Account 17
2.5. Access Control 20
2.6. Auditing and Logging 25
2.7. Network 27
2.8. Default Settings 31
2.9. Information Disclosure 37

3. Audit Evidence 40

3.1. Conduct the Audit 40
3.2. Measure Residual Risk 67
3.3. Is the System Auditable? 68

4. Audit Report 69

4.1. Executive Summary 69
4.2. Audit Findings 70
4.3. Costs..... 75
4.4. Compensating Controls 76

References 77

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract

This paper provides a detailed technical checklis t to evaluate the security status of Apache for Windows web server. The target audience of this paper is system administrators and security auditors who are familiar with Windows NT/2000 server and Apache web server.

This paper focuses on web server secu rity only. Audit for underlying operating system, web application, network, and security policies is not covered.

This checklist is applied to a real -life customer survey web server running Apache on Windows 2000 server. Sixteen checklist items and their corresponding results are listed , addressing the most important security concerns on the survey web server. A summary report with audit findings, recommendations and estimated cost is presented as well.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1. Research in Audit, Measurement Practice and Control

1.1. Introduction

The subject of this audit is EMCA company[1] customer survey web server running Apache and Tomcat on top of Windows 2000 Server (Service Pack 3). Apache is the web server software; Tomcat is an open-source implementation of Java Servlet and JavaServer Pages which are used to build interactive web applications. The server hardware is an IBM NetVista Desktop A40 machine with a single PIII 733MHz processor and 256MB RAM.

Due to the business nature of EMCA company, which is providing IT services to clients in global market, customer satisfaction is critical to company business and is therefore continuously monitored. The survey web server (called CUS hereafter) hosts customer survey web site. The survey information collected is used to find out what things the company is doing well and which areas need improvement, both at an individual client level and across the organization. This site is also used for employee satisfaction surveys at branches in different geographic locations, and any other internal surveys people might want to use it for. In addition, EMCA company can also run a survey for an external client if they want one.

There are two types of customers who use the site - those who are completing a survey, in which case they access the survey by clicking on a link which is emailed to them, and those who create surveys, in which case they log onto the application via a special link.

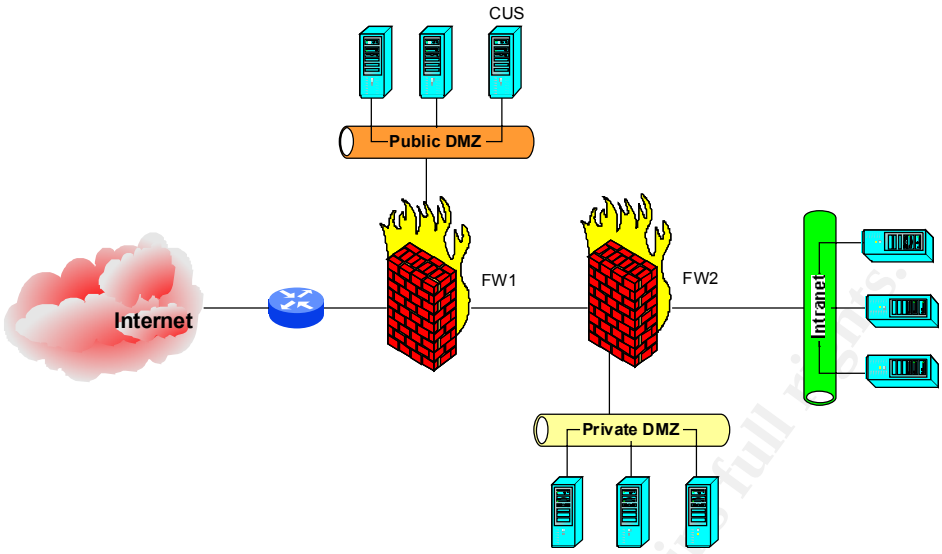
This server is not mission-critical as it only needs to be available when a survey is being conducted or created. However, it is very important to the business because the survey information reflects customers' perception on how well the company performs. The information has a very sensitive and confidential nature.

CUS web server sits in the public DMZ of EMCA company. The simplified network diagram is shown in Figure 1.

[1] All references to the audited organization have been deleted. For the purpose of this paper, the organization is referred to as EMCA company.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Figure 1 EMCA simplified network diagram



1.2. Purpose and scope of audit

The purpose of this audit is to ensure CUS web server conforms to industry best practices and has been configured as a secure web server .

This audit will focus on Apache web server security. Of course there is not much point discuss ing web server security without touching base operating system security. However, a det ailed base OS security audit is beyond the scope of this document. There are several guides and checklist s on securing Windows 2000 freely available on Internet. Some of them are listed in References pages at the end of this document. Certain OS checking s teps will still be covered to ensure the base OS has a minimum level of security.

EMCA company's system security policies are an important part of web server security. These policies mainly focus on base OS security and standard security tools used to mon itor system security status. Therefore security policy audit is not covered in this audit.

Network security is also part of web server security. Normally, there is a firewall or router sitting between public web server and the Internet. As in the case of base OS security, a detailed network security audit is beyond the scope of this document. Some resources can be found in References pages.

Web application security will not be covered. Instead, it will be addressed in a separate audit.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

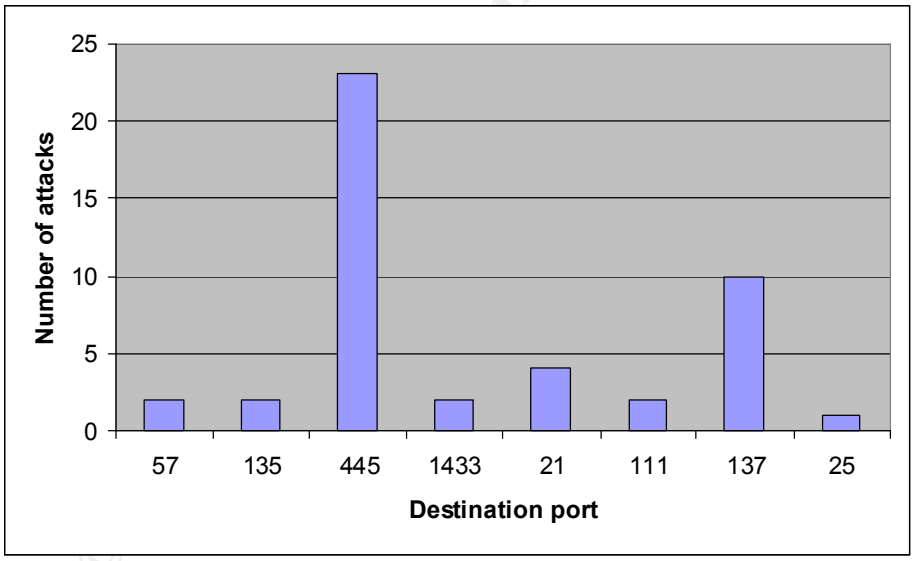
1.3. Risks to the system

In Feb 2003, Symantec released the Internet Security Threat Report for Q3 and Q4 2002, which shows that the risk of cyber attacks is high for all Internet - connected companies. On average, companies experienced 30 attacks per company per week and almost 80% of attackers use Microsoft Windows platform[2]. According to ISS[3], port 80 was the most common attack destination port from 28th September through to 31 st December 2002, which contributed to 57% of all attack destination ports . Down to 27.95% for Q1 200 3, port 80 was the 2nd most common attack destination port with the 1 st one being port 137 (36.55%) because of the Bugbear worm.

Because of the popularity of Apache web server, which account ed for about 62.5% percent of web server market share until April 2003[4], it is a common target of hackers, and administrators tend to think Apache is the best web server product and does not require hardening. However, like many other products, Apache web server is NOT secure by default, and even apache.org web site was compromised in May 200 1[5].

Figure 2 shows the network attacks on CUS web server logged by Internet firewall FW1 on a normal day 14 March 2003.

Figure 2 Network attacks on CUS on 14 March 2003



Some attacks on port 80 which is allowed by firewall were captured in Apache log:

151.99.139.15 - - [14/Mar/2003:10:50:58 +1300] "GET /NULL.idq" 404 -
151.99.139.15 - - [14/Mar/2003:10:51:09 +1300] "GET /NULL.idq" 404 -

[2] http://enterprisesecurity.symantec.com/Content.cfm?articleID=1964&EID=0
[3] https://gtoc.iss.net/documents/summaryreport.pdf
[4] http://news.netcraft.com/archives/2003/04/13/april_2003_web_server_survey.html
[5] http://www.apache.org/info/20010519-hack.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
211.233.15.120 - - [14/Mar/2003:13:53:08 +1300] "GET
/scripts/..%25 5c%255c../winnt/system32/cmd.exe?/c+dir" 404 -
211.233.15.120 - - [14/Mar/2003:13:53:09 +1300] "GET
/msadc/..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir" 404 -
211.233.15.120 - - [14/Mar/2003:13:53:10 +1300] "GET /scripts/root.exe?/c+dir" 404 -
211.233.15.120 - - [14/Mar/2003:13:53:11 +1300] "GET
/scripts/..%255c%255c../winnt/system32/cmd.exe?/c+dir" 404 -
211.233.15.120 - - [14/Mar/2003:13:53:12 +1300] "GET
/msadc/..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir" 404 -
211.233.15.120 - - [14/Mar/2003:13:53:12 +1300] "GET /scripts/root.exe?/c+dir" 404 –
200.54.68.140 - - [14/Mar/2003:14:25:11 +1300] "GET
/default.ida?NNNN
```

Risk	Probability	Impact
	software vulnerabilities may cause system to crash.	reputation will be jeopardized.
Unauthorized system and file access	High Internal users are generally trusted by default and easily gain access. Potential remote attackers may exploit web server software flaws and gain access to the system.	This is a confidentiality attack because sensitive information may be exposed, and competitors may have access to this information. This is also availability and integrity attack as information stored on server may be deleted or changed. Company reputation will be affected.
System information disclosure	High By default HTTP header and footer messages contain web software and OS information.	Information about web server software and OS can be used to analyze the possible vulnerabilities the server may have and create attack target profile.
Lack of system logging and auditing	High System auditing is not turned on by default. System administrators are often too busy to review logs.	In case of security incidents, it will be very difficult to find out when and how the incident happened, as well as what caused it. Early detection of security incident is almost impossible.
Lack of physical access control	High Company staff are trusted by default.	Web server can be brought down easily due to easy access to the console. Easy access to the information stored on server may lead to information theft and destruction.
Remote access	High Company staff are trusted by default. Quite often, many people share the same login	Employee's home machine may not be properly secured and may be infected by virus or may have Trojans,

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk	Probability	Impact
	account which is a local administrator account on web server. Remote access often bypasses firewall.	backdoors, etc. installed. This may cause unauthorized system and file access to web server. In case of security breach, it is very hard to find out who did what as everyone shares the same login credentials.
Lack of change management	High Administrators tend to fix things quickly instead of following procedures.	It is hard to maintain baseline security because change happens quite often. It is also difficult to detect security breach by comparing current configuration with known baseline as there is no record of what has been done.
Lack of documentation	High Documentation is generally lacking for IT companies, even if there is some, it may not be up-to-date.	Without standard installation and configuration document, different people may build the server in a different way which results into different secure status, and web server is vulnerable if it is not properly secured.
Lack of backup	Low Companies normally have a backup/restore procedure.	Server cannot be restored in case of disaster. Company reputation is jeopardized.
Virus	Medium Most companies use antivirus software but the product may not be running with latest signature files.	Infected machine may try to scan and infect other machines. Zombie, Trojans and backdoors on infected server machine may lead to system compromise and unauthorized system

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Risk	Probability	Impact
		and file access. Company reputation will be affected.
Lack of patch management process	High Administrators tend to ignore patch installation as long as the system is running okay .	Server is vulnerable and may be compromised . Company reputation is jeopardized .

1.4. Current state of practice

Extensive research was conducted by using common Internet search engine Google (http://www.google.com) for terms like "hardening Apache" and "Apache security". Apache web site (http://httpd.apache.org) and SANS reading room (http://www.sans.org/rr/) were used as well to search for information.

Given the popularity of Apache, one would imagine that there should be plenty of resources available on how to secure Apache web server. The fact is, however, there are not that many, especially for the Windows platform. Most information on Apache security talks about SSL , PKI implementation or vulnerabilities and exploits in Apache.

SANS lists some of the critical vulnerabilities found in Apache web server in The Twenty Most Critical Internet Security Vulnerabilities report (http://www.sans.org/top20/). Apache site provides security tips for server configuration (http://httpd.apache.org/docs/misc/security_tips.html). There are several guidelines on how to secure Apache installation , like the white paper published by Thai Computer Emergency Response Team on how to secure Apache web server in UNIX environment (http://thaicert.nectec.or.th/event/itsec2002 -material/Apache.pdf), the presentation provided by Jason Novotny and Marcia Perry on how to build a secure Apache and Tomcat server on Solaris and Linux (http://doesciencegrid.org/Grid/public/events/GPDW/slides/webserver.pdf), and the white paper released by Mark J Cox discussing the general security issues in Apache web server (http://www.awe.com/mark/apcon2002/tu04 -handout.pdf).

However, the platforms discussed are overwhelmingly different flavors of UNIX. There is little information about securing A pache on Windows platform , despite the fact that about 200,000 Apache web servers were reportedly running on Windows [6]. Even in the UNIX world, I have not found any specific checklist developed to secure Apache web server. Apache site has

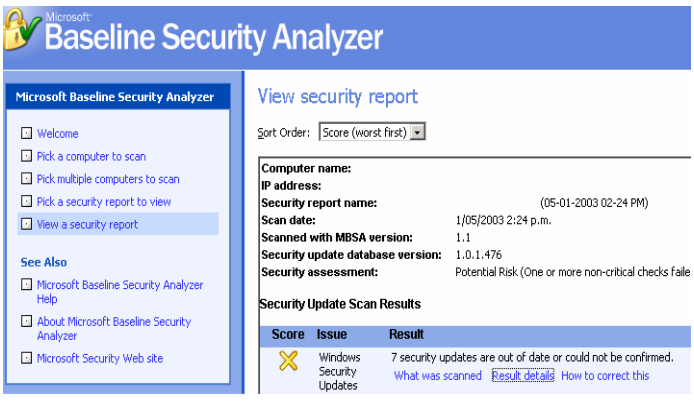
[6] http://news.netcraft.com/archives/2003/02/25/apache_on_windows_struggling.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

information about using Apache on Windows (http://httpd.apache.org/docs/windows.html), but not focused on security. Windows NT/2000 Server Hardening Checklist from Mark Lachniet provides some information on Apache s ecurity in Windows environment (http://www.mtip.net/aware/MarkLachnietChecklist.pdf). InterSect Alliance has also released a document on Apache security in Windows environment (http://www.intersectalliance.com/projects/ApacheConfig/).

2. Create an Audit Checklist

2.1. Base OS

Checklist 1.	**Latest OS service packs and security patches are installed**
Reference	http://www.microsoft.com/technet/security/prodtech/windows/secwin2k/default.asp
Control objective	There are no known base OS vulnerabilities existing on the server.
Risk	By exploiting known vulnerabilities, an attacker may compromise the web server, and use this server to attack other Internet servers, or gain access to the information stored on the web server. Probability: High
Compliance	The latest service pack (NT4 SP6a, Win2K SP3) is installed, and all relevant security patches have been applied. There shouldn't be any missing patches reported.
Testing	Use Microsoft Baseline Securi ty Analyzer to check patch level. 

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

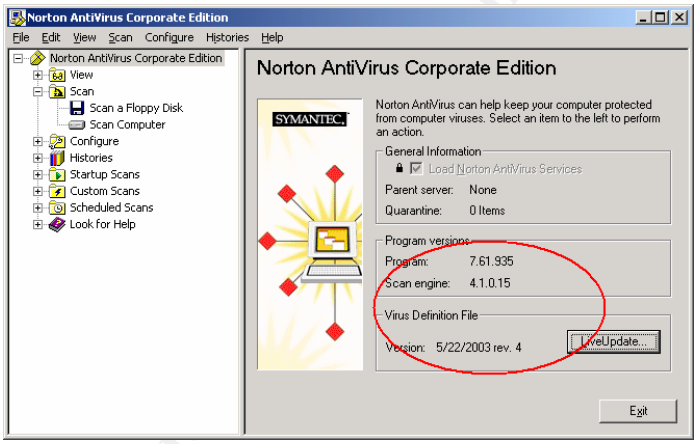
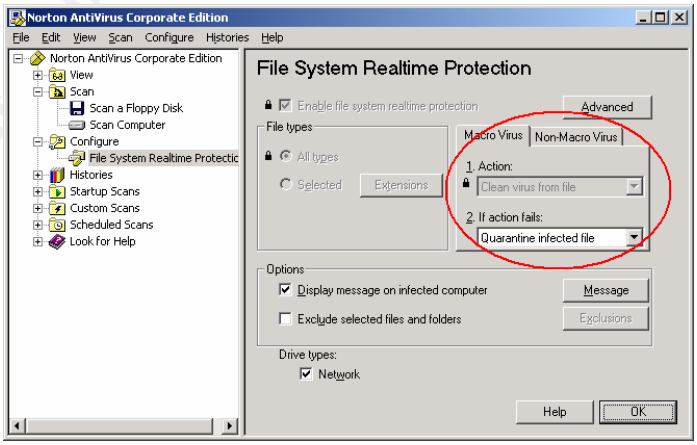
Checklist 1.	**Latest OS service packs and security patches are installed**
	In case the server does not have Internet access, use HFNETCHK tool for security update check : *hfnetchk –v –s 1 –x mssecure.xml* where mssecure.xml is a local copy of the latest version of XML file and can be downloaded at: http://www.microsoft.com/technet/security/search/mssecure.xml
Objective / Subjective	Objective

Checklist 2.	**All drives are in NTFS format**
Reference	http://www.linuxroot.org/apachecon/W07.pdf
Control objective	File level security is implemented.
Risk	Lack of file level security may result in u nauthorized access to, deletion or change of file content, or even system compromise. Probability: High
Compliance	All drives are in NTFS format .
Testing	Use Disk Management snap-in to check file system format.
Objective / Subjective	Objective

2.2. Antivirus

Checklist 3.	**Antivirus product is running and virus signature file is up to date, action is set to Cure and Quarantine**
Reference	http://securityresponse.symantec.com/avcenter/defs.download.html (Norton, for example)
Control objective	The server is protected from any known viruses.
Risk	Virus may result in system compromise, mass mailing, information disclosure, backdoor or Trojan placement, etc.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 3.	**Antivirus product is running and virus signature file is up to date, action is set to Cure and Quarantine**
	Probability: High
Compliance	Antivirus product is installed and running with the latest signature file, and the action is set to Cure first, then Quarantine.
Testing	To check if it is running with the latest signature file (Norton, for example):  To check real-time scanning action (Norton, for example), select Configure → File System Realtime Protection,  Check the setting for both Macro virus and Non - Macro virus. To confirm that server is protected against known virus, create a text file containing following EICAR test string: X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H* Send this file to server to s ee whether antivirus software can detect it and take appropriate action .

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 3. Antivirus product is running and virus signature file is up to date, action is set to Cure and Quarantine	
Objective / Subjective	Objective

2.3. Apache Installation and Basic Configuration

Checklist 4. Latest version of Web server application is installed	
Reference	http://www.intersectalliance.com/projects/ApacheConfig/
Control objective	There are no known web server software vulnerabilities existing on the server.
Risk	By exploiting known vulnerabilities, an attacker can cause server compromise, denial of service, malicious code placement, information disclosure, etc. Probability: High
Compliance	The latest stable version for Apache 1.3 is 1.3.27 , the latest stable version for Apache 2.0 is 2.0.4 6, the current product quality release for Tomcat 3.x is 3.3, and the latest release for Tomcat 4.1.x is 4.1.24. (http://httpd.apache.org/dist/httpd/binaries/win32/ , http://jakarta.apache.org/tomcat/index.html)
Testing	Run following command from \apache\bin directory to find out the version of Apache running on the server: *apache –v* For Tomcat, there is no similar way to check version number. Instead, the technical documentation coming with Tomcat (\Tomcat\doc\readme) will give version information. Default Tomcat home page (\Tomcat\webapps\ROOT\index.html) also contains version information.
Objective / Subjective	Objective

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 5.	**Web content file is on a different volume than system or program files**
Reference	http://www.mtip.net/aware/MarkLachnietChecklist.pdf
Control objective	System files are protected and access is restricted.
Risk	Directory traversal attack or web configuration mistakes may expose system files, to which an attacker may have access and cause system compromise. Probability: Medium
Compliance	Web directory is on different volume than system and program files.
Testing	SET command will show where system files are, and DocumentRoot directive in httpd.conf file specifies where the web content files are. To confirm the settings, use Internet Explorer to access the web site.
Objective / Subjective	Objective

Checklist 6.	**Log files are stored in a different directory or volume as website root**
Reference	http://www.macromedia.com/v1/DocumentCenter/Partners/ASZ_ASWPS_Securing_Apache.pdf http://www.mtip.net/aware/MarkLachnietChec klist.pdf
Control objective	Log files are protected and access is restricted.
Risk	Log files contain important information which is important to web server operation and especially to security audit and security violation investigation. If log files are in the same directory as web content files, potential attackers may have access to log files, and make an attack unnoticed by deleting log entries. Probability: High
Compliance	Log files are in a different directory than web root. For example, if the web root directory is D:\apache\httpd, log files should not be in

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 6.	**Log files are stored in a different directory or volume as website root**
	D:\apache\httpd\logs directory. Preferably, the log files are stored in a different volume than web root.
Testing	DocumentRoot directive in httpd.conf file specifies where web content files ar e. ServerRoot, ErrorLog and CustomLog directives define where web log files are. Check these directives in httpd.conf file.
Objective / Subjective	Objective

Checklist 7.	**Basic authentication files must not be within the web site directory tree**
Reference	http://www.linuxroot.org/apachecon/W07.pdf http://www.baylisa.org/library/slides/2002/10/BayLISAApacheWUFTP.pdf
Control objective	Authentication files are protected and access is restricted.
Risk	Authentication files , which contain user credentials , may be downloaded by malicious users or indexed by search engine . Probability: High
Compliance	User authentication file and group authentication file should be placed above web root directory. For example, if web root directory is D: \apache\httpd, authentication file s should be placed in D:\apache directory.
Testing	AccessFileName directive in httpd.conf file defines the name of authentication file. Check this directive to find out what the authentication file name is and check authentication file location using Windows explorer.
Objective / Subjective	Objective

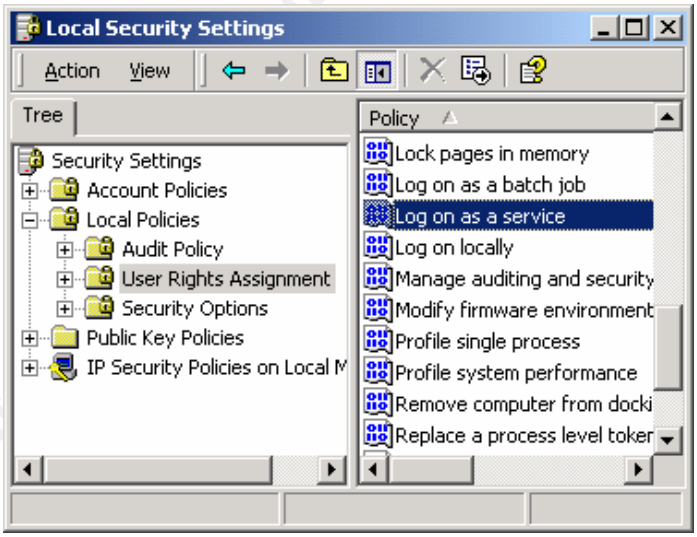
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.4. User Account and Group Account

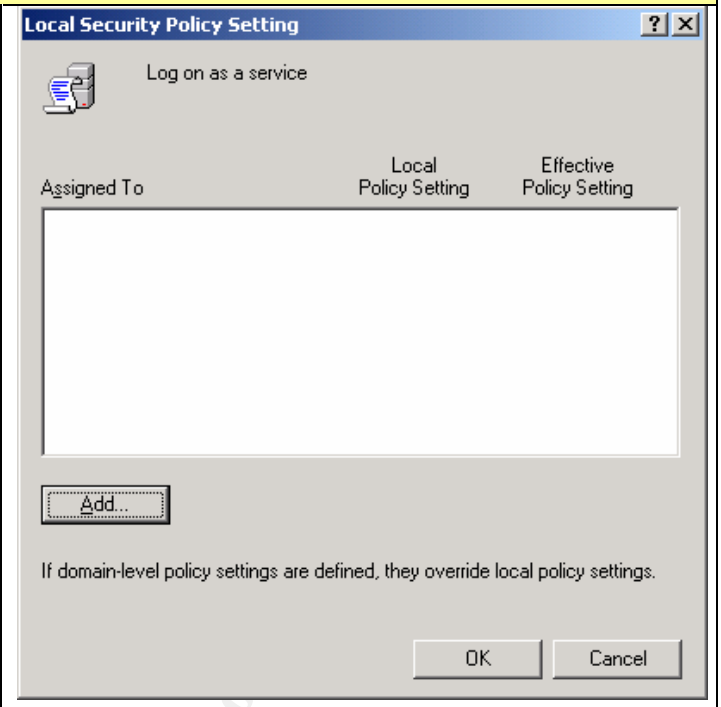
Checklist 8.	**Separate user and group account are created and used for Apache, and defined in httpd.conf**
Reference	http://www.linuxroot.org/apachecon/W07.pdf http://www.baylisa.org/library/slides/2002/10/BayLISAApacheWUFTP.pdf
Control objective	Apache runs under normal user account , NOT privileged account.
Risk	Web server software or web application error or failure may result in full access to web server with administrative rights and s ystem compromise . Probability: High
Compliance	Following directives are defined in httpd.conf file: *User* *Group* Apache service is running under the normal user account defined in httpd.conf file, and this user account is a member of local Users group .
Testing	Review httpd.conf file to check a separate normal user account is defined for Apache, and u se Local Users and Groups snap -in to check property and group membership for this account. To confirm Apache is running under t his account, go to Control Panel → Administrative Tools → Services, select Apache service, and check Log On properties: 
Objective / Subjective	Objective

Checklist 9.	**Appropriate right s are set for Apache service account**
Reference	http://www.linuxroot.org/apachecon/W07.pdf http://httpd.apache.org/docs/win_service.html
Control objective	Web server starts automatically without the need to log on and keeps running after logoff.
Risk	If the Apache account does not log on as a service, the web server will stop when console is logged off

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 9. Appropriate right s are set for Apache service account	
	or the web server will not start automatically when the server machine boots. Probability: High
Compliance	"Log on as a service" user right is granted to Apache service account. If any network resources will be used such as shared pages, following additional user rights should be granted as well: 1). Act as part of operating system 2). Backup files and dir ectories 3). Restore files and directories
Testing	To check user rights granted to Apac he service account, use Control Panel → Administrative Tools → Local Security Policy :  To check "Log on as a service" user right, double click on this right, and check if Apache service account is listed under Assigned to column:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 9. Appropriate rights are set for Apache service account	
	
Objective / Subjective	Objective

Checklist 10. Different roles are defined for different user groups with different duties on web server	
Reference	http://thaicert.nectec.or.th/event/itsec2002_-material/Apache.pdf
Control objective	Different people have different access to different areas of web site based on their roles.
Risk	Unauthorized access to, change or deletion of files and even system compromise would happen if everyone has full access to everywhere on web server. Probability: High
Compliance	Different groups of people may have different responsibilities for and permissions on different parts of web server. Generally the roles can be: 1) web developers who are responsible for web application and content development; 2) web authors who are responsible for web server content design and update; or 3) webmasters who are responsible for web server operation .

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 10. Different roles are defined for different user groups with different duties on web server	
Testing	Use Local Users and Groups snap -in to check if there are any groups defined for different roles .
Objective / Subjective	Objective

2.5. Access Control

Checklist 11. Base system directory NTFS permissions for Apache service account	
Reference	http://www.intersectalliance.com/projects/ApacheConfig/ http://www.linuxroot.org/apachecon/W07.pdf
Control objective	Apache service account is given appropriate access permissions on system directory.
Risk	Unauthorized access to, change or deletion of files and even system compromise could happen if Apache service account has full access to system drive on web server. On the other hand, if Apache service account does not have enough permission on system directories, the web server will not work. Probability: High
Compliance	Following permissions should be assigned to Apache service account: **Directory** / **Permission** %systemdrive% \ — Read, Execute %systemroot% \ — Read %systemdrive% \Program Files — Read, Execute %systemroot% \system32 — Read Apache account needs Read access to %systemroot% directory and its subdirectories, except %systemroot% \Profiles directory where original permission should remain unchanged. Appropriate NTFS permissions must be applied for

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 11. Base system directory NTFS permissions for Apache service account	
	other accounts such as local administrator, system account, etc, but this is not the scope of this document.
Testing	Check directory NTFS permission with native Windows 2000 tool CACLS.EXE: *cacls directory_path* To confirm Apache service account has been given appropriate permissions, log on locally to web server with Apache service account and try Read, Delete, Write and Execute operation on system directories.
Objective / Subjective	Objective

Checklist 12. Web directory NTFS permissions	
Reference	http://www.macromedia.com/v1/DocumentCenter/Partners/ASZ_ASWPS_Securing_Apache.pdf http://www.intersectalliance.com/projects/ApacheConfig/ http://www.linuxroot.org/apachecon/W07.pdf http://thaicert.nectec.or.th/event/itsec2002_-material/Apache.pdf http://httpd.apache.org/docs/misc/security_tips.html http://httpd.apache.org/docs/win_service.html
Control objective	Appropriate NTFS permissions are assigned on Apache web directory.
Risk	With inappropriate permissions, unauthorized access to, change or deletion of files and even system compromise could happen or the web server will not work. Probability: High
Compliance	**Directory** / **Permission** Apache drive: Apache: Read, Admin: Full Apache root directory: Apache: Read , Execute

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 12. Web directory NTFS permissions

	Admin: Full
CGI-Bin	Apache: Read, Execute Webmaster: Change Web developer: Cha nge Admin: Full
Web document	Apache: Read, Execute Webmaster: Change Web developer: Change Web author: Change Admin: Full
Log directory	Apache: Change Webmaster: Read Admin: Full
Cache directory	Apache: Change Admin: Full
Bin directory	Apache: Read, Ex ecute Webmaster: Change Web developer: Change Admin: Full
Configuration directory	Apache: R ead, Execute Webmaster: Change Admin: Full

where Web developer, Web author and Webmaster are group accounts.

Testing

Check directory NTFS permission with native Windows 2000 tool CACLS.EXE:

cacls directory_path

Log on locally as a normal user account and ensure this user account does not have access to any web directory. Also log on locally using Apache service account and member account of W ebmaster, Web developer or Web author group and try to access web directories to ensure proper permissions have been given to different groups and Apache service account.

Objective / Subjective	Objective

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 13. Authentication file NTFS permission	
Reference	http://www.sans.org/rr/web/apcahe_sec.php
Control objective	Access to authentication file s is restricted at file level.
Risk	This file contains user account and password information. Unrestricted access could lead to system compromise. Probability: High
Compliance	**File** / **Permission** Basic authentication file / Apache: Read Admin: Full
Testing	Check file NTFS permission with native Windows 2000 tool CACLS.EXE: *cacls file_patch \file_name* Log on locally using normal user account and Apache service account and try to access basic authentication file to confirm proper permissions have been assigned.
Objective / Subjective	Objective

Checklist 14. Disallow web access to authentication file	
Reference	http://www.macromedia.com/v1/DocumentCenter/Partners/ASZ_ASWPS_Securing_Apache.pdf
Control objective	Web access to authentication file is not permitted.
Risk	Internet users may get local user credentials and gain access to the system. Probability: High
Compliance	<Files> section has following directive settings for .htaccess file in httpd.conf file (.htaccess is the authentication file): *<Files ~ "\.htaccess$">* *Order deny, allow* *Deny from all*

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 14. Disallow web access to authentication file	
	</Files> Or *<Files ~ "^\.ht>* *Order deny, allow* *Deny from all* *</Files>*
Testing	Check the <Files> section in httpd.conf file and try to access authentication file from Internet Explorer to confirm web access to this file is not permitted.
Objective / Subjec tive	Objective

Checklist 15. Settings for Document Root in httpd.conf	
Reference	http://www.baylisa.org/library/slides/2002/10/BayLISAApacheWUFTP.pdf http://httpd.apache.org/docs/misc/security_tips.html
Control objective	Users can access the web site and a single security policy is maintained throughout the web document tree.
Risk	Unauthorized access and potential system compromise may be caused by mistaken configuration as well as different and complex security policies. Probability: Medium
Compliance	The root Directory section in httpd.conf should be: *<Directory />* *AllowOverride None* *Order deny, allow* *Deny from all* *</Directory>* For public web site, this may be changed to: *<Directory />* *AllowOverride None* *Order allow, deny* *Allow from all* *</Directory>*
Testing	Check root directory settings in the <Directory /> section in httpd.conf file.
Objective / Subjective	Objective

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 16. Basic access control settings in http d.conf	
Reference	http://www.baylisa.org/library/slides/2002/10/BayLISAApacheWUFTP.pdf
Control objective	Access to secure p ages is restricted.
Risk	Directory traversal attack may result in unauthorized access to secure pages, which may lead to user account information disclosure and even system compromise. Probability: Medium
Compliance	Following directives should be defined in <Directory> section in httpd.conf file for any restricted director ies: *AccessFileName file_name* *<Directory "/path/to/ restricted /directory">* *AuthType Basic* *AuthName "message prompt"* *AuthUserFile* *"path/to/authentication/file /file_name "* *Require valid -user* *</Directory>*
Testing	Check the <Directory> section in httpd.conf file to see if any directory is protected . If there are, then try to access these directories in Internet Explorer to confirm a username/password box pops up and only a valid user with corr ect password can get access.
Objective / Subjective	Objective

2.6. Auditing and Logging

Checklist 17. HTTP logging is enabled for entire web	
Reference	http://www.intersectalliance.com/projects/ApachConfig/ http://httpd.apache.org/docs/logs.html
Control objective	Web site access is logged.
Risk	Without logging, early detection of potential attacks

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 17. HTTP logging is enabled for entire web	
	would be very difficult. It is also difficult to find out when security incident happened, how it happened, and who did what, etc. Probability: Low
Compliance	Web site access is logged; optionally referrer and user agent information is logged as well. The CustomLog directive in httpd.conf file is something like: *CustomLog /path/to/audit/logs/access_log common* *CustomLog /path/to/audit/logs/referrer_log referrer* *CustomLog /path/to/audit/logs/agent_log agent*
Testing	Check CustomLog directive in httpd.conf file and confirm web site access is logged by v isiting the web site and checking \apache\logs\access.log file.
Objective / Subjective	Objective

Checklist 18. Maximum HTTP fields are logged in W3 Extended log file format	
Reference	http://www.intersectalliance.com/projects/ApacheConfig/ http://httpd.apache.org/docs/logs.html
Control objective	Maximum amount of information is logged for web access.
Risk	Attack source and patterns may not be identified without logging enough information. Probability: Medium
Compliance	Maximum information is logged for web site access, and optionally for referrer and user agent as well. The LogFormat directive in httpd.conf file is something like: *LogFormat "%h %l %u %t \"%r\" %>s %b" common* *LogfFormat "%{Referer}i -> %U" referrer* *LogFormat "%{User -agent}i" agent* where: %h=remote host %l=remote log name %u=remote user %t=time

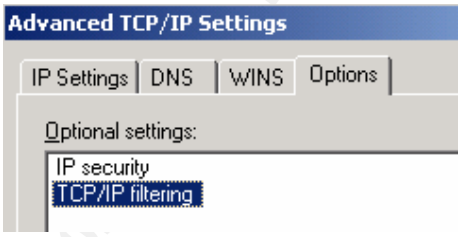
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 18. Maximum HTTP fields are logged in W3 Extended log file format	
	%r=first line of request %>s=last request status code %b=bytes sent, excluding HTTP headers
Testing	Check LogFormat directive in httpd.conf file and confirm maximum information is logged by visiting the web site and checking \apache\logs\access.log file.
Objective / Subjective	Objective

2.7. Network

Checklist 19. Web server process is bound for localhost (not default "All Unsigned")	
Reference	http://www.intersectalliance.com/projects/ApacheConfig/ http://www.baylisa.org/library/slides/2002/10/BayLISAApacheWUFTP.pdf
Control objective	Web site is bound to a particular IP address.
Risk	Web server will not work in case of DoS attack on the DNS server. On a multi-homed server, web server may bind to all available IP addresses and result in unauthorized access to the web server. Probability: High
Compliance	Following directives are set in httpd.conf file: *ServerName localhost* *BindAddress 127.0.0.1* *Listen 127.0.0.1:port* (for Apache 2.0)
Testing	Check ServerName, BindAdress or Listen directive in httpd.conf file. If the web server has more than one IP address, try to access the web site at a different IP address or even a different port (such as 8080) to confirm the site does listen on one particular I P address and one port only.
Objective / Subjective	Objective

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 20. TCP/IP filtering is configured	
Reference	N/A
Control objective	Only required network connection is permitted.
Risk	Port scanning may expose vulnerable ports; unauthorized network connection may lead to system compromise. Probability: Medium
Compliance	Only required network connection ports are allowed, such as port 80 for web server, port 3389 for terminal services, etc.
Testing	To check TCP/IP filtering, go to the Properties page for Local Area Connection. In Advanced TCP/IP Settings, check the Properties of TCP/IP filtering:  TCP/IP filtering should be enabled and restrictions on destination ports are set.
Objective / Subjective	Objective

Checklist 21. Denial of Service	
Reference	http://www.openna.com/documentations/articles/apache/index.php http://httpd.apache.org/docs/mod/core.html http://www.intersectalliance.com/projects/ApacheConfig/ http://httpd.apache.org/docs/windows.html
Control objective	The system is protected against denial of service attack.
Risk	The web site could be under denial of service attack and legitimate users can not access the web

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 21. Denial of Service	
	site. Probability: Low
Compliance	Following directives are set in h ttpd.conf file: *MaxRequestsPerChild 0* *ThreadsPerChild 50* *MaxClients 512* *KeepAliveTimeout 1 0* *MaxKeepAliveRequests 0* *TimeOut 60* *RLimitCPU: unset* *RLimitMEM: unset* *RLimitPROC: unset*
Testing	Check the settings for above directives in httpd.conf file.
Objective / Subjective	Objective

Checklist 22. Buffer Overflo w	
Reference	http://thaicert.nectec.or.th/event/itsec2002 - material/Apache.pdf
Control objective	The system is protected from buffer overflow attack.
Risk	Buffer overflow ma y cause web server to crash or give web users full access to system. Probability: Medium
Compliance	Following directives are set in httpd.conf file: *LimitRequestBody 10240* *LimitRequestFields 40* *LimitRequestFieldsize 100* *LimitRequestLine 500*
Testing	Check the settings for above directives in httpd.conf file.
Objective / Subjective	Objective

Checklist 23. Listening ports	
Reference	N/A

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 23. Listening ports	
Control objective	Only necessary ports are listening.
Risk	Port scanning may reveal system configuration information and lead to sys tem identification or even system compromise. Some ports and services have vulnerabilities which may be used by potential attackers to exploit the system. Probability: High
Compliance	There are no unnecessary ports listening on the server.
Testing	To check what ports are listening on web server, run NMAP tool (http://www.insecure.org/nmap) with following options: *nmap –sS –sR –g20 –vv –O –n –r –oN <log file> –P0 <target IP address>* NMAP needs to be run twice , once from Internet and once from Intranet. To determine which process is running on a particular port, run FPORT tool (http://www.foundstone.com/) locally on web server.
Objective / Subjective	Objective

Checklist 24. Known network vulnerabilities are fixed	
Reference	N/A
Control objective	There are no known network vulnerabilities existing on web server.
Risk	By exploiting known vulnerabilities, an attacker may compromise the web server, and use this server to attack other Internet servers, or gain access to the information stored on the web server. Probability: High
Compliance	All known vulnerabilities are fixed . Number of security holes should be zero.
Testing	Scan CUS web server with NESSUS tool (http://www.nessus.org) from Internet and Intranet .
Objective / Subjective	Objective

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

2.8. Default Settings

Checklist 25. Server Side Include (SSI) is disabled	
Reference	http://httpd.apache.org/docs/misc/security_tips.html http://www.baylisa.org/library/slides/2002/10/BayLISAApacheWUFTP.pdf
Control objective	Executing commands from files on web server should be disallowed.
Risk	SSI-enabled files can execute any CGI scripts or programs under Apache service account 's context. Commands executed from web files may have unexpected consequences which expose the system to an attack or causes system crash, etc. Probability: Medium
Compliance	Options directive is NOT set to following in httpd.conf file: *Options Includes* and mod_include module is disabled. Because mod_include module is bound into Apache binary distribution for Windows and is active in default Apache installation, to disable this module, ClearModuleList directive must be used and other core modules be loaded individually. If SSI is required, the recommended setting is: *Options IncludesNOEXEC*
Testing	Check Options directive in httpd.conf file.
Objective / Subjective	Objective

Checklist 26. Indexing is disabled	
Reference	http://www.baylisa.org/library/slides/2002/10/BayLISAApacheWUFTP.pdf
Control objective	Directory listing should be disabled.
Risk	If Indexing is turned on, web server will show a

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 26. Indexing is disabled	
	directory listing of all files and subdirecto ries in the specified directory if index.htm file does not exist in that directory. Sensitive and confidential information may be exposed. Probability: High
Compliance	Options directive is NOT set to following in httpd.conf file and Tomcat configuration file included in httpd.conf file : *Options Indexes* and mod_autoindex module is disabled. Because mod_autoindex module is bound into Apache binary distribution for Windows and is active in default Apache installation, to disable this module, ClearModuleList directive must be used and other core modules be loaded individually.
Testing	Check Options directive in httpd.conf file and Tomcat configuration file. To confirm if Indexing is turned on or not, try to display the directory content by using Internet Explorer .
Objective / Subjective	Objective

Checklist 27. Symbolic links are removed	
Reference	http://www.baylisa.org/library/slides/2002/10/BayLISAApacheWUFTP.pdf
Control objective	Access to files other than those in web tree should be disallowed.
Risk	Accidentally creating a symbolic link which points to a critical system configuration file will expose the content to the whole world. Probability: Medium
Compliance	Options directive is NOT set to following in httpd.conf file and Tomcat configuration file : *Options FollowSymLinks*
Testing	Check Options directive in httpd.conf file and Tomcat configuration file.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 27. Symbolic links are removed	
Objective / Subjective	Objective

Checklist 28. Proxy functionality is disabled	
Reference	http://www.mtip.net/aware/MarkLachnietChecklist.pdf
Control objective	The web server should not be used as a web proxy.
Risk	Internet users may potentially use this web server as a proxy to browse internal or external web sites. Probability: High
Compliance	mod_proxy module is not loaded.
Testing	Check LoadModule directive in httpd.conf file. To confirm proxy functionality is disabled, use NETCAT tool (http://www.atstake.com/research/tools/) to connect to another site (Microsoft, for example) using CUS as web proxy: *nc cus.emca.local 80* *get http://www.microsoft.com http/1.0*
Objective / Subjective	Objective

Checklist 29. Unnecessary aliases are disabled	
Reference	http://www.macromedia.com/v1/DocumentCenter/Partners/ASZ_ASWPS_Securing_Apache.pdf
Control objective	Internet users can only have access to document tree.
Risk	Internet users may have access to other directories not in document tree, which may expose web server to an attack. Probability: Medium
Compliance	No unnecessary aliases are defined in httpd.conf file and Tomcat configuration file. For example, /icons/ alias can be disabled. If Alias is not required, disable mod_alias module.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 29. Unnecessary aliases are disabled	
	Because mod_alias module is bound into Apache binary distribution for Windows and is active in default Apache installation, to disable this module, ClearModuleList directive must be used and other core modules be loaded individually.
Testing	Check Alias directive in httpd.conf file and Tomcat configuration file , and use Internet Explorer to confirm whether alias is used or not.
Objective / Subjective	Objective

Checklist 30. Unnecessary script aliases are disabled	
Reference	http://www.macromedia.com/v1/DocumentCenter/Partners/ASZ_ASWPS_Securing_Apache.pdf
Control objective	Running scripts on web server should be disallowed.
Risk	Script aliases allow users to execute scripts (CGI scripts, for example) from any directory. Commands executed from files not in document root may have unexpected consequences which expose system to an attack or cause system to crash, etc. Probability: High
Compliance	No unnecessary script aliases are defined in httpd.conf file and Tomcat configuration file . If ScriptAlias is not required, disable mod_alias module. Because mod_alias module is bound into Apache binary distribution for Windows and is active in default Apache in stallation, to disable this module, ClearModuleList directive must be used and other core modules be loaded individually.
Testing	Check ScriptAlias directive in httpd.conf file and Tomcat configuration file .
Objective / Subjective	Objective

Checklist 31. Unnecessary handlers are removed

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 31. Unnecessary handlers are removed	
Reference	http://www.macromedia.com/v1/DocumentCenter/Partners/ASZ_ASWPS_Securing_Apache.pdf
Control objective	File extension mappings (similar to ISAPI filters in IIS) should be disallowed.
Risk	Handlers tell the server to process a file in a special way based on file extension name or location. For example, a handler can cause a CGI script to execute when a request for files with h tml extension is received. Third party Internet server extensions such as DLLs and ISAPI may be vulnerable . Handlers may also allow scripts to run from different directories . Probability: High
Compliance	Handlers are not defined in httpd.conf file.
Testing Objective / Subjective	Check AddHandler directive in httpd.conf file . Objective

Checklist 32. Web server is disabled on port 8080 for Tomcat	
Reference	http://doesciencegrid.or g/Grid/public/events/GPDW/slides/webserver.pdf http://jakarta.apache.org/tomcat/tomcat -3.2-doc/tomcat-apache-howto.html#configuring_tomcat
Control objective	Tomcat should not be listening on port 8080 for HTTP request.
Risk	By default, Tomcat comes with a HTTP server on port 8080. This service might be vulnerable, and in some cases Apache may not start if Tomcat is running because port 8080 can be used by Apache as well. Probability: High
Compliance	Following should be commented out in server.xml: *<Connector className="org.apache.tomcat.service.SimpleTcpConnector">* *<Parameter name="handler" value="org.apache.tomcat.service.http.HttpC*

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 32. Web server is disabled on port 8080 for Tomcat	
	onnectionHandl er"/> <Parameter name="port" value="8080"/> </Connector>
Testing	Check the <Connector> section in server.xml file to make sure port 8080 is disabled. To confirm, u se NETCAT tool to test connection to port 8080 : *nc cus.emca.local 8080* *get / http/1. 0*
Objective / Subjective	Objective

Checklist 33. Unneeded files have been removed	
Reference	http://www.macromedia.com/v1/DocumentCenter/Partners/ASZ_ASWPS_Securing_Apache.pdf
Control objective	Unnecessary sample file, shipped scripts, etc. are removed.
Risk	Many sample files have known security holes and contain software package information which may reveal server information and may be helpful for potential attackers. Probability: High
Compliance	There are no sample files on the web server .
Testing	Check all sample applications, sample scripts, etc from Apache installation and ot her installation such as Tomcat, also check any documentation aliases in httpd.conf file to make sure sample files are removed from those directories.
Objective / Subjective	Objective

Checklist 34. Unneeded modules have been removed	
Reference	http://www.macromed ia.com/v1/DocumentCenter/Partners/ASZ_ASWPS_Securing_Apache.pdf http://www.intersectalliance.com/projects/ApacheConfig/
Control objective	Only required modules are installed and loa ded.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 34. Unneeded modules have been removed	
Risk	The more modules web server loads, the more potential vulnerabilities exist which could lead to system crash or compromise. Probability: Medium
Compliance	Minimum modules include: *mod_log_config* *mod_mime* *mod_dir* *mod_imap* *mod_access (disabled fo r Internet web server, enabled for internal web server)* Following compiled modules are required as well in Windows environment : *core* *http_core* *mod_so* *mpm_winnt*
Testing	Review httpd.conf file for modules loaded by default installation, and run following command from \apache\bin directory to check compiled modules : *apache –l*
Objective / Subjective	Objective

2.9. Information Disclosure

Checklist 35. ServerTokens directive	
Reference	http://www.intersec talliance.com/projects/ApacheConfig/ http://httpd.apache.org/docs/mod/core.html
Control objective	Web server OS version number is not disclosed.
Risk	Potential attackers may get useful informat ion of server configuration and derive targeted attack profile. Probability: Medium
Compliance	ServerTokens directive is set to Prod in httpd.conf file:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 35. ServerTokens directive	
	ServerTokens Prod
Testing	Check ServerTokens directive in httpd.conf file and use NETCAT tool to check HTTP response header information: *nc cus.emca.local 80* *head / http/1.0*
Objective / Subjective	Objective

Checklist 36. Server Header	
Reference	http://httpd.apache.org/docs/mod/mod_headers.html http://www.cs.tut.fi/~jkorpela/http.html
Control objective	HTTP response header does not contain server information.
Risk	Potential attackers may get useful information of server configuration and deri ve targeted attack profile. Probability: Medium
Compliance	mod_headers module is loaded and following directive is set in httpd.conf file: *Header unset Server*
Testing	Check Header directive in httpd.conf file and use NETCAT tool to check HTTP response header information: *nc cus.emca.local 80* *head / http/1.0*
Objective / Subjective	Objective

Checklist 37. ServerSignature directive	
Reference	http://www.baylisa.org/library/slides/2002/10/BayLISAApacheWUFTP.pdf http://httpd.apache.org/docs/mod/core.html
Control objective	Footer message, which contains web server

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 37. ServerSignature directive	
	version number and server name , is removed.
Risk	Potential attac kers may get useful information of server configuration and derive targeted attack profile. Probability: Medium
Compliance	ServerSignature directive is turned off in httpd.conf file: *ServerSignature off*
Testing	Check ServerSignature directive in httpd.conf file and use Internet Explorer to check footer message .
Objective / Subjective	Objective

Checklist 38. Error messages do not contain server information	
Reference	http://www.openna.com/ documentations/articles/apache/index.php
Control objective	Server and OS information is not revealed in error message.
Risk	Customized error message may contain server information which can be used by potential attackers to create targeted attack profil e. Probability: Medium
Compliance	Directive ErrorDocument setting does not contain server information in httpd.conf file for following error codes: *400, 401, 403, 404, 405, 408, 410, 411, 412, 413, 414, 415, 500, 501, 502, 503, 506* etc.
Testing	Check Err orDocument directive in httpd.conf file and generate errors to confirm server information is not disclosed.
Objective / Subjective	Objective

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3. Audit Evidence

3.1. Conduct the Audit

A full audit has been performed based on the developed checklist. Among them, 16 most significant tests and their result s are listed below in detail . These tests address the most important security concerns on CUS web server. In following tables, the real server name is replaced with CUS, IP address is replaced with xxx, tracerout e information is removed.

Checklist 1. Latest OS service packs and security patches are installed	
Compliance	The latest service pack (NT4 SP6a, Win2K SP3) is installed, and all relevant security patches have been applied. There shouldn't be any missing patches reported.
Tool/Command	hfnetchk –v –s 1 –x mssecure.xml

The latest OS service pack is applied , but security patches are not up to date, including some critical ones . IIS is installed on the Apache web server and is not patched to the latest level. Following is the result of the scanning performed on 26 May 2003:

```
---------------------------
CUS (xxx.xxx.xxx.xxx)
---------------------------

        * WINDOWS 2000 SERVER SP3

        Patch NOT Found       MS02-063        329834
        File C:\WINNT\system32\drivers\raspptp.sys has an invalid checksum
        and its file version is equal to or less than what is expected.

        Patch NOT Found       MS02-070        329170
        File C:\WINNT\system32\localspl.dll has an invalid checksum and its
        file version is equal to or less than what is expected.

        Patch NOT Found       MS02-071        328310
        File C:\WINNT\system32\msgina.dll has an invalid checksum and its
        file version is equal to or less than what is expected.

        Patch NOT Found       MS03-010        331953
        File C:\WINNT\system32\ole32.dll has an invalid checksum and its
        file version is equal to or less than what is expected.

        Patch NOT Found       MS03-011        816093
        File C:\WINNT\system32\msjava.dll has an invalid checksum and its
        file version is equal to or less than what is expected.

        Patch NOT Found       MS03-013        811493
        File C:\WINNT\system32\basesrv.dll has an invalid checksum and its
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 1. Latest OS service packs and security patches are installed

file version is equal to or less than what is expected.

* INTERNET INFORMATION SERVICES 5.0

Patch NOT Found MS02-062 327696
File C:\WINNT\system32\adsiis.dll has an invalid checksum and its file version is equal to or less than what is expected.

* INTERNET EXPLORER 6 SP1

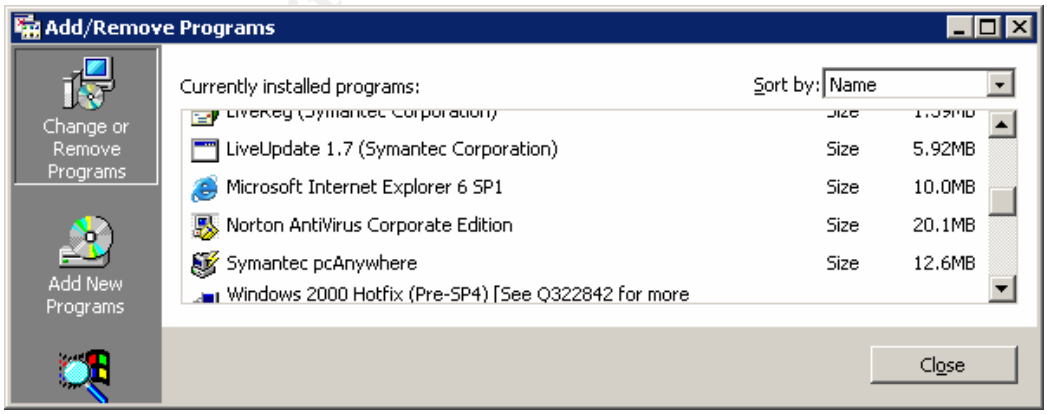
Patch NOT Found MS03-015 813489
The registry key **SOFTWARE \Microsoft\Internet Explorer\ActiveX Compatibility\{06DD38D3-D187-11CF-A80D-00C04FD74AD8}** should have a value of 1024. It has a value of 32.

Conclusion: FAIL

Checklist 3. Antivirus product is running and virus signature file is up to date, action is set to Cure and Quarantine

Compliance	Antivirus product is installed and running with the latest signature file, and the action is set to Cure first, then Quarantine.
Tool/Command	Norton AntiVirus Corporate Edition and EICAR test file.

Norton AntiVirus Corporate Edition is installed on the web server as shown below:



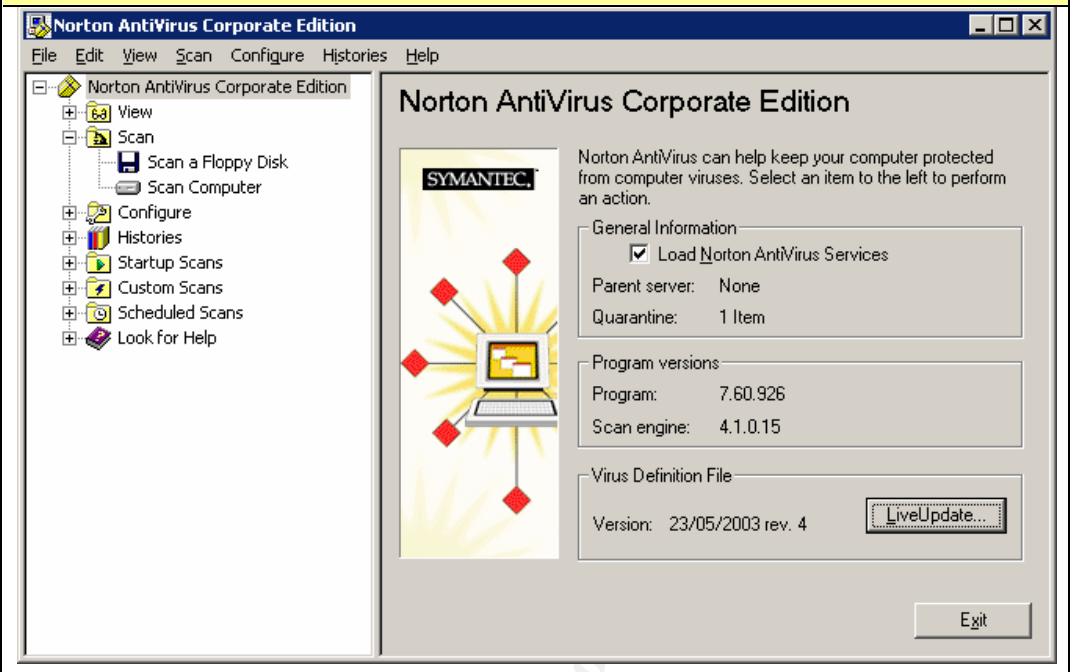
Norton icon is also shown in system tray on t he server:



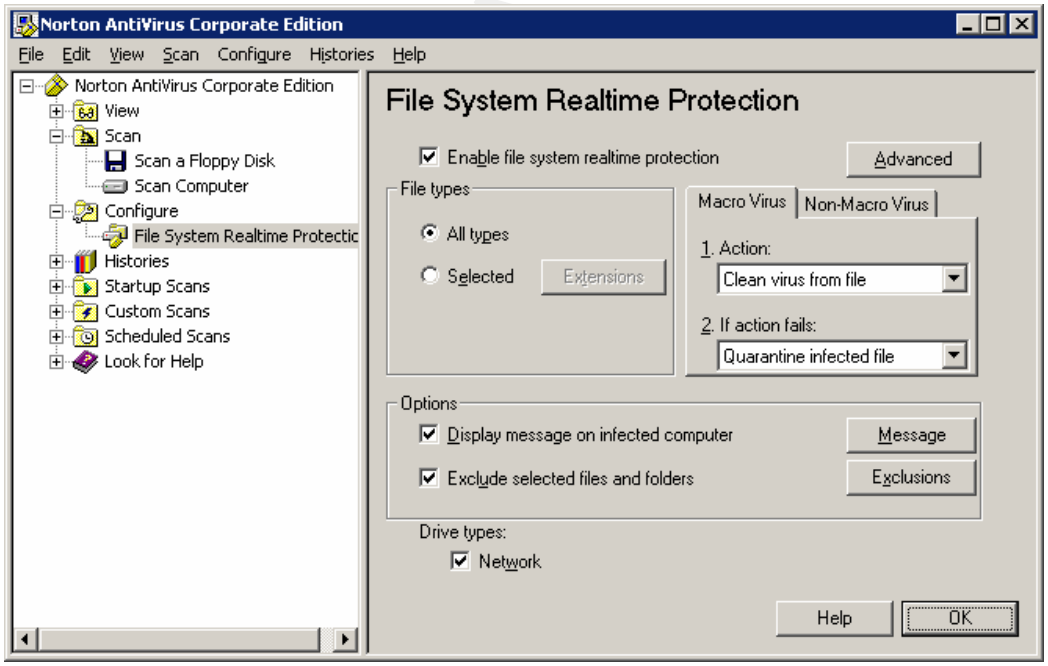
The virus definition file version is shown below:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 3. Antivirus product is running and virus signature file is up to date, action is set to Cure and Quarantine

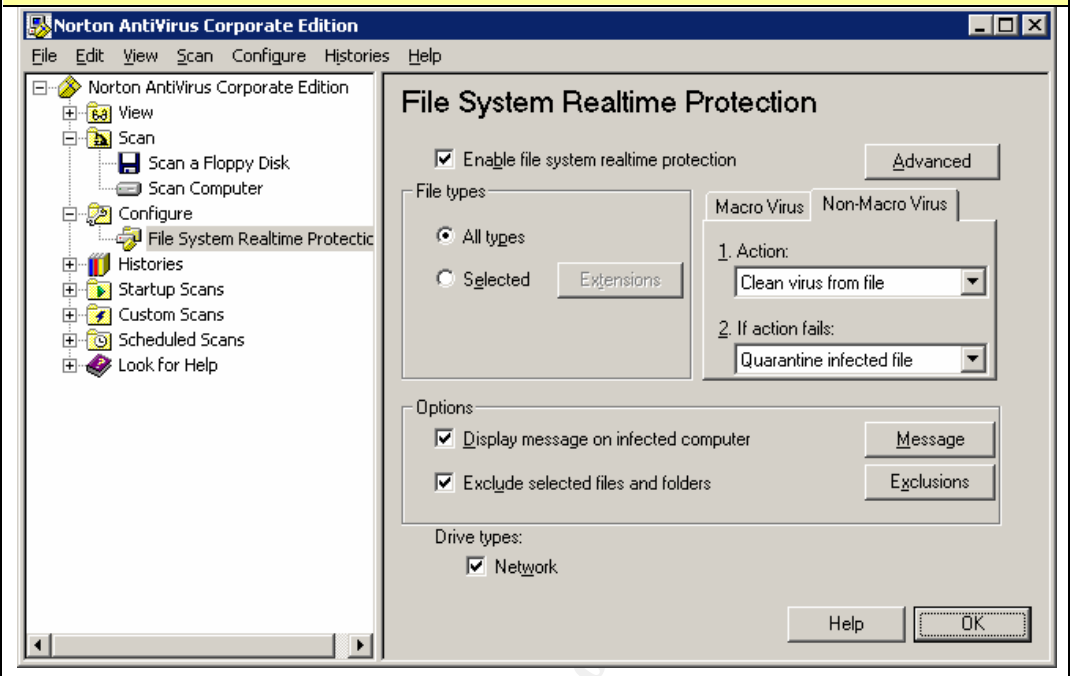


Click on Configure menu item and select File System Realtime Protection, the realtime scanning action is shown below:



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

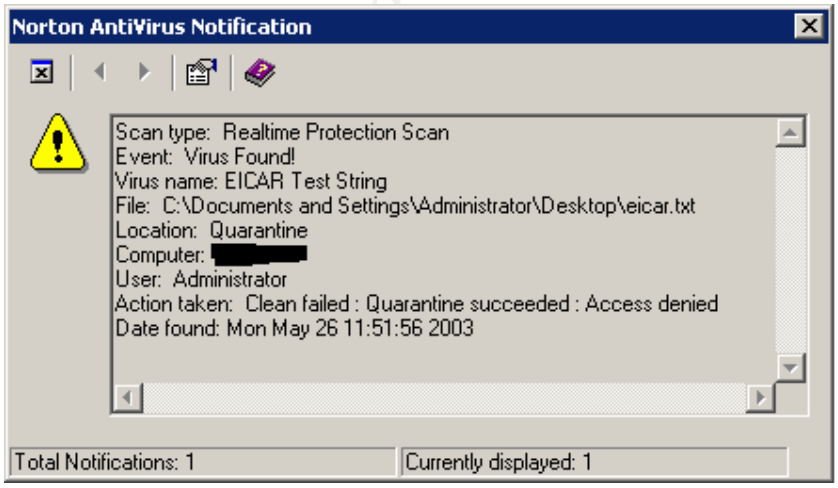
Checklist 3. Antivirus product is running and virus signature file is up to date, action is set to Cure and Quarantine



To confirm the server is protected against virus, a text file was created containing following string:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

The file was named eicar.txt and saved on desktop. Immediately, Norton detected this file and following notification message came out:



First Norton tried to clean it, but failed, then tried to quarantine it and succeeded.

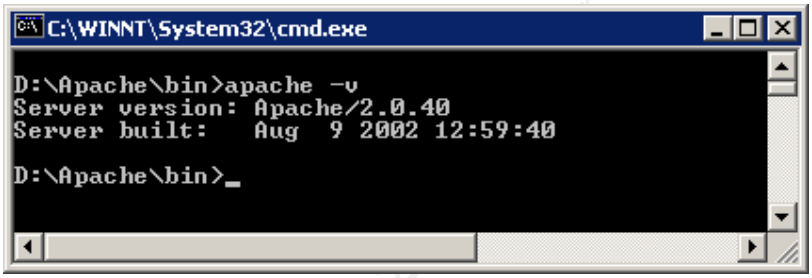
Antivirus program is properly installed and configured, and is actively protecting the web server. It is running with the latest signature file (the test was performed on 26/05/2003; the definition file date was 23/05/2003).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

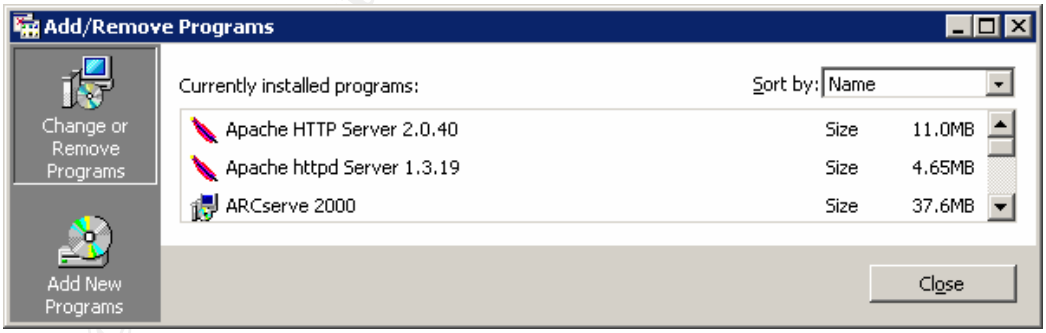
Checklist 3. Antivirus product is running and virus signature file is up to date, action is set to Cure and Quarantine
Conclusion: PASS

Checklist 4. Latest version of Web server application is installed	
Compliance	The latest stable version for Apache 1.3 is 1.3.27, the latest stable version for Apache 2.0 is 2.0.46, the current product quali ty release for Tomcat 3.x is 3.3, and the latest release for Tomcat 4.1.x is 4.1.24.
Tool/Command	1). apache –v 2). \Tomcat\doc\readme file 3). \Tomcat\webapps\ROOT\index.html file

It's found that Apache 2.0.40 is running on the web server:



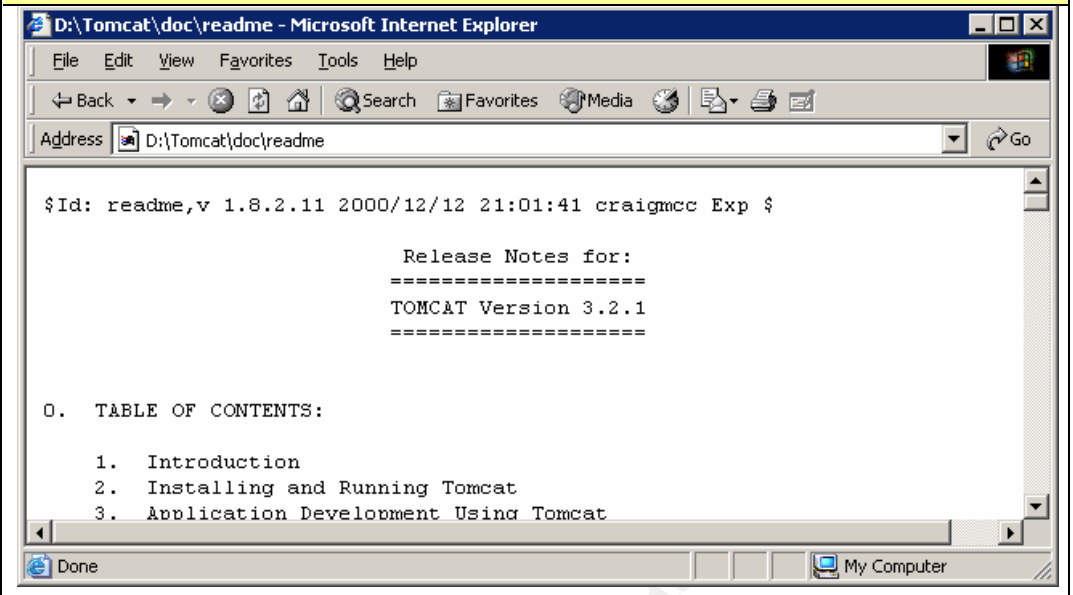
In Add/Remove Programs, two Apache installations show up:



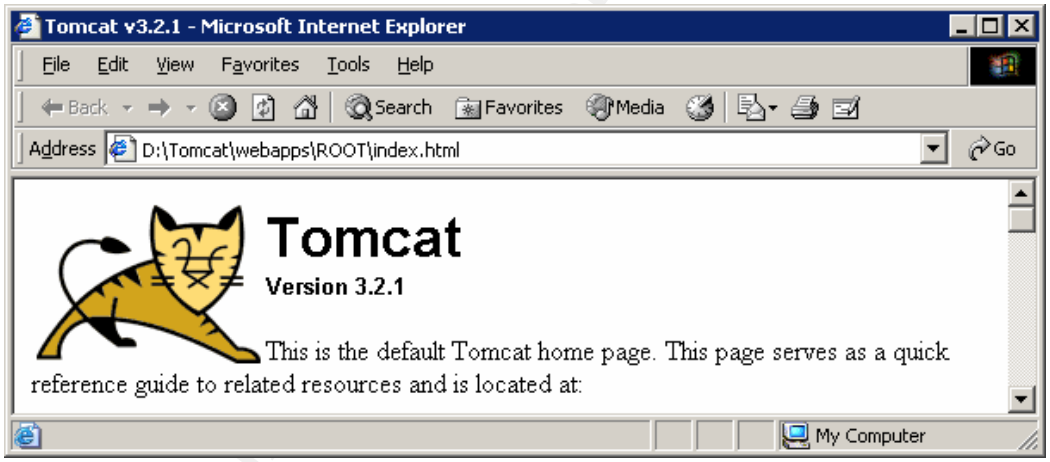
Tomcat is installed on D drive. D:\Tomcat\doc\readme shows Tomcat version is 3.2.1.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 4. Latest version of Web server application is installed



D:\Tomcat\Webapps\ROOT\index.html page also shows the version for Tomcat is 3.2.1.



Apache is running an old version 2.0.40 which h as well known vulnerabilities. For example, certain URLs may give users access to any files on the system [7].

Conclusion: FAIL

Checklist 8. Separate user and group account are created and used for Apache, and defined in httpd.conf file

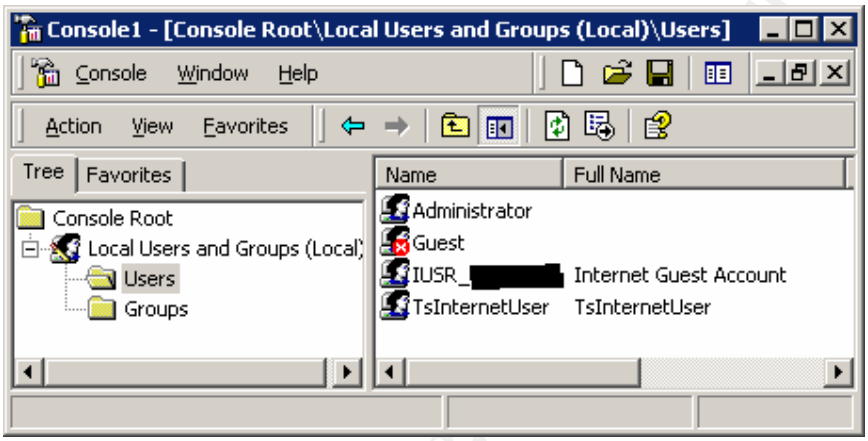
Compliance	Following directives are defined in httpd.conf file: *User*

[7] http://www.apacheweek.com/features/security-20

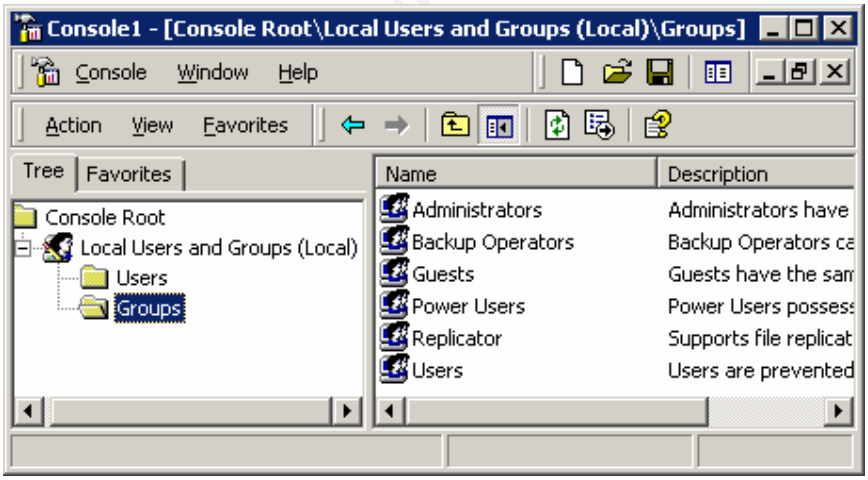
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 8. Separate user and group account are created and used for Apache, and defined in httpd.conf file	
	Group Apache service is running under the normal user account defined in httpd.conf file, and this user account is a member of local Users group.
Tool/Command	1). User and Group directive in httpd.conf file 2). Local Users and Groups snap -in

User and Group directive are not defined in httpd.conf fil e, and no specific user account is defined for Apache service:



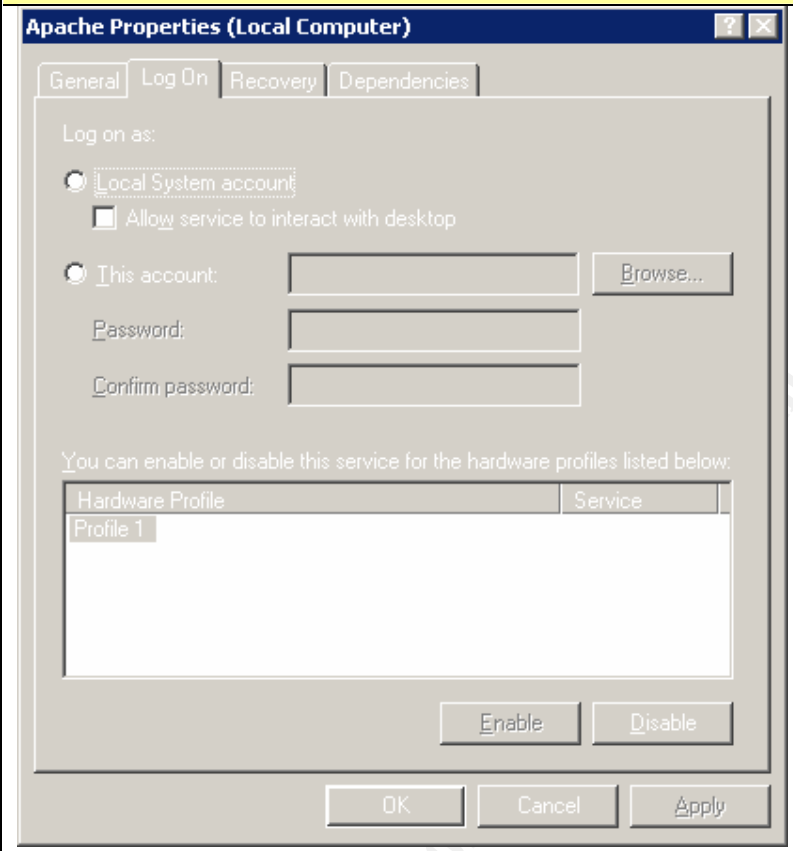
There is no group account defined for Apache either:



Apache is running under Loca l System account:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 8. Separate user and group account are created and used for Apache, and defined in httpd.conf file

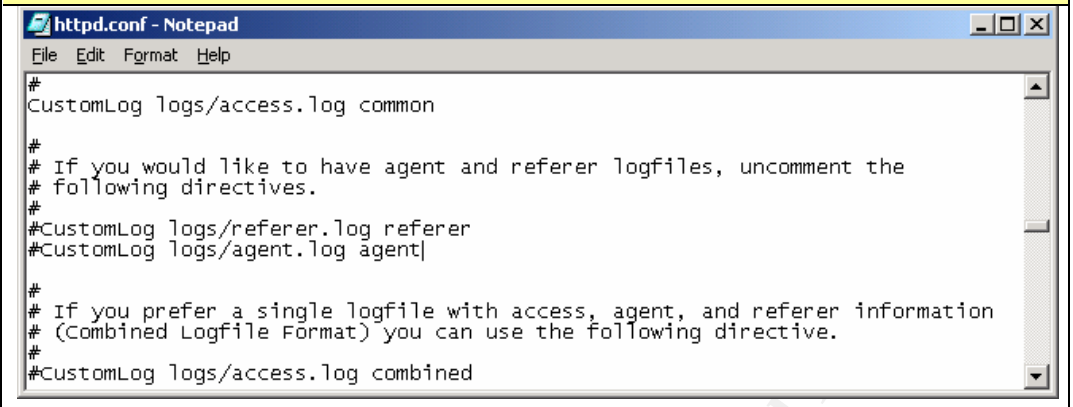


Conclusion: FAIL

Checklist 17. HTTP logging is enabled for entire web	
Compliance	Web site access is logged; optionally referrer and user agent information is logged as well. The CustomLog directive in httpd.conf file is something like: *CustomLog /path/to/audit/logs/access_log common* *CustomLog /path/to/audit/logs/referrer_log referrer* *CustomLog /path/to/audit/logs/agent_log agent*
Tool/Command	CustomLog directive in httpd.conf file and \apache\logs\access.log file.
CustomLog setting in httpd.conf file is:	

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 17. HTTP logging is enabled for entire web



Web site access is logged; Referrer log and user agent log are not required for CUS web site.

Access to survey web site was made and following are the log entries in d:\apache\logs\access.log file (Apache is installed on D drive) :

xxx.xxx.xxx.xxx - - [21/May/2003:11:53:37 +1200] "GET /survey/style_main.css HTTP/1.1" 200 3931
xxx.xxx.xxx.xxx - - [21/May/2003:11:53:38 +1200] "GET /survey/includes/gotoUrl.js HTTP/1.1" 200 129
xxx.xxx.xxx.xxx - - [21/May/2003:11:53:51 +1200] "GET /surve y/marketing/maint_menu.html HTTP/1.1" 200 16913
xxx.xxx.xxx.xxx - - [21/May/2003:11:53:52 +1200] "GET /survey/marketing/demo -only2.gif HTTP/1.1" 200 2018
xxx.xxx.xxx.xxx - - [21/May/2003:11:53:52 +1200] "GET /survey/marketing/maint_menu_files/style_main.cs s HTTP/1.1" 200 3931
xxx.xxx.xxx.xxx - - [21/May/2003:11:54:10 +1200] "GET /survey/survey.jsp?s=19&c=118&p=survey03 HTTP/1.1" 200 25225
xxx.xxx.xxx.xxx - - [21/May/2003:11:54:10 +1200] "GET /survey/images%5csurvey_top.gif HTTP/1.1" 200 232
xxx.xxx.xxx.xxx - - [21/May/2003:11:54:11 +1200] "GET /survey/images%5csurvey_end.gif HTTP/1.1" 200 850

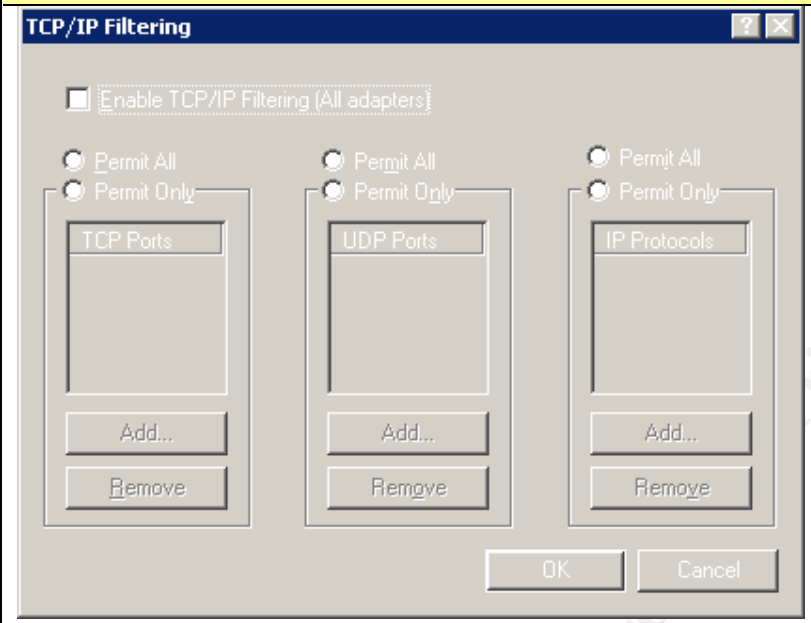
Conclusion: PASS

Checklist 20. TCP/IP filtering is configured

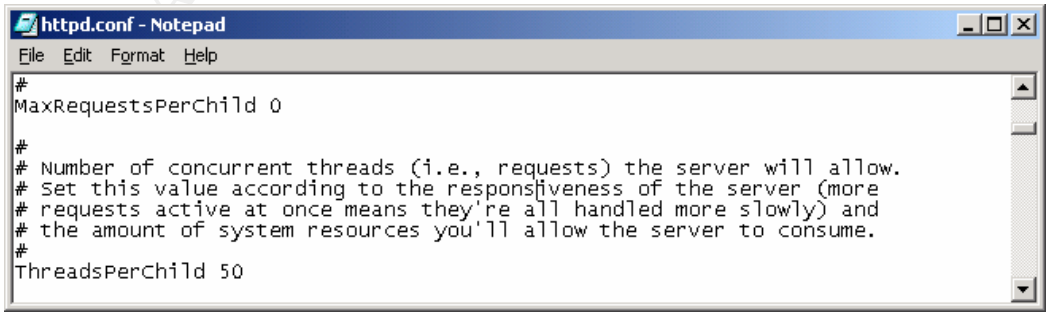
Compliance	Only required network connection ports are allowed, such as port 80 for web server, port 33 89 for terminal services, etc.
Tool/Command	Advanced TCP/IP settings

TCP/IP filtering is not enabled:

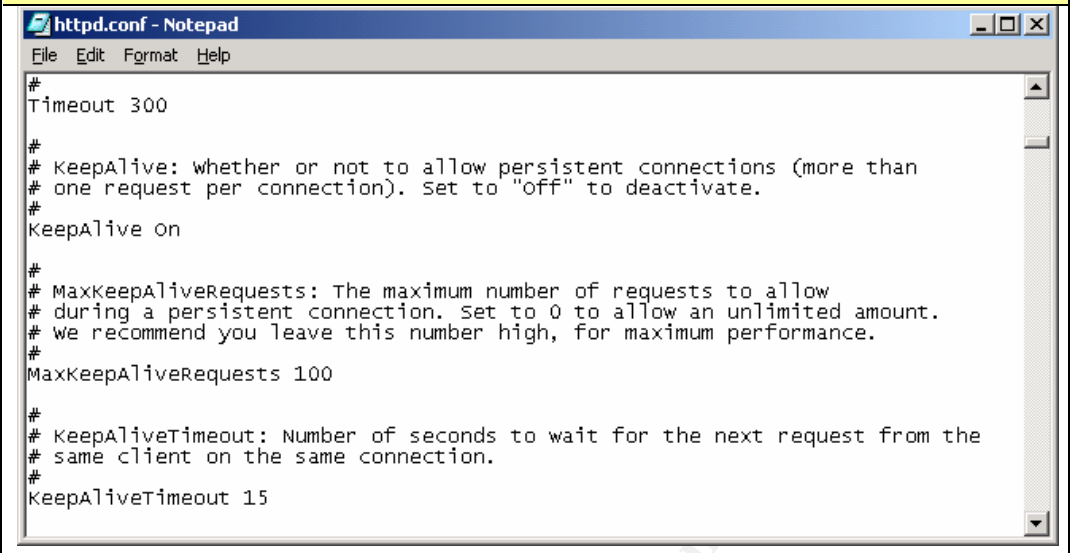
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 20. TCP/IP filtering is configured

Conclusion: FAIL

Checklist 21. Denial of Service	
Compliance	Following directives are set in h ttpd.conf file: *MaxRequestsPerChild 0* *ThreadsPerChild 50* *MaxClients 512* *KeepAliveTimeout 1 0* *MaxKeepAliveRequests 0* *TimeOut 60* *RLimitCPU: unset* *RLimitMEM: unset* *RLimitPROC: unset*
Tool/Command	Check above directives in httpd.conf file .



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 21. Denial of Service

Timeout value 300 seconds is far more than necessary in most situatio ns; number of requests allowed per connection (MaxKeepAliveRequests) is limited to 100 only.
Conclusion: FAIL

Checklist 22. Buffer Overflow	
Compliance	Following directives are set in httpd.conf file: *LimitRequestBody 10240* *LimitRequestFields 40* *LimitRequestFieldsize 100* *LimitRequestLine 500*
Tool/Command	Check above directives in httpd.conf file .
None of these directives is defined in httpd.conf file. Abno rmal client request behavior can not be controlled.	
Conclusion: FAIL	

Checklist 23. Listening po rts	
Compliance	There are no unnecessary ports listening on the server.
Tool/Command	1). nmap –sS –sR –g20 –vv –O –n –p 1-10000 –r –oN <log file> –P0 <target IP address>

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 23. Listening ports	
	2). FPORT

NMAP scanning from Internet :

```
# nmap 3.27 scan initiated Fri May 16 18:13:01 2003 as: nmap -sS -sR -g20 -vv -O -n -p 1-
10000 -r -oN cus.txt -P0 xxx.xxx.xxx.xxx
Interesting ports on xxx.xxx.xxx.xxx:
(The 9997 ports scanned but not shown below are in state: filtered)
Port       State       Service (RPC)
80/tcp     open        http
113/tcp    closed      auth
443/tcp    closed      https
Remote operating system guess: FreeBSD 2.2.1 - 4.1
OS Fingerprint:
TSeq(Class=RI%gcd=1%SI=1038B%IPID=I%TS=0)
T1(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=N)
T3(Resp=Y%DF=Y%W=402E%ACK=S++%Fl ags=AS%Ops=MNWNNT)
T4(Resp=N)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(Resp=N)

TCP Sequence Prediction: Class=random positive increments
                         Difficulty =66443 (Worthy challenge)
TCP ISN Seq. Numbers: 5BE95E7D 5BEAB1AE 5BEE78E5 5BF15BAA
IPID Sequence Generation: Incremental

# Nmap run completed at Fri May 16 18:36:19 2003 -- 1 IP address (1 host up) scanned in
1399.472 seconds
```

NMAP scanning from Intranet :

```
# nmap 3.27 scan initiated Sun May 18 12:24:47 2003 as: nmap -sS -sR -g20 -vv -O -n -p 1-
10000 -r -oN cus.txt -P0 xxx.xxx.xxx.xxx
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open
and 1 closed TCP port
All 10000 scanned ports on xxx.xxx.xxx.xxx are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=3.27%P=i686-pc-windows-windows%D=5/18%Time=3EC6D79F%O= -1%C=-1)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

# Nmap run completed at Sun May 18 12:45:19 2003 -- 1 IP address (1 host up) scanned in
1232.322 seconds
```

FPORT:

```
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com
```


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 23. Listening ports

```
Pid   Process          Port  Proto Path
1388  inetinfo       -> 21    TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
592   Apache         -> 80    TCP   D:\Apache\Apache.exe
428   svchost        -> 135   TCP   C:\WINNT\system32\svchost.exe
8     System         -> 139   TCP
8     System         -> 445   TCP
496   msdtc          -> 1025  TCP   C:\WINNT\System32\msdtc.exe
1108  MSTask         -> 1030  TCP   C:\WINNT\system32\MSTask.exe
1388  inetinfo       -> 1034  TCP   C:\WINNT\System32\inetsrv\inetinfo.exe
8     System         -> 1038  TCP
496   msdtc          -> 3372  TCP   C:\WINNT\System32\msdtc.exe
2188  awhost32       -> 5631  TCP   C:\Program Files\Symantec\pcAnywhere\awhost32.exe
948   casmrtbk       -> 6055  TCP   C:\Program
Files\ComputerAssociates\ARCserve\casmrtbk.exe
1308  java           -> 8007  TCP   d:\jdk1.2.2\bin\java.exe
1308  java           -> 8080  TCP   d:\jdk1.2.2\bin\java.exe

428   svchost        -> 135   UDP   C:\WINNT\system32\svchost.exe
8     System         -> 137   UDP
8     System         -> 138   UDP
8     System         -> 445   UDP
244   lsass          -> 500   UDP   C:\WINNT\system32\lsass.exe
232   services       -> 1033  UDP   C:\WINNT\system32\services.exe
1388  inetinfo       -> 3456  UDP   C:\WINNT\System32\inetsrv\inetinfo.exe
2188  awhost32       -> 5632  UDP   C:\Program Files\Symantec\pcAnywhere\awhost32.exe
1760  MsgSys         -> 38037 UDP   C:\WINNT\System32\MsgSys.EXE
```

NMAP scanning from Internet found only port 80 is listening, scanning from Intranet did not find any listening ports. However, FPORT scanning reveals that locally some unnecessary services are running such as port 8080 and 21.

Conclusion: FAIL

Checklist 24. Known network vulnerabilities are fixed

Compliance	All known vulnerabilities are fixed. Number of security holes should be zero.
Tool/Command	NESSUS scanning from both Internet and Intranet

From Internet

NESSUS was running off a Windows console on Windows 2000 Professional machine, NESSUS server was a RH Linux 7.3 machine. The result is shown below:

	Scan Details
Hosts which where alive and responding during test	1
Number of security holes found	2
Number of security warnings found	3

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 24. Known network vulnerabilities are fixed

Host List

Host(s)	Possible Issue
cus.emca.local	Security hole(s) found

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
cus.emca.local	http (80/tcp)	Security hole found
cus.emca.local	general/tcp	Security notes found
cus.emca.local	general/udp	Security notes found

Security Issues and Fixes: cus. emca.local

Type	Port	Issue and Fix
Vulnerability	http (80/tcp)	Older versions of JServ (including the version shipped with Oracle9i App Server v1.0.2) are vulnerable to a cross site scripting attack using a request for a non-existent .JSP file. Solution: Upgrade to the latest version of JServ available at java.apache.org. Also consider switching from JServ to TomCat, since JServ is no longer maintained. Risk factor : Medium Nessus ID : 10957
Vulnerability	http (80/tcp)	The remote host appears to be vulnerable to the Apache Web Server Chunk Handling Vulnerability. If Safe Checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched Apache versions 1.2.2 and above, 1.3 through 1.3.24 and 2.0 through 2.0.36, the remote server may be running a patched version of Apache *** Note : as safe checks are enabled, Nessus solely relied on the banner to issue this alert Solution : Upgrade to version 1.3.26 or 2.0.39 or newer See also : http://httpd.apache.org/info/security_bulletin_20020617.txt http://httpd.apache.org/info/security_bulletin_20020620.txt Risk factor : High CVE : CAN-2002-0392 BID : 5033 Nessus ID : 11030
Warning	http (80/tcp)	The /cgi-bin directory is browsable. This will show you the name of the installed common scripts and those which are written by the webmaster and thus may be exploitable. Solution : Make the /cgi-bin non-browsable.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 24. Known network vulnerabilities are fixed

		Risk factor : Medium Nessus ID : 10039
Warning	http (80/tcp)	The remote host appears to be running a version of Apache which is older than 1.3.27 There are several flaws in this version, you should upgrade to 1.3.27 or newer. *** Note that Nessus solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive Solution : Upgrade to version 1.3.27 See also : http://www.apache.org/dist/httpd/Announcement.html Risk factor : Medium CVE : CAN-2002-0840 BID : 5847 Nessus ID : 11137
Warning	http (80/tcp)	Your webserver supports the TRACE and/or TRACK methods. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for 'Cross-Site-Tracing', when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials. Solution: Disable these methods. If you are using Apache, add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK) RewriteRule .* - [F] If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html Risk factor : Medium Nessus ID : 11213
Informational	http (80/tcp)	A web server is running on this port Nessus ID : 10330
Informational	http (80/tcp)	The remote web server type is : Apache/1.3.19 (Win32) tomcat/1.0 Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 24. Known network vulnerabilities are fixed

		headers. Nessus ID : 10107
Informational	http (80/tcp)	The following directories were discovered: /cgi-bin, /examples, /help, /icons, /images, /includes, /marketing, /test Nessus ID : 11032
Informational	general/tcp	Remote OS guess : FreeBSD 2.2.1 - 4.1 CVE : CAN-1999-0454 Nessus ID : 11268

From Intranet

NESSUS was running off a Windows console on Windows 2000 Professional machine, NESSUS server was a RH Linux 7.3 machine sitting in public DMZ. The result is shown below:

Summary of scanned hosts

Host	Holes	Warnings	Open ports	State
xxx.xxx.xxx.xxx	2	14	3	Finished

xxx.xxx.xxx.xxx

Service	Severity	Description
ftp (21/tcp)	Info	Port is open
http (80/tcp)	Info	Port is open
pcanywheredata (5631/tcp)	Info	Port is open
http (80/tcp)	High	The remote host appears to be vulnerable to the Apache Web Server Chunk Handling Vulnerability. If Safe Checks are enabled, this may be a false positive since it is based on the version of Apache. Although unpatched Apache versions 1.2.2 and above, 1.3 through 1.3.24 and 2.0 through 2.0.36, the remote server may be running a patched version of Apache *** Note : as safe checks are enabled, Nessus solely relied on the banner to issue this alert Solution : Upgrade to version 1.3.26 or 2.0.39 or newer See also : http://httpd.apache.org/info/security_bulletin_20020617.txt http://httpd.apache.org/info/security_bulletin_20020620.txt Risk factor : High CVE : CAN-2002-0392 BID : 5033
ftp (21/tcp)	High	It may be possible to make the remote FTP server crash by sending the command 'STAT *?AAA...AAA. An attacker may use this flaw to prevent your site from distributing files *** Warning: we could not verify this vulnerability. *** Nessus solely relied on the banner of this server Solution : Apply the relevant hotfix from Microsoft See:http://www.microsoft.com/technet/security/bulletin/ms02-018.asp Risk factor : High

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 24. Known network vulnerabilities are fixed

		CVE : CAN-2002-0073 BID : 4482
ftp (21/tcp)	**Low**	This FTP service allows anonymous logins. If you do not want to share data with anyone you do not know, then you should deactivate the anonymous account, since it can only cause troubles. Under most Unix system, doing : echo ftp >> /etc/ftpusers will correct this. Risk factor : Low CVE : CAN-1999-0497
ftp (21/tcp)	**Low**	Remote FTP server banner : 220 cus Microsoft FTP Service (Version 5.0).
general/tcp	**Low**	Remote OS guess : Windows 2000 Advanced Server SP3 CVE : CAN-1999-0454
ftp (21/tcp)	**Low**	An FTP server is running on this port. Here is its banner: 220 cus Microsoft FTP Service (Version 5.0).
general/udp	**Low**	For your information, here is the traceroute to xxx.xxx.xxx.xxx : xxx.xxx.xxx.xxx
http (80/tcp)	**Low**	A web server is running on this port
general/tcp	**Low**	The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host. An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things. Solution : Contact your vendor for a patch Risk factor : Low
http (80/tcp)	**Low**	The following CGI have been discovered : Syntax : cginame (arguments [default value]) /survey/marketing/ (D [A] M [A] N [D] D=D [] S [A]) /survey/marketing/Assign_access_to_Surveys_files/ (D [A] M [A] N [D] S [A]) /survey/marketing/Maintain_Surveys1_files/ (D [A] M [A] N [D] S [A]) /survey/marketing/cust_sat_preview2.html (javascriptOn [no]) /survey/marketing/maint_menu.html (clientPassword [xx] clientEmail [joe_bloggs@emca.local] positionListButton [list] clientPosition [Senior Manager] clientName [joe bloggs] action [second time around] surveyAccess_3 [true] cancel [Cancel] surveyAccess_4 [true] clientCompany [emca] subject [] companyListButton [list] surveyAccess_7 [] clientPhone [555-2222] clientValid [true] clientFax [1234567] clientComment [] clientAction [second time around] copyToSenderString [true] from [] surveyAccess_-1 [true] passwordInUTLString [true]) /icons/ (D [A] M [A] N [D] S [A]) /survey/marketing/Email_Survey_Link_to_Client_files/ (D [A] M [A] N [D] S [A]) Directory index found at /survey/marketing/ Directory index found at /icons/ Directory index found at /survey/marketing/Assign_access_to_Surveys_files/ Directory index found at /survey/marketing/Email_Survey_Link_to_Client_files/ Directory index found at /survey/marketing/Maintain_Surveys1_files/

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 24. Known network vulnerabilities are fixed		
http (80/tcp)	**Low**	The remote web server type is: Apache/1.3.19 (Win32) tomcat/1.0 Solution: You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.
http (80/tcp)	**Low**	The remote host appears to be running a version of Apache which is older than 1.3.27 There are several flaws in this version, you should upgrade to 1.3.27 or newer. *** Note that Nessus solely relied on the version number *** of the remote server to issue this warning. This might *** be a false positive Solution : Upgrade to version 1.3.27 See also : http://www.apache.org/dist/httpd/Announcement.html Risk factor : Medium CVE : CAN-2002-0839, CAN-2002-0840, CAN-2002-0843 BID : 5847, 5884, 5995, 5996
http (80/tcp)	**Low**	The following Word files (.doc) are available on the remote server : /survey/marketing/Overview_Short.doc /survey/marketing/Overview.doc You should make sure that none of these files contain confidential or otherwise sensitive information. An attacker may use these files to gain a more intimate knowledge of your organization and eventually use them do perform social engineering attacks (abusing the trust of the personel of your company). Solution: sensitive files should not be accessible by everyone, but only by authenticated users.
http (80/tcp)	**Low**	Older versions of JServ (including the version shipped with Oracle9i App Server v1.0.2) are vulnerable to a cross site scripting attack using a request for a non-existent .JSP file. Solution: Upgrade to the latest version of JServ available at java.apache.org. Also consider switching from JServ to TomCat, since JServ is no longer maintained. Risk factor : Medium
http (80/tcp)	**Low**	The following directories were discovered: /admin, /cgi-bin, /examples, /help, /icons, /images, /includes, /marketing, /test
http (80/tcp)	**Low**	Your webserver supports the TRACE and/or TRACK methods. It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for 'Cross-Site-Tracing', when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials. Solution: Disable these methods. If you are using Apache, add the following lines for each virtual host in your configuration file : RewriteEngine on RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)

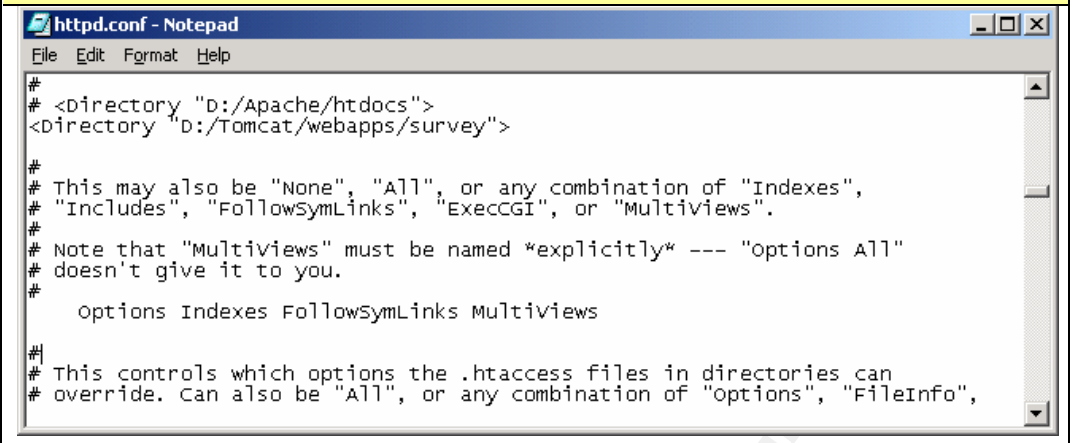
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

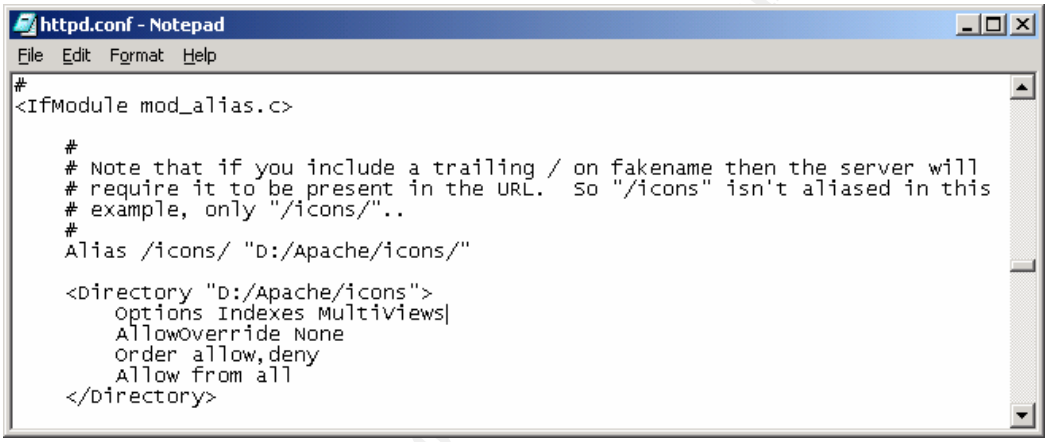
Checklist 24. Known network vulnerabilities are fixed	
	RewriteRule .* - [F] If you are using Microsoft IIS, use the URLScan tool to deny HTTP TRACE requests or to permit only the methods needed to meet site requirements and policy. See http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html Risk factor : Medium
Several security holes were identified. One of the se curity holes is related to an old Apache Chunk Handling vulnerability existing in version 1.3.26. This is caused by the incorrect server banner detected by NESSUS as two instances of Apache installation (version 2.0.40 and version 1.3.19) appear to exist o n CUS web server. An old version of JServer was found running on the server, which is vulnerable for cross site scripting attacks. JServer should be either replaced with Tomcat or upgraded to the latest version. The FTP server allows anonymous login, which is a potential security risk. CUS web server is used for customer survey, not file transfer, FTP should be removed. TRACE and TRACK method should be disabled otherwise the server is vulnerable for cross site scripting attacks as well .	
Conclusion: FAIL	

Checklist 26. Indexing is disabled	
Compliance	Options directive is NOT set to following in httpd.conf file and Tomcat configuration file included in httpd.conf file : *Options Indexes* and mod_autoindex module is disabled. Because mod_autoindex module is bo und into Apache binary distribution for Windows and is active in default Apache installation, to disable this module, ClearModuleList directive must be used and other core modules be loaded individually.
Tool/Command	Check Options directive in both httpd .conf file and Tomcat configuration file, and then use Internet Explorer to confirm
Indexing is enabled for following directories in httpd.conf file:	

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

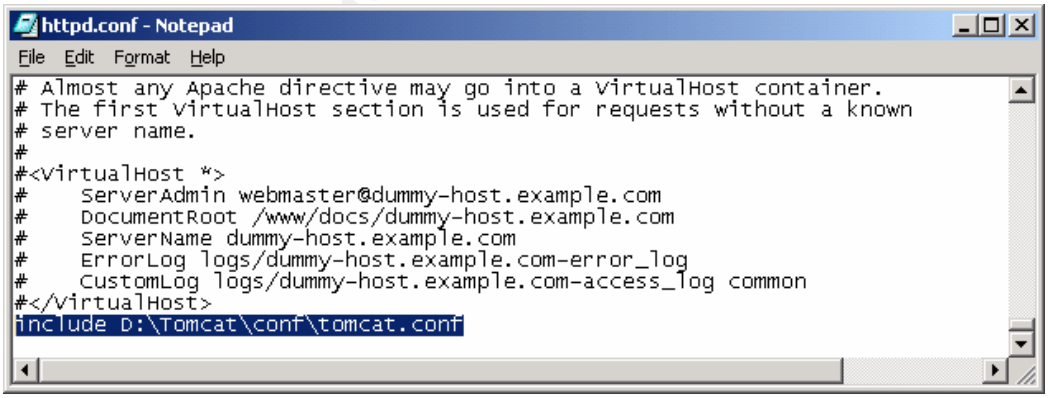
Checklist 26. Indexing is disabled





mod_alias module is loaded by default in Apache for Windows installation.

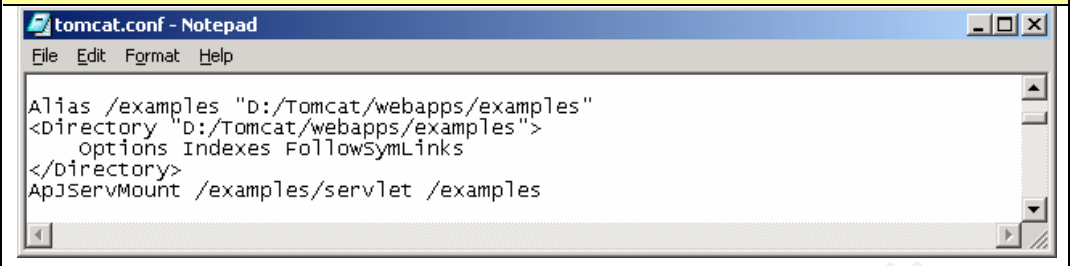
Tomcat configuration file i ncluded in httpd.conf file is tomcat.conf:

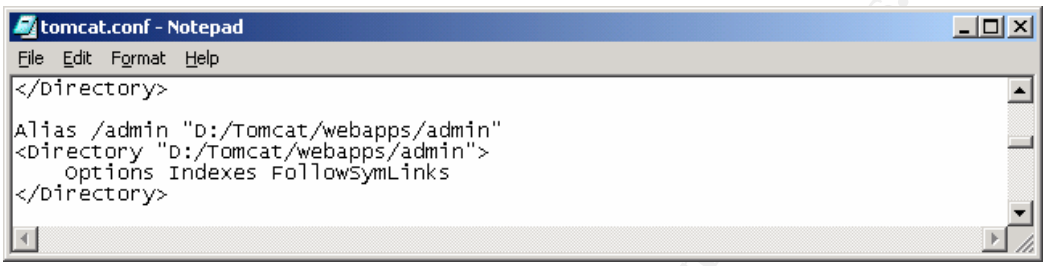


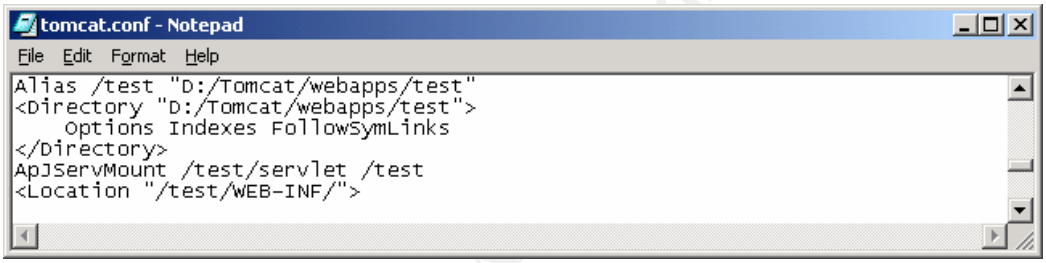
Indexing is also enabled in tomcat.conf file:

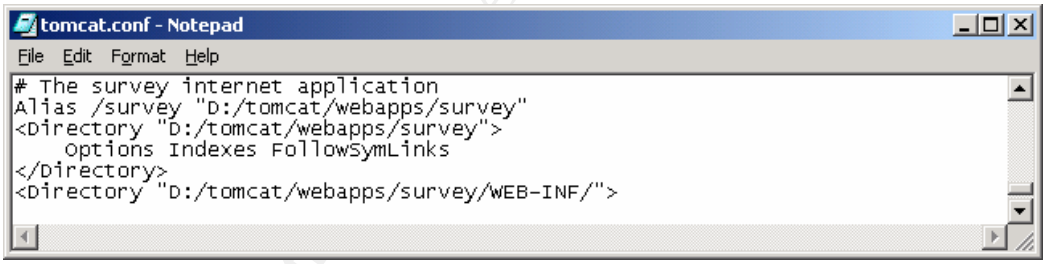
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 26. Indexing is disabled





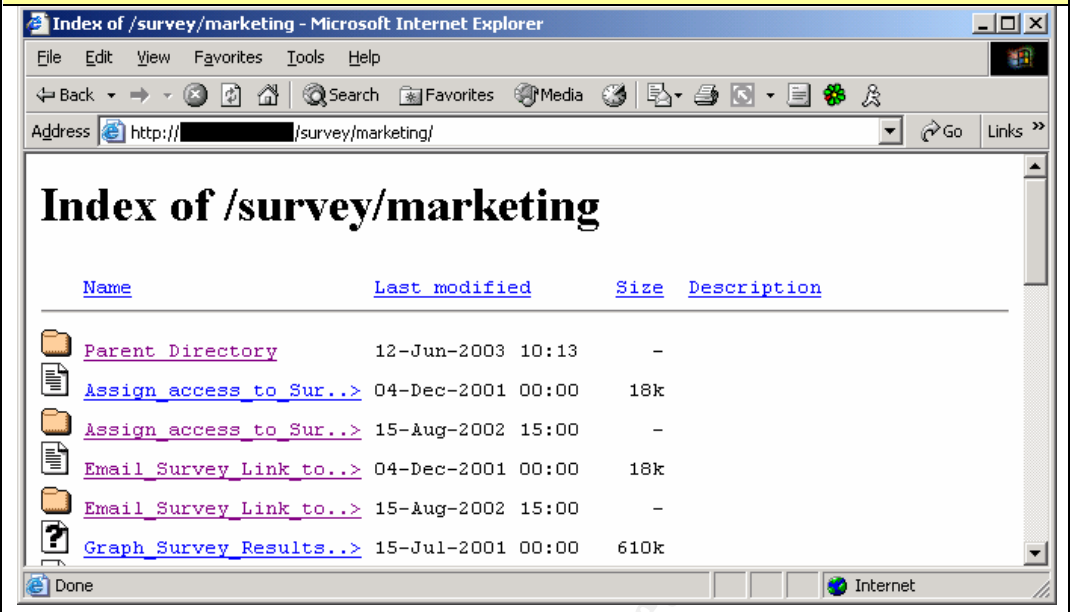




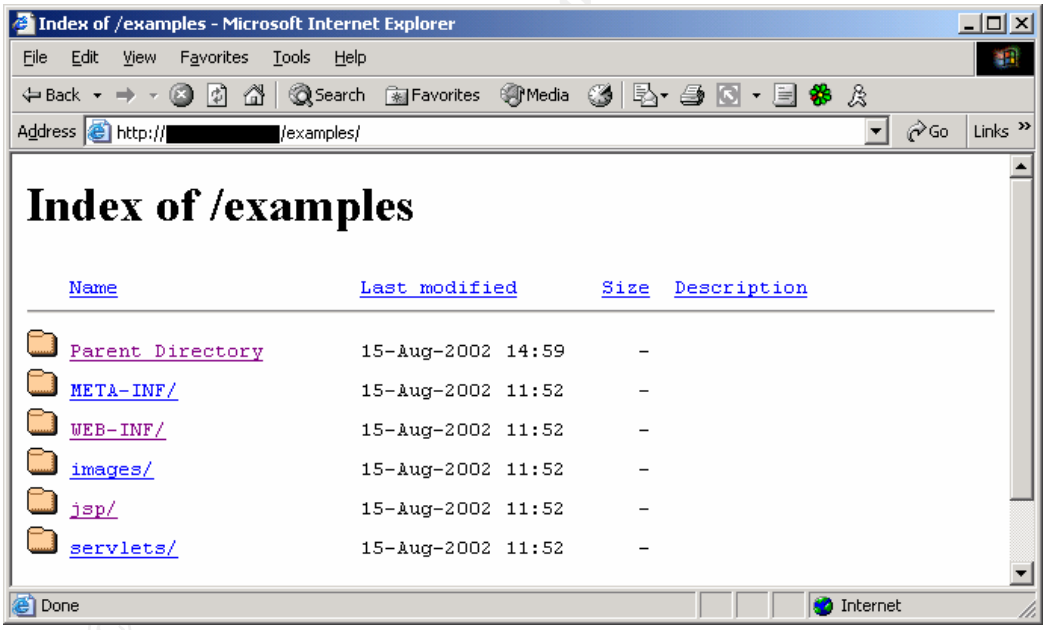
http://cus.emca.local/survey/marketing/ displays the content of D:\Tomcat\webapps\survey\marketing directory:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 26. Indexing is disabled



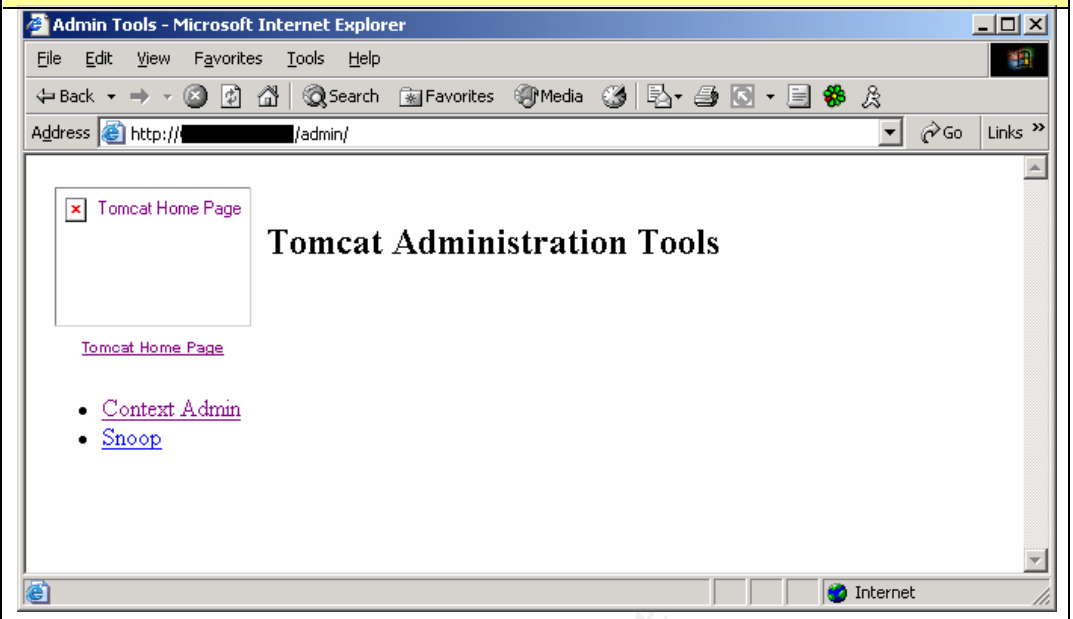
http://cus.emca.local/examples/ displays the sample files in d:\Tomcat\webapps\examples directory:



and http://cus.emca.local/admin/ shows the Tomcat admin tools in d:\Tomcat\webapps\admin directory:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 26. Indexing is disabled

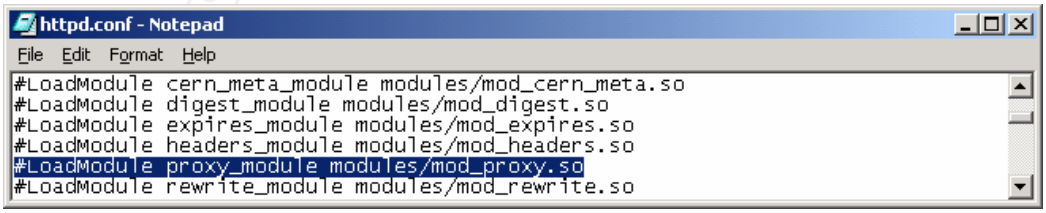


Content of different directories are exposed, especially those directories containing sample files and scripts.

Conclusion: FAIL

Checklist 28. Proxy functionality is disabled	
Compliance	mod_proxy module is not loaded.
Tool/Command	1). LoadModule directive in httpd.conf file 2). nc cus.emca.local 80 get http://www.microsoft.com http/1.0

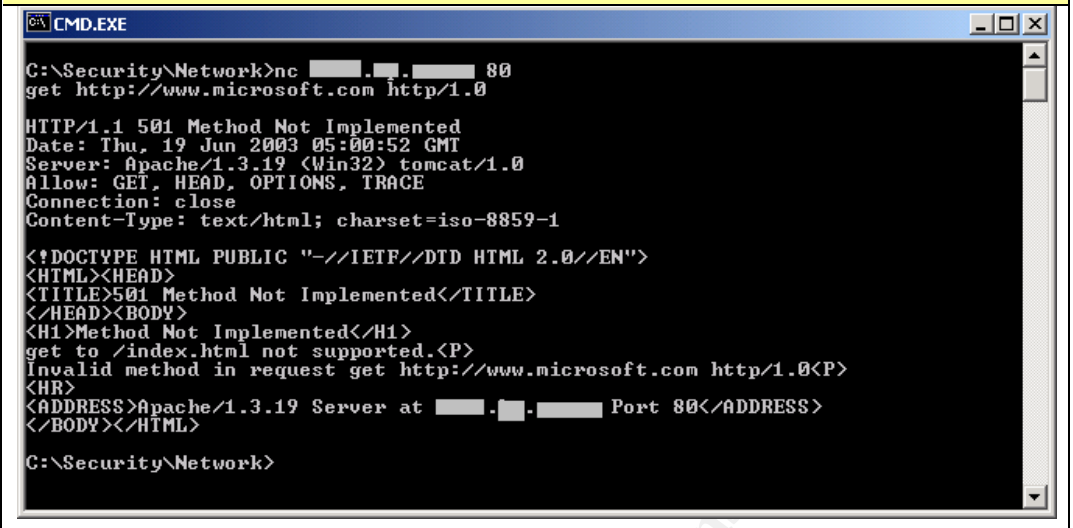
mod_proxy module is not load ed:



NETCAT command output is:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 28. Proxy functionality is disabled



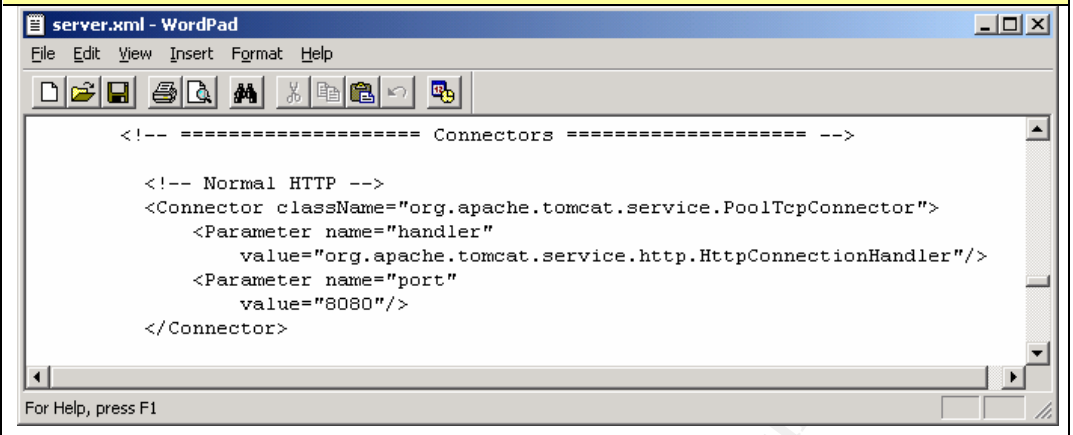
Request to Microsoft home page generated 5 01 error code, which means CUS web server does not support the functionality required to fulfill this request, that is, CUS web server does not provide web proxy functionality.

Conclusion: PASS

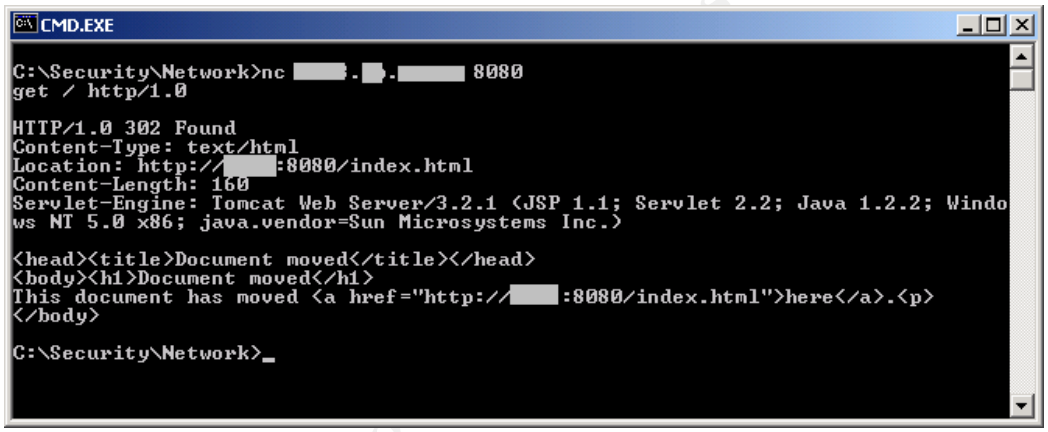
Checklist 32. Web server is disabled on port 8080 for Tomcat	
Compliance	Following should be commented out in server.xml: *<Connector className="org.apache.tomcat.service.SimpleTcpConnector">* *<Parameter name="handler" value="org.apache.tomcat.service.http.HttpConnectionHandler"/>* *<Parameter name="port" value="8080"/>* *</Connector>*
Tool/Command	1). <Connector> section in server.xml file 2). nc cus.emca.local 8080 get / http/1.0
<Connector> setting in server.xml file is:	

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 32. Web server is disabled on port 8080 for Tomcat



NETCAT command output is:



Tomcat is listening on port 8080 for connections. This also shows Tomcat version is 3.2.1.

Conclusion: FAIL

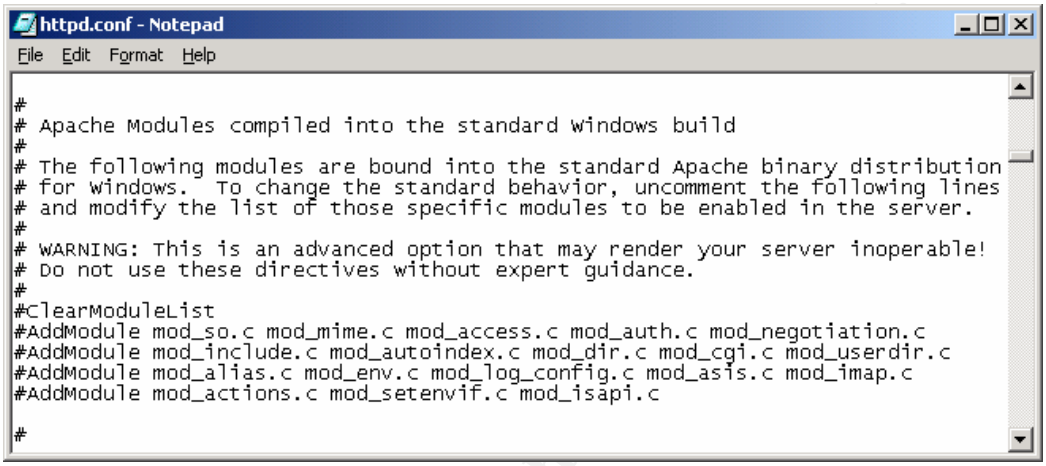
Checklist 34. Unneeded modules have been removed

Compliance	Minimum modules include: *mod_log_config* *mod_mime* *mod_dir* *mod_imap* *mod_access (disabled for Internet web server, enabled for internal web server)* Following compiled modules are required as well in Windows environment: *core* *http_core* *mod_so*

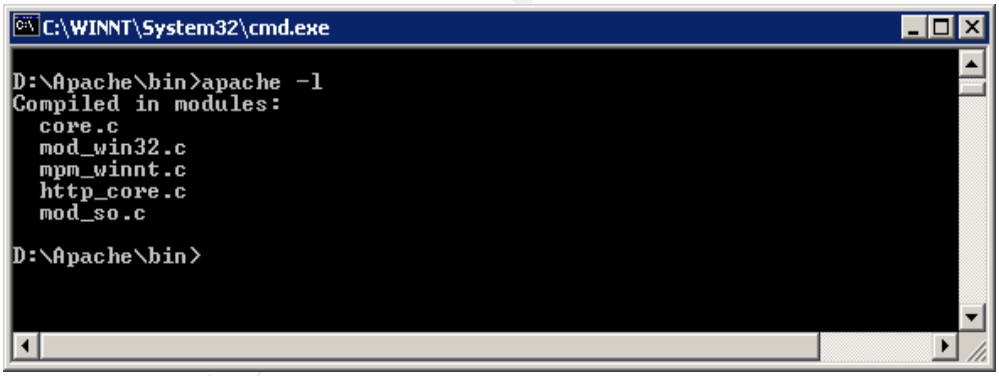
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 34. Unneeded modules have been removed	
	mpm_winnt
Tool/Command	1). httpd.conf file 2). apache -l

By default, following modules are active in Apache installation on Windows platform:



Apache –l command reveals following compiled in modules:

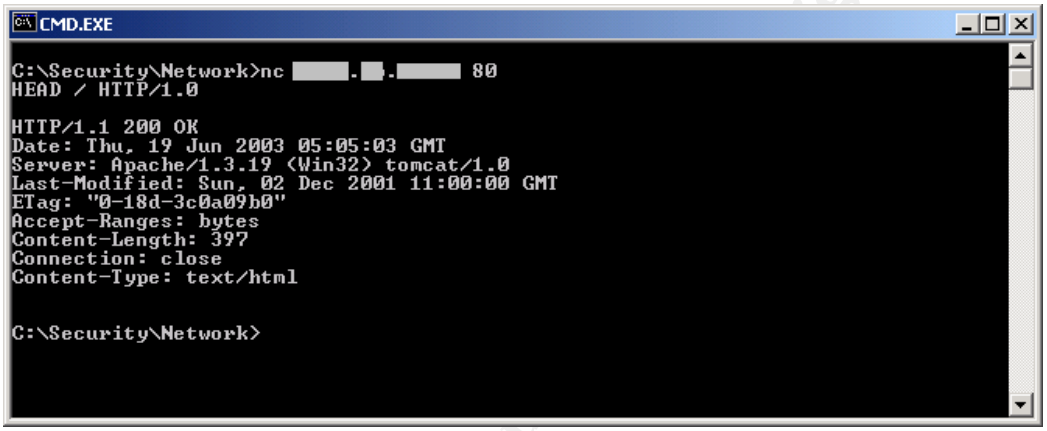


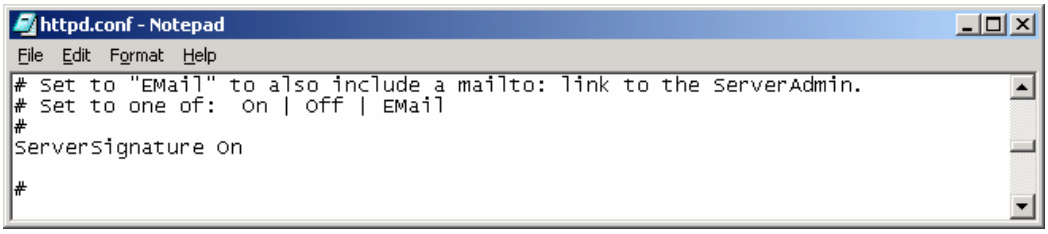
These modules are more than necessary to run the web site. ClearModuleList directive should be used and only necessary mod ules are loaded by using AddModule directive.

Conclusion: FAIL

Checklist 35. ServerTokens directive	
Compliance	ServerTokens directive is set to Prod in httpd.conf file: *ServerTokens Prod*

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

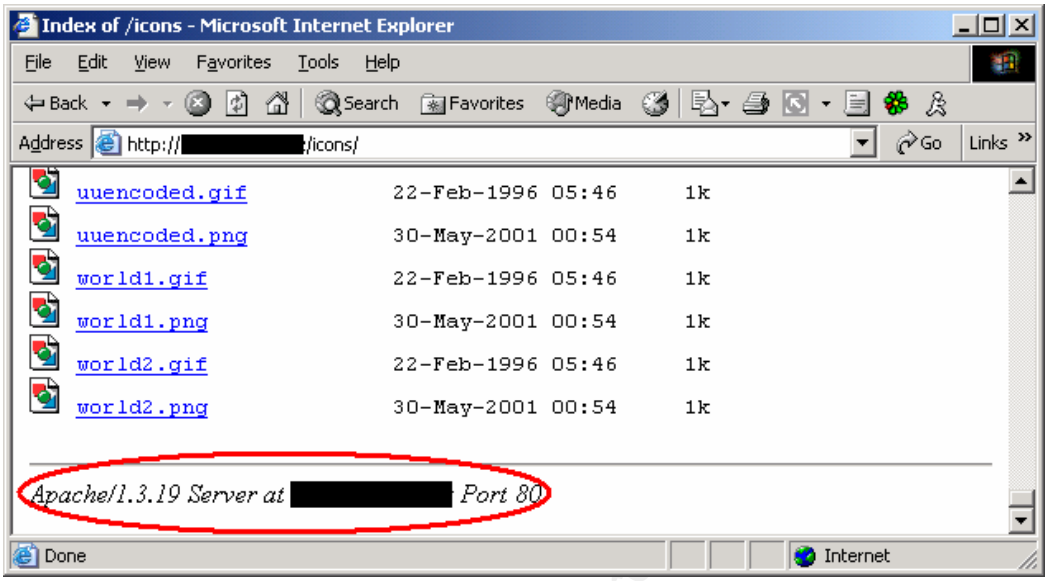
Checklist 35. ServerTokens directive	
Tool/Command	1). ServerTokens directive in httpd.conf file 2). nc cus.emca.local 80 head / http/1.0
This directive is not present in httpd.conf file. If it is not specified, by default, ServerTokens directive is set to Full. NETCAT command output is:  OS type of the web server and compiled in module inform ation are shown in response header.	
Conclusion: FAIL	

Checklist 37. ServerSignature directive	
Compliance	ServerSignature directive is turned off in httpd.conf file: *ServerSignature off*
Tool/Command	1). ServerSignature directive in httpd.conf file 2). Internet Explorer
ServerSignature is turned on in httpd.conf file:  	

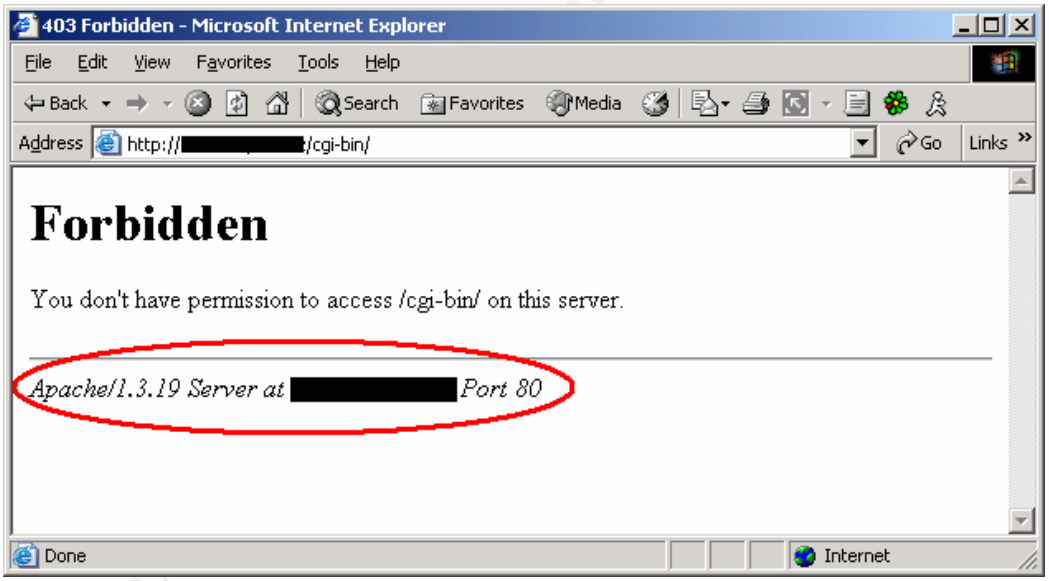
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Checklist 37. ServerSignature directive

Directory content page displays software information :



Error message page also shows software information:



Web server software and version information is e xposed.

Conclusion: FAIL

3.2. Measure Residual Risk

According to EMCA company's system security policy, the public web server CUS is categorized as Internet server, which means it must conform to the highest security standard . The scope of this audit is fo r Apache only, and

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

based on the audit result, although CUS web server provides customer survey functionality, it fails to meet most of the security requirements stated in the checklist.

Most of the vulnerabilities found on CUS web server are a result of inappropriate Apache server installation and configuration. Lack of security processes and control of these processes contributes to the poor security status on CUS web server as well. For example, quite a few base OS patches are not applied; Apache and Tom cat are not the latest version. To fix these issues, additional Apache configuration must be performed, security patch management process must be applied and regular security audit must be conducted to ensure the process is followed and web server security status is maintained.

Customer access to survey web site is via Internet, that is, HTTP traffic to destination port 80. However, port 80 traffic can also contain malicious packets, such as Code Red worm, buffer overflow attack, Unicode attack, etc. The risk always exists and cannot be eliminated as long as port 80 traffic is allowed on firewall. To reduce the risk, one of the detective controls that can be implemented is host based intrusion detection (HIDS). Depending on the product in use, the cost can range from zero (free IDS such as SNORT) to about US$600 (ISS Server Sensor). Together with IDS, a proper altering and incidence handling process should be utilized in order to respond to port 80 attacks quickly and effectively. The cost for implementing this control would be software cost, half-day installation and configuration, plus on-going management.

Ideally, only necessary modules are loaded on Apache web server. In reality, there are many modules that are active in default Apache installation on Windows platform. You could clear all default modules and only load those required ones in httpd.conf configuration file, but in most cases, people just keep those modules running. The risk does exist that having more modules running means more potential vulnerabilities and security holes, but it is small because even if the modules are loaded, they may not be actually in use. For example, mod_autoindex and mod_alias module are loaded by default, however, there will not be any security concerns for index, alias and script alias if they are not used at all, although the security concern for running too many modules still exists. To address this kind of security concern, periodic security audit should be performed to make sure the latest software is installed and patches are up to date. With a checklist available, this audit should be finished within two working days.

3.3. Is the System Auditable?

Based on the purpose and scope of this audit, the checklist, with all items being objective, is effective and appropriate to audit Apache web server on Windows platform.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

All items can be audited against best practices indicated in the references, except checklist 38 because it is easy to generate 403, 404 and several other errors, but difficult to reproduce all error codes to check compliance.

Security is a process, and maintaining secure status is also an important part of overall web site security. Therefore, to have a complete picture of web server security, process audit should be performed, which may include patch management process, incident response process, monitoring and alerting process, access control (physical and remote) process, change management process, backup/restore process, etc.

4. Audit Report

4.1. Executive Summary

This audit examined the security of customer survey web server CUS running Apache web server and Tomcat on Windows 2000 platform. The purpose of the audit was to make the server more secure by checking server configurations against industry best practices. The audit focused on web server configuration only, base OS, network and application security were out of scope.

The audit objective was achieved. The biggest security concern of this server is software is not patched to the latest level, including base operating system, Apache and Tomcat. As a result, well-known software flaws and security vulnerabilities exist on this server. These flaws and vulnerabilities can be used by malicious users to attack this box.

Another security concern is the web server was installed to its default configuration, which led to unnecessary services and modules running, as well as server software information disclosure. More services and modules means more chances of system flaws and security holes. By reading server software information, potential attackers may derive targeted attack profile.

Default Apache configuration also enabled indexing on the CUS web server. This exposed the content of several directories containing sample files and scripts. Any remote user can run these sample files and scripts that may have security holes and would expose server for potential attacks.

Apache web server was also found running as a privileged user on the system with full permissions on local drives and local system resources. The chances are remote attacker may conduct further exploits under privilege account's context such as gaining full access to local system by attacking Apache service.

Although most of the security weaknesses found on the CUS web server can be fixed easily by server configuration change, it does suggest that there is an

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

issue of following existing company security processes and policies, and lacking effective controls that ensure the processes and policies are followed. On the other hand, this audit shows the importance and the value of regular security audit.

4.2. Audit Findings

Following items were found during the audit not complying with control objectives.

4.2.1. Server software is not patched to the latest level

Reference: Checklist 1, Checklist 4, Checklist 2 4, Checklist 32

Microsoft patch checking tool HFNETCHK and the latest MSSECURE.XML file were used to check the patch level of Windows 2000 Server. Apache command and Tomcat homepage were used to check version information for web server software.

It's found that there were critical patches missing fo r Windows 2000 Server and IIS (page 40-41). It was also found that Apache and Tomcat were not running with the latest version (page 44-45). Besides, two versions of Apache appeared in Add/Remove Programs, this might be caused by Apache upgrade from one version to another instead of a fresh installation.

Because of un-patched software running on CUS web server, network vulnerability scanning discovered security holes on the box (page 53-58).

Background/Risks

In most cases, security patches and software u pgrade are released to specifically fix certain flaws and vulnerabilities in software packages. These vulnerabilities are normally discovered by individuals or third party companies rather than software vendors, and in most cases these vulnerabilities are well-known on Internet. Exploit codes can be written to specifically attack machines with known security vulnerabilities and these codes are often freely available to download. Code Red worm is a classic example of how vulnerability, even an old one, can c ause a major security breach and business damage and interruption that cost millions or even billions of dollars.

Because the software on CUS web server is not patched to the latest level, potential attackers could exploit the known vulnerabilities existi ng in Windows 2000, Apache or Tomcat to attack this box. They could potential gain access to the sensitive and confidential customer survey data stored on the box, or they could cause a denial of service attack so legitimate users could not create or compl ete a customer survey. They could also use this server as a zombie to attack other Internet machines. In whatever case, damage will be done on EMCA company business and reputation.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Recommendation

Immediate solution is to apply all missing security patches for Windows 2000 and Apache (Apache patches can be found at http://www.apache.org/dist/httpd/patches/). If possible, upgrade Apache and Tomcat to the latest release.

To keep up with the latest vulnerabilities, Windows and Apache administrators should subscribe to security mailing lists such as BUGTRAQ and those from software vendors. Patch management process should be followed and regular security audit should be performed to ensure appropriate patch level is maintained. Basic security training for Windows and Apache administrators would also help.

4.2.2. Apache server is running under privileged user account

Reference: Checklist 8

Apache was running as a service on CUS web server using local system account (page 47). Local system account is a privileged account with full access to any system resources locally. Therefore Apache service account has full access to all local drives, including Windows and Apache system directory and Apache log directory.

Background/Risks

Potential attackers may use buffer overflow or other techniques to crash Apache server and obtain user rights as privileged local system account, and have full access to web server machine. This would give malicious users full access to sensitive and confidential data stored on the machine. They may change, delete or add information into survey database to compromise the integrity of information stored on the box. This would make the survey information totally useless.

Recommendation

A separate user account should be created for Apache server. This user account is a normal user account and a member of local Users group. This account also needs to have "Log on as a service" user right.

Control mechanism should be put in place to make sure Apache is running under normal user account. For example, a process can be established to have security team audit and approve every public web server installation and configuration before they go into production environment.

4.2.3. Network setting are not appropriate to prevent attacks

Reference: Checklist 20, Checklist 21, Checklist 22

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TCP/IP filtering is not enabled to allow connection attempts only to legitimate ports the web server is listening on (page 49). Apache server comes with some settings to give administrators greater controls over client request time out, maximum number of remote clients, and abnormal client request behavior, etc. This provides another layer of protection against denial of service attacks and buffer overflow attacks. However, these settings are absent or not properly set on CUS web server (page 49-50).

Background/Risks

Without TCP/IP filtering, a server may accept any connection attempts to any ports which are listening. This may not be an issue for external connection requests as Internet firewall should block illegal connections, it does provide an additional level of security. For internal requests, however, this is a potential risk. One scenario could be an internal user attacks vulnerable ports which are listening on the machine, or a malicious user connects to a Trojan or backdoor placed on the server via a special port. By doing so, this user may take control of the web server and use it for other malicious purposes.

Using malformed HTTP packets, a potential attacker could bring down CUS web server and prevent other legitimate users from accessing customer survey web site. Even worse, as the Apache service on CUS web server is running under privileged local system account, a successful buffer overflow attack could give potential attacker full access to CUS web server, which leads to the loss of data confidentiality and integrity. Either way, DoS attack or full access to the web server will have a major business impact and EMCA company reputation would be damaged.

Recommendation

Immediate resolution is to implement TCP/IP filtering and configure those Apache network settings to reduce the possibility of any potential network attacks. In addition, a host based intrusion detection product may be deployed on this server to provide early detection of any network attacks.

Periodic security audit process should be established to ensure web server's security is maintained. Besides, as suggested in 4.2.2, a process should be in place to allow security team to audit web server security before it goes into production.

4.2.4. Indexing is enabled and directory content is exposed

Reference: Checklist 26

Apache configuration file httpd.conf and Tomcat configuration file tomcat.conf were reviewed. It's found that indexing was enabled for several directories containing sample files, scripts and admin tools (page 59-62).

Background/Risks

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

If a URL points to a directory on web server, the defined index file (index.html, for example) for that directory will be displayed. If, however, the index file does not exist, the content of the directory is displayed in the browser instead. Indexing may be useful and required if the web server is used for file sharing, such as Intranet server. However, in case of public web server, if directory index file is deleted by mistake, then the files and subdirectories in that particular directory will be exposed.

The directories exposed on CUS web server contain sample files and scripts. Many sample files and scripts have known security holes and contain software package information. Remote malicious users may exploit these security holes or derive attack target profile based on the software information.

Recommendation

Because CUS is a public web server, Indexing should be disabled on this web site.

A process should be in place to audit web server security before it goes into production.

4.2.5. Unnecessary services and modules are running

Reference: Checklist 23, Checklist 24, Checklist 32, Checklist 34

NMAP and FPORT tools were used to check listening ports on CUS web server (page 51-52). It turned out that some unnecessary ports were listening on the server such as port 8080 for Tomcat and port 21 for FTP (page 53-58 and 64).

NMAP scanning from internal network did not find any listening ports on CUS web server although this box is internally accessible via pcAnywhere. This is because internal connection to CUS web server has to go through Intranet firewall which requires user authentication. In case of NMAP scanning, user authentication was not performed so connection to CUS web server was dropped and NMAP could not find any ports listening. When NESSUS was used to scan network vulnerabilities, the actual NESSUS server sit in the same public DMZ as CUS web server, therefore the ports listening on the CUS box could be detected.

Apache for Windows distribution has many modules compiled in (page 65). Apache on CUS web server was installed to its default configuration. Therefore there are many modules active on the server.

Background/Risks

More services and modules mean more potential vulnerabilities. Apache.org just released Apache 2.0.46 to address some critical security vulnerabilities. One of them is a server crash (that is, denial of service) can be triggered

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

remotely through module mod_dav and possible other mechanisms[8]. Minimizing the number of active modules and services also reduces the possibilities of potential future exploits. For example, the server will still be protected if vulnerable service is not running or vulnerable module is not active on the server.

Recommendation

IIS service was installed to provide FTP functionality. FTP service is not really required on CUS web server because the server provides customer survey functionality, not file transfer. IIS service should be removed. This will also close those listening ports used by IIS service (inetinfo.exe).

Tomcat default web server on port 8080 should be disabled because it is not used.

When Apache for Windows was compiled, many modules were included. If any of these modules are not needed, they can be removed with ClearModuleList directive in httpd.conf file. However, Apache does not provide a way to remove those compiled in modules individually; you have to remove them all and then add back those required modules individually with AddModule directive.

Alternatively, these modules can be left running on the web server, but relevant directives or functions should be disabled. For example, mod_autoindex module is bound into Apache for Windows distribution, but Indexes can be disabled on web server. In this case, keeping patches up to date is very important as these modules may have flaws and vulnerabilities. A patch management process and security audit process should be followed.

4.2.6. Server information is disclosed

Reference: Checklist 35, Checklist 37

NETCAT tool was used to check any header information sent back to client. It's found that web server OS, version information, Tomcat information, base OS information, etc, was disclosed (Page 66). Internet Explorer was used to check the footer message and it's found web server software information was disclosed as well (page 67).

Background/Risks

One of the important steps involved in network attack is information gathering. Attackers need to find out what software is running on the target machine and its version information, what services are running, etc. HTTP header is a great place to find out this information. With this information, attackers can build target profile and research for the vulnerabilities of the software and services running on target machine, and then attack.

[8] http://www.apache.org/dist/httpd/Announcement2.html

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

This information gathering task can be fully automated, and there are scripts freely available on Internet which can do the job. For example, some worms can trigger the attack automatically based on the HTTP response header information[9].

Recommendation

The immediate solution is to configure Apache to hide web server OS information in header and footer, or completely remove server header from HTTP response header.

A long term solution would be a process in place to have security team audit all public web servers before they go into production. Alternatively, a secure web server build document can be maintained by security team on how to build an Apache server in a secure manner.

4.3. Costs

Most of the remedy works are related to manpower and time required to modify Apache server configuration, apply security patches and maintain web server security. Estimated cost is listed in following tables.

Table 2 Cost for one-off activities

One-Off Activity	Cost
Apply missing base OS security patches	1 hour
Upgrade Apache and Tomcat to the latest version	4 hours
Security essentials training	US$3000
Apache configuration change, such as creating separate Apache service account, TCP/IP filtering, httpd.conf file modification, etc.	1 hour
Host based IDS software (ISS Server Sensor)	US$600
Host based IDS deployment and configuration	4 hours
IDS product training	US$3000

Table 3 Cost for ongoing activities

Ongoing Activity	Cost

[9] http://www.securityfocus.com/bid/5363/discussion/

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Ongoing Activity	Cost
Maintain web server patch level	4 hours / month
Quarterly security audit	2 days
Host based IDS management	30 minutes / day

4.4. Compensating Controls

Except the security training and host based IDS implementation and training, other costs are normal operation costs.

Management may consider online training as a cost-effective alternative to live training. Not only is the course fee cheaper, but also the cost for accommodation and travel is eliminated.

Free IDS product such as SNORT can be used to reduce the cost for software purchase and maintenance. However, this requires the administrator to have a deeper networking knowledge.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

1. McClure Stuart, Shah Saumil, Shah Shreeraj. Web Hacking, Attacks and Defense. Boston: Addison-Wesley, July 2002

2. "Microsoft Solution for Securing Windows 2000 Server ". Microsoft. 5 February 2003. URL: http://www.microsoft.com/technet/security/prodtech/windows/secwin2k/default.asp (13 June 2003)

3. "Microsoft Windows 2000 Security Hardening Guide ". Microsoft. 11 April 2003. URL: http://www.microsoft.com/technet/security/prodtech/windows/win2khg/default.asp (13 June 2003)

4. "Security Operations Guide for Windows 2000 Server". Microsoft. March 2002. URL: http://www.microsoft.com/brasil/security/content/resources/resources/SOG_download.pdf (13 June 2003)

5. "Security Recommendation Guides". National Security Agency. 5 March 2003. URL: http://www.nsa.gov/snac/win2k/download.htm (13 June 2003)

6. "Firewall & Perimeter Protection". SANS InfoSec Reading Room. URL: http://www.sans.org/rr/catindex.php?cat_id=21 (13 June 2003)

7. "Symantec Internet Security Threat Report Volume III". Symantec. February 2003. URL: http://enterprisesecurity.symantec.com/Content.cfm?articleID=1964&EID=0 (13 June 2003)

8. "Internet Risk Summary for September 28 th through December ". Internet Security Systems. URL: https://gtoc.iss.net/documents/summaryreport.pdf (13 June 2003)

9. "Market Share for Top Servers Across All Domains August 1995 – April 2003". Netcraft. 13 April 2003. URL: http://news.netcraft.com/archives/2003/04/13/april_2003_web_server_survey.html (13 June 2003)

10. "Apache.org compromise report". Apache. 22 September 2001. URL: http://www.apache.org/info/20010519-hack.html (13 June 2003)

11. "Apache on Windows struggling?". Netcraft. 25 February 2003. URL: http://news.netcraft.com/archives/2003/02/25/apache_on_windows_struggling.html (13 June 2003)

12. "The Twenty Most Critical Internet Security Vulnerabilities". SANS. 29 May 2003. URL: http://www.sans.org/top20/ (16 June 2003)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

13. "Security Tips for Server Configuration". Apache. URL: http://httpd.apache.org/docs/misc/security_tips.html (16 June 2003)

14. Thai Computer Emergency Response Team. "Apache HTTP Server Project". NECTEC. September 2002. URL: http://thaicert.nectec.or.th/event/itsec2002_-material/Apache.pdf (16 June 2003)

15. Novotny, Jason. Perry, Marcia. "Building a Secure Web Server". 4 June 2001. URL: http://doesciencegrid.org/Grid/public/events/GPDW/slides/webserver.pdf (17 June 2003)

16. Cox, J. Mark. "Apache Security Secrets: Revealed". ApacheCon 2002. October 2002. URL: http://www.awe.com/mark/apcon2002/tu04_-handout.pdf (16 June 2003)

17. "Using Apache with Microsoft Windo ws". Apache. URL: http://httpd.apache.org/docs/windows.html (16 June 2003)

18. Lachniet, Mark. "Windows NT / 2000 Server Hardening Checklist". 20 May 2002. URL: http://www.mtip.net/aware/MarkLachnietChecklist.pdf (16 June 2003)

19. "Apache Security Configuration Document". Intersect Alliance. URL: http://www.intersec talliance.com/projects/ApacheConfig/ (16 June 2003)

20. Rowe Jr., A. William. "Apache/WinNT Security". ApacheCon/Europe 2000 track W08. 25 October 2000. URL: http://www.linuxroot.org/apachecon/W07.pd f (16 June 2003)

21. "Securing Apache". Allaire Corporation. 08 January 2001. URL: http://www.macromedia.com/v1/DocumentCenter/Partners/ASZ_ASWPS_Securing_Apache.pdf (16 June 2003)

22. Pomeranz, Hal. "WU-FTPD and Apache Security Basics". Deer Run Association. October 2002. URL: http://www.baylisa.org/library/slides/2002/10/BayLISA_ApacheWUFTP.pdf (16 June 2003)

23. "Running Apache for Windows as a Service". Apache. URL: http://httpd.apache.org/docs/win_service.html (15 June 2003)

24. "Apache HTTP Server Log Files". Apache. URL : http://httpd.apache.org/docs/logs.html (16 June 2003)

25. Mourani, Gerhard. Henry, Colin. " How to Build, Install, Secure & Optimize Apache 2.x". Open Network Architecture Inc. 04 December 2002. URL: http://www.openna.com/documentations/articles/apache/index.php (17 June 2003)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

26. "Apache Core Features". Apache. URL: http://httpd.apache.org/docs/mod/core.html (16 June 2003)

27. "Overview of security vulnerabilities in Apache httpd 2.0". Apacheweek. 29 May 2003. URL: http://www.apacheweek.com/features/security -20 (16 June 2003)

28. "Apache 2.0.46 Released". Apache. 28 May 2003. URL: http://www.apache.org/dist/httpd/Announcement2.html (16 June 2003)

29. "OpenSSL SSLv2 Malformed Client Key Remote Buff er Overflow Vulnerability". SecurityFocus. URL: http://www.securityfocus.com/bid/5363/discussion/ (17 June 2003)

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.