GIAC
CERTIFICATIONS

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.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing & Monitoring Networks, Perimeters & Systems (Audit 507)"
at http://www.giac.org/registration/gsna

An Administrator's Report on Auditing a Web Application Server with Retina Network Security Scanner

GSNA Practical Version 2.1 (amended July 5, 2002)

Author: Sean Mitchell
Date: August 25, 2003

© SANS Institute 2003, Author retains full rights.

Abstract

This practical will summarize the audit of the web application component of a medical records system of a healthcare organization. The majority of the audit was conducted using the Retina Network Security Scanner tool by eEye Digital Security.

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

Table of Contents

An Administrator's Report on Auditing a Web Application Server with Retina Network Security Scanner 1
Abstract 1
Table of Contents 2
Assignment 1 — Research in Audit, Measurement, Practice and Control 4
- Identify the System to be Audited 4
- Evaluate the Risk to the System 6
- Current State of Practice 8
- Improvement of Current Methods and Techniques 10

Assignment 2: Create an Audit Checklist 10
- Introduction 10
- Conventions 11
- Objectives 11
- Scope 12
- Audit Checklist 13

Assignment 3: Audit Evidence 22
- Conduct the Audit 22
  - Item 5 – Identify Open Ports Results: PASS 22
  - Item 9 – SNMP Result: FAIL 24
  - Item 13 – Sendmail Result: FAIL 24
  - Item 16 – Remote Access – Telnet Result: FAIL 25
  - Item 6 – RPC Services Result: FAIL 26
  - Item 7 – Apache Web Server Result: FAIL 27
  - Item 15 – Accounts with no passwords Result: PASS 30
  - Item 18 – Determine OS Patch Status Result: PASS 30
  - Item 19 – Determine Security Patch Status Result: PASS 30
  - Item 20 – UID 0 Accounts Results: FAIL 31
  - Item 21 – Web Application Logon Results: FAIL 31
- Measure Residual Risk 31
- Evaluate the Audit 32

Assignment 4: Risk Assessment 33
- Summary 33
- Background/Risk and Remediation 33
  - Finding Item 9 – SNMP 33
  - Finding Item 13 – Sendmail 34
  - Finding Item 16 – Remote Access – Telnet 34
  - Finding Item 6 – RPC Services 35
  - Finding Item 7 – Apache Web Server 35
  - Finding Item 19 – Determine Security Patch Status 36
  - Finding Item 20 – UID 0 Accounts 36
  - Finding Item 21 – Web Application Logon 37
- System Changes and Further Testing 37
  - System Changes 37
  - Remediation Item 9 – SNMP 37

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

Remediation Item 13 – Sendmail 38
Remediation Item 16 – Remote Access – Telnet 38
Remediation Item 6 – RPC Services 38
Remediation Item 7 – Apache Web Server 38
Remediation Item 19 – Determine Security Patch Status 39
Corrective Action 39
Remediation Item 20 –UID 0 Accounts 39
Remediation Item 21 – Web Logon 39
Re-testing Results 39
Re-testing Item 5 – Identify Open Ports Results: PASS 39
Re-testing Item 9 – SNMP Result: PASS 40
Re-testing Item 7 – Sendmail Result: PASS 40
Re-testing Item 16 – Remote Access – Telnet Result: PASS 40
Re-testing Item 6 – RPC Services Result: FAIL 41
Re-testing Item 7 – Apache Web Server Result: FAIL 41
Re-testing Item 19 –Security Patch Status Result: Not Tested 42
Re-testing Item 20 – UID 0 Accounts Result: FAIL 42
Re-testing Item 21 – Web Application Logon Result: FAIL 42
Re-testing Item 8 – SSH Result: PASS 43
System Justification 45
Item 20 – UID 0 Accounts 45
Mitigating controls 45
Conclusion - Practical 45
Conclusion – Real-World Audit 46
References 47

© SANS Institute 2003, Author retains full rights.

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

Assignment 1 — Research in Audit, Measurement, Practice and Control

Identify the System to be Audited

Overview

I am auditing a web server that is hosting the ChartMaxx Web application for a healthcare organization. The ChartMaxx Web application is a front-end application that provides a web interface to the back-end ChartMaxx Electronic Patient Record system. The ChartMaxx system is used as an Electronic Medical Record and the ChartMaxx Web server is to be used by physicians for offsite chart completion via the Internet. The system is currently residing on the internal network pending audit completion and remediation when it will be moved to the organization's DMZ network. The system was installed and configured by the vendor with little involvement by the organization's IT staff.

System Components

The ChartMaxx Web application consists of the following hardware and software components.

Web Application Server

1. Hewlett-Packard 9000 A500 Enterprise Server hardware
2. Hewlett-Packard HP-UX 11.xx operating system
3. Apache 1.3.x web server
4. MedPlus ChartMaxx Web application version 3.3

The back-end ChartMaxx system consists of (2) HP 9000 rp2400 series servers running HP-UX 11.xx configured in a High-Availability cluster hosting the main ChartMaxx application version 3.3 and an Oracle database. This system is not subject to this audit.

System Requirements

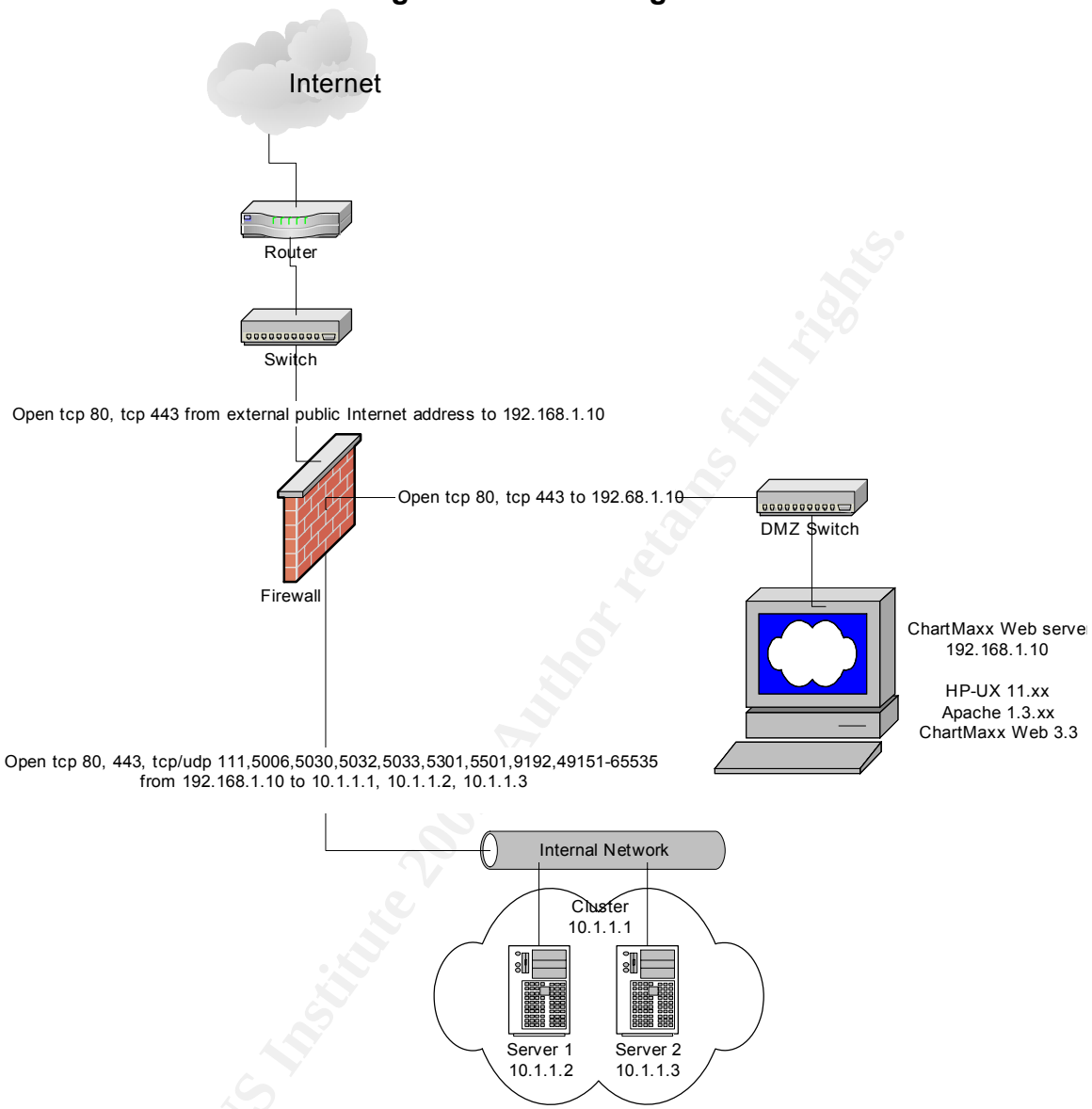
The ChartMaxx Web application has the following requirements.

1. External users will need to access the Web Application server from the Internet via http and https (TCP port 80 and 443).
2. Internal users will need to access the Web Application server from the internal network via http and https (TCP port 80 and 443).
3. The ChartMaxx Web application will need to access the ChartMaxx system on the internal network from the DMZ via RPC (TCP port 111) and the following additional TCP/UDP ports (5006, 5030, 5032, 5033, 5301, 5501, 9192, 49151 – 65535).

The following diagram shows the ChartMaxx Web application server's placement in the DMZ.

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

Figure 1 — DMZ Diagram



Audit Goal

It is the goal of this audit to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA), specifically section 164.306 (a)(1), which states that covered entities must "ensure the confidentiality, integrity, and availability of all protected health information the covered entity creates, receives, maintains, and transmits."[1]

To meet this objective, the following system components of the ChartMaxx Web application server will be the subject of my audit:

[1]Final HIPAA Security Rule http://www.hipaadvisory.com/regs/finalsecurity/finalsecurity.txt sec 164.306(a)(1)

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

1. HP-UX 11.xx operating system software
    a. Only necessary services for the proper functioning of the application should be running.
        i. Web Services on port 80 and 443
        ii. RPC Services
    b. All required operating system patches should be applied unless they adversely affect the proper functioning of the application.
    c. Document accounts with administrator rights.
2. Apache 1.3.x web server software
    a. All known web server software vulnerabilities should be addressed via configuration changes or software patches.
3. ChartMaxx Web application
    a. Verify that the application logon is enabled using https (TCP port 443) and not http (TCP port 80).

The audit will not cover the DMZ network components such as the firewall and its configuration. For the purposes of this audit, it is assumed that the firewall is properly configured and patched to support the ChartMaxx Web application server in a secure manner.

Evaluate the Risk to the System

Overview

The ChartMaxx Web application server is a front-end web interface for the ChartMaxx Electronic Patient Record system that resides on the internal network. The purpose of the application is to allow healthcare providers to access patient medical records in order to review and complete the patient medical charts via the Internet.

The risks to this system consist of misconfiguration of system components , unnecessary services that are running, and unpatched software that would introduce security holes that could be exploited to gain unauthorized access to patient information. These risks will be discussed by system component.

HP-UX Operating System

The operating system on this server was pre-installed from the hardware vendor with little modification by the ChartMaxx Web application vendor. The risk is that unnecessary default operating system services and configurations are implemented and pose a security risk. For example, the R-services are implemented by default and must be turned off. Also, telnet is used to manage the server and should be replaced with SSH since the server will reside in the DMZ. Since the IT department had little involvement in the installation and configuration of this server, it is important that an audit of the OS be performed to determine system configuration and determine if there are any outstanding security holes that need to be patched. Failure to do so could lead to system

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

compromise and disclosure of protected health information, violation of HIPAA, and damage to the organization's public image.

Apache 1.3.x Web Server Software
The Apache Web Server software is integral to the ChartMaxx Web application. The Apache software was installed and configured by the ChartMaxx Web application vendor. Again, since there was little IT department involvement, the Apache software needs to be audited for any configuration security risks and any outstanding security holes that need to be patched.

ChartMaxx Web Application version 3.3
The end-user has to logon to the application via web browser and there is a risk that the user can logon via http instead of https. The risk of logon via http is that the username and password would transmit unencrypted. The ChartMaxx Web application will need to be audited to ensure that logons can only occur using https.

Risk Summary
The greatest risk to the system and its data will be due to any unnecessary services or misconfigured services running, and any unpatched software. Assuming all unnecessary services are terminated and all patches have been applied, the risk to the system will be low and limited by access controls implemented at the firewall. External access to the system will be limited to TCP port 80 and TCP port 443, restricted by the firewall. Access from the DMZ to the internal network will be limited by only allowing the ChartMaxx Web application server to access certain internal network servers on specific TCP/UDP ports. Internal network access to the ChartMaxx Web application server will not be restricted in any way. The result of these access configurations is that the server has higher risk of compromise from internal threats than external threats. Thus, it is important to reduce the number of running services on the server to the minimum necessary to perform its function.

Below is a table that summarizes the risks to this system.

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

Table 1 – Risk Summary			
Risk	Vulnerability	Exposure	Impact
Unneeded services running	Additional services provide opportunities of exploitation due to misconfiguration or unpatched software.	Low – access from Internet due to port blocking High – access from internal network due to unrestricted access.	System compromise could lead to disclosure of patient information, denial of service, or use of system for unintended purposes.
Misconfigured services	Misconfiguration of services could leave security holes that could be exploited despite other mitigating controls such as software patching.	High – access from Internet via port 80 and 443 High - access from internal network due to unrestricted access	System compromise could lead to disclosure of patient information, denial of service, or use of system for unintended purposes.
Unpatched software	Unpatched software could leave security holes that could be exploited despite other mitigating controls such as correct configuration of services.	High – access from Internet via port 80 and 443 High - access from internal network due to unrestricted access	System compromise could lead to disclosure of patient information, denial of service, or use of system for unintended purposes.

Current State of Practice

Research Methodology

Research for checklists was conducted by running a search on Google. The search parameters were "UNIX security checklists". This returned 11,900 references. I was able to find references to my security information sources of choice: SANS, NIST, CERT, and CIS. It is from these sources that I obtained UNIX checklists. I also found a book which provided a comprehensive UNIX audit checklist.

For Apache checklists, I used "Apache security checklists" on Google and got 3,200 references. I was not able to find any checklists that I thought were of the same quality as my UNIX sources, but I did find 3 that I thought were okay.

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

UNIX
I was able to find a number of audit checklists for UNIX systems. The following references provided UNIX checklists:

- SANS / FBI Top 20 List – http://www.sans.org/top20/
- Center for Internet Security HP-UX Level 1 Benchmark – http://www.cisecurity.com/bench_HPUX.html
- CERT UNIX Security Checklist v.2.0 – http://www.cert.org/tech_tips/unix_security_checklist2.0.html
- NIST CSRC Unix Security Checklist – http://csrc.nist.gov/pcig/cig.html
- Yusufali F. Musaji, Auditing and Security (New York: John Wiley & Sons, 2001) p. 421-447

The majority of the checklists deal with hardening a system at the time of installation before any third-party application is installed. The vendor was not able to provide me a list of which services were required and which services were not required for their application. This presented an obstacle to using completely any of the checklists from beginning to end for fear of breaking the application. As a result, I created a checklist by using the results from running the Retina Network Security Scanner by eEye Digital Security to check for open ports, running services, and unpatched security holes. I used parts of the SANS / FBI Top 20 List and the CIS HP-UX Level 1 Benchmark to cover areas that the Retina scanner cannot detect, namely account permissions. If I were installing an HP-UX server from scratch, I would use the CIS HP-UX Level 1 Benchmark document due to it being a consensus document drawn from many sources.

Apache
I was able find some audit checklists for Apache. The following references provided Apache checklists:

- InterSect Alliance – Apache Security Configuration Document – http://www.intersectalliance.com/projects/ApacheConfig/index.html
- Apache Software Foundation – Security Tips for Server Configuration – http://httpd.apache.org/docs/misc/security_tips.html
- Open Source Conference 3 – Apache Security from A-Z – http://modperl.com:9000/perl_conference/apache_security/

I did not use any of these checklists in auditing the Apache server software. The Apache software was installed by the vendor and is vendor supported. No information was provided by the vendor regarding configuration of Apache. My audit checklist for Apache is limited to identification of any patches needed by the Retina scanner. The Center for Internet Security is currently developing a Level-2 Benchmark for Apache, which I look forward to reviewing and using once it is completed.

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

ChartMaxx Web Application
There are no audit checklists available for this application. Basically, my audit checklist consists of making sure that the logon screen for the application is displayed only with a secure https connection.

Improvement of Current Methods and Techniques

Most of the checklists that I discovered deal with securing a system during the time of install. The checklists assume that a systems administrator will have the expertise to install the operating system in accordance with the checklist. In the case of the ChartMaxx Web application server, the organization had no in-house staff with the expertise to install and configure the HP-UX operating system and had to rely on the application vendor. During the installation, the organization had no defined certification and accreditation process to insure that the operating system and applications were installed to a defined security standard. Without any defined standard, the vendor installed the system using a default installation of the server operating system. They then installed the Apache web server software as part of their application installation.

Since there was little IT department involvement regarding the installation and configuration of this server, it was determined that the audit checklist would be created from the results of the Retina security scan and augmented by selected items from the SANS/FBI Top 20 List and the CIS HP-UX Level-1 Benchmark checklists. The Retina security scan would help determine the need for security patches and identify running services and open ports while the two checklists would provide the audit items that the Retina security scanner would miss.

Assignment 2: Create an Audit Checklist

Introduction

The project manager for implementation of the ChartMaxx Web application system has requested that an audit be performed to certify that the server is secure enough for deployment in the organization's DMZ for access from the Internet. Since the system will be used to access patient health information, the system needs to be as secure as possible to protect patient data and the organization from negative publicity and fines that would occur if there were unauthorized disclosure of information.

The system currently resides on the organization's internal network. Although the server will be deployed in the DMZ, auditing and securing this server on the internal network will not have any significant impact on the outcome of this audit. Indeed, it is preferable to secure the system before it is placed in its production environment in the DMZ.

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

The audit will be conducted by the Security Administrator. Since he does not have any extensive Unix expertise, he will be assisted by the UNIX Systems Administrator. The Security Administrator will conduct the audit by running the Retina scanner against the server. He will then analyze the results and create a remediation checklist for the Unix Systems Administrator to implement using the results of the Retina scanner and other security checklists. The Systems Administrator will address each item on the remediation checklist. Addressing each item means executing the recommended remediation suggested by the Security Administrator, suggesting an alternative method of remediation, or documenting why the item cannot be remediated. After the Systems Administrator has addressed the remediation checklist, the Security Administrator will validate the remediation by re-running the Retina scanner and manually checking the system for items that the scanner cannot detect. This will be an iterative process that will be repeated as often as necessary to produce a secure system.

The Retina scanner will be used extensively in this audit as both a verification tool as well as a remediation checklist generator. The reports from the scanner identify the vulnerability as well as provide information on how to remediate the vulnerability. The Retina scanner will produce false positives and each of the vulnerabilities discovered needs to be investigated to determine the scanners accuracy. Thus, it is important to have manual checklists to verify the scanner results and to cover any vulnerability that the scanner cannot detect. The Retina scanner will also test for the SANS Top 20 vulnerabilities as part of a complete scan. The following checklist assumes that the Retina scanner will be used to complete checklist items.

Conventions

- Commands to be executed will be listed in **bold**.
- Commands will be executed in the order listed.
- Subjective tests will be indicated by S.
- Objective tests will be indicated by O.

Objectives

The purpose of this audit is to certify that the system secure enough for deployment into the organization's DMZ for access from the Internet. The system will be deemed secure for deployment when:

1. All known security vulnerabilities that can be patched have been patched.
2. All services not necessary for the functioning of the ChartMaxx Web application are disabled.
3. All services that are necessary are configured in a manner to promote the security of the system.

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

The system exists to provide health care providers access to patient medical record information in a secure manner via the Internet. The system provides access to these information assets as well as protects them from unauthorized use. This is accomplished by using a challenge/response mechanism (username and password) to provide access. This mechanism is conducted via an encrypted SSL connection to prevent disclosure of the username and password

Scope

This audit will focus on the server hosting the ChartMaxx Web application. Specifically, the audit will be confined to the following system components:

1. HP-UX 11.xx operating system software
    a. Only necessary services for the proper functioning of the application should be running.
        i. Web Services on port 80 and 443
        ii. RPC Services
    b. All required operating system patches should be applied unless they adversely affect the proper functioning of the application.
    c. Document accounts with administrator rights.
2. Apache 1.3.x web server software
    a. All known web server software vulnerabilities should be addressed via configuration changes or software patches.
3. ChartMaxx Web application
    a. Verify that the application logon is enabled using https (TCP port 443) and not http (TCP port 80).

© SANS Institute 2003, Author retains full rights.

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

Audit Checklist

Item	Audit Test & Reference	Control Objective	Risk	Compliance / Expected Results	Testing	Type
			Administrative Section			
1	Obtain written permission to perform the audit that states system to be tested and times and dates that testing can be performed. *Source:* Personal Experience	To prove that the audit testing is indeed sanctioned and not mistaken for a hacking attempt. Define acceptable times to perform audit.	If written permission is not obtained, there is no proof of permission and there is no accountability for actions.	Written permission filed with the audit working papers.	N/A	S
2	Obtain system information including system name, ip address, hardware information, software information including operating system and applications, system purpose. *Source:* Personal Experience	Information is needed to perform the audit and research items for audit checklist.	Without accurate information, audit will not be successful in identify and managing risk of system.	Documents that list appropriate system information filed with audit working papers.	N/A	S
			Retina Scanner Section			
3	From scanner workstation, ping target system by name. *Source:* Personal Experience	To determine if system name is defined in network DNS and if the system is on the network.	If system name is not defined in network DNS, scanner will have to target the system by ip address.	Positive ping response that shows name to IP address resolution.	**Ping <*system name*>**	O
4	Run Retina scanner against target system using system name or ip address with the following Policy options: • Enable connect mode scan. • Perform Full Port Scan. • Enable all audits. *Source:* Personal Experience	To provide an overview of system security status to form the basis of preliminary audit report and remediation checklist.	The Retina scanner will miss items that it is not designed to detect. The full port scan will take time to perform since it is scanning all 65535 ports.	Successful scan will generate a report that can be reviewed online or printed.	Launch the Retina Scanner. On the Menu bar, click on **Tools**, **Policies**. Ensure that **Complete Scan** is showing from drop list. Click on **Ports**. Check On **Perform Full Port Scan**. Click on **Audits**. Check On all Audits listed starting with	O

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

					Accounts and ending with **Wireless**. Click OK. In **Address:** field of the main screen, enter the system name or ip address and press Enter to start scan.	
5	Identify any open ports. *Source*: Personal Experience	To determine which ports are open.	Ports that are open are indications of running services that may be unnecessary and could pose a security risk.	If open ports are detected, they will usually indicate a running service.	Reference results of item 4 to determine what open ports are running.	O
The following section details one of the Audit checklists within Retina that is executed when a Complete Scan is done. The text of the checklist is from SANS, but I will be relying on the Retina scanner to perform the audit tests. Some of these items have manual commands that can be used to validate the Retina scan. The specific Retina audit tests are listed below each checklist item as a bullet. Detailed information for these Retina audit tests can be found at the URL listed.						
SANS Top 20 – UNIX Vulnerabilities Audit						
6	SANS Top 20 U1 – Remote Procedure Calls (RPC) *Source:* SANS http://www.sans.org/top20/ • RPC cachefsd service • RPC mountd service • RPC rexd non root command execute • RPC rpc.cmsd service • RPC rpc.nisd service • RPC rpc.statd service • RPC rpc.yppasswdd service • RPC rpc.ypupdated service • RPC rwalid service • RPC sadmind overflow • RPC tooltalk services *Details:* eEye Digital Security http://www.eeye.com/html/Products/Retina/RTHs/Rpc_Services/	To determine if RPC services are running on the system.	There is a history of security vulnerabilities related to RPC services. These vulnerabilities can be exploited resulting in system compromise with administrative privileges. The compromised system could then be used to attack other systems.	If RPC services are running, determine need for RPC services for this system. If needed, secure by installing latest version from vendor and/or installing any patches for service. If not needed, disable services. This service should be running because the application is dependent on this service. The service should be the latest version, correctly configured, and have any vulnerabilities patched.	Reference results of scan from Item 4 to determine if RPC services are running. You can manually check by running: **rpcinfo -p** for a list of services that are running. *Source:* Yusufali F. Musaji, Auditing and Security (New York: John Wiley & Sons, 2001) p. 444 Item 58	O
7	SANS Top 20 U2 – Apache Web Server	To determine if Apache Web Server	Apache may have security	Web server should be	Reference results of	O

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

	Source: SANS http://www.sans.org/top20/ • Apache chunking integer overflow vulnerability • Apache mod_ssl session caching buffer overflow • Apache Tomcat servlet cross-site scripting vulnerability • CGI - ash Interpreter • CGI - bash Interpreter • CGI - ksh Interpreter • CGI - Perl Interpreter • CGI - rksh Interpreter • CGI - sh Interpreter • CGI - tcsh Interpreter • CGI - zcsh Interpreter • OpenSSL ASCII Integer Representation Vulnerability • OpenSSL ASN.1 Parsing Error Denial Of Service Vulnerability • OpenSSL CBC encryption timing attack vulnerability • OpenSSL Kerberos Enabled SSLv3 Key Exchange Vulnerability • OpenSSL PRNG weakness • OpenSSL SSLv2 Malformed Client Key Remote Buffer Overflow *Details:* eEye Digital Security http://www.eeye.com/html/Products/Retina/RTHs/Web_Servers/	is running on system and if any patches need to be applied.	vulnerabilities that need to be patched and services that are misconfigured.	running on TCP port 80 and/or TCP port 443. Determine if web services needed. If so, apply any security patches. If not needed, disable services. This service should be running because the application is dependent on this service. The service should be the latest version available, correctly configured, and have any vulnerabilities patched.	scan from Item 4 to determine if Apache is running on TCP port 80 and/or TCP port 443 and to determine if there are any security patches that need to be applied.	
8	SANS Top 20 U3 – Secure Shell (SSH) *Source:* SANS http://www.sans.org/top20/ • OpenSSH 3.0 channel code buffer overflow vulnerability • OpenSSH 3.3 PAMAuth Integer Overflow • OpenSSH 3.3 Remote Challenge Integer Overflow	To determine if SSH is running on the server and if any patches need to be applied.	SSH may have security vulnerabilities that need to be patched. These vulnerabilities could be exploited and result in system compromise.	If SSH is running, it will show up running on TCP port 22. Determine if SSH is needed. If so, apply any security patches. If not needed, disable service. This service should not be running since there is no explicit application need for it.	Reference results of scan from Item 4 to determine if SSH is running on TCP port 22. You can manually check by running: **ssh –V** and checking to see if the version is	O

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

	• OpenSSH Client Unauthorized Remote Forwarding Vulnerability • OpenSSH UseLogin Environment Variable Passing Vulnerability • OpenSSH UseLogin Vulnerability • OpenSSH UseLogin Vulnerability • SSH 1.2.27 Kerberos Ticket Cache Exposure Vulnerability • SSH 1.5 PKCS #1 Version 1.5 Session Key Retrieval Vulnerability • SSH Communications Security Short Password Login Vulnerability • SSH CRC-32 Compensation Attack Detector Vulnerability • SSH scp file overwrite vulnerability • SSH Secure-RPC Weak Encrypted Authentication Vulnerability • SSH1 SSH Daemon Logging Failure Vulnerability *Details:* eEye Digital Security http://www.eeye.com/html/Products/Retina/RTHs/SSH_Servers/				vulnerable. You can also check by using a terminal emulator program and connecting via port 22.	
9	SANS Top 20 U4 – Simple Network Management Protocol (SNMP) *Source:* SANS http://www.sans.org/top20/ • An SNMP community name is guessable • Default public SNMP community string • HP SNMPv1 Request/Trap vulnerabilities • SNMP default community name *Details:* eEye Digital Security http://www.eeye.com/html/Products/Retina/RTHs/SNMP_Servers/	To determine if SNMP is running on the server and if any configuration induced security vulnerabilities exist and if any patches need to be applied.	SNMP has both configuration and technical security vulnerabilities. Configuration vulnerabilities include blank, public, or weak passwords and community strings.	If SNMP is running, it will show up running on TCP port 161 and/or TCP 162. It will also be running as snmp in the process list. This service should not be running since the organization does not have any SNMP management software deployed.	Reference results from Item 4 to determine if SNMP is running on TCP port 161 and/or TCP port 162. You can manually check by running: **ps –e | grep 'snmp'**	O
10	SANS Top 20 U5 – File Transfer Protocol (FTP) *Source:* SANS	To determine if FTP is running on the server and if any patches need to be applied.	FTP transmission is inherently insecure. FTP services have been shown to have security vulnerabilities.	If FTP is running, it will show up on TCP port 21. This service should not be	Reference results from Item 4 to determine if FTP is running on TCP port 21.	O

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

	http://www.sans.org/top20/ • Anonymous FTP • Anonymous Write *Details:* eEye Digital Security http://www.eeye.com/html/Products/Retina/RTHs/FTP_Servers/			running because there is no explicit application need for this service.		
11	SANS Top 20 U6 – R-Services – Trust Relationships *Source:* SANS http://www.sans.org/top20/ • rexec service • rlogin service • rsh service *Details:* eEye Digital Security http://www.eeye.com/html/Products/Retina/RTHs/IP_Services/	To determine if the R-Services are running on the server.	The R-services are inherently insecure due to lack of encryption and weak host authentication. One server with incorrectly configured R-services can compromise all other servers that trust it.	If R-Services are running, it will show up on TCP ports 512, 513, and 514 for rexec, rlogin, and rsh. These services should not be running because there is no explicit application need for these services.	Reference results from Item 4 to determine if the R-services are running.	O
12	SANS Top 20 U7 – Line Printer Daemon (LPD) *Source:* SANS http://www.sans.org/top20/ • Multiple Vulnerabilities in LPD *Details:* eEye Digital Security http://www.eeye.com/html/Products/Retina/RTHs/Remote_Access/	To determine if the LPD service is running on the server.	The LPD service has inherent security flaws that could allow an attacker gain root privileges.	If the LPD service is running, it will show up on TCP port 515. This service should not be running because there is no explicit application need for this service.	Reference results from Item 4 to determine if the LPD service is running.	O
13	SANS Top 20 U8 – Sendmail *Source:* SANS http://www.sans.org/top20/ • Berkeley Sendmail v5 DEBUG Vulnerability • Sendmail 5.5 • Sendmail 5.61 • Sendmail 5.65 • Sendmail 5.65c	To determine if sendmail is running on the server.	Older versions of sendmail have vulnerabilities that could be exploited that would allow for privilege escalation. Misconfigured sendmail can be used as a mail relay.	If sendmail is running, it will show up on TCP port 25. This service should not be running because there is no explicit application need for this service.	Reference results from Item 4 to determine if sendmail is running.	O

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

	• Sendmail 8.6.10 • Sendmail 8.6.12 local root • Sendmail 8.6.9 ident execute attack • Sendmail 8.6.9 remote root via ident overflow • Sendmail 8.7.5 and lower overflows • Sendmail 8.7.5 and lower resource depletion • Sendmail 8.7.5 GECOS local root overflow • Sendmail 8.8.1 MIME remote root overflow • Sendmail 8.8.2 Daemon Mode Vulnerability • Sendmail 8.8.4 MIME overflow • Sendmail 8.8.4 overflow • Sendmail 8.8.5 DoS • Sendmail 8.8.6 DoS • Sendmail 8.8.8 HELO buffer overflow • Sendmail 8.9.1 DoS • Sendmail 8.9.2 DoS • Sendmail address field parsing buffer overflow • Sendmail aliases Database vulnerability • Sendmail Debug Command Line Integer Overflow Vulnerability • Sendmail Debugger Arbitrary Code Execution Vulnerability • Sendmail DNS Map TXT Overflow • Sendmail ETRN DoS • Sendmail group permissions escalation • Sendmail Invalid MAIL/RCPT Vulnerability • Sendmail maillocal vulnerability • Sendmail outdated • Sendmail prescan() address buffer overflow • Sendmail socket hijack vulnerability • Sendmail V5 local temporary file race condition • Sendmail version 5 remote root cmd execution • SMTP Relaying • SMTP Service Potential Security Hazard					

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

	• VRFY Command Enabled *Details:* eEye Digital Security http://www.eeye.com/html/Products/Retina/RTHs/Mail_Servers/					
14	SANS Top 20 U9 – BIND/DNS *Source:* SANS http://www.sans.org/top20/ • BIND 4 nslookupComplain() Buffer Overflow • BIND 4 nslookupComplain() Format Bug • BIND 8 Internal Memory Disclosure Vulnerability • BIND 8 Transaction Signatures Buffer Overflow • BIND 8.2.1 Buffer overflow in via NXT records • BIND 8.2.1 fdmax Denial of Service • BIND 8.2.1 maxdname Denial of Service • BIND 8.2.1 so_linger Denial of Service • BIND 9 chain response vulnerability • BIND Cache Poisoning • BIND iquery overflow *Details:* eEye Digital Security http://www.eeye.com/html/Products/Retina/RTHs/Dns_Services/	To determine if BIND/ DNS is running on the server.	Older versions of BIND/DNS have vulnerabilities that could be exploited to compromise the system or other systems due to security holes that need to be patched or due misconfiguration of services.	If BIND/DNS is running, it will show up on UDP port 53. This service should not be running because there is not explicit application need for this service.	Reference results from Item 4 to determine if BIND/DNS is running.	O
15	SANS Top U10 – General UNIX Authentication – Accounts with No Passwords or Weak Passwords *Source:* SANS http://www.sans.org/top20/	To determine if there are any accounts with no passwords or weak passwords.	Passwords are the primary means to secure system accounts. Accounts with no passwords or weak passwords can be compromised more easily than accounts with strong passwords.	If you run the manual command check, there should not be any lines of output if there are no accounts without passwords. There should be no accounts with blank passwords.	You can manually check for accounts with no passwords by running: **logins –p** To check for weak passwords, run a cracker program against the etc/passwd file.	O

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

16	Remote Access Audits *Source:* eEye Digital Security Policy Definition for SANS Top 20 (UNIX) in Retina • CDE Subprocess Control Service (dtspcd) BoF • Modem Installed • Multiple vendor login environment variable buffer overflow • Outdated SSH • telnet service • VNC server detected *Details:* eEye Digital Security http://www.eeye.com/html/Products/Retina/RTHs/Remote_Access/	To determine what remote access services are running.	Unauthorized and/or misconfigured remote access services can result in compromised systems. Examples include modem, VNC server, and Telnet.	If telnet service is running, it will show up on TCP port 23. The telnet service should be running in order to manage the system remotely. The service should be the latest version available, correctly configured, and have any vulnerabilities patched.	Reference results of scan from Item 4 to determine if Remote Access services are running.	O
17	IP Services Audits *Source:* eEye Digital Security Policy Definition for SANS Top 20 (UNIX) in Retina • CHARGEN service (Simple TCP Services on Windows) • echo service • finger service • gopher service • netstat service • systat service • uucp service • VPN Server • X Windows Font Server (XFS) *Details:* eEye Digital Security http://www.eeye.com/html/Products/Retina/RTHs/IP_Services/	To determine if any unnecessary services are running.	Unnecessary services can be exploited for unintended purposes regardless of configuration of patch status. For example, the chargen program could be used for a denial of service attack on another system.	Running services will show up on various TCP/UDP ports. These services should not be running except for echo because they are not explicitly needed by the application.	Reference results from Item 4 to determine if other services are running.	O

The following section details audit items that the Retina scanner will not detect. These items have to be executed manually, logged into the system as root.

Center for Internet Security HP-UX Benchmark v1.0.4 – Selected Items

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

18	Determine OS patch status. *Source:* Center for Internet Security, HP-UX Benchmark v1.0.4, Item 2.1 (modified) http://www.cisecurity.com/bench_HPUX.html	To determine patch level of the system and make sure that latest appropriate patches are installed.	Unpatched operating system files can leave security vulnerabilities unaddressed that can be exploited to compromise the system.	A listing of patches installed on the system.	Show list of patches by running: **swlist -l bundle |grep -i patch**	O
19	Determine security patch status. *Source:* Center for Internet Security, HP-UX Benchmark v1.0.4, Item 2.1 (modified) http://www.cisecurity.com/bench_HPUX.html Running this utility will require a download from hp and installation of the utility. Instructions to do this is found in section 2.1 of the source document.	To determine what security patches that need to be installed.	Unpatched operating system files can leave security vulnerabilities unaddressed that can be exploited to compromise the system.	A listing of recommended security patches to install.	Show list of patches by running the security patch scanner: **security_patch_check –c security_catalog**	O
20	Verify that no UID 0 accounts exist other than root. *Source:* Center for Internet Security, HP-UX Benchmark v1.0.4, Item 9.4 http://www.cisecurity.com/bench_HPUX.html	To determine which accounts have superuser rights.	Any account with UID 0 has superuser rights. The only account that should these rights is root.	A listing of accounts that have superuser rights.	Show list by running: **logins –d | grep ‘ 0 ‘**	O
The following section consists of checklist items that are not found on any checklist source.						
Miscellaneous Section						
21	Determine that users of the ChartMaxx Web application can only logon to the system via https. *Source:* Personal Experience	To determine if the logon page is accessible via http.	Logon pages that are accessible from http will transmit the logon information via clear text, which can be intercepted resulting in system compromise.	If a logon page is accessible via http, then the application logon is not secure. The logon page should only be accessible from https.	Connect to the ChartMaxx Web server via http and determine if the logon page is displayed.	O

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

Assignment 3: Audit Evidence

The items below represent the most significant findings of this audit.

Conduct the Audit

Item 5 – Identify Open Ports **Results: PASS**

The following ports were detected as open by the Retina scanner.

7: ECHO - Echo
Port State: Open

9: DISCARD - Discard
Port State: Open

13: DAYTIME - Daytime
Port State: Open

19: CHARGEN - Character Generator
Port State: Open

21: FTP - File Transfer Protocol [Control]
Detected Protocol: FTP
Port State: Open
Version: 220 SYSTEM FTP SERVER (VERSION 1.1.214.8 FRI APR 20 07:27:42 GMT 2001) READY. 500 'GET / HTTP/1.0': COMMAND NOT UNDERSTOOD. 500 ": COMMAND NOT UNDERSTOOD.

23: TELNET - Telnet
Detected Protocol: TELNET
Port State: Open
Version:

25: SMTP - Simple Mail Transfer Protocol
Detected Protocol: SMTP
Port State: Open
Version: 220 SYSTEM ESMTP SENDMAIL 8.8.6 (PHNE_17190)/8.8.6; TUE, 3 JUN 2003 16:28:18 -0700 (PDT)

37: TIME - Time
Port State: Open

80: WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
Detected Protocol: HTTP
Port State: Open
Version: APACHE/1.3.20 (UNIX) MOD_SSL/2.8.4 OPENSSL/0.9.6A

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

111: SUNRPC - SUN Remote Procedure Call
Port State: Open

113: IDENT - Authentication Service
Port State: Open

135: RPC-LOCATOR - RPC (Remote Procedure Call) Location Service
Port State: Open

161: UDP: SNMP - SNMP (Simple Network Management Protocol)
161: HP-UX system B.11.00 U 9000/800

443: HTTPS - HTTPS (Hyper Text Transfer Protocol Secure) - SSL (Secure Socket Layer)
Detected Protocol: HTTP
Port State: Open
Version: APACHE/1.3.20 (UNIX) MOD_SSL/2.8.4 OPENSSL/0.9.6A

512: EXEC - Remote Process Execution
Port State: Open

513: LOGIN - Remote Login via Telnet;
Port State: Open

514: SHELL - Automatic Remote Process Execution
Port State: Open

515: PRINTER - Printer Spooler
Port State: Open

543: KLOGIN -
Port State: Open

544: KSHELL - krcmd
Port State: Open

752: QRH -
Port State: Open

4045: LOCKD - NFS Lock Daemon
Port State: Open

6112: DTSPCD - dtspcd (sun.com)
Port State: Open

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

The following five audit findings are defined by Retina as high-risk. Only the high-risk findings are reported below. The results are taken directly from the Retina scanner results report.

Item 9 – SNMP Result: FAIL

The SNMP service is running with default community names. This service is not needed. If it were needed, the default community name should be changed.

SNMP Servers: public - SNMP default community name
Risk Level: High
Description: The community name set for the SNMP service was detected, this may be due to the fact it is a default community name enabled after installation.
How To Fix:
Disable this community name, or password protect use of it.
URL1: UCD-SNMP Home Page (http://ucd-snmp.ucdavis.edu/)
URL2: A Simple Network Management Protocol (SNMP) (ftp://ftp.isi.edu/in-notes/rfc1157.txt)
CVE: CAN-1999-0517

SNMP Servers: snmpd - SNMP default community name
Risk Level: High
Description: The community name set for the SNMP service was detected, this may be due to the fact it is a default community name enabled after installation.
How To Fix:
Disable this community name, or password protect use of it.
URL1: UCD-SNMP Home Page (http://ucd-snmp.ucdavis.edu/)
URL2: A Simple Network Management Protocol (SNMP) (ftp://ftp.isi.edu/in-notes/rfc1157.txt)
CVE: CAN-1999-0517

Item 13 – Sendmail Result: FAIL

The sendmail service is running. This service is not needed. If it were, the following vulnerabilities would need to be addressed.

Mail Servers: TCP:25 - Sendmail 8.8.6 DoS
Risk Level: High
Description: Holes exist in some Sendmail versions 8.8.6 and earlier that can allow a local user to initiate a denial of service (DoS) attack.
How To Fix:
Upgrade to the current version of Sendmail.
URL1: Sendmail Homepage. (http://www.sendmail.org)
CVE: CAN-1999-0684

Mail Servers: TCP:25 - Sendmail address field parsing buffer overflow
Risk Level: High

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

Description: Sendmail 8.12.7 and earlier contains a flaw in its message header address field parsing routine that can be leveraged to cause a buffer overflow. A remote attacker can exploit this vulnerability, using a specially-crafted "From", "To", or "CC" header, to execute arbitrary code in the context of the sendmail daemon.
How To Fix:
Upgrade to the most current version of Sendmail, or apply the appropriate vendor-provided patch.
URL1: Sendmail Consortium home page (http://www.sendmail.org/)
URL2: CERT Advisory CA-2003-07 (http://www.cert.org/advisories/CA-2003-07.html)
CVE: CAN-2002-1337
BugtraqID: 6991

Mail Servers: TCP:25 - Sendmail DNS Map TXT Overflow
Risk Level: High
Description: A remotely exploitable buffer overflow exists in Sendmail, versions 8.12.0 through 8.14.4. This vulnerability only exhibits itself if you have modified the configuration file to look up TXT records in DNS.
This check is also a sanity check to ensure you have the latest SendMail.
How To Fix:
Upgrade to the latest version.
URL1: Sendmail Homepage. (http://www.sendmail.org)

Mail Servers: TCP:25 - Sendmail prescan() address buffer overflow
Risk Level: High
Description: Sendmail 8.12.8 and earlier contains a buffer overflow vulnerability in its handling of e-mail addresses that can be precipitated by the use of a special character value. An attacker can exploit this vulnerability to execute arbitrary code in the context of the mail server.
How To Fix:
Upgrade to the most current version of Sendmail, or apply the appropriate vendor-supplied patch.
URL1: Sendmail Consortium home page (http://www.sendmail.org/)
URL2: CERT Advisory CA-2003-12 (http://www.cert.org/advisories/CA-2003-12.html)
CVE: CAN-2003-0161
BugtraqID: 7230

Item 16 – Remote Access – Telnet **Result: FAIL**

The telnet service was found to be running as expected. The scanner results indicate a buffer overflow vulnerability and recommendation that the Telnet service be replaced with SSH. The scanner also notes that this may be a false positive.

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

Remote Access: TCP:23 - Multiple vendor login environment variable buffer overflow
Risk Level: High
Description: The login program implementation utilized by multiple vendors is vulnerable to a buffer overflow condition that can allow attackers to execute arbitrary code. The problem is due to login not correctly handling environment variables of excessive length. Remote attackers can supply certain variables to programs that use login, such as telnetd or rlogin, to execute arbitrary code with root privileges. This may be a false positive.
How To Fix:
It is recommended you use SSH only, and disable login and rlogin.
Upgrade to the latest version.
Vulnerable Versions and Fixes:
IBM AIX 5.1, 4.3: ftp://aix.software.ibm.com/aix/efixes/security/tsmlogin_efix.tar.Z APAR for AIX 5.1 IY26221 APAR for AIX 4.3 IY26443 Sun Solaris: Solaris 8: 111085-02 Solaris 8_x86: 111086-02 Solaris 7: 112300-01 Solaris 7_x86: 112301-01 Solaris 6: 105665-04 Solaris 6_x86: 105666-04 Solaris 2.5.1: 106160-02 Solaris 2.5.1_x86: 106161-02 SCO Unix:
ftp://stage.caldera.com/pub/security/openserver/CSSA-2001-SCO.40/erg711877.506.tar.Z
ftp://stage.caldera.com/pub/security/openserver/CSSA-2001-SCO.40/erg711877.505.tar.Z
URL1: CERT Advisory CA-2001-34 (http://www.cert.org/advisories/CA-2001-34.html)
CVE: CVE-2001-0797
BugtraqID: 3681

Item 6 – RPC Services **Result: FAIL**

The RPC services are running as expected. The scanner results indicate that there are certain RPC services that have vulnerabilities that need to be addressed.

Rpc Services: RPC rpc.cmsd service
Risk Level: High
Description: The CDE Calendar Manager Service Daemon (rpc.cmsd) is running. Several severe vulnerabilities have been discovered in this RPC service in the past. Many of the vulnerabilities discovered in rpc.cmsd can lead to remote root compromise.
How To Fix:
Verify you have the most current version of cmsd from your vendor, or if this service is unnecessary, remove it following your vendor's directions.
CVE: CVE-1999-0320 CVE-1999-0696
BugtraqID: 524

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

Rpc Services: RPC rpc.statd service
Risk Level: High
Description: The Network Status Monitor RPC service (statd) is running. This service has had a long history of severe vulnerabilities affecting multiple vendors. Several of the vulnerabilities discovered in statd can lead to the remote root compromise of vulnerable servers.
How To Fix:
Verify you have the most current version of rpc.statd from your vendor, or if this service is unnecessary, remove it following your vendor's directions. It should be noted that, with some vendors, this service is included in the nfs-utils package.
CVE: CVE-1999-0018 CVE-1999-0019 CVE-1999-0493 CVE-2000

Rpc Services: RPC statd format string attack
Risk Level: High
Description: Several versions of the statd RPC service contain format string vulnerabilities that can be exploited by a remote attacker to execute code under the context of the root user.
How To Fix:
We recommend disabling this service due to it's vulnerable nature. If do not wish do disable this service obtain and install the latest version from your vendor.
CVE: CVE-2000-0666
BugtraqID: 1480

Rpc Services: RPC tooltalk services
Risk Level: High
Description: The tooltalk RPC services are running. Tooltalk services have had a long history of severe vulnerabilities. Several buffer overflow and format string vulnerabilities discovered in tooltalk implementations can be exploited to gain remote root access to servers running vulnerable tooltalk RPC services.
How To Fix:
Due to the vulnerable nature of tooltalk we recommend that you disable or remove it if you do not use it. If you do in fact use this service, we recommend that you verify you have all the latest patches installed that are available from your vendor.
URL1: CERT Advisory CA-2002-20: Multiple Vulnerabilities in CDE ToolTalk (http://www.cert.org/advisories/CA-2002-20.html)
URL2: CERT Advisory CA-2002-26: Buffer Overflow in CDE ToolTalk (http://www.cert.org/advisories/CA-2002-26.html)
CVE: CVE-1999-0003 CVE-1999-0693 CVE-2001-0717
BugtraqID: 122

Item 7 – Apache Web Server **Result: FAIL**

The Apache web server software is running as expected. The scanner results indicate that buffer overflow and denial of service vulnerabilities exist that need to be addressed.

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

Web Servers: TCP:443 - Apache chunking integer overflow vulnerability
Risk Level: High
Description: An integer overflow in the chunking implementation in many versions of the Apache web server can be exploited to gain remote access to the vulnerable web server.
How To Fix:
The Apache group has released updated versions of Apache on their website that eliminate this vulnerability.
URL1: Apache HTTP Group (http://httpd.apache.org/)
CVE: CVE-2002-0392
BugtraqID: 5033

Web Servers: TCP:80 - Apache chunking integer overflow vulnerability
Risk Level: High
Description: An integer overflow in the chunking implementation in many versions of the Apache web server can be exploited to gain remote access to the vulnerable web server.
How To Fix:
The Apache group has released updated versions of Apache on their website that eliminate this vulnerability.
URL1: Apache HTTP Group (http://httpd.apache.org/)
CVE: CVE-2002-0392
BugtraqID: 5033

Web Servers: TCP:443 - Apache mod_ssl session caching buffer overflow
Risk Level: High
Description: A vulnerability in session caching can be exploited by remote attackers to execute arbitrary code via a large client certificate that is signed by a trusted Certificate Authority (CA).
How To Fix:
Upgrade to the most recent version of OpenSSL to eliminate this and other vulnerabilities discovered in the past.
URL1: mod_ssl Homepage (http://www.modssl.org/)
URL2: Apache Webserver (http://httpd.apache.org)
CVE: CVE-2002-0082
BugtraqID: 4189

Web Servers: TCP:80 - Apache mod_ssl session caching buffer overflow
Risk Level: High
Description: A vulnerability in session caching can be exploited by remote attackers to execute arbitrary code via a large client certificate that is signed by a trusted Certificate Authority (CA).
How To Fix:
Upgrade to the most recent version of OpenSSL to eliminate this and other vulnerabilities discovered in the past.

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

URL1: mod_ssl Homepage (http://www.modssl.org/)
URL2: Apache Webserver (http://httpd.apache.org)
CVE: CVE-2002-0082
BugtraqID: 4189

Web Servers: TCP:443 - OpenSSL ASN.1 Parsing Error Denial Of Service Vulnerability
Risk Level: High
Description: A remotely exploitable denial of service condition has been reported in the OpenSSL ASN.1 library. This vulnerability is due to parsing errors and affects SSL, TLS, S/MIME, PKCS#7 and certificate creation routines. Using this vulnerability an attacker can disable a remote client or server by issuing a denial of service attack.
How To Fix:
Upgrade your OpenSSL package to eliminate this and other vulnerabilities discovered in the past.
URL1: OpenSSL Homepage (http://www.openssl.org)
URL2: Apache Web Server (http://httpd.apache.org)
CVE: CAN-2002-0659
BugtraqID: 5366

Web Servers: TCP:80 - OpenSSL ASN.1 Parsing Error Denial Of Service Vulnerability
Risk Level: High
Description: A remotely exploitable denial of service condition has been reported in the OpenSSL ASN.1 library. This vulnerability is due to parsing errors and affects SSL, TLS, S/MIME, PKCS#7 and certificate creation routines. Using this vulnerability an attacker can disable a remote client or server by issuing a denial of service attack.
How To Fix:
Upgrade your OpenSSL package to eliminate this and other vulnerabilities discovered in the past.
URL1: OpenSSL Homepage (http://www.openssl.org)
URL2: Apache Web Server (http://httpd.apache.org)
CVE: CAN-2002-0659
BugtraqID: 5366

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

The following items are stimulus / response items. There is an additional stimulus / response item in Assignment 4.

Item 15 – Accounts with no passwords **Result: PASS**

There are no accounts with no passwords.

```
root@system[/etc/rc.config.d]logins –p
root@system[/etc/rc.config.d]
```

Note: I was unable to test for weak passwords on the system due to problems with installing the password cracking program.

Item 18 – Determine OS Patch Status **Result: PASS**

The patch status is displayed.

```
root@system[/]swlist -l bundle |grep -i patch

  HWE1100          B.11.00.0203.5 Hardware Enablement Patches for HP-UX
11.00, March 2002
  XSWGR1100          B.11.00.47.08  General Release Patches, November
1999 (ACE)
```

Item 19 – Determine Security Patch Status **Result: PASS**

The systems administrator had to install the HP Security Patch Scanner since it is not installed by default. The security patch status is displayed.

```
root@system[/opt/sec_mgmt/spc/bin/security_patch_check –c security_catalog

*** BEGINNING OF SECURITY PATCH CHECK REPORT ***
Report generated by: /opt/sec_mgmt/spc/bin/security_patch_check.pl, run as root
Analyzed localhost (HP-UX 11.00) from system
Security catalog: security_catalog
Security catalog created on: Tue Aug 19 18:32:47 2003
Time of analysis: Wed Aug 20 10:30:18 2003

List of recommended patches for most secure system:

#  Recommended  Bull(s) Spec? Reboot? PDep? Description
-------------------------------------------------------------------------------
1  PHNE_28449   209     No    No      No    Bind 4.9.7 components
2  PHNE_28809   246 253 Yes   No      Yes   sendmail(1m) 8.9.3
3  PHNE_29231   270     No    Yes     No    nettl(1M) & nettladm(1M) cumulative
-------------------------------------------------------------------------------
*** END OF REPORT ***
NOTE: Security bulletins can be found ordered by number at
```


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

http://itrc.hp.com/cki/bin/doc.pl/screen=ckiSecurityBulletin

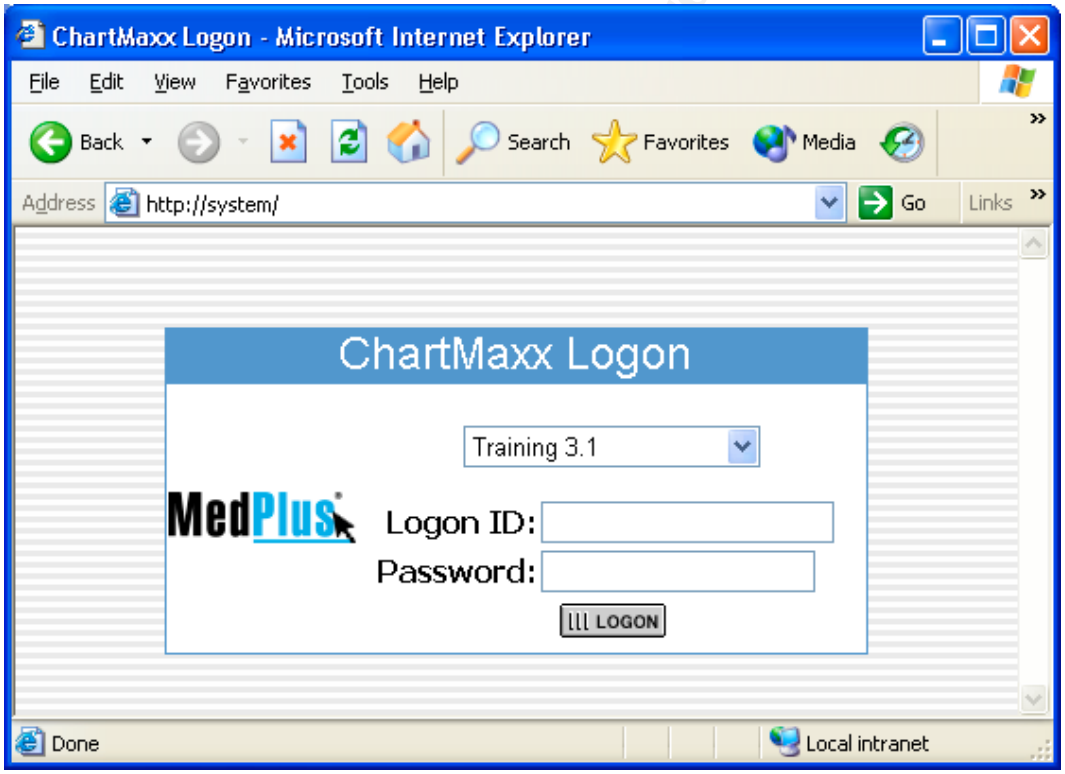
Item 20 – UID 0 Accounts **Results: FAIL**

There are other accounts with administrator rights. The actual account names except for root have been sanitized.

```
root@system[/etc/rc.config.d]logins -d | grep '0'
vendor      0     sys       3     MedPlus Diagnostic User
root        0     sys       3
software          203       software        203       ChartMaxx
Software
appadmin          203       software        203       ChartMaxx
Administrator
```

Item 21 – Web Application Logon **Results: FAIL**

The web logon is displayed using http.



Measure Residual Risk

Overall, the system is insecure. There are too many unnecessary services running and too many necessary services have unaddressed vulnerabilities, especially in core services such as web services. The good news is that these

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

vulnerabilities can be easily addressed by disabling the unnecessary services and patching the necessary services. This will take relatively minimal effort and cost.

Disabling the following services will leave no residual risk:

- SNMP.
- Sendmail.
- Telnet.
- Unneeded RPC services.

Patching the following services should leave no residual risk:

- Apache.

Installing the following software should leave no residual risk:

- SSH.

Installing the following patches should leave no residual risk, but we need to check with the vendor regarding impact to the application:

- OS patches.
- Security patches.

Modifying the following software should leave no residual risk, but we need to check with the vendor regarding impact to the application:

- Only allow https for logon page.

The following items do have some residual risk:

- Accounts other than root with administrator rights.

The total number of other accounts with administrator rights is three. These three accounts all are needed for the application to run and/or needed to provide support.

Evaluate the Audit

The system is auditable using the audit checklist. If the checklist steps are followed, the Retina scanner makes the system auditable. The Retina scanner makes the execution of the checklist less time consuming. The time saved by the scanner can be used to perform a better analysis of results and allow for more time to be spent on those items that are manually performed. Although there is improved time efficiency because of the scanner, the auditor needs to keep in mind to analyze the results and make sure they are reasonable. The auditor also needs to keep in mind that there is a greater chance of false positives due to the use of the scanner. This means that the auditor needs to take more care regarding analyzing the results.

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

Assignment 4: Risk Assessment

Summary

The objective of this assessment is to ensure that all vulnerabilities of this system are identified and address before the system is put into production for access via the Internet. The system state was tested against the SANS 20 Most Critical Internet Security Vulnerabilities for UNIX systems with the Retina Network Security Scanner. Additional manual tests were performed to test vulnerabilities that the Retina scanner cannot test.

The scope of the testing was confined to the operating system, the web server software, and the application software. These system components were tested to ensure that no unnecessary services were running, that there are no known unaddressed vulnerabilities, and that the software is securely configured.

Deficiencies were found in the following two areas:

- Unnecessary services are running and need to be disabled.
- Necessary services have security vulnerabilities that need to be addressed.

Background/Risk and Remediation

<u>Finding Item 9 – SNMP</u>

Background

The SNMP service is running with default community names. The organization is does not have any SNMP management software installed to manage the system utilizing this protocol. Since it is not needed, the service should be disabled.

Risk

The SNMP service is used to monitor and configure network devices. Unauthorized access to this service can lead to configuration changes that could result in a denial of service to this system. This would threaten the availability of this system and result in physicians not being able to access the data they need. Since this service is only accessible from the internal network, the likelihood of a malicious attack from someone external to the organization is low. But since most security breaches occur from inside a network, it is best practice to disable any unnecessary services.

Remediation

Since the organization is not using SNMP to monitor any systems, the service should be disabled. If later the service is needed, the SNMP software should be patched for any vulnerability and configured securely.

Cost

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

The cost to perform this is approximately 10 minutes of system administrator time.

Finding Item 13 – Sendmail

Background
The sendmail service is running. There is no need for this service to be running on this system. Since it is not needed, the service should be disabled.

Risk
The sendmail service is used to transport mail from system to system using SMTP. Improperly configured or unpatched sendmail systems can be used as mail relays to launch denial of service attacks against other systems. These same vulnerabilities can be used to compromise the security of the system running the service, letting an attacker to run commands with the same rights as the service. Since the organization already allows SMTP traffic from the Internet through the firewall in order to provide mail services, allowing this service to run on this system could expose it to attack from the Internet through the existing SMTP port on the firewall. Additionally, an internal user could use this server for unauthorized e-mail distribution by configuring their mail client to point to this server. Thus, it is best practice to disable unnecessary services.

Remediation
Since this server does not need mail services for its function, the sendmail service should be disabled.

Cost
The cost to perform this is approximately 10 minutes of system administrator time.

Finding Item 16 – Remote Access – Telnet

Background
The telnet service is running. This service is needed to remotely administer the system by both the organization's staff and the vendor.

Risk
The telnet service is by nature insecure. Each telnet session's data is sent unencrypted. If an attacker were able to capture the traffic between an administrator and the system, they would be able to obtain usernames and passwords with administrator rights. Additionally, there are vulnerabilities that could be exploited that could allow an attacker to execute code on the system with administrator privileges. Although the chance of these scenarios happening is low, best practices dictate that the telnet service be replaced with SSH.

Remediation

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

Disable the telnet service and replace with SSH.

Cost
The cost to perform this is approximately 2 hours of system administrator time.

Finding Item 6 – RPC Services

Background
RPC services are needed by the ChartMaxx Web application. The Retina scanner has detected vulnerabilities with some RPC services. . Some of these RPC services may or may not be needed by the ChartMaxx Web application.

Risk
The vulnerabilities detected with these RPC services can be exploited to allow administrator privileges on the system. The source for such an attack would be from the organization's internal network and would be unlikely to occur.

Remediation
A determination needs to be made whether the RPC services with vulnerabilities are needed by the ChartMaxx Web application. Those services that are not needed should be disabled. Services that are needed should be upgraded to the latest version.

Cost
The cost to perform this is approximately 30 minutes of system administrator time.

Finding Item 7 – Apache Web Server

Background
The Apache Web server software is critical to the functioning of the ChartMaxx Web application.

Risk
The version of the software that is installed has vulnerabilities in both the web server software and in the OpenSSL software that could allow an attacker to gain remote access to the server, execute code, or launch a denial of service attack. The risk of this occurring is high due to exposure to the Internet via ports 80 and 443, which are needed for access to the application.

Remediation
The Apache software should be upgraded to a version that has these vulnerabilities fixed. The OpenSSL software should be upgraded as well.

Cost
The cost to perform this is approximately 1 hour of system administrator time.

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

Finding Item 19 – Determine Security Patch Status

Background

The security patch scanner recommended 3 patches to be installed. The system administrator has determined that 2 of the 3 patches are not needed due to the services not being enabled – BIND and Sendmail.

Risk

The remaining patch that is recommended will be installed by the system administrator pending research into impact on the system and application.

Cost

The cost to perform this is approximately 1 hour of system administrator time.

Finding Item 20 – UID 0 Accounts

Background

UID 0 accounts are accounts that have administrator rights. Best practice states that only 1 account should have administrator rights by default.[2] There are 3 additional accounts with administrator rights on this system.

Risk

Multiple administrator accounts means that more than one account can be used to access the system with administrator rights. The *vendor* account is used by the vendor to provide system support. The *software* account is used by the ChartMaxx Web application and is need for the application to run. The *appadmin* account is used by the organization's IT staff to maintain the system. If the application is compromised by an attacker from a flaw in the application, since it is operating with administrator rights, the attacker will have administrator rights on the system. Since the application requires this configuration to run, it is important that any software the application depends on is patched.

Additionally, the use by the IT staff and the vendor of specific accounts with administrator rights could pose an accountability risk. If different support personnel are logging on to the system using these accounts, how can anyone be held accountable for the actions performed? Who knows who did what and when?

Remediation

The use of the *software* account cannot be remediated because of an application needed to run in an administrator context. The use of the *vendor* and *appadmin* accounts can be remediated by establishing adopting the practice of logging into

[2] CIS HP-UX Benchmark v1.0.4 Item 9.4 p. 35

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

the system using a non-privileged account and using the **su** command to obtain the needed administrator rights.[3]

Cost
The cost to perform this is approximately 1 hour of system administrator time and a change in operational process.

Finding Item 21 – Web Application Logon

Background
The ChartMaxx Web application logon page is accessible via http.

Risk
The http protocol sends data unencrypted. The logon page asks for a username and password. This data would be sent to the web server from the client unencrypted. The impact of this is that someone performing a man-in-the-middle attack could obtain account information that could be used to gain unauthorized access to the system and to the patient records that they system allows access to. Although the chance of this happening is low, best practice is to secure web logons with https.

Remediation
Configure the web server software to allow only https access to the logon page.

Cost
The cost to perform this is approximately 10 minutes of system administrator time.

System Changes and Further Testing

System Changes

The following corrective actions will be taken:

Remediation Item 9 – SNMP

The SNMP service will be disabled by the system administrator by changing the following parameters:

Corrective Action[4]

1. In the */etc/rc.config.d/SnmpHpunix* file, set SNMP_HPUNIX_START to 0 (**SNMP_HPUNIX_START=0**).

[3] CIS HP-UX Benchmark v1.0.4 Item 9.4 p. 35
[4] CIS HP-UX Benchmark v1.0.4 Item 4.9 p. 18

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

2. In the */etc/rc.config.d/SnmpMaster* file, set SNMP_MASTER_START to 0 (**SNMP_MASTER_START=0**).
3. In the */etc/rc.config.d/SnmpMib2* file, set SNMP_MIB2_START to 0 (**SNMP_MIB2_START=0**).
4. In the */etc/rc.config.d/SnmpTrpDst* file, set SNMP_TRAPDEST_START to 0 (**SNMP_TRAPDEST_START=0**).

Remediation Item 13 – Sendmail

The sendmail service will be disabled by the system administrator by changing the following parameters:

Corrective Action[5]

1. In the */etc/rc.config.d/mailservs* file, set SENDMAIL_SERVER to 0 (**SENDMAIL_SERVER=0**).

Remediation Item 16 – Remote Access – Telnet

The telnet service will be disabled by the system administrator and the SSH service will be installed.

Corrective Action[6]

1. In */etc/inetd.conf*, comment out the following: **telnet stream tcp nowait root /usr/lbin/telnetd telnetd** by adding a # before the first telnet (**#telnet stream tcp nowait root /usr/lbin/telnetd telnetd**).

Remediation Item 6 – RPC Services

The RPC.statd service is needed by the application. The other RPC services are not needed and will be disabled by the system administrator.

Corrective Action

1. The system administrator created a script to take care of this remediation item and the security administrator is relying on his expertise in this matter.

Remediation Item 7 – Apache Web Server

The Apache Web server vulnerabilities will be remediated by upgrading to the latest version of the Apache software that is compatible with the ChartMaxx Web application. The application vendor will be responsible for this remediation.

Corrective Action

[5] CIS HP-UX Benchmark v1.0.4 Item 4.7 p. 17
[6] CIS HP-UX Benchmark v1.0.4 Item 3.2 p. 8 (modified)

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

1. The vendor will be performing the steps necessary to accomplish this.

Remediation Item 19 – Determine Security Patch Status

The system administrator will install the recommended patch pending a determination as to impact on the system and application.

Corrective Action

1. The system administrator will perform the steps necessary to accomplish this.

Remediation Item 20 –UID 0 Accounts

The security administrator will recommend to the system owner that both the IT staff and the vendor be assigned non-privileged accounts that can be used logon purposes and then raised to privileged status via the **su** command.

Corrective Action

1. The system owner will need to determine whether she accepts this recommended remediation.

Remediation Item 21 – Web Logon

The web logon page will be made accessible only via http. The application vendor will be responsible for this remediation.

Corrective Action

1. The vendor will be performing the steps necessary to accomplish this.

Re-testing Results

The following results were produced after re-testing the system for compliance.

Re-testing Item 5 – Identify Open Ports Results: PASS

The following ports were detected as open by the Retina scanner.

7: ECHO - Echo
Port State: Open

9: DISCARD - Discard
Port State: Open

13: DAYTIME - Daytime

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

Port State: Open

22: SSH - SSH (Secure Shell) Remote Login Protocol
Detected Protocol: SSH
Port State: Open
Version: SSH-1.99-OPENSSH_3.5P1

37: TIME - Time
Port State: Open

80: WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
Detected Protocol: HTTP
Port State: Open
Version: APACHE/1.3.26 (UNIX) MOD_SSL/2.8.10 OPENSSL/0.9.6E

111: SUNRPC - SUN Remote Procedure Call
Port State: Open

135: RPC-LOCATOR - RPC (Remote Procedure Call) Location Service
Port State: Open

443: HTTPS - HTTPS (Hyper Text Transfer Protocol Secure) - SSL (Secure Socket Layer)
Detected Protocol: HTTP
Port State: Open
Version: APACHE/1.3.26 (UNIX) MOD_SSL/2.8.10 OPENSSL/0.9.6E

1508: DIAGMOND - diagmond
Port State: Open

4045: LOCKD - NFS Lock Daemon
Port State: Open

Re-testing Item 9 – SNMP **Result: PASS**

There is no SNMP service running as evidenced by the port scan results.

Re-testing Item 7 – Sendmail **Result: PASS**

There is no sendmail service running as evidenced by the port scan results.

Re-testing Item 16 – Remote Access – Telnet **Result: PASS**

There is no Telnet service running as evidenced by the port scan results.

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

Re-testing Item 6 – RPC Services Result: FAIL

Re-testing for RPC services still shows vulnerabilities with this service.

Rpc Services: RPC rpc.statd service
Risk Level: High
Description: The Network Status Monitor RPC service (statd) is running. This service has had a long history of severe vulnerabilities affecting multiple vendors. Several of the vulnerabilities discovered in statd can lead to the remote root compromise of vulnerable servers.
How To Fix:
Verify you have the most current version of rpc.statd from your vendor, or if this service is unnecessary, remove it following your vendor's directions. It should be noted that, with some vendors, this service is included in the nfs-utils package.
CVE: CVE-1999-0018 CVE-1999-0019 CVE-1999-0493 CVE-2000

Rpc Services: RPC statd format string attack
Risk Level: High
Description: Several versions of the statd RPC service contain format string vulnerabilities that can be exploited by a remote attacker to execute code under the context of the root user.
How To Fix:
We recommend disabling this service due to it's vulnerable nature. If do not wish do disable this service obtain and install the latest version from your vendor.
CVE: CVE-2000-0666
BugtraqID: 1480

Re-testing Item 7 – Apache Web Server Result: FAIL

Re-testing for Apache Web Server still shows vulnerabilities with this service.

Web Servers: TCP:443 - ApacheBench multiple buffer overflows
Risk Level: High
Description: The ApacheBench benchmark support program (ab.c) included in versions of Apache prior to 1.3.27, and 2.0.x versions prior to 2.0.43, may allow a local attacker or a malicious web server to execute arbitrary code on a machine executing a susceptible version of the utility.

Note that this alert may be a false positive, as Retina cannot directly determine the presence of the vulnerable program.
How To Fix:
Upgrade to the latest version of Apache to eliminate this vulnerability, or as a workaround, simply remove the utility or avoid running it against untrusted hosts.
URL1: Apache HTTP Server Project home page (http://httpd.apache.org/)
URL2: Bugtraq: BID 5996 (http://www.securityfocus.com/bid/5996)
CVE: CAN-2002-0843
BugtraqID: 5995

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

Web Servers: TCP:80 - ApacheBench multiple buffer overflows
Risk Level: High
Description: The ApacheBench benchmark support program (ab.c) included in versions of Apache prior to 1.3.27, and 2.0.x versions prior to 2.0.43, may allow a local attacker or a malicious web server to execute arbitrary code on a machine executing a susceptible version of the utility.

Note that this alert may be a false positive, as Retina cannot directly determine the presence of the vulnerable program.
How To Fix:
Upgrade to the latest version of Apache to eliminate this vulnerability, or as a workaround, simply remove the utility or avoid running it against untrusted hosts.
URL1: Apache HTTP Server Project home page (http://httpd.apache.org/)
URL2: Bugtraq: BID 5996 (http://www.securityfocus.com/bid/5996)
CVE: CAN-2002-0843
BugtraqID: 5995

Re-testing Item 19 –Security Patch Status **Result: Not Tested**

The system administrator has not completed his research regarding impact of this patch.

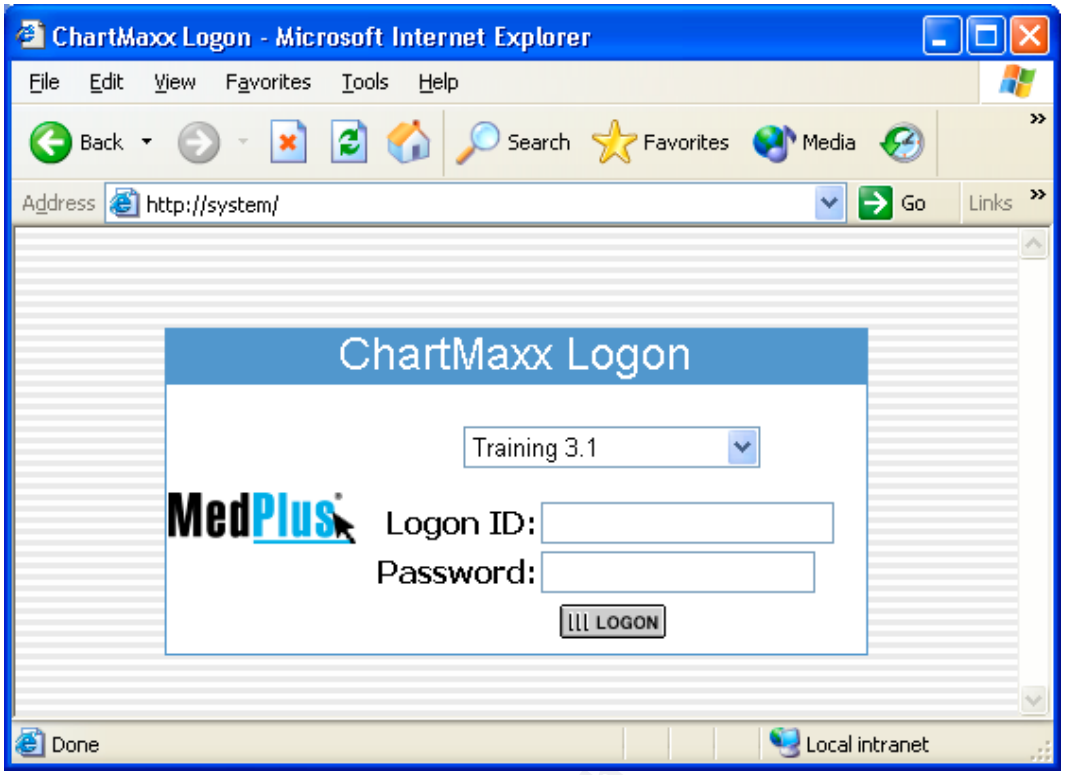
Re-testing Item 20 – UID 0 Accounts **Result: FAIL**

The system owner has rejected the security administrator's remediation recommendation.

Re-testing Item 21 – Web Application Logon **Result: FAIL**

Re-testing the Web Application Logon still shows vulnerabilities.

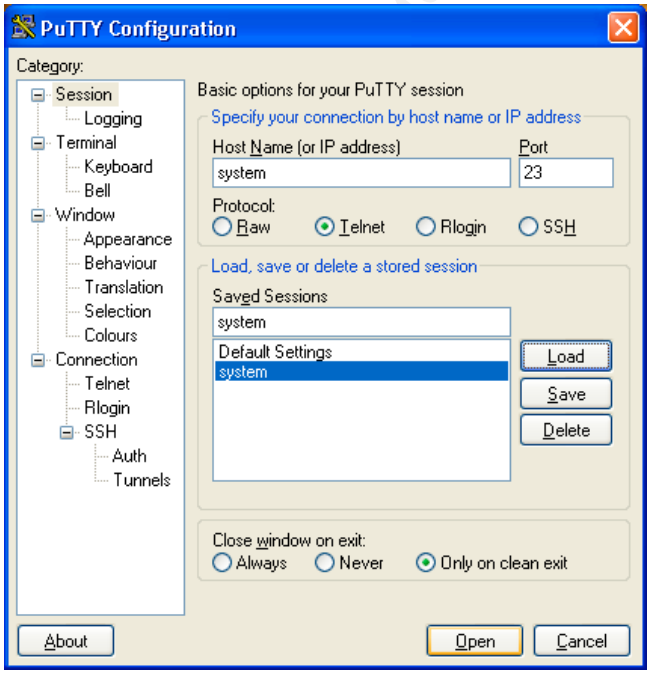
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



The following test is a stimulus/response test to ensure that administrators are able to logon to the system via SSH now that Telnet is disabled.

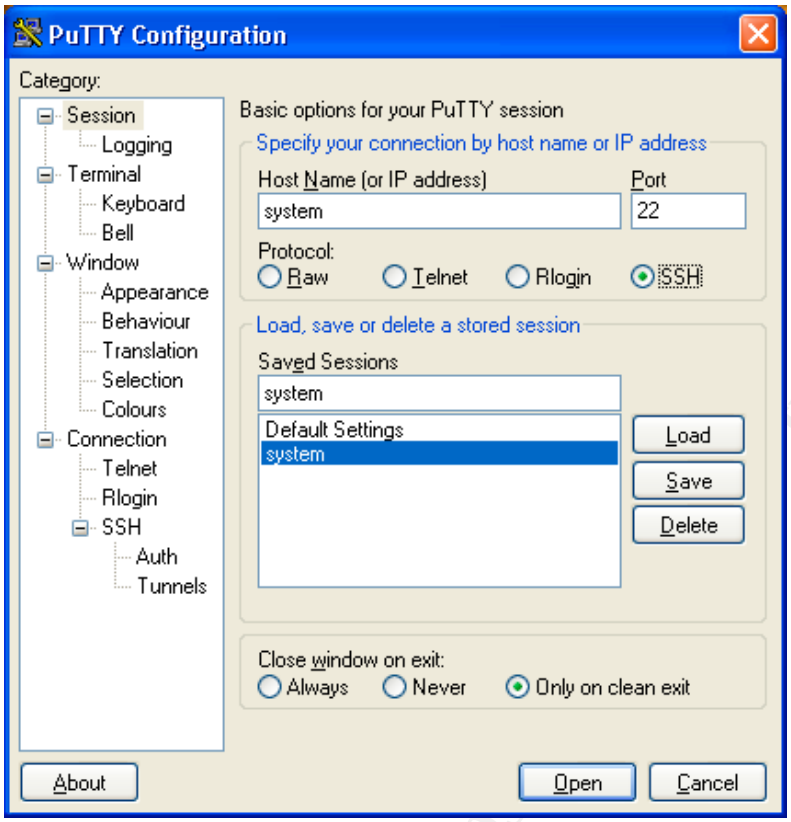
Re-testing Item 8 – SSH **Result: PASS**

Attempting to connect via Telnet fails, …



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

but SSH succeeds.



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

System Justification

The data used for this practical was taken from a real-world audit that resulted in three separate test, analyze, remediate, and re-test iterations. The test results from the first iteration were used for Assignment 3. The test results from the second iteration were used for the re-test results for Assignment 4. The results from the third iteration will be used for the System Justification section of Assignment 4. As with the previous sections, only items deemed high-risk by the Retina scanner are reported on.

In the third iteration, the following items found insecure in the second iteration were secured:

Item 6 – RPC Services
Item 7 – Apache Web Server
Item 19 – Security Patch Status
Item 21 – Web Application Logon

The following items were left in an insecure or less-than-ideal state:

Item 20 – UID 0 Accounts

It was determined by the system owner that the recommended remediation would place an undue burden on the business process of the organization, to both the IT staff and support vendor.

Mitigating controls

The support vendor accesses the system via VPN. This access is provided by individual user account and is logged. Although the support vendor is using a single account to access the ChartMaxx Web application server, the VPN access log can be used to determine who at the support vendor was connected to the organization's network. This information can be cross-referenced with the ChartMaxx Web application server logs to determine use of the support vendor administrator account by the vendor.

The system owner has agreed to accept the other risks associated with this item.

Conclusion - Practical

With the exception of Item 20, the other audit items were remediated. By submitting this system to the audit process and testing for best practice items, the organization has acted with reasonable care in securing this system for its intended function and environment.

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

Conclusion – Real-World Audit

All together, the scanner reported 17 high-risk, 10 medium-risk, 5 low-risk, and 1 informational vulnerabilities. Only the high-risk vulnerabilities were mentioned in this practical. The real-world audit of this system included all the Retina scanner findings, which were remediated. Two more iterations of test, report, remediate, and re-test were performed until the scanner reported that 2 medium-risk, 3 low-risk, and 1 informational vulnerabilities remained. These remaining risks were accepted by the organization due to the inability to mitigate them. The only way to mitigate was to upgrade the Apache software to a version that the vendor did not support.

This process occurred between May and August of 2003. Overall, this audit process was a success in the real-world. The cost of doing it was approximately 8 hours of system administrator time to mitigate the risks and 24 hours of security administrator time to test, analyze, and report the risks. This cost is much less than the cost of deploying an insecure system and having it compromised. The cost to the organization's reputation, plus any fines incurred, and the rebuilding and deployment of a new system would be much greater than the cost to secure the system in the first place.

© SANS Institute 2003, Author retains full rights.

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

References

- Final HIPAA Security Rule http://www.hipaadvisory.com/regs/finalsecurity/finalsecurity.txt
- SANS / FBI Top 20 List – http://www.sans.org/top20/
- Center for Internet Security HP-UX Level 1 Benchmark – http://www.cisecurity.com/bench_HPUX.html
- CERT UNIX Security Checklist v.2.0 – http://www.cert.org/tech_tips/unix_security_checklist2.0.html
- NIST CSRC Unix Security Checklist – http://csrc.nist.gov/pcig/cig.html
- Musaji,Yusufali F., Auditing and Security (New York: John Wiley & Sons, 2001) p. 421-447

© SANS Institute 2003, Author retains full rights.

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

Last Updated: May 1st, 2017

Upcoming Training

SANS Secure Europe 2017	**Amsterdam, Netherlands**	**Jun 12, 2017 - Jun 20, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**