



# 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 permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Auditing Systems, Applications, and the Cloud (Audit 507)"  
at <http://www.giac.org/registration/gsna>

# **Auditing a phpWebSite/MySQL Intranet System – An Administrator's Perspective**

.....

By John Van Hoogstraten

GSNA Practical Assignment

Version 2.1

Option 1

November 22, 2003

# **Table of Contents**

<b><u>Table of Contents</u></b> .....	2
<b><u>Abstract</u></b> .....	4
<b><u>Research in Audit, Measurement Practice and Control</u></b> .....	5
<i><u>Identify the System to be Audited:</u></i> .....	5
<i><u>Evaluate the Risk to the System:</u></i> .....	7
<i><u>Current State of Practice:</u></i> .....	10
<b><u>Create an Audit Checklist</u></b> .....	12
<i><u>Physical Environment Checklist</u></i> .....	12
<i><u>Backup &amp; Recovery Checklist</u></i> .....	13
<i><u>Network Checklist</u></i> .....	15
<i><u>Server &amp; Operating System Checklist</u></i> .....	17
<i><u>Web Server &amp; phpWebSite Checklist</u></i> .....	26
<i><u>Database Server Checklist</u></i> .....	28
<i><u>End User and IT Administrator InfoSec Training</u></i> .....	31
<b><u>Audit Evidence</u></b> .....	33
<i><u>Perform the Audit</u></i> .....	33
<i><u>Measure Residual Risk</u></i> .....	78
<i><u>Is the System Auditable?</u></i> .....	79
<b><u>Risk Assessment</u></b> .....	81
<i><u>Summary</u></i> .....	81
<i><u>Background/Risk</u></i> .....	82
<i><u>System Changes and Further Testing</u></i> .....	83
<i><u>System Justification</u></i> .....	100
<b><u>Appendix 1 – Nmap Results</u></b> .....	103
<i><u>IPCMS Portal &amp; Content Management Server:</u></i> .....	103
<i><u>IPCMS Database Server:</u></i> .....	103
<b><u>Appendix 2 – Nessus Results</u></b> .....	104
<i><u>IPCMS Portal &amp; Content Management Server:</u></i> .....	104
<i><u>IPCMS Database Server:</u></i> .....	113

<a href="#"><u>Appendix 3 – Nessus Retest Results</u></a> .....	120
<a href="#"><u>IPCMS Portal &amp; Content Management Server:</u></a> .....	120
<a href="#"><u>IPCMS Database Server:</u></a> .....	125
<a href="#"><u>References</u></a> .....	129

© SANS Institute 2003, Author retains full rights.

## **Abstract**

Until recently, the company that is the subject of this paper steered clear of open source software, preferring the security and accountability of large, closed source industry vendors such as Microsoft, Sun and IBM.

With the increase in mindshare that Linux is enjoying in the enterprise and its steady growth towards critical mass status, the management mindset that frowned upon open source software in general has been changing.

As open source operating systems and software have slowly started replacing non-critical company systems and proving their value and reliability, management's willingness to use these tools in higher risk systems has slowly increased.

After researching a number of closed and open source replacement alternatives for their aging Intranet system, a decision was made to use this opportunity as a showcase for the application of open source software in the company.

Red Hat Linux 8.0, phpWebSite and MySQL were chosen as the base components upon which the Intranet system would be built. Webmin and SSH would provide administrators easy access to the system from their desktop workstations.

As the majority of the company's administrators were from a Microsoft background and unfamiliar with UNIX and open source tools, a concerted effort was made to use visual administration interfaces wherever possible to ease the transition.

Because an IT system does not really exist unless it has an acronym, the project was dubbed IPCMS for Intranet Portal and Content Management System.

While the IPCMS system was to be a highly visible and important business tool, it was not deemed tier-one business critical. As such, it was a perfect way to show off the capabilities of open source software without putting the company in serious jeopardy should something go wrong.

On the other hand, important and potentially sensitive information that needed to be protected would reside on this high profile system that everyone in the company would be accessing.

Information security and system backup and recovery were therefore taken into account from the early design stages.

The IPCSM system was built, configured, tested and staged for the move into production over a period of several months. The final step in this process, an information security audit, is the subject of this paper.

# **Research in Audit, Measurement Practice and Control**

## **Identify the System to be Audited:**

### **System Description**

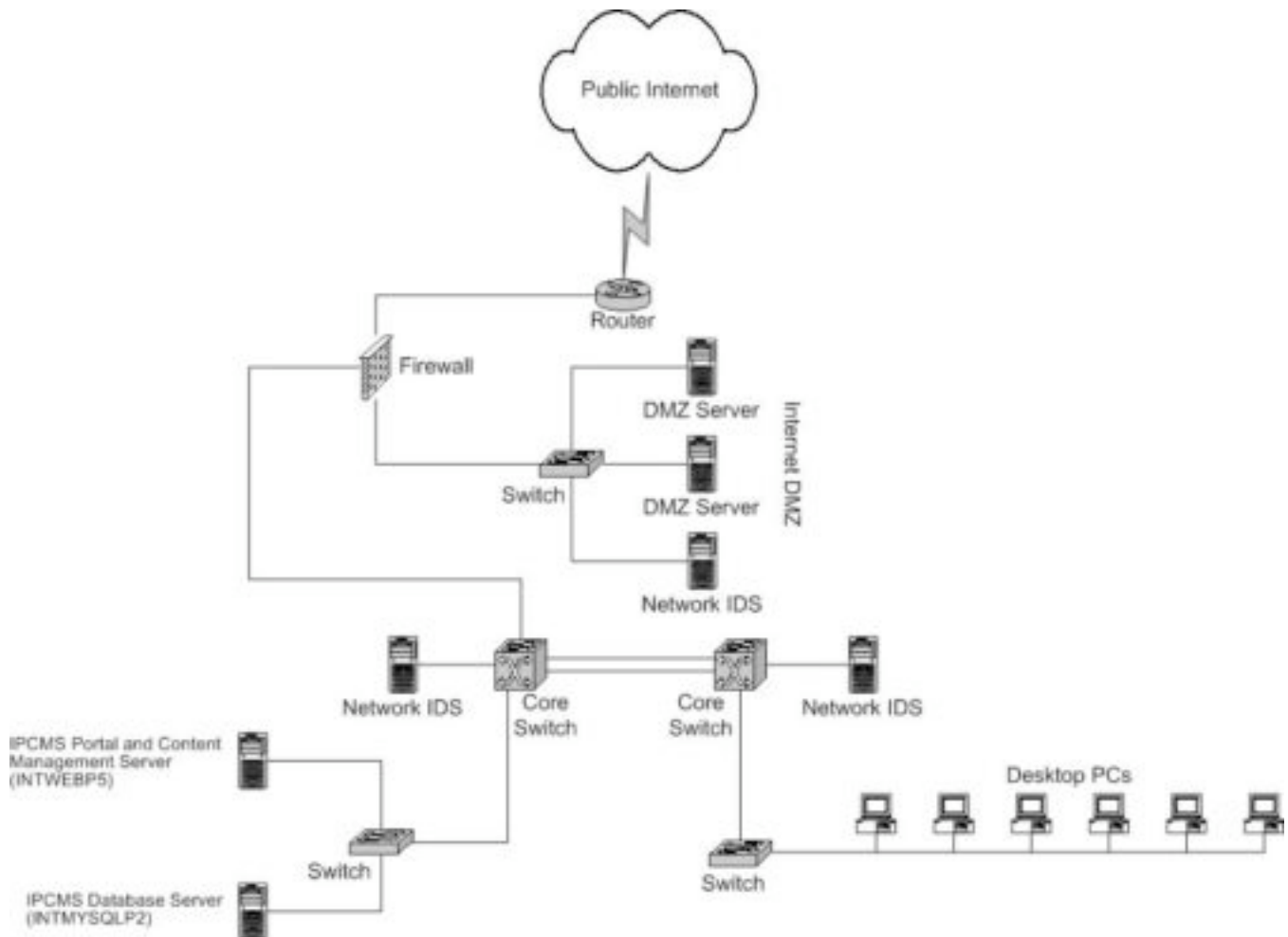
The system that I will be auditing is a new Intranet portal and content management system that will be serving the employees of a medium sized (approximately 500 employees) company.

The system has been through a change management process that includes proof of concept, development and staging phases and is now ready to be deployed in the company's production environment. Prior to the final step of moving the system into production, a security audit has been commissioned.

One of the goals of the Intranet Portal and Content Management System (IPCMS) project was to produce an enterprise ready system that uses open source and free software wherever possible without sacrificing functionality or reliability over proprietary, closed source solutions. After much evaluation and testing the following configuration was chosen for the system:

- 2 dedicated servers running Red Hat Linux 8.0.
  - Server 1 - Portal and Content Management Server
    - phpWebSite version 0.9.3-1
    - Apache version 2.0.4.0
    - PHP version 4.2.2
    - Webmin 1.110
    - SSH version 3.4
    - apt for Red Hat Linux 0.5.5
  - Server 2 - Database Server
    - MySQL version 3.23.58
    - Webmin version 1.110
    - SSH version 3.4
    - apt for Red Hat Linux 0.5.5

The 2 servers are connected together by a Cisco switch and protected from the Internet by a Cisco PIX firewall and ISS intrusion detection system. These network components are audited separately on a regular basis and are considered out of scope for the purpose of this paper.



## **Role of the System**

The Intranet Portal and Content Management System is for company employee use only and has no requirement for a direct connection to the Internet. Employees requiring access to the system from the Internet can do so through a VPN connection to the company's network.

The purpose of the system is to centralize and consolidate a number of disparate sources of content and information, as well as provide a forum for discussion and collaboration. The IPCMS system will provide the following functionality to the company:

- Company and department news and updates.
- Company employee directory.
- Employee submitted articles and news.
- Repository for the company's policies and procedures (Human resources, Information Security, etc).
- Company document and forms repository.
- Listing of open jobs available for internal posting.
- Company monthly newsletter.
- Discussion forums and electronic bulletin board.

- Company announcements, press releases and events calendar.
- Submission of suggestions and polls/surveys.

While not considered to be a tier 1 business critical system, important, potentially sensitive and proprietary information will be stored on the IPCMS system and its security must therefore be assured. To this end, the IT department made a point of taking security into account during the design and configuration of the system. Whether these security precautions are sufficient will be the subject of the audit described in this paper.

The audit will take into consideration the physical, operating system and application security of each of the two servers as well as the security of the IPCMS system as a whole.

### **Evaluate the Risk to the System:**

While the IPCMS system is not considered to be critical to business functionality it will contain sensitive, proprietary company and employee information and the security of this data must be protected.

As this system is intended primarily for access from within the internal network it is more likely that an IPCMS system breach would originate from an insider rather than someone outside the firewall.

An attack by an outsider cannot be ruled out, however as the system is open to the VPN and an attacker that breached the firewall would then be free to try and compromise the IPCMS system.

The following risks are considered to be the greatest causes for concern:

Threat	Likelihood	Consequence	Risk
An employee, insider working for a competitor or outside attacker gains inappropriate access to the IPCMS system and/or its data through improperly configured operating system security.	Low	High	Medium
An employee, insider working for a competitor or outside attacker gains inappropriate access to the IPCMS system and/or its data through improperly configured application security.	Medium	High	High
An employee, insider working for a competitor or outside attacker gains inappropriate access to the IPCMS system and/or its data through improperly configured database security.	Low	High	Medium



Threat	Likelihood	Consequence	Risk
An employee, insider working for a competitor or outside attacker gains inappropriate access to the IPCMS system and/or its data through improperly configured Webmin or SSH security.	Low	High	Medium
An employee, insider working for a competitor or outside attacker exploits an unpatched operating system vulnerability to gain inappropriate access to the IPCMS system and/or its data.	Medium	High	High
An employee, insider working for a competitor or outside attacker exploits an unpatched application vulnerability to gain inappropriate access to the IPCMS system and/or its data.	Medium	High	High
An employee, insider working for a competitor or outside attacker exploits an unpatched database vulnerability to gain inappropriate access to the IPCMS system and/or its data.	Medium	High	High
An employee, insider working for a competitor or outside attacker exploits an unpatched Webmin or SSH vulnerability to gain inappropriate access to the IPCMS system and/or its data.	Medium	High	High
An employee, insider working for a competitor or outside attacker exploits an unneeded application or service that has been left running on one of the servers in order to gain access to the IPCMS system and/or its data.	Low	High	Medium
An employee, insider working for a competitor or outside attacker successfully guesses or brute forces a user's account and uses it to gain inappropriate access to the IPCMS system and/or its data.	Medium	Medium	Medium
An employee, insider working for a competitor or outside attacker successfully guesses or brute forces an administrator's account and uses it to gain inappropriate access to the IPCMS system and/or its data.	Low	High	Medium

Threat	Likelihood	Consequence	Risk
An employee, insider working for a competitor or outside attacker successfully guesses or brute forces a service account and uses it to gain inappropriate access to the IPCMS system and/or its data.	Low	High	Medium
An employee, insider working for a competitor or outside attacker uses a network sniffer to intercept unencrypted traffic being transferred between the IPCMS system and end users.	Medium	Medium	medium
An employee, insider working for a competitor or outside attacker uses a network sniffer to intercept unencrypted traffic being transferred between the IPCMS system and an administrator's workstation.	Medium	High	High
An employee, insider working for a competitor or outside attacker uses a network sniffer to intercept unencrypted traffic being transferred between the Portal and Content Management Server and the Database Server.	Low	High	Medium
An employee, insider working for a competitor or outside attacker uses an operating system or application exploit or weakness to initiate a denial of service on the system.	Medium	Medium	Medium
An employee, insider working for a competitor or outside attacker obtains physical access to the servers and uses it to gain inappropriate access to the IPCMS system and/or its data.	Low	High	Medium
The freshrpms.net apt repository is compromised and security patches replaced with trojaned versions, leading to a denial of service or inappropriate access to the IPCMS system and/or its data.	Low	High	Medium
An employee, insider working for a competitor or outside attacker uses social engineering techniques to obtain a user ID and password.	High	Medium	High
An employee, insider working for a competitor or outside attacker uses social engineering techniques to obtain an administrator ID and password.	Medium	High	High

## **Current State of Practice:**

The audit requirements for the Intranet Portal and Content Management System can be broken down into 3 distinct categories:

- Physical Server, Red Hat 8.0 operating system, Webmin, SSH and apt for RPM administration tools which together make up the base platform on which the IPCMS system runs.
- The phpWebSite software, Apache and PHP which compromise the Portal and Content Management Server.
- The MySQL software that provides database backend functionality.

For each of these categories I researched books and used search engines in an attempt to find general security information, configuration guides and audit checklists.

What I discovered was that there was an abundance of information on securing and auditing UNIX and Linux, a fair amount of data on Internet and Intranet servers, and a relative scarcity of MySQL specific information.

After much research I narrowed down the books and Internet Web sites to the following list which includes the best and most valuable sources of InfoSec and audit information that I could find. In addition to personal knowledge and experience gained over the course of my IT and InfoSec career, I used a number of these resources in researching and writing this paper (See the *References* section for detailed information).

- **Books & Documents**

- O'Reilly & Associates - *Building Secure Servers with Linux*
- O'Reilly & Associates - *Linux Security Cookbook*
- O'Reilly & Associates - *Managing and using MySQL, 2<sup>nd</sup> Edition*
- O'Reilly & Associates - *Practical UNIX and Internet Security, 3<sup>rd</sup> Edition*
- O'Reilly & Associates - *Web Security, Privacy and Commerce, 2<sup>nd</sup> Edition*
- phpWebSite Documentation
- Printed course materials from SANS Track 7 (GSNA) - Auditing Networks, Perimeters, and Systems
- QUE Publishing – *MySQL, Second Edition*

- **Web Sites & Resources**

- [http://cio.ost.dot.gov/it\\_security/server\\_checklist.doc](http://cio.ost.dot.gov/it_security/server_checklist.doc)
- <http://csrc.nist.gov/publications/drafts.html>
- <http://www.auditnet.org/>
- <http://www.giac.org/GCUX.php>
- <http://www.giac.org/GSNA.php>
- <http://www.sans.org/score/>
- <http://www.sans.org/top20/>
- <http://www.theiia.org/itaudit/>

In addition to the above resources I also contacted my company's internal audit department to see if they had performed any similar audits, or had any checklists that I might be able to use. Unfortunately I drew a blank here, although they assured me that they would be interested in looking at anything that I produced.

© SANS Institute 2003, Author retains full rights.

## Create an Audit Checklist

### Physical Environment Checklist

<b>Step #</b>	<b>A1</b>
<b>Control Objective</b>	Ensure the IPCMS system's servers are secured against physical access.
<b>Risk</b>	Physical access to the servers would give an attacker the opportunity to gain console access and/or physically disable the system.
<b>Compliance</b>	The servers should be installed in an environment that limits access via locks or (preferably) card swipes with access logs.
<b>Test</b>	Ensure that the system's servers cannot be physically accessed without passing through an access control mechanism.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

<b>Step #</b>	<b>A2</b>
<b>Control Objective</b>	Ensure that only authorized employees and personnel have unescorted access to the IPCMS physical servers.
<b>Risk</b>	Cleaning staff, facilities workers and other non-IT workers could gain access to the systems console and/or physically disable the system.
<b>Compliance</b>	Only IT administrators and other authorized data center operations employees should have unescorted access to the data center.
<b>Test</b>	Review who has been issued keys or swipe card access to the secure server environment. Review swipe card access logs if they exist.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

<b>Step #</b>	<b>A3</b>
<b>Control Objective</b>	Ensure that the IPCMS system's servers have clean, reliable and uninterrupted power.
<b>Risk</b>	Unreliable power, brownouts and blackouts could all cause system downtime and/or corruption of data.
<b>Compliance</b>	The servers should be connected to a line filter or power distribution unit (PDU) and to an interruptible power supply (UPS).
<b>Test</b>	Check that the servers are physically connected to a line filter or power distribution unit (PDU) and to an interruptible power supply (UPS).
<b>Objective/Subjective</b>	Objective

<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience
<b>Step #</b>	<b>A4</b>
<b>Control Objective</b>	Ensure that the server environment has adequate temperature and humidity control systems (air conditioning).
<b>Risk</b>	Server overheating or condensation could lead to hardware failures that could cause system downtime and/or corruption of data.
<b>Compliance</b>	The server environment should have adequate temperature and humidity control systems (air conditioning) and a means to monitor changes in these parameters.
<b>Test</b>	Check for the existence of adequate temperature and humidity control (air conditioning) and monitoring systems.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

### **Backup & Recovery Checklist**

<b>Step #</b>	<b>B1</b>
<b>Control Objective</b>	Ensure that regular backups are being performed.
<b>Risk</b>	If backups of the system are not performed a system failure could result in significant downtime and the potential loss of all data.
<b>Compliance</b>	(1) Weekly full and nightly incremental/differential backups are performed. (2) Backup jobs complete successfully.
<b>Test</b>	(1) Review daily and weekly backup logs from the system to ensure that backups are being performed as required. (2) Review backup logs to ensure that jobs are not failing (a few failures are acceptable).
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

<b>Step #</b>	<b>B2</b>
<b>Control Objective</b>	Ensure that backups of the system can be successfully recovered.
<b>Risk</b>	Even though a backup job might complete successfully, a number of factors (storage, age, media quality, misconfiguration) can lead to the inability to restore the backed up data.
<b>Compliance</b>	The system and its data should be able to be successfully restored from backup media.
<b>Test</b>	Have an administrator restore the IPCMS system to 2 test servers from randomly selected backup media.

<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

<b>Step #</b>	<b>B3</b>
<b>Control Objective</b>	Ensure that backups of the system are stored off-site.
<b>Risk</b>	If backups are stored on-site, a disaster such as a fire could destroy the backups along with the production IPCMS system.
<b>Compliance</b>	Daily and weekly backups should be cataloged and stored off-site.
<b>Test</b>	Review backup storage procedures and obtain a listing of tapes stored off site, the date they were stored and their location.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

<b>Step #</b>	<b>B4</b>
<b>Control Objective</b>	Ensure that an adequate disaster recovery plan for the IPCMS system is in place and that it is tested regularly.
<b>Risk</b>	Without an adequate plan, the IPCMS system would be subject to significant downtime and the potential loss of all data in a disaster.
<b>Compliance</b>	An adequate, written, up to date and annually tested disaster recovery plan exists.
<b>Test</b>	Review the current disaster recovery plan for the IPCMS system and the results of the last 3 tests of the plan.
<b>Objective/Subjective</b>	Subjective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

**Network Checklist**

<b>Step #</b>	<b>C1</b>
<b>Control Objective</b>	Ensure that patch panels, routers, switches and other physical network components that connect to the IPCMS system are secured against physical access.
<b>Risk</b>	Physical access to network components would give an attacker the opportunity to monitor network traffic and/or physically disable the system.
<b>Compliance</b>	Patch panels, routers, switches and other physical network components that connect to the IPCMS system should be installed in an environment that limits access via locks or (preferably) card swipes with access logs.
<b>Test</b>	Ensure that Patch panels, routers, switches and other physical network components that connect to the IPCMS system cannot be physically accessed without passing through an access control mechanism.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

<b>Step #</b>	<b>C2</b>
<b>Control Objective</b>	Ensure that the IPCMS servers are connected to a switch, not a hub.
<b>Risk</b>	Switched network traffic is much harder to intercept and/or modify than traffic traversing a hub.
<b>Compliance</b>	The IPCMS servers should be attached to a network switch.
<b>Test</b>	Check that the IPCMS servers are connected to a network switch.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience



<b>Step #</b>	<b>C3</b>
<b>Control Objective</b>	Ensure that the IPCMS servers are protected by a network perimeter firewall
<b>Risk</b>	If the IPCMS servers are not protected from the open Internet by a network perimeter firewall, they are open to attack, compromise, denial of service and loss of data.
<b>Compliance</b>	The IPCMS system must be protected from the open Internet by a network perimeter firewall.
<b>Test</b>	(1) Review current network diagrams and documentation. (2) Review a printout of the current firewall rule set. (3) Use Nmap to scan the firewall from the outside (Internet).
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> O'Reilly & Associates - <i>Building Secure Servers with Linux</i> Personal Experience

<b>Step #</b>	<b>C5</b>
<b>Control Objective</b>	Ensure that the IPCMS servers are protected by a network based intrusion detection system.
<b>Risk</b>	Without a network based intrusion detection system an attacker could potentially compromise the IPCMS system without being detected.
<b>Compliance</b>	A network based intrusion detection system must be installed on a spanned port or network tap that has visibility into all network traffic originating from and terminating at the IPCMS servers.
<b>Test</b>	(1) Review network diagrams and/or question administrators to determine brand and placement of network IDS. (2) Review recent (within the past week) output from the network IDS. (3) Review network IDS output after audit steps <b>D5</b> (Nmap Scan) and <b>D7</b> (Nessus Scan) have been completed. Ensure that these simulated attacks are successfully detected.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

**Server & Operating System Checklist**

<b>Step #</b>	<b>D1</b>
<b>Control Objective</b>	Ensure that the IPCMS servers are protected by netfilter/iptables host based firewalls.
<b>Risk</b>	An attack that successfully compromised the network perimeter firewall or that originated on the internal company network would leave the IPCMS servers open to attack, compromise, denial of service and loss of data. The use of host based firewalls enhances protection of the system by providing “security in depth.”
<b>Compliance</b>	netfilter/iptables must be installed on each of the IPCMS system’s servers.
<b>Test</b>	Use Webmin’s <i>Bootup and Shutdown</i> module to verify that netfilter/iptables is installed and running.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O’Reilly & Associates - <i>Practical UNIX and Internet Security</i> O’Reilly & Associates - <i>Linux Security Cookbook</i> O’Reilly & Associates - <i>Building Secure Servers with Linux</i> Personal Experience

<b>Step #</b>	<b>D2</b>
<b>Control Objective</b>	Ensure that the IPCMS servers are protected by a host based intrusion detection system.
<b>Risk</b>	Network based intrusion detection systems are often unable to detect application layer attack attempts.
<b>Compliance</b>	A host based intrusion detection system must be installed on each of the IPCMS system’s servers.
<b>Test</b>	(1) Review system installation documentation and/or question administrators to determine if a host based IDS is installed and if so what brand. (2) Use Webmin’s <i>Bootup and Shutdown</i> module to verify that the host based IDS is installed and running. (3) Review the host based IDS output after audit steps <b>D5</b> (Nmap Scan) and <b>D7</b> (Nessus Scan) have been completed. Ensure that these simulated attacks are successfully detected.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O’Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

<b>Step #</b>	<b>D3</b>
<b>Control Objective</b>	Ensure that the IPCMS servers are protected by host based anti-virus software.
<b>Risk</b>	Infection of the servers by a virus or worm could lead to the system being compromised, downtime, loss of data and denial of service,
<b>Compliance</b>	Antivirus software must be installed on all of the IPCMS servers.
<b>Test</b>	<p>(1) Review system installation documentation and/or question administrators to determine if host based antivirus software is installed and if so what brand.</p> <p>(2) Use Webmin's <i>Bootup and Shutdown</i> module to verify that the antivirus software is installed and running.</p> <p>(3) Obtain a copy of the eicar test virus from <a href="http://www.eicar.org/">http://www.eicar.org/</a>. Copy it to each of the IPCMS servers and ensure that the antivirus software can detect it.</p>
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

<b>Step #</b>	<b>D4</b>
<b>Control Objective</b>	Ensure that only required services are running on the Portal and Content Management Server and the Database Server.
<b>Risk</b>	Unneeded services could potentially have no default security configuration, security vulnerabilities or be exploited to gain access to the IPCMS system. This could lead to the system being compromised, loss of data and denial of service.
<b>Compliance</b>	<p>Only the following services should be running:</p> <p><b>Portal and Content Management Server:</b></p> <ul style="list-style-type: none"> <li>• anacron</li> <li>• apmd</li> <li>• atd</li> <li>• autofs</li> <li>• chond</li> <li>• gpm</li> <li>• httpd</li> <li>• iptables</li> <li>• keytables</li> <li>• kudzu</li> <li>• network</li> <li>• ntpd</li> <li>• random</li> <li>• sshd</li> <li>• syslog</li> </ul>

	<ul style="list-style-type: none"> <li>• webmin</li> <li>• xfs</li> <li>• xinetd</li> </ul> <p><b>Database Server</b></p> <ul style="list-style-type: none"> <li>• anacron</li> <li>• apmd</li> <li>• atd</li> <li>• autofs</li> <li>• chond</li> <li>• gpm</li> <li>• iptables</li> <li>• keytables</li> <li>• kudzu</li> <li>• mysqld</li> <li>• network</li> <li>• ntpd</li> <li>• random</li> <li>• sshd</li> <li>• syslog</li> <li>• webmin</li> <li>• xfs</li> <li>• xinetd</li> </ul>
<b>Test</b>	<p>(1) Use Webmin's <i>Bootup and Shutdown</i> module to verify that only the services listed above are running.</p> <p>(2) Use Webmin's <i>Bootup and Shutdown</i> module to verify that none of the stopped services are set to start on boot.</p>
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	<p>O'Reilly &amp; Associates - <i>Practical UNIX and Internet Security</i></p> <p>O'Reilly &amp; Associates - <i>Building Secure Servers with Linux</i></p> <p>Personal Experience</p>

<b>Step #</b>	<b>D5</b>
<b>Control Objective</b>	Ensure that only known and necessary network ports are open on the IPCMS servers.
<b>Risk</b>	Unknown and/or unnecessary network ports could potentially have no default security configuration, security vulnerabilities or be exploited to gain access to the IPCMS system. This could lead to the system being compromised, loss of data and denial of service.
<b>Compliance</b>	<p>Only the following network ports should be open on the IPCMS servers:</p> <p>Portal and Content Management Server:</p> <ul style="list-style-type: none"> <li>• SSH on tcp port <b>22</b>.</li> <li>• HTTP on port <b>80</b>.</li> <li>• Webmin on port <b>10000</b>.</li> </ul> <p>Database Server</p> <ul style="list-style-type: none"> <li>• SSH on tcp port <b>22</b>.</li> <li>• MySQL on tcp port <b>3306</b>.</li> <li>• Webmin on tcp port <b>10000</b>.</li> </ul>
<b>Test</b>	Use Nmap with default settings to scan the IPCMS Portal and Content Management Server and Database Server from the local network.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	<p>O'Reilly &amp; Associates - <i>Practical UNIX and Internet Security</i></p> <p>O'Reilly &amp; Associates - <i>Building Secure Servers with Linux</i></p> <p>Printed course materials from SANS Track 7 (GSNA) - Auditing Networks, Perimeters, and Systems</p> <p>Personal Experience</p>

<b>Step #</b>	<b>D6</b>
<b>Control Objective</b>	Ensure that all available system security patches have been applied to the IPCMS servers.
<b>Risk</b>	Unpatched vulnerabilities provide an easy means for an attacker to compromise the IPCMS system, gain unauthorized access to data and/or cause a denial of service.
<b>Compliance</b>	All IPCMS servers must be updated with the latest available (stable) system security patches. Unapplied system and application patches that are not security related are acceptable.
<b>Test</b>	Use the Webmin <i>Software Patches</i> module to check for new and updated system security patches with the following options:  <b>Upgrade All Packages</b> Resynchronize package list (update) – Yes Perform distribution upgrade (upgrade-dist) – No Only show which packages would be upgraded – Yes
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Building Secure Servers with Linux</i> Printed course materials from SANS Track 7 (GSNA) - Auditing Networks, Perimeters, and Systems Personal Experience

<b>Step #</b>	<b>D7</b>
<b>Control Objective</b>	Ensure that there are no known high, serious or medium security risks on the IPCMS servers.
<b>Risk</b>	Known high, serious or medium security risks could potentially lead to the IPCMS system being compromised, loss of data and denial of service.
<b>Compliance</b>	A Nessus security scan should not return any high, serious or medium security risks. Low security risks are acceptable as long as they are investigated and documented.
<b>Test</b>	Use Nessus to scan all IPCMS servers using the “Enable all but dangerous plugins” option.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Printed course materials from SANS Track 7 (GSNA) - Auditing Networks, Perimeters, and Systems. Personal Experience

<b>Step #</b>	<b>D8</b>
<b>Control Objective</b>	Ensure that only authorized administrators have Linux login accounts on the IPCMS system's servers.
<b>Risk</b>	Users require only Web based access to the IPCMS system (User IDs and passwords are stored on the Database Server). Unauthorized user access to the IPCMS server's Linux operating system would increase the risk of system compromise, loss of data and denial of service.
<b>Compliance</b>	Only authorized administrators should have Linux accounts on the IPCMS system's servers.
<b>Test</b>	Use Webmin's <i>Users and Groups</i> module to ensure that only authorized administrators' accounts are present.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> O'Reilly & Associates - <i>Building Secure Servers with Linux</i> Personal Experience

<b>Step #</b>	<b>D9</b>
<b>Control Objective</b>	Ensure that the IPCMS server's Root and administrator account settings comply with the company's Password Protection InfoSec Policy.
<b>Risk</b>	Root and administrative accounts that do not have sufficiently complex, regularly changed passwords are open to dictionary and brute force attacks. A successful attack against the root or administrative accounts would give an attacker full access to the IPCMS system.
<b>Compliance</b>	Root and administrative passwords must be at least 8 characters long and be changed every 60 days.
<b>Test</b>	(1) Examine all IPCMS servers' /etc/login.defs file for the following entries:  <div style="margin-left: 40px;"> PASS_MAX_DAYS      60  PASS_MIN_LEN        8 </div> (2) Attempt to change the password of a test account to one that is non-complaint.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Knowledge

<b>Step #</b>	<b>D10</b>
<b>Control Objective</b>	Ensure that security logs are being maintained and checked daily on each of the IPCMS servers operating systems.
<b>Risk</b>	If security logs are not being maintained and checked regularly an attacker could compromise the IPCMS system and go undetected.
<b>Compliance</b>	(1) All successful and unsuccessful operating system logon attempts must be logged. (2) Logs must be reviewed daily.
<b>Test</b>	(1) Use Webmin's <i>System Logs</i> Module to verify the existence of the security log (/var/log/secure) and confirm that it is running. (2) Attempt to access each of the IPCSM server's operating systems using a valid and invalid password. Review the security log to verify that these access attempts were logged. (3) Randomly select 3 security exceptions from the log and question the system's administrators on how they handled and followed up on the alerts.
<b>Objective/Subjective</b>	Test 1 and 2 are objective. Test 3 is subjective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Printed course materials from SANS Track 7 (GSNA) - Auditing Networks, Perimeters, and Systems Personal Experience



## Administration Tool Checklist

<b>Step #</b>	<b>E1</b>
<b>Control Objective</b>	Ensure Webmin is configured to use SSL encryption.
<b>Risk</b>	An unencrypted Webmin session could potentially be monitored and/or hijacked by an attacker.
<b>Compliance</b>	All Webmin connections to the IPCMS servers must be via SSL.
<b>Test</b>	<p>(1) Inspect the <i>Webmin Configuration/SSL Encryption</i> Module for the following settings:</p> <p>Enable SSL if available – Yes  Private key file: /etc/webmin/miniserv.pem  Certificate file: Same file as private key  Redirect non-SSL requests to SSL mode – Yes</p> <p>(2) Connect to the Webmin server from a Web browser (<i>Server IP address/hostname:10000</i>) and ensure that the browser's navigation toolbar shows <b>https://server IP/hostname:10000</b>.</p> <p>(3) Attempt to establish a non SSL connection to the Webmin server (<b>http://server IP/hostname:10000</b>).</p>
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Building Secure Servers with Linux</i> O'Reilly & Associates - <i>Web Security, Privacy and Commerce</i> Personal Experience

<b>Step #</b>	<b>E2</b>
<b>Control Objective</b>	Ensure that Webmin logons are only allowed from the company's internal network.
<b>Risk</b>	Allowing outside access to Webmin significantly increases the system's exposure to compromise by an Internet attacker.
<b>Compliance</b>	Webmin logons should only be allowed from the company's internal IP address range.
<b>Test</b>	<p>Inspect the <i>Webmin Configuration/IP Access Control</i> module for the following settings:</p> <p><b>Access control options</b>  Only allow from address: <i>Company's Internal Address Range</i>  Resolve hostnames on every request – Selected</p>
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Building Secure Servers with Linux</i> Personal Knowledge

<b>Step #</b>	<b>E3</b>
<b>Control Objective</b>	Ensure that only authorized administrators have Webmin login accounts.
<b>Risk</b>	Webmin accounts have elevated or full administrative privileges on the IPCMS servers, which could potentially allow an unauthorized user to gain unrestricted access to the system and its data.
<b>Compliance</b>	Only authorized IPCMS administrators should have Webmin accounts.
<b>Test</b>	Use Webmin's <i>Webmin User</i> module to display all configured logon accounts.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

<b>Step #</b>	<b>E5</b>
<b>Control Objective</b>	Ensure that the SSH server is configured to deny remote logon by the Root account.
<b>Risk</b>	(1) If a remote attacker compromises the root account they would have unlimited access to the system and its data. (2) Administrators remotely logging on as root are not as accountable for their actions.
<b>Compliance</b>	(1) The SSH server should be configured to deny remote login by the root account. (2) Administrators should log on with their user account and use the <b>su</b> command to elevate their permissions when necessary.
<b>Test</b>	(1) Inspect the Webmin <i>SSH Server/Authentication</i> Module for the following setting:  <b>Login and authentication options</b> Allow login by root? – No  (2) Establish an SSH connection to each of the IPCMS servers from a workstation on the company's network and attempt to logon as root.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

## **Web Server & phpWebSite Checklist**

<b>Step #</b>	<b>F1</b>
<b>Control Objective</b>	Ensure that phpWebSite post-installation security configuration changes and removal of setup code was performed per the documentation.
<b>Risk</b>	<p>(1) Failure to implement phpWebSite post-installation security configuration changes leaves several system directories in a world writable (777) state.</p> <p>(2) Failure to remove the phpWebSite setup code could potentially allow an attacker to use these files as a means to reconfigure and compromise the phpWebSite application.</p>
<b>Compliance</b>	<p>(1) All phpWebSite post-installation security changes must be implemented.</p> <p>(2) All phpWebSite setup code must be removed.</p>
<b>Test</b>	<p>(1) Check that the following directory ownerships are set in the phpWebSite root directory (/var/www/html/):</p> <p style="padding-left: 40px;">/conf/ - <i>phpwebsite (user)</i>          /conf/ - <i>phpwebsite (group)</i>          /conf/branch/ - <i>apache (user)</i>          /conf/branch/ - <i>apache (group)</i></p> <p>(2) There should be no ./setup directory in the phpWebSite root directory.</p> <p>(3) Attempt to connect to the following URL: <i>intranet server address/setup</i></p>
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	<p>phpWebSite Documentation</p> <p>Personal Experience</p>

<b>Step #</b>	<b>F2</b>
<b>Control Objective</b>	Ensure that all applicable phpWebSite vulnerabilities listed on bugtraq and CVE have been researched, addressed and documented.
<b>Risk</b>	phpWebSite vulnerabilities that have not been addressed could potentially lead to the IPCMS system and its data being compromised by an attacker.
<b>Compliance</b>	All applicable phpWebSite vulnerabilities listed on bugtraq and CVE must have been researched, addressed and documented. If a vulnerability cannot be addressed, the reason and associated risk must be documented in a Risk Memo and signed by the company's Chief Security Officer (CSO).
<b>Test</b>	Search bugtraq and CVE for applicable phpWebSite vulnerabilities. Request documentation from the IPCMS administrators that describes how each vulnerability was addressed.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Printed course materials from SANS Track 7 (GSNA) - Auditing Networks, Perimeters, and Systems Personal Experience

<b>Step #</b>	<b>F3</b>
<b>Control Objective</b>	Ensure that phpWebSite's user and administrator accounts comply with the company's Password Protection InfoSec Policy.
<b>Risk</b>	phpWebSite user and administrator accounts that do not have sufficiently complex, regularly changed passwords are open to dictionary and brute force attacks. A successful attack against an administrator accounts would give an attacker full access to the IPCMS Intranet application.
<b>Compliance</b>	(1) User passwords must be at least 6 characters long and be changed every 60 days. (2) Administrator passwords must be at least 8 characters and be changed every 60 days.
<b>Test</b>	Inspect the configuration settings in phpWebSite's <i>Administration/User Administration/settings</i> module to verify that they conform to the company's Password Protection InfoSec Policy.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> O'Reilly & Associates - <i>Building Secure Servers with Linux</i> Personal Experience

## **Database Server Checklist**

<b>Step #</b>	<b>G1</b>
<b>Control Objective</b>	Ensure that the IPCMS Database Server's MySQL Root account has a password set.
<b>Risk</b>	A default MySQL installation leaves the Root account's password blank. This would allow an attacker to easily gain access to the MySQL server and its databases.
<b>Compliance</b>	The IPCMS Database Server's MySQL root account must have a password set.
<b>Test</b>	<p>(1) Use the Webmin <i>MySQL Database Server/User Permissions</i> module to check that all instances of the root account have an encrypted password set.</p> <p>(2) Attempt to connect to the MySQL Root account from the server console and a remote workstation using a blank password.</p>
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	<p>O'Reilly &amp; Associates - <i>Practical UNIX and Internet Security</i></p> <p>O'Reilly &amp; Associates - <i>Managing and using MySQL</i></p> <p>Personal Experience</p>

<b>Step #</b>	<b>G2</b>
<b>Control Objective</b>	Check that the phpWebSite application's MySQL account has a password and that it is set to only allow access from the IPCMS Portal and Content Management server
<b>Risk</b>	An attacker could use the phpWebSite application's MySQL account to gain full access to the MySQL server and its databases.
<b>Compliance</b>	(1) The phpWebSite application's MySQL account must have a password. (2) The phpWebSite application's MySQL account must be configured to only allow logons from the Portal and Content Management Server's IP address.
<b>Test</b>	<p>(1) Use the Webmin <i>MySQL Database Server/User Permissions</i> module to check that the phpWebSite application's MySQL account has an encrypted password set.</p> <p>(2) Use the Webmin <i>MySQL Database Server/User Permissions</i> module to check that the phpWebSite application's account is set to only accept connections from the IPCMS Portal and Content Management Server.</p> <p>(3) Attempt to log into the MySQL server from the Portal and Content Management Server using no password:  <b>mysql -D phpwebsite -h database server hostname or IP address</b></p> <p>(4) Attempt to log into the MySQL server from a location other than the Portal and Content Management Server, using the valid phpWebSite user account and password.</p>
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Managing and using MySQL</i> QUE Publishing – <i>MySQL</i> Personal Experience

<b>Step #</b>	<b>G3</b>
<b>Control Objective</b>	Ensure that only authorized database administrators have MySQL login accounts.
<b>Risk</b>	Only authorized database administrators (DBAs) require access to the IPCMS system's MySQL server. Non DBA access to the IPCMS system's MySQL server increases the risk of intentional or unintentional loss/corruption of data and denial of service.
<b>Compliance</b>	Only authorized DBAs should have access to the IPCMS system's MySQL server.
<b>Test</b>	Use the Webmin <i>MySQL Database Server/User Permissions</i> module to verify that only authorized database administrators have accounts.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> O'Reilly & Associates - <i>Managing and using MySQL</i>

	Personal Experience
--	---------------------

<b>Step #</b>	<b>G4</b>
<b>Control Objective</b>	Ensure that only the phpWebSite and MySQL databases exist on the IPCMS Database Server.
<b>Risk</b>	The MySQL database server is intended to be dedicated to the IPCMS system. The existence of non-IPCMS databases would indicate an increased information security exposure from unidentified applications and users connecting to the server.
<b>Compliance</b>	Only the phpWebSite and MySQL databases should exist on the IPCMS Database Server.
<b>Test</b>	Use the Webmin <i>MySQL Database Server</i> module to verify that only phpWebSite and MySQL databases exist on the IPCMS Database Server.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	Personal Experience

<b>Step #</b>	<b>G5</b>
<b>Control Objective</b>	Ensure that the database connection between the MySQL server and the IPCMS Portal and Content Management Server is strongly encrypted.
<b>Risk</b>	An unencrypted or weakly encrypted database connection between the MySQL server and the IPCMS Portal and Content Management Server could potentially be monitored and/or hijacked by an attacker.
<b>Compliance</b>	The database connection between the MySQL server and the IPCMS Portal and Content Management Server must be strongly encrypted.
<b>Test</b>	Request relevant IPCMS design and configuration documentation from the system's administrators, developers and architects. Use this documentation to confirm that a strong encryption solution has been implemented for the database connection.
<b>Objective/Subjective</b>	Subjective
<b>Reference</b>	O'Reilly & Associates - <i>Managing and using MySQL</i> QUE Publishing – <i>MySQL</i> Personal Experience

**End User and IT Administrator InfoSec Training**

<b>Step #</b>	<b>H1</b>
<b>Control Objective</b>	Ensure that all users of the IPCMS system have received end user information security training and have read and signed the company's InfoSec Acceptable Use Policy.
<b>Risk</b>	Lack of information security training and awareness can lead to social engineering attacks, user accounts being compromised and user security transgressions (inadvertent and willful).
<b>Compliance</b>	(1) All users of the IPCMS system must attend an in-house information security training session. (2) All users of the IPCMS system must read and sign the company's InfoSec Acceptable Use Policy.
<b>Test</b>	(1) Have HR review all IPCMS users' training records for evidence that they have attended one of the company's in-house information security training classes. (2) Have HR review all IPCMS users' files for evidence that they have signed the company's InfoSec Acceptable Use Policy.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i> Personal Experience

<b>Step #</b>	<b>H2</b>
<b>Control Objective</b>	Ensure that all administrators of the IPCMS system have attended SANS Security Essentials and the CISSP 10 Domains training (or comparable training) and have read and signed the company's InfoSec Acceptable Use Policy.
<b>Risk</b>	Lack of administrator InfoSec training and awareness can lead to an insecurely configured and maintained IT environment, social engineering attacks, administrator accounts being compromised and administrator security transgressions (inadvertent and willful).
<b>Compliance</b>	(1) All administrators of the IPCMS system must attend SANS Security Essentials and the CISSP 10 Domains training sessions (or comparable training). (2) All administrators of the IPCMS system must read and sign the company's InfoSec Acceptable Use Policy.
<b>Test</b>	(1) Have HR review all IPCMS administrators' training records for evidence that they have attended a SANS Security Essentials and the CISSP 10 Domains training session (or comparable training). (2) Have HR review IPCMS administrators' files for evidence that they have signed the company's InfoSec Acceptable Use Policy.
<b>Objective/Subjective</b>	Objective
<b>Reference</b>	O'Reilly & Associates - <i>Practical UNIX and Internet Security</i>



	Personal Experience
--	---------------------

© SANS Institute 2003, Author retains full rights.

## **Audit Evidence**

### **Perform the Audit**

A full audit of the IPCMS system was carried out using the checklists from the previous section.

For the purpose of this paper I chose to include the results from 11 particularly interesting checklist items to support my audit findings and risk assessment.

I have tried to balance the audit results I chose to include between those that were significant because they passed the audit and those that failed.

The included checklist items are:

- (1) **Step D4** – Ensure that only required services are running on the Portal and Content Management Server and the Database Server
- (2) **Step D5** – Ensure that only known and necessary network ports are open on the IPCMS servers.
- (3) **Step D6** – Ensure that all available system security patches have been applied to the IPCMS Servers.
- (4) **Step D7** – Ensure that there are no known high, serious or medium security risks on the IPCMS servers.
- (5) **Step D9** – Ensure that the IPCMS server's Root and administrator account settings comply with the company's Password Protection InfoSec Policy.
- (6) **Step E1** – Ensure Webmin is configured to use SSL encryption.
- (7) **Step E5** – Ensure that the SSH server is configured to deny remote logon by the Root account.
- (8) **Step F1** – Ensure that phpWebSite post-installation security configuration changes and removal of setup code was performed per the documentation.
- (9) **Step F3** – Ensure that phpWebSite's user and administrator accounts comply with the company's Password Protection InfoSec Policy.
- (10) **Step G2** – Check that the phpWebSite application's MySQL account has a password and that it is set to only allow access from the IPCMS Portal and Content management server.

- (11) **Step G5** – Ensure that the database connection between the MySQL server and the IPCMS Portal and Content Management Server is strongly encrypted.

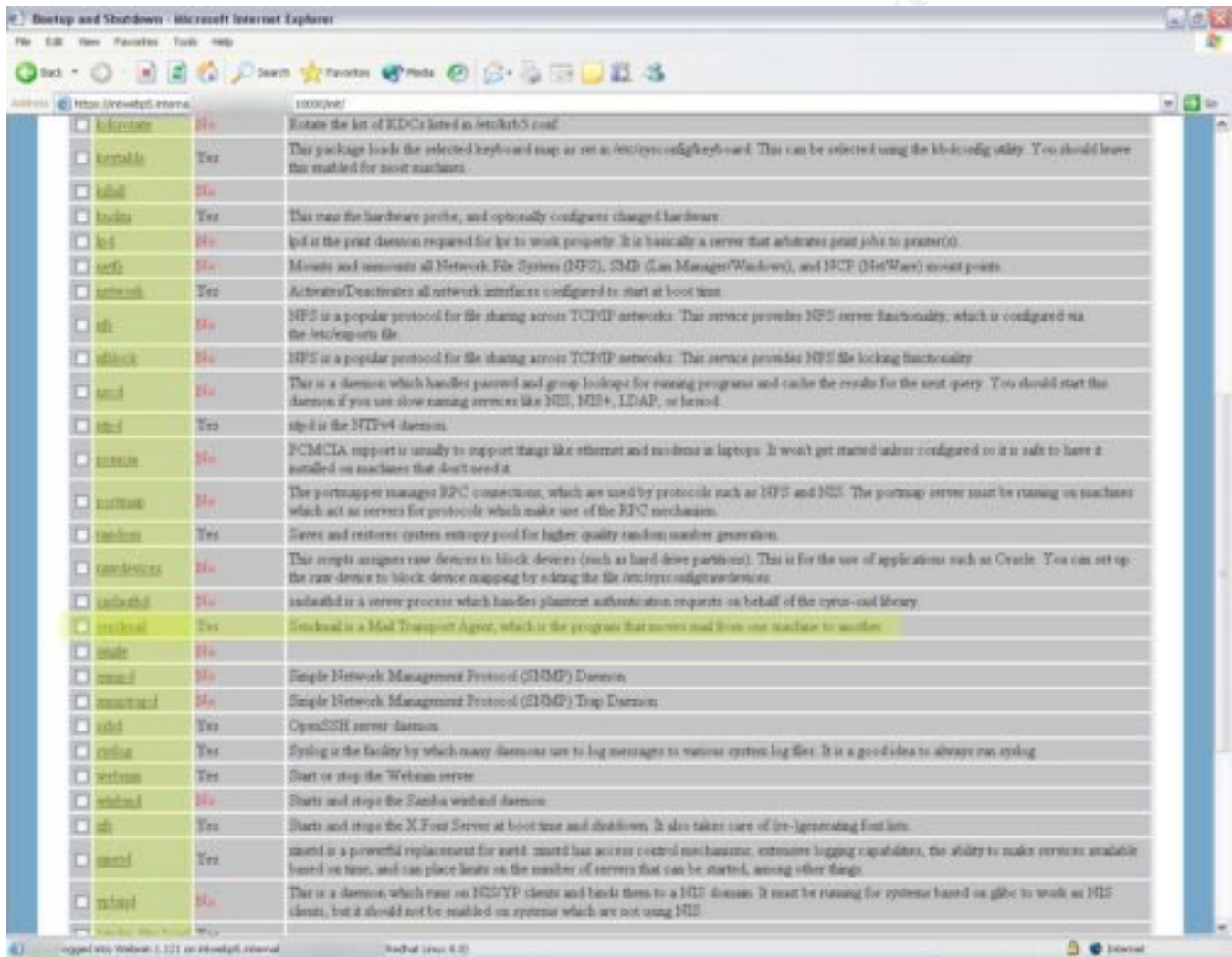
© SANS Institute 2003, Author retains full rights.

## Step D4

The control objective of this step is to ensure that only required services are running on the Portal and Content Management Server and the Database Server.

### Step D4(1)a

For this step Webmin's *Bootup and Shutdown module* was used to list all running and stopped services on the IPCMS Portal and Content Management Server.



The following list of services was found to be running on the IPCMS Portal and Content Management Server.

- anacron
- apmd
- atd
- autofs

- chond
- gpm
- httpd
- iptables
- keytables
- kudzu
- network
- ntpd
- random
- **sendmail**
- sshd
- syslog
- webmin
- xfs
- xinetd

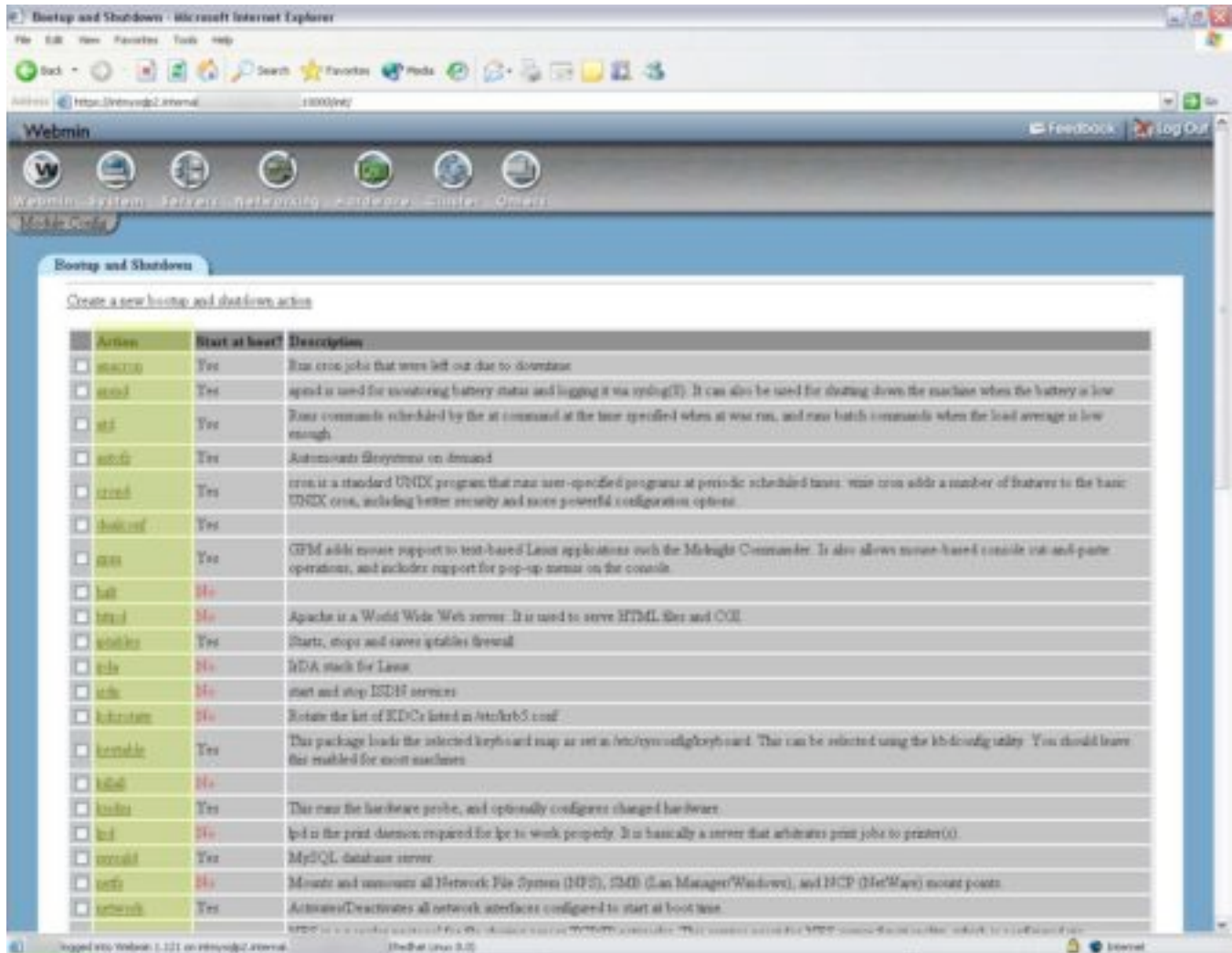
**Result:** As can be seen from the screenshot and list of services above, the IPCMS Portal and Content Management Server has the sendmail service running, which is not a required service.

**Pass/Fail:** **Fail**

© SANS Institute 2003, Author retains full rights.

**Step D4(1)b**

For this step Webmin's *Bootup and Shutdown module* was used to list all running and stopped services on the IPCMS Database Server.



The following list of services was found to be running on the IPCMS Database Server.

- anacron
- apmd
- atd
- autofs
- chronpd
- gpm
- iptables
- keytables
- kudzu
- mysqld
- network

- ntpd
- random
- sshd
- syslog
- webmin
- xfs
- xinetd

**Result:** Only the required services were found to be running on the IPCMS Database Server.

**Pass/Fail:** **Pass**

© SANS Institute 2003, Author retains full rights





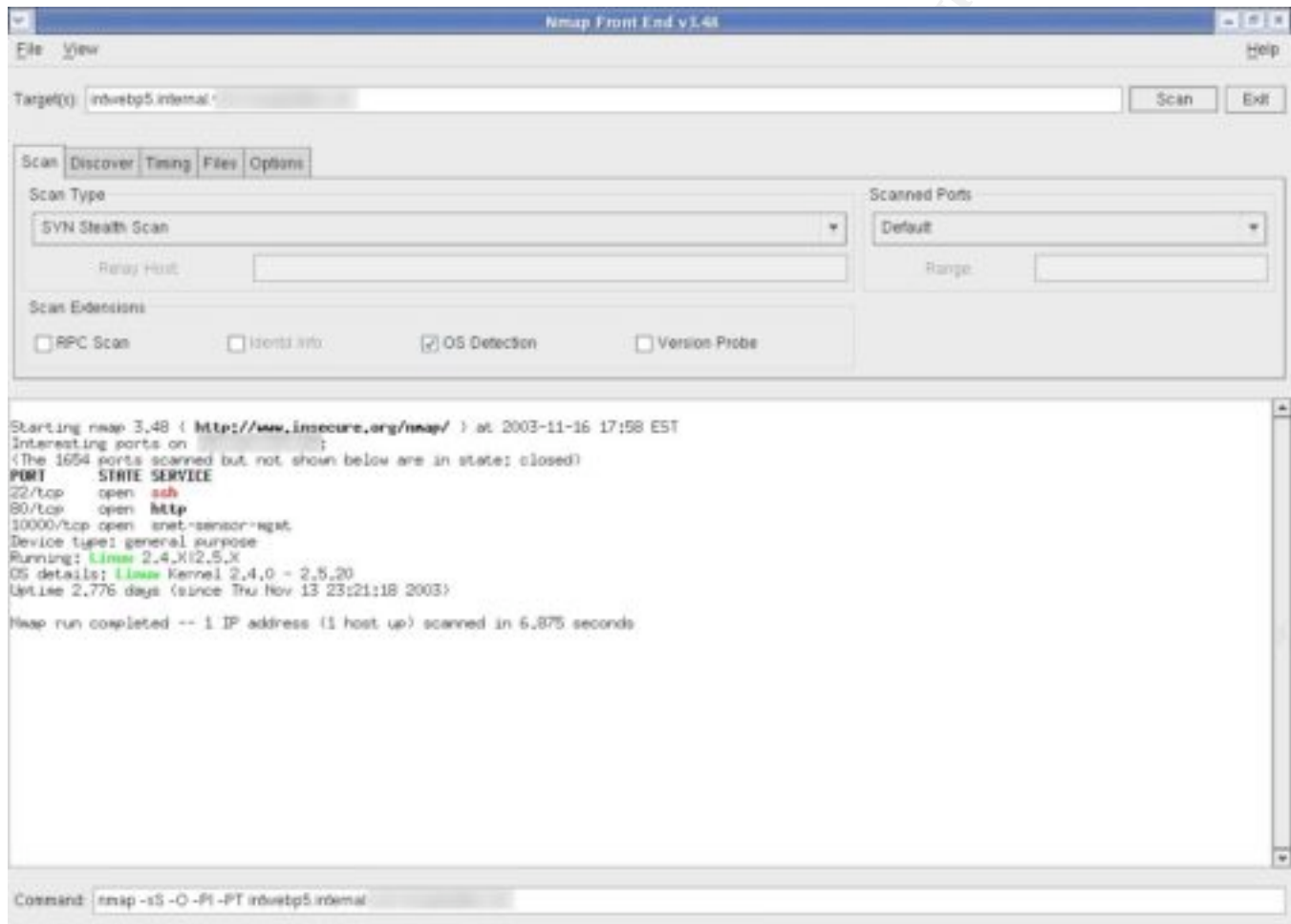


## **Step D5**

The control objective of this step is to ensure that only known and necessary network ports are open on the IPCMS servers.

### ***Step D5a***

Nmap version 3.48 (available from [www.insecure.org](http://www.insecure.org)) was used with default settings to scan the IPCMS Portal and Content Management Server.



The following network ports were found to be open on the IPCMS Portal and Content Management Server:

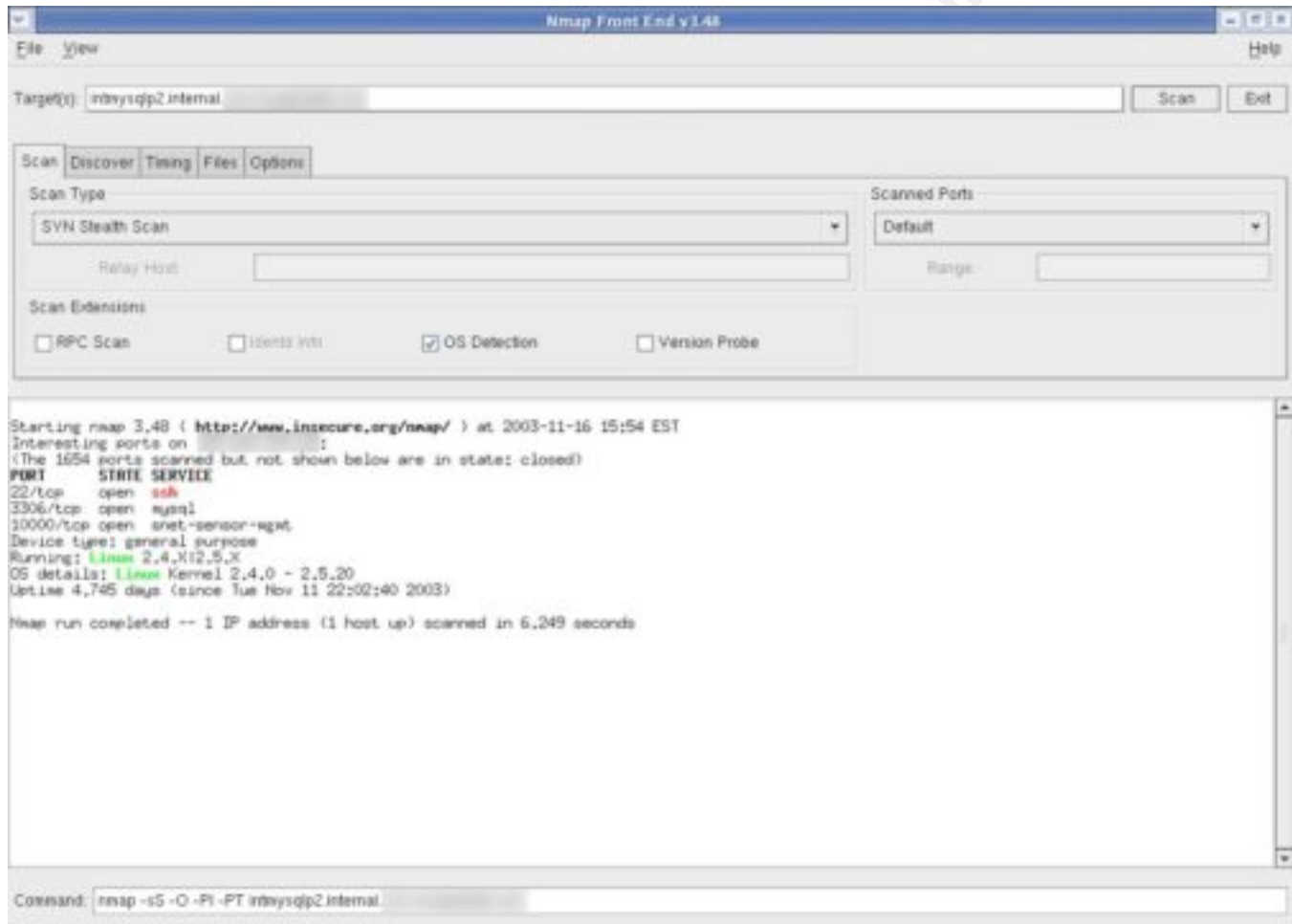
- SSH on tcp port **22**.
- HTTP on port **80**.
- Webmin on port **10000**.

**Result:** The open network ports on the IPCMS Portal and Content Management Server were found to be compliant with the audit requirements (See appendix 1 for complete Nmap results).

**Pass/Fail:** **Pass**

## Step D5b

Nmap version 3.48 (available from [www.insecure.org](http://www.insecure.org)) was used with default settings to scan the IPCMS Database Server.



The following network ports were found to be open on the IPCMS Database Server:

- SSH on tcp port **22**.
- MySQL on tcp port **3306**.
- Webmin on tcp port **10000**.

**Result:** The open network ports on the IPCMS Database server were found to be compliant with the audit requirements (See appendix 1 for complete Nmap results).

**Pass/Fail:** **Pass**

© SANS Institute 2003, Author retains full rights.

## **Step D6**

The control objective of this step is to ensure that all available system security patches have been applied to the IPCMS Servers.

### **Step D6a**

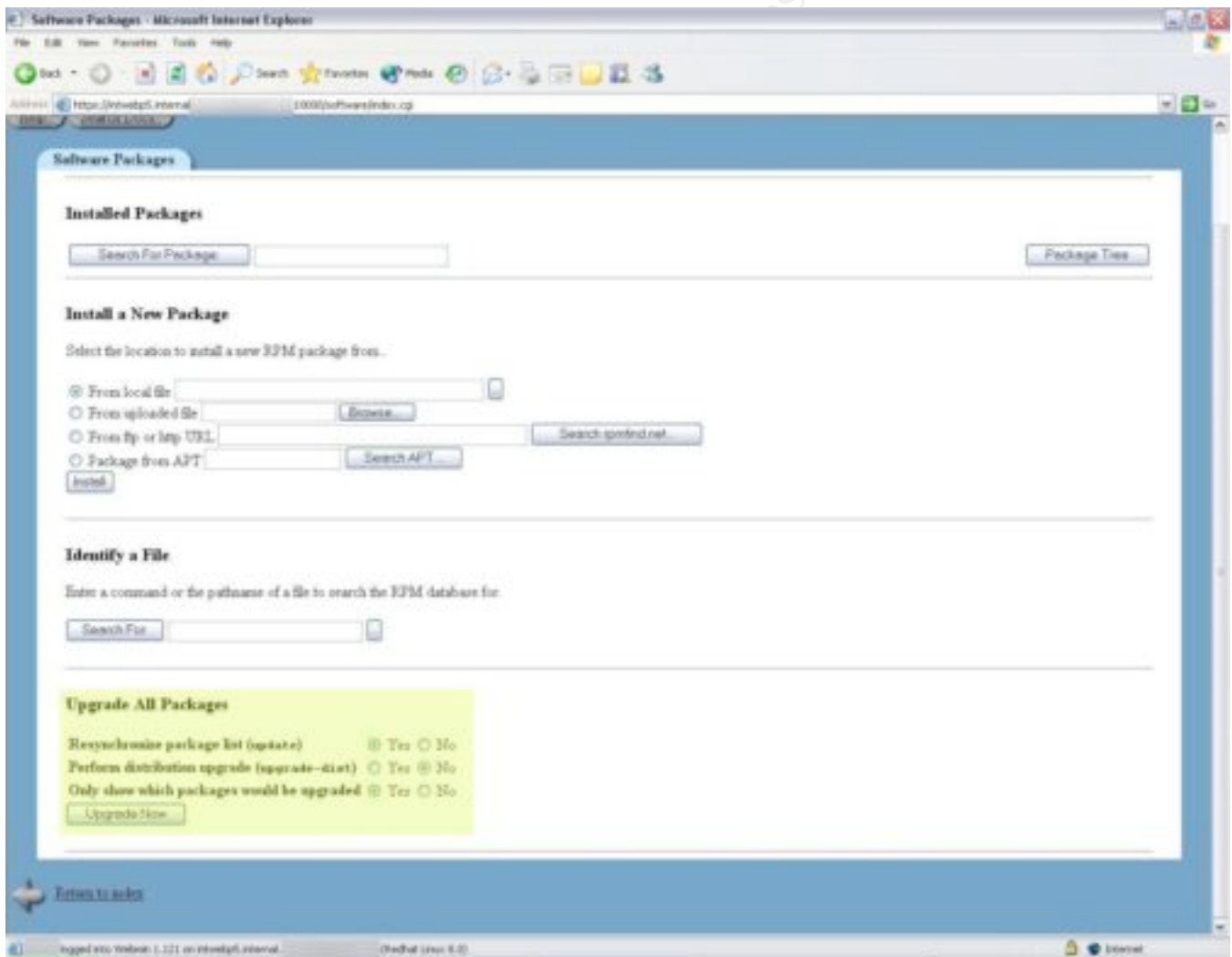
The Webmin *Software Patches* module was used to check the IPCMS Portal and Content Management Server for security (and other) patches using the following options:

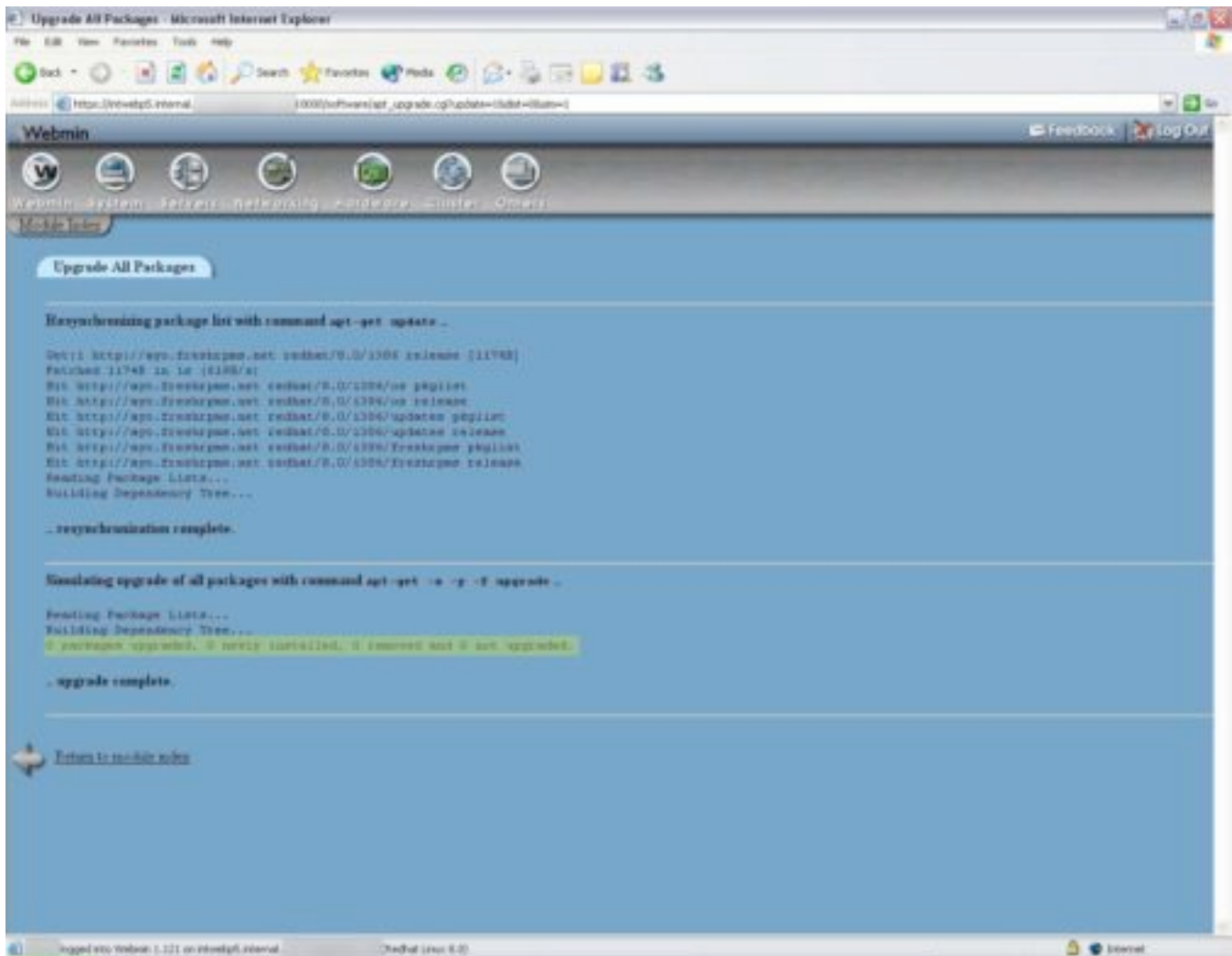
#### **Upgrade All Packages**

Resynchronize package list (update) – Yes

Perform distribution upgrade (upgrade-dist) – No

Only show which packages would be upgraded – Yes





**Result:** No unapplied security (or other) patches or updates were found for the IPCMS Portal and Content Management Server.

**Pass/Fail:** **Pass**

## Step D6b

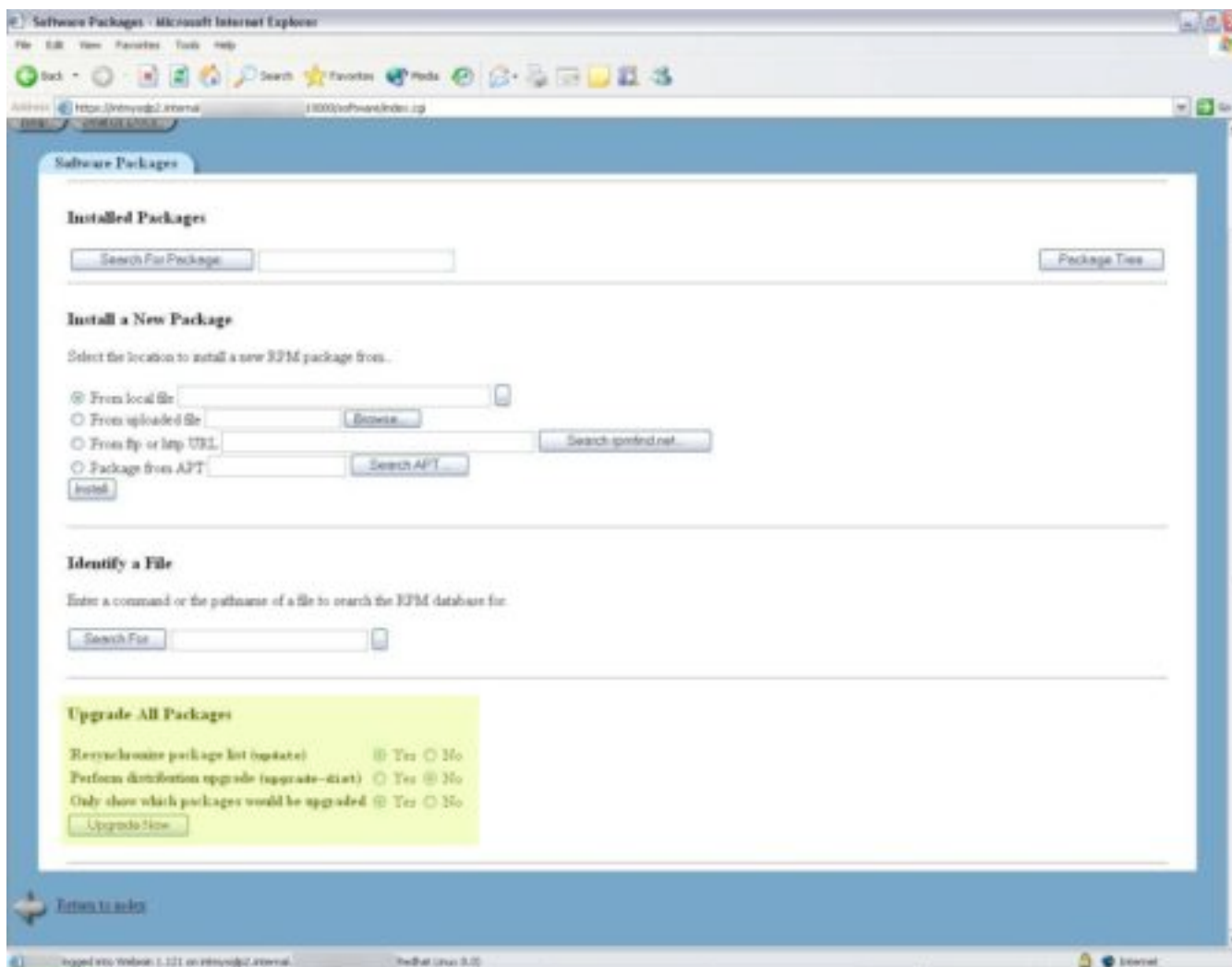
The Webmin *Software Patches* module was used to check the IPCMS Database Server for security (and other) patches using the following options:

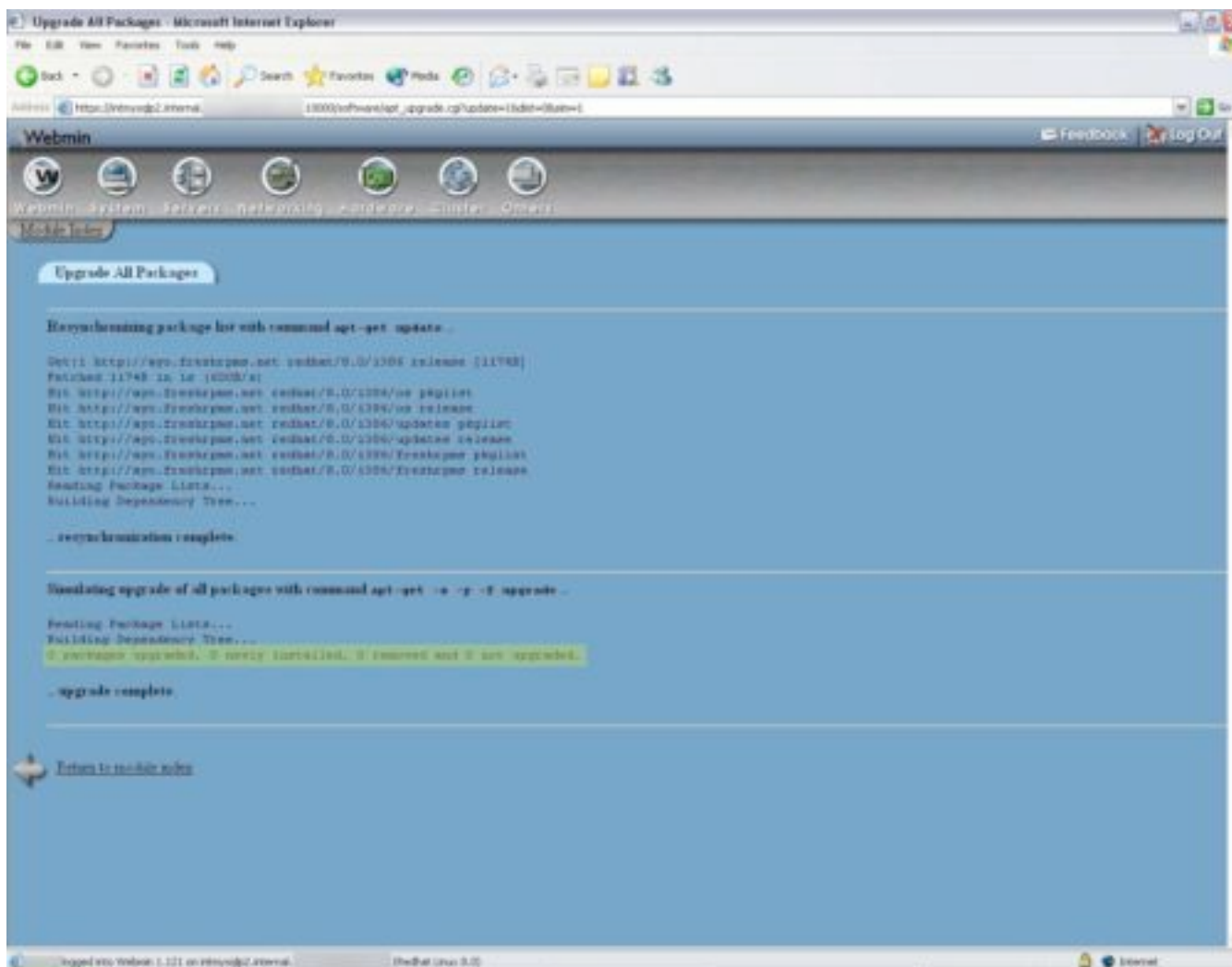
### Upgrade All Packages

Resynchronize package list (update) – Yes

Perform distribution upgrade (upgrade-dist) – No

Only show which packages would be upgraded – Yes





**Result:** No unapplied security (or other) patches or updates were found for the IPCMS Database Server.

**Pass/Fail:** Pass

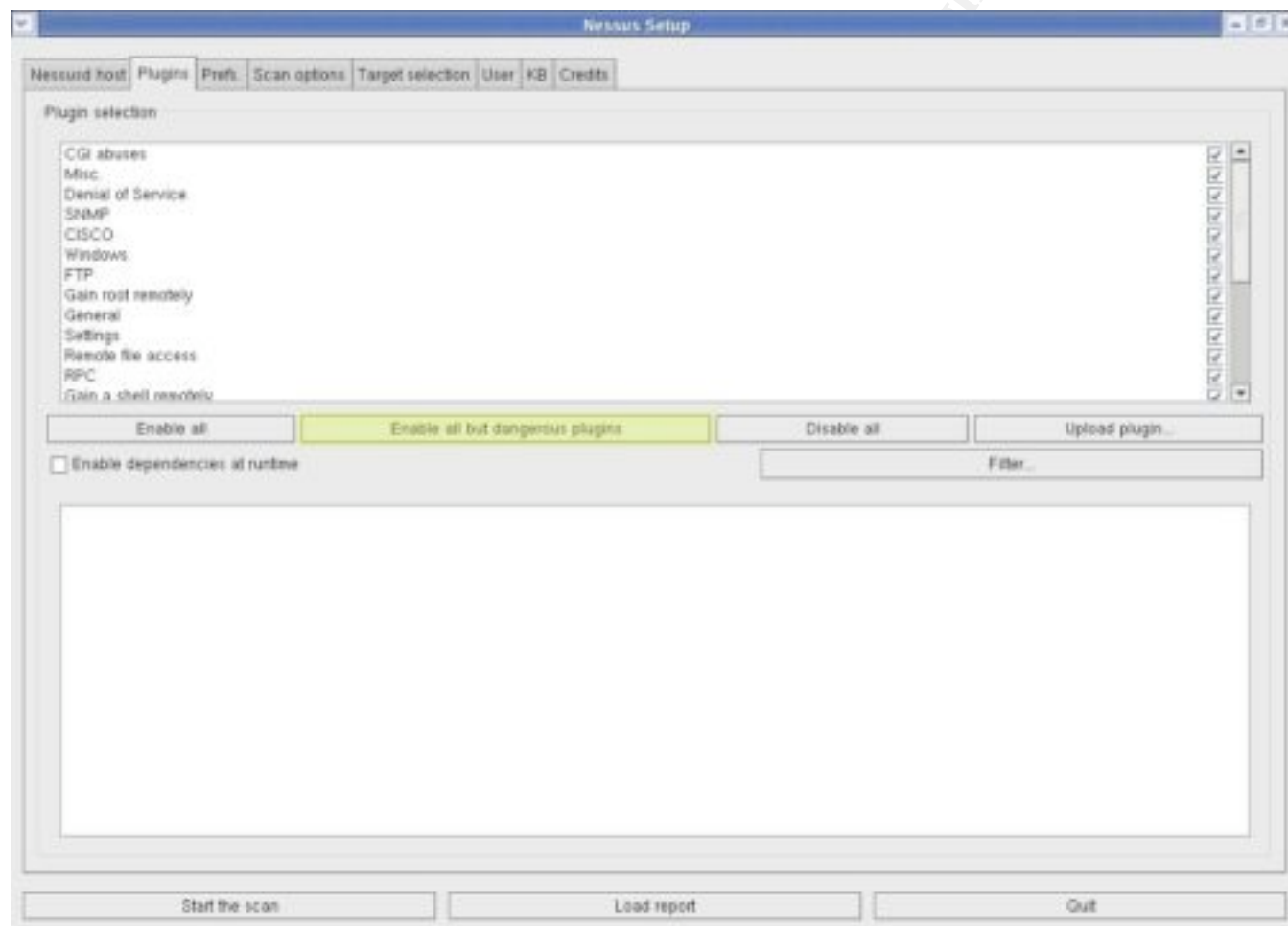


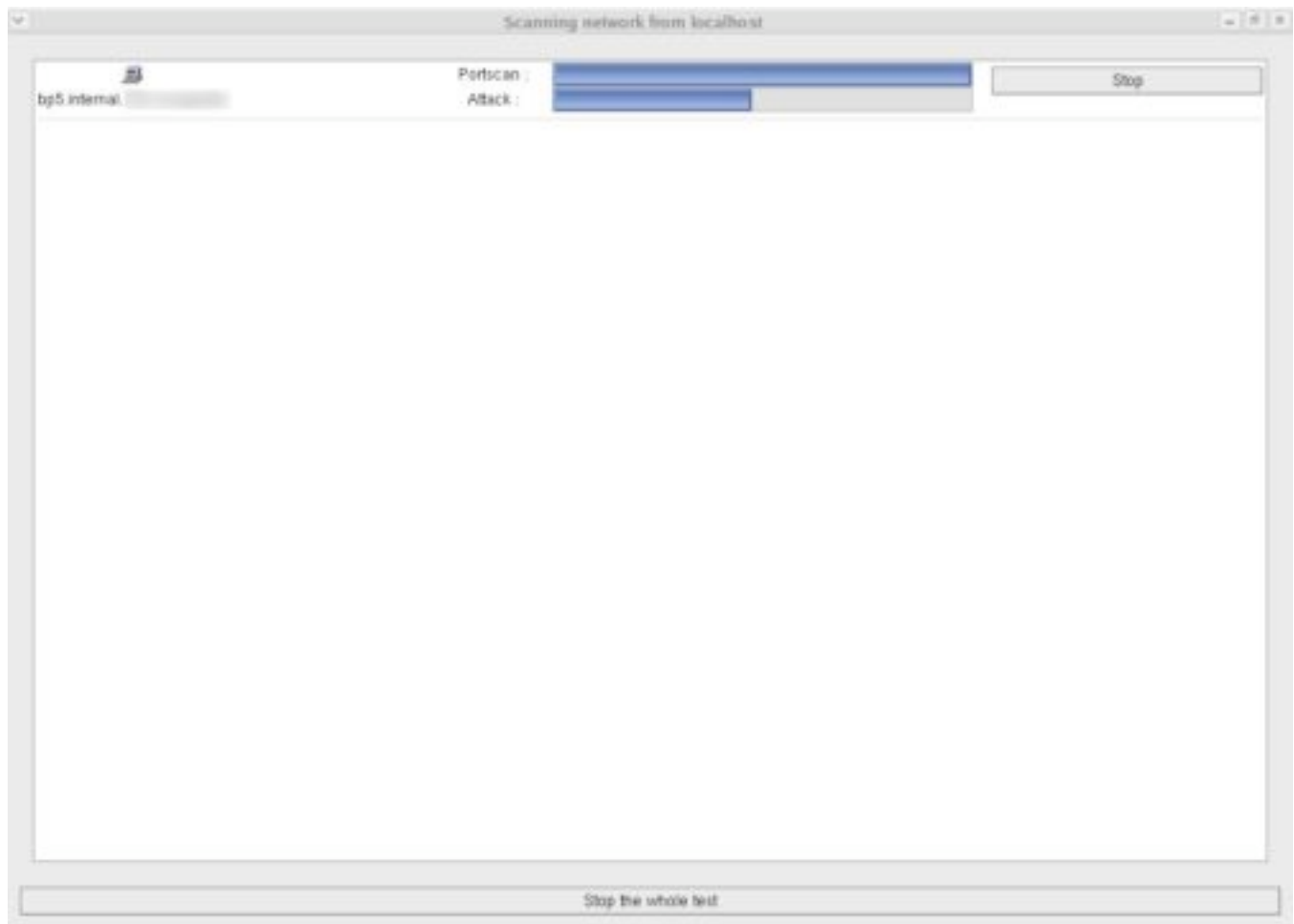
## **Step D7**

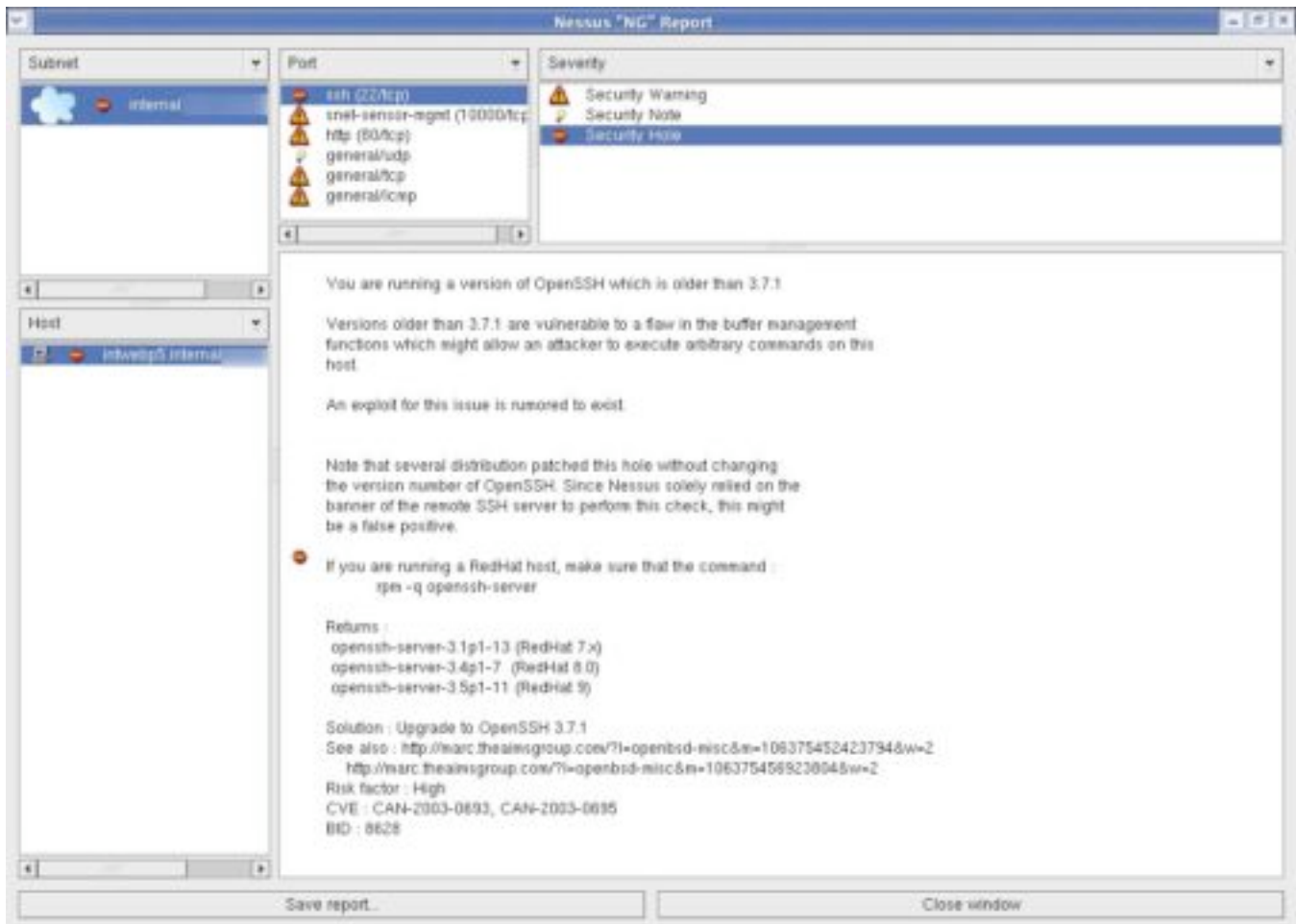
The control objective of this step is to ensure that there are no known high, serious or medium security risks on the IPCMS servers.

### **Step D7a**

Nessus 2.0.9 ([www.nessus.org](http://www.nessus.org)) was used to scan the IPCMS Portal and Content Management Server for vulnerabilities using the “Enable all but dangerous plugins” option.







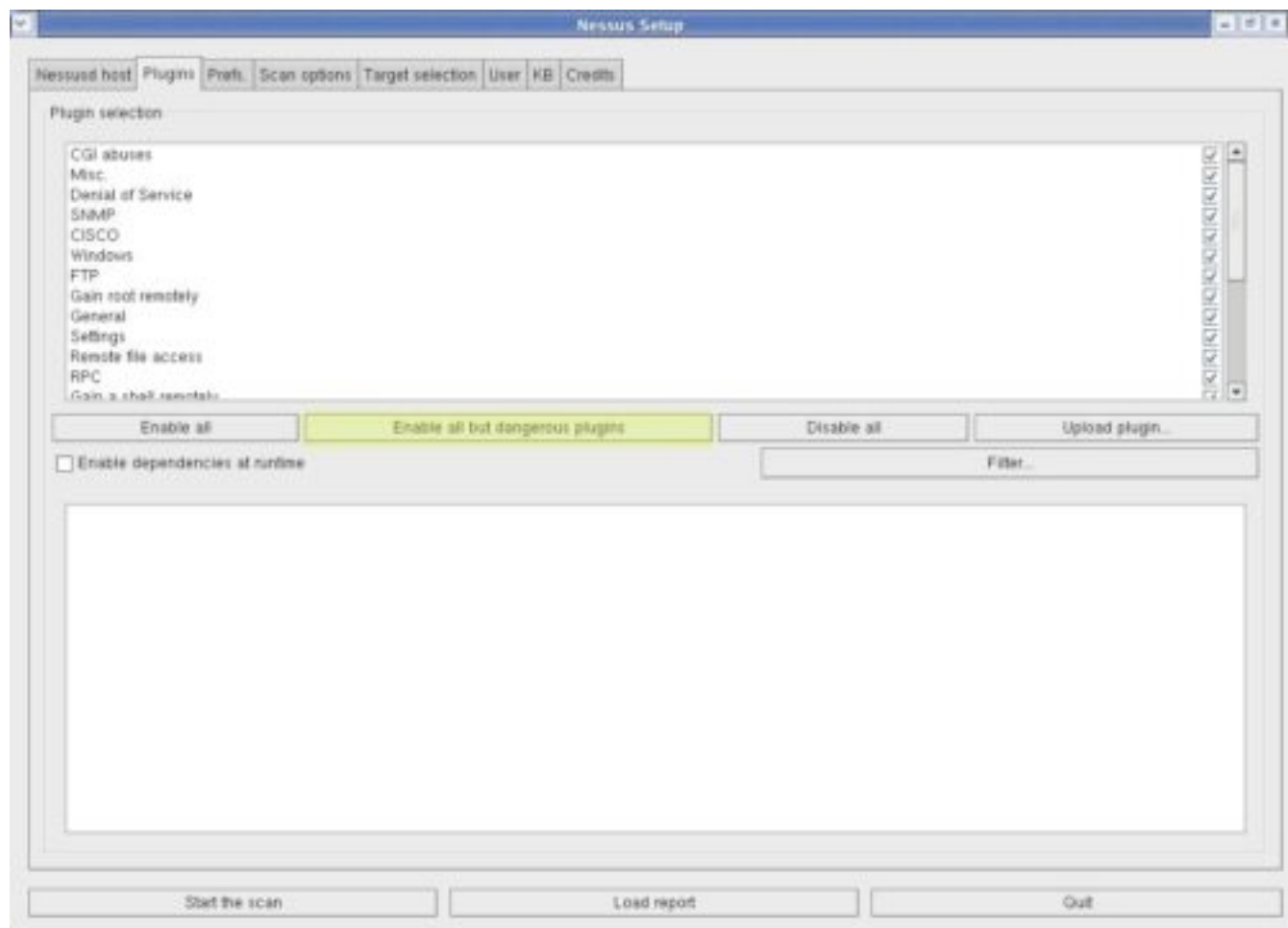
**Result:** Nessus returned the following security risk results for the IPCMS Portal and Content Management Server (see appendix 2 for complete Nessus results):

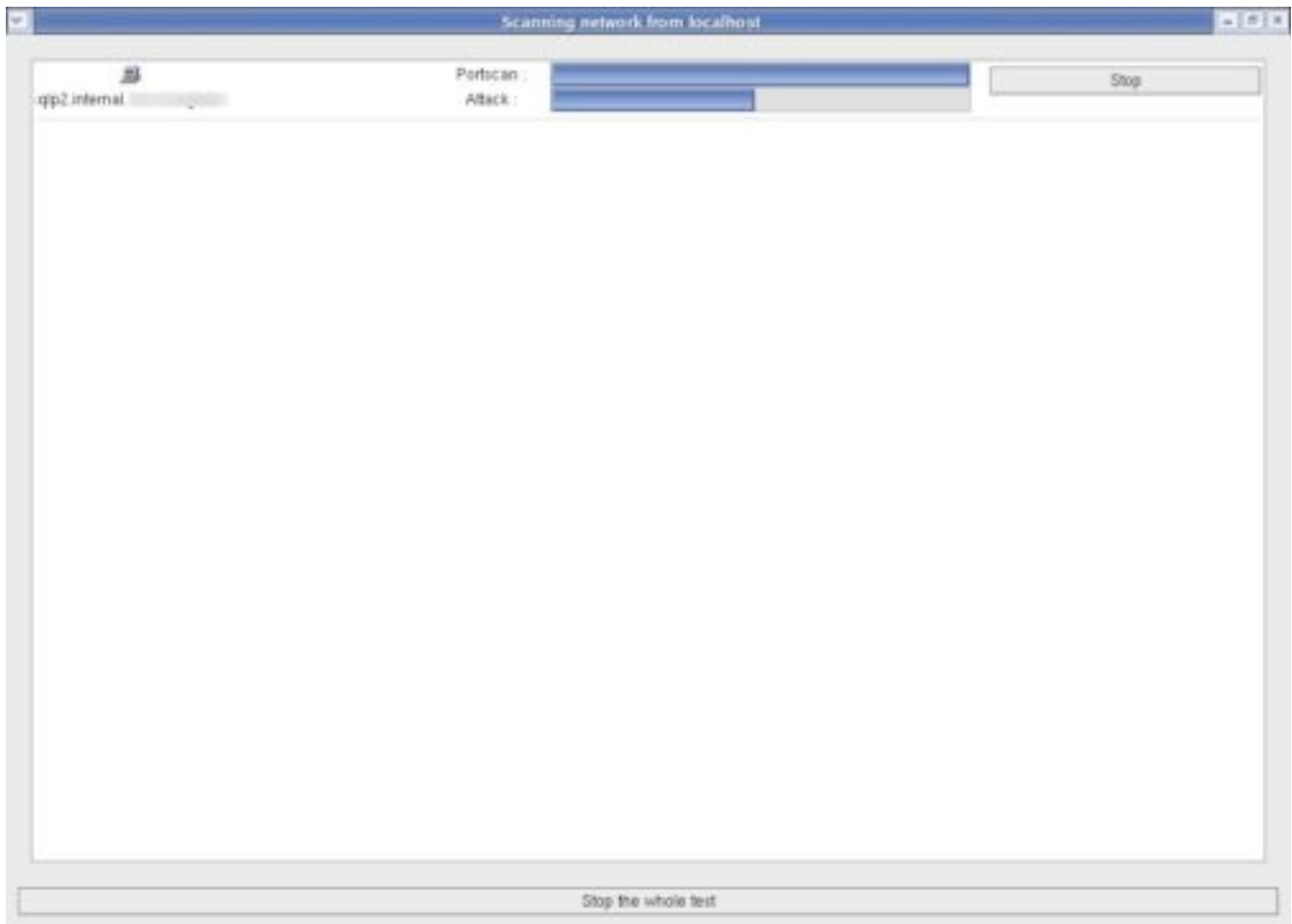
**High:** 1  
**Serious:** 0  
**Medium:** 7  
**Low:** 5

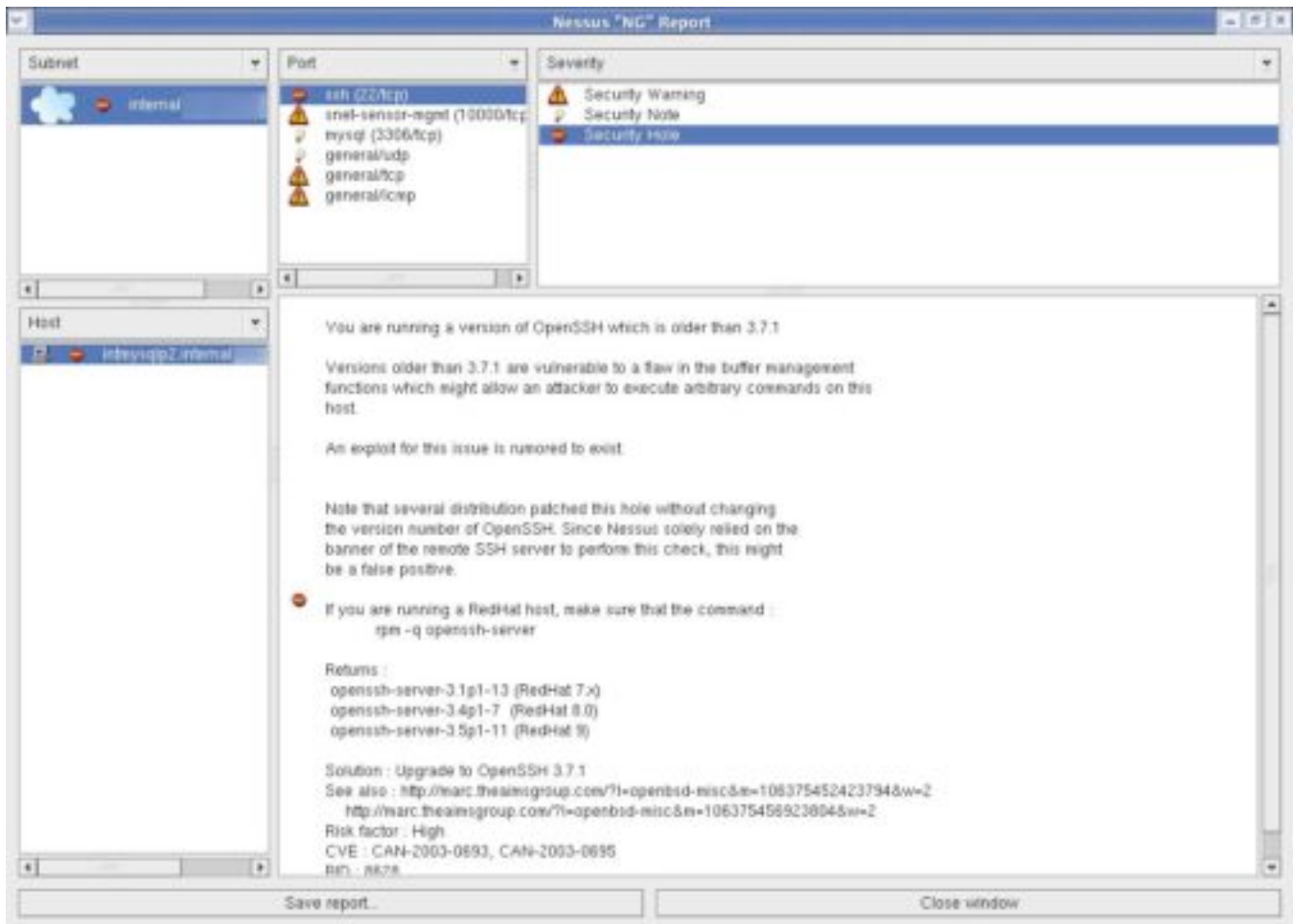
**Pass/Fail:** **Fail**

## Step D7b

Nessus 2.0.9 ([www.nessus.org](http://www.nessus.org)) was used to scan the IPCMS Database Server for vulnerabilities using the “Enable all but dangerous plugins” option.







**Result:** Nessus returned the following security risk results for the IPCMS Database Server (see appendix 2 for complete Nessus results):

High: 1  
 Serious: 0  
 Medium: 1  
 Low: 3

**Pass/Fail: Fail**

## Step D9

The control objective of this step is to ensure that the IPCMS Server's Root and administrator account settings comply with the company's Password Protection Policy.

### **Step D9(1)a**

The IPCMS Portal and Content Management Server's /etc/login.defs file was inspected for the following entries:

```
PASS_MAX_DAYS    60
PASS_MIN_LEN     8
```

```
# *REQUIRED*
#   Directory where mailboxes reside, _or_ name of file, relative to the
#   home directory.  If you _do_ define both, MAIL_DIR takes precedence.
#   QMAIL_DIR is for Qmail
#
#QMAIL_DIR      Maildir
MAIL_DIR        /var/spool/mail
#MAIL_FILE      .mail

# Password aging controls:
#
#   PASS_MAX_DAYS   Maximum number of days a password may be used.
#   PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#   PASS_MIN_LEN    Minimum acceptable password length.
#   PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   60
PASS_MIN_DAYS   0
PASS_MIN_LEN    8
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
/etc/passwd
```

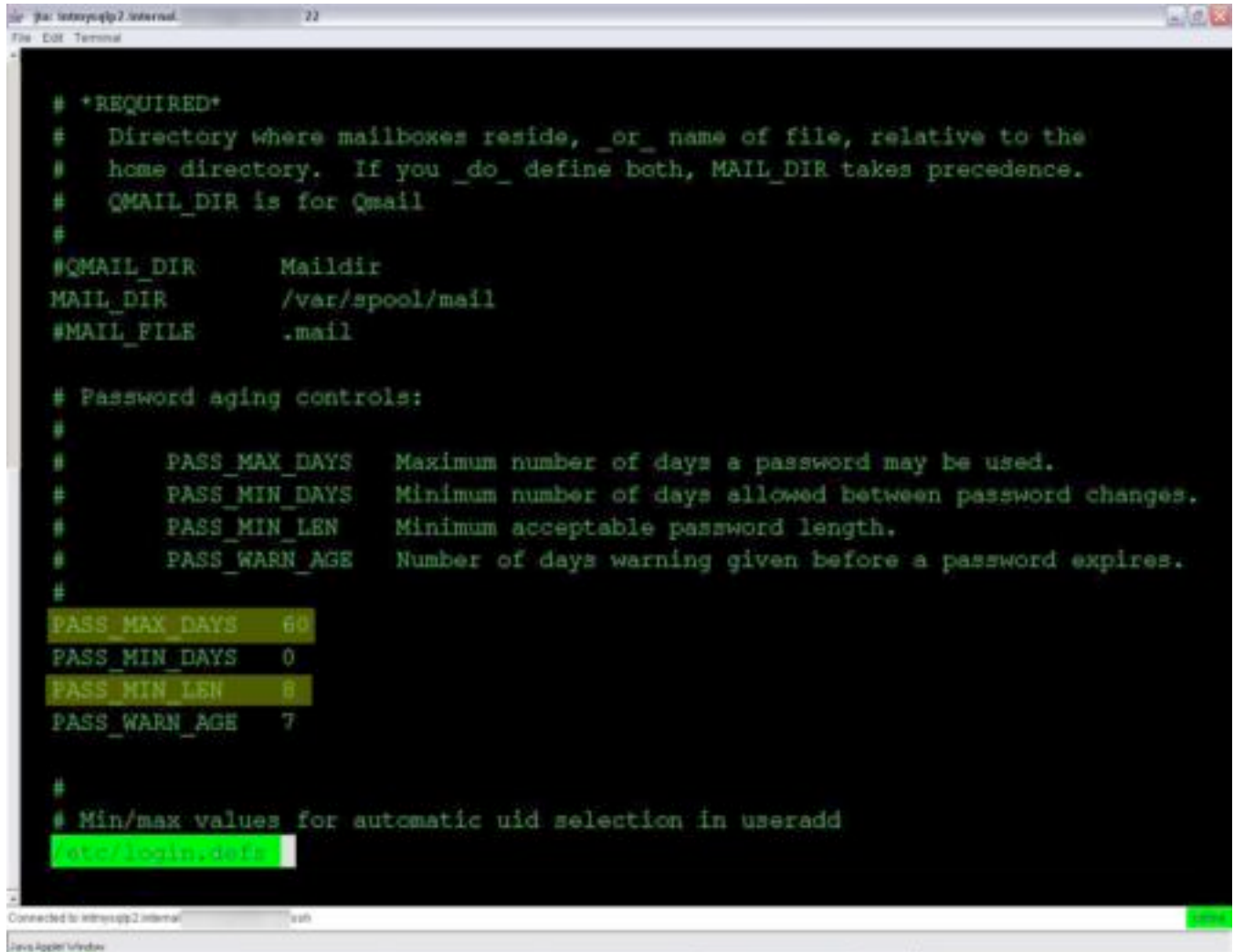
**Result:** The IPCMS Portal and Content Management Server's root and administrator account settings were found to be compliant with the company's Password Protection Policy.

**Pass/Fail:** **Pass**

**Step D9(1)b**

The IPCMS Database Server's /etc/login.defs file was inspected for the following entries:

```
PASS_MAX_DAYS    60
PASS_MIN_LEN     8
```



```
# *REQUIRED*
# Directory where mailboxes reside, _or_ name of file, relative to the
# home directory.  If you _do_ define both, MAIL_DIR takes precedence.
# QMAIL_DIR is for Qmail
#
#QMAIL_DIR      Maildir
MAIL_DIR        /var/spool/mail
#MAIL_FILE      .mail

# Password aging controls:
#
#      PASS_MAX_DAYS   Maximum number of days a password may be used.
#      PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#      PASS_MIN_LEN    Minimum acceptable password length.
#      PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   60
PASS_MIN_DAYS   0
PASS_MIN_LEN    8
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
/etc/login.defs
```

**Result:** The IPCMS Database Server's root and administrator account settings were found to be compliant with the company's Password Protection Policy.

**Pass/Fail:** **Pass**



## Step D9(2)a

An attempt was made to change the password of both the IPCMS Portal and Content Management Server's root account and a test administrator account to a non-compliant length (3 characters):

```
Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.20-20.8 on an i686

intwebp5 login: root
Password:
Last login: Sun Nov 16 10:58:24 on tty1
You have new mail.
[root@intwebp5 root]# passwd
Changing password for user root.
New password:
BAD PASSWORD: it's WAY too short
Retype new password: _
```

```
Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.20-20.8 on an i686

intwebp5 login: audit
Password:
Last login: Sun Nov 16 10:23:53 from 192.168.1.100
-ssh-2.05b$ bash
[audit@intwebp5 audit]$ passwd
Changing password for user audit.
Changing password for audit
(current) UNIX password:
New password:
BAD PASSWORD: it's WAY too short
New password: _
```

**Result:** The passwords for the IPCMS Portal and Content Management Server's root account and test administrator account could not be changed to a non compliant length.

Pass/Fail: **Pass**

### Step D9(2)b

An attempt was made to change the password of both the IPCMS Database Server's root account and a test administrator account to a non-compliant length (3 characters):

```
Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.20-20.8 on an i686

intmysqlp2 login: root
Password:
Last login: Sun Nov 16 12:46:34 on tty1
[root@intmysqlp2 root]# passwd
Changing password for user root.
New password:
BAD PASSWORD: it's WAY too short
Retype new password: _
```

```
Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.20-20.8 on an i686

intmysqlp2 login: audit
Password:
Last login: Sat Nov 15 22:15:50 from [REDACTED]
-sh-2.05b$ bash
[audit@intmysqlp2 audit]$ passwd
Changing password for user audit.
Changing password for audit
(current) UNIX password:
New password:
BAD PASSWORD: it's WAY too short
New password: _
```

**Result:** The passwords for the IPCMS Database Server's root account and test administrator account could not be changed to a non compliant length.

**Pass/Fail:** **Pass**

© SANS Institute 2003, Author retains full rights.

## **Step E1**

The control objective of this step is to ensure that Webmin is configured to use SSL encryption.

### **Step E1(1)a**

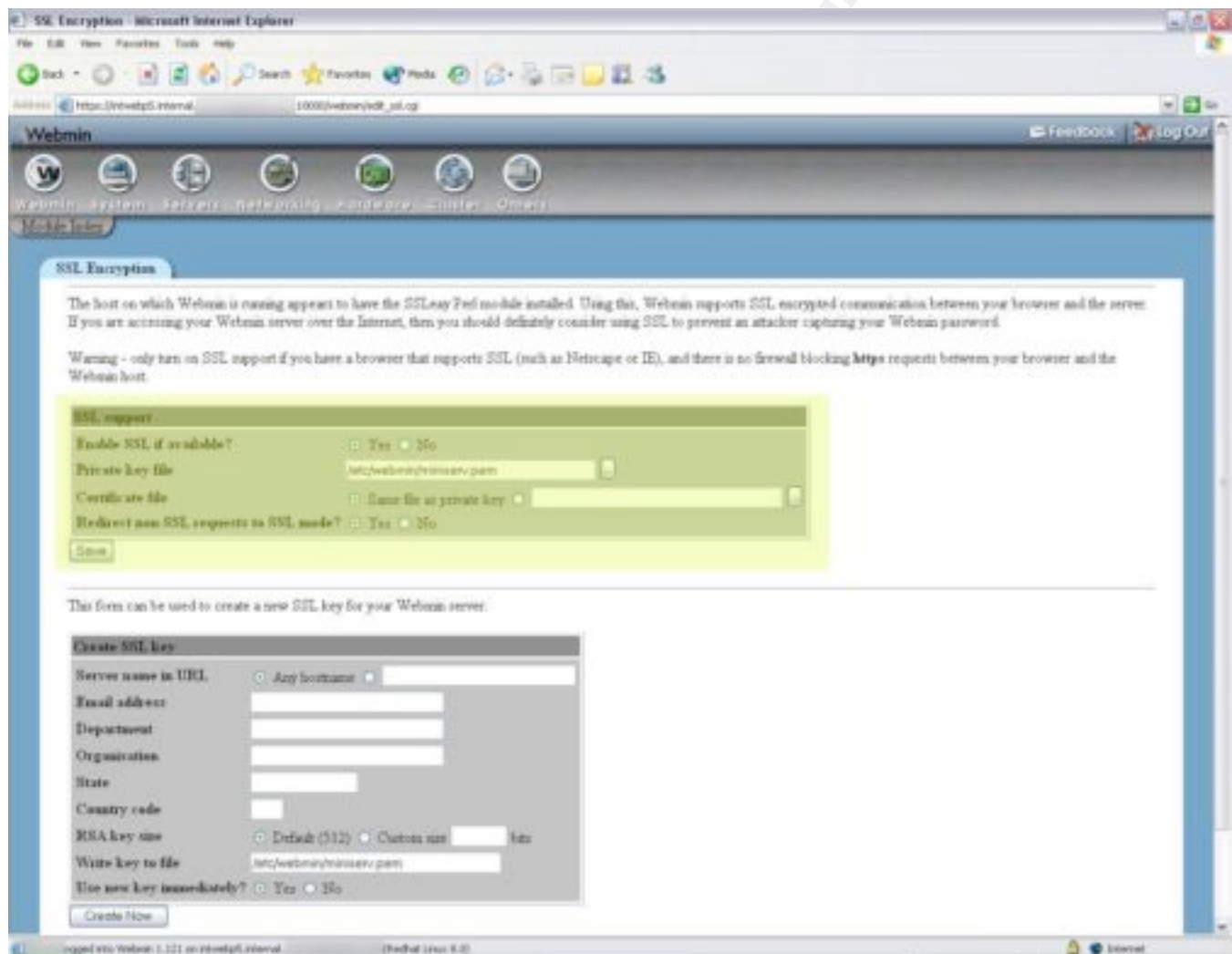
The IPCMS Portal and Content Management Server's *Webmin configuration/SSL Encryption* module was checked for the following settings:

Enable SSL if available – Yes

Private key file: /etc/webmin/miniserv.pem

Certificate file: Same file as private key

Redirect non-SSL requests to SSL mode – Yes



**Result:** The IPCMS Portal and Content Management Server's *Webmin configuration/SSL Encryption* module's settings were found to comply with the audit requirements.

**Pass/Fail:** **Pass**

## Step E1(1)b

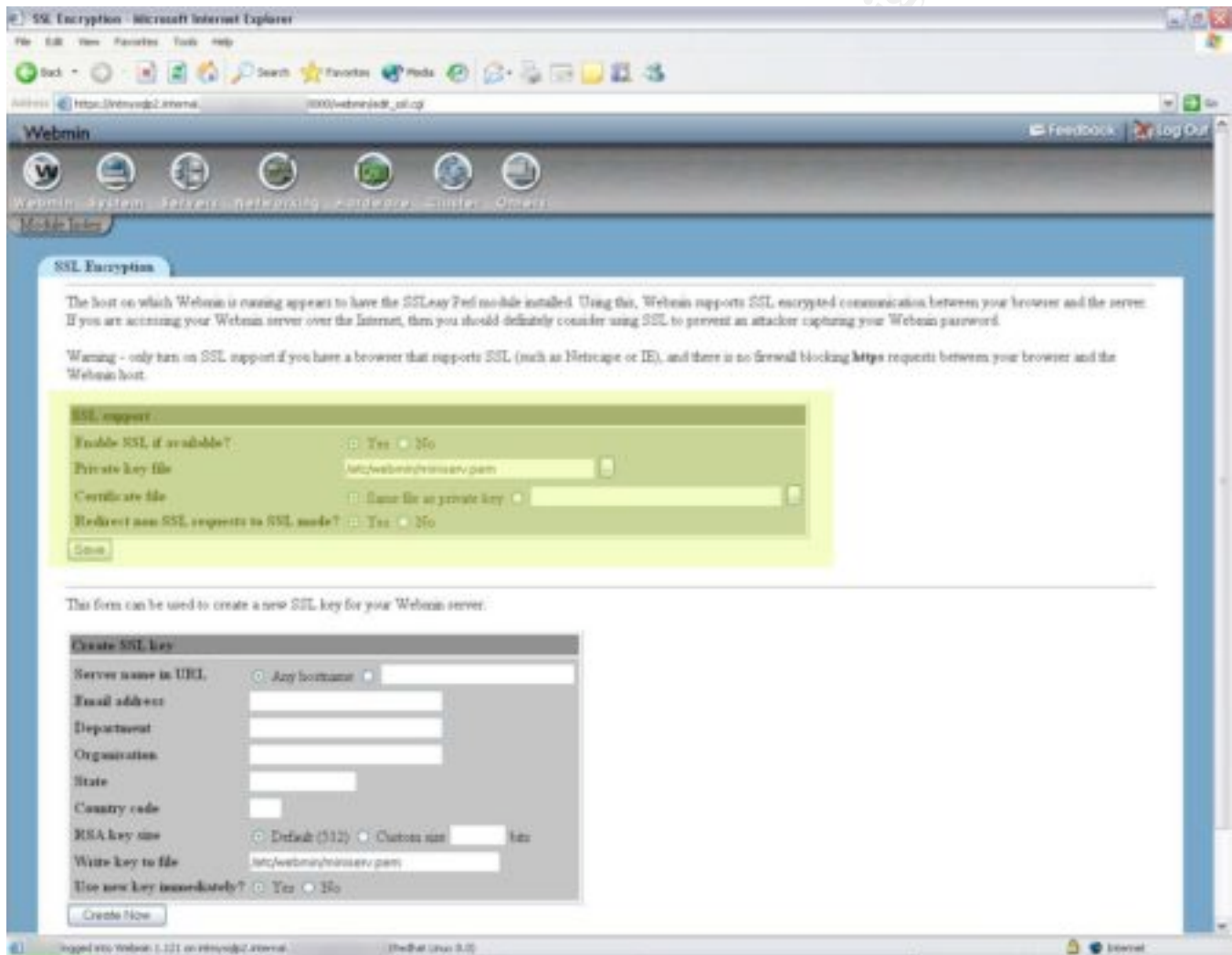
The IPCMS Database Server's *Webmin configuration/SSL Encryption* module was checked for the following settings:

Enable SSL if available – Yes

Private key file: /etc/webmin/miniserv.pem

Certificate file: Same file as private key

Redirect non-SSL requests to SSL mode – Yes

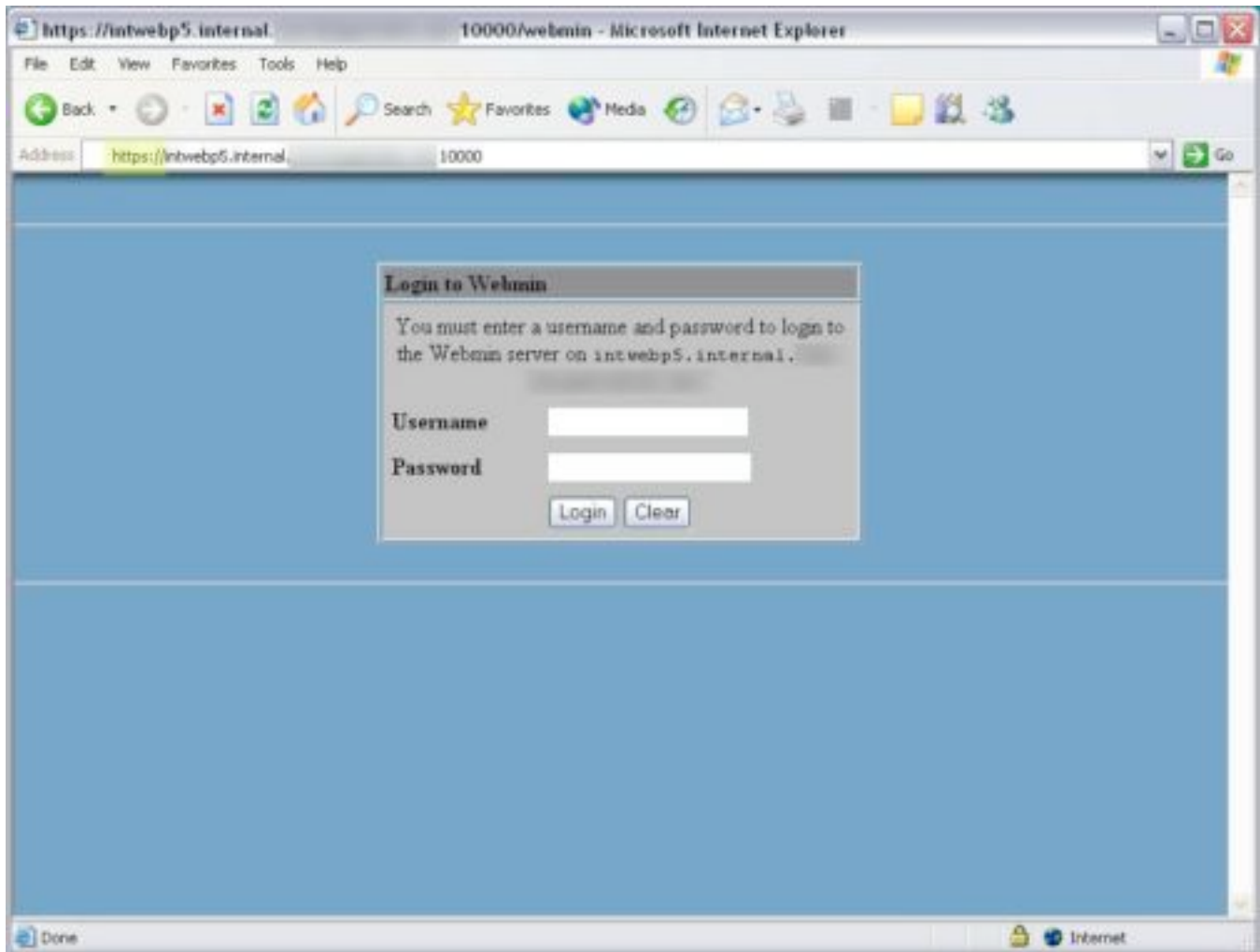


**Result:** The IPCMS Database Server's *Webmin configuration/SSL Encryption* module's settings were found to comply with the audit requirements.

**Result:** **Pass**

## Step E1(2)a

A connection was made to Webmin on the IPCMS Portal and Content Management Server from a Web browser. The URL in the navigation toolbar was inspected to verify that it displayed **https://hostname:10000**.



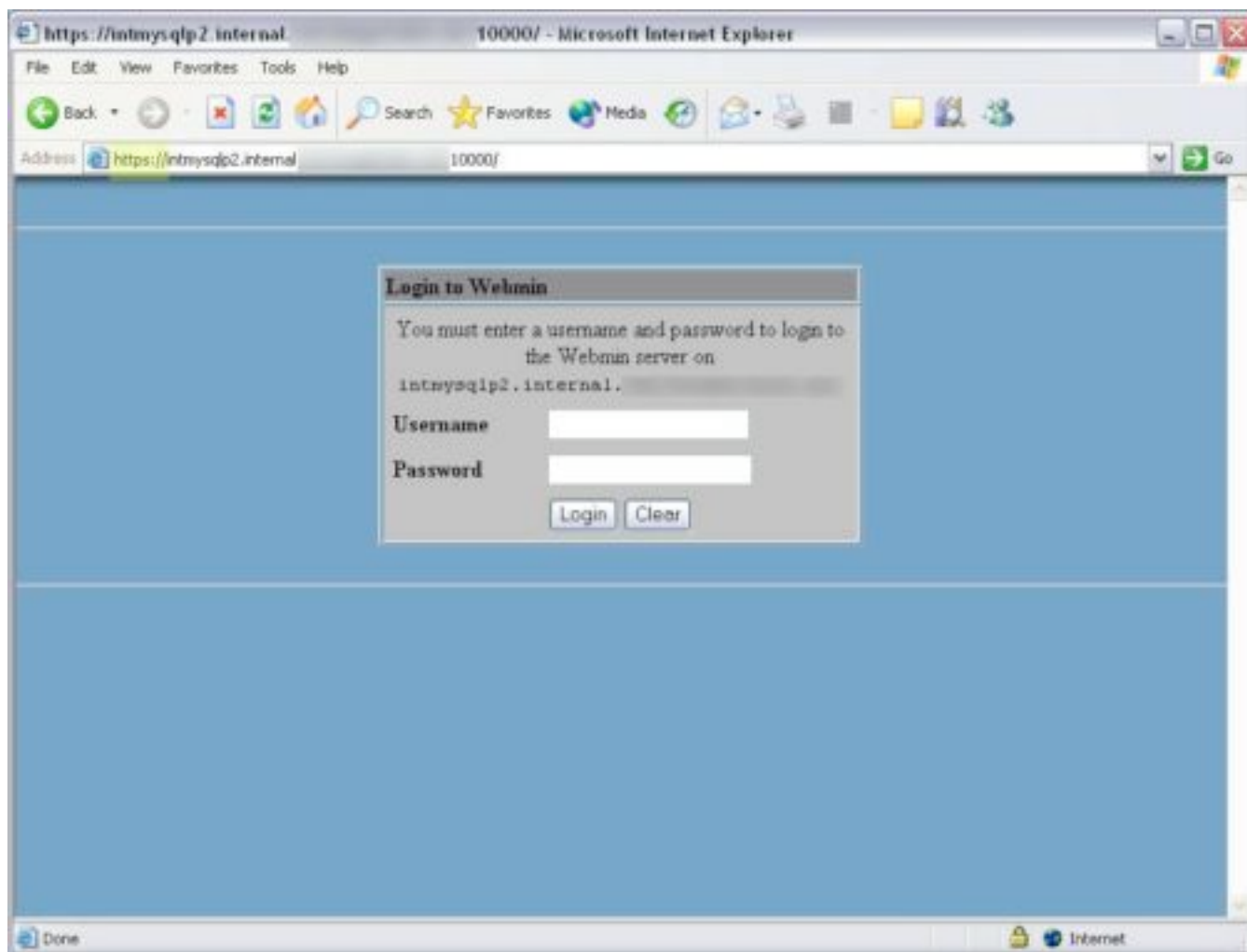
**Result:** The browser displayed **https://hostname:10000** indicating a secure SSL connection to the IPCMS Portal and Content Management Server.

**Pass/Fail:** Pass



## Step E1(2)b

A connection was made to Webmin on the IPCMS Database Server from a Web browser. The URL in the navigation toolbar was inspected to verify that it displayed **https://hostname:10000**.

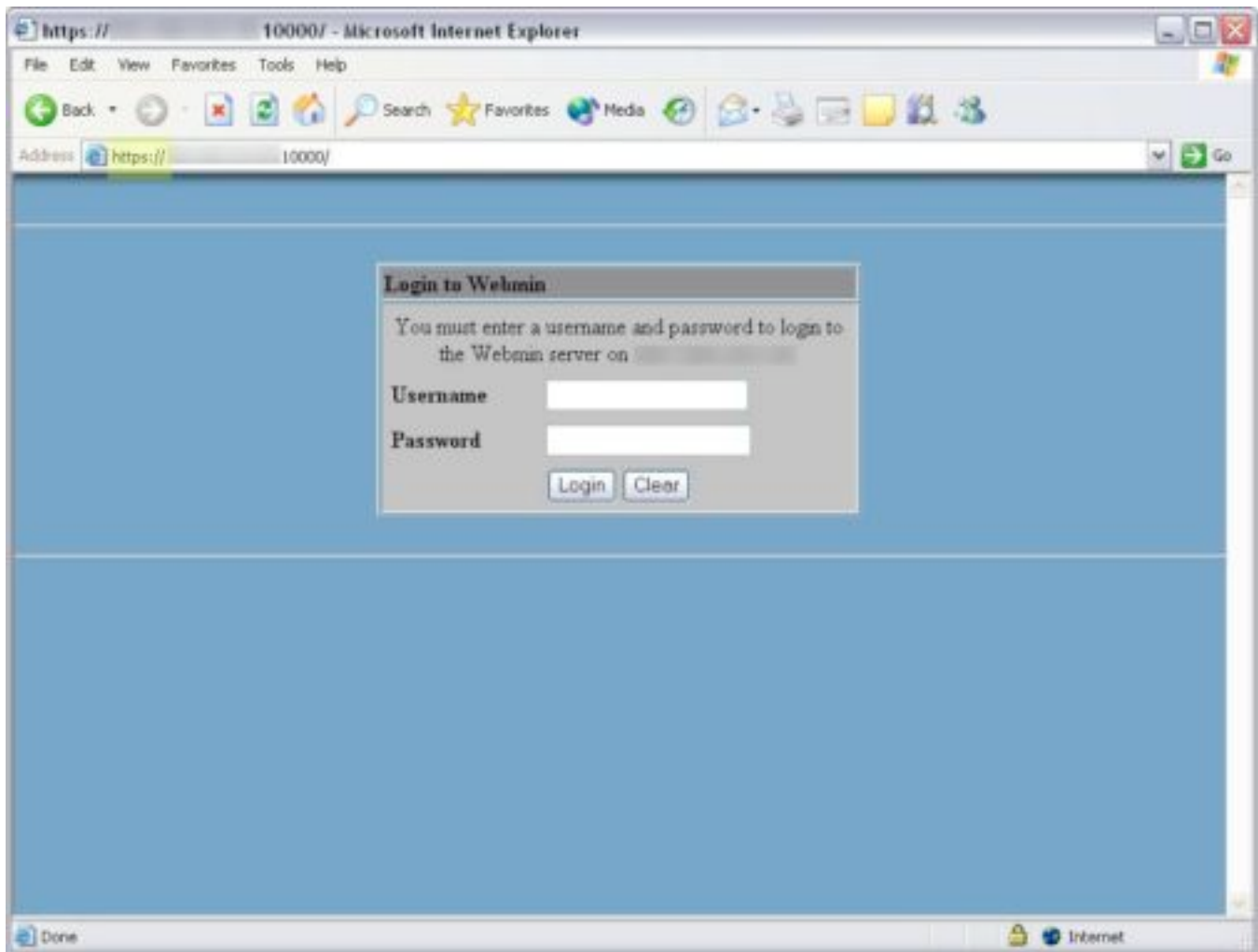


**Result:** The browser displayed **https://hostname:10000** indicating a secure SSL connection to the IPCMS Database Server.

**Pass/Fail:** **Pass**

## Step E1(3)a

An attempt was made to connect to Webmin on the IPCMS Portal and Content Management Server using a non SSL connection (***http://hostname:10000***).



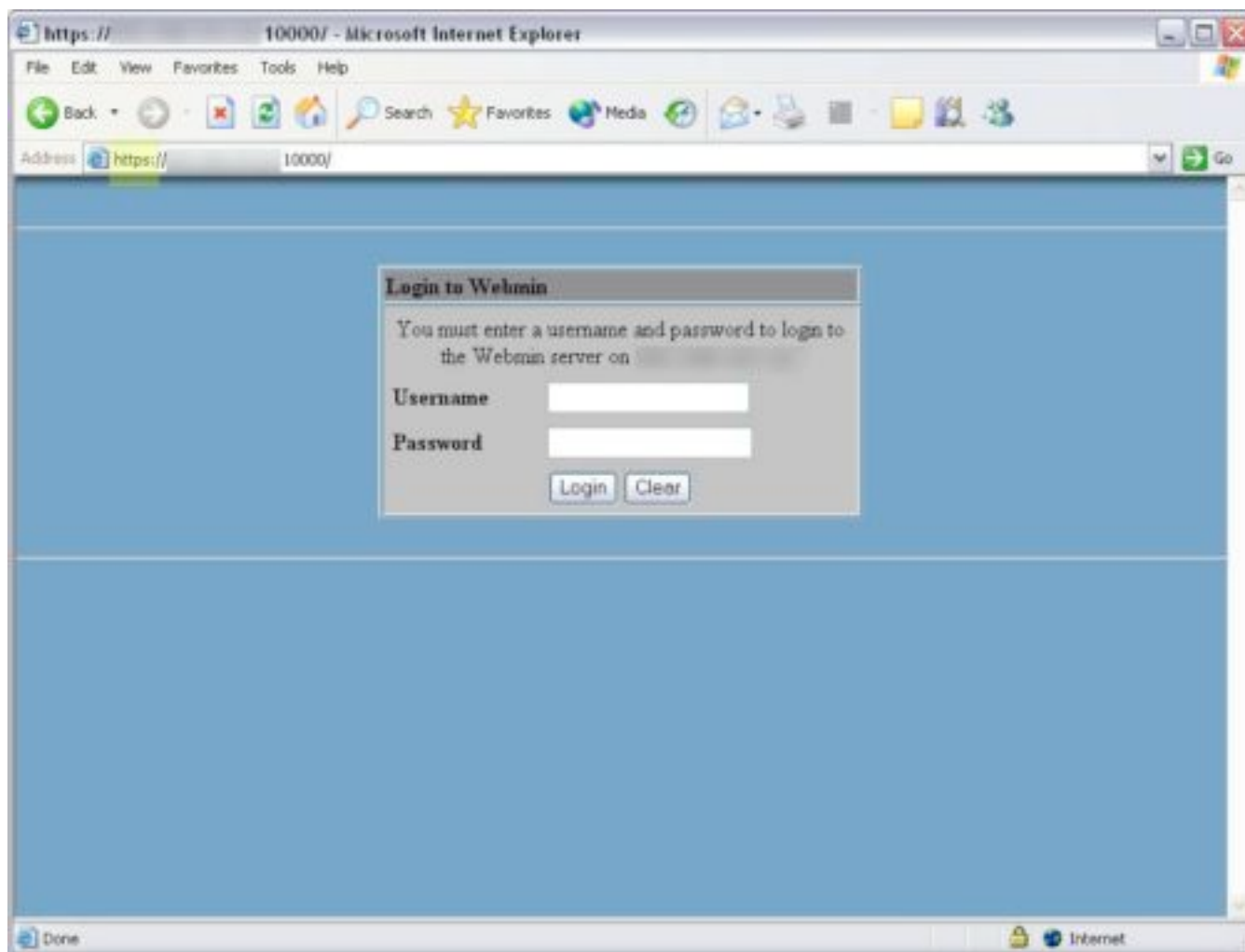
**Result:** Webmin redirected the non secure connection to a secure one (***https://server IP:10000***).

**Pass/Fail:** Pass



## Step E1(3)b

An attempt was made to connect to Webmin on the IPCMS Database Server using a non SSL connection (***http://hostname:10000***).



**Result:** Webmin redirected the non secure connection to a secure one (***https://server IP:10000***).

**Pass/Fail:** Pass

## **Step E5**

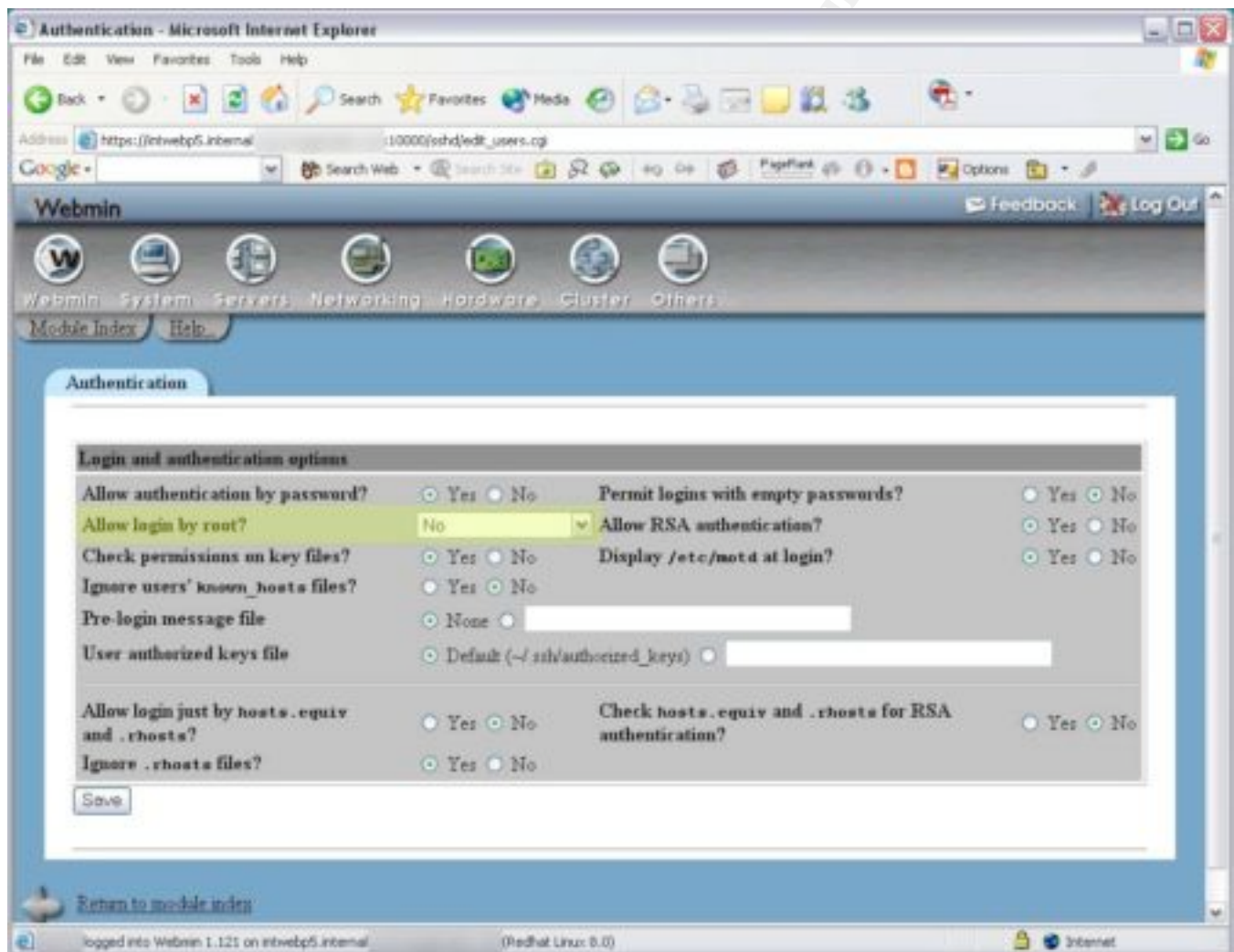
The control objective of this step is to ensure that the SSH server is configured to deny remote login by the Root account.

### **Step E5(1)a**

The IPCMS Portal and Content Management Server's Webmin *SSH Server/Authentication* Module was checked for the following settings:

#### **Login and authentication options**

Allow login by root? – No



**Result:** The IPCMS Portal and Content Management Server's SSH server settings were found to comply with the audit requirements.

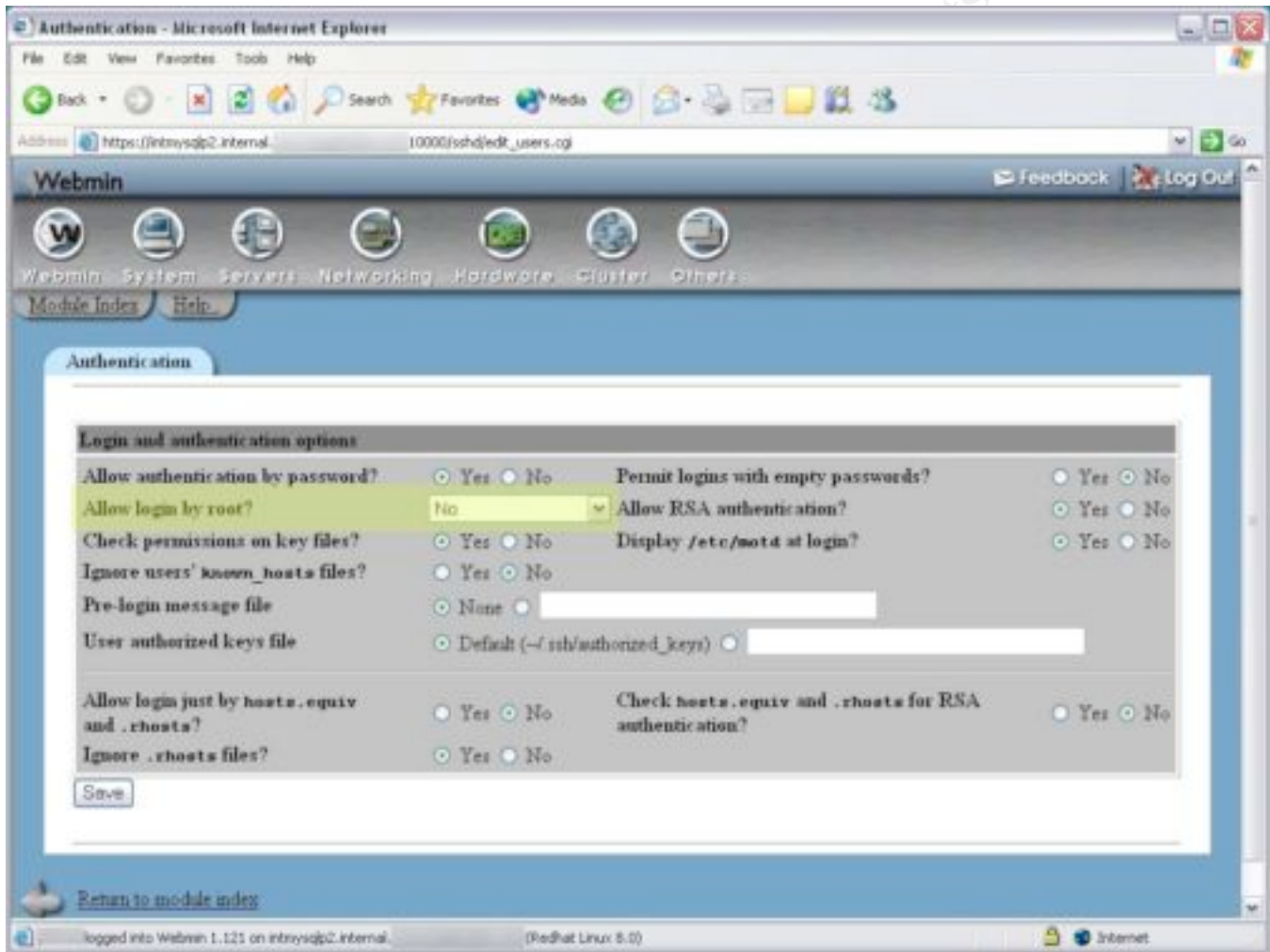
**Pass/Fail:** Pass

## Step E5(1)b

The IPCMS Database Server's Webmin *SSH Server/Authentication* Module was checked for the following settings:

### Login and authentication options

Allow login by root? – No

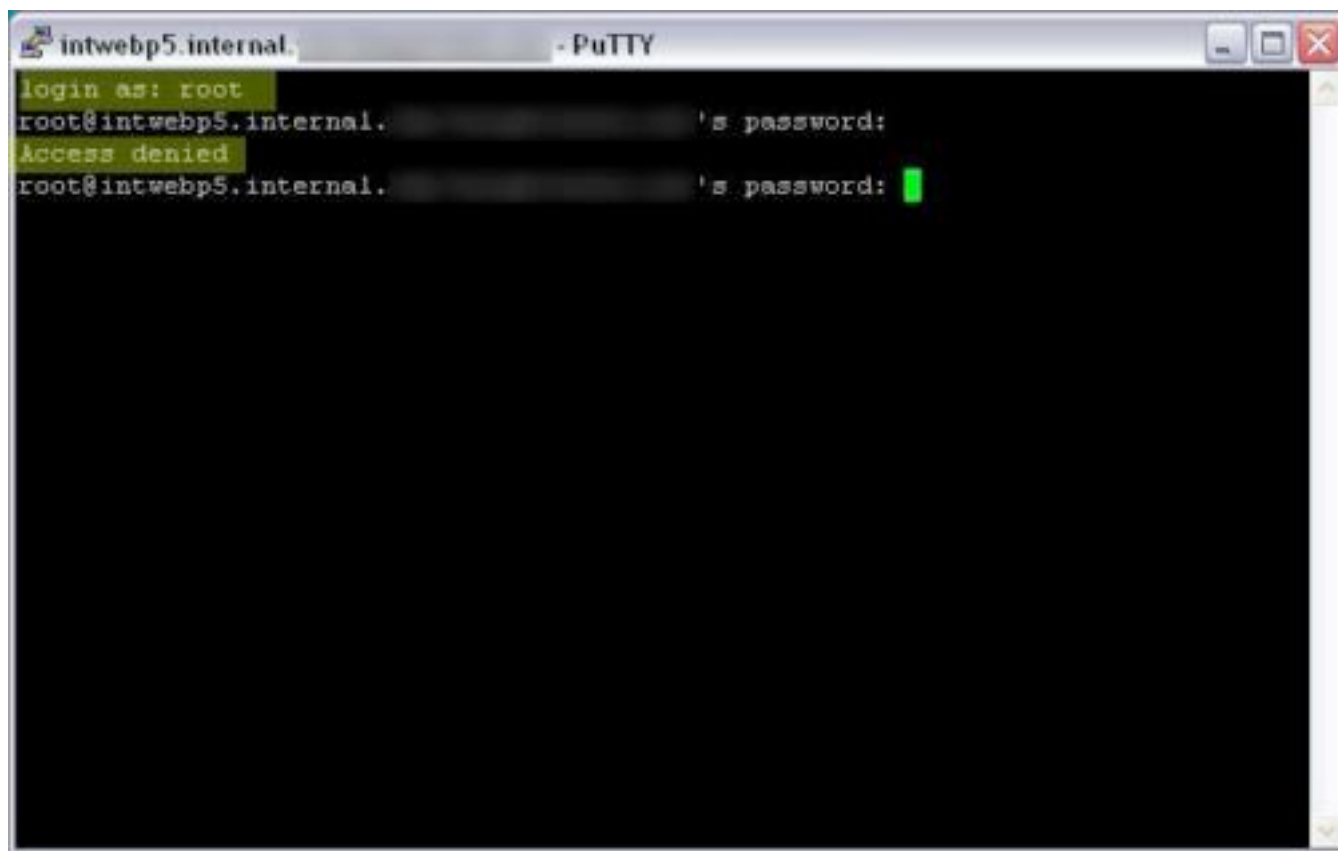


**Result:** The IPCMS Database Server's SSH server settings were found to comply with the audit requirements.

**Pass/Fail:** Pass

### Step E5(2)a

An SSH connection to the IPCMS Portal and Content Management Server using the Root account was attempted from a workstation on the company's network.



```
intwebp5.internal. - PuTTY
login as: root
root@intwebp5.internal.'s password:
Access denied
root@intwebp5.internal.'s password: █
```

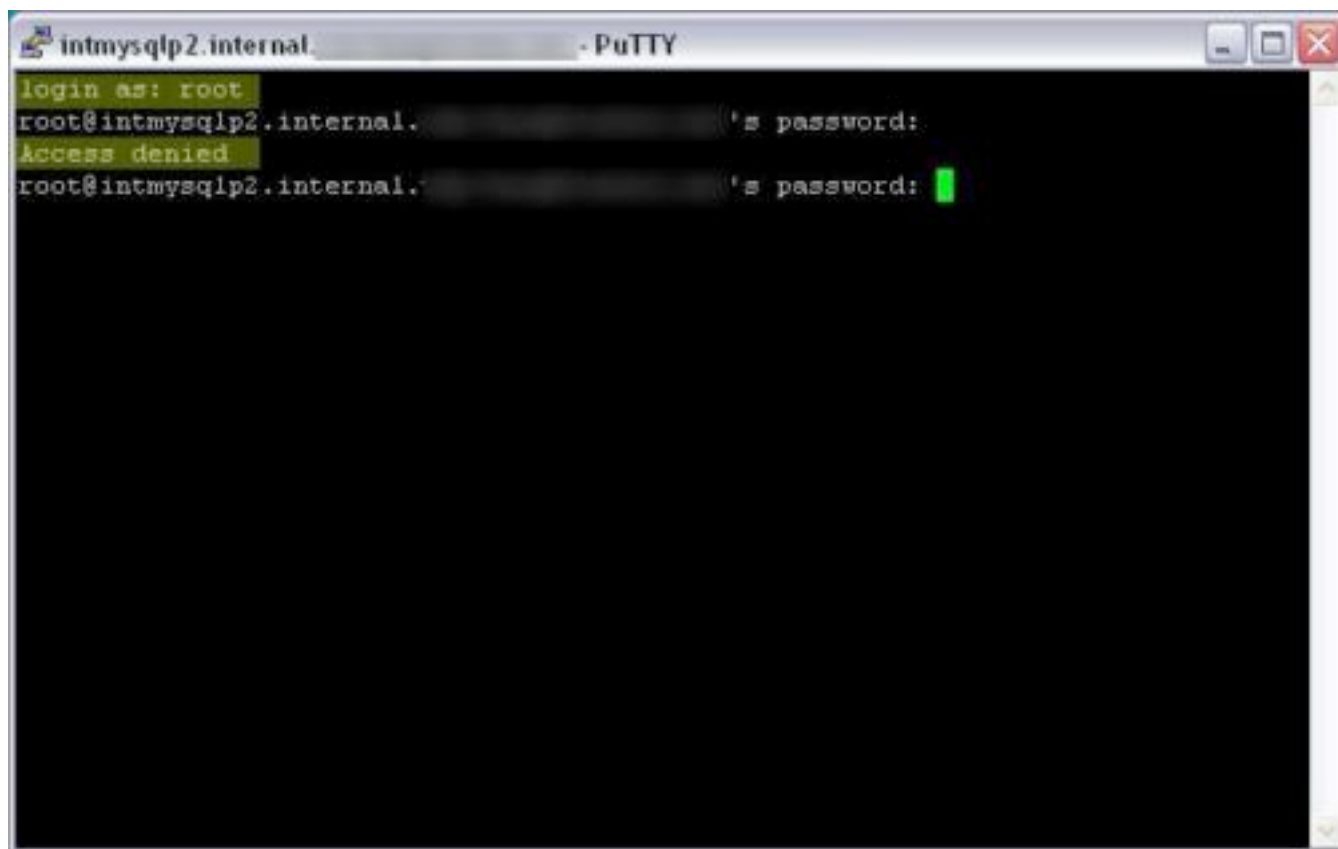
**Result:** The attempt to log into the SSH server as Root from a workstation on the company's network was denied.

**Pass/Fail:** Pass

© SANS Institute

## Step E5(2)b

An SSH connection to the IPCMS Database Server using the Root account was attempted from a workstation on the company's network.



```
intmysqlp2.internal - PuTTY
login as: root
root@intmysqlp2.internal.'s password:
Access denied
root@intmysqlp2.internal.'s password: █
```

**Result:** The attempt to log into the SSH server as Root from a workstation on the company's network was denied.

**Pass/Fail:** Pass

© SANS Institute

## **Step F1**

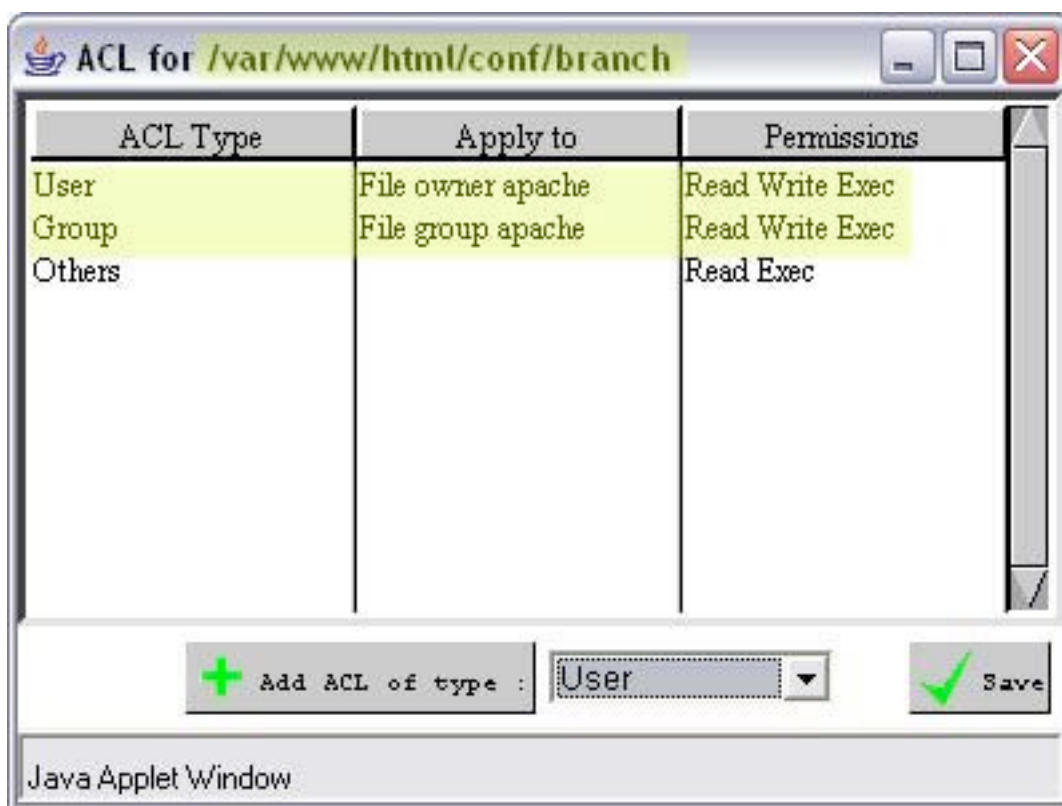
The control objective of this step is to ensure that all phpWebSite post-installation security configuration changes and removal of setup code was performed per the documentation.

### ***Step F1(1)***

The phpWebSite root directory (/var/www/html/) on the IPCMS Portal and Content Management Server was checked for the following settings:

*/conf/ - phpwebsite (user)*  
*/conf/ - phpwebsite (group)*  
*/conf/branch/ - apache (user)*  
*/conf/branch/ - apache (group)*





**Result:** The directory ownership settings were found to comply with the audit requirements.

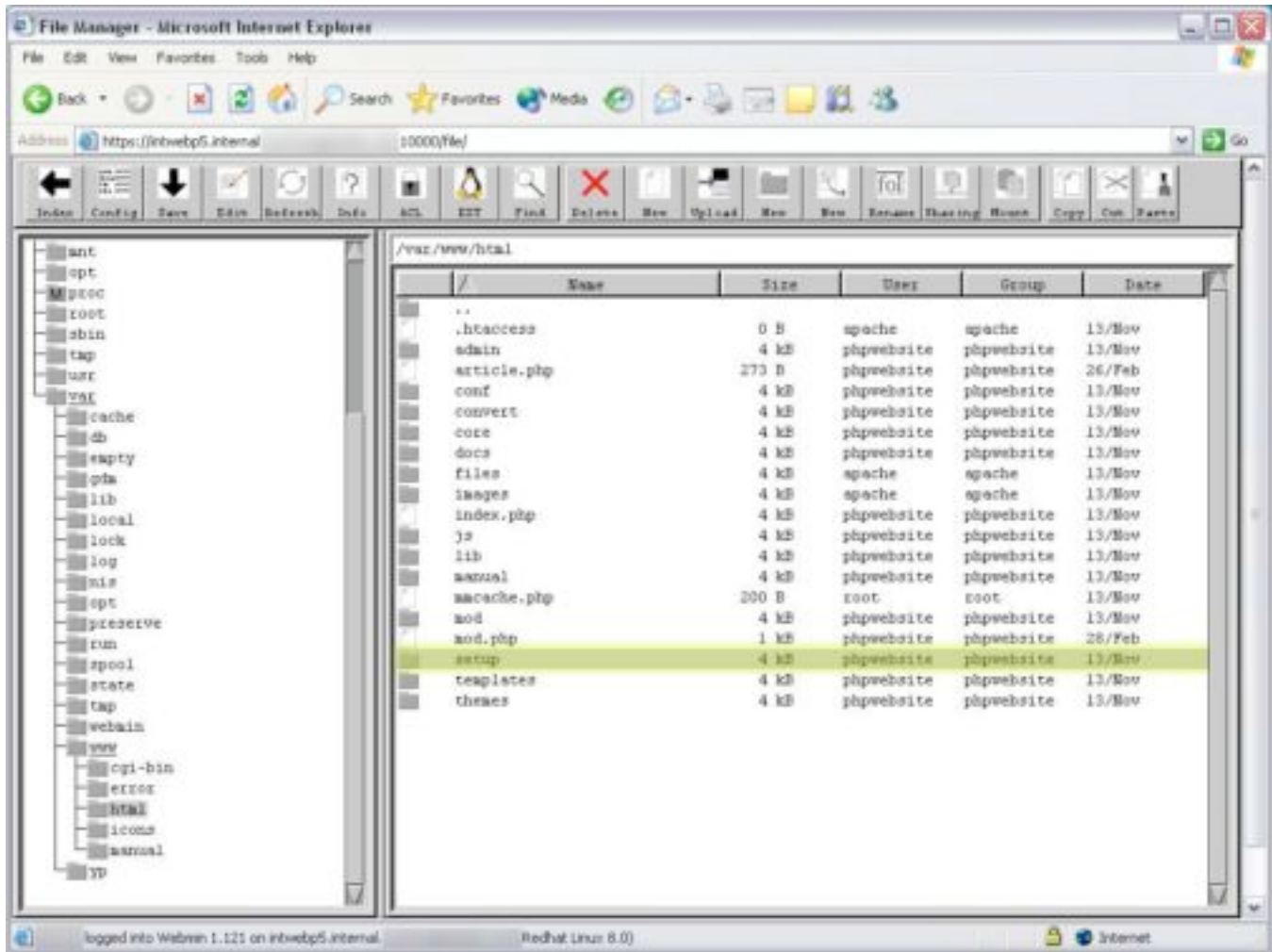
**Pass/Fail:** **Pass**

© SANS Institute 2003, All Rights Reserved



**Step F1(2)**

The phpWebSite root directory (/var/www/html/) on the IPCMS Portal and Content Management Server was checked for the presence of the **./setup** directory:



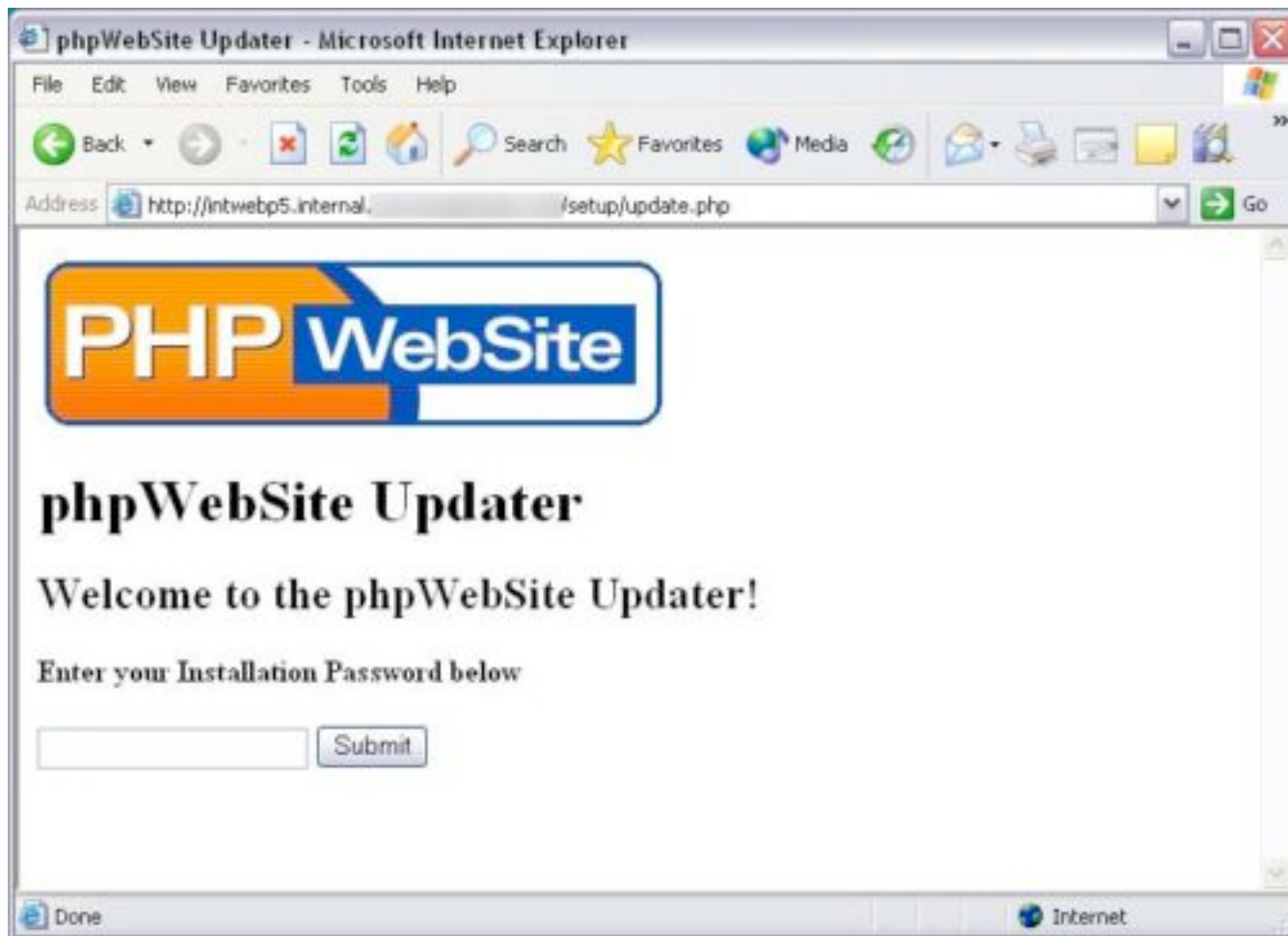
**Result:** The **./setup** directory was present in the phpWebSite root directory (/var/www/html/) on the IPCMS Portal and Content Management Server.

**Pass/Fail:** **Fail**



## Step F1(3)

An attempt was made to connect to the following URL: *intranet server address/setup*.



**Result:** The connection was successful. Password protection of the phpWebSite updater had been enabled.

**Pass/Fail:** **Fail**

## Step F3

The control objective of this step is to ensure that phpWebSite's user and administrator accounts comply with the company's Password Protection Policy.

The configuration settings in phpWebSite's *Administration/User Administration settings* module were inspected to verify that they conform to the company's Password Protection InfoSec Policy.

The screenshot shows the 'User Defaults' configuration page in the phpWebSite application. The browser window is titled 'IPCMS - Microsoft Internet Explorer' and the address bar shows 'http://inweb05.internat...'. The page has a navigation bar with links: 'Add User', 'Manage Users', 'Add Group', 'Manage Groups', and 'Settings'. The main content area is divided into several sections:

- User Defaults**: A section header.
- Contact Information**: Contains fields for 'User Email Contact' (set to 'admin@'), 'Subject Line' (set to 'Welcome to the Intranet Portal an'), and 'Greeting' (set to 'acceptance of and agreement with the terms and conditions of the Acceptable Use Policy. Non-compliance and/or violations of the Acceptable Use Policy are subject to management').
- Allow New User Signup**: Contains radio buttons for 'None', 'All users can apply', and 'Only approved users can apply' (which is selected).
- Authentication Method**: Contains radio buttons for 'Local Database' (selected) and 'External PHP function' (with an external filename field set to 'external\_authorization.p').
- Show Login Box**: A checkbox that is checked.
- Update**: A button at the bottom of the configuration section.

On the left side of the page, there is a sidebar with a 'Hello audit' section, a 'Home Control Panel' link, a 'Log Out' link, and a 'Calendar' section for November 2003.

**Result:** It was found that the phpWebSite application does not provide a built in mechanism for enforcing password length or duration.

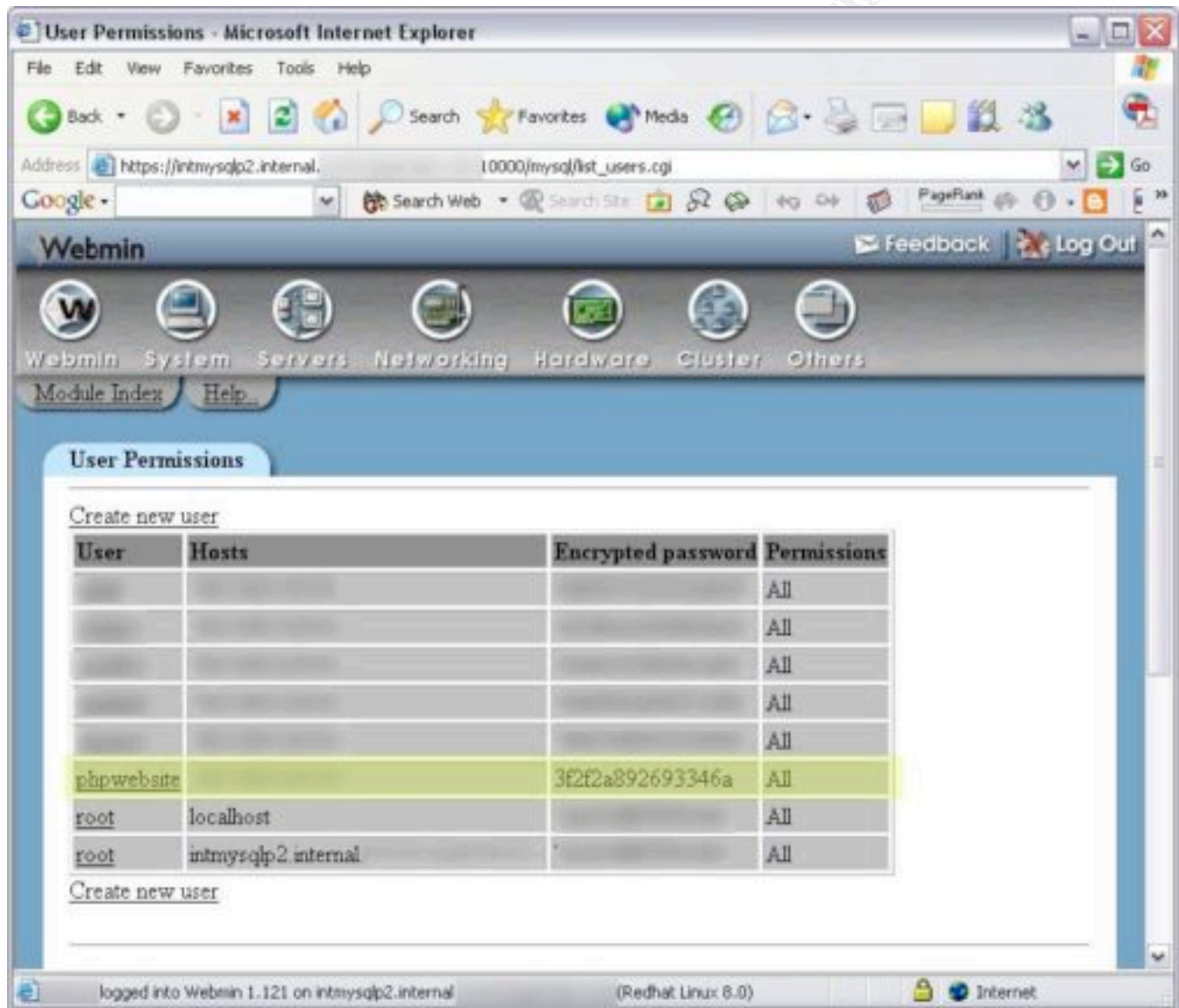
**Pass/Fail:** **Fail**

## Step G2

The control objective of this step is to check that the phpWebSite application's MySQL account has a password and that it is set to only allow access from the IPCMS Portal and Content Management Server.

### Step G2(1)

The Webmin *MySQL Database Server/User Permissions* module was used to check that the phpWebSite application's MySQL user account had an encrypted password set.

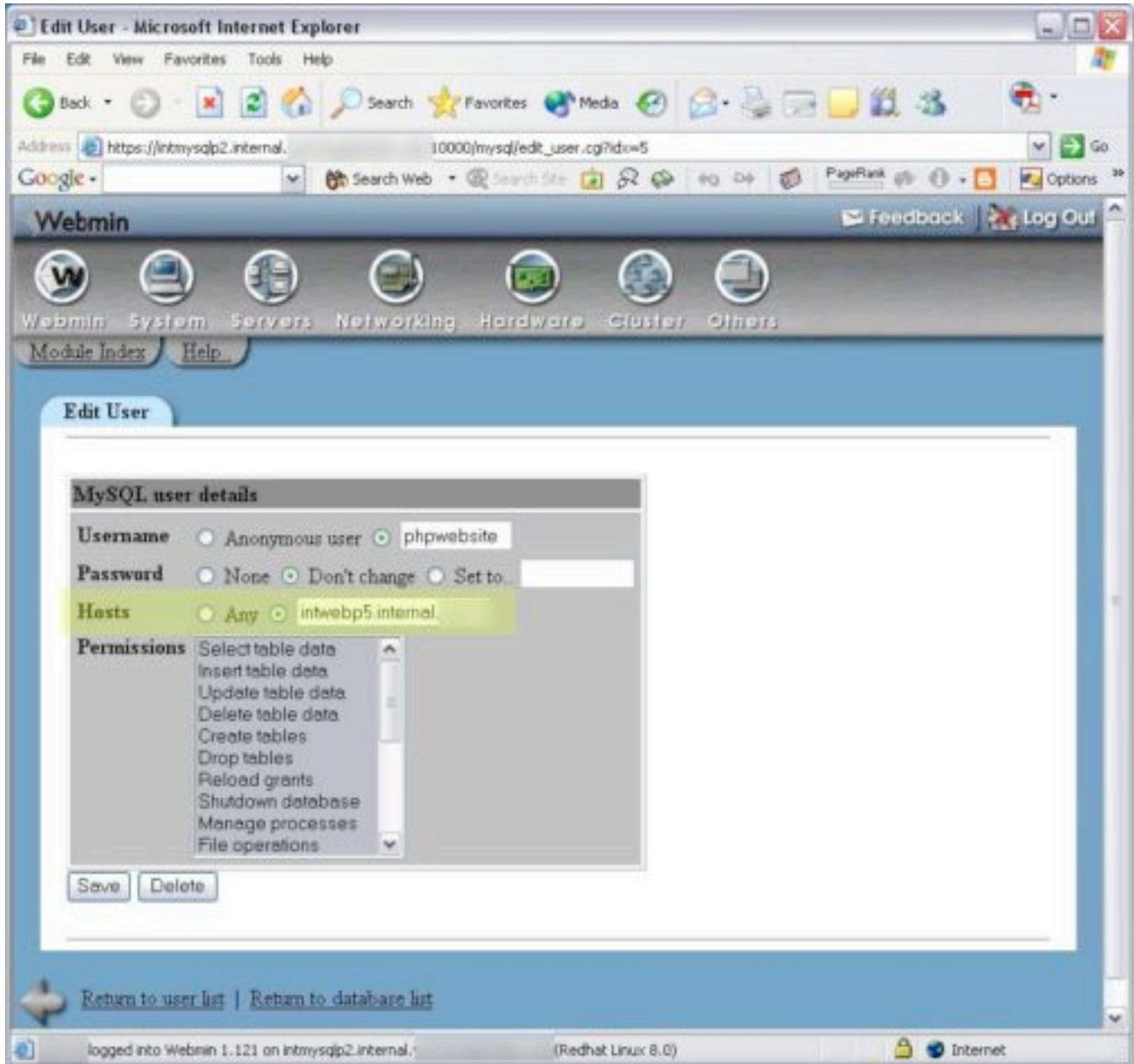


**Result:** The phpWebSite application's MySQL user account had an encrypted password set.

**Pass/Fail:** Pass

## Step G2(2)

The Webmin *MySQL Database Server/User Permissions* module was used to check that the phpWebSite application's MySQL user account was set to only accept connections from the IPCMS Portal and Content Management Server.



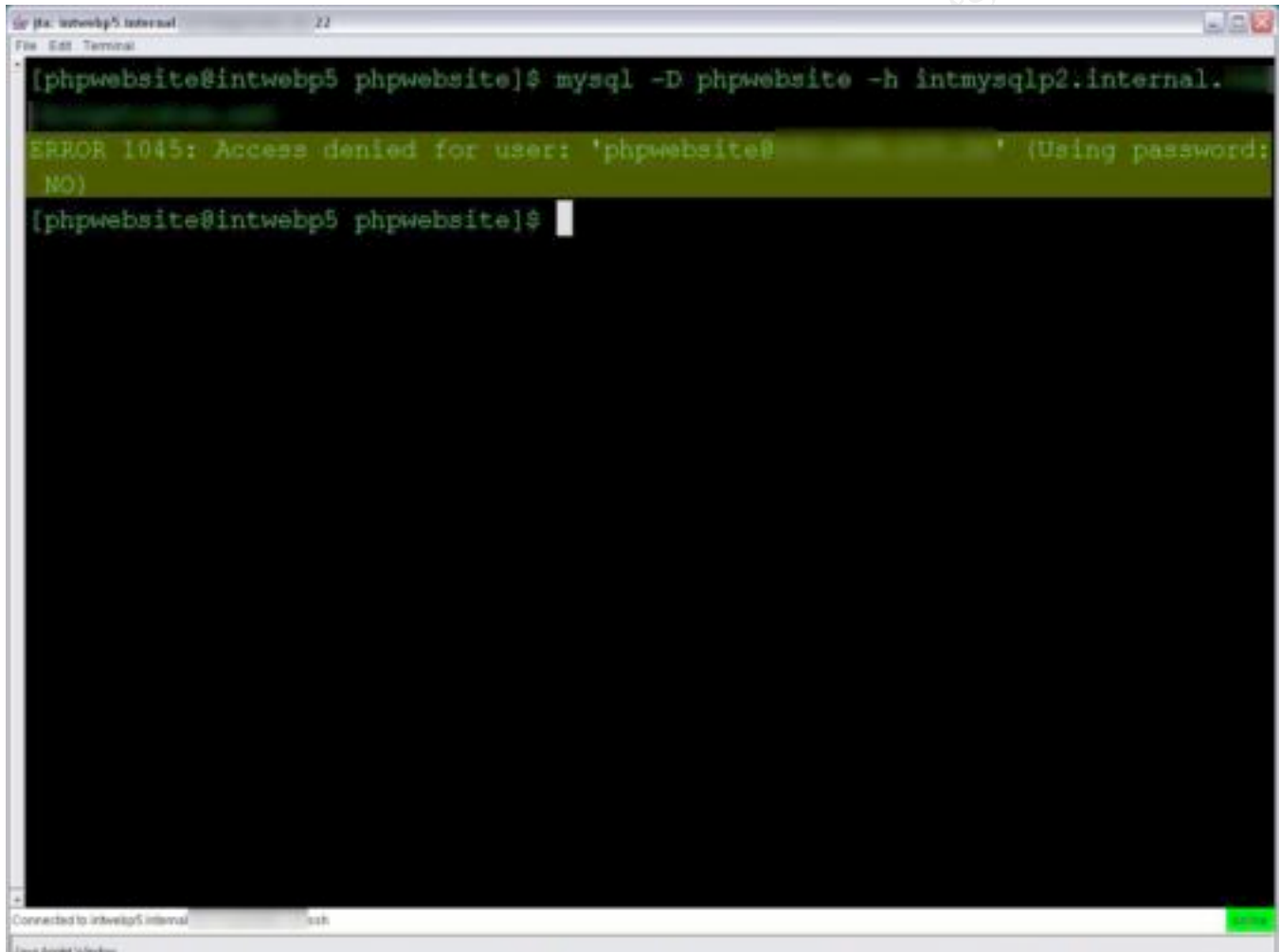
**Result:** The phpWebSite application's MySQL user account was set to only accept connections from the IPCMS Portal and Content Management Server.

**Pass/Fail:** **Pass**

### Step G2(3)

An attempt was made to connect to the MySQL server from the IPCMS Portal and Content Management Server using the phpWebSite application's MySQL user account with no password:

`mysql -D phpwebsite -h database server hostname or IP address`

A terminal window titled 'ssh: intwebp5.internal' with a menu bar (File, Edit, Terminal) and a status bar at the bottom ('Connected to intwebp5.internal', 'ssh'). The terminal shows a command prompt '[phpwebsite@intwebp5 phpwebsite]\$' followed by the command 'mysql -D phpwebsite -h intmysqlp2.internal.'. The output is 'ERROR 1045: Access denied for user: 'phpwebsite@' (Using password: NO)'. The prompt returns to '[phpwebsite@intwebp5 phpwebsite]\$' with a cursor. The terminal background is black with green text.

```
[phpwebsite@intwebp5 phpwebsite]$ mysql -D phpwebsite -h intmysqlp2.internal.  
ERROR 1045: Access denied for user: 'phpwebsite@' (Using password: NO)  
[phpwebsite@intwebp5 phpwebsite]$
```

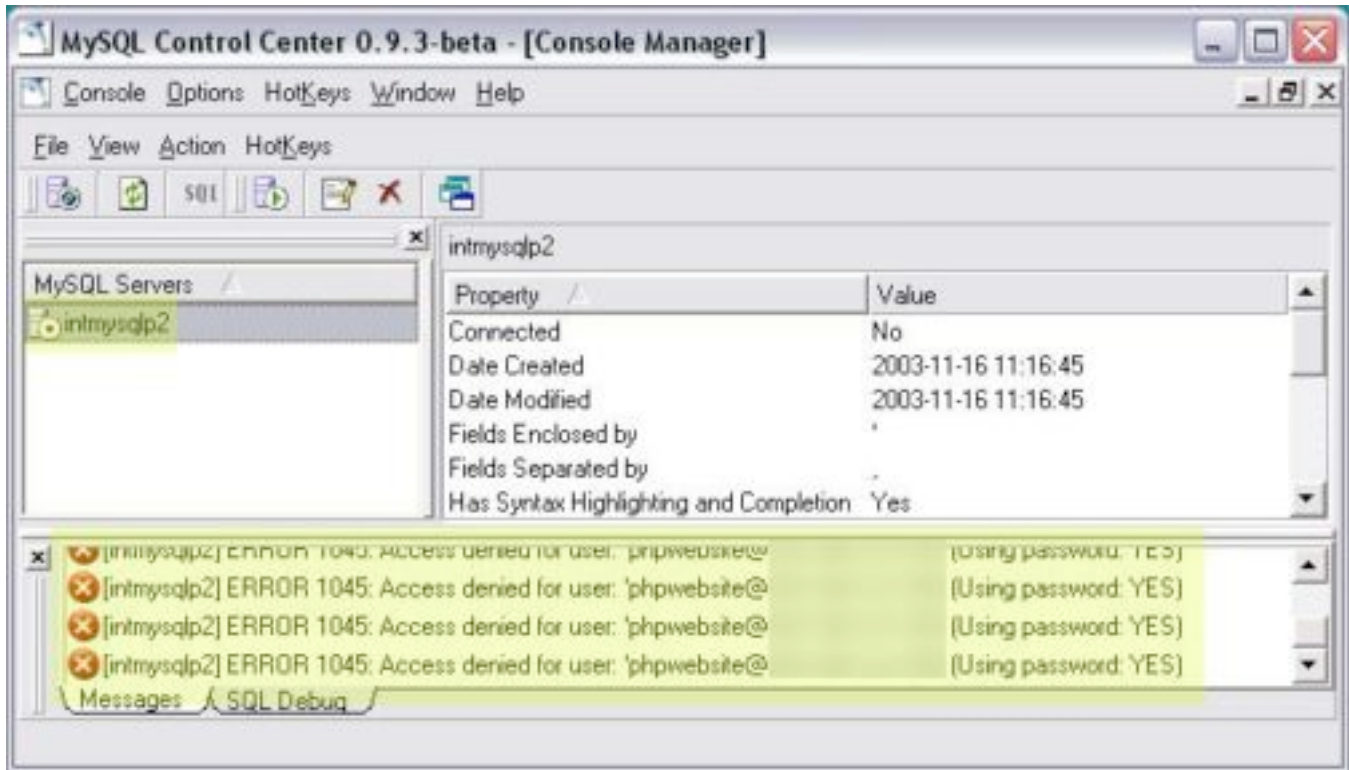
**Result:** The attempt to connect to the MySQL server from the IPCMS Portal and Content Management Server using the phpWebSite application's MySQL user account without a password was denied.

**Pass/Fail:** Pass



**Step G2(4)**

An attempt was made to connect to the MySQL server from a location other than the IPCMS Portal and Content Management Server (a workstation on the company's network), using the valid phpWebSite user account and password.



**Result:** The attempt to connect to the MySQL server from a location other than the IPCMS Portal and Content Management Server (a workstation on the company's network), using the valid phpWebSite user account and password was denied.

**Pass/Fail:** **Pass**

## **Step G5**

The control objective of this step is to ensure that the database connection between the MySQL server and the IPCMS Portal and Content Management Server is strongly encrypted.

Relevant IPCMS design and configuration documentation was requested from the system's administrators, developers and architects to confirm that a strong encryption solution had been implemented for the database connection.

**Result:** Relevant documentation was not available. The IPCMS system's administrators, developers and architects informed me that no encryption solution at all had been implemented to secure the MySQL connection between the Database Server and the Portal and Content Management Server.

**Pass/Fail:** **Fail**

## **Measure Residual Risk**

The overall security of the Intranet Portal and Content Management System is above average, with a few perplexing exceptions.

Obvious thought and effort had been put into backup and recovery procedures and planning.

Security also appears to have been a priority for the physical environment, network, operating system, administration tools, database, Web server and applications. Unneeded services have been disabled, security patches have been applied and network connections have been hardened.

These security precautions are offset to a certain extent by a few puzzling omissions and oversights.

- (1) The Sendmail service was left running on the IPCMS Portal and Content Management Server, even though it was not required. Sendmail has had a history of security vulnerabilities and is often targeted by attackers. As it is not needed it should have been disabled.
- (2) Nessus uncovered one high and a number of medium security risks on both servers which had not been investigated, documented and/or addressed. This leads me to believe that even though fairly thorough security precautions were taken during the design and configuration of the servers, a security scan was never run to verify the results.
- (3) Setup and configuration files were never removed after installation of the phpWebSite application, even though other security configuration steps in the documentation were followed. The documentation clearly states that the setup files and directory are not required after installation, pose a security risk, and should be removed.

- (4) The phpWebSite application has no built in mechanism for enforcing password policies (length, expiration, complexity, etc.). A user or administrator would have nothing stopping them from using a password that did not comply with the company's Password Protection Policy.
- (5) The last and most perplexing security omission is that the connection between the MySQL database server and the IPCMS Portal and Content Management Server is unencrypted. Obvious thought and effort has been put into securing and encrypting all other server connections so why this critical one was overlooked is puzzling.

The security risk posed by an unencrypted connection between the MySQL database server and the IPCMS Portal and Content Management Server is reduced to some extent by the fact that both servers are connected to the same switch. An attacker could still potentially use ARP cache poisoning tools, proxies and sniffers to circumvent this setup, however.

Given the IPCMS systems role as a non tier-one business critical application, the fact that it exclusively services internal company users, the presence on an intrusion detection system, and the switched network architecture, the residual risk is low and the control objectives of this audit were achieved.

Despite the low residual security risk to the IPCMS system, weaknesses and vulnerabilities discovered during this audit should still be investigated, documented and where possible fixed.

The staging and configuration process should also be reviewed to ensure that systems are being scanned for security vulnerabilities prior to being placed in production.

If the IPCMS system had been scanned for security vulnerabilities during the staging and configuration process, a number, if not all of the discovered weaknesses and vulnerabilities could have been detected and fixed before the systems were released to production.

### **Is the System Auditable?**

The Intranet Portal and Content Management System lends itself well to auditing as it is build upon open, well understood and thoroughly tested components.

Because of the number of components used to build the Intranet Portal and Content Management System and the complexity of the overall solution, it was challenging to narrow down the audit requirements to those that were most indicative of the systems overall security.

Each of the subcomponents of the Intranet Portal and Content Management System could easily have been the subject of their own exhaustive audits, but considering the function and placement of the system this would have been overkill.



The items that were included in this audit were chosen as the best indicators of the overall security stance of the Intranet Portal and Content Management System and the results appear to validate these choices and achieve the overall audit objectives.

© SANS Institute 2003, Author retains full rights.

## **Risk Assessment**

### **Summary**

Overall, the security of the Intranet Portal and Content Management System is above average considering its non tier-one (business critical) application status and the fact that it resides on the most secure part of the company's internal network

The IPCMS System failed seven audit checklist items out of a total of 35:

**Item D4(1)a:** Ensure that only required services are running on the IPCMS Portal and Content Management Server.

**Result:** It was found that a non-required service (Sendmail) was running on the IPCMS Portal and Content Management Server.

**Item D7a:** Ensure that there are no known high, serious or medium security risks on the IPCMS Portal and Content Management Server.

**Result:** One high and seven medium security risks were discovered (see appendix 2).

**Item D7b:** Ensure that there are no known high, serious or medium security risks on the IPCMS Database Server.

**Result:** One high and one medium security risk were discovered (see appendix 2).

**Item F1(2):** Ensure that the phpWebSite setup directory and files were removed after the application had been installed.

**Result:** The setup directory and files were found to still be present.

**Item F1(3):** Attempt to establish a Web browser connection to the phpWebSite setup tools on the IPCMS Portal and Content Management Server.

**Result:** The setup tools had been protected with an installation password but a connection was still possible.

**Item F3:** Ensure that phpWebSite's user and administrator accounts comply with the company's Password Protection Policy.

**Result:** The phpWebSite application has no built in mechanism for enforcing password length or duration.

**Item G5:** Ensure that the database connection between the MySQL server and the IPCMS Portal and Content Management Server is strongly encrypted.

**Result:** No relevant documentation was available and the IPCMS system's administrators, developers and architects informed me that no encryption solution at all had been implemented to secure the MySQL connection between the Database Server and the Portal and Content Management Server.

**Background/Risk**

The following table lists each of the non-compliant audit items and the associated risk:

Item #	Non-Compliant Item	Associated Risk
<b>Item D4(1)a</b>	The Sendmail service was found to be running on the IPCMS Portal and Content Management server, even though it was not required.	Sendmail has a history of security vulnerabilities and is often targeted by attackers. A Sendmail vulnerability could potentially allow an attacker to gain access to the operating system, other application and services and/or data.
<b>Item D7a</b>	One high and seven medium security risks were discovered on the IPCMS Portal and Content Management Server.	<p>Due to a vulnerability in SSH, the high security risk could potentially allow an attacker to execute arbitrary commands on the server.</p> <p>The medium risks, which are caused by vulnerabilities in Apache, PHP and the TCP protocol, could result in unauthorized disclosure of data, denial of service and the ability to bypass certain firewall's rule sets.</p>
<b>Item D7b</b>	One high and one medium security risk were discovered on the IPCMS Database Server.	<p>Due to a vulnerability in SSH, the high security risk could potentially allow an attacker to execute arbitrary commands on the server.</p> <p>The medium risk is caused by a vulnerability in the TCP protocol and could result in the ability to bypass certain firewall's rule sets.</p>
<b>Item F1(2)</b>	Setup and configuration files were never removed after installation of the phpWebSite application.	An attacker who managed to gain access to the phpWebSite configuration tools could use them to reconfigure the application to allow him/her unlimited access to the system and its data. They could also use them maliciously to delete application components and data.
<b>Item F1(3)</b>	Even though the phpWebSite setup tools had been protected with an installation password, a connection was still possible.	The phpWebSite tools were available via a web browser to anyone that knew their location, with only a password to protect them. An attacker could use a brute force remote password cracking tool such as Brutus to compromise this protection.

Item #	Non-Compliant Item	Associated Risk
<b>Item F3</b>	The phpWebSite application has no built in mechanism for enforcing password length or duration.	An IPCMS user or administrator could use a weak password that did not comply with the company's Password Protection Policy. This would make it easier for an attacker to compromise the user or administrator's account using a remote password cracking tool such as Brutus.
<b>Item G5</b>	No encryption solution at all had been implemented to secure the MySQL connection between the Database Server and the Portal and Content Management Server.	While the risk of an unencrypted connection between the MySQL database and the IPCMS Portal and Content Management Server is reduced somewhat by the fact that they are connected to the same switch, an attacker could still potentially use ARP cache poisoning tools, proxies and sniffers to intercept and/or modify the data stream between these servers.

## **System Changes and Further Testing**

### **Suggested Corrective Actions**

In order to improve information security on the IPCMS system the following corrections and changes were recommended.

- (1) To address the requirements of audit checklist item **D4(1)a** and ensure that only required services are running on the IPCSM Portal and Content Management Server the Sendmail service should be stopped in Webmin's *Bootup and Shutdown module* and configured to not start on boot.
- (2) To address the requirements of audit checklist item **D7a** and ensure that there are no known high, serious or medium security risks on the IPCMS Portal and Content Management Server, the following items from the Nessus scan must be addressed:

- a. You are running a version of OpenSSH which is older than 3.7.1.

Versions older than 3.7.1 are vulnerable to a flaw in the buffer management functions which might allow an attacker to execute arbitrary commands on this host.

An exploit for this issue is rumored to exist.

Note that several distributions patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command:

```
rpm -q openssh-server
```

Returns:

openssh-server-3.1p1-13 (RedHat 7.x)

openssh-server-3.4p1-7 (RedHat 8.0)

openssh-server-3.5p1-11 (RedHat 9)

Solution: Upgrade to OpenSSH 3.7.1

See also:

<http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2>

<http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2>

Risk factor: High

CVE: CAN-2003-0693, CAN-2003-0695

BID: 8628

- b. Your Web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

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 junction 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.

If you are using Sun ONE Web Server releases 6.0 SP2 and later, add the following to the default object section in obj.conf:

```
<Client method="TRACE">
AuthTrans fn="set-variable"
remove-headers="transfer-encoding"
set-headers="content-length: -1"
error="501"
</Client>
```

If you are using Sun ONE Web Server releases 6.0 SP2 or below, compile the NSAPI plugin located at:

<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603>

See [http://www.whitehatsec.com/press\\_releases/WH-PR-20030120.pdf](http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf)  
<http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html>  
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603>  
<http://www.kb.cert.org/vuls/id/867593>

Risk factor: Medium

- c. The remote host appears to be running a version of Apache 2.x which is older than 2.0.43.

This version allows an attacker to view the source code of CGI scripts via a POST request made to a directory with both WebDAV and CGI enabled.

\*\*\* 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 2.0.43  
See also: [http://www.apache.org/dist/httpd/CHANGES\\_2.0](http://www.apache.org/dist/httpd/CHANGES_2.0)  
Risk factor: Medium  
CVE: CAN-2002-1156, CAN-2003-0083  
BID: 6065

- d. The remote host is running a version of PHP earlier than 4.2.2.

The mail() function does not properly sanitize user input.

This allows users to forge email to make it look like it is coming from a different source other than the server.

Users can exploit this even if SAFE\_MODE is enabled.

Solution: Contact your vendor for the latest PHP release.  
Risk factor: Medium

CVE: CAN-2002-0985

BID: 5562

- e. The remote host appears to be running a version of Apache 2.x which is older than 2.0.46.

This version is vulnerable to various flaws:

There is a denial of service vulnerability which may allow an attacker to disable basic authentication on this host.

There is a denial of service vulnerability in the mod\_dav module which may allow an attacker to crash this service remotely.

Solution: Upgrade to version 2.0.46

See also: [http://www.apache.org/dist/httpd/CHANGES\\_2.0](http://www.apache.org/dist/httpd/CHANGES_2.0)

Risk factor: Medium

CVE: CAN-2003-0245, CAN-2003-0189

BID: 7723, 7725

- f. The remote host appears to be running a version of Apache 2.x which is older than 2.0.45.

This version is vulnerable to various flaws:

There is a denial of service attack which may allow an attacker to disable this server remotely

The httpd process leaks file descriptors to child processes, such as CGI scripts. An attacker who has the ability to execute arbitrary CGI scripts on this server (including PHP code) would be able to write arbitrary data in the file pointed to (in particular, the log files).

Solution: Upgrade to version 2.0.45

See also: [http://www.apache.org/dist/httpd/CHANGES\\_2.0](http://www.apache.org/dist/httpd/CHANGES_2.0)

Risk factor: Medium

CVE: CAN-2003-0132

BID: 7254, 7255

- g. The remote host appears to be running a version of Apache 2.x which is older than 2.0.47.

This version is vulnerable to various flaws which may allow an attacker to disable this service remotely and/or locally.

Solution: Upgrade to version 2.0.47

See also: [http://www.apache.org/dist/httpd/CHANGES\\_2.0](http://www.apache.org/dist/httpd/CHANGES_2.0)

Risk factor: Medium

CVE: CAN-2003-0192, CAN-2003-0253, CAN-2003-0254

BID: 8134, 8135, 8137, 8138

- h. The remote host does not discard TCP SYN packets which have the FIN flag set.

Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.

See also: <http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>  
<http://www.kb.cert.org/vuls/id/464113>

Solution: Contact your vendor for a patch

Risk factor: Medium

BID: 7487

- (3) To address the requirements of audit checklist item **D7b** and ensure that there are no known high, serious or medium security risks on the IPCMS Database Server, the following items from the Nessus scan must be addressed:

- a. You are running a version of OpenSSH which is older than 3.7.1.

Versions older than 3.7.1 are vulnerable to a flaw in the buffer management functions which might allow an attacker to execute arbitrary commands on this host.

An exploit for this issue is rumored to exist.

Note that several distributions patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command:

```
rpm -q openssh-server
```

Returns:

```
openssh-server-3.1p1-13 (RedHat 7.x)
```

```
openssh-server-3.4p1-7 (RedHat 8.0)
```

```
openssh-server-3.5p1-11 (RedHat 9)
```

Solution: Upgrade to OpenSSH 3.7.1

See also:

<http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2>

<http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2>



Risk factor: High

CVE: CAN-2003-0693, CAN-2003-0695

BID: 8628

- b. The remote host does not discard TCP SYN packets which have the FIN flag set.

Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.

See also: <http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>  
<http://www.kb.cert.org/vuls/id/464113>

Solution: Contact your vendor for a patch

Risk factor: Medium

BID: 7487

- (4) To address the requirements of audit checklist item **F1(2)** and ensure that all phpWebSite setup directory and files are removed the **./setup** directory should be deleted from **/var/www/html/** on the IPCMS Portal and Content Management Server (intwebp5).
- (5) To address the requirements of audit checklist item **F1(3)** and ensure that an attacker cannot connect to the phpWebSite setup tools, a Web browser connection should be attempted to *intranet server address/setup* after step 4 has been performed. Once the **./setup** directory has been removed a connection to this URL should be impossible.
- (6) To address the requirements of audit checklist item **F3** and ensure that phpWebSite's user and administrator accounts comply with the company's Password Protection Policy the current phpWebSite *Administration/User Administration settings* module needs to be modified to include this functionality or a new module coded that addresses these requirements.
- (7) To address the requirements of audit checklist item **G5** and ensure that the database connection between the MySQL server and the IPCMS Portal and Content Management Server is strongly encrypted, a MySQL server-to-server encryption solution such as SSH tunneling should to be researched, tested and implemented.

## Implementation of Suggested Changes

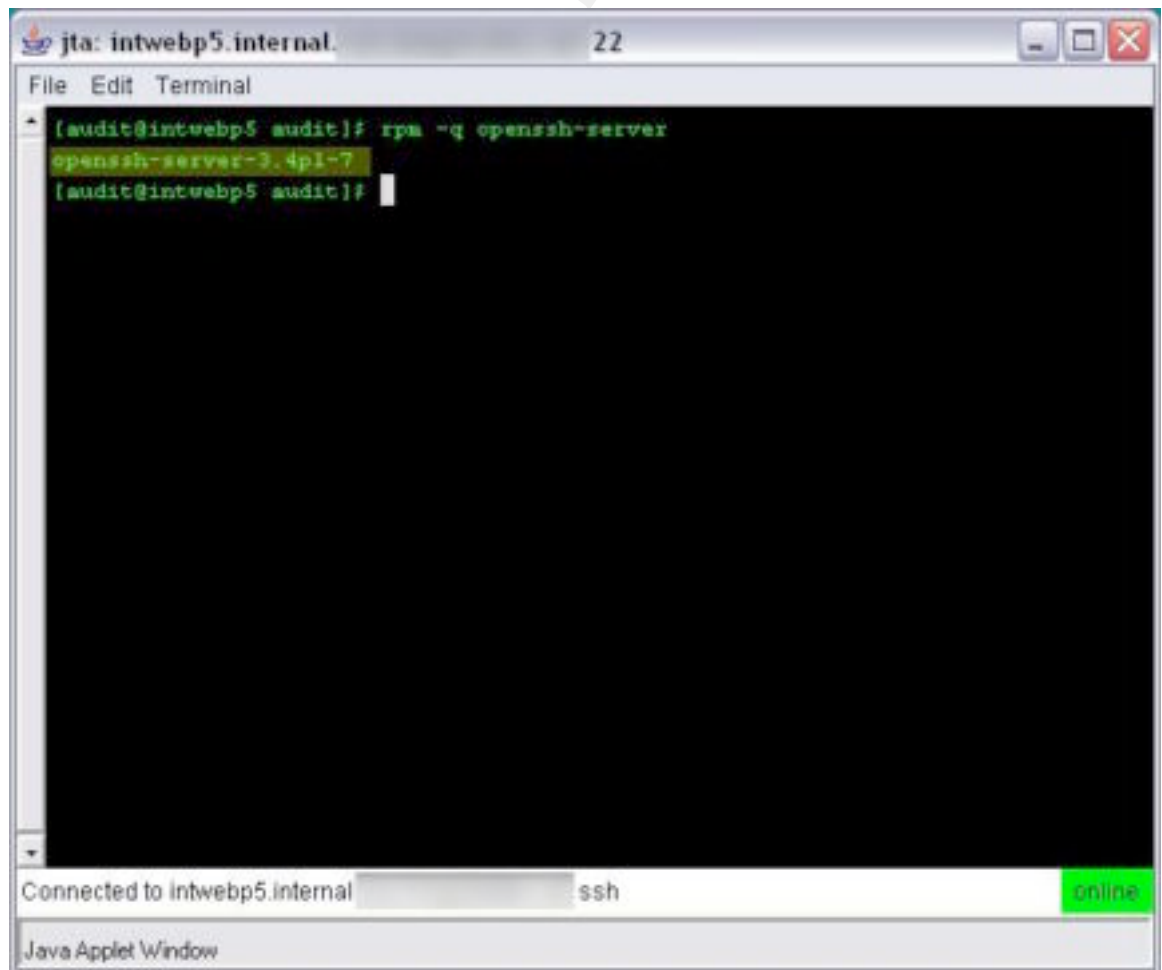
- (1) To address the requirements of audit checklist item **D4(1)a** the Sendmail service was stopped in Webmin's *Bootup and Shutdown module* and configured to not start on boot.
- (2) To meet the requirements of audit checklist item **D7a** the following items from the Nessus scan were addressed:
  - a. Because the server was running the Red Hat 8.0 operating system the following procedure (as documented in the Nessus alert) was followed to determine if the installed version of SSH was vulnerable.

**rpm -q openssh-server**

This returned the following results:

**openssh-server-3.4p1-7**

This alert was therefore a **False Positive**.



```
jta: intwebp5.internal. 22
File Edit Terminal
[audit@intwebp5 audit]$ rpm -q openssh-server
openssh-server-3.4p1-7
[audit@intwebp5 audit]$
Connected to intwebp5.internal ssh online
Java Applet Window
```

- b. The following lines were added to the Apache configuration file (httpd.conf) and the httpd service was restarted.:

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```



- c. According to Red Hat (<http://rhn.redhat.com/errata/RHSA-2003-139.html>), The CVE CAN-2002-1156 and CAN-2003-0083 vulnerabilities are addressed in their httpd-2.0.40-11.3+ updates to Apache.

The version of Apache running on the IPCMS Portal and Content Management Server is httpd 2.0.40-11.7.

This alert was therefore a **False Positive**.

- d. Suggested information security changes for audit checklist item **F3** were not implemented. See the System Justification section for more information on why this decision was made.
- e. According to Red Hat (<http://rhn.redhat.com/errata/RHSA-2003-186.html>), The CVE CAN-2003-0245 and CAN-2003-0189 vulnerabilities are addressed in their httpd-2.0.40-11.5+ updates to Apache.

The version of Apache running on the IPCMS Portal and Content Management Server is httpd 2.0.40-11.7.

This alert was therefore a **False Positive**.

- f. According to Red Hat (<http://rhn.redhat.com/errata/RHSA-2003-139.html>), The CVE CAN-2003-0132 vulnerability was addressed in their httpd-2.0.40-11.3+ updates to Apache.

The version of Apache running on the IPCMS Portal and Content Management Server is httpd 2.0.40-11.7.

This alert was therefore a **False Positive**.

- g. According to Red Hat (<http://rhn.redhat.com/errata/RHSA-2003-240.html>), The CVE CAN-2003-0192, CAN-2003-0253 and CAN-2003-0254 vulnerabilities were addressed in their httpd-2.0.40-11.7+ updates to Apache.

The version of Apache running on the IPCMS Portal and Content Management Server is httpd 2.0.40-11.7.

This alert was therefore a **False Positive**.

- h. A vendor fix from Red Hat for BugTraq Vulnerability ID 7487 was researched and found to not exist.

Research at the following URLs:

<http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>

<http://www.kb.cert.org/vuls/id/464113>

Indicated that even without a patch the server was not vulnerable because the company:

- i. Does not use a routable IP address space except inside their DMZ.
- ii. Uses stateful filtering on their firewalls.

Based upon the above information this vulnerability was determined to be inapplicable to the companies IT environment and a minimal security risk (See the System Justification section for more information).

- (3) To meet the requirements of audit checklist item **D7b** the following items from the Nessus scan were addressed:

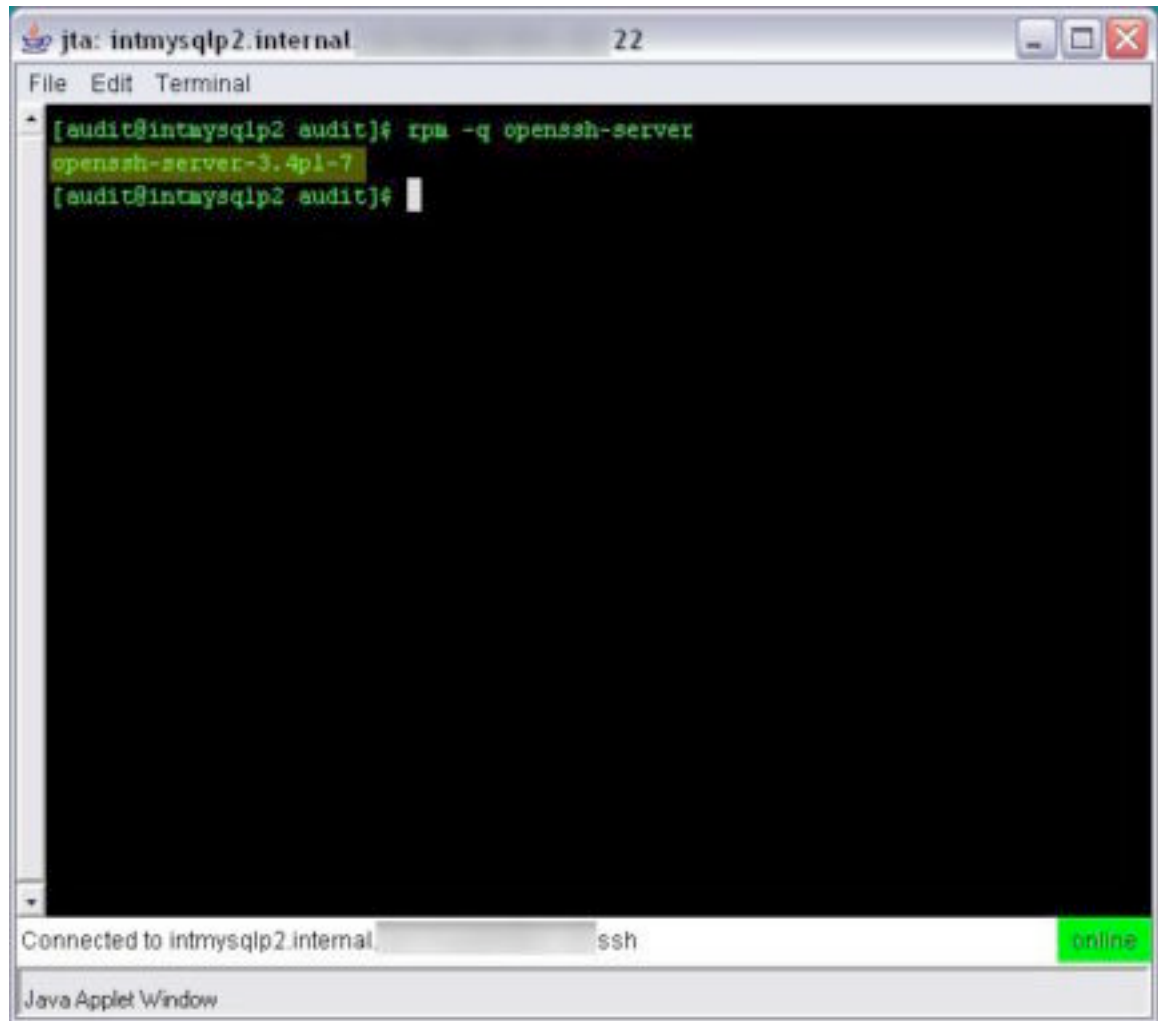
- a. Because the server was running the Red Hat 8.0 operating system the following procedure (as documented in the Nessus alert) was followed to determine if the installed version of SSH was vulnerable.

**rpm -q openssh-server**

This returned the following results:

**openssh-server-3.4p1-7**

This alert was therefore a **False Positive**.



```
jta: intmysqlp2.internal 22
File Edit Terminal
[audit@intmysqlp2 audit]# rpm -q openssh-server
openssh-server-3.4p1-7
[audit@intmysqlp2 audit]#
Connected to intmysqlp2.internal ssh online
Java Applet Window
```

- b. A vendor fix from Red Hat for BugTraq Vulnerability ID 7487 was researched and found to not exist.

Research at the following URLs:

<http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>

<http://www.kb.cert.org/vuls/id/464113>

Indicated that even without a patch the server was not vulnerable because the company:

- iii. Does not use a routable IP address space except inside their DMZ.
- iv. Uses stateful filtering on their firewalls.

Based upon the above information this vulnerability was determined to be inapplicable to the companies IT environment and a minimal security risk (See the System Justification section for more information).

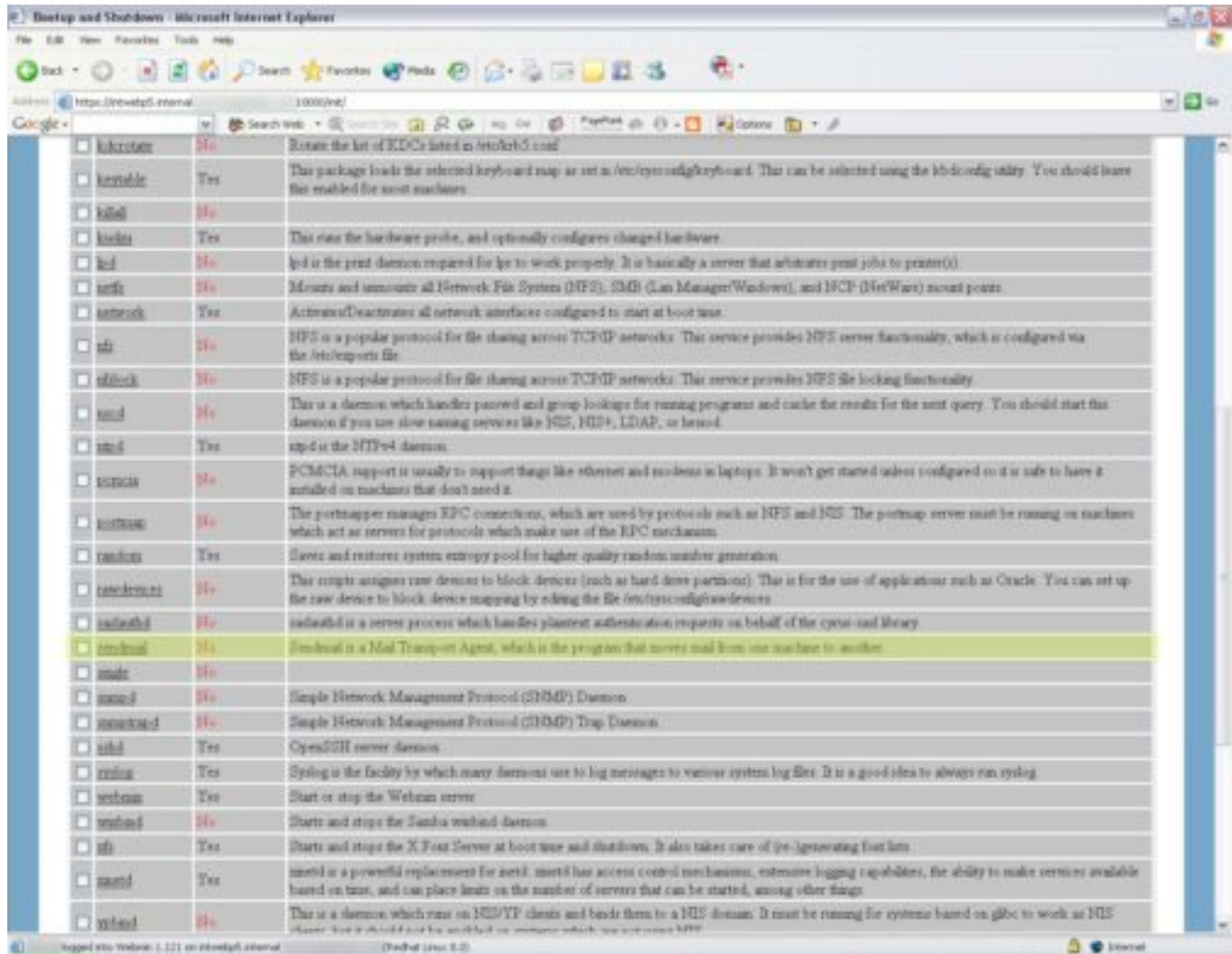
- (4) To address the requirements of audit checklist item **F1(2)** the **./setup** directory was deleted from **/var/www/html/** on the IPCMS Portal and Content Management Server (intwebp5).
- (5) To address the requirements of audit checklist item **F1(3)** a Web browser connection was attempted to *intranet server address/setup* after step 4 had been performed to ensure that a connection to this URL was impossible.
- (6) Suggested information security changes for audit checklist item **F3** were not implemented. See the System Justification section for more information on why this decision was made.
- (7) Suggested information security changes for audit checklist item **G5** were not implemented. See the System Justification section for more information on why this decision was made.

© SANS Institute 2003, Author retains full rights.

## Re-Test of Corrected/fixed audit checklist items

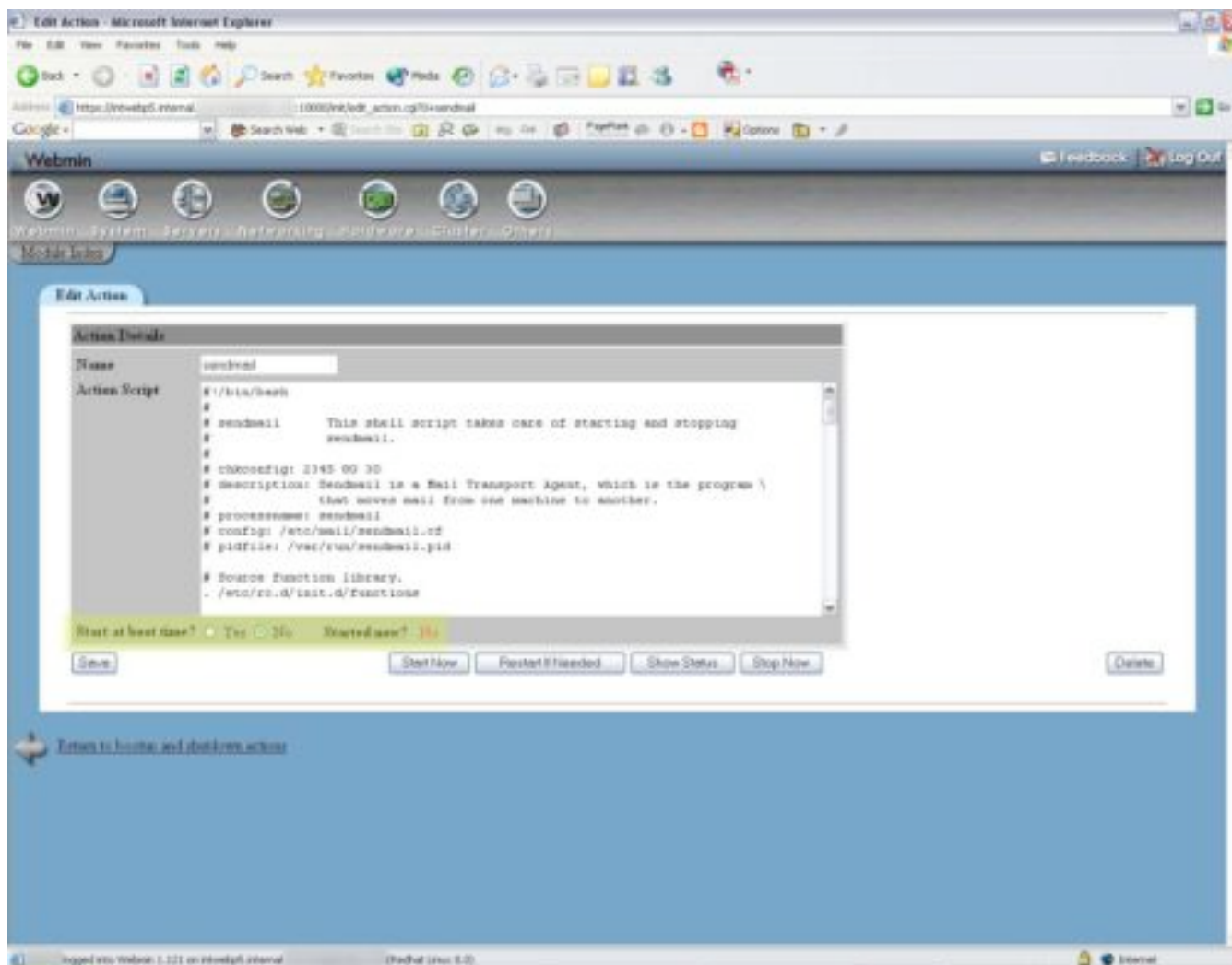
### Step D4(1)a

For this step Webmin's *Bootup and Shutdown module* was used to list all running and stopped services on the IPCMS Portal and Content Management Server.



The screenshot shows the 'Bootup and Shutdown' module in Webmin, displaying a list of system services. The table has three columns: a checkbox for enabling/disabling the service, the service name, its status (Yes/No), and a description. The 'inetd' service is highlighted in yellow.

Service	Status	Description
libcrypt	No	Rotates the list of KDCs listed in /etc/krb5.conf
keyboard	Yes	This package loads the selected keyboard map as set in /etc/sysconfig/keyboard. This can be selected using the kbconfig utility. You should leave this enabled for most machines.
lbdm	No	
lckd	Yes	This runs the hardware probe, and optionally configures changed hardware.
lpd	No	lpd is the print daemon required for lp to work properly. It is basically a server that arbitrates print jobs to printer(s).
netfs	No	Mounts and unmounts all Network File Systems (NFS), SMB (Lan Manager/Windows), and NCP (NetWare) mount points.
network	Yes	Activates/Deactivates all network interfaces configured to start at boot time.
nfs	No	NFS is a popular protocol for file sharing across TCP/IP networks. This service provides NFS server functionality, which is configured via the /etc/export file.
nfslock	No	NFS is a popular protocol for file sharing across TCP/IP networks. This service provides NFS file locking functionality.
nmd	No	This is a daemon which handles password and group lookups for running programs and cache the results for the next query. You should start this daemon if you use slow naming services like NIS, NIS+, LDAP, or LDAP.
nsd	Yes	nsd is the NTPv4 daemon.
pcmcia	No	PCMCIA support is usually to support things like ethernet and modems in laptops. It won't get started unless configured to it is safe to have it installed on machines that don't need it.
portmap	No	The portmapper manages RPC connections, which are used by protocols such as NFS and NIS. The portmap server must be running on machines which act as servers for protocols which make use of the RPC mechanism.
random	Yes	Saves and restores system entropy pool for higher quality random number generation.
rawdevices	No	This script assigns raw devices to block devices (such as hard drive partitions). This is for the use of applications such as Oracle. You can set up the raw device to block device mapping by editing the file /etc/sysconfig/rawdevices.
radiusd	No	radiusd is a server process which handles plaintext authentication requests on behalf of the cryptd and library.
sendmail	No	Sendmail is a Mail Transport Agent, which is the program that moves mail from one machine to another.
smc	No	
smcfsd	No	Simple Network Management Protocol (SNMP) Daemon.
smcnetd	No	Simple Network Management Protocol (SNMP) Trap Daemon.
sshd	Yes	OpenSSH server daemon.
syslog	Yes	Syslog is the facility by which many daemons send log messages to various system log files. It is a good idea to always run syslog.
webmin	Yes	Start or stop the Webmin server.
wired	No	Starts and stops the Samba wireless daemon.
xfs	Yes	Starts and stops the X Font Server at boot time and shutdown. It also takes care of (re-)generating font lists.
xmcd	Yes	xmcd is a powerful replacement for xinetd. xmcd has access control mechanisms, extensive logging capabilities, the ability to make services available based on time, and can place limits on the number of servers that can be started, among other things.
xmcd	No	This is a daemon which runs on NIS/YYP clients and binds them to a NIS domain. It must be running for systems based on glibc to work as NIS clients. It is not needed for systems which use their own NIS.



The following list of services was found to be running on the IPCMS Portal and Content Management Server.

- anacron
- apmd
- atd
- autofs
- chronod
- gpm
- httpd
- iptables
- keytables
- kudzu
- network
- ntpd
- random
- sshd
- syslog



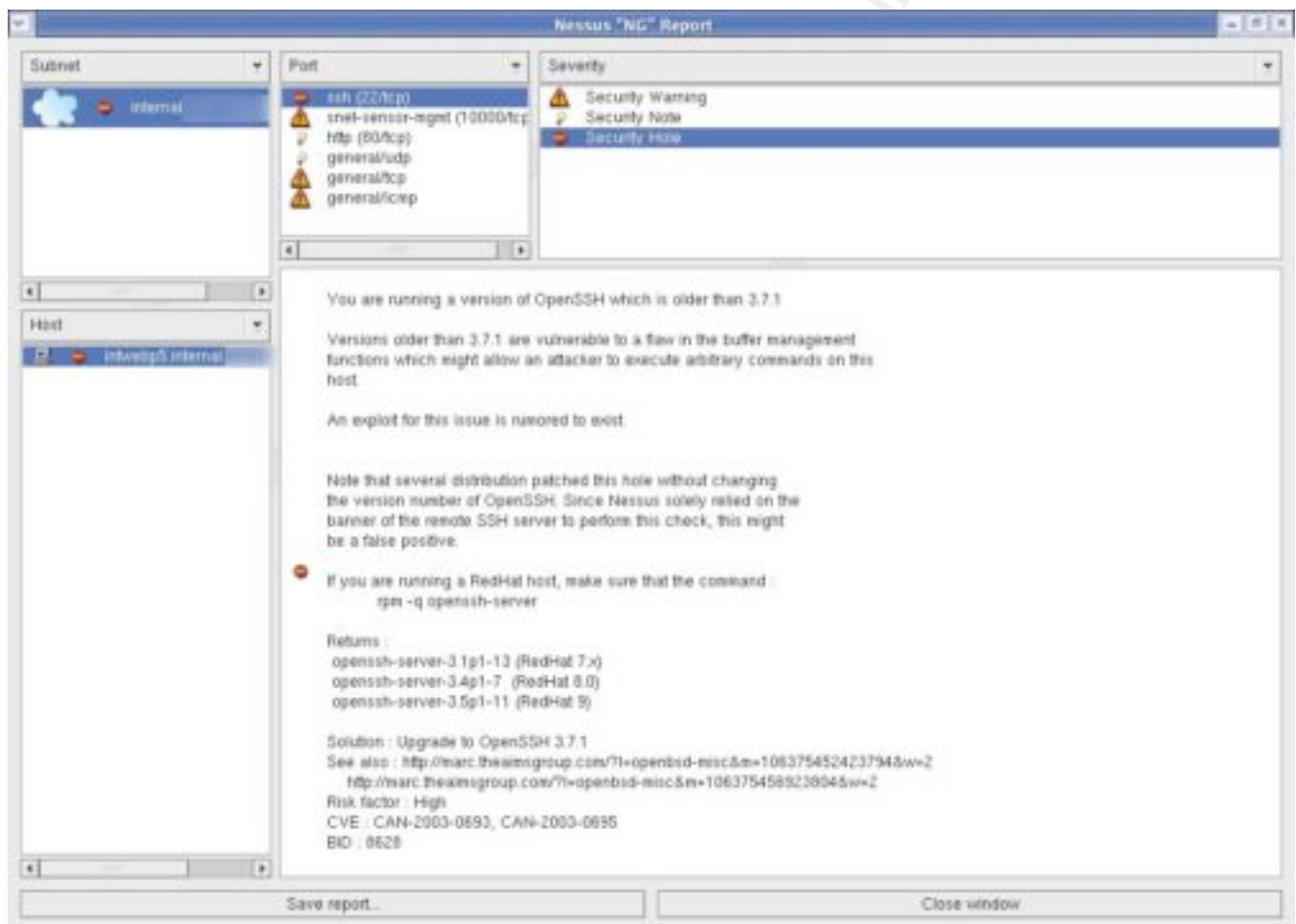
- webmin
- xfs
- xinetd

**Result:** Only the required services were found to be running on the IPCMS Database Server.

**Pass/Fail:** **Pass**

### Step D7a

Nessus 2.0.9 ([www.nessus.org](http://www.nessus.org)) was used to scan the IPCMS Portal and Content Management Server for vulnerabilities using the “Enable all but dangerous plugins” option.

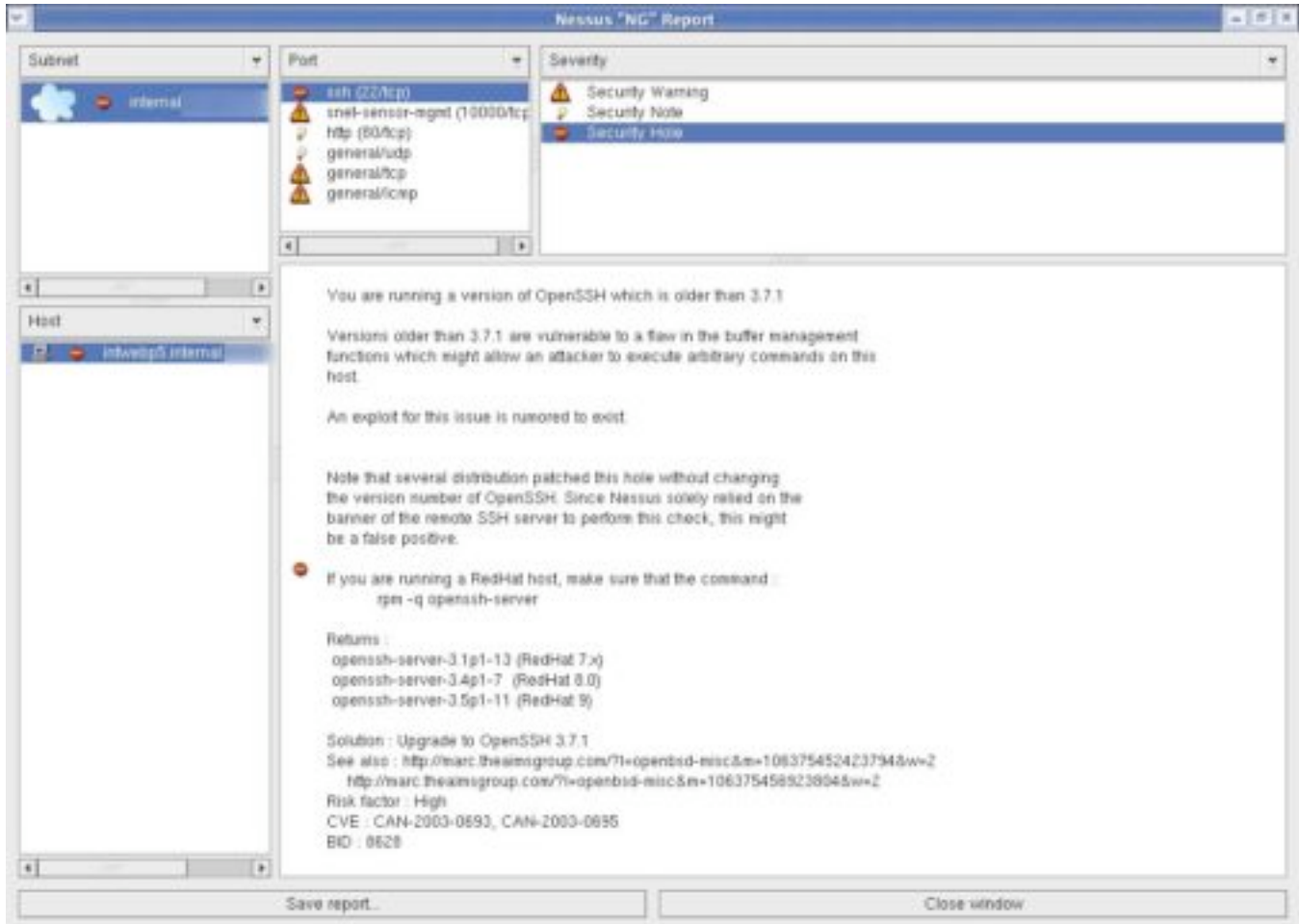


**Result:** Taking into account the false positives noted in the Implementation of Suggested Changes section, Nessus returned results for the IPCMS Portal and Content Management Server that indicated that the implemented security fixes were successful (see appendix 3 for complete Nessus retest results):

**Pass/Fail:** **Pass**

## Step D7b

Nessus 2.0.9 ([www.nessus.org](http://www.nessus.org)) was used to scan the IPCMS Database Server for vulnerabilities using the “Enable all but dangerous plugins” option.

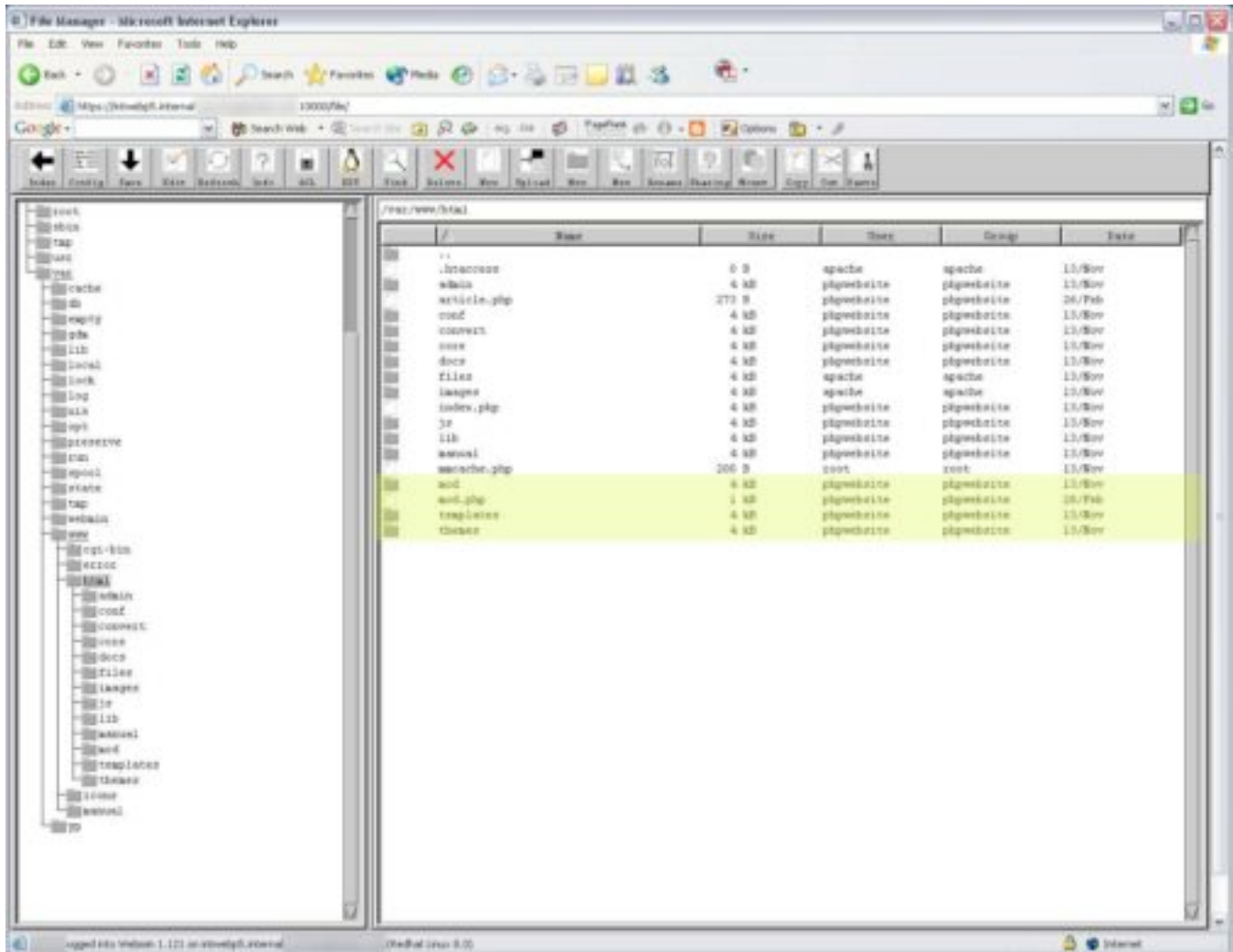


**Result:** Taking into account the false positives noted in the Implementation of Suggested Changes section, Nessus returned results for the IPCMS Database Server that indicated that the implemented security fixes were successful (see appendix 3 for complete Nessus retest results):

**Pass/Fail:** **Pass**

**Step F1(2)**

The phpWebSite root directory (/var/www/html/) on the IPCMS Portal and Content Management Server was checked for the presence of the **./setup** directory:

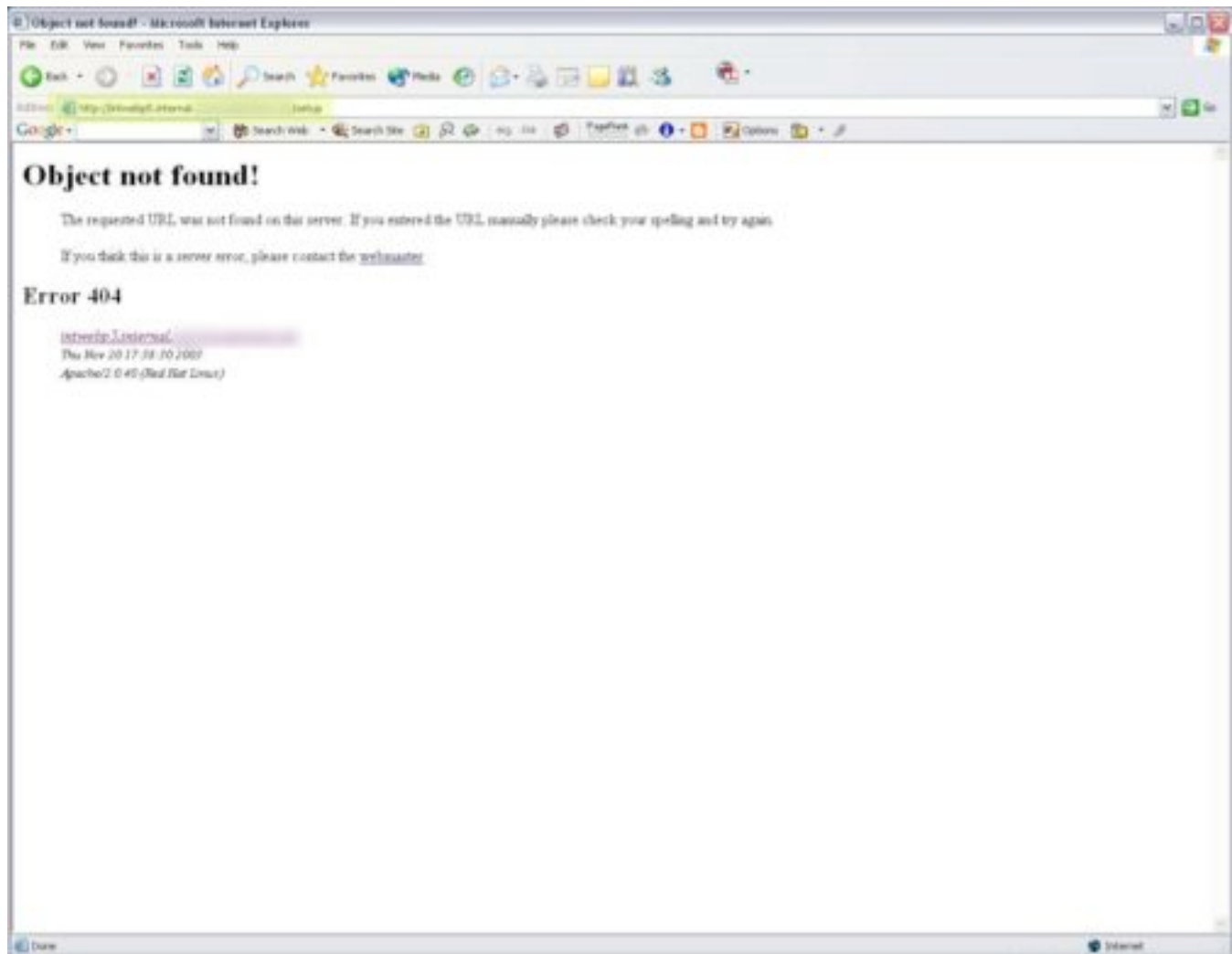


**Result:** The **./setup** directory was not present in the phpWebSite root directory (/var/www/html/) on the IPCMS Portal and Content Management Server.

**Pass/Fail:** **Pass**

## Step F1(3)

An attempt was made to connect to the following URL: *intranet server address/setup*.



**Result:** A connection to the *intranet server address/setup* URL was unsuccessful.

**Pass/Fail:** Pass

## Step F3

No retest was performed as the suggested information security changes for audit checklist item **F3** were not implemented. See the System Justification section for more information on why this decision was made.

**Pass/Fail:** N/A

## Step G5

No retest was performed as the suggested information security changes for audit checklist item **G5** were not implemented. See the System Justification section for more information on why this decision was made.

Pass/Fail: N/A

## System Justification

A number of vulnerabilities that were flagged by Nessus as being of high or medium severity turned out to be false positives after they had been thoroughly researched. Red Hat seems to make a practice of backward porting security fixes rather than releasing new versions of software packages.

This had a marked effect on the outcome of audit checklist items **D7a** and **D7b** (See the Implementation of Suggested Changes section for more details):

- For checklist item **D7a** five out of eight Nessus scan results turned out to be false positive, including one high and four mediums. Of the two remaining valid alerts, one was applicable to the companies IT environment and the other was not.
- For checklist item **D7b** one of the two Nessus scan results turned out to be a false positive and the other was not applicable to the company's IT environment.

The following item from audit checklist item **D7a** was determined to be a valid vulnerability:

The remote host is running a version of PHP earlier than 4.2.2.

The mail() function does not properly sanitize user input.

This allows users to forge email to make it look like it is coming from a different source other than the server.

Users can exploit this even if SAFE\_MODE is enabled.

Solution: Contact your vendor for the latest PHP release.

Risk factor: Medium

CVE: CAN-2002-0985

BID: 5562

According to the company's IPCMS system developers the mail() function was not being used on the IPCMS system and without extensive testing the upgrade to the latest version of PHP had the potential to break customized application components.

Based on the above information, the low current risk to the system and the presence of network and host based intrusion detection systems, management decided that the upgrade to the latest version of PHP should be postponed until the next revision of the IPCMS system is released (six to eight months).

While a valid vulnerability detected by Nessus in audit steps **D7a** and **D7b**, the following item could not be directly addressed on the IPCMS servers.

The remote host does not discard TCP SYN packets which have the FIN flag set.

Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.

See also: <http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>  
<http://www.kb.cert.org/vuls/id/464113>

Solution: Contact your vendor for a patch  
Risk factor: Medium  
BID: 7487

A vendor fix from Red Hat for BugTraq Vulnerability ID 7487 was researched and found to not exist.

Research at the following URLs:

<http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>

<http://www.kb.cert.org/vuls/id/464113>

Indicated that even without a patch the server was not vulnerable because the company:

- (1) Does not use a routable IP address space except inside their DMZ.
- (2) Uses stateful filtering on their firewalls.

Based upon the above information this vulnerability was determined to be inapplicable to the companies IT environment and a minimal security risk so no further action was taken.

Suggested information security changes for audit checklist item **F3** were not implemented because management determined that the amount of development time and effort required to modify the current code or write a new module for the IPCMS system would jeopardize the project's go live date.

The control objective for audit step **F3** was to ensure that phpWebSite's user and administrator accounts comply with the company's Password Protection Policy.

The audit determined that the phpWebSite application had no built in mechanism for enforcing password length or duration.

Because this item was not fixed the possibility exists that an IPCMS user or administrator could use a weak password that did not comply with the company's Password Protection Policy. This would make it easier for an attacker to compromise the user or administrator's account using a brute force password cracking tools, such as Brutus.

A compromise was reached in this case. A mechanism for enforcing password length and duration would be added to the requirements for the next release of the IPCMS application (six to eight months) and the company's Password Protection Policy requirements would be incorporated into user and administrator training for the system.

In addition, quarterly e-mail reminders of the company's Password Protection Policy would be sent out to all employees until such time as a mechanism for enforcing password length and duration on the IPCMS system was implemented.

Suggested information security changes for audit checklist item **G5** were not implemented because management determined that concerns about system performance from the encryption overhead and testing of the new configuration would jeopardize the project's go live date

The control objective for audit step **G5** was to ensure that the database connection between the MySQL server and the IPCMS Portal and Content Management Server was strongly encrypted.

The audit determined that no encryption solution at all had been implemented to secure the MySQL connection between the Database Server and the Portal and Content Management Server.

Because a fix for this vulnerability was not implemented, an attacker could potentially use ARP cache poisoning tools, proxies and sniffers to intercept and/or modify the data stream between the IPCMS system's servers.

The risk to the IPCMS system was determined to be minimal because the servers are attached to the same switch and located in the most secure area on the network. The IPCMS system is also protected by both network and host based intrusion detection systems, which further reduces the risk to the system.

Management has committed to ensuring that a fix for this vulnerability is researched and included in the requirements for the next release of the IPCMS system (six to eight months).

## **Appendix 1 – Nmap Results**

### **IPCMS Portal & Content Management Server:**

```
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-16 17:58 EST
Interesting ports on [removed for security reasons]:
(The 1654 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 2.776 days (since Thu Nov 13 23:21:18 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 6.875 seconds
```

### **IPCMS Database Server:**

```
Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2003-11-16 15:54 EST
Interesting ports on [removed for security reasons]:
(The 1654 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
22/tcp    open  ssh
3306/tcp   open  mysql
10000/tcp  open  snet-sensor-mgmt
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 4.745 days (since Tue Nov 11 22:02:40 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 6.249 seconds
```



## **Appendix 2 – Nessus Results**

### **IPCMS Portal & Content Management Server:**

Nessus Scan Report

-----

#### SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 1
- Number of security warnings found : 13
- Number of security notes found : 15

#### TESTED HOSTS

intwebp5.internal.*[removed for security reasons]* (Security holes found)

#### DETAILS

- + intwebp5.internal.*[IP address removed for security reasons]* :
  - . List of open ports :
    - o ssh (22/tcp) (Security hole found)
    - o http (80/tcp) (Security warnings found)
    - o snet-sensor-mgmt (10000/tcp) (Security warnings found)
    - o general/udp (Security notes found)
    - o general/tcp (Security warnings found)
    - o general/icmp (Security warnings found)
  - . Vulnerability found on port ssh (22/tcp) :

You are running a version of OpenSSH which is older than 3.7.1

Versions older than 3.7.1 are vulnerable to a flaw in the buffer management functions which might allow an attacker to execute arbitrary commands on this host.

An exploit for this issue is rumored to exist.

Note that several distribution patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :

```
rpm -q openssh-server
```

Returns :

```
openssh-server-3.1p1-13 (RedHat 7.x)
openssh-server-3.4p1-7 (RedHat 8.0)
openssh-server-3.5p1-11 (RedHat 9)
```

Solution : Upgrade to OpenSSH 3.7.1

See also :

```
http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2
http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2
```

Risk factor : High

CVE : CAN-2003-0693, CAN-2003-0695

BID : 8628

. Warning found on port ssh (22/tcp)

You are running OpenSSH-portable 3.6.1p1 or older.

If PAM support is enabled, an attacker may use a flaw in this version to determine the existence of a given login name by comparing the times the remote sshd daemon takes to refuse a bad password for a non-existent login compared to the time it takes to refuse a bad password for a valid login.

An attacker may use this flaw to set up a brute force attack against the remote host.

\*\*\* Nessus did not check whether the remote SSH daemon is actually using PAM or not, so this might be a false positive

Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer

Risk Factor : Low

CVE : CAN-2003-0190

BID : 7482, 7467, 7342

. Warning found on port ssh (22/tcp)

You are running OpenSSH-portable 3.6.1 or older.

There is a flaw in this version which may allow an attacker to bypass the access controls set by the administrator of this server.

OpenSSH features a mechanism which can restrict the list of hosts a given user can log from by specifying a pattern in the user key file (ie: \*.mynetwork.com would let a user connect only from the local network).

However there is a flaw in the way OpenSSH does reverse DNS lookups. If an attacker configures his DNS server to send a numeric IP address when a reverse lookup is performed, he may be able to circumvent this mechanism.

Solution : Upgrade to OpenSSH 3.6.2 when it comes out

Risk Factor : Low  
CVE : CAN-2003-0386  
BID : 7831

. Information found on port ssh (22/tcp)

An ssh server is running on this port

. Information found on port ssh (22/tcp)

Remote SSH version : SSH-2.0-OpenSSH\_3.4p1

. Information found on port ssh (22/tcp)

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.99
- . 2.0

. Warning found on port http (80/tcp)

Your webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

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.

If you are using Sun ONE Web Server releases 6.0 SP2 and later, add the following to the default object section in obj.conf:

```
<Client method="TRACE">
  AuthTrans fn="set-variable"
  remove-headers="transfer-encoding"
  set-headers="content-length: -1"
  error="501"
</Client>
```

If you are using Sun ONE Web Server releases 6.0 SP2 or below, compile the NSAPI plugin located at:

<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603>

See [http://www.whitehatsec.com/press\\_releases/WH-PR-20030120.pdf](http://www.whitehatsec.com/press_releases/WH-PR-20030120.pdf)  
<http://archives.neohapsis.com/archives/vulnwatch/2003-q1/0035.html>  
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F50603>  
<http://www.kb.cert.org/vuls/id/867593>

Risk factor : Medium

. Warning found on port http (80/tcp)

The remote host is running a version of PHP which is older than 4.3.2

There is a flaw in this version which may allow an attacker who has the ability to inject an arbitrary argument to the function `socket_iovec_alloc()`

to crash the remote service and possibly to execute arbitrary code.

For this attack to work, PHP has to be compiled with the option `--enable-sockets` (which is disabled by default), and an attacker needs to be able to pass arbitrary values to `socket_iovec_alloc()`.

Other functions are vulnerable to such flaws : `openlog()`, `socket_recv()`, `socket_recvfrom()` and `emalloc()`

Solution : Upgrade to PHP 4.3.2

Risk factor : Low

CVE : CAN-2003-0172

BID : 7187, 7197, 7198, 7199, 7210, 7256, 7259

. Warning found on port http (80/tcp)

The remote host appears to be running a version of Apache 2.x which is older than 2.0.43

This version allows an attacker to view the source code of CGI scripts via a POST request made to a directory with both WebDAV and CGI enabled.

\*\*\* Note that Nessus solely relied on the version number  
\*\*\* of the remote server to issue this warning. This might  
\*\*\* be a false positive

## John Van Hoogstraten \_ GSNA Practical Assignment Version 2.1 \_ Option 1

Solution : Upgrade to version 2.0.43  
See also : [http://www.apache.org/dist/httpd/CHANGES\\_2.0](http://www.apache.org/dist/httpd/CHANGES_2.0)  
Risk factor : Medium  
CVE : CAN-2002-1156, CAN-2003-0083  
BID : 6065

. Warning found on port http (80/tcp)

The remote host appears to be running a version of Apache 2.x which is older than 2.0.48.

This version is vulnerable to a bug which may allow a rogue CGI to disable the httpd service by issuing over 4K of data to stderr.

To exploit this flaw, an attacker would need the ability to upload a rogue CGI script to this server and to have it executed by the Apache daemon (httpd).

Solution : Upgrade to version 2.0.48 when it is available  
See also : [http://nagoya.apache.org/bugzilla/show\\_bug.cgi?id=22030](http://nagoya.apache.org/bugzilla/show_bug.cgi?id=22030)  
Risk factor : Low  
CVE : CVE-2002-0061, CAN-2003-0789, CAN-2003-0542  
BID : 8926

. Warning found on port http (80/tcp)

The remote host is running a version of PHP earlier than 4.2.2.

The mail() function does not properly sanitize user input. This allows users to forge email to make it look like it is coming from a different source other than the server.

Users can exploit this even if SAFE\_MODE is enabled.

Solution : Contact your vendor for the latest PHP release.

Risk factor : Medium  
CVE : CAN-2002-0985  
BID : 5562

. Warning found on port http (80/tcp)

The remote host appears to be running a version of Apache 2.x which is older than 2.0.46

This version is vulnerable to various flaws :

- There is a denial of service vulnerability which may allow an attacker to disable basic authentication on this host
- There is a denial of service vulnerability in the mod\_dav module

which may allow an attacker to crash this service remotely

Solution : Upgrade to version 2.0.46  
See also : [http://www.apache.org/dist/httpd/CHANGES\\_2.0](http://www.apache.org/dist/httpd/CHANGES_2.0)  
Risk factor : Medium  
CVE : CAN-2003-0245, CAN-2003-0189  
BID : 7723, 7725

. Warning found on port http (80/tcp)

The remote host appears to be running a version of  
Apache 2.x which is older than 2.0.45

This version is vulnerable to various flaws :

- There is a denial of service attack which may allow an attacker to disable this server remotely
- The httpd process leaks file descriptors to child processes, such as CGI scripts. An attacker who has the ability to execute arbitrary CGI scripts on this server (including PHP code) would be able to write arbitrary data in the file pointed to (in particular, the log files)

Solution : Upgrade to version 2.0.45  
See also : [http://www.apache.org/dist/httpd/CHANGES\\_2.0](http://www.apache.org/dist/httpd/CHANGES_2.0)  
Risk factor : Medium  
CVE : CAN-2003-0132  
BID : 7254, 7255

. Warning found on port http (80/tcp)

The remote host appears to be running a version of  
Apache 2.x which is older than 2.0.47

This version is vulnerable to various flaws which may allow an attacker to disable this service remotely and/or locally.

Solution : Upgrade to version 2.0.47  
See also : [http://www.apache.org/dist/httpd/CHANGES\\_2.0](http://www.apache.org/dist/httpd/CHANGES_2.0)  
Risk factor : Medium  
CVE : CAN-2003-0192, CAN-2003-0253, CAN-2003-0254  
BID : 8134, 8135, 8137, 8138

. Information found on port http (80/tcp)

A web server is running on this port

. Information found on port http (80/tcp)

The following directories were discovered:  
/cgi-bin, /conf, /core, /docs, /error, /files, /icons, /images, /js, /lib,

/manual, /templates

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

. Information found on port http (80/tcp)

The remote web server type is :

Apache/2.0.40 (Red Hat Linux)

Solution : You can set the directive 'ServerTokens Prod' to limit the information emanating from the server in its response headers.

. Information found on port http (80/tcp)

Nessus was not able to reliably identify this server. It might be: Apache/2.0.48 (Gentoo Linux)

The fingerprint differs from these known signatures on 4 point(s)

If you know what it is, please send this signature to  
www-signatures@nessus.org :

:xxx:200:200:200:200:200:xxx:501:200:200:HTM:xxx:200:400:400:404:405:405:200:200:405:405

and the following banner:

Server: Apache/2.0.40 (Red Hat Linux)

. Warning found on port snet-sensor-mgmt (10000/tcp)

The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack

Solution: disable those ciphers and upgrade your client software if necessary

. Information found on port snet-sensor-mgmt (10000/tcp)

A SSLv2 server answered on this port

## John Van Hoogstraten \_ GSNA Practical Assignment Version 2.1 \_ Option 1

. Information found on port snet-sensor-mgmt (10000/tcp)

A web server is running on this port through SSL

. Information found on port snet-sensor-mgmt (10000/tcp)

Here is the SSLv2 server certificate:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=US, ST=FL, O=Webmin on

intwebp5.internal.[removed for security reasons],

CN=intwebp5.internal.[removed for security reasons]/emailAddress=[removed for security reasons]

Validity

Not Before: Nov 1 15:01:14 2003 GMT

Not After : Oct 30 15:01:14 2008 GMT

Subject: C=US, ST=FL, O=Webmin on intwebp5.internal.[removed for security reasons], CN=intwebp5.internal.[removed for security reasons]/emailAddress=[removed for security reasons]

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (512 bit)

Modulus (512 bit):

00:c1:2c:c0:60:55:07:41:22:29:94:e2:75:1c:db:

44:ee:70:06:66:1e:0f:78:8a:c5:3d:b7:95:d6:84:

2a:f9:f0:5d:c0:22:2c:8d:cf:a8:5c:9e:4d:61:17:

39:8b:44:9c:cf:3b:3b:14:06:9d:a7:6c:12:4f:56:

45:1a:4b:38:49

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

E6:24:39:EE:D1:1C:52:27:D1:29:C5:07:24:8E:F0:B8:72:CF:50:18

X509v3 Authority Key Identifier:

keyid:E6:24:39:EE:D1:1C:52:27:D1:29:C5:07:24:8E:F0:B8:72:CF:50:18

DirName:/C=US/ST=FL/O=Webmin on intwebp5.internal.[removed for security reasons]/CN=intwebp5.internal.[removed for security reasons]/emailAddress=[removed for security reasons]

serial:00

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

6a:f3:db:39:b7:9c:ac:dd:b4:78:9c:e2:81:46:7f:de:a8:22:

ed:99:82:3d:fd:ac:1d:2b:c2:ed:e5:36:62:3f:a9:0b:0a:83:

88:28:97:03:96:a9:b1:88:d9:f5:2f:12:ed:b3:7c:7d:60:f4:

3b:07:1f:99:ff:25:c1:33:cc:2f

. Information found on port snet-sensor-mgmt (10000/tcp)



Here is the list of available SSLv2 ciphers:

RC4-MD5  
EXP-RC4-MD5  
RC2-CBC-MD5  
EXP-RC2-CBC-MD5  
DES-CBC-MD5  
DES-CBC3-MD5  
RC4-64-MD5

. Information found on port snet-sensor-mgmt (10000/tcp)

This SSLv2 server also accepts SSLv3 connections.  
This SSLv2 server also accepts TLSv1 connections.

. Information found on port snet-sensor-mgmt (10000/tcp)

This web server is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map or search page or authentication page instead.

Unfortunately, we were unable to find a way to recognize this page, so some CGI-related checks have been disabled.

To work around this issue, please contact the Nessus team.

. Information found on port snet-sensor-mgmt (10000/tcp)

Nessus was not able to reliably identify this server. It might be:  
AOLserver/4.0  
Gordano Web Server v5.06.0016  
Resin/2.1.9 (Gentoo/Linux)  
The fingerprint differs from these known signatures on 19 point(s)

. Information found on port general/udp

For your information, here is the traceroute to *[removed for security reasons]*  
:  
*[removed for security reasons]*  
*[removed for security reasons]*

. Warning found on port general/tcp

The remote host does not discard TCP SYN packets which have the FIN flag set.

Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.

See also : <http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>  
<http://www.kb.cert.org/vuls/id/464113>

Solution : Contact your vendor for a patch  
Risk factor : Medium  
BID : 7487

. Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk factor : Low  
CVE : CAN-1999-0524

-----  
This file was generated by the Nessus Security Scanner

## **IPCMS Database Server:**

Nessus Scan Report  
-----

### SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 1
- Number of security warnings found : 5
- Number of security notes found : 13

### TESTED HOSTS

intmysqlp2.internal.[removed for security reasons] (Security holes found)

## DETAILS

- ```
+ intmysqlp2.internal.[removed for security reasons] :  
. List of open ports :  
  o ssh (22/tcp) (Security hole found)  
  o mysql (3306/tcp) (Security notes found)  
  o snet-sensor-mgmt (10000/tcp) (Security warnings found)  
  o general/udp (Security notes found)  
  o general/tcp (Security warnings found)  
  o general/icmp (Security warnings found)  
  
. Vulnerability found on port ssh (22/tcp) :
```

You are running a version of OpenSSH which is older than 3.7.1

Versions older than 3.7.1 are vulnerable to a flaw in the buffer management functions which might allow an attacker to execute arbitrary commands on this host.

An exploit for this issue is rumored to exist.

Note that several distributions patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :  
rpm -q openssh-server

Returns :  
openssh-server-3.1p1-13 (RedHat 7.x)  
openssh-server-3.4p1-7 (RedHat 8.0)  
openssh-server-3.5p1-11 (RedHat 9)

Solution : Upgrade to OpenSSH 3.7.1

See also :

<http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2>  
<http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2>

Risk factor : High

CVE : CAN-2003-0693, CAN-2003-0695

BID : 8628

- ```
. Warning found on port ssh (22/tcp)
```

You are running OpenSSH-portable 3.6.1p1 or older.

If PAM support is enabled, an attacker may use a flaw in this version to determine the existence of a given login name by comparing the times the remote sshd daemon takes to refuse a bad password for a non-existent

login compared to the time it takes to refuse a bad password for a valid login.

An attacker may use this flaw to set up a brute force attack against the remote host.

\*\*\* Nessus did not check whether the remote SSH daemon is actually using PAM or not, so this might be a false positive

Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer

Risk Factor : Low

CVE : CAN-2003-0190

BID : 7482, 7467, 7342

. Warning found on port ssh (22/tcp)

You are running OpenSSH-portable 3.6.1 or older.

There is a flaw in this version which may allow an attacker to bypass the access controls set by the administrator of this server.

OpenSSH features a mechanism which can restrict the list of hosts a given user can log from by specifying a pattern in the user key file (ie: \*.mynetwork.com would let a user connect only from the local network).

However there is a flaw in the way OpenSSH does reverse DNS lookups. If an attacker configures his DNS server to send a numeric IP address when a reverse lookup is performed, he may be able to circumvent this mechanism.

Solution : Upgrade to OpenSSH 3.6.2 when it comes out

Risk Factor : Low

CVE : CAN-2003-0386

BID : 7831

. Information found on port ssh (22/tcp)

An ssh server is running on this port

. Information found on port ssh (22/tcp)

Remote SSH version : SSH-2.0-OpenSSH\_3.4p1

. Information found on port ssh (22/tcp)

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.99
- . 2.0

- . Information found on port mysql (3306/tcp)

An unknown service is running on this port.  
It is usually reserved for MySQL

- . Information found on port mysql (3306/tcp)

Remote MySQL version : 3.23.58

- . Warning found on port snet-sensor-mgmt (10000/tcp)

The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack

Solution: disable those ciphers and upgrade your client software if necessary

- . Information found on port snet-sensor-mgmt (10000/tcp)

A SSLv2 server answered on this port

- . Information found on port snet-sensor-mgmt (10000/tcp)

A web server is running on this port through SSL

- . Information found on port snet-sensor-mgmt (10000/tcp)

Here is the SSLv2 server certificate:

Certificate:

Data:

Version: 3 (0x2)  
Serial Number: 0 (0x0)  
Signature Algorithm: md5WithRSAEncryption  
Issuer: C=US, ST=Florida, O=Webmin Webserver on  
intmysqlp2.internal.*[removed for security reasons]*,  
CN=intmysqlp2/emailAddress=*[removed for security reasons]*  
Validity  
Not Before: Oct 26 19:48:10 2003 GMT  
Not After : Oct 24 19:48:10 2008 GMT  
Subject: C=US, ST=Florida, O=Webmin Webserver on  
intmysqlp2.internal.*[removed for security reasons]*,  
CN=intmysqlp2/emailAddress=*[removed for security reasons]*  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
RSA Public Key: (512 bit)  
Modulus (512 bit):

## John Van Hoogstraten \_ GSNA Practical Assignment Version 2.1 \_ Option 1

```
00:9d:5f:7f:c0:9b:0f:b3:aa:d3:e4:d8:6b:36:f1:
30:12:32:5e:3a:15:78:f3:e3:3a:d2:50:e4:f8:e3:
45:15:62:cc:73:43:5b:89:d5:ed:31:41:83:0f:f3:
f4:fe:2b:f6:ba:9c:3c:9c:df:6c:65:21:84:f5:e6:
84:8f:2d:57:2d
Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Subject Key Identifier:
    3F:CF:18:22:E2:2F:FC:1E:6D:B1:5D:AC:7D:CF:72:42:B0:8D:F6:37
  X509v3 Authority Key Identifier:

keyid:3F:CF:18:22:E2:2F:FC:1E:6D:B1:5D:AC:7D:CF:72:42:B0:8D:F6:37
  DirName:/C=US/ST=Florida/O=Webmin Webserver on
  intmysqlp2.internal.[removed for security
reasons]/CN=intmysqlp2/emailAddress=[removed for security reasons]
  serial:00

X509v3 Basic Constraints:
  CA:TRUE
Signature Algorithm: md5WithRSAEncryption
  98:c7:51:c4:f5:5d:50:f6:5b:a7:98:3c:9f:8b:cc:1c:0d:61:
  47:67:43:eb:1b:33:8b:5b:cb:f5:5f:36:98:61:42:e7:8d:06:
  e6:e1:6a:8c:90:4d:f1:45:90:7d:cc:52:8c:2f:81:82:a1:47:
  b2:f8:3f:2d:43:6c:1c:03:80:be
```

. Information found on port snet-sensor-mgmt (10000/tcp)

Here is the list of available SSLv2 ciphers:

```
RC4-MD5
EXP-RC4-MD5
RC2-CBC-MD5
EXP-RC2-CBC-MD5
DES-CBC-MD5
DES-CBC3-MD5
RC4-64-MD5
```

. Information found on port snet-sensor-mgmt (10000/tcp)

This SSLv2 server also accepts SSLv3 connections.  
This SSLv2 server also accepts TLSv1 connections.

. Information found on port snet-sensor-mgmt (10000/tcp)

This web server is [mis]configured in that it does not return '404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map or search page or authentication page instead.

Unfortunately, we were unable to find a way to recognize this page, so some CGI-related checks have been disabled.

To work around this issue, please contact the Nessus team.

- . Information found on port snet-sensor-mgmt (10000/tcp)

Nessus was not able to reliably identify this server. It might be:  
AOLserver/4.0  
Gordano Web Server v5.06.0016  
Resin/2.1.9 (Gentoo/Linux)  
The fingerprint differs from these known signatures on 19 point(s)

- . Information found on port general/udp

For your information, here is the traceroute to *[removed for security reasons]*  
:  
*[removed for security reasons]*  
*[removed for security reasons]*

- . Warning found on port general/tcp

The remote host does not discard TCP SYN packets which have the FIN flag set.

Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.

See also : <http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>  
<http://www.kb.cert.org/vuls/id/464113>

Solution : Contact your vendor for a patch  
Risk factor : Medium  
BID : 7487

- . Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk factor : Low

CVE : CAN-1999-0524

-----  
This file was generated by the Nessus Security Scanner

© SANS Institute 2003, Author retains full rights.



## **Appendix 3 – Nessus Retest Results**

### **IPCMS Portal & Content Management Server:**

Nessus Scan Report

-----

#### SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 1
- Number of security warnings found : 5
- Number of security notes found : 13

#### TESTED HOSTS

intwebp5.internal.*[removed for security reasons]* (Security holes found)

#### DETAILS

- + intwebp5.internal.*[removed for security reasons]* :
  - . List of open ports :
    - o ssh (22/tcp) (Security hole found)
    - o http (80/tcp) (Security notes found)
    - o snet-sensor-mgmt (10000/tcp) (Security warnings found)
    - o general/udp (Security notes found)
    - o general/tcp (Security warnings found)
    - o general/icmp (Security warnings found)
  - . Vulnerability found on port ssh (22/tcp) :

You are running a version of OpenSSH which is older than 3.7.1

Versions older than 3.7.1 are vulnerable to a flaw in the buffer management functions which might allow an attacker to execute arbitrary commands on this host.

An exploit for this issue is rumored to exist.

Note that several distribution patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :

```
rpm -q openssh-server
```

Returns :

```
openssh-server-3.1p1-13 (RedHat 7.x)
openssh-server-3.4p1-7 (RedHat 8.0)
openssh-server-3.5p1-11 (RedHat 9)
```

Solution : Upgrade to OpenSSH 3.7.1

See also :

```
http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2
http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2
```

Risk factor : High

CVE : CAN-2003-0693, CAN-2003-0695

BID : 8628

. Warning found on port ssh (22/tcp)

You are running OpenSSH-portable 3.6.1p1 or older.

If PAM support is enabled, an attacker may use a flaw in this version to determine the existence of a given login name by comparing the times the remote sshd daemon takes to refuse a bad password for a non-existent login compared to the time it takes to refuse a bad password for a valid login.

An attacker may use this flaw to set up a brute force attack against the remote host.

\*\*\* Nessus did not check whether the remote SSH daemon is actually using PAM or not, so this might be a false positive

Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer

Risk Factor : Low

CVE : CAN-2003-0190

BID : 7482, 7467, 7342

. Warning found on port ssh (22/tcp)

You are running OpenSSH-portable 3.6.1 or older.

There is a flaw in this version which may allow an attacker to bypass the access controls set by the administrator of this server.

OpenSSH features a mechanism which can restrict the list of hosts a given user can log from by specifying a pattern in the user key file (ie: \*.mynetwork.com would let a user connect only from the local network).

However there is a flaw in the way OpenSSH does reverse DNS lookups. If an attacker configures his DNS server to send a numeric IP address when a reverse lookup is performed, he may be able to circumvent this mechanism.

Solution : Upgrade to OpenSSH 3.6.2 when it comes out

## John Van Hoogstraten \_ GSNA Practical Assignment Version 2.1 \_ Option 1

Risk Factor : Low  
CVE : CAN-2003-0386  
BID : 7831

. Information found on port ssh (22/tcp)

An ssh server is running on this port

. Information found on port ssh (22/tcp)

Remote SSH version : SSH-2.0-OpenSSH\_3.4p1

. Information found on port ssh (22/tcp)

The remote SSH daemon supports the following versions of the SSH protocol :

- . 1.99
- . 2.0

. Information found on port http (80/tcp)

An unknown service is running on this port.  
It is usually reserved for HTTP

. Information found on port http (80/tcp)

A web server seems to be running on this port

. Information found on port http (80/tcp)

The following directories were discovered:

/cgi-bin, /conf, /core, /docs, /error, /files, /icons, /images, /js, /lib,  
/manual, /templates

While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

. Information found on port http (80/tcp)

Nessus was not able to reliably identify this server. It might be:  
Apache/2.0.48 (Unix) Debian GNU/Linux  
The fingerprint differs from these known signatures on 9 point(s)

. Warning found on port snet-sensor-mgmt (10000/tcp)

The SSLv2 server offers 5 strong ciphers, but also 0 medium strength and 2 weak "export class" ciphers. The weak/medium ciphers may be chosen by an export-grade or badly configured client software. They only offer a limited protection against a brute force attack

Solution: disable those ciphers and upgrade your client software if necessary

- . Information found on port snet-sensor-mgmt (10000/tcp)

A SSLv2 server answered on this port

- . Information found on port snet-sensor-mgmt (10000/tcp)

Here is the SSLv2 server certificate:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=US, ST=FL, O=Webmin on

intwebp5.internal.*[removed for security reasons]*,

CN=intwebp5.internal.*[removed for security reasons]*/emailAddress=*[removed for security reasons]*

Validity

Not Before: Nov 1 15:01:14 2003 GMT

Not After : Oct 30 15:01:14 2008 GMT

Subject: C=US, ST=FL, O=Webmin on intwebp5.internal.*[removed for security reasons]*, CN=intwebp5.internal.*[removed for security reasons]*/emailAddress=*[removed for security reasons]*

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (512 bit)

Modulus (512 bit):

00:c1:2c:c0:60:55:07:41:22:29:94:e2:75:1c:db:

44:ee:70:06:66:1e:0f:78:8a:c5:3d:b7:95:d6:84:

2a:f9:f0:5d:c0:22:2c:8d:cf:a8:5c:9e:4d:61:17:

39:8b:44:9c:cf:3b:3b:14:06:9d:a7:6c:12:4f:56:

45:1a:4b:38:49

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

E6:24:39:EE:D1:1C:52:27:D1:29:C5:07:24:8E:F0:B8:72:CF:50:18

X509v3 Authority Key Identifier:

keyid:E6:24:39:EE:D1:1C:52:27:D1:29:C5:07:24:8E:F0:B8:72:CF:50:18

DirName:/C=US/ST=FL/O=Webmin on intwebp5.internal.v*[removed for security reasons]*/CN=intwebp5.internal.*[removed for security reasons]*/emailAddress=*[removed for security reasons]*

serial:00

X509v3 Basic Constraints:

CA:TRUE

## John Van Hoogstraten \_ GSNA Practical Assignment Version 2.1 \_ Option 1

Signature Algorithm: md5WithRSAEncryption

6a:f3:db:39:b7:9c:ac:dd:b4:78:9c:e2:81:46:7f:de:a8:22:  
ed:99:82:3d:fd:ac:1d:2b:c2:ed:e5:36:62:3f:a9:0b:0a:83:  
88:28:97:03:96:a9:b1:88:d9:f5:2f:12:ed:b3:7c:7d:60:f4:  
3b:07:1f:99:ff:25:c1:33:cc:2f

. Information found on port snet-sensor-mgmt (10000/tcp)

Here is the list of available SSLv2 ciphers:

RC4-MD5  
EXP-RC4-MD5  
RC2-CBC-MD5  
EXP-RC2-CBC-MD5  
DES-CBC-MD5  
DES-CBC3-MD5  
RC4-64-MD5

. Information found on port snet-sensor-mgmt (10000/tcp)

This SSLv2 server also accepts SSLv3 connections.  
This SSLv2 server also accepts TLSv1 connections.

. Information found on port snet-sensor-mgmt (10000/tcp)

This port was detected as being open by a port scanner but is now closed.  
This service might have been crashed by a port scanner or by a plugin

. Information found on port general/udp

For your information, here is the traceroute to *[removed for security reasons]*:  
*[removed for security reasons]*  
?  
*[removed for security reasons]*

. Warning found on port general/tcp

The remote host does not discard TCP SYN packets which  
have the FIN flag set.

Depending on the kind of firewall you are using, an  
attacker may use this flaw to bypass its rules.

See also : <http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>  
<http://www.kb.cert.org/vuls/id/464113>

Solution : Contact your vendor for a patch

Risk factor : Medium

BID : 7487

. Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk factor : Low

CVE : CAN-1999-0524

-----  
This file was generated by the Nessus Security Scanner

## **IPCMS Database Server:**

Nessus Scan Report

### SUMMARY

- Number of hosts which were alive during the test : 1
- Number of security holes found : 1
- Number of security warnings found : 4
- Number of security notes found : 4

### TESTED HOSTS

intmysqlp2.internal.[removed for security reasons] (Security holes found)

### DETAILS

+ intmysqlp2.internal.[removed for security reasons] :  
. List of open ports :

- o ssh (22/tcp) (Security hole found)
- o mysql (3306/tcp) (Security notes found)

- o snet-sensor-mgmt (10000/tcp)
  - o general/udp (Security notes found)
  - o general/tcp (Security warnings found)
  - o general/icmp (Security warnings found)
- . Vulnerability found on port ssh (22/tcp) :

You are running a version of OpenSSH which is older than 3.7.1

Versions older than 3.7.1 are vulnerable to a flaw in the buffer management functions which might allow an attacker to execute arbitrary commands on this host.

An exploit for this issue is rumored to exist.

Note that several distribution patched this hole without changing the version number of OpenSSH. Since Nessus solely relied on the banner of the remote SSH server to perform this check, this might be a false positive.

If you are running a RedHat host, make sure that the command :  
rpm -q openssh-server

Returns :

openssh-server-3.1p1-13 (RedHat 7.x)  
openssh-server-3.4p1-7 (RedHat 8.0)  
openssh-server-3.5p1-11 (RedHat 9)

Solution : Upgrade to OpenSSH 3.7.1

See also :

<http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375452423794&w=2>  
<http://marc.theaimsgroup.com/?l=openbsd-misc&m=106375456923804&w=2>

Risk factor : High

CVE : CAN-2003-0693, CAN-2003-0695

BID : 8628

- . Warning found on port ssh (22/tcp)

You are running OpenSSH-portable 3.6.1p1 or older.

If PAM support is enabled, an attacker may use a flaw in this version to determine the existence of a given login name by comparing the times the remote sshd daemon takes to refuse a bad password for a non-existent login compared to the time it takes to refuse a bad password for a valid login.

An attacker may use this flaw to set up a brute force attack against the remote host.

\*\*\* Nessus did not check whether the remote SSH daemon is actually  
\*\*\* using PAM or not, so this might be a false positive

## John Van Hoogstraten \_ GSNA Practical Assignment Version 2.1 \_ Option 1

Solution : Upgrade to OpenSSH-portable 3.6.1p2 or newer  
Risk Factor : Low  
CVE : CAN-2003-0190  
BID : 7482, 7467, 7342

. Warning found on port ssh (22/tcp)

You are running OpenSSH-portable 3.6.1 or older.

There is a flaw in this version which may allow an attacker to bypass the access controls set by the administrator of this server.

OpenSSH features a mechanism which can restrict the list of hosts a given user can log from by specifying a pattern in the user key file (ie: \*.mynetwork.com would let a user connect only from the local network).

However there is a flaw in the way OpenSSH does reverse DNS lookups. If an attacker configures his DNS server to send a numeric IP address when a reverse lookup is performed, he may be able to circumvent this mechanism.

Solution : Upgrade to OpenSSH 3.6.2 when it comes out  
Risk Factor : Low  
CVE : CAN-2003-0386  
BID : 7831

. Information found on port ssh (22/tcp)

An ssh server is running on this port

. Information found on port ssh (22/tcp)

Remote SSH version : SSH-2.0-OpenSSH\_3.4p1

. Information found on port mysql (3306/tcp)

An unknown service is running on this port.  
It is usually reserved for MySQL

. Information found on port general/udp

For your information, here is the traceroute to [removed for security reasons]:  
[removed for security reasons]  
[removed for security reasons]

. Warning found on port general/tcp

The remote host does not discard TCP SYN packets which



have the FIN flag set.

Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules.

See also : <http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html>  
<http://www.kb.cert.org/vuls/id/464113>

Solution : Contact your vendor for a patch

Risk factor : Medium

BID : 7487

. Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentication protocols.

Solution : filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

Risk factor : Low

CVE : CAN-1999-0524

-----  
This file was generated by the Nessus Security Scanner

© SANS Institute 2003, Author retains full rights.

## **References**

### ***Books & Documents***

- [1] Bauer, Michael D. – Building Secure Servers with Linux – O'Reilly, October 2002 – ISBN: 0-596-00217-3
- [2] Barrett, Daniel J. Byrnes, Robert G. & Silverman, Richard – Linux Security Cookbook – O'Reilly, June 2003 – ISBN: 0-596-00391-9
- [3] King, Tim Reese, George & Yarger, Randy Jay – Managing and Using MySQL, 2nd Edition – O'Reilly, April 2002 – ISBN: 0-596-00211-4
- [4] Garfinkel, Simson Schwartz, Alan & Spafford, Gene – Practical UNIX and Internet Security, 3<sup>rd</sup> Edition – O'Reilly, February 2003 – ISBN: 0-596-00323-4
- [5] Garfinkel, Simson – Web Security, Privacy & Commerce, 2nd Edition – O'Reilly, November 2001 – ISBN: 0-596-00045-6
- [6] DuBois, Paul – MySQL, Second Edition – Que, January 2003 – ISBN: 0-7357-1212-3
- [7] Cameron, Jamie – Managing Linux Systems with Webmin: System Administration and Module Development – Prentice Hall, August 2003 – ISBN: 0-131-40882-8

### ***Web Sites & Resources***

- [1] U.S. Department of Transportation, Office of the Secretary – Server Security Checklist – [http://cio.ost.dot.gov/it\\_security/server\\_checklist.doc](http://cio.ost.dot.gov/it_security/server_checklist.doc)
- [2] National Institute of Standards and Technology, Computer Security Resource Center (CSRC) – NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems – <http://csrc.nist.gov/publications/drafts.html>
- [3] Kaplan, Jim – AuditNet – <http://www.auditnet.org/>
- [4] Global Information Assurance Certification – GCUX (UNIX Security Administrator) Posted Practicals – <http://www.giac.org/GCUX.php>
- [5] Global Information Assurance Certification – GSNA (GIAC Systems and Network Auditor) Posted Practicals – <http://www.giac.org/GSNA.php>
- [6] SANS Institute – Security Consensus Operational Readiness Evaluation (S.C.O.R.E) – <http://www.sans.org/score/>

[7] SANS Institute – The Twenty Most Critical Internet Security Vulnerabilities (Updated) – <http://www.sans.org/top20/>

[8] The Institute of Internal Auditors – ITAudit – <http://www.theiia.org/itaudit/>

© SANS Institute 2003, Author retains full rights.