Global Information Assurance Certification Paper

Auditing a CacheFlow Proxy Solution: An Auditors Perspective

Option 1

GSNA Practical Assignment
Version 2.1 (amended July 5 2002)

Author: Leigh Haig
Completion Date: 4 July 2003

Table of Contents

Table of Figures

Abstract

Web access is a large requirement for most Internet connected companies. In connecting to the Internet, it is important for companies to ensure that their internal network and IP address space is not advertised over the Internet. To facilitate secure connectivity to the Internet and for efficiencies, many companies deploy proxy devices.

The purpose of this paper is to review and audit one proxy device available that provides a means of accessing the World Wide Web for a large corporation. The CacheFlow product is one such device capable of providing this type of Internet connectivity.

Assignment 1

Identify the system to be audited

LaP Engineering is a multinational corporation that utilises proxy devices to connect to the Internet. When proxy devices are used, systems (PC's, servers etc) are configured to direct all web browser traffic to the proxy device for dispatch to the Internet. The return traffic will then come back to the system via the proxy device. In this way, the Internet does not know anything about LaP's internal IP addresses. Furthermore, this results in a minimal number of ports being opened on LaP's firewall, thus reducing the number of points for an attack.

The audit detailed in this paper will cover the equipment used by LaP as their proxy device, a CacheFlow 525i. The overall web access configuration also includes two Cisco routers, which provide the link between the Internet and the Intranet. At the time of writing, the web browser used by LaP is Microsoft Internet Explorer 6.0. The below diagram illustrates this environment.

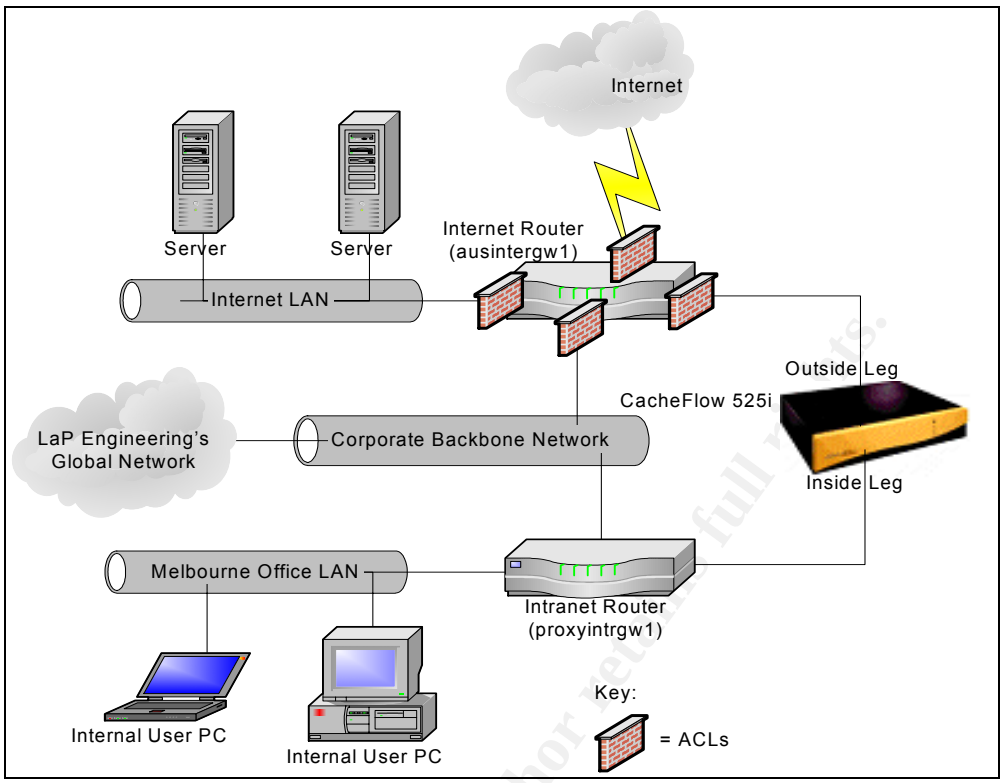

Figure 1: Network Diagram

The routers, web browser, computers used by LaP employees, and the infrastructure and service provided by the ISP are not within the scope of this audit. This information has only been provided to give the complete overview of the environment used within the company.

CacheFlow

The CacheFlow is a proxy device that was first released by CacheFlow Corporation[1]. LaP uses the multi legged CacheFlow 525i, meaning it has multiple Ethernet interfaces. In the LaP configuration, two of these interfaces (legs) are used - an *inside leg* connects to the intranet, whilst an *outside leg* provides the link to the Internet. The 525i also comes with ~17GB of disk storage (two by 8.54GB drives), 384MB of RAM, and provides a WAN throughput of 2 – 10MB[2]. This device has three DNS entries, one for each of the interfaces (aus-cf-int.au.lap.com for the internal (inside) leg, and aus-cf-ext.au.lap.com for the external (outside) leg) and ausproxy.lap.com.au, which is the hostname associated with the Internet routable IP address of the CacheFlow[3]. Unless

[1] CacheFlow Corporation officially changed its name to Blue Coat Systems on August 21, 2002. http://www.bluecoat.com/news/releases/2002/082102_cflo_2bcs.html

[2] As described in the CacheFlow 500 data sheet: http://www.consulintel.es/Html/Productos/Cacheflow/DataSheets/cf500_data.pdf

[3] The 'Internet Router' performs Network Address Translation. The IP associated with the 'outside leg' is not an Internet routable IP. As such, this router will translate any traffic from this IP into an IP address assigned by the ISP used by LaP. This has not been done as a security measure.

specifically referring to the external interface, the name aus-cf-int will be used when specifying the CacheFlow in general.

Aus-cf-int runs the patented CacheOS™ embedded software, version CA 4.1.09. When connected to the CacheFlow via a telnet connection, the CacheOS™ has a feel very akin to Cisco's IOS. CacheOS™ has been written and designed by CacheFlow Corporation for the express purpose of optimizing the performance offered by a caching device. This is done through DNS Caching, Object Pipelining, Transparent Caching and Active Caching. For further details on each of these, refer to "http://www.cacheflow.com/files/installguides/cf500ecins.pdf", pages four and five.

The CacheFlow has a show version command, the results of which are included here for reference.

```
aus-cf-int>show version
Version: CA 4.1.09
Release id: 18366
Backplane PIC: not applicable on this platform
Serial number: <removed>
NIC 0 MAC: <removed>
aus-cf-int >exit
```

Figure 2: Show version from the CacheFlow

A proxy device offers several advantages for any corporation:

1. Reduces the number of systems that are open to the Internet. The advantage of this is that all effort to maximize the security of the entry points into the company can be focused on these few devices. This minimizes the number of access points between the Internet and the local intranet.
2. A cost reduction in Internet access. A large advantage of the proxy server is to cache previously accessed devices, thus resulting in subsequent requests for the same site being retrieved from the cache, and not from the web site. The cost reduction comes where the ISP, through which your organization links to the Internet, charges per megabyte (or equivalent 'unit' of traffic) of download. The caching of web sites reduces the amount of traffic that must traverse this link.
3. Performance improvement. If a web site can be retrieved from the proxy and does not have to be downloaded from the Internet, the end users can expect improved performance.

The CacheFlow assists with each of the above. The 525i model with the two interfaces allows one interface to be Internet accessible, while the other is connected directly to the intranet. This is the model adopted by LaP.

Evaluate the risk to the system

One of the largest information security risks to any organization comes from the Internet - “Internet access opens the way to Web-based threats such as Web viruses and malicious code which can infect the entire network.”[4] Consequently, any computer systems that provide a link to the Internet and are therefore Internet accessible are at risk of an attack. As the CacheFlow forms a gateway between the organizations intranet and the highly insecure Internet, it too is at risk.

Within LaP Engineering, security reviews of Internet facing servers are carried out frequently. This covers aspects such as application security, patch management and account configuration. But the CacheFlow, whilst also being Internet facing, is very rarely reviewed from a security perspective. Since its installation in 2000, several security or OS upgrades have been applied but no further security measures, such as a thorough audit, have been conducted.

The CacheFlow is accessible by all LaP employees, but is used primarily by its Australian and New Zealand staff. As it is open to approximately 1000 internal users, there is considerable risk from not only the Internet, but also LaP’s intranet. In the event of staff retrenchment or dissatisfaction, the opportunity for vengeful action from the intranet becomes a large issue. Based on this double source of threat, the audit will need to focus on the two interfaces of the CacheFlow, assessing the risk from Internet sources, and internal users.

LaP Engineering is taking some measures against threat from the Internet by using Access Control Lists on the routers that connect it to the Internet. This provides a rudimentary filtering of traffic between the CacheFlow and the Internet. However, as figure 1 depicts, there are no restrictions in place between the LaP intranet and the CacheFlow, hence it can be a prime target for malicious activity from disgruntled LaP employees.

LaP has an acceptable use policy that governs the use of the Internet by its employees. As the CacheFlow is the means for staff to access the Internet, there is the very real potential that the staff will abuse it. To ensure that this abuse can be minimized, the CacheFlow needs to contain the mechanism to restrict access as deemed appropriate by LaP management, and review the access that has been made.

Finally, there is the risk of unauthorised access and configuration changes to the CacheFlow. Should this occur, Internet connectivity could be lost, or even worse, misconfiguration may allow external sources to use the CacheFlow as a proxy server into the LaP intranet. This would allow the exposure of business sensitive information, greatly impacting the brand image of LaP, and presenting the potential for loss of company plans and directions.

[4] http://www.bluecoat.com/products/sg400/index.html

What is the current state of practice, if any?

Research indicates that the security of the proxy device is one that does not receive the attention it warrants. The tools and details for auditing routers and firewalls are quite pervasive (with tools such as CI Securities Router Audit Toolkit, and the NSA Router Security Configuration Guide), but the author's research did not find much evidence of proxy audit information. This could be largely due to the various types of proxy devices that exist today, and the differences between these.

Where a proxy application is run on a widely available operating system such as UNIX, Linux or Windows, this aspect of the proxy server can be audited, for which techniques exist. This would then just leave the application itself, for which basic tests could be performed. Things this would cover could be use of passwords, level of logging the application performs, etc. With the CacheFlow, it is a single device that includes the hardware it runs on, the operating system that powers it, and also the application that performs the actual proxying and caching.

Some sites that were consulted in reviewing the current state of practice were:

- SANS Reading Room (http://rr.sans.org)
- SANS Posted Practicals for GIAC Systems and Network Auditor (GSNA) – (http://www.giac.org/GSNA.php)
- The website for ISACA (Information Systems Audit and Control Association – www.isaca.org)
- The Center for Internet Security (http://www.cisecurity.com)
- Google (www.google.com). For this site, some of the searches performed were using the keywords "proxy servers", "proxy server audit", "audit proxy server", and "CacheFlow audit".

From these searches, it was very hard to find anything specific to the CacheFlow, or auditing of a proxy server in general.

Assignment 2

This assignment will detail the checklist to be used in the audit of LaP Engineering's Internet proxy device, the CacheFlow 525i.

Objectives

The primary objective of this audit is to analyse the security risk and exposure for LaP Engineering with the setup of their World Wide Web proxy solution. The design set forth by LaP is already actively used, so it is important that the configuration of the CacheFlow prevents any security risk. But as the solution is already in use, care needs to be taken so as to not disrupt the Internet access whilst the audit is conducted.

To minimize the potential impact to the organization, all tests against the infrastructure will be done during non-office hours and will follow the company's change management process. The support teams involved with the proxy solution will be made aware of the tests being conducted, and provided the contact details of the person conducting these tests, thus ensuring any negative impact or result can halt further testing and be promptly addressed by the relevant persons.

Secondary to the security aspect, the audit will determine the ability of the CacheFlow to be used to assist with the enforcement of LaP's general 'acceptable use' policy[5].

Scope

The audit of LaP will primarily focus on the security aspect of the web browsing solution used by LaP Engineering. While this audit focuses on the CacheFlow device that is used by LaP, it is recommended that a thorough review of the entire web access solution including the routers and associated network devices be conducted in the future. There will be a brief review of the visibility of the LaP CacheFlow to the Internet, and an examination of the measures taken to safe guard it from attack or any unauthorised use.

While the audit will be focused on how the CacheFlow is configured and used within LaP, the ability to incorporate best practices will be included. Doing this will highlight the areas where LaP IT staff need to manually increase the efforts they apply, and not rely on the minimum requirements allowed by the CacheFlow. It may also help to identify 'quick wins' for LaP – items that can be modified for minimal effort that provide large security gains.

Audit Checklist

The checklist that will be used to perform the audit is detailed below. For each checklist item, the following fields are provided:

- **Identifier:** *The unique identifier for this particular test. This will allow the correlation between the checklist item, and the results as depicted in Assignment 3.*
- **Reference:** *The source of this checklist item.*
- **Control Objective:** *The purpose for this particular test, and what it is designed to achieve.*
- **Risk:** *This will contain three sections:*
    - **Description:** *A brief overview of the type of risk that is posed by this area not being managed at an adequate level.*
    - **Likelihood:** *This will examine the potential that this weakness or threat can be exploited.*
    - **Impact:** *This gives a rating as to the impact if the weakness or threat can be exploited.*

[5] See Appendix A: LaP Employee Business Conduct

For both Impact and Likelihood, three classifications will be used: High, Medium and Low.

- **Compliance:** *The expected result of the audit that would see the item as not being a concern for the organization.*
- **Testing:** *The method to be used in this checklist item to perform the desired test.*
- **Subjective/Objective:** *Indicates the type of test that the checklist item performs.*

Any actual commands that need to be input to allow the test to be conducted will be marked in **bold** to make them easily identifiable. Any parameters that are required as part of the command line will be in ***bold italics***.

Note: A Windows XP computer will be used to conduct all tests in Assignment 3. As such, some of the checklist items below will be written with steps based around the use of the Windows XP operating system.

A: CacheFlow Login Access Controls

Identifier	CLI-A.1
Reference	1. CacheFlow installation/configuration documentation: http://www.cacheflow.com/files/installguides/cf500ecins.pdf 2. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	To determine if access to the CacheFlow is using a unique per user login.
Risk	Description: For purposes of auditability it is important to be able to identify who has been logged on to the CacheFlow making changes. Without using unique user accounts, it is very difficult to identify who may have been logged in at any given time. It also means that if one person from the knowledge community leaves, rather than deleting that person's account, the master account password needs to be modified and communicated to all appropriate staff. This in itself presents the opportunity for the password to be inadvertently disclosed. Likelihood: Low Impact: Medium
Compliance	The configuration of the CacheFlow will ensure that each administrator accesses the device with a unique login name and password. A generic account will not be used.
Testing	Interview CacheFlow administrator to identify if the CacheFlow login is a shared amongst administrators. Login to the CacheFlow and review the configuration: o Enter URL http://ausproxy.lap.com.au:8081/ into a web browser of a computer connected to the intranet. o Once the page has loaded, select **'Management'**, the second

	option in the list. o Login to the CacheFlow providing the 'User name' and 'Password'. o From the Management page, select the sixth option, **'Security'**. o Review the login configuration details on the '**Account**' tab. o Review the selected information from the '**External**' tab.
Subjective/Objective	Objective: review of the CacheFlow configuration. Subjective: interview with the CacheFlow support team.

Identifier	CLI-A.2a
Reference	1. CacheFlow installation/configuration documentation: http://www.cacheflow.com/files/installguides/cf500ecins.pdf 2. Company password policy and standard documentation – see Appendix B.
Control Objective	Test that authorization is required for remote telnet login access to the CacheFlow.
Risk	Description: Unauthenticated access to the CacheFlow would allow unintentional or malicious configuration changes, or information disclosure. This could result in sensitive information about the organization being stolen, or configuration changes that would result in Internet connectivity being lost or opened up fully, with the risk of Internet initiated connections being able to access the LaP Intranet. Likelihood: Medium Impact: High
Compliance	Authorisation (username and password) is required before administrative access can be attained.
Testing	o Open a DOS prompt on an intranet connected machine, and enter the command **telnet *aus-cf-int.au.lap.com***. o Observe the telnet session to see if a login is required. o Try and login to the CacheFlow with a blank username and password. o Observe and record the results.
Subjective/Objective	Objective.

Identifier	CLI-A.2b
Reference	1. CacheFlow installation/configuration documentation: http://www.cacheflow.com/files/installguides/cf500ecins.pdf 2. Company password policy and standard documentation – see Appendix B.
Control Objective	Test that authorization is required for remote web browser login access to the CacheFlow.
Risk	Description: Unauthenticated access to the CacheFlow would allow unintentional or malicious configuration changes, or information disclosure. This could result in sensitive information

	about the organization being stolen, or configuration changes that would result in Internet connectivity being lost or opened up fully, with the risk of Internet initiated connections being able to access the LaP Intranet. Likelihood: Medium Impact: High
Compliance	Authorisation (username and password) is required before administrative access can be attained.
Testing	o Enter URL http://ausproxy.lap.com.au:8081/ into a web browser of a computer connected to the intranet. o Once the page has loaded, select **'Management'**, the second option in the list. o Attempt to login by pressing the OK button with the 'User name:' and 'Password:' fields blank.
Subjective/Objective	Objective

Identifier	CLI-A.2c
Reference	1. CacheFlow installation/configuration documentation: http://www.cacheflow.com/files/installguides/cf500ecins.pdf 2. Company password policy and standard documentation – see Appendix B.
Control Objective	Test that authorization is required for local console access to the CacheFlow.
Risk	Description: Unauthenticated access to the CacheFlow would allow unintentional or malicious configuration changes, or information disclosure. This could result in sensitive information about the organization being stolen, or configuration changes that would result in Internet connectivity being lost or opened up fully, with the risk of Internet initiated connections being able to access the LaP Intranet. Likelihood: Low Impact: High
Compliance	Authorisation (username and password) is required before administrative access can be attained.
Testing	o Connect a computer to the CacheFlow 525i with a serial cable between the devices serial ports. o Open terminal emulation software, and select the serial connection option o Observe the output of the emulation software to see if a username and/or password is required. o Try and login to the CacheFlow using a blank username and password.
Subjective/Objective	Objective.

Identifier	CLI-A.3
Reference	1. Company password policy and standard documentation –

	see Appendix B. 2. CacheFlow installation/configuration documentation: http://www.cacheflow.com/files/installguides/cf500ecins.pdf 3. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	Test to ensure the administrator password is configured to meet the LaP password policy. This will cover the following: - Configuration for complexity; - Minimum length; - Minimum and maximum ageing; - History of previous passwords;
Risk	Description: A weak or poorly configured password offers minimal protection to a device. If the password can be easily defeated, unauthorised access to the system is possible. This can result in the loss of sensitive configuration information, or can be used to make system changes creating a Denial of Service attack or an increase in web flow activity, voiding restrictions that should be in place. Likelihood: Medium Impact: High
Compliance	All items listed under Control Objective need to adhere to the requirements for LaP as detailed in its password policy and standard documents[6].
Testing	The password used to access the system will be compared against the password policy and standard document to check that it is meeting these requirements. The support personnel will be interviewed to see if password aging and history is in place, and meeting the policy and standards. A further test will be done where a blank or easily guessable password will be entered as the new password, to see if the CacheFlow will accept it. This will be conducted only from an intranet web connection to the CacheFlow. To perform this test, the flowing steps are required: o Open a web browser on an intranet connected machine, and enter the URL http://aus-cf-int.au.lap.com:8081. o Select the **'Management'** option. o Provide a valid 'User name:' and 'Password:' then select the **OK** button. o From the Management page, select the sixth option, **'Security'**. o Enter in a weak password such as a single character into the 'New password' field. o Re-enter the same password into the 'Verify password' field.

[6] Refer to Appendix B: LaP Password Policy and Standard

	○ Select the **'Apply'** button.
Subjective/Objective	Objective: confirmation of current password length and complexity and the testing of password enforcement by the CacheFlow. Subjective: the interview process to determine aging and history compliance.

Identifier	CLI-A.4a
Reference	1. This is an item based on personal experience and industry good practice. 2. CacheFlow installation/configuration documentation: http://www.cacheflow.com/files/installguides/cf500ecins.pdf 3. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	Determine if the CacheFlow provides the same error message upon failed telnet login attempts, regardless of the invalid entry being the username or password.
Risk	Description: If login requires a username and password for authentication, this means any potential attacker must know two pieces of information to gain entry. If the CacheFlow provides one error message when the username is right but the password wrong, and a different message when the username is incorrect, an attacker is able to determine when they have the correct username. This then allows them to try a brute force password attempt using the gained username. If the username is not known, then the attacker will not know if they are attempting passwords against a valid username. Likelihood: Low Impact: Medium
Compliance	A single error message will be provided irrespective of the particular piece of entered information that is wrong.

Testing	○ Open a DOS prompt on an intranet connected machine, and enter the command **telnet *aus-cf-int.au.lap.com***.
	○ Enter in the following combinations:
	  ○ Valid username, invalid password
	  ○ Invalid username, valid password
	  ○ Invalid username, invalid password
	○ Observe the results of each to see what response the CacheFlow provides to each of the three combinations

Subjective/Objective	Objective

Identifier	CLI-A.4b
Reference	1. This is an item based on personal experience and industry good practice. 2. CacheFlow installation/configuration documentation:

	http://www.cacheflow.com/files/installguides/cf500ecins.pdf 3. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	Determine if the CacheFlow provides the same error message upon failed web login attempts, regardless of the invalid entry being the username or password.
Risk	Description: If login requires a username and password for authentication, this means any potential attacker must know two pieces of information to gain entry. If the CacheFlow provides one error message when the username is right but the password wrong, but a different message when the username is incorrect, an attacker is able to determine when they have the correct username. This then allows them to try a brute force password attempt using the gained username. If the username is not known, then the attack will not know if they are attempting passwords against a valid username. Likelihood: Low Impact: Medium
Compliance	Irrespective of the incorrect information provided, the response from the CacheFlow (via the browser) should be the same.
Testing	○ From an intranet connected machine, open a web browser and enter the URL http://aus-cf-int.au.lap.com:8081. ○ Once the page has loaded, select **'Management'**, the second option in the list. ○ Attempt to login using the following combinations: ○ Valid username, invalid password ○ Invalid username, valid password ○ Invalid username, invalid password ○ Observe the results of each to see what response the CacheFlow provides to each of the three combinations
Subjective/Objective	Objective

Identifier	CLI-A.4c
Reference	1. This is an item based on personal experience and industry good practice. 2. CacheFlow installation/configuration documentation: http://www.cacheflow.com/files/installguides/cf500ecins.pdf 3. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	Determine if the CacheFlow provides the same error message upon failed console login attempts, regardless of the invalid entry being the username or password.
Risk	Description: If login requires a username and password for authentication, this means any potential attacker must know two

	pieces of information to gain entry. If the CacheFlow provides one error message when the username is right but the password wrong, but a different message when the username is incorrect, an attacker is able to determine when they have the correct username. This then allows them to try a brute force password attempt using the gained username. If the username is not known, then the attack will not know if they are attempting passwords against a valid username. Likelihood: Low Impact: Low
Compliance	Irrespective of the incorrect information provided, the response from the console session to the CacheFlow should be the same.

Testing	o Connect a computer to the CacheFlow 525i with a serial cable between the two devices serial ports.
	o Open terminal emulation software, and select the serial connection option.
	o Attempt to login to the CacheFlow using the following combinations:
	  o Valid username, invalid password
	  o Invalid username, valid password
	  o Invalid username, invalid password
	o Observe the results of each to see what response the CacheFlow provides to each of these combinations.

Subjective/Objective	Objective

Identifier	CLI-A.5a
Reference	This is an item based on personal experience and industry good practice.
Control Objective	Configuration information is not available until after full user authentication via telnet.
Risk	Description: To launch an attack, it is helpful for the attacker to know details of the equipment that is being targeted. If sensitive information can be obtained without the need to login, then an attack against the system is more likely to succeed. Likelihood: Low Impact: Medium
Compliance	Prior to full login authentication, no information about the system or its configuration is available. In this test, sensitive information is considered any of the following: - CacheOS™ version; - Network information; - Details of web sites being blocked; - Passwords (login, SNMP, etc);
Testing	o Open a DOS prompt and enter **telnet *aus-cf-int.au.lap.com***. Make sure this machine is connected to the intranet. o Observe the CacheFlow response for any potentially

	sensitive information.
Subjective/Objective	Objective

Identifier	CLI-A.5b
Reference	This is an item based on personal experience and industry good practice.
Control Objective	Configuration information is not available until after full user authentication via web access.
Risk	Description: To launch an attack, it is helpful for the attacker to know details of the equipment that is being targeted. If sensitive information can be obtained without the need to login, then an attack against the system is more likely to succeed. Likelihood: Low Impact: Medium
Compliance	Prior to full login authentication, no information about the system or its configuration is available. In this test, sensitive information is considered any of the following: - CacheOS™ version; - Network information; - Details of web sites being blocked; - Passwords (login, SNMP, etc);
Testing	o From an intranet connected machine, open a web browser and enter the URL http://aus-cf-int.au.lap.com:8081. o Observe the website to determine if sensitive information is evident; o Proceed through the menu options (Browser Configuration, Statistics, Documentation, FAQ and Technical Support) to identify the type of information displayed.
Subjective/Objective	Objective

Identifier	CLI-A.5c
Reference	This is an item based on personal experience and industry good practice.
Control Objective	Configuration information is not available until after full user authentication via console.
Risk	Description: To launch an attack, it is helpful for the attacker to know details of the equipment that is being targeted. If sensitive information can be obtained without the need to login, then an attack against the system is more likely to succeed. Likelihood: Low Impact: Medium
Compliance	Prior to full login authentication, no information about the system or its configuration is available. In this test, sensitive information is considered any of the following: - CacheOS™ version; - Network information;

	- Details of web sites being blocked; - Passwords (login, SNMP, etc);
Testing	o Connect a computer to the CacheFlow 525i with a serial cable between the computers and CacheFlows serial ports. o Open terminal emulation software, and select the serial connection option. o Observe the output of the emulation software to see what information is presented
Subjective/Objective	Objective

Identifier	CLI-A.6a
Reference	This is an item based on personal experience and industry good practice.
Control Objective	Test to see if a remote telnet login prompts the user with a banner message warning about unauthorised access being prohibited.
Risk	Description: It is important to ensure that any login access to a system clearly shows that authorization is required. By not having this message visible prior to login, it is possible that a person who gained unauthorised access may be able to escape legal prosecution. Likelihood: Low Impact: Low
Compliance	Before being able to gain access to the CacheFlow via telnet, there will be some form of banner or message stating the requirement for company authorization for any access to the equipment.
Testing	o Open a DOS prompt and enter the command **telnet *aus-cf-int.au.lap.com***. o Review the returned information from the connection to see if a warning message is presented. o Login to the CacheFlow with username and password, and look to see if a legal message is displayed after login.
Subjective/Objective	Objective

Identifier	CLI-A.6b
Reference	This is an item based on personal experience and industry good practice.
Control Objective	Test to see if remote web login prompts the user with a banner or equivalent message warning about unauthorised access being prohibited.
Risk	Description: It is important to ensure that any login access to a system clearly shows that authorization is required. By not having this message visible prior to login, it is possible that a person who gained unauthorised access may be able to escape legal prosecution.

	Likelihood: Low Impact: Low
Compliance	Before being able to access the CacheFlow via the web browser, there will be some form of banner or message stating the requirement for company authorization for system access.
Testing	o Open a web browser o Enter URL http://aus-cf-int.au.lap.com:8081/ into the browser o When the page has loaded, select the second option from the list, **'Management'**. o Observe the web browser for any legal banner. o Enter in the login information and again look for any legal disclaimer or message.
Subjective/Objective	Objective.

Identifier	CLI-A.6c
Reference	This is an item based on personal experience and industry good practice.
Control Objective	Test to see if console login prompts the user with a banner message warning about unauthorised access being prohibited.
Risk	Description: It is important to ensure that any login access to a system clearly shows that authorization is required. By not having this message visible prior to login, it is possible that a person who gained unauthorised access may be able to escape legal prosecution. Likelihood: Low Impact: Low
Compliance	Before being able to access the CacheFlow via the console method of logon, there will be some form of banner or message stating the requirement for company authorization for any access to the equipment.
Testing	o Connect a computer to the CacheFlow 525i by connecting a serial cable between the PC and CacheFlow serial ports. o Run terminal emulation software, selecting the serial option. o Review the returned information for any type of warning message. o Login in to the CacheFlow and observe any messages that are displayed afterwards.
Subjective/Objective	Objective

Identifier	CLI-A.7a
Reference	This is an item based on personal experience
Control Objective	Check to ensure that a telnet session to the CacheFlow will be timed-out after a defined period of inactivity.
Risk	Description: If the CacheFlow does not have an idle timeout configured, then once a user is logged in, they will never be disconnected from the system. This can result in an unauthorised

	person gaining access from the authorized persons computer or terminal. Unauthorised access can result in loss of sensitive configuration information, or create an availability issue through malicious misconfiguration of the device. Likelihood: Low Impact: High
Compliance	A telnet connection that has been authenticated should be terminated if it is left without activity for a period of time.
Testing	o Open a DOS prompt and enter command **telnet *aus-cf-int.au.lap.com***. o Enter in the login name and password. o Leave the telnet connection open for one hour, with no activity performed. o After this time, check to see if the connection has been terminated.
Subjective/Objective	Objective.

Identifier	CLI- A.7b
Reference	This is an item based on personal experience
Control Objective	Check to ensure that connections to the CacheFlow via a web browser will timeout after a defined period of inactivity.
Risk	Description: If the CacheFlow does not have an idle timeout configured, then once a user is logged in, they will never be disconnected from the system. This can result in an unauthorised person gaining access from the authorized persons computer or terminal. Unauthorised access can result in loss of sensitive configuration information, or create an availability issue (DoS) through malicious misconfiguration of the device. Likelihood: Low Impact: High
Compliance	A web connection to the CacheFlow that is left for an extended period of time without activity will result in a disconnection of the web session to the CacheFlow.
Testing	o Open a web browser and enter the URL http://aus-cf-int.au.lap.com:8081/. o When the page has loaded, select '**Management**', the second option in the list. o Enter in the login information and select the **'Login'** button. o Minimise the browser and leave for one hour. o Check the browser to determine if the login has been terminated.
Subjective/Objective	Objective

Identifier	CLI-A.7c
Reference	This is an item based on personal experience
Control Objective	Check to ensure that console connections to the CacheFlow

	timeout after a defined period of inactivity.
Risk	Description: If the CacheFlow does not have an idle timeout configured, then once a user is logged in, they will never be disconnected from the system. This can result in an unauthorised person gaining access from the authorized persons computer or terminal. Unauthorised access can result in loss of sensitive configuration information, or create an availability issue (DoS) through malicious misconfiguration of the device. Likelihood: Low Impact: High
Compliance	Leaving a console connection connected for an extended period of time will result in the connection being terminated.
Testing	o Connect a serial cable from the CacheFlows serial port to the serial port of the computer used for this test. o Launch the terminal emulating software. o Enter username and password to log into the CacheFlow. o Minimise the emulation software and leave for one hour. o Check emulation software to see if the console connection has been disabled.
Subjective/Objective	Objective

Identifier	CLI-A.8
Reference	This is an item based on personal experience
Control Objective	To identify if the CacheFlow allows the ability to reconnect, without providing login credentials, to a web management session after logging out of that session.
Risk	Description: If an attacker is able to use a web session that has previously been connected to the management area of the CacheFlow, and return to that authorized access, the password enforcement and controls are being defeated. If this happens, it may be possible for an attacker to gain access to configuration information, or be able to make configuration changes without requiring any login credentials. Likelihood: Low Impact: High
Compliance	Once the web browser is no longer within the 'Management' area of the CacheFlow, any subsequent attempts to gain access will require user authentication.
Testing	To be comprehensive, several tests will be conducted for this item. For each of these tests, step a will be the same. 1. a) After logging in to the CacheFlow, navigate to various other websites within the same browser window. b) Using the browser 'Back' button, return to the logged in page and see if changes can be made to the configuration. 2. a) See 1 a) above for details. b) Into the browser Address field enter the URL http://aus-cf-

	int.au.lap.com:8081/. c) Select the 'Management' option and observe to see if a prompt for login details is presented. 3. a) See 1 a) above for details. b) Into the Address field of the browser, enter the URL http://aus-cf-int.au.lap.com:8081/Secure/Local/console/cm1a1.htm. This is the URL that is connected to after providing login credentials.
Subjective/Objective	Objective

Identifier	CLI-A.9
Reference	1. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	Controls have been put in place to limit the available access to the CacheFlow based on source address.
Risk	Description: By restricting the location of machines that are able to connect to the CacheFlow can further safeguard it from a remote attack. If the username and password were learned, the attacker would also need to know the range of IP addresses that are approved for access. This attacker would then need to be able to spoof an approved address if he/she was not able to connect to a network that is configured to allow access. Likelihood: Medium Impact: Medium
Compliance	The CacheFlow will be configured with some restrictions on he source IP address of any connectivity. This should be limited down to only those machines for which management access is required. It must not allow any IP addresses that are not internal to LaP.
Testing	This testing will be done in three parts. 1. Confirm that restrictions have been put in place. o Open a web browser and enter in the URL http://aus-cf-int.au.lap.com:8081/ and wait for the page to load. o Select the '**Management**' option from the list. o Enter in the Username and Password and select the '**OK**' button. o Select the '**Security**' option from the list on the left hand side. o In the grey applet, select the 'Access list' tab. o Record the information from this screen. 2. Test if telnet access is possible from a non-authorised IP address. o From a machine with an IP address that is not in the authorised list, open a command prompt and enter the command **telnet *aus-cf-int.au.lap.com***.

	○ Observe and record the result of the telnet. 3. Test if web login access is possible from a non-authorised IP address. ○ From a machine that has a non-approved IP address, open a web browser. ○ Enter in the URL http://aus-cf-int.au.lap.com:8081/. ○ If the CacheFlow page opens, select the '**Management**' option. ○ If the login dialogue box opens, enter in the username and password, then select the 'OK' button. ○ Observe to see if authenticated access is established. Note: tests 2 and 3 assume that there is a network available that is not configured to allow access – the tests will be performed from this network. And the tests must be performed from inside LaP so that no firewall can be blocking the access.
Subjective/Objective	Objective

Identifier	CLI-A.10a
Reference	1. CacheFlow installation/configuration documentation: http://www.cacheflow.com/files/installguides/cf500ecins.pdf 2. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	Identify if the CacheFlow has account lockout after excessive failed login attempts via telnet.
Risk	Description: If an account does not lockout after a set number of failed login attempts, it is highly possible that an attacker can launch a brute force attack in an attempt to gain access. This attack is perpetrated by sending a stream of different passwords until a successful logon is achieved. Likelihood: Low Impact: Medium
Compliance	The CacheFlow will lock the account for a predefined time if ten unsuccessful login attempts are made in a period of time, or between successful logins.
Testing	To test this, first 'excessive failed login attempts' must be defined. If an account does not lock out after 10 failed attempts, it would be considered as a fail. ○ Open a DOS prompt on an intranet connected machine, and enter the command **telnet *aus-cf-int.au.lap.com***. ○ Enter in the correct login name, and then provide an incorrect password. ○ Repeat the above step a further nine times. ○ Enter in the correct username and password to see if access is obtained. If at any time the entering of an incorrect password disconnects

	the telnet session, re connect through the use of the first step.
Subjective/Objective	Objective

Identifier	CLI-A.10b
Reference	1. CacheFlow installation/configuration documentation: http://www.cacheflow.com/files/installguides/cf500ecins.pdf 2. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	Identify if the CacheFlow has account lockout after excessive failed login attempts via the web.
Risk	Description: If an account does not lockout after a set number of failed login attempts, it is highly possible that an attacker can launch a brute force attack in an attempt to gain access. This attack is perpetrated by sending a stream of different passwords until a successful logon is achieved. Likelihood: Low Impact: Medium
Compliance	The CacheFlow will lock the account for a predefined time if ten unsuccessful login attempts are made in a period of time, or between successful logins.
Testing	As with CLI-A.10a, ten failed login attempts will be considered excessive. o Open a web browser on your PC and enter in the URL http://aus-cf-int.au.lap.com:8081/ and wait for the page to load. o Select the '**Management**' option from the list. o Enter in the correct Username, but provide an incorrect password. o Repeat the above step a further nine times. o Enter the correct Username and Password and observe if access is obtained. If at any time during this process a new page appears indicating that login attempt has failed, repeat the first two steps and continue with the incorrect passwords entry.
Subjective/Objective	Objective

B: Physical Security

Identifier	CLI-B.1
Reference	This is an item based on personal experience.
Control Objective	Test the physical security aspects of the CacheFlow within the data centre.
Risk	Description: If physical access is defeated, then there is no further defence that can prevent, at a minimum, availability issues and down time. This could be the result of the equipment simply being powered down, or vandalized so it can no longer be

	used. Even within a data centre, there is the chance of accidental actions that result in the equipment becoming unavailable. Likelihood: Low Impact: Medium
Compliance	The CacheFlow will be located in a secure data centre. Within this data centre the equipment will be secured within a locked rack.
Testing	Inspect the physical environment where the equipment is located. Of particular importance: o Is the equipment located in a rack? o Are the rack doors locked? o Are the keys to the doors left in the lock? o Are there any racks nearby that share the same key, which is easily retrievable?
Subjective/Objective	Objective

Identifier	CLI-B.2
Reference	Data Centre physical access checklist – see Appendix E.
Control Objective	Identify the processes that are in place to gain access into the data centre where the CacheFlow is located.
Risk	Description: If physical access is defeated, then there is no further defence that can prevent, at a minimum, availability issues and down time. This could be the result of the equipment simply being powered down, or vandalized so it can no longer be used. Even within a data centre, there is the chance of accidental actions that result in the equipment becoming unavailable. Likelihood: Low Impact: Medium
Compliance	Unauthorised users are not permitted into the data centre without a valid business requirement.
Testing	Interview the data centre manager about physical access. Review any policies and ensure that they are being enforced. Specific questions to be asked: o Who currently has data centre access? o How does an unauthorised employee gain access to the data centre? o How does an unauthorised non-employee gain access to the data centre? o Are unauthorised people escorted into the data centre? o Is a record kept of all access in to an out of the data centre?
Subjective/Objective	Subjective

C: Supportability

Identifier	CLI-C.1
Reference	This is an item based on personal experience (ITIL Essentials).
Control Objective	Documentation exists and accurately reflects the current

	configuration and setup.
Risk	Description: Lack of system and setup documentation can lead to problems with support of the environment. If the primary owner is unavailable, and there are issues with the setup, it is important that junior staff can learn enough about the environment to ensure troubles are promptly resolved. Failure for this to happen will result in an availability issue, thus preventing employees from having Internet access. Likelihood: Low Impact: Medium
Compliance	All documentation and support information is accurate, and readily available to all staff that has the responsibility to support the CacheFlow, and all unauthorised staff do not have access.
Testing	Interview the CacheFlow administrators and ask to see a copy of all current documentation. Clarity also needs to be sought about the trigger for document changes, and making sure that a change request will result in documentation being updated. Identify how the documentation is safeguarded from unauthorised access.
Subjective/Objective	Subjective

Identifier	CLI-C.2
Reference	This is an item based on personal experience (ITIL Essentials).
Control Objective	Confirm that a rigorous change management process is in place for the CacheFlow.
Risk	Description: It is important to ensure that any changes made to the infrastructure are recorded and reviewed. Failure to do this can result in changes being made without awareness of management and other system administrators, thus resulting in problems with troubleshooting and supporting the environment. Likelihood: Low Impact: Medium
Compliance	A change management tool is deployed and used for any changes made to the CacheFlow.
Testing	Interview the CacheFlow administrator to identify the processes used when changes need to be made to it. Primary areas to be covered are: o Is there a tool used to manage the 'change management' for the CacheFlow? o What information is recorded and stored with regards to the changes made? o For how long is the history of changes made kept? o What approval is required before the change request can be completed? Review some previous CacheFlow changes to ensure that the details as obtained during the interview are being carried out.

Subjective/Objective	Subjective: the interview with the CacheFlow administrator. Objective: review of the records kept from previous changes made to the proxy configuration.

Identifier	CLI-C.3
Reference	This is an item based on personal experience (ITIL Essentials).
Control Objective	Disaster recovery plan and/or process exists for circumstances of hardware failure or similar event of system unavailability.
Risk	Description: If there is a physical failure with the CacheFlow, LaP's access to the Internet will be lost. This could have a large business impact to the organization if this access is down for an extended period of time. However as it is only for Internet (web) access, functionality such as electronic mail would not be impacted. Likelihood: Low Impact: Medium
Compliance	There must be some form of contingency plan that allows for prompt replacement of failed hardware, or the ability to point PC clients to a separate infrastructure so web access remains.
Testing	Interview the CacheFlow administrators to discuss the existence of any DR plans in the event of CacheFlow unavailability. Areas to be covered during interview include: o The ability to redirect client PC's to a different proxy server. o Hardware replacement/fix contracts for the CacheFlow.
Subjective/Objective	Subjective

Identifier	CLI-C.4
Reference	1. Blue Coat System Security Advisory web site (http://www.bluecoat.com/support/knowledge/security_advisories.html)
Control Objective	To ensure that a patch management processes is in place for the CacheFlow.
Risk	Description: Almost every piece of equipment running code will eventually be detected to have some form of vulnerability. Often these vulnerabilities can lead to that equipment being available to attack from an unauthorised person, or being used for non-approved activities. Patches and/or mitigating actions will be released to correct these vulnerabilities, and hence it is vital to ensure appropriate action is taken. Likelihood: High Impact: High
Compliance	The version of the CacheOS™ should be current based on what is available from Blue Coat. It is also important to make sure the CacheFlow support staff have a defined process to receive and review notices of new vulnerabilities for prompt corrective action.
Testing	Review the Blue Coat website (http://www.bluecoat.com) to

	locate the history of patch deployments and new CacheOS™ for the CacheFlow device. The CacheFlow will be checked to see how recent the installed revision is. Interview the system administrator to determine the process for patch/upgrade notifications, and the processes for deployment to the environment.
Subjective/Objective	Objective – looking at the latest level on the device and comparing this to the most recent version that is available. Subjective – meeting with the CacheFlow administrator to discuss the process for becoming aware of new versions, reviewing and then deploying these.

Identifier	CLI-C.5
Reference	1. Employee Business Conduct – acceptable use of company resources – see Appendix A. 2. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	Determine the level of logging of users web activity that passes through the CacheFlow.
Risk	Description: If there is no means of logging the web access of employees, then there is no way to ensure that users are complying with company acceptable use policies and requirements. This can result in staff not effectively using their time in the office to perform their work related duties. Likelihood: High Impact: Low
Compliance	It will be possible to identify URL's accessed by users of the CacheFlow; along with the time the access was made and the system that made the access.
Testing	Firstly, review the configuration of the CacheFlow: o Open a browser and enter the URL http://aus-cf-int.au.lap.com:8081/. o Login to the CacheFlow by providing the Username and Password after selecting the '**Management**' option. o From the Management section, select the '**Logging'** option. o Ensure that 'Enable URL access logging' has been selected on the '**General**' tab. o From the '**Upload Site**' tab, record the details in the fields '**Host:**' and '**Path:**'. These will be used later to obtain a log sample. o At the '**Log Limits**' tab record the maximum log size. With the above details, obtain access to the server used for logging (as described on the 'Upload Site' tab) and make the following checks: o Take a size sampling of at least 10 log files and compare the

	size of these to the 'Log Limits' size. Review a sample of the usage log information that is recorded. Ensure the following details are included: o Time of URL access o IP Address of source PC requesting web page o Actual URL accessed
Subjective/Objective	Objective

Identifier	CLI-C.6
Reference	1. Employee Business Conduct – acceptable use of company resources – see Appendix A. 2. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	Identify how the CacheFlow has been configured to provide filtering on web sites that can be accessed.
Risk	Description: A large area of concern for may companies is with what their workers are doing whilst using company resources – web surfing can result in much loss of productivity. Web sites can also be a source of threat, or a location to download malicious software. Being able to control the sites that users can access is of great benefit. Likelihood: Medium Impact: Low
Compliance	As many corporations are interested in controlling the access that it's employees have to the Internet, the CacheFlow will need to have the provision to block websites.
Testing	Interview the CacheFlow administrator to determine if filtering is being used. Identify the process for updating filters, and how these are applied to the CacheFlow. If filters are in use, confirm that they are appropriately configured: o Open a browser and enter the URL http://aus-cf-int.au.lap.com:8081/. o Login to the CacheFlow by providing the Username and Password after selecting the '**Management**' option. o From the left hand selection, choose '**Maintenance**'. o Scroll across the java applet until the '**Filters**' tab is visible, and then select this. o Check to see that the '**Local file:**' field has an entry configured. Select the '**View**' button to review the validity of the file. o Check to see that '**Central file**:' field has an entry configured. Select the '**View**' button to review the validity of the file. o Ensure that "**Automatically install new Filter List when central file changes**" has been selected.

	○ Select the '**Filter List**' button to determine if a filter is currently applied to the CacheFlow.
Subjective/Objective	Subjective – interview with the CacheFlow administrator. Objective – information obtained through the review of the CacheFlow configuration.

Identifier	CLI-C.7
Reference	1. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	Identify the level of logging performed by the CacheFlow based on events affecting the system.
Risk	Description: To be aware of attacks against the system, information must first be logged. Failure to log will mean that anything affecting the system may go unnoticed, and have a severe impact to the CacheFlow availability, and the security of LaP. Logging of events also make troubleshooting problems easier as the log can indicate what has been occurring. Likelihood: Medium Impact: Medium
Compliance	The CacheFlow will be logging the changes made, as well as events that may be affecting its performance or security.
Testing	○ Open a browser and enter the URL http://aus-cf-int.au.lap.com:8081/. ○ Login to the CacheFlow by providing the Username and Password after selecting the '**Management**' option. ○ From the Management section, select the '**Events'** option. ○ On the '**Level**' tab check to see what event logging is being used. ○ From the '**Size**' tab record the details of the limit to the log file size. Also observe the choice for '**When event log reaches maximum size:**'. ○ Check to see that valid system administrator e-mail addresses have been configured on the '**Mail**' tab, along with a valid SMTP server. ○ From the '**Syslog**' tab, check to see that '**Enable syslog**' is selected and a valid server is provided in the '**Loghost:**' field. If the last point includes a syslog server, obtain access to the listed server to review the syslog.log file. If required, make changes on the CacheFlow to see what is recorded in this file.
Subjective/Objective	Objective

Identifier	CLI-C.8
Reference	1. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf

Control Objective	To determine if the SNMP configuration used on the CacheFlow is secure and not open for malicious use.
Risk	Description: Simple Network Management Protocol is a very useful protocol, but it can also be very risky if incorrectly used. Through SNMP it is possible to not only review configuration information on a device, but also modify details. Likelihood: Low Impact: Medium
Compliance	If SNMP is installed and running, it will be configured with SNMP community strings that are meeting the company password policy. All servers listed as approved trap destinations will be valid.
Testing	o From an intranet connected machine, open a browser and enter URL http://aus-cf-int.au.lap.com:8081/. o Select the '**Management**' option and provide login information. o From the list of options on the left, select '**SNMP**'. o Record the details provided on each of the three tabs ('**General**', '**Community strings**' and '**Traps**'). o Analyse results from the review and determine risks that are in place.
Subjective/Objective	Objective

Identifier	CLI-C.9
Reference	Blue Coat Systems course descriptions (http://www.bluecoat.com/resources/training/courses.html)
Control Objective	To determine if the CacheFlow administrators have been adequately trained in the management of the device.
Risk	Description: A large opportunity for security risk with any device is through system administrator's inexperience with the product. This can lead to either error in configuration due to lack of training, or more secure functions not being enabled, as they are unknown. The result of this will vary depending on the features not configured, or those configured incorrectly. Likelihood: Medium Impact: Medium
Compliance	The administrators have been on appropriate training as offered by the vendor or a suitable alternative.
Testing	Interview the CacheFlow administrators to determine what training and experience they have had.
Subjective/Objective	Subjective

D: Sniffing and Scanning

Identifier	CLI-D.1
Reference	1. IP Port Number – Full Listing (http://www.good-stuff.co.uk/useful/portfull.php)

	2. CacheFlow installation/configuration documentation: http://www.cacheflow.com/files/installguides/cf500ecins.pdf 3. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	Identify if non-expected ports are listening on the CacheFlow, and if they are in fact required.
Risk	Description: As the number of ports that devices listen on increase, so to does the risk of exposure of system compromise. The CacheFlow is used from internal systems to allow access to this Internet. As a result of this, the Internet facing leg should not be listening on any ports that are not for an already established communication channel. With the ACL's potentially preventing a real view of the ports the CacheFlow is listening on, a false sense of security may result from this test. If a future ACL misconfiguration is to occur, the CacheFlow may be open to potentially exploitable attacks. A successful port scan by a hacker would give them information that would allow them to plan for a future attack, thus resulting in loss of brand image and a potential Denial of Service attack, as Internet access could be lost. Likelihood: High Impact: High
Compliance	From the intranet, the only ports that the CacheFlow should be listening on are those required for it to successfully function. This will include web (TCP 8081), telnet and the web proxy service itself. There should be no ports that are available from the Internet as this poses a much greater risk.
Testing	Testing will be run from a Windows XP PC using NMapWin v1.3.0. This section assumes that the required software is already installed on the system. The scan will be conducted twice – once from a host on the Internet, the other from an intranet connected system. NMapWin v1.3.0: o Launch NMapWin. o If the scan is from the intranet, enter in 'aus-cf-int.au.lap.com' into the 'Host' line. If the scan is from the Internet enter 'ausproxy.lap.com.au' instead. o On the 'Scan' tab, ensure that 'SYN Stealth' is selected. Select the 'Port Range' checkbox, and enter '1-65535'. o On the 'Discover' tab, make sure that 'Don't Ping' is selected, as we want to run this test even if the device cannot be pinged. o From the 'Options' tab, ensure that 'OS Detection' from the 'options' section is selected. o The 'Timing' tab should have 'Normal' from the Throttle

	section selected. All other items are to remain unchecked. o Nothing should be selected from the 'Files' tab. o Settings from the 'Service' and 'Wn32' tabs should be left as default. o Select the 'Scan' button to commence the scan. All ports that are identified will then go through some basic testing to check for the security configuration of each, and to determine the need for these. Tests that may be performed include, but will not be limited to: o Review CacheFlow documentation to determine why these ports and services are in use. o Telnet to the CacheFlow using the open port (for example if port 8081 is open, use command **telnet *aus-cf-int 8081***). o Establish a web connection to device using the open port (for example if port 8081 is open, enter the URL http://aus-cf-int.au.lap.com:8081 into a browser). o Interview the CacheFlow administrators to understand the purpose or reason that the services are available. o Use an authenticated web session to review the CacheFlow configuration.
Subjective/Objective	This is an objective test, as tools are going to be used to perform the testing. The results from these tests will be self evident in showing which ports are available.

Identifier	CLI-D.2
Reference	1. Common Vulnerabilities and Exposures (CVE) - http://cve.mitre.org 2. CacheFlow Security Advisories (Blue Coat Systems) - http://www.bluecoat.com/support/knowledge/security_advisories.html 3. CacheOS – Fixes for CA v4.1.09 (http://download.cacheflow.com/release/CA/4.1.00-docs/CACacheOS41fixes.htm) 4. Blue Coat System Security Advisory web site (http://www.bluecoat.com/support/knowledge/security_advisories.html)
Control Objective	Perform a vulnerability scan against the CacheFlow from the intranet. This will help determine if the CacheFlow has any known vulnerabilities that may allow an attack against the system.
Risk	Description: The majority of attacks against systems are launched against known weaknesses in an attempt to exploit them. System vulnerabilities can lead to varying risk, the largest of which will allow a remote attacker to gain full system access with root user capabilities. Likelihood: High

	Impact: High
Compliance	The vulnerability scan should show no known vulnerabilities with the CacheFlow that cannot be confirmed as false positives.
Testing	This test assumes that the Retina software has already been installed and configured on the source machine. o Launch eEye's Retina Scanner software. o In the '**Address**' field, enter in the IP address of the CacheFlows inside leg. o From the '**Tools**' menu, select '**Policies**'. o Ensure that '**Complete Scan**' is selected in the pull down list. o For the Internet scan, select the '**Disable Ping and Traceroute Attempts**' checkbox. o Place a check mark in the box next to '**Enable Connect Scan Mode**'. o Leave the four (FTP, POP3, SMTP and HTTP) **CHAM** check boxes unchecked. o Select the '**Ports**' option from the left menu. o Ensure that '**Perform Full Port Scan**' is selected. o Select the '**Audits**' option from the left menu. o For completeness, select all checkboxes in the first column, with the exception of **Wireless**. o Select '**OK**' and then the '**Start**' option from the '**Action**' menu. o Once the scan has completed, create a report of the results by selecting the 'Reports' option from the 'Tools' menu. o Review the report and analyse* the findings. *The results of the scan will need to be examined to rule out false positives, and review the risk of reported issues. As the action taken will depend on the information reported, these steps will not form part of this testing plan.
Subjective/Objective	This test is objective. The eEye scanner will produce a report detailing any known issues that it is able to detect.

Identifier	CLI-D.3
Reference	1. CacheFlow installation/configuration documentation: http://www.cacheflow.com/files/installguides/cf500ecins.pdf 2. CacheOS Management and Configuration Guide version 3: http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf
Control Objective	To determine if the CacheFlow web login passes the login credentials in clear text across the network.
Risk	Description: We already know that telnet is an insecure program in that all information is sent in the clear. For this reason, it is important that the CacheFlow does not pass the web based login credentials in an insecure format. Failure to protect this information in a secured fashion provides for the opportunity that

	the login information can be gained by sniffing the network. This may provide an attacker with direct access to the CacheFlow, or enough information to launch some form of attack against it. Likelihood: Medium Impact: High
Compliance	All data between the web browser and the CacheFlow will either be encrypted, or in manner that prevents sensitive information from being sniffed off the network.
Testing	To perform this test, a network sniffing tool will be used on the machine from which the test will be run. In this case, the tool will be Ethereal[7], version 0.9.11. The details here assume Ethereal has already been installed on the test machine. o Launch Ethereal. o Select the '**Start**' option from the '**Capture**' menu (or press **CTRL-K**). o Ensure that the device selected under the 'Interface' options is the LAN card that is connected to the intranet. o Select the 'Capture packets in promiscuous mode' toggle button. o Open a web browser on your PC and enter in the URL http://aus-cf-int.au.lap.com:8081/ and wait for the page to load. o Now return to the 'Ethereal: Capture Options' dialogue box, and select the 'OK' button to start capturing packets. o Return to the web browser and select the '**Management**' option from the list. o Enter in the Username and Password and select the 'OK' button. o Return to the 'Ethereal: Capture' dialogue box and hit the 'Stop' button. o When data capture has loaded, setup a filter to exclude all traffic not related to this test: o Click on the 'Filter:' button located in the bottom left corner of the Ethereal program window (dialogue box title 'The Ethereal Network Analyzer'). o In the 'Filter String' enter the following: ***(ip.addr eq <aus-cf-int.au.lap.com IP> and ip.addr eq <host running Ethereal IP>) and (tcp.port eq 8081)***. o Click 'Apply' and then 'OK' o Review the TCP Stream of the packets making up the communication between the machine and the CacheFlow: o From the list of items in the top window of Ethereal, select a single entry of the communication to be viewed. o Select the 'Tools' menu and then the 'Follow TCP Stream'

[7] Ethereal can be downloaded from http://www.etheral.com

	option. o Select the 'ASCII' radio button at the bottom of the newly opened 'Contents of TCP stream' application window. o Save the ASCII communication by selecting the 'Save As' button. Enter an appropriate path and file name and then select 'Done' o Open the newly created file in your favourite editor (notepad, for example) and perform a search for the login credentials.
Subjective/Objective	Objective

Assignment 3

In the preceding assignment, 24 unique audit tests were documented. As there are six of these that have multiple parts, a total of 35 items are listed. Included within this assignment will be a complete write up of the ten audit items that are most reflective of the details that will be reported in assignment 4. To provide the complete audit result however, each of the other checklist items will be listed, along with a simple 'pass' or 'fail' to indicate the result of that test.

As the results from tests can be unexpected or warrant further investigation, it is possible that extra, undocumented tests will be required to further establish the level of security, etc. In cases where this is required in the items that are fully documented below, the extra actions performed will be provided, along with the results. By taking this approach, it will be possible to get a more thorough and accurate audit result.

Audit Results

A: CacheFlow Login Access Controls
CLI-A.1: Fail
Control Objective: To determine if access to the CacheFlow is using a unique per user login.

The configuration of the CacheFlow is with a single username and password that is used by all employees needing to access it. This was identified through the interview with the administrator. This was confirmed through a login to the CacheFlow – there is configuration information on the 'Account' tab under the 'Security' settings. This had details in the 'User name' and 'New' and 'Verify password' fields. Moving across to the 'External' tab showed that there was no external source configured – the 'External authentication' setting selected is 'No external authentication'.

The below screen shot highlights the current configuration of the CacheFlow with respect to external authentication.

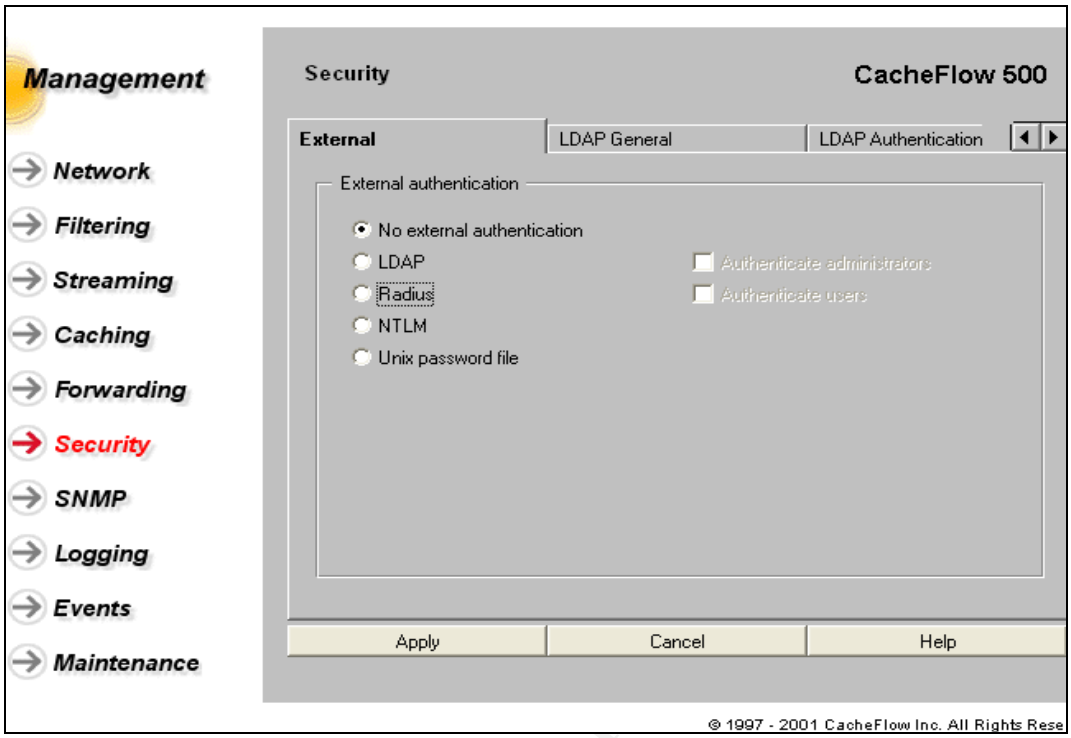

Figure 3: Configuration options for remote authentication

Through selecting the 'Help' button from the screen shown above, it was confirmed that it is possible to configure the CacheFlow to use an external source for administrative authentication: "CacheOS supports external authentication of administrators and users through the use of Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), NT Login Manager (NTLM) and a UNIX password file." [The external authentication setting can also be used to ensure that usage of the CacheFlow, as a web proxy device, requires user authentication.]

Due to the CacheFlow being in production, unfortunately it was not possible to perform testing with these other authentication methods.

CLI-A.2a: Pass
Control Objective: Test that authorization is required for remote telnet login access to the CacheFlow.

Figure 4 shows the results of trying to telnet to the CacheFlow whilst connected directly to the LaP intranet, and attempting to login with the use of no user ID or password.

```
This is a private system operated by LaP Engineering. Authorization from LaP management is required to
use this system. Use by unauthorized person is prohibited.

Username:
Password:
```

```
Username: XXXXXXXX
Password:
aus-cf-int>
```

Figure 4: Login attempt with blank username and password

As the output shows, when a blank 'Username' and 'Password' was entered, the CacheFlow returns to the 'Username' prompt. The second login attempt was made with the actual username and password, which resulted in a successful login.

CLI-A.2b: Pass
Control Objective: Test that authorization is required for remote web browser login access to the CacheFlow.

The following figure shows the login prompt that the CacheFlow displays when attempting to login to it from an intranet connected machine. This is reached when the '**Management**' option is selected from the main page.

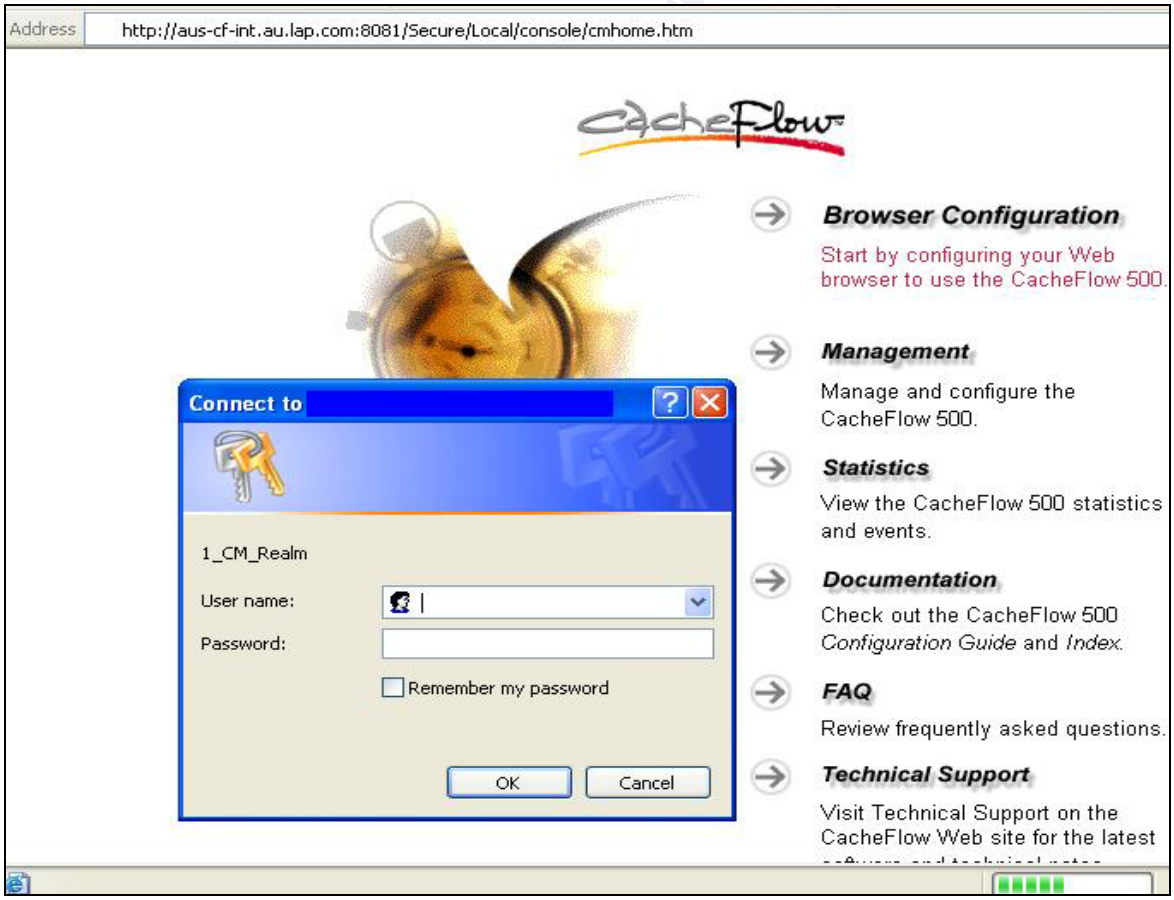

Figure 5: Web based CacheFlow login screen

Selecting the 'OK' button from the login box three times without a username or password entered, yields the below result.

Figure 6: Web based 'blank password' login failure

CLI-A.2c: Fail
Control Objective: Test that authorization is required for local console access to the CacheFlow.

When connecting to the CacheFlow via the console, you are first presented with the below screen. This is provided without the need to enter a username or password.

```
      Welcome to the CacheOS Serial Console

         Version: CA 4.1.09 Release id: 18366

------------------------- MENU -----------------------------

1) Command Line Interface
2) Setup Console

------------------------------------------------------------

Enter option:
```

Figure 7: Initial console access screen shot

If option 1 is selected, the CacheFlow will enter into configuration mode, the same as that offered by the telnet connection. However the first level access is given without the need to enter a username and/or password. To gain access into the enable level, a password is required.

```
Enter option: 1

Type "exit" at the main prompt to quit

This is a private system operated by LaP Engineering. Authorization from LaP management is required to
use this system. Use by unauthorized person is prohibited.

aus-cf-int>en
Password:
aus-cf-int>
```

Figure 8: Entering Command Line Interface via a console connection

Selecting the second option from the initial console screen presents you with the LAN interface configuration mode. No password is required to gain this access.

CLI-A.3: Fail
Control Objective: Test to ensure the administrator password is configured to meet the LaP password policy. This will cover the following:

- Configuration for complexity;
- Minimum length;
- Minimum and maximum ageing;
- History of previous passwords;

The CacheFlow support team provided the currently configured password to allow these below tests to take place.

Configuration for complexity
The current password was compared against the LaP password policy (see Appendix B for full details) with respect to complexity. The complexity requirement states:

> At least three of the following four rules
>
> a. At least two numeric character (0 – 9)
> b. At least one special character (/, [, -, =, +, !, #, $, white space, etc.) chosen from the ISO 8859-1 (Latin-1) character set.
> c. At least two lower case character (a – z)
> d. At least one upper case character (A – Z)

The current password fails this requirement. It is only meeting two out of the required 'three of four' rule. The two that are included are 'a' and 'c'.

Minimum length
The LaP policy states the following for password length:

> The password must contain a minimum of eight characters

This rule is currently being met as the password is configured with greater than eight characters. It should however be noted that there is no way to enforce this requirement within the CacheOS™ – it relies on support staff manually meeting this requirement.

Minimum and maximum ageing
The password policy of LaP specifies the following requirements for password aging (maximum and minimum):

1. Accounts that allow administrative access must be aged to no more than 45 days. If the account is for non-administrative access, then the password must expire at not more than 90 days after it was first set.
2. A password must not be able to be changed within 24 hours of it being changed. This does not apply to passwords for brand new accounts, which must be changed the first time the account is accessed.

The maximum ageing could only be confirmed through an interview with the CacheFlow administrator. This is due to there being no means within the CacheOS™ to set a maximum (or for that matter, a minimum) password aging period. There is currently no process in place to meeting the maximum age of 45 days. In fact the current password has already been in place for at least 19 weeks (or 133 days), far exceeding the company requirements.

As there is no ability with the CacheFlow to limit the ageing period, this policy requirement can only be met through good practices by the CacheFlow support team. This was confirmed by running a test on the CacheFlow. A new password was set, and within 5 minutes, the previous password was re-entered. The CacheFlow allowed the change to go through. This clearly violated the company policy of 24 hour minimum password age.

Via an interview with the team, the minimum ageing requirement would be met, as they cannot foresee the need to ever change a password within 24 hours of a new password being set. However, it is not being met through best practice or policy enforcement!

History of previous passwords
Policy requirement states the following:

> The history for password re-use must be set to at least three. This means that if a person wishes to cycle through passwords, they will have to have at least four passwords in the cycle.

The CacheFlow does not support any means to track previous passwords. This was confirmed through hands on testing. A new password was applied, with the previous password being reused within five minutes of setting it. The CacheFlow allowed this old password to be immediately re-used.

CacheFlow Support of Password Complexity
The test here was to see if the CacheFlow would allow a weak password to be entered. For this test, a weak password is considered anything that does not meet the password requirements as set in the LaP password policy (refer to Appendix B).

There is no enforcement in place on the password configuration with the CacheFlow. The password 'a' was entered, and applied. As the figure below illustrates, the CacheFlow accepted this password.

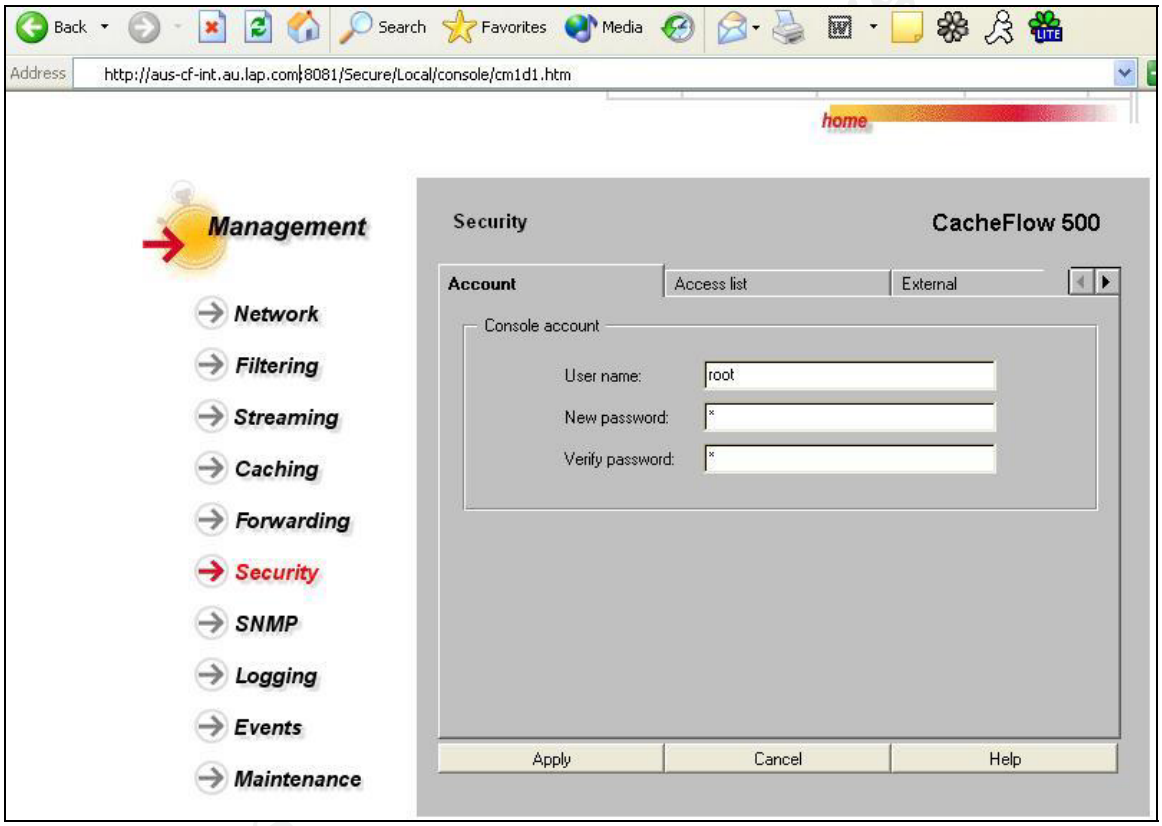

Figure 9: Web based password configuration screen

Further to this test, a blank password was also attempted, and accepted by the CacheFlow. This highlights that the CacheFlow is not performing any enforcement on password complexity or strength.

CLI-A.4a: Pass
Control Objective: Determine if the CacheFlow provides the same error message upon failed telnet login attempts, regardless of the invalid entry being the username or password.

The details of this test have been excluded from this report.

CLI-A.4b: Pass
Control Objective: Determine if the CacheFlow provides the same error message upon failed web login attempts, regardless of the invalid entry being the username or password.

The details of this test have been excluded from this report.

CLI-A.4c: Not Applicable
Control Objective: Determine if the CacheFlow provides the same error message upon failed console login attempts, regardless of the invalid entry being the username or password.

The details of this test have been excluded from this report.

CLI-A.5a: Pass
Control Objective: Configuration information is not available until after full user authentication via telnet.

The details of this test have been excluded from this report.

CLI-A.5b: Fail
Control Objective: Configuration information is not available until after full user authentication via web access.

The details of this test have been excluded from this report.

CLI-A.5c: Fail
Control Objective: Configuration information is not available until after full user authentication via console.

The details of this test have been excluded from this report.

CLI-A.6a: Pass
Control Objective: Test to see if a remote telnet login prompts the user with a banner message warning about unauthorised access being prohibited.

The details of this test have been excluded from this report.

CLI-A.6b: Fail
Control Objective: Test to see if remote web login prompts the user with a banner or equivalent message warning about unauthorised access being prohibited.

The details of this test have been excluded from this report.

CLI-A.6c: Fail

Control Objective: Test to see if console login prompts the user with a banner message warning about unauthorised access being prohibited.

The details of this test have been excluded from this report.

CLI-A.7a: Pass
Control Objective: Check to ensure that a telnet session to the CacheFlow will be timed-out after a defined period of inactivity.

After leaving an established telnet connection idle for one hour, the CacheFlow timed this session out. The results of the time out can be seen in the below figure.

```
This is a private system operated by LaP Engineering. Authorization from LaP management is required to
use this system. Use by unauthorized person is prohibited.

Username: user
Password:
aus-cf-int>

Connection to host lost.

C:\>
```

Figure 10: CacheFlow telnet connection time out

To further identify a more specific time limit for the idle time out connection, the CacheFlow was connected to via a web connection. From reviewing this, there is no configuration that specifies the time out setting. To further refine the timeout period, a second telnet connection was established, and monitored to see how long it would take to time out. This resulted in a period of five minutes being identified.

CLI-A.7b: Fail
Control Objective: Check to ensure that connections to the CacheFlow via a web browser will timeout after a defined period of inactivity.

After leaving a web connection to the CacheFlow for one hour, it had not timed out. The connection remained established, and there was no requirement to re-authenticate before further administrative action could be taken. The test was run a second time, this time leaving the web session idle for a time of four hours. Once again, the session remained established, and no authentication was required to allow administrative changes.

CLI-A.7c: Fail
Control Objective: Check to ensure that console connections to the CacheFlow timeout after a defined period of inactivity.

The result of this test indicated that there is no timeout of the console connection at any time. This was tested from both the initial console screen (see figure 7) and also after entering into configuration mode (see figure 8). Based on the CacheFlow allowing access without the need to authenticate, this is not an unexpected result.

CLI-A.8: Fail
Control Objective: To identify if the CacheFlow allows the ability to reconnect to a web management session after logging out of that session.

For this checklist item, there were three tests outlined. In each one of these, access could be regained from a browser that had been previously authenticated to the CacheFlow. This is compounded by the fact that there is no logout option once authentication has been attained. Add to this the fact that a web connected session to the CacheFlow does not appear to have a time out setting.

To further ensure that password authentication would always be needed, an attempt was made to bypass the login prompt completely. This was performed through opening a new web browser session, and entering in the URL http://aus-cf-int.au.lap.com:8081/Secure/Local/console/cm1a1.htm (this is the URL that you are redirected to after providing the login credentials). The result of this was that the login prompt as detailed in figure 5 was displayed. This does mean that someone who knows the correct URL cannot circumvent the login information.

CLI-A.9: Pass
Control Objective: Controls have been put in place to limit the available access to the CacheFlow based on source address.

The configuration of the CacheFlow does provide for some limitation with who can access it. The implementation of this within LaP is not very effective however as it is allowing the entire internal IP range access. Whilst this is protecting access to the device from an external means, it does not protect against malicious internal users.

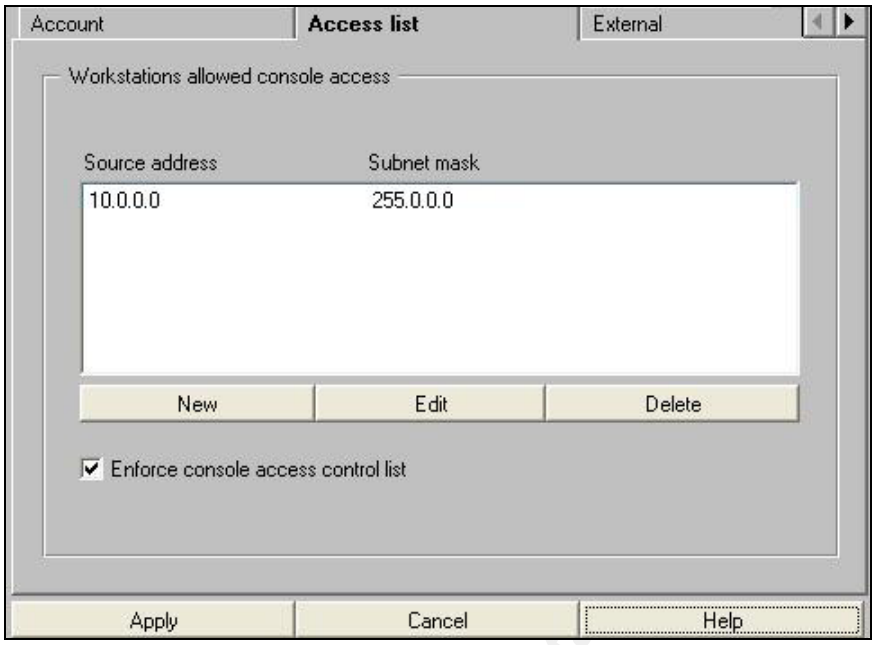

Figure 11: Remote console management access-list configuration

It was not possible to make a connection to the CacheFlow through either telnet or web console when the client machine was using a non-corporate IP address. The telnet connection simply failed to connect. The web console displayed the initial CacheFlow web page, but when the 'Management' option was selected the screen as indicated in figure 6 was returned.

When the specific IP address of the test machine was added to the access list, it was then possible to connect via both telnet and web console. This shows that this is a valid and acceptable method of limiting remote login access to the CacheFlow.

CLI-A.10a: Not Conducted (due to CacheFlow being in production)
Control Objective: Identify if the CacheFlow has account lockout after excessive failed login attempts via telnet.

The details of this test have been excluded from this report.

CLI-A.10b: Not Conducted (due to CacheFlow being in production)
Control Objective: Identify if the CacheFlow has account lockout after excessive failed login attempts via the web.

The details of this test have been excluded from this report.

B: Physical Security
CLI-B.1: Fail

Control Objective: Test the physical security aspects of the CacheFlow within the data centre.

The details of this test have been excluded from this report.

CLI-B.2: Pass
Control Objective: Identify the processes that are in place to gain access into the data centre where the CacheFlow is located.

The details of this test have been excluded from this report.

C: Supportability
CLI-C.1: Pass
Control Objective: Documentation exists and accurately reflects the current configuration and setup.

The details of this test have been excluded from this report.

CLI-C.2: Pass
Control Objective: Confirm that a rigorous change management process is in place for the CacheFlow.

The details of this test have been excluded from this report.

CLI-C.3: Pass
Control Objective: Disaster recovery plan and/or process exists for circumstances of hardware failure or similar event of system unavailability.

The details of this test have been excluded from this report.

CLI-C.4: Fail
Control Objective: To ensure that a patch management processes is in place for the CacheFlow.

The details of this test have been excluded from this report.

CLI-C.5: Pass
Control Objective: Determine the level of logging of users web activity that passes through the CacheFlow.

The details of this test have been excluded from this report.

CLI-C.6: Pass
Control Objective: Identify how the CacheFlow has been configured to provide filtering on web sites that can be accessed.

The details of this test have been excluded from this report.

CLI-C.7: Fail
Control Objective: Identify the level of logging performed by the CacheFlow based on events affecting the system.

The CacheFlow has been configured to send all recorded events to a syslog server. Two e-mail addresses have also been configured to receive events. Both e-mail addresses are current and for valid CacheFlow administrators. However after discussing this with one of these administrators, it was reported that they do not receive any messages from the CacheFlow!

Knowing that the CacheFlow is recording events to a syslog server, the syslog.log file was examined for days when many of the tests from this audit were conducted. Of particular interest, the following tests had been conducted:

- Retina scan against the CacheFlow from both Internet and intranet.
- NMap scan against the CacheFlow from the intranet and Internet.
- Multiple failed login attempts via web browser and telnet.
- Reconfiguration of the CacheFlow settings.

As can be seen in the below figure, there are only four entries that were logged to syslog during the three days of primary audit activities. None of these in anyway indicated the tests that were run, implying that nothing was triggered on the CacheFlow as a reportable incident. This is a severe shortage in the logging – at a minimum a series of failed login attempts should be flagged. It would also be nice to know that scanning (vulnerability and port) would be detected and reported. Yet when the time on the CacheFlow is out of synch with the corporate NTP server, this is an event worthy of logging to the syslog server.

When reviewing the level of logging that is configured on the CacheFlow, the following was observed.

```
Jun 13 04:40:04 aus-cf-int.au.lap.com CacheOS: A0000 SMTP: DNS error looking up gateway
'intmailsrv.uk.lap.com'(0) SEVERE_ERROR smtp.cpp 257
Jun 14 04:39:50 aus-cf-int.au.lap.com CacheOS: A0000 SMTP: DNS error looking up gateway
'intmailsrv.uk.lap.com'(0) SEVERE_ERROR smtp.cpp 257
Jun 15 04:39:37 aus-cf-int.au.lap.com CacheOS: A0000 SMTP: DNS error looking up gateway
'intmailsrv.uk.lap.com'(0) SEVERE_ERROR smtp.cpp 257
Jun 15 23:55:48 aus-cf-int.au.lap.com CacheOS: 90000 NTP: Periodic query of server
corpntpsrv.uk.lap.com, ntp time significantly different from system clock (off -5 seconds). Updated system
clock.(0) SEVERE_ERROR ntp.cpp 696
```

Figure 12: CacheFlow information recorded to syslog

The first three entries seem to indicate that there is a problem with the relaying of mail via the server intmailsrv.uk.lap.com – this is the server that was configured as the mail relay server within the CacheFlow. Performing an nslookup on the hostname 'intmailsrv.uk.lap.com' results in a host not found error! This explains why the two configured administrators are not receiving e-mails from the

CacheFlow. To determine the type of information that is sent via e-mail, the auditors' e-mail was added to the 'Mail notifications to:' list, and a valid SMTP server was included. This resulted in an e-mail being delivered to the auditor. The information that is sent out from the CacheFlow is not actually events with reference to that included in the syslog.log file, but rather general 'health' and 'statistics' of the CacheFlow.

When reviewing the level of logging that is configured on the CacheFlow, the following was observed.

Figure 13: Level of logging for event detection

This indicates that there are an extra two levels of logging that could be enabled.

CLI-C.8: Pass
Control Objective: To determine if the SNMP configuration used on the CacheFlow is secure and not open for malicious use.

The details of this test have been excluded from this report.

CLI-C.9: Fail
Control Objective: To determine if the CacheFlow administrators have been adequately trained in the management of the device.

The details of this test have been excluded from this report.

D: Sniffing and Scanning
CLI-D.1: Fail
Control Objective: Identify if non-expected ports are listening on the CacheFlow, and if they are in fact required.

Intranet NMap Scan
The expectation is that the ports that will be listening from this scan are: telnet (TCP/23), web-proxy (TCP/8088) and web management (TCP/8081).

When the NMap application was run the details as shown in figure 14 were obtained.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Interesting ports on against aus-cf-int.au.lap.com (10.150.162.243):
(The 65529 ports scanned but not shown below are in state: closed)
Port       State       Service
21/tcp     open        ftp
23/tcp     open        telnet
80/tcp     open        http
113/tcp    open        auth
8081/tcp   open        blackice-icecap
8088/tcp   open        unknown
Remote OS guesses: CacheOS 3.1 on a CacheFlow 6000, Cacheflow 6x5 running CacheOS 3.1.19-4.1.05
Uptime 62.989 days (since Mon Apr 14 14:22:03 2003)
Nmap run completed -- 1 IP address (1 host up) scanned in 118 seconds
```

Figure 14: Output from NMapWin intranet scan

As the above shows, the CacheFlow has six ports that are actively listening, three more than what would be expected. All of these have been broken down here and further analysis conducted to ensure the security of each, even those that were expected to be found.

TCP/21

This was an unexpected port to be open. To determine the need for this port, further investigation was performed. As the standard use for port TCP/21 is FTP, an attempt was made to connect to the CacheFlow using FTP.

```
C:\>ftp aus-cf-int
Connected to aus-cf-int.au.lap.com.
Connection closed by remote host.

C:\>
```

Figure 15: Attempted FTP access to the CacheFlow

The expected result of FTP'ing to a device was not obtained. Failure was also seen with an attempt to telnet to port 21 (**telnet *aus-cf-int 21***).

A review of the different CacheFlow documents (see those within the Reference) was not able to determine the need for the FTP port to be listening. To resolve this, CacheFlow were contacted directly. The result of this is that FTP is configured to allow the CacheFlow to support transparent FTP services. However as the transparent FTP service is not used within LaP, this port is not required to be available.

TCP/23

This was an expected result. It has already been detailed that telnet is an option with the CacheFlow to provide support and configuration for administrators. There are concerns with allowing this port to be open and actively available – telnet connectivity between a client and server is not encrypted. This means that not only is the username and password sent in the clear across the network, but also all other commands to the CacheFlow and reply communication. The below

is the result of a simple capture of network traffic using Ethereal – it shows clearly that the login information can be detected in the clear, along with the command entered, and the results that are displayed to the client.

```
ÿû└ ÿý└ ÿû┌ ÿý This is a private system operated by LaP Engineering. Authorization from LaP
management is required to use this system. Use by unauthorized person is prohibited.

Username: ÿý┌ ÿûÿú P ├ ÿðuusseerr

Password: <removed>

melwebcache2>sshh  ??
 accelerated-pac        Accelerated PAC file
 access-log             Access log settings
 arp-table              ARP information
 bandwidth-gain         Bandwidth-gain settings
 bypass-list            Bypass list
 cache-systems          CacheOS Systems
 caching                Caching settings
 clock                  Current time
 commands               Show available CLI commands
 content-distribution   Sizes of objects in cache
 cpu                    CPU usage
 diagnostics            Remote diagnostics
 direct-deny-list       Direct or deny list
 disk                   Disk status and information
 dns                    DNS servers and name imputing
 download-paths         Downloaded configuration paths
 dynamic-bypass         Dynamic bypass configuration
 efficiency             Efficiency statistics
 environmental          Environmental Information
 event-log              Event log setting
 filter-list            Current filter list
 forwarding             Forwarding settings
 hostname               Hostname
--More-- ← [2K← [120D http-stats            HTTP statistics
```

Figure 16: Clear text capture of telnet activity

TCP/80

Through the tests and analysis done so far, TCP/80 was not expected to be a valid service. It is not possible to access the CacheFlow via a web browser on TCP/80 – this can be confirmed through use of the following URL: http://aus-cf-int.au.lap.com. If trying this, the result is a standard 'There was a communication problem' reported by Internet Explorer.

Trying to telnet to the CacheFlow on port TCP/80 (**telnet *aus-cf-int.au.lap.com 80***) yields a series of HTML responses. Placing this response into a file and saving it with a 'HTML' extension and then opening this in a browser, shows that the information is in relation to an 'Invalid Request'.

Problem Report	The system detected HTTP Error **Invalid Request** while attempting to retrieve the URL: .
Message ID	REQUEST_INVALID
Problem Description	The system did not accept the HTTP request.
Possible Problem Cause	The browser used " and generated a malformed HTTP request. This problem should not be encountered by a stable commercial browser.
Possible Solution	Contact your Web browser technical support team if the problem persists.

Figure 17: Results of port 80 telnet viewed as html page

As this result was also seen when establishing a telnet session on TCP/8088, a test was conducted to see if TCP/80 actually allows a client to use this port in it's proxy configuration. To test this, the 'Port:' field within the LAN Settings of Internet Explorer's Internet Options/Connections was modified to port 80. An attempt was then made to access an Internet accessible website (http://www.google.com/). The result was that the website could be successfully accessed, indicating that port 80 is an additional port that can be used to proxy traffic (in addition to TCP/8088).

To try and confirm that this was true, the CacheFlow administrators were consulted and asked about the need for TCP/80. Sadly, the answer provided was a disappointing "that is the way it was originally setup, and we have not been asked to change it, nor informed of its purpose." Further research on this topic through direct consultation with an employee of Blue Coat Systems, identified that this port is available to provide transparent HTTP services for the CacheFlow. What this allows is for client machines to not be reconfigured to point to the CacheFlow. Instead, network equipment (routers or load-balancers) are configured to pass any traffic on port 80 to the CacheFlow. The CacheFlow will then proxy this traffic. To allow it to receive this redirected web traffic, it needs to be listening on the HTTP port. This also clarifies why TCP/80 could be used as the proxy port in the web browser configuration. As with TCP/21 (transparent FTP), transparent HTTP is not used by LaP, as such there is no business need for this port to be available on the CacheFlow.

TCP/113

This was an unexpected port to be listening. So far in this audit, there has been no reference to this port, or the purpose that it serves. The 'well known use' of this port is for 'authentication service'[8].

As initial investigation, a couple of very rudimentary tests were performed:

[8] As indicated at the web site: http://www.good-stuff.co.uk/useful/portfull.php.

1. Attempt to telnet to aus-cf-int on this port – the command for this is **telnet *aus-cf-int 113***.

```
C:\>telnet aus-cf-int 113

: USERID : UNIX : aus-cf-int

Connection to host lost.

C:\>
```

Figure 18: Result of CacheFlow telnet port 113

2. Attempt a web browser connection to the CacheFlow on port TCP/113. This is achieved by entering the URL http://aus-cf-in.au.lap.com:113 into a browser:

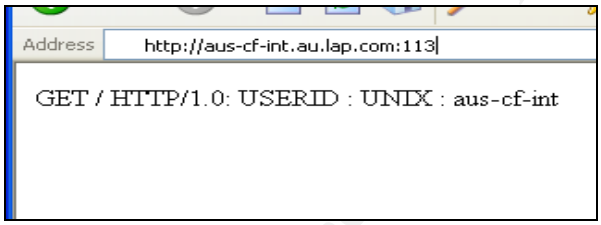

Figure 19: Result of web access to CacheFlow on port 113

To further analyse this, a web session to the CacheFlow was established, and under the 'Network' option, the 'Services' highlighted the services that are configured on the CacheFlow. Port TCP/113 is not one of those listed.

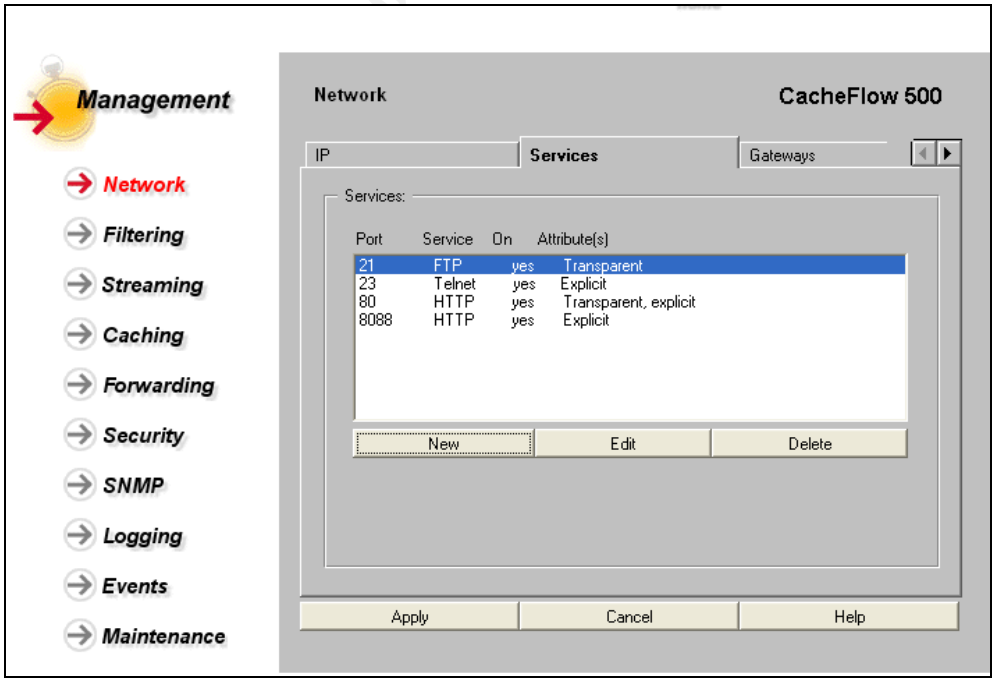

Figure 20: Services configured on the CacheFlow

None of these steps were able to provided details about the need for port TCP/113. To further identify the purpose, the following CacheFlow documents were reviewed:

1. CacheOS Version 2.2.1 Management and Configuration Guide
2. CacheOS 3.0 – Management and Configuration Guide
3. CacheFlow 500ec Series Installation Guide

None of these indicated the exact requirement of TCP/113. After contacting CacheFlow directly, port TCP/113 was identified as an 'ident server used for SOCKS 4 authentication'[9]. Having this knowledge, it was then easier to identify the relevant details from the CahceOS Version 2.2.1 Management Configuration Guide. It describes the ability to use a SOCKS server for a 'primary or alternative forwarding gateway'[10]. For this to work, the CacheFlow needs to be able to authenticate with the SOCKS server, and hence the use of this port. As this functionality is not employed within the company, the service is actually not required.

TCP/8081

The port scan conducted by NMap suggested that the service listening on TCP/8081 is 'blackice-icecap'. This is not so in this case – NMap associates the service name with the port based on the file "C:\Program Files\NMapWin\data\nmap-services" (when the install of NMapWin is to the default location). In this case, the entry in the nmap-service file is "blackice-icecap 8081/tcp # ICECap user console".

In reality, this port is used to provide web based Management Console access to the CacheFlow. The port for this service can be set based on administrator preference. This is done through the following steps:

- Open a browser window and enter the URL http://aus-cf-int.au.lap.com:8081/.
- Select the '**Management**' option and provide the username and password.
- Select the '**Network**' from the list on the left hand side of the browser.
- In the grey window on the right, use the right arrow to scroll across until the 'Console' tab is available.
- Select the Console tab and enter the required port to act as the 'Management Console' port.
- Click Apply.

TCP/8088

Internally LaP direct their web browser traffic on this port. For any traffic to be proxied via the CacheFlow, it must be listening on TCP/8088.

Miscellaneous Information

[9] Direct quote taken from an e-mail received by Blue Coat's Jason Chai.
[10] CacheOS Version 2.2.1 Management and Configuration Guide, page 114.

The NMap scan has also been able to take a 'guess' at the version of the CacheOS™, its suggestion being 3.1.19-4.1.05. This is close, but the current version that is being run on aus-cf-int is 4.1.09. This information will still give an attacker a good neutral point from which an attack can be launched. Although the true version of CacheOS™ is available by simply entering in the URL http://aus-cf-int.au.lap.com:8081/, as such the NMap scan is not required to obtain this information.

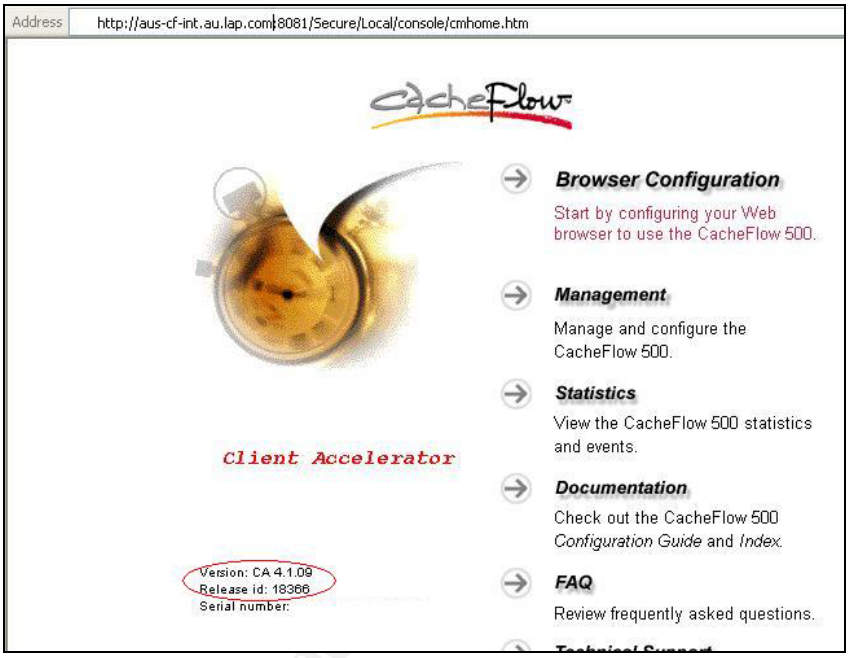

Figure 21: Pre-authentication access displaying CacheOS version information

Internet NMap Scan

With this test being conducted from the Internet, it is possible that the results will not accurately reflect what ports the CacheFlow is actually listening on with the outside leg. In the case of LaP, access-control lists may block the access that would otherwise be available if this perimeter defence was not in place.

Unlike the NMap scan conducted from the intranet, the Internet scan yielded no ports as being available – all ports were identified as 'filtered'.

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Warning:  OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed
TCP port
All 65535 scanned ports on ausproxy.lap.com.au (172.18.105.234) are: filtered
Too many fingerprints match this host for me to give an accurate OS guess
Nmap run completed -- 1 IP address (1 host up) scanned in 21655 seconds
```

Figure 22: Output from NMapWin Internet scan

Within NMap, when a port is recorded as filtered it is often a result of "…a firewall, filter, or other network obstacle is covering the port and preventing nmap

from determining whether the port is open"[11]. This is an expected result as the router that sits between the CacheFlow and the Internet contains two interfaces with incoming and outgoing ACL's.

CLI-D.2: Pass
Control Objective: Perform a vulnerability scan against the CacheFlow from the Internet and intranet. This will help determine if the CacheFlow has any known vulnerabilities that may allow an attack against the system.

Intranet Retina Scan.
The full report that was generated for the intranet scan by the Retina software has been attached in Appendix C. In summary, the scan produced a result of three vulnerabilities in total – two medium risks and one high. It also provided two informational alerts, although these were both warning about the same thing (anonymous HTTP proxy detected), as this is configured on two different ports of the CacheFlow.

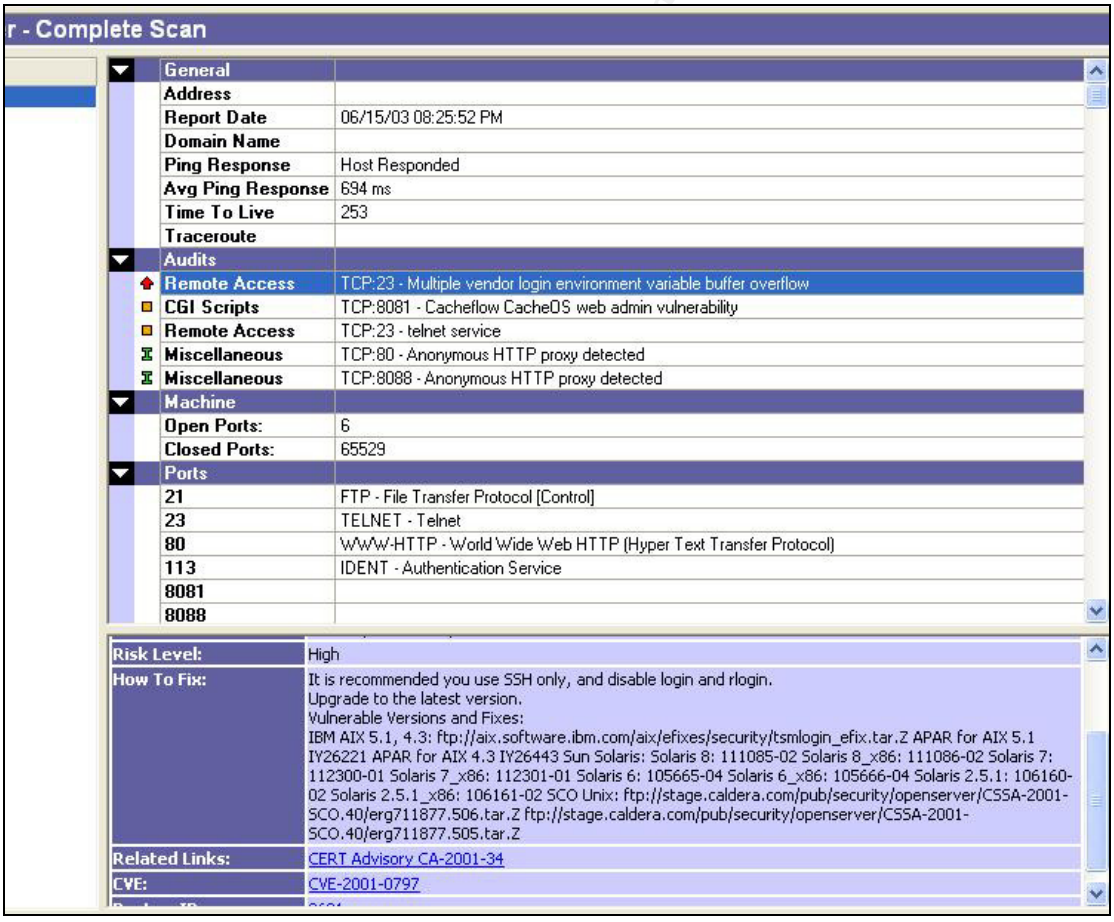

Figure 23: Screen shot of the Retina scan results

[11] Taken from "NMap Manual Page" from the NMapWin Help file

High Risk Vulnerability.
The retina scanner detected this high risk vulnerability with the telnet access to the CacheFlow. The problem description does however state that there is the potential for this to be a false positive.

A review was made on each of the three related links provided (CERT Advisory CA-2001-34, CVE-2001-0797 and BugtraqID 3681), and none of these indicated that the CacheOS™ was an impacted operating system. All those that are impacted have been based on implementation of the Unix System V operating system. There is no documentation that can be found that indicates that CacheOS™ is a derivative of System V.

Through use of the CVE, CERT and BugtraqID's, research was performed on the known vulnerabilities released by the CacheFlow vendor. This item was not located amongst the three published vulnerabilities, and nor was it mentioned as a fix in any of the new CacheOS™ releases. Based on all this information, the alert is being considered a false positive.

Medium Risk Vulnerabilities.
As indicated, there were two alerts of this level – a vulnerability with CGI scripting on port TCP/8081, and a remote access alert for telnet on port TCP/23.

CGI Scripting: of the three vulnerabilities detected by the scan, this is the only one that is exclusively a CacheOS™ problem. The issue is that a telnet connection to the web management console port may result in the CacheFlow "leaking" information such as parts of URLs being accessed by a client currently connected to the cache server."[12]

There is a published exploit (http://www.securityfocus.com/bid/3841/exploit/) for this vulnerability. When trying this particular exploit code against the CacheFlow, the results do not indicate that the CacheFlow is actually vulnerable. If the vulnerability is present, then a series of keystrokes should be possible. However on the LaP CacheFlow, as soon as a single key is entered after the telnet command is issued, the connection times out and returns to the command prompt. This test was attempted multiple times, always with the same result.

```
HTTP/1.0 405 Invalid method

Method not allowed

Connection to host lost.

C:\>
```

Figure 24: Results of attempted CVE-2002-0107 vulnerability exploit

[12] http://www.securityfocus.com/bid/3841/discussion/

Also by reviewing the versions of CacheOS™ that were vulnerable to this exploit, version 4.1.09 is not listed. Based on this information, the flagging of this error is being attributed to a false positive.

Remote Access: this alert is not referencing an actual vulnerability with the system, but is simply concerning the inherent issues with telnet in that all traffic is transmitted in plain text. Due to the fact that this is not actually referencing a design flaw or bug in the way code has been written (this is just how telnet is, and is not doing something unexpected), it has not been officially included in the CVE list. As such it will not be further investigated in this audit.

Internet Retina Scan.
The full report that was generated for the Internet scan by the Retina software has been attached in Appendix D. The Retina scan reported that from the Internet, there is a single high risk vulnerability and one informational item.

High Risk Vulnerability.
This vulnerability implies that the vulnerable device is a Microsoft Internet Information Server (IIS). However the CacheFlow is not running this Microsoft service, and nor does it run DLL's for file with extensions .HTR, .STM and .IDC. A review of the SecurityFocus vulnerability alert (http://www.securityfocus.com/bid/307) fails to mention that CacheFlow is a vulnerable system. To further test this to see if it is a false positive, the exploit as detailed at http://www.securityfocus.com/bid/307/exploit/ was attempted. This failed to return any of the expected results should this vulnerability have actually been present, and did not impact the performance of the CacheFlow in any way.

Information Alert.
The information alert was for the 'anonymous HTTP proxy detected', which is the same as reported and discussed previously with the intranet scan. Even though this has already been reviewed and discussed in the intranet scan section, it needs to be reviewed here. The concern is that the CacheFlow has been detected as being a proxy device from the Internet. It needs to be analysed to ensure that the CacheFlow cannot be used by an Internet machine – for either access to Internet facing web sites, or worse, the LaP corporate network!

To test this, an Internet connected machine was configured to use the Internet IP address of the CacheFlow as its proxy server with port 80 as the proxy port. Upon doing this, an attempt was made to visit an Internet site (www.google.com), the result being that the web page was retrieved. More web access was made, in all cases access being allowed. Changing the proxy port from 80 to 8088 resulted in attempted access to web sites to fail, with Internet Explorer reporting 'This page cannot be displayed'.

Further analysis into this through the use of Ethereal was performed. By capturing several minutes of web activity, it was indeed demonstrated that the

communication between the client and the CacheFlow was passing the web pages. The packet capture also showed the three-way handshake being performed between the two systems, and never once did the client system receive the web traffic from the actual web site visited – it always came from the CacheFlows IP address.

In addition to the Ethereal packet capture, a review of the usage logs for the time the web activity took place was carried out. This did not identify any access attempts direct from the Internet – all included IP addresses were internal to LaP.

Based on this information, it was important to ensure that the CacheFlow does not provide access to systems on LaP's intranet. To test this, several LaP intranet server names and IP addresses were entered into a browser. None of these resulted in access to the website – the browser always returned the error message "This page cannot be displayed".

The final test performed here was to attempt to visit a website that the LaP CacheFlow has been configured to block. When this was entered in, the website was successfully connected to. This indicates that the CacheFlow configuration was not used as part of the web access, as if it were, the default LaP message for blocked web sites would have been displayed.

CLI-D.3: Pass
Control Objective: To determine if the CacheFlow web login passes the login credentials in clear text across the network.

After running Ethereal during a connection to the CacheFlow via a web browser, it was clear that the login credentials, whilst not being in the clear, might be in a non-secure fashion.

The traffic between the client and CacheFlow is not part of a single communication. It seems that whenever a change is made on the web page of the CacheFlow, a new TCP conversation is established (three-way handshake, etc). This is evident as the source port is not consistent across the entire communication between the CacheFlow and web browser, but will increment after a non-specific number of packet transmission.

With the Ethereal capture not beginning until immediately prior to attempting to authenticate on the CacheFlow, the amount of traffic to contend with was reduced. In the short test, there were still seven different communications established based on there being seven different source ports between the client and CacheFlow all with the destination port of 8081. Each one of these 'conversations' was saved out of Ethereal and used to see if the password and or username could be identified.

From the first of these communications, the header provided the following snippet of information

```
GET /Secure/Local/console/cm1a1.htm HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint,
application/vnd.ms-excel, application/msword, application/x-shockwave-flash, */*
Accept-Language: en-au
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; T312461; LaP Engineering IE5.5-SP2;
.NET CLR 1.0.3705)
Host: aus-cf-int.au.lap.com:8081
Connection: Keep-Alive
Cookie: WTO_CLIENT=1

HTTP/1.0 401 Unauthorized
WWW-Authenticate: Basic realm="3_CM_Realm"
```

Figure 25: Initial communication information for first data stream

As the final two lines show, the CacheFlow is requesting for authentication. In the second data-stream (see below figure), the authentication information has been provided. Along with this information is a substantial amount of HTML code which, when reviewed in a web browser, displays the post login screen to the CacheFlow similar to that depicted in figure 9. This leads to the conclusion that after receiving the initial traffic in the below figure, the user has been authenticated. The figure below shows this TCP conversation, minus the HTML code.

```
GET /Secure/Local/console/cm1a1.htm HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint,
application/vnd.ms-excel, application/msword, application/x-shockwave-flash, */*
Referer: http://aus-cf-int.au.lap.com:8081/Secure/Local/console/cmhome.htm
Accept-Language: en-au
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; T312461; LaP Engineering IE5.5-SP2;
.NET CLR 1.0.3705)
Host: aus-cf-int.au.lap.com:8081
Connection: Keep-Alive
Cookie: WTO_CLIENT=1
Authorization: Basic <random string of characters removed>

HTTP/1.0 200 OK
Content-length: 5142
Content-type: text/html
Pragma: no-cache
Cache-Control: no-cache
```

Figure 26: Initial communication information for second data stream

Whilst it is not shown in the above (it has been omitted for security reasons), the 'Authorization: Basic' line included much garbled text, which had the appearance of an encrypted piece of text.

To better understand the meaning of the 'Authorization: Basic …' string, the 'Proxy User Authentication'[13] document was reviewed. Whilst this document refers to the process of providing basic user-authentication, it does mention the use of basic authorization. The paper goes into detail and identifies the format used to generate the encrypted form of the passwords, that being 'htpasswd'. A Google (www.google.com) search on htpasswd returned 85,400 matches! This is quite a well-documented function. Finally, the paper also states that the encoding of the user credentials follows the methods described in RFC 1421 – again this information is readily available for review. With all this information, it would give an attacker a very good starting point to trying to defeat the login security of the CacheFlow via the web browser.

To finalise this item, one further test was conducted. Ethereal was used to capture two failed login attempts to the CacheFlow.

- In the first login attempt, the correct username was used, but the password supplied had an extra character appended to the end. Comparing the 'encrypted' version indicated exactly the same string with the exception of two extra characters on the end – the other 20 characters were the same as a successful login.
- The second attempt used the correct username, but a random set of characters as the password. The comparisons showed that the encrypted string had the same first seven characters, but the remainder were different.

These test indicate that the whole username and password string may not be used in the encryption process, but rather each piece (username and password) or individual character. This would further trivialise the process of trying to defeat the login credentials.

Measure Residual Risk

Through the process of conducting this audit, it is evident that there is considerable risk with the CacheFlow and it's implementation within LaP Engineering. These risks are found in both the way it has been implemented and deployed within the environment, but also generic issues or limitations with the CacheOS™ itself. To resolve some of these limitations would require investment in additional equipment, or the redeployment of obsolete equipment, to provide improved security provisions.

The important thing to note however is that many of the risks are faced from internal threat and not externally (Internet) launched attacks. The exposure from outside of the LaP environment was identified as solely being that the CacheFlow could be used as a remote proxy device. Whilst the security impact to LaP of this seems to be minimal, the potential liability is large. The CacheFlow could be used to perform hacking attempts, or illegal download of software, as just two

[13] http://download.cacheflow.com/support/common/docs/v2200/Technical_Notes/PUATN.pdf

examples. As the IP is registered to LaP, it will be their responsibility to prove that the access was not originating from within their environment – but with new laws in prosecuting against cyber crime, LaP may still be held accountable and liable.

The internal threats against the CacheFlow are predominantly around the ability for non-authorised people to gain access to it through poor measures of protecting the login security. Some key examples of this are:

- The full level of configurability of the CacheFlow is not available via the web connection. This means that either telnet or console is required. With all of the support staff being remote to the CacheFlow, in depth configuration requires the use of telnet, which passes the login credentials in clear text across the network.
- Web management of the CacheFlow will not timeout if left idle. This allows the opportunity for a malicious person to gain access to a logged in session.
- Access via the console does not require a password to enter into a first level configuration mode. Nor is it required to enter into the interface configuration option.
- The login credentials for a web management connection appear to use a relatively low level of encryption.

The CacheFlow has been configured to minimise the IP addresses from which management connections can be established. Whilst this will prevent people from out side the firewall being able to remotely gain access (should an error in this ACL implementation allow it), the current configuration is such that any internal IP address is approved for connectivity. With the above concerns over the requirement for telnet, the ability for the passwords to be gained from the network ensures that current restrictions based on IP address are ineffective. A further reduction in the approved IP addresses would need to be deployed to reduce the risk of unauthorised access to the CacheFlow.

The potential impact of unauthorised configuration level access to the CacheFlow is primarily the risk of a Denial of Service of Internet access for the LaP employees. It also presents the opportunity for actions such as:

- Filters of denied websites being altered, allowing employees access to sites previously blocked.
- The destination for logged events to be altered (syslog) and therefore users actions not available for review.
- The destination for the URL's accessed report to be redirected – this would then allow the person to visit undesirable sites without detection as the report would not be available for the authorized CacheFlow team.

The biggest win of the CacheFlow audit was its ability to provide a web proxy service to the LaP employees, and to limit this access in compliance with the company policies. This included the ability for the CacheFlow to log the access

made by users for future review and enforcement of company policies through filters.

Is the System Auditable?

The CacheFlow that was the focus of this audit is definitely an auditable device. Through the use of many stimulus tests, not only was the 'concept' of various configurations reviewed, but also the practical aspects of those configurations. With the audit being conducted on a device that is already in production, the opportunity to fully validate some of the documented configuration features of the CacheFlow were hindered. This however did not prevent the opportunity to validate the large majority of the audit steps depicted in Assignment 2's checklist.

A very large area of concern that was identified is with the lack of logging from the CacheFlow itself (CLI-C.7, page 48). During the audit, many intrusive scans and changes were performed, but the level of logging that exists with the current configuration failed to capture these activities. Due to it being in production, the level of logging on the CacheFlow could not be altered to examine the potential logging that is possible from the device. With the current poor level of logging, the CacheFlow could be the target of many attacks, none of which will be detected. This is further compounded by the configuration error that is preventing the CacheFlow from providing event logging direct to the CacheFlow administrator's email.

There was no method to audit the level of training that the CacheFlow administrators have. Whilst none of them have attended formal training, they have acquired on the job skills from the years of administration. There is no formal method to determine the skill-set, so this can only be measured based on the configuration of the device, and the ability of the employees to explain the why's and how's of the implementation.

The good audit features that the CacheFlow presented are the logging and restricting of web usage. In both tests for these features, the audit result was a pass. This provides the LaP management with the ability to not only enforce the limitation of non-business use of the CacheFlow (through filters), but also closely monitor the usage of sites that are not filtered, and determine any misuse of the service.

Assignment 4

Executive Summary

An audit has been conducted on aus-cf-int – the CacheFlow installed in the Australian head office of LaP Engineering. The purpose of the audit was to review the CacheFlow to determine the level of security of this device, along with its ability to meet appropriate policies and requirements of LaP.

The audit results indicate that the larger security threat to the CacheFlow is from internal employees. There is one considerable risk identified from an external source, and this is that the CacheFlow can be used from the Internet to visit websites. This does not allow access into LaP, however it does provide for potential legal concerns should the CacheFlow be used by an external person to perform illegal actions against any Internet facing companies. With the IP address of the CacheFlow being registered to LaP, the legal responsibility is with LaP to ensure that its employees or external parties cannot misuse its equipment. A simple configuration change on either the network equipment (blocking access to port TCP/80) or the CacheFlow itself (remove the HTTP service) can eliminate this threat.

From an internal perspective, the CacheFlow is open to attack and potential breach by the LaP employees located on the corporate network. The level of security surrounding login is not adequate – there is no means of enforcing the company's password policy, and the credentials when logging in are seemingly easy to recover from the network. Should unauthorised access happen, the person will be able to prevent Internet access for all Australian and New Zealand users, or have the potential to misuse the web connectivity and ensure that this is not detected through covering up or removing the 'electronic' evidence.

The CacheFlow does however provide a good ability to track employees' web activity, and also prevent access to sites that are accessible, based on site name or IP address. In addition, the DR plan that exists is very effective, along with the documentation describing the physical and logical installation of the CacheFlow.

In overall summary, whilst the CacheFlow is very adequately able to perform its primary function of providing World Wide Web connectivity for LaP employees, it has not been deployed in a very secure fashion. Some of these security related issues are a result of the method of deployment, whilst some are inherent in the actual CacheFlow design, which would require additional investment to rectify. The requirement of time and cost to address these issues is highly recommended – the good practices currently deployed can be circumvented if the weaknesses are exploited.

Audit Findings

This section will provide greater details on the primary areas of concern that were identified during the audit. Whilst there were good aspects, these will not be detailed here, as the purpose of this is to highlight the concerns and areas requiring corrective action.

Audit Finding 1: Unauthorised usage of CacheFlow from the Internet.
Priority: Critical
Reference: CLI-D.2, page 56

Observation
Machines connected directly to the Internet can use the CacheFlow to proxy their World Wide Web requests. This was determined through an Internet launched vulnerability scan against the CacheFlow, which detected that port TCP/80 was accessible. Tests were conducted by configuring an Internet connected machine to use the Internet routable IP address of the CacheFlow as its proxy server, with TCP/80 as the port. Attempts were made to access Internet facing web sites, all of which were successful. When attempts were made to access intranet web sites, this was not successful.

Background/Risk
The CacheFlow has been deployed into LaP to provide Internet connectivity for the employees. As it can be used by non-authorised parties to browse the web, not only does this utilise the network bandwidth of LaP adding a cost to the company, but also infers that any malicious activities performed by these people will be attributed to LaP. If these activities result in legal action, LaP will be required to prove that the access was not from an employee. The magnitude of this risk is dependent on the malicious activities performed. For example, if the proxy is used by an attacker to illegally download software, the complaint of this action will be directed at LaP as the owner of the offending source address.

Recommendation
Configuration changes would be required to completely remove this risk. Neither of these are difficult changes, and could be performed with no disruption to the web connectivity. In both cases, the access to port TCP/80 will be removed from Internet availability, which is the root cause of this problem. The two configuration options available are:

1. Remove the HTTP (TCP/80) service from the CacheFlow. This will halt the ability for remote proxying on this port for both internal and external users. However, as this service is not used internally, there is no need for this to be configured.
2. Modify the ACL's between the CacheFlow and the Internet to specifically block TCP/80. Preferably, all ports below 1023 should be blocked to prevent any traffic that is not part of an internally initiated communication out to the Internet from being possible.

The existence of this problem is due to the CacheFlow being configured with more services than are actually required. This could be a result of planned changes to the environment never making it into production, or a result of the lack of formal training of the CacheFlow administrators.

To fully ensure that the CacheFlow is secured from the Internet, a full analysis on the router and access control lists should also be performed. Standard configuration documentation that details how the CacheFlow must be configured should be created. This documentation should be updated every time a change is made to the CacheFlow configuration. Updates to the

documentation need to be included as part of the change management process.

Cost
There is no monetary cost to this recommendation. Simple configuration changes would address the problem. The expectation is that one hour of an engineers time would be all that is required to rectify this issue. For a full audit of the Internet facing router and its access-list configuration, one week should be allowed.

Due to no financial outlay to correct this problem, the advantage of taking some proactive action is strongly encouraged. This will address both the legal issues, but also the potential damage to company brand and image. The cost of legal liability should malicious actions be performed exploiting this risk are far greater than the required effort to resolve the issue.

Compensating Controls
TCP/8088 was not available from the Internet, as such this port may already be explicitly denied.

Audit Finding 2: Potential for unauthorised login access.
Priority: High
Reference: CLI-A.1, page 36; CLI-A.3, page 40; CLI-A.6a, page 43; CLI-A.9, page 45; CLI-C.7, page 48; CLI-D.3, page 59

Observation
The current implementation and abilities of the CacheFlow make it very likely that an internal employee with knowledge and an interest in gaining access to it, will be able to do so. There are several areas of the audit that illustrate this problem. Firstly, the heavy reliance on telnet to perform in depth technical configuration of the CacheFlow is resulting in login credentials traversing the network in the clear. This can be seen in Figure 16, earlier in this paper. As such, a simple sniff of the network traffic can provide the username and password. Add to this that a single username and password is used for all administrators accessing the CacheFlow, it will be difficult to identify if an unauthorised access has been made.

Not quite as straight forward as telnet, but capturing the network traffic of a web management login gives a very good grounding to defeat the security. Figure 26 shows a capture of network traffic, and it can be seen that the username and password is passed (although this information was removed fore security reasons). Whilst this is in an encrypted state, as detailed in the report for CLI-D.3 (page 59) the level of encryption appears to be quite weak.

The other area that creates a high risk situation is with the configuration of the CacheFlow that allows any IP address from the LaP intranet to be authorised

as the source of a management connection (web and telnet). Figure 11 illustrates this configuration setting.

Background/Risk

The risk that is posed by this problem is that the current setup makes it quite a trivial process for an unauthorised person to be able to gain access to the CacheFlow. As this threat has been limited to people with access to internal connected machines (whether they are authorised people, or have defeated company physical security), the impact is slightly minimised. However, with access to the CacheFlow it is possible to cause a Denial of Service situation where the CacheFlow is modified in such a way that it is no longer able to proxy or cache web traffic. The business impact of this is that legitimate need for web connectivity would be lost, thus creating issues in being able to meet customer demand, or perform core business functions that are reliant on connectivity to the Internet.

Further to this, a malicious person would be able to modify the CacheFlow such that filters could be removed effectively removing web site restrictions, and all this could be performed without administrators knowing due to the minimal levels of event logging (see CLI-C.7). A final risk that could be faced is if the 'trespasser' is to change the login name and password for remote access. This would prevent the legitimate administrators from being able to connect remotely!

Recommendation

There are several items that would be required to address the root cause of this problem, which is the inability of the CacheFlow installation to provide strong user authentication methods. Due to the inability of the CacheFlow to provide a more secure means of remote connectivity (such as Secure Shell (SSH)), restrictions need to be put in place on the IP addresses of the machines allowed to access the CacheFlow. This way, even if the login credentials were 'sniffed' off the network, the attacker would need to either connect to a machine with an authorised IP address, or 'pretend' to be one of those machines by spoofing the IP address.

A management server needs to be deployed into the environment, and the CacheFlow configured to only allow this IP address to have authorisation to make a management connection. If this management server was deployed onto the same LAN as the inside leg of the CacheFlow it would limit the exposure to the login credentials as they would only be passed between the two devices on the single network.

A final recommendation to add an extra level of security would be to change the default TCP/23 port for telnet. As highlighted in Figure 20, it is possible to 'edit' the ports that are used for the different services. If a person was sniffing the network, they would be getting more information than is realistically possible to

filter through. To prevent this, filters may be set to review only telnet traffic (i.e. port TCP/23). If a non-standard port is used, then a filter looking for TCP/23 traffic may in fact allow the clear text login information to pass through undetected on a non-standard port.

Whilst this solution would considerably alter the way the CacheFlow is supported, the benefits of securing the access would outweigh the process changes required. To fully ensure accessibility, a second management server should be considered in the event that the primary server is unavailable. All these recommendations need to be included in configuration documentation to ensure that future implementations maintain the security of the CacheFlow. This also assists with ensuring a standardised configuration is deployed and administrators are able to support the CacheFlow easily.

Cost

The recommended solution requires the placement of a dedicated management server (or two if redundancy is included) to be used to access the CacheFlow for management purposes. For this to be achieved, hardware would be required. As this server would spend much of its time idle, and is only proposed as a Citrix or pcAnywhere server, the hardware requirements would be quite minimal. It would be expected that hardware would be readily available to perform this function – as a system is replaced or obsolete, it could be redeployed as the management server. This would then leave the costs associated simply with the configuration of both the server and the CacheFlow. One day would be required for the server configuration and deployment, whilst one hour for CacheFlow configuration (modification of the 'access list' setting as with Figure 11) and testing of the overall changed environment.

Compensating Controls

There are no compensating controls for this finding.

Audit Finding 3: Use of telnet allows full view of all inter device communication.
Priority: High
Reference: CLI-D.1, page 49

Observation

During the review of the results from the NMap scan, investigation was performed into the inherent weakness of the telnet application. Whilst there were no surprises here, the issues with information being passed in the clear were documented.

Background/Risk

The design of the telnet application provides minimal security, as all traffic between the client and server is sent across the network in the clear. This means that not only is the username and password clearly available through the use of a network sniffing tool (see Figure 16), but also all information

passed within the communication (both commands entered and the results displayed).

Through capturing this information direct from the network, not only would the login credentials be provided to an unauthorised person but also other information such as configuration details. This may allow the attacker to gain access to the CacheFlow, or at a minimum (if the beginning of the telnet communication was not captured) to obtain sensitive configuration information, allowing a plan for attack to be created.

Recommendation

Due to the high risk of the telnet service, as highlighted with the Retina scan (see Appendix C and CLI-D.2), ideally this service would be disabled, removing the root cause of this weakness. At a minimum, the port used should be set to a non-standard one. As the Command Line Interface (CLI) presented by both the telnet and console connectivity is required to perform some of the more in depth technical configuration, this access mode is required. Whilst the recommendation put forward with Audit Finding 2 helps to mitigate the risk, telnet is still enabled and therefore the risk of information being captured off the network still exists. To allow for telnet to be disabled, but still provide the remote ability to perform CLI configuration, a device such as the Cisco Access Server could be deployed. This could be connected to the serial port of the CacheFlow, and Secure Shell could be used to connect from the client to the Access Server. This would ensure that the login credentials were sent in a secure fashion. Once authentication to the Access Server is approved, access to the console CLI would allow the full functionality of that offered by a console connection, which is equivalent to telnet.

Cost

The recommendation outlined in this finding requires a Cisco Access Server (or equivalent), along with the appropriate cable for connecting it to the CacheFlows serial port. From discussions with other teams, a Cisco Access Server has been deployed and is used by the Unix team for remote serial connectivity to their servers. There are three ports that are available, however it is unknown if the IOS contains the correct feature set to allow SSH to be configured. An IOS upgrade may be required, which may incur a monetary cost if extra FLASH or DRAM is required. The cable to connect the two devices would also be needed.

Compensating Controls

If the recommendation put forward in Audit Finding 2 was to be deployed, then the high risk associated with the telnet port is largely mitigated, as the information is not passed across multiple networks, thus reducing the ability for this to be captured from the network.

Audit Finding 4: CacheFlow listening on ports that are not required.

Priority: Medium
Reference: CLI-D.1, page 49; CLI-D.2, page 56; CLI-D.3, page 59

Observation

Through the running of an NMap port scan (CLI-D.1) and a Retina vulnerability scan (CLI-D.2) against the CacheFlow, unexpected ports were identified. In both cases, these scans were conducted from the Internet as well as the intranet. To determine if these ports were actually required, investigations were performed into the purpose of the services using those ports. In most cases, the ports were performing required functions, however in some cases the features that the services offer, are not in use by LaP. As such, the CacheFlow is potentially open to an increased number of threats.

Background/Risk

A common practice to increase the level of security to a device is to eliminate all services available that are not actively used. As the number of services available increases so to does the number of points of potential attack, or the areas of weakness with the deployment. These attacks can range from people trying to determine information, attempts to obtain access or even the ability for the services to be abused by unauthorised parties. As was highlighted in CLI-D.1, with the ports that are open, NMap was able to take a reasonably accurate guess at the operating system. Whilst the guess was not exact, NMap did detect that the device is a CacheFlow, which gives attackers a point from which to start their attack. Of even more relevance, the CacheFlow has the potential to be used by unauthorised persons, as has been detailed with Audit Finding 1.

Recommendation

It has been discussed within CLI-D.1 that LaP is not using the 'transparent' feature that the CacheFlow offers. Yet as the screen shot from figure 20 shows, both HTTP (TCP/80) and FTP (TCP/21) have been enabled in transparent mode. The risk of this was highlighted through the tests from CLI-D.2, where it was demonstrated that the CacheFlow could be used from the Internet as a proxy server. If port TCP/80 was not listening, then this risk would not have been present.

The method of correcting this finding is through the removal of all ports that are not required. The ports identified that fit into this category are:

TCP/80 – Transparent HTTP
TCP/21 – Transparent FTP
TCP/113 – Ident server for SOCKS Authentication

The first two of these ports can easily be removed, as highlighted with Figure 20. However TCP/113 seems to not be a configurable service/port. As such, if there is no way that the port can be disabled on the CacheFlow, then a block to this port should be put in place at the network layer.

This issue stems from a lack of configuration documentation and poor planning during deployment. To ensure a secure CacheFlow is deployed in the future any recommendations that are implemented must be included in the appropriate documentation.

Cost

The cost of this recommendation is in man hours only. To remove the FTP and HTTP is a simple CacheFlow configuration change, which would take less than half an hour to perform. Some time may be required to investigate TCP/113 and see if it is possible to disable this port within the CacheFlow. Four hours should be allowed for this research, and if details cannot be identified, then a network engineer can apply an access-list addition to the network layer, which would require half of an hour to complete.

Compensating Controls

Deploying an access-list onto the intranet router could be one way of limiting the ports that are 'available' on the CacheFlow – security by obscurity.

Audit Finding 5: Weak logging of events concerning the CacheFlow itself.
Priority: Medium
Reference: CLI-C.7, page 48

Observation

When performing the test plan from CLI-C.7, it was identified that the level of logging performed by the CacheFlow with reference to events concerning it, is not acceptable. This was evident based on a sample of the events logged (see Figure 12) after some intrusive tests had been run against the CacheFlow. A review of the event logging level indicates that only the two highest levels of events are currently being logged, with a further two levels available – see Figure 13. The CacheFlow does provide the ability for information to be e-mailed to administrators, but this is currently incorrectly configured and hence no e-mails are being sent.

Background/Risk

When people with malicious intent are launching attacks against systems, they would most likely leave some form footprint or tell tale sign of their actions. Plus, in the lead up to the attack, some preliminary 'investigation' may have taken place, that would also leave some form of evidence. If the level of logging is not able to detect these preliminary actions, then it is equally likely that the actual attack may also go undetected. If an attack is not detected, then you will never know if and when an attack has been successful. With the CacheFlow acting as a proxy device, if it were breached, there is every chance that it would allow the attacker access to the LaP intranet, and any web sites housed therein. The potential loss of intellectual property along with brand image could have a severe negative impact to the company's profitability.

Recommendation
Three key steps would be required to enhance the level of logging, and the ability for this to be used to take corrective actions should events be detected.

Tests should be performed on the additional two levels of logging (Informational and Verbose) to identify the types of details logged. The amount of log information generated also needs to be known to determine the ability of the syslog server to store this information. The testing should include various attacks against the CacheFlow to identify what information is logged. With this information, custom scripts should be created to analyse the syslog.log file, and make some alert to the support staff should events considered 'malicious' be detected.

To also ensure that the CacheFlow administrators are aware of the status of the CacheFlow at all times, the SMTP server needs to be updated to a valid server that will allow the status e-mails to be delivered.

Once again, a lack of configuration documentation and poor planning during deployment has caused this problem. To ensure future CacheFlow deployment is done in a secure fashion, any recommendations that are implemented must be included in the documentation.

Cost
The reconfiguration of the CacheFlow to ensure that e-mails will be sent to the administrators requires five minutes of reconfiguration. To test the extra levels of logging offered by the 'informational' and 'verbose' options, a week should be set aside. This will not require a solid week dedicated to this, but would potentially take between eight and 16 man-hours.

A further week would ideally be available for a coder to create a script/program to analyse the syslog.log file looking for the events as identified during the week of testing the additional logging.

Compensating Controls
The CacheFlow administrators are already configured to receive the system status e-mails – as such it is likely that this functionality has been used in the past. The CacheFlow is also configured to log the events to a remote syslog server, which assists in the ability to quickly deploy the above recommendations.

Audit Finding 6: Lack of idle timeout setting for web management connectivity.
Priority: Low
Reference: CLI-A.7b, page 44; CLI-A.8, page 45
Observation
When performing the tests to check for idle timeout, the web management sessions were shown to not timeout an authenticated session.

Background/Risk
The lack of an idle timeout for the CacheFlow web sessions present an additional opportunity for unauthorised parties to gain access. If a system administrator does not shutdown the web browser when they have finished performing changes or reviews of the CacheFlow, this presents that ability for an attacker to gain access to the CacheFlow without the need to know the username and password. Administrative access to the CacheFlow presents the opportunity for the person to cripple the Internet connectivity for LaP, or make changes from which they could benefit (removing web site filters, etc). Even worse, the changes could allow external people to use the CacheFlow to access internal web sites, and therefore confidential and private information.

Recommendation
From the review of available CacheFlow configuration documents, there are no references to any ability to enforce an idle timeout on a web management connection. As such, there are no recommendations that can be enforced to specifically address this problem. The recommendation that was put forward in 'Audit Finding 2' can however assist. As the remote management software provides the ability to drop connections that have been left idle, this can then be relied on to perform closure of idle sessions.

Cost
As there are no recommendations to explicitly address this problem, the costs identified for the 'Audit Finding 2' recommendations can be shared with this item.

Compensating Controls
As has already been detailed under 'Audit Finding 2', it is possible to deploy a management server that will be used to establish all web management connections. Through the use of the remote management software such as pcAnywhere, it is possible to configure an idle timeout[14]. This will allow a web session to be terminated through the disconnection of the remote management software itself.

An additional step that can be put in place to help to mitigate this threat is to ensure that the client systems used by the administrators have a password protected screen saver set to come on at an interval of five minutes of system inactivity.

Audit Finding 7: Poor ability to enforce strong password practices.
Priority: Low
Reference: CLI-A.3, page 40

[14] Symantec pcAnywhere User's Guide (ftp://ftp.symantec.com/public/english_us_canada/products/pcanywhere/pcanywhere32/ver11.0/manuals/pca_user.pdf) page 165.

Observation
When reviewing the current password it was found to not be meeting the company requirements for complexity and aging. It was also found that it was not possible to configure the CacheFlow to enforce LaP's password policy and standard.

Background/Risk
The need for strong password enforcement is key in helping to prevent unauthorised access to the CacheFlow. If an easy password is used, then brute force attacks to break the password will take less time. Similarly, the longer a password is used, the more likelihood of it being made available to unauthorised people through either accidental exposure, or a longer time being available to attempt to crack the password. As has already been emphasised in this report, defeating the password defence of the CacheFlow will allow the attacker to have access to break the Internet connectivity, or perform changes from which they could benefit.

Recommendation
A process needs to be created and conveyed to the CacheFlow administrators. This is the primary issue that is allowing this to be a problem. This process would need to cover the key areas of the password policy, including:

1) Enforcement of a strong password.
2) Enforcement of the appropriate aging requirements.
3) Ability to adhere with the password re-use specifications.

To assist with the enforcement of this policy, particularly one and three above, an account could be created on a Unix system. This server would need to have password enforcement tools installed that are configured to meet the password policies. Before a password can be set on the CacheFlow, the new password would be tested on this Unix account. If the change is successful, then this new password can then be used on the CacheFlow.

Cost
As this recommendation is primarily based around the defining of a process, the cost is in person time only. To setup the server allowing the team to use this, and then the documenting of the process should take not more than two business days. If new tools need to be installed onto the server to allow the password policy enforcement, this may extend the time required, and also add a financial cost if a commercial application is recommended.

Compensating Controls
If the details as described in Audit Finding 2 are implemented, then the level of password protection is largely offset, as the source of the management connection attempts must be the authorised server. This server will be able to enforce the password policy as set by the LaP Security team. It does not however ensure that the CacheFlow itself is in compliance with the policy.

References

1. Combs, Gerald. Ethereal – Network Protocol Analyzer, version 0.9.11. Ethereal Web Site: http://www.ethereal.com (Last Accessed: April 13, 2003)

2. James, Geoffrey, "The Auditors are Coming, the Auditors are Coming … and that Could be Good News for You". CIO Magazine, April 15, 2003. http://www.cio.com/archive/041503/audit.html. (Last Accessed: June 1, 2003)

3. Reif, Peter. "Re: httpd to squid native log format convertor?" January 7 2000. http://www.squid-cache.org/mail-archive/squid-users/200001/0178.html (Last Accessed: June 12, 2003)

4. Stewart, Brian "Router Audit Tool: Securing Cisco Routers Made Easy!", March 2002. http://www.sans.org/rr/paper.php?id=238 (Last Accessed: May 31, 2003)

5. Blue Coat Systems "CacheOS Edition™ CA 4.1.10 Service Build 1 Release Notes". Document Revision: 1.01 (March, 2003). Copyright 2002 Blue Coat Systems, Inc. http://download.cacheflow.com/release/CA/4.1.10SB1/relnotes.htm (Last Accessed: June 18, 2003)

6. Blue Coat Systems "Course Descriptions." Copyright 2003 Blue Coat Systems Inc. http://www.bluecoat.com/resources/training/courses.html (Last Accessed: June 27, 2003)

7. Blue Coat Systems, News Releases 2002, copyright Blue Coat Systems 2002. http://www.bluecoat.com/news/releases/2002/082102_cflo_2bcs.html (Last Accessed: May 15, 2003)

8. Blue Coat SG400 Product Overview, copyright 2002, Blue Coat Systems, Inc. http://www.bluecoat.com/products/sg400/index.html (Last Accessed: June 2, 2003)

9. "CacheFlow 500 Data Sheet version 1.0", copyright 8/99 CacheFlow Inc. http://www.consulintel.es/Html/Productos/Cacheflow/DataSheets/cf500_data.pdf (Last Accessed: June 2, 2003)

10. "CacheFlow 500ec Series Installation Guide", copyright 1999 – 2000 CacheFlow Inc. http://www.cacheflow.com/files/installguides/cf500ecins.pdf (Last Accessed: June 2, 2003)

11. CacheFlow Security Advisories (Blue Coat Systems), copyright 2003 Blue Coat Systems, Inc. http://www.bluecoat.com/support/knowledge/security_advisories.html (Last Accessed: June 19, 2003)

12. CacheFlow Software Download Area, copyright 2002 CacheFlow Inc. http://download.cacheflow.com/release/CA/4.1.00-docs/CAupgradeNEW.html (Last Accessed: June 18, 2003)

13. CacheFlow Technical Note: "Proxy User Authentication Using CacheOS™ Version 2.1". Copyright 1999 CacheFlow, Inc. http://download.cacheflow.com/support/common/docs/v2200/Technical_Notes/PUATN.pdf (Last Accessed June 26, 2003)

14. "CacheOS 3.0 – Management and Configuration Guide", copyright 1997 – 2000 CacheFlow Inc. http://www.cacheflow.com/files/installguides/Management_and_Configuration_Guide_3_0.pdf (Last Accessed: June 29, 2003)

15. "CacheOS Release Notes for CA v4.0.16." Date: 03/1/2002, Document Revision 1.01 (07/26/2002). Copyright 2002 CacheFlow Inc. http://download.cacheflow.com/release/CA/4.0.16/relnotes.htm (Last Accessed: June 18, 2003)

16. "CacheOS Version 2.2.1 Management and Configuration Guide", copyright 1997 – 2000 CacheFlow Inc. http://www.cacheflow.com/files/installguides/cfosconfig.pdf (Last Accessed: June 29, 2003)

17. Common Vulnerabilities and Exposures. Copyright 2003 The MITRE Corporation. Last Updated Thursday June 26, 2003. http://cve.mitre.org (Last Accessed: July 1, 2003)

18. "Good Stuff IT Services", copyright 2003 Good Stuff IT Services. http://www.good-stuff.co.uk/useful/portfull.php (Last Accessed June 27, 2003)

19. ISACA (Information Systems Audit and Control Association) www.isaca.org. (Last Accessed: July 3, 2003)

20. "Router Security Configuration Guide Version 1.1", September 27, 2002. Report Number: CF-040R-02. http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf (Last Accessed: June 1, 2003)

21. SANS Institute “Track 7 – Auditing Networks, Perimeters and Systems Course notes”, copyright 2003, SANS Institute

22. SANS Posted Practicals for GIAC Systems and Network Auditor (GSNA) – (http://www.giac.org/GSNA.php) (Last Accessed: June 17, 2003)

23. SANS Reading Room (http://rr.sans.org) (Last Accessed: June 27, 2003)

24. SecurityFocus, copyright 1999 – 2003 SecurityFocus. http://www.securityfocus.com/ (Last Accessed June 27, 2003)

25. “Symantec pcAnywhere User’s Guide”, copyright 2003 Symantec Corporation. ftp://ftp.symantec.com/public/english_us_canada/products/pcanywhere/pcanywhere32/ver11.0/manuals/pca_user.pdf (Last Accessed: June 27, 2003)

26. The Center for Internet Security, copyright 2001 – 2003 Center for Internet Security. http://www.cisecurity.com/ (Last Accessed: June 19, 2003)

Appendix A: LaP Employee Business Conduct

Important note: sections of LaP's true Employee Business Conduct have been omitted, as they were not relevant to highlight the purpose of its inclusion here.

In order for you, an employee of LaP Engineering to conduct company business, a wide variety of assets are provided for your use. These assets include but are not limited to computers, communications systems and other equipment and materials. While occasional use of these resources and assets for incidental personal activities is allowed, it is your duty to ensure that this usage is kept to a minimum. You must also be in accordance with all LaP policies and guidelines when performing this incidental personal activity.

Excessive use of LaP resources for personal use increases the expenses to LaP, and reduces the availability of these resources for LaP's business needs. This has an adverse effect, and may impact your job performance within the organization. The below rules apply to your use of LaP resources, whether located within an LaP facility or while remote.

- Staff may occasionally use LaP's resources to send or receive personal messages, access the Internet for non business-related purposes, or to create personal documents or files. This activity must however be kept to a minimum.
- LaP resources cannot be used in any activity that is in violation of the law. You may not allow any non-LaP employee, including friends and family, to use LaP resources for any purpose. You must not use any LaP resource to create, transmit, store or display messages, images or materials that are for personal gain, solicitations, chain letters, or are threatening, sexually explicit, harassing or otherwise demeaning to any person or group.
- Inspection. LaP has the right to inspect all company resources that you may use for personal activity, inclusive of computers, servers, telephones, voicemail systems, desks, lockers, cabinets, vehicles. You must not have any expectation of personal privacy in any messages or information stored on a resource owned by LaP. LaP may inspect persons and property on LaP premises at any time and without notice, subject to applicable local laws.

Appendix B: LaP Password Policy and Standard

Important note: sections of LaP's true policy have been omitted, as they were not relevant to highlight the purpose of its inclusion here.

Summary

This policy establishes the minimum requirements for password management of LaP Engineering and its employees. In this policy, a password is referencing any string that is required in conjunction with a user ID to gain authorization to any operating system, application or network device used with LaP. In circumstances where a user ID cannot be entered, the single string of information used to gain authorization is the password.

Scope

This policy applies to all operating systems, Database Management Systems, applications, network operating systems, and devices that require a user ID and password.

Password Selections and Rules

Passwords complexity must be enforced on all passwords created and maintained on LaP equipment. Where it is possible through the technology, the complexity requirements as stated in this policy must be enforced when passwords are created and/or changed. The standards that passwords must meet are:

1. The password must contain a minimum of eight characters
2. An attempt of five incorrect logins without an intervening successful login must result in the account being locked out, where the technology allows it. A minimum of 60 minutes is required before the account will re-enable on its own terms. An authorized support person is able to re-enable the account prior to this 60 minute window.
3. At least three of the following four rules
    a. At least two numeric character (0 – 9)
    b. At least one special character (/, [, -, =, +, !, #, $, white space, etc.) chosen from the ISO 8859-1 (Latin-1) character set.
    c. At least two lower case character (a – z)
    d. At least one upper case character (A – Z)
4. Accounts that allow administrative access must be aged to no more than 45 days. If the account is for non-administrative access, then the password must expire at not more than 90 days after it was first set.
5. A password must not be able to be changed within 24 hours of it being changed. This does not apply to passwords for brand new accounts, which must be changed the first time the account is accessed.
6. The history for password re-use must be set to at least three. This means that if a person wishes to cycle through passwords, they will have to have at least four passwords in the cycle.

Appendix C: Intranet Report from Retina Scan

Note: some sections of the report have been removed due to lack of details in those sections.

Retina® Network Security Scanner
Superior Vulnerability Assessment & Remediation Management

Executive Summary 1 - 1

On Retina performed a vulnerability assessment of 1 system[s] in order to determine the security posture of those systems and to outline fixes for any found vulnerabilities.

The systems audited were: 010.150.162.243

Retina's goals in this attack were as follows:

- Perform network scan to determine all systems and services within your scan range.
- Analysis of those systems and services and perform information gathering techniques.
- Attack and exploit any known holes in the server software and examine the likelihood of being vulnerable to those attacks.
- Generate information on how to fix all found vulnerabilities.
- Create security report for your organization.

Your network had 0 low risk vulnerabilities, 2 medium risk vulnerabilities, and 1 high risk vulnerabilities. There were 1 host[s] that were vulnerable to high risk vulnerabilities and 1 host[s] that were vulnerable to medium risk vulnerabilities. Also on average each system on your network was vulnerable to 1.00 high risk vulnerabilities, 2.00 medium risk vulnerabilities and 0.00 low risk vulnerabilities.

The overall security of the systems under review was deemed rather insecure. Your organizations network is completely vulnerable. It is imperative that you take immediate actions in fixing the security stance of your organizations network.

Retina® Network Security Scanner
Superior Vulnerability Assessment & Remediation Management

Vulnerability Summary 2 - 1

Introduction

This report was generated on 16/06/2003 07:43:15. Network security scan was performed using the default security policy. Security audits in this report are not conclusive and to be used only as reference, physical security to the network should be examined also. All audits outlined in this

report where performed using Retina - The Network Security Scanner, Version 4.9.94

Retina® Network Security Scanner
Superior Vulnerability Assessment & Remediation Management

Address 010.150.162.243 3 - 1

General: 010.150.162.243

Address: 10.150.162.243
No More Details Available

Report Date: 06/15/03 08:25:52 PM
No More Details Available

Domain Name: aus-cf-int.au.lap.com
No More Details Available

Ping Response: Host Responded
No More Details Available

Avg Ping Response: 694 ms
No More Details Available

Time To Live: 253
No More Details Available

Traceroute: <Details Removed>
No More Details Available

Audits: 010.150.162.243

Remote Access: TCP:23 - Multiple vendor login environment variable buffer overflow

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

CGI Scripts: TCP:8081 - Cacheflow CacheOS web admin vulnerability

Risk Level: Medium
Description: By sending a certain request, malicious hosts can view parts of web pages and URLs transferred through the cache at the time of exploitation.
How To Fix:
Upgrade to the most current version of CacheOS to eliminate this and possibly other security vulnerabilities present in the firmware.
URL1: CacheFlow Inc. (http://www.cacheflow.com/)
CVE: CVE-2002-0107
BugtraqID: 3841

Remote Access: TCP:23 - telnet service

Risk Level: Medium
Description: Telnet is a service that allows a remote user to connect to a machine. Telnet sends all usernames, passwords, and data unencrypted.
How To Fix:
Consult your user manual or help file for information on how to disable your telnet service. If no user manual or help file exists then contact your software vendor.
CVE: CAN-1999-0619

Miscellaneous: TCP:80 - Anonymous HTTP proxy detected

Risk Level: Information
Description: Retina has detected an HTTP proxy running on the scanned host that will process requests without user authentication. An anonymous proxy may be accessed without its owner's knowledge by malicious users and other individuals, in order to make their online actions more difficult to trace.
How To Fix:
We recommend configuring the HTTP proxy to require user authentication.
CVE: GENERIC-MAP-NOMATCH

Miscellaneous: TCP:8088 - Anonymous HTTP proxy detected
Risk Level: Information
Description: Retina has detected an HTTP proxy running on the scanned host that will process requests without user authentication. An anonymous proxy may be accessed without its owner's knowledge by malicious users and other individuals, in order to make their online actions more difficult to trace.
How To Fix:
We recommend configuring the HTTP proxy to require user authentication.
CVE: GENERIC-MAP-NOMATCH

Machine: 010.150.162.243

Open Ports: 6
No More Details Available

Closed Ports: 65529
No More Details Available

Ports: 010.150.162.243

21: FTP - File Transfer Protocol [Control]
Port State: Open

23: TELNET - Telnet
Port State: Open

80: WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
Detected Protocol: HTTP
Port State: Open
Version: SERVER: Unknown

113: IDENT - Authentication Service
Port State: Open

8081:
Detected Protocol: HTTP
Port State: Open
Version: SERVER: Unknown

8088:
Detected Protocol: HTTP
Port State: Open
Version: SERVER: Unknown

END OF REPORT

Appendix D: Internet Report from Retina Scan

Note: some sections of the report have been removed due to lack of details in those sections.

Retina® Network Security Scanner
Superior Vulnerability Assessment & Remediation Management

Executive Summary 1 - 1

On Retina performed a vulnerability assessment of 1 system[s] in order to determine the security posture of those systems and to outline fixes for any found vulnerabilities.

The systems audited were: 172.018.105.234

Retina's goals in this attack were as follows:

- Perform network scan to determine all systems and services within your scan range.
- Analysis of those systems and services and perform information gathering techniques.
- Attack and exploit any known holes in the server software and examine the likelihood of being vulnerable to those attacks.
- Generate information on how to fix all found vulnerabilities.
- Create security report for your organization.

Your network had 0 low risk vulnerabilities, 0 medium risk vulnerabilities, and 1 high risk vulnerabilities. There were 1 host[s] that were vulnerable to high risk vulnerabilities and 0 host[s] that were vulnerable to medium risk vulnerabilities. Also on average each system on your network was vulnerable to 1.00 high risk vulnerabilities, 0.00 medium risk vulnerabilities and 0.00 low risk vulnerabilities.

The overall security of the systems under review was deemed rather insecure. Your organizations network is completely vulnerable. It is imperative that you take immediate actions in fixing the security stance of your organizations network.

Retina® Network Security Scanner
Superior Vulnerability Assessment & Remediation Management

Vulnerability Summary 2 - 1

Introduction

This report was generated on 21/06/2003 08:44:47. Network security scan was performed using the default security policy. Security audits in this report are not conclusive and to be used only as

reference, physical security to the network should be examined also. All audits outlined in this report where performed using Retina - The Network Security Scanner, Version 4.9.97

Retina® Network Security Scanner
Superior Vulnerability Assessment & Remediation Management

Address 172.018.105.234 3 - 1

General: 172.018.105.234

Address: 172.018.105.234
No More Details Available

Report Date: 06/20/03 08:38:06 PM
No More Details Available

Domain Name: ausproxy.lap.com.au
No More Details Available

Ping Response: Host Did Not Respond
No More Details Available

Traceroute: <Details Removed>
No More Details Available

Audits: 172.018.105.234

Web Servers: TCP:80 - Malformed HTR Request - NT4
Risk Level: High
Description: A vulnerability in IIS involves an unchecked buffer in the filter DLLs for the following file types: .HTR, .STM and .IDC files. The .htr, .STM and .IDC extensions are used by ISAPI filters so an attacker can therefore overflow those ISAPI filters and remotely execute code as SYSTEM.
How To Fix:
Install the Microsoft supplied fix.
URL1: Microsoft Hotfix.

(http://support.microsoft.com/support/kb/articles/Q234/9/05.ASP)
URL2: Microsoft Advisory.
(http://www.microsoft.com/technet/security/bulletin/ms99-019.asp)
URL3: eEye Digital Security Advisory.
(http://www.eeye.com/html/research/Advisories/AD19990608.html)
CVE: CVE-1999-0874
BugtraqID: 307

Miscellaneous: TCP:80 - Anonymous HTTP proxy detected
Risk Level: Information
Description: Retina has detected an HTTP proxy running on the scanned host that will process requests without user authentication. An anonymous proxy may be accessed without its owner's knowledge by malicious users and other individuals, in order to make their online actions more difficult to trace.
How To Fix:
We recommend configuring the HTTP proxy to require user authentication.
CVE: GENERIC-MAP-NOMATCH

Machine: 172.018.105.234

Open Ports: 1
No More Details Available

Closed Ports: 65534
No More Details Available

Ports: 172.018.105.234

80: WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
Port State: Open

END OF REPORT

Appendix E: Data Centre physical access checklist

Data Centre Physical Access Controls	Rating Pass/Fail	Reason for Rating
1. Security measures are in place to adequately control and monitor access to the data centre.		
2. A list is maintained and updated of who has access.		
3. Those who have access have a business reason for that access.		
4. Procedures are in place to manage access authorization (including by the data centre owner).		
5. Procedures are in place for regular review of access authorization, badges and privileges.		
6. Processes are in place to control, log and escort all visitors to the operations centre.		
7. Operations Centre Security Policy is communicated to all employees.		
8. Are logs maintained for entry and exit details to/from the Data Centre?		
9. Do all areas of the data centre have cameras?		
10. Is there a central control and management console for the cameras?		