Global Information Assurance Certification Paper

GSNA Practical v4.0 Option 1

Audit of a Corporate Internet Gateway

Stuart Unsworth

April 14, 2005

Contents

Abstract

This report was written to satisfy the practical assignment portion of the SANS Institute's GIAC Systems and Network Auditor (GSNA) certification program and contains an audit of an Internet gateway used by a client of the author.

The document is divided into four main sections and two annexes:

- The first section introduces the context of the paper and identifies the target system to be audited.
- The second section presents a discussion on a risk based approach to auditing and provides a context of the risk analysis requirement for the paper. The three risks to be evaluated in the subsequent sections of the paper and the rationale for their choice are presented. The highlight of this section is that business risk management is the ultimate driver for IT security auditing.
- The third section develops tests that, when run, will result in the identification of the presence of vulnerabilities and their degrees of overall risk.
- The fourth section provides a summary of the findings from running the tests developed in step three and presents recommendations to improve the security of the gateway. An executive summary, using a risk based presentation, is included to conclude the findings.
- Annex A presents a colour coded, tabular overview (developed by the author) of the security configuration of the router evaluated.
- Annex B presents an edited version of the configuration of the router for reference.

2 Target Identification

The author was recently commissioned by a client to conduct a security assessment of the servers and infrastructure that comprise their internet facing environment. This company also had a subsidiary (known as 'Project Zebra') which had its own connection to the Internet using a Cisco 3600 router as a firewall. This connection had been installed by 'someone who understood a bit about networks'. Additionally, the subsidiary had a direct connection into the corporate backbone.

The parent company's management team was concerned that, should the subsidiary's Internet connection be successfully attacked, the whole network could be compromised. Architecture and security configuration assessments were required.

Accordingly, the objective of the assessment was to determine what, if any, risks existed for the company due to these connections to the Internet and, secondly, to determine suitable mitigation activities for identified vulnerabilities.

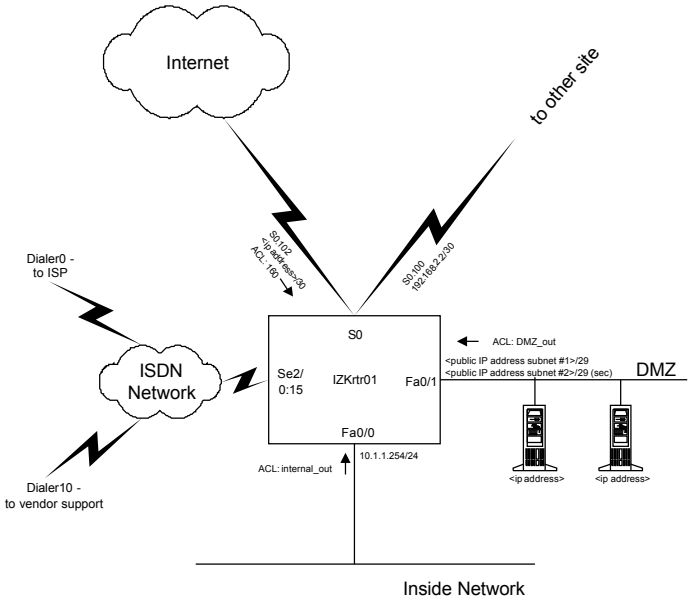
The scope of the overall audit was twofold:

1. An assisted network based vulnerability assessment (from the Internet) of both gateways; and

2. A review of the configuration of the subsidiary's Internet connected router.

If the assessment is 'assisted', the client provides as many details as possible about the infrastructure to the auditor before the scans begin. An unassisted test is when the client wants to see how much information can be readily obtained by 'an outsider' about the infrastructure and then how much an attacker can penetrate into the network. Both types of audit are useful – the unassisted version usually takes longer due to the additional research required by the auditor to find the (correct) targets.

In the context of this paper, the scope is reduced to analysing the three highest risks posed by the existence of the company's Internet connections. It was determined that these three risks were related to the Project Zebra internet connection, the network topology of which is shown below. The risks identified are discussed in the next section.



3 Risk Analysis

3.1 Definition of Risk

> Risk is the chance of something happening that will have an impact upon objectives and is inherent in everything we do: riding a bicycle or driving a car, managing a project, dealing with clients, determining work priorities, purchasing new systems and equipment, making decisions about the future or deciding not to take any action at all.

We manage risks continuously, sometimes consciously and sometimes without realising it, but rarely systematically. The need to manage risk systematically applies to all organisations and to all functions and activities within an organisation and should be recognised as of fundamental importance by all managers and staff. [1]

So, whilst "Auditing is a measure of conformance"[2], risk management is the ultimate reason why audits are performed. This applies not only to a company's financial audits, but to IT system/network audits as well. Expenditure on security hardware, software or time spent hardening servers, etc is a necessary function of general business requirements to run profitably, meet governance requirements and, in the most extreme case, preserve life itself (e.g. securing/isolating a nuclear power plant's control systems from unauthorised network access).

A risk management process[3] is presented in the figure below and provides some context for the second section of this assignment – the risk analysis. Risk analysis is an essential component of risk management.

Risk analysis is about developing an understanding of the risk. It provides an input to decisions on whether risks need to be treated and the most appropriate and cost-effective risk treatment strategies. [4]

The level of risk is the combination of the likelihood of a risk occurring, and the consequences if it does occur. Risk Analysis, therefore, involves consideration of the threat likelihood applied to an asset and an assessment of the consequences of the threat being realised. Threat likelihood can be affected by existing controls, which are considered in most circumstances. The combined outcome of the threat likelihood and consequences becomes the identified risk level:

Risk = Threat Likelihood x Consequence

Because risk is based on uncertainty, the results of a risk assessment are a function of probability. Probability can be generally determined in two different ways:

qualitatively or quantitatively. The quantitative approach uses a strictly numeric approach derived from modelling or real world data. Analysis using a qualitative approach will use factual information and expert opinion to derive the risk ratings. IT security risk analysis is typically qualitative in nature.

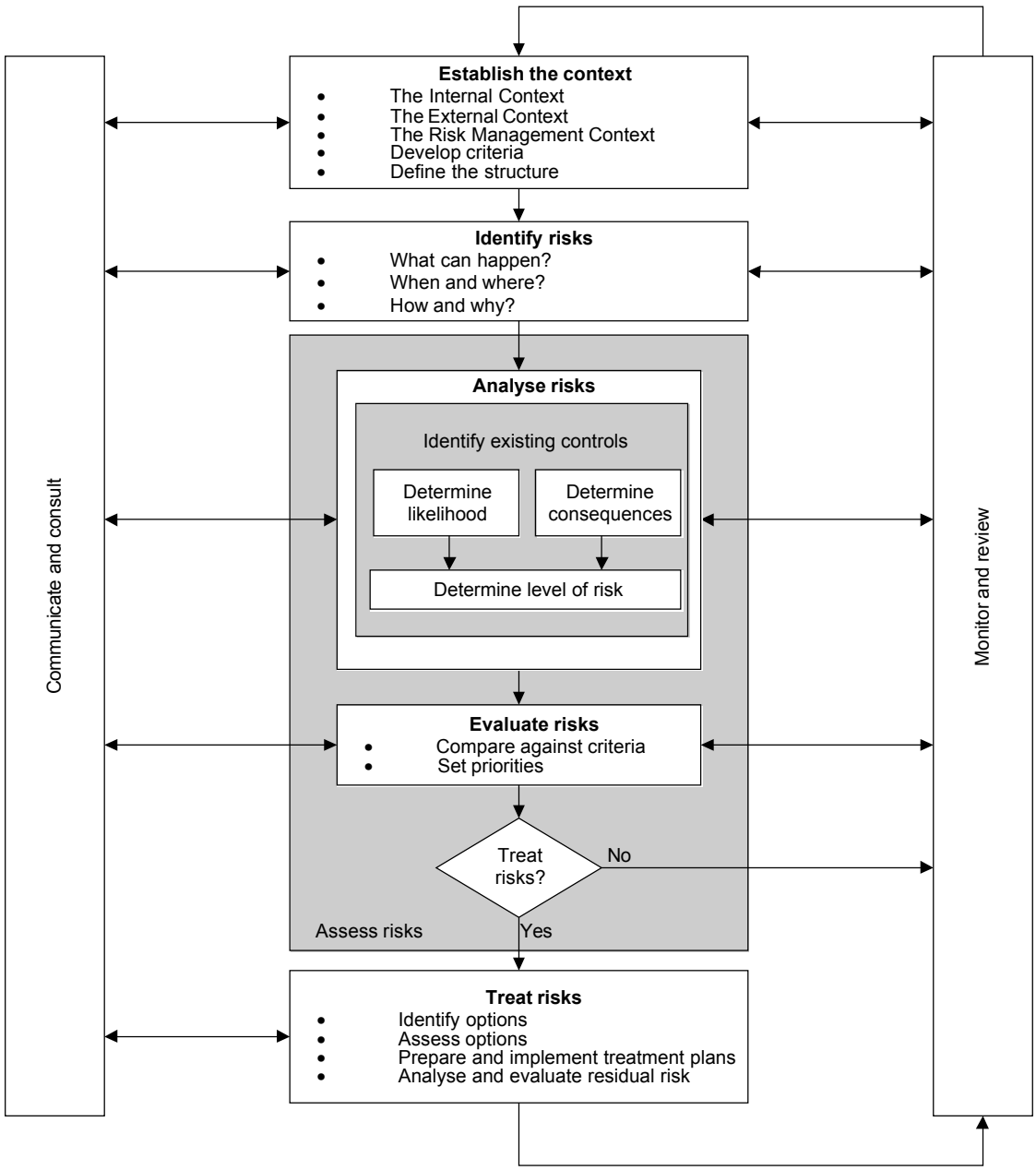


Figure 1 - Risk Management Process

3.2 Risk Identification

All too often information security is misunderstood to be merely a function of the IT department, whereas it should be seen in the context of overall business risk and addressed accordingly. Recent governance requirements (e.g. HIPAA, Sarbanes-Oxley) and the widespread publication of standards (e.g. ISO/IEC 17799[5]) have both been important drivers for a change in management attitude. Indeed, the 17799 standard provides us with 127 main controls and over 500 detailed controls that may be used when conducting enterprise wide risk assessments and policy development. The 17799 standard partitions information security into ten categories:

1. Security policy
2. Organizational security
3. Asset classification and control
4. Personnel security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Systems development and maintenance
9. Business continuity management
10. Compliance

Now, risks to a business may be ascertained in a number of ways. Two examples are:

1. Brain-storming (identification of risks by empirical analysis of business processes) and
2. Examining well documented controls and working backwards to determine what risks exist if each control is NOT in place.

Further, as can be seen from the risk management process in Figure 1 above, a necessary precursor to conducting a risk analysis is the completion of the risk identification phase. For this audit, a number of high level business risks were derived during discussion with the client ('Establishing the context') using the 17799 categories for reference. The primary aspect of the infrastructure that was determined to pose the greatest risk to the business was in the area of 'Access control'.

The specific issues for which the client required detailed attention are listed in the table on the following pages. The estimated threat and consequence levels were

determined in consultation with the client and, using the Qualitative Measures of Threat Level and Consequence found in Table 2 and Table 3, a Risk Rating was assigned to each issue. It is interesting to note that often prior to formally calculating the Risk Ratings clients will advise that “such and such” a risk is ‘critical’ to the business. Only once realistic threat likelihood and consequence values are assigned can a meaningful risk rating be determined. Without such objectivity all risks become ‘critical’ (which often means risks are not treated in an appropriate order).

Once the primary business risks had been identified the work of developing suitable tests to audit the infrastructure began.

Table 1 - Top Three System Impacts

	Issue	Scenario of Exposure	Possible effects	Estimated Threat Likelihood	Estimated Consequence	Calculated Risk[1]	Relevant ISO 17799 Section
1	Backdoor access into the parent company.	Exploitation of an insecure Internet gateway into the subsidiary's network coupled with 'intranet' connection to corporate network.	Compromise of corporate data and intellectual property. Internal file servers being compromised and subsequent loss of data confidentiality, integrity or availability.	Medium	Serious	High	9.4 – Network Access Control: Objective: Protection of networked services. Access to both internal and external networked services should be controlled. This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services by ensuring: a) appropriate interfaces between the organization's network and networks owned by other organizations, or public networks; b) appropriate authentication mechanisms for users and equipment; c) control of user access to information services.

[1] See Tables 2, 3 & 4 for risk calculation matrices

2	Security of Subsidiary's Internet connection	Exploitation of an incorrectly configured border.	Loss of data confidentiality, data Integrity or Availability of the Internet connection. Data confidentiality / integrity can be compromised should a GRE tunnel to a hostile location be created and configured as the default gateway on a border router.	Low	Minor	Low	9.4 – Network Access Control
3	Email spoofing	Exploitation of incorrectly configured or unpatched email server (i.e. access control policy not correctly implemented).	Loss of customer confidence and potential domain name blacklisting due to spam email/viruses emanating from the client's domain.	Low	Minor	Low	9.6.1 – Application Access Control Users of application systems, including support staff, should be provided with access to information and application system functions in accordance with a defined access control policy, based on individual business application requirements and consistent with organizational information access policy.

Table 2: Threat Likelihood Rating

Likelihood		
A	Very High	The event is expected to occur in most circumstances
B	High	The event will probably occur in most circumstances
C	Medium	The event should occur at some time
D	Low	The event could occur at some time
E	Very Low	The event may occur only in exceptional circumstances

Table 3: Qualitative Measures of Consequence or Impact

Consequence		
1	Insignificant	Low impact / loss
2	Minor	Medium impact / loss
3	Significant	High impact / loss
4	Serious	Major impact / loss
5	Critical	Huge impact / loss

Table 4: Qualitative risk analysis matrix - levels of risk

Qualitative risk analysis matrix - level of risk.					
Likelihood	**Consequence**				
	Insignificant	**Minor**	**Significant**	**Serious**	**Critical**
Very High	**Moderate**	**High**	**High**	**Extreme**	**Extreme**
High	**Low**	**Moderate**	**High**	**High**	**Extreme**
Medium	**Low**	**Moderate**	**Moderate**	**High**	**High**
Low	**Very Low**	**Low**	**Low**	**Moderate**	**Moderate**
Very Low	**Very Low**	**Very Low**	**Low**	**Low**	**Low**

(These tables are based on well accepted Risk Analysis methodologies, e.g. AS/NZS4360)

4 Testing

In this section detailed tests, corresponding to the three risks identified in Section 2, are developed. These tests will be subsequently used to determine whether the vulnerabilities exist or not. Often (to vary degrees) the details of the tests would be included in a *test plan* that would need to be approved by the client prior to the auditor performing the tests.

4.1 Backdoor Access Into The Parent Company

The security of the subsidiary's Internet connection was tested using a five step approach:

Activity 1: Host Discovery – employment of specialised tools to programmatically map the subsidiary's internet connection on the provided domain and IP address ranges;

Activity 2: Service Scanning – scanning for services that are present and listening on TCP/UDP service ports on hosts that are determined to be 'alive' as a result of Activity 1;

Activity 3: Information Retrieval – extraction of as much information as possible from the target system, for example, operating system types and application types; and

Activity 4: Vulnerability Scan – execution of scans on each target host determined to be 'alive' as a result of Activity 1 using a range of freely available and commercial tools.

Activity 5: Vulnerability Analysis – analysis of the results from the previous activities to 1) minimise/remove false positives and 2) determine the potential impact of the vulnerabilities. An assessment is also made as to whether further action, by way of vulnerability exploitation, is warranted. Such action would usually require written customer consent.

Some rules of engagement were also defined:

4.1.1 Rules for Determining Compromise

For each target host, the testing will be conducted to the point where the auditor is satisfied that a level of access has been attained that would be otherwise

unauthorised. The auditor will consider that unauthorised access has been obtained if any of the following actions can be performed:

- Able to read sensitive files (such as host configuration information);
- Able to write or modify files; and/or
- Able to execute arbitrary commands.

4.1.2 Rules for Halting a Test

The auditor will halt testing on a particular host if any of the conditions listed below are satisfied:

- Evidence of previous compromise is discovered;
- Further progression of the test will likely result in a required rebuild of the affected host to restore the secure state;
- Further progression of the test will likely result in a denial of service from the affected host; and/or
- The auditor identifies that an additional tool should be used to attempt exploitation of vulnerabilities on the host.

The auditor will use the agreed escalation procedure described below in the event that any of the conditions listed above arise.

4.1.3 Escalation Criteria

The characteristics of all identified vulnerabilities and associated host computer/systems will be analysed during testing. Those that are considered to fall into the Extreme or High impact categories will be immediately reported to the client. The potential exposure will be determined according to Table 5 below, an Impact Rating table developed for the author's employer.

Table 5: Guidelines for Determining Impact of Vulnerabilities

	Impact Rating				
	Extreme	**High**	**Moderate**	**Low**	**Very Low**

Attack Characteristics	Attack source (e.g. local, remote)	Remote	Remote	Either	Local	Local
	Ease of realisation	Simple	Simple	Complex	Complex	Highly Complex
	Resulting privilege level	Privileged	Privileged	Either	Unprivileged	Unprivileged
	Type of data access attained	Read, Write and Execute	Read and Write	Read or Write	Read Only	Read Only
	Certainty of result	Guaranteed	Probable	Possible	Unlikely	Theoretical
	Detectability	Undetectable	Knowledge of attack required	Detectable	Detectable	Detectable and captive
Target Characteristics	Number of vulnerable hosts	Many	Many	Some	Some	None
	Required access to vulnerable systems	Public	Public	DMZ	Inside knowledge required	Inside knowledge required
	Sensitivity of information processed	Highly sensitive or Personal Information	Sensitive	Internal Use	Internal Use	Public
	Sensitivity to business operations	Fundamental	Very Important	Important	Important	Unimportant

4.1.4 Test Details

Steps 1, 2 and 3 (Host discovery, service scanning and information retrieval) will be performed simultaneously using Fyodor's Nmap tool[6]. The root account on a Linux server will be used to conduct the scan. (The author notes that a comprehensive, self booting auditing CD incorporating current versions of Linux, Nmap, Nessus and many other tools can be downloaded from http://remote-exploit.org/[7]. For auditors that normally use a Windows based laptop, this tool provides nearly every pen testing tool you will need).

The following syntax will be used (note that the actual IP address has been changed to preserve anonymity):

```
# nmap -sT -P0 -O –p 1-65535 -oA TCPscan --append_output -sV -n -v 203.xxx.yyy.zz/28
```

A brief explanation of the command line options chosen follows:

-sT conduct a TCP scan (UDP scans usually don't work in a firewalled environment as every port appears to be open. They can also take an extraordinary amount of time).

-P0	do not attempt to ping the remote host – firewalls typically block ICMP these days.
-p 1-65535	scan ports 1 through 65535 (i.e. all TCP ports)
-oA TCPscan	record the results in all supported formats using the filename 'TCPscan'. Supported formats include: normal text, XML, and a text format that is grepable.
--append_output	the author uses this parameter to prevent accidental deletion of output files should a 'recall last command' be accidentally executed which then overwrites previously generated results. Such an accident can be very painful if the results took a very long time to run in the first place! (Yes, it's been done!)
-sV	Version scan probes open ports determining service & application names/versions.
-n	don't perform reverse DNS lookups on hosts being scanned – speeds up the scan a bit.
-v	verbose output – easier to monitor scanning progress with this enabled.
203.xxx.yyy.zz/28	the IP address range (supplied by the customer) to be scanned.

As the environment being audited is NOT protected by a firewall, UDP scanning will probably be successful. Accordingly, the following scan should be run:

```
# nmap -sU -P0 -O –p 1-65535 -oA UDPscan --append_output -n -v 203.xxx.yyy.zz/28
```

Step 4 involves the use of the Nessus vulnerability scanning tool[8]. The setup and operation of this tool is considered assumed knowledge for the purpose of this paper (otherwise see http://www.securityfocus.com/infocus/1741[9] and http://www.securityfocus.com/infocus/1753[10] for an excellent Introduction to Nessus from SecurityFocus).

A scan of the client's IP address space will be performed using the following options (and referring to the article: http://www.securityfocus.com/infocus/1741):

- Select the Enable plugin dependencies at runtime checkbox (see Figure 4 in the article) to minimise unnecessary testing
- Select 'Enable all but dangerous plugins' (see Figure 6) to prevent Denial of Service plugins from being run
- Enable Safe Checks (see Figure 7)
- Select Well-known service port scan (see Figure 8) – this will port scan privileged ports and some ports that some Trojans are known to use.

Once the scan is complete, the results can be analysed. Should Nessus not have a plug-in for any ports detected as open then manual tests will need to be performed

on an as-needed basis.

4.2 Security of Subsidiary's Internet Connection

The security of the subsidiary's Internet connection will be further tested by reviewing the configuration of the router used to connect and firewall their network. A three step process will be used:

Activity 1: Router Vulnerabililty Scan – run Nmap and (if applicable) Nessus against the router in a similar fashion to that described in Section 3.1.4. Scans should be run against both the Internet (serial) port address and the DMZ ethernet port address.

Activity 2: Router Hardening Analysis – review the configuration of the router using the Router Audit Tool[11] (RAT) and manual inspection to compare its configuration against best practice (as defined by the Centre for Internet Security's Cisco IOS Router Baseline).

(See http://www.giac.org/certified_professionals/practicals/gsna/0189.php[12] for a detailed article on the use of RAT).

Activity 3: Rule Base Analysis – review the Access Control Lists used to implement the subsidiary's access policy to ensure that the risk of unauthorised access into the network is minimised.

The router's configuration was supplied by the client for analysis (see Annex B) and is assessed during Activities 2 and 3.

The Router Audit Tool is run using the following command:

```
D:\temp> rat router_config_file.txt
```

This produces files providing the analysis (in HTML format) and a text file that can be modified and then run on the router to fix any problems that were discovered.

The output of the RAT will be converted (by hand) to a format that the author has developed. This format can be used to provide a better view (in the author's opinion) of the consistency (or otherwise) of router configurations across many devices in a network. In this instance, however, as only one device is being reviewed the visual impact is not as great. It is, however, still considered a useful tool from a management reporting perspective. One improvement that could be made to the table is to priortorise the setting findings.

The rule base analysis (Activity 3) is a manual review of the access lists deployed on each interface. The rule base structure will be checked for good practice. The business requirements for incoming and outgoing connections should be compared against the rules imposed by the router and observations made.

4.3 Email Spoofing

The security of the client email gateway will be tested using handcrafted attacks to simulate unauthorised proxying of email (although it was subsequently realised that Nessus has a plug-in that tests this anyway!).

The email gateway will be contacted on its SMTP TCP port from a host anywhere on the Internet using the following command:

telnet emailhost.domain.com.au 25

The following command is then sent:

HELO hackerdomain.com

A '250 emailhost.domain.com.au Hello' message should be received. Then send:

MAIL FROM:<spammer@bogusdomain.com.au>

A '250 Sender OK' message should follow. Then send:

RCPT TO:<victim@victimdomain.com>

If a '550 Unable to relay for victim@victimdomain.com' message is returned then the gateway is secured against proxying spam. If a 'Recipient OK' message is received then the gateway is probably incorrectly configured and can be used to route spam email.

Send

QUIT

to close the connection.

Should a 'Recipient OK' message be received, a complete message transfer should be used to fully test the finding. Should this occur the following commands will need to be executed:

telnet emailhost.domain.com.au 25

HELO hackerdomain.com

MAIL FROM:<spammer@bogusdomain.com.au>

RCPT TO:<valid-email-address@valid-domain.com>

DATA

Subject: this is a spam test from client gateway

This is a test message.

.

QUIT

Valid responses should be received at every step except after the DATA command. Note the blank line between the Subject and the message body ("This is a test message") and the full stop by itself on a line – that closes the DATA portion of the message. (http://support.microsoft.com/kb/q153119/[13] contains a more detailed overview of telneting on Port 25 to test SMTP Communication)

5 Audit

In this section the tests that were developed in the previous section are performed.

5.1 Audit: Backdoor Access Into The Parent Company

5.1.1 Port Scanning Results

Using Nmap each network was scanned for open ports (available services) using the following command:

```
# nmap -sT -P0 -O –p 1-65535 -oA TCPscan --append_output -sV -n -v 203.xxx.yyy.zz/28
```

The following results were obtained for the server in DMZ:

TCP SCAN

```
Interesting ports on 203.xxx.yyy.178:
(The 65522 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE          VERSION
21/tcp   open     ftp?
25/tcp   open     smtp
80/tcp   open     http             Microsoft IIS webserver 5.0
135/tcp  filtered msrpc
443/tcp  open     https?
445/tcp  open     microsoft-ds     Microsoft Windows 2000 microsoft-ds
626/tcp  open     microsoft-rdp    Microsoft Terminal Service (Windows 2000 Server)
1720/tcp filtered H.323/Q.931
2301/tcp open     http             Compaq Insight Manager 2.1
4444/tcp filtered krb524
4899/tcp open     radmin?
6103/tcp open     RETS-or-BackupExec?
9999/tcp open     abyss?

Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Professional RC1+ through final release
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=53844 (Worthy challenge)
IPID Sequence Generation: Busy server or unknown class
```

UDP SCAN

```
# nmap -sU -v -n -oA Genesis-UDP 203.xxx.yyy.178

(The 65528 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
53/udp   open  domain
135/udp  open  msrpc
161/udp  open  snmp
445/udp  open  microsoft-ds
500/udp  open  isakmp
3456/udp open  IISrpc-or-vat
3457/udp open  vat-control
```

5.1.2 Vulnerability Scanning Results

A Nessus Server was deployed on a RedHat 7.3 server attached to the Internet and the NessusWX[14,15] graphical Windows front end used to control the server. A snapshot of the NessusWX results screen is provided below.

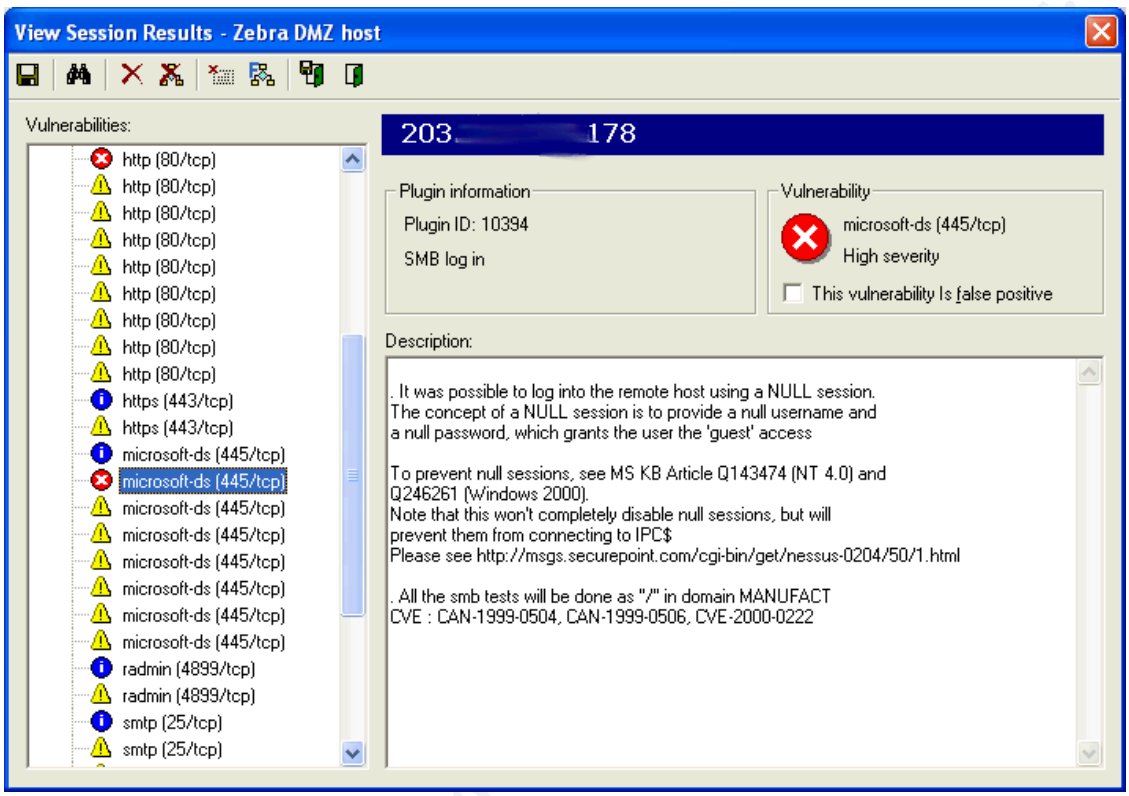


Figure 2 - NessusWX Results

For tempcntabsetaTPot9 9s rmhNasaicneenhtCpr99io pen. Basic research (http://www.google.com.au/search?q=tcp+9999) reveals that this port has been known to be associated with a Trojan horse however there is currently no Nessus plug-in to test this. The client was advised to ensure that the server had the latest virus definition files loaded to mitigate this risk.

TCP port 6103 is associated with the Veritas Tape Backup Executive which Nmap detected as being open to the Internet. Whilst there is a known vulnerability with certain versions of the Veritas backup software on TCP port 6101, the finding delivered to the client proposed that port 6103 might be found to be vulnerable in the future and that it should be blocked from Internet access.

The following table summarises the vulnerabilities detected by Nessus in the client's Internet Facing infrastructure. Proposed risk mitigation treatments are also presented.

Table 6: Vulnerability Scan Results

IP Address/Host	Port	Details
DMZ Host	FTP/21	The service closed the connection after 0 seconds without sending any data. It might be protected by some TCP wrapper.
	TCP/80	It appears that the web server running on this host has Microsoft FrontPage extensions enabled. Recommendation: If not used these should be disabled. If they are used it is important to ensure that patches are kept up to date.
	UDP/161	An SNMP Agent responded as expected with community name: public Important information can be obtained using SNMP such as valid users and LanMan share details. Recommendation: Restrict access to this port.
	TCP/445	It was possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access. CVE : CVE-2000-0222 The host's domain is MANU and its name is ZPROJET. A list of valid usernames was gleaned from this server: Administrator, Guest, TsInternetUser, IUSR_ZPROJET, IWAM_ZPROJET, BackupExecAdmin, WebAdmin Recommendation: Restrict access to this port.
	TCP/2301	The host is running Remote Compaq HTTP server version 2.1. There are known vulnerabilities with unpatched versions of this software. It is considered best practice to restrict access from the Internet to such services. Recommendation: Disable or restrict access to this service.
	TCP/4899	RAdmin is running on this host. RAdmin is used for remote access and permits full console access to the server using simple password access control. Make sure that a strong password is configured, otherwise a cracker may brute-force it and control your machine. Recommendation: disable this service if it is not used.
	ICMP	The remote host responds to ICMP Timestamp requests. Recommendation: Such requests should be filtered at the border router/firewall.

5.2 Audit: Security of Subsidiary's Internet Connection

Activity 1: Router Vulnerabililty

The first test was to run Nmap against the router's serial and (DMZ) ethernet addresses. Note that the actual IP addresses have been obfuscated to preserve the anonymity of the client.

The serial and ethernet ports were scanned and produced identical open port results. The serial port scan result is shown below:

```
# nmap -sT -P0 -O –p 1-65535 -oA ZebraRouter --append_output -sV -n –v 203.xxx.yyy.zz

(The 65525 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE     VERSION
23/tcp   filtered telnet
135/tcp  filtered msrpc
1720/tcp filtered H.323/Q.931
2033/tcp open     telnet      Cisco telnetd (IOS 12.X)
2034/tcp open     telnet      Cisco telnetd (IOS 12.X)
2035/tcp open     imsldoc?
2036/tcp open                 Cisco telnetd (IOS 12.X)
2037/tcp open                 Cisco telnetd (IOS 12.X)
2038/tcp open     telnet      Cisco telnetd (IOS 12.X)
4444/tcp filtered krb524

TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
IPID Sequence Generation: All zeros
```

This shows that anyone on the Internet can telnet to the router on ports 2033 through 2038, which is considered poor security because no one should need to access the device in this fashion. The router's configuration (see Annex B) indicates that 'aaa authentication' is enabled so the router should prompt for a Username when such a connection is established. This was tested:

```
# telnet 203.xxx.yyy.zz 2033
Trying 203.xxx.yyy.zz
Connected to 203.xxx.yyy.zz
Escape character is '^]'.

User Access Verification


Username: admin
Password:

% Authentication failed.
```

So whilst more than just a password is required to login to the router, our first test fails because an unsafe service is available from the Internet. A UDP scan revealed that there were no open ports on the router.

Activity 2: Router Hardening Analysis

The Cisco Router Review process compares forty-three configuration parameters against best practice. The Zebra router complies with twenty of the forty-three parameters. Below is a summary of the most important issues and the recommended changes. See Annex A for a tabular representation of the results below and see Annex B for a (modified) copy of the router's configuration.

Table 7 - Router Hardening Analysis

No.	Issue	Impact/Risk	Risk Factor	Recommended Change
1.	TCP ports 2033 – 2038 on this router all permitted interactive login to the router. These ports appear to be in the configuration to permit dialin access via interface Group-Async0	Anyone from the Internet can connect and attempt to login in to the router (A valid Username and password is required, however).	High	Modify ACL 160 (used on the S0/0.102 interface) to restrict access to TCP ports 2033-2038. A better option is to change the stance of the interface to default deny and change the use of telnet to SSH.
2.	Access List violations are not logged.	The client has no visibility as to whether this router is under attack.	Medium	Ensure that significant 'deny' statements in ACLS also use the key-word 'log' after them.
3.	Anti-spoofing filtering Access Control Lists are not employed.	Illegal traffic (e.g. RFC-1918 type packets) can enter the router and potentially compromise the client's hosts.	Medium	Improve the anti-spoofing filters in access-list 160 by filtering packets with source addresses as per RFC-2827.
4.	CDP is running	CDP advertises details about routers and switches. It should be disabled if not required as it may become an avenue for future attacks.	Low	Configure the router with: no cdp run
5.	IP source routing is permitted	Source routing can be used to define the route packets are to take. It is not required and should be disabled.	Low	Configure the router with: no ip source-route

6.	Dynamic Routing protocols are not authenticated	Authenticated routing updates give a higher level of assurance that their source is valid.	Very Low	This is more suited to a larger network where multiple organisations exchange routing updates. Recommendation: none.

The router's configuration was accordingly deemed to **fail** the review.

Activity 3: Rule Base Analysis

The router's configuration may be found in Annex B. A full business process flow analysis was unable to be performed due to limitations with access to the required data and so the rationale for the existence of each rule was unable to be determined. The following observations, however, were made following a manual review of the configuration:

- ACL 'DMZ_out' has numerous access elements defined following a 'permit ip any any' command. The 'permit ip any any' command will positively match all IP packets and, as such, no more access list elements are checked. The auditor recommends that this ACL be reviewed and revised as necessary. Recommendation: Review ACL and remove redundant configurations to improve readability.

- Access list 160 (used on the inbound Internet connection) is largely a 'permit any' stance. The auditor recommends that the ACL should explicitly permit access to valid services and implicitly deny all other access. It is noted that tcp/135 and tcp/4444 are explicitly blocked – these two ports are used by the Blaster worm. A default deny stance would have negated the need for the 'anti-Blaster' configuration.
  Recommendation: Rewrite this ACL using a 'default deny' stance.

- ACL 160 permits all ICMP packet types into the network. Best practice dictates that ICMP types be restricted to echo-request, echo-response and destination-unreachable. Other ICMP packet types can be used for network mapping and to compromise host computers.
- ACL 160 does not include sufficient anti-spoofing 'deny' statements as the first entries.
  Recommendation: Include anti-spoofing rules.

- Access elements in ACL 160 that deny packets with '10' addresses as the destination should be consolidated into a small number of elements. While packets with a '10' address as the destination should not, as per RFC-1918, be routed on the Internet, it is prudent to filter them anyway.
  Recommendation: Include anti-spoofing rules for RFC 1918 addresses as per RFC-2827.

- ACL 160 incorporates rules to prevent a known Cisco Denial of Service (DoS)

attack as described in CERT Advisories CA-2003-15 and CA-2003-17. Such rules are only required if a default permit stance is configured.

- The use of the public IP addresses 198.xxx.yyy.65/29 on the DMZ is not entirely clear. These addresses are not currently routable via the Internet as determined by a BGP query using the Optus looking glass (http://looking-glass.optus.net.au):

  BGP routing table entry for 198.xxx.yyy.0/19, version 574274612

  Paths: (3 available, best #3, table Default-IP-Routing-Table)

  Not advertised to any peer

  Recommendation: Remove this configuration unless there is a business reason to keep it.

- It appears that a number of access elements have been added to access lists DMZ_out and 160. The construction of these new elements is somewhat confusing as they explicitly define host source ports for, assumedly, established TCP connections to what appears to be a web proxy server at 198.xx.yy.66. If this is the case the configuration should be simplified by using the 'established' keyword. e.g. instead of

  permit tcp host 198.xx.yy.66 eq 8080 host 10.10.1.15 eq 4943

  use

  permit tcp host 198.xx.yy.66 eq 8080 host 10.10.1.15 established

- In access list 160, defining the source port for a DNS query may only work very occasionally:

  permit udp host 128.xx.yy.90 eq domain host 10.10.1.2 eq 1112

  Use the following instead:

  permit udp host 128.xx.yy.90 eq domain host 10.10.1.2

Overall, then, given the number of findings and their nature, it was decided to **fail** the router's access list rule base.

5.3 Audit: Email Spoofing

The test was conducted by connecting to the SMTP port on the Internet facing mail relay:

```
telnet emailhost.domain.com.au 25

220 zebraproj WebShield SMTP V4.5 MR1a Network Associates, Inc. Ready at Thu Oct 14 23:39:48

HELO hackerdomain.com
```

250 zebraproj Hello [152.xx.23.88]

MAIL FROM:<spammer@bogusdomain.com.au>

250 spammer@bogusdomain.com.au....Sender OK

RCPT TO:<victim@victimdomain.com>

550 Unable to relay for victim@victimdomain.com

QUIT

As can be seen, the mail server rejected our request to relay email to a domain that it was not responsible for. This section of the audit therefore receives a **pass**.

5.4 Management Summary of Key Findings

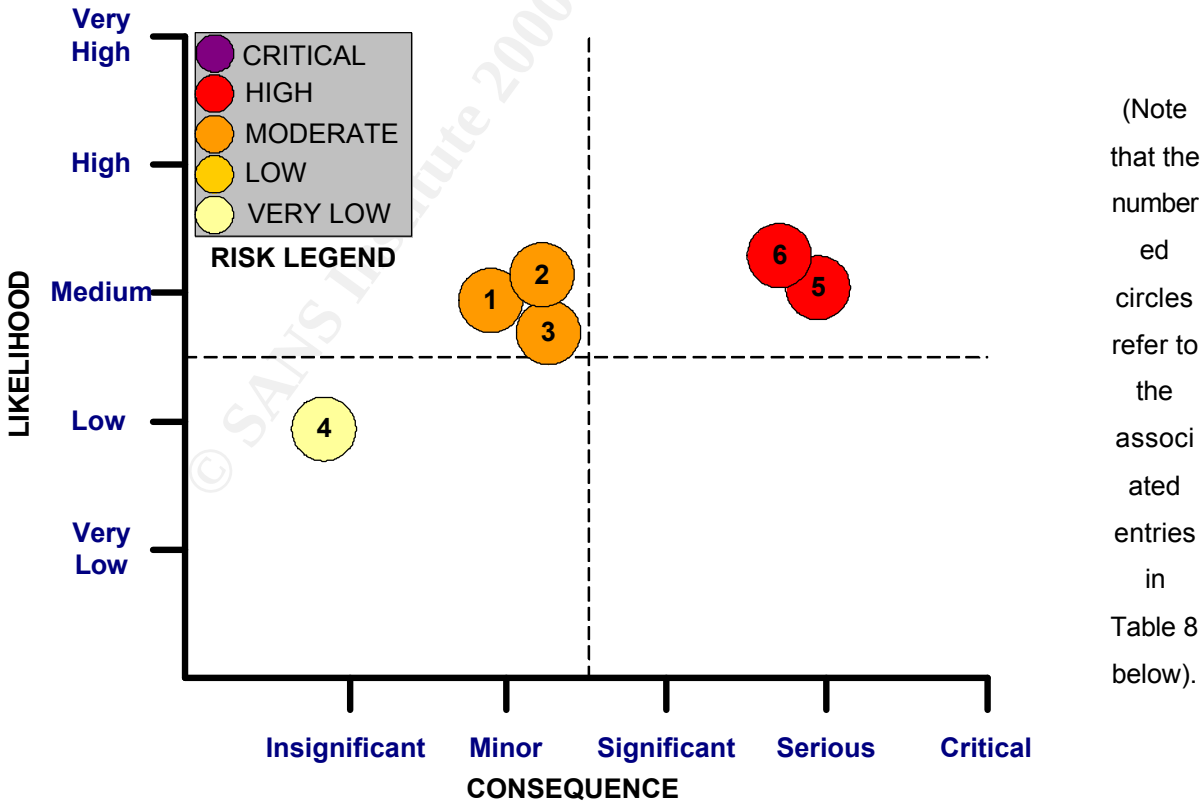
The auditor analysed the vulnerabilities identified in the client environment during the audit. At the completion of testing, the auditor had identified a total of six vulnerabilities with 2 rated as 'high' within the PROJECT ZEBRA Internet presence. A number of configuration deficiencies were identified with the PROJECT ZEBRA Router that require immediate attention.

The PROJECT ZEBRA DMZ host has a number of potentially vulnerable services available for access from the Internet. The auditor recommends that the risk of compromise of these services be mitigated through tighter security on the border router.

The risk profile in Figure 3 below graphs an assessment by the auditor of the likelihood of discovery and exploitation of each vulnerability against the potential consequence to the client. The auditor has analysed the results of the testing and conclude that the identified vulnerabilities do not pose a critical risk to the normal business operation of the client, however the auditor recommends the identified risks be addressed as soon as possible.

NOTE that it is the auditor's opinion that the Zebra DMZ should be protected with a suitable **firewall** instead of a router with ACLs as a firewall provides a much stronger security posture.

Figure 3: Risk Profile for Identified Vulnerabilities



(Note that the numbered circles refer to the associated entries in Table 8 below).

Table 8: Vulnerabilities Identified From Penetration Testing

No.	Affected Host	Technical Exposure	Estimated Threat Likelihood	Potential Consequence	Calculated Risk	Threat Mitigated By	Mitigated Risk Level
1	DMZ Host	It appears that the web server running on this host has Microsoft FrontPage extensions enabled. If not used these should be disabled. If they are used it is important to ensure that patches are kept up to date.	**Medium**	**Minor** FrontPage Extensions have been used in the past as avenues to attack Microsoft based web servers.	**Moderate**	Disable the extensions if not required or ensure patch levels are maintained if the extensions are required.	**Very Low**
2		SNMP is configured on the server with the default community string: public.	**High**	**Minor** SNMP can be used to obtain large amounts of information about a server that is useful for an attacker.	**Moderate**	Disable SNMP if is not used or use a stronger community string and filter SNMP access at the border router.	**Very Low**
3		It is possible to log into the remote host using a NULL session. The concept of a NULL session is to provide a null username and a null password, which grants the user the 'guest' access. CVE-2000-0222	**High**	**Minor** A list of valid usernames can be gleaned from this server which may be used to launch an attack. the auditor obtained the following user accounts: Administrator, Guest, TsInternetUser, IUSR_ZPROJET, IWAM_ZPROJET, BackupExecAdmin, WebAdmin	**Moderate**	Deny NetBIOS traffic to/from the Internet via the border router or firewall.	**Very Low**

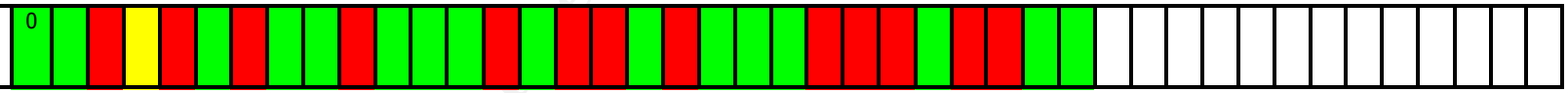
4		The host is running the Remote Compaq HTTP server.	**Low**	**Minor** This service may become an avenue for attack in the future.	**Low**	Disable the service or block access to it from the Internet at the border router.	**Very Low**
5		The host is running the RAdmin server	**Medium**	**Serious** An attacker can use brute-force password cracking in an attempt to gain complete control of the server.	**High**	Disable the service or 1) ensure a strong password is configured and (if possible) 2) define source IP addresses that can access the service (This is an RAdmin configuration parameter).	**Very Low**
6	Zebra Router	Telnet access to the border router from the Internet is possible.	**High**	**Significant** An attacker could login to the router and modify its configuration.	**High**	Change the default security stance on inbound connections to 'default deny'. Apply ACL to all VTY ports. Change the use of telnet to SSH if possible.	**Very Low**

Annex A. PROJECT ZEBRA Router Configuration Overview

The following table provides an overview of the output of the Router Audit Tool. This format is particularly powerful when a number of routers are compared across an enterprise as inconsistencies in configurations are easily highlighted. The template is an Excel spreadsheet which uses conditional formatting to automatically colour code each cell. CSV data files can be imported into the template to quickly populate the table. A PERL script could be written to convert the output of the RAT into the CSV file, however the process was performed by hand for this assignment.

Table 9 - Router Configuration Analysis

Router	IOS Version	No. of published Sev. 1 Cisco bugs for this IOS version	Warning Banner configured	AntiSpoofing ACL used	Dynamic routing protocol routing updates authenticate	no ip bootp server	no ip http server	no cdp run	no service config	service password encryption	tcp keepalive service	no tcp-small-servers	no udp-small-servers	no IP finger	forbid SNMP read-write	forbid SNMP without ACLs	no ip source-route	no directed broadcast	exec-timeout	disable aux	login default	no enable password	enable secret	apply VTY ACL	service timestamps logging	service timestamps debug	enable logging	set syslog server	logging console critical	logging trap info or higher	ntp server OR master	ntp server 2	VTY transport SSH	apply VTY SSH ACL	Create Emergency Local User Account	aaa new-model	aaa authentication login	aaa authentication enable	aaa accounting exec	aaa accounting commands	aaa accounting network	aaa accounting connection	aaa accounting system	no tftp server

IZKrtr01	12.1(5)T15	0 

Legend:	
	Meets best practice
	Does not meet best practice
	Not Applicable

Annex B. (Edited) PROJECT ZEBRA Router Configuration.

```
version 12.1
no service single-slot-reload-enable
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname IZKrtr01
!
logging buffered 10000 debugging
logging rate-limit console 10 except errors
aaa new-model
aaa authentication login vtymethod group tacacs+ enable
aaa authentication ppp raccess local group radius
enable secret 5 <removed>
!
username <removed> password 7 <removed>
username all
clock timezone AEST 10
clock summer-time AEDT recurring last Sun Oct 2:00 last Sun Mar 2:00
modem country mica australia
ip subnet-zero
!
!
no ip finger
ip tftp source-interface Loopback10
no ip domain-lookup
ip host sec_dns_server 203.2.75.12
ip host dns_server 203.2.75.2
!
ip inspect name isp cuseeme
ip inspect name isp ftp
ip inspect name isp realaudio
ip inspect name isp smtp
ip inspect name isp h323
ip inspect name isp tftp
ip inspect name isp vdolive
ip inspect name isp tcp
ip inspect name isp udp
ip inspect name isp sqlnet
ip audit notify log
ip audit po max-events 100
isdn switch-type primary-net5
!
!
controller E1 2/0
 pri-group timeslots 1-10,16
!
!
interface Loopback10
 ip address 10.10.10.254 255.255.255.0
!
interface FastEthernet0/0
 description LAN interface for internal network, VLAN 1 & 2
 ip address 10.10.1.254 255.255.255.0
```

```
 ip access-group internal_out in
 ip directed-broadcast 161
 ip nat inside
 ip inspect isp in
 speed auto
 full-duplex
!
interface Serial0/0
 no ip address
 encapsulation frame-relay IETF
 logging event subif-link-status
 logging event dlci-status-change
 no fair-queue
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
!
interface Serial0/0.100 point-to-point
 description connected to corporate network
 bandwidth 384
 ip address 192.168.245.26 255.255.255.252
 frame-relay class 384-768
 frame-relay interface-dlci 100
!
interface Serial0/0.102 point-to-point
 description Connection to the Internet
 bandwidth 256
 ip address 203.xxx.yyy.zz 255.255.255.252
 ip access-group 160 in
 frame-relay class 256-256
 frame-relay interface-dlci 200
!
interface FastEthernet0/1
 description LAN interface for DMZ
 ip address <203 address> 255.255.255.248 secondary
 ip address <198 address> 255.255.255.248
 ip access-group DMZ_out in
 ip accounting output-packets
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
 clockrate 2000000
!
interface Serial2/0:15
 no ip address
 encapsulation ppp
 dialer pool-member 1
 isdn switch-type primary-net5
 isdn incoming-voice modem
 fair-queue 64 256 0
 ppp authentication chap
!
interface Group-Async0
 ip unnumbered FastEthernet0/0
 ip access-group internal_out in
```

```
 ip nat inside
 ip inspect isp in
 encapsulation ppp
 ip tcp header-compression passive
 async mode dedicated
 peer default ip address pool default
 ppp authentication pap raccess
 group-range 33 38
!
interface Dialer0
 description ISDN link to Internet
 ip address <ip address> 255.255.255.0
 ip access-group Internet_in in
 ip nat outside
 encapsulation ppp
 shutdown
 dialer pool 1
 dialer idle-timeout 2000000
 dialer string 022345678
 dialer max-call 1
 dialer-group 1
 no cdp enable
 ppp authentication chap callin
 ppp pap sent-username ZEBRAprojec password 7 <removed>
!
interface Dialer10
 description ISDN Link to Netbridge Support
 bandwidth 64
 ip address 10.10.254.253 255.255.255.252
 ip nat inside
 encapsulation ppp
 dialer pool 1
 dialer remote-name <remote router>
 dialer idle-timeout 180
 dialer-group 2
 peer default ip address 10.10.254.254
 ppp authentication chap
!
router eigrp 100
 network 10.0.0.0
 network 192.168.245.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip local pool default 10.10.10.1 10.10.10.253
ip nat pool client-VPN <ip address pool> netmask 255.255.255.248
ip nat inside source route-map client-VPN pool client-VPN
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0.102
ip route 0.0.0.0 0.0.0.0 Dialer0 20
ip tacacs source-interface Loopback10
no ip http server
!
!
ip access-list extended DMZ_out
 remark In production this acl is applied inbound on the DMZ interface
 remark to control traffic out from the DMZ network
 remark
```

```
 remark Allow Mail traffic back to internal network
 permit tcp host <internal IP address> 10.10.1.0 0.0.0.255 eq smtp
 remark
 remark Allow web requests back to internal network
 permit tcp host <internal IP address> 10.10.1.0 0.0.0.255 eq www
 remark
 remark Allow SQLNet (tcp/1521) to internal network
 permit tcp host <internal IP address> 10.10.1.0 0.0.0.255 eq 1521
 remark
 remark Allow client  (tcp/6009) to internal network
 permit tcp host <internal IP address> 10.10.1.0 0.0.0.255 eq 6009
 permit ip host <internal IP address> host 10.10.1.5
 remark
 remark Allow icmp for troubleshooting
 permit icmp any any
 remark
 remark Deny anything else to internal network
 deny   ip any 10.10.1.0 0.0.0.255
 remark
 remark permit anything to Internet
 permit ip any any
remark
 remark Allow Mail traffic back to internal network2
 permit tcp host <internal IP address2> 10.10.1.0 0.0.0.255 eq smtp
 remark
 remark Allow web requests back to internal network2
 permit tcp host <internal IP address2> 10.10.1.0 0.0.0.255 eq www
 remark
 remark Allow SQLNet (tcp/1521) to internal network2
 permit tcp host <internal IP address3> 10.10.1.0 0.0.0.255 eq 1521
 remark
 permit tcp host <internal IP address3> 10.10.1.0 0.0.0.255 eq 6009
 permit ip host <internal IP address3>  host 10.10.1.5
 remark In production this acl is applied inbound on the DMZ interface
 remark to control traffic out from the DMZ network

ip access-list extended Internet_in
 deny   ip 134.xx.yyy.64 0.0.0.7 any
 deny   ip host 198.xxx.yyy.107 any
 permit tcp any host 134.xxx.yyy.66 eq www
 permit tcp any host 134.xxx.yyy.66 eq 443
 permit udp host 129.xx.yy.3 eq ntp any eq ntp
 permit udp any host 203.2.75.2 eq domain
 permit tcp any host 134.xxx.yyy.66 eq smtp
 permit tcp host 203.2.75.12 host 203.2.75.2 eq domain
 permit tcp any host 81.xx.yy.178 eq smtp
 permit tcp any host 81.xx.yy.178 eq www
 permit tcp any host 81.xx.yy.178 eq 443
 permit icmp any any
 deny   ip any any

ip access-list extended client-VPN
 remark Defines VPN traffic to client
remark Allow udp/500 traffic for Cisco IPSec NAT Encapsulation
 permit udp any host 199.xx.yy.59 eq isakmp
 permit udp any host 199.xx.yy.60 eq isakmp
 remark
 remark Allow PPTP connections using tcp/1723 and GRE
```

```
 permit tcp any host 199.xx.yy.59 eq 1723
 permit tcp any host 199.xx.yy.60 eq 1723
 permit gre any host 199.xx.yy.59
 permit gre any host 199.xx.yy.60

ip access-list extended internal_out
 remark In production this acl is applied outbound on the internal Ethernet interfaces
 remark to control traffic out from the internal network
 permit ip any any
!
logging 10.10.1.10
access-list 2 permit 10.10.1.0 0.0.0.255
access-list 10 permit 129.xx.yy.20
access-list 10 permit 129.xx.yy.30
access-list 10 permit 129.xx.yy.41
access-list 10 permit 129.xx.yy.141
access-list 80 permit any
access-list 90 permit 10.10.1.86
access-list 99 permit 10.10.254.254
access-list 99 permit 10.100.1.1
access-list 99 permit 10.10.1.0 0.0.0.255
access-list 99 permit 10.10.8.0 0.0.0.255
access-list 99 permit 10.10.10.0 0.0.0.255
access-list 151 remark Debug SQL Traffic
access-list 151 permit tcp host 134.xxx.yyy.66 host 10.10.1.5 eq 1521
access-list 151 permit tcp host 10.10.1.5 eq 1521 host 134.xxx.yyy.66
access-list 151 permit tcp host 134.xx.yy.66 host 10.10.1.5 eq 6009
access-list 151 permit tcp host 10.10.1.5 eq 6009 host 134.xxx.yyy.66
access-list 152 deny   tcp host 134.xxx.yyy.66 host 10.10.1.5 eq 1521
access-list 152 deny   tcp host 10.10.1.5 eq 1521 host 134.65.39.66
access-list 152 permit ip host 134.xxx.yyy.66 host 10.10.1.5
access-list 152 permit ip host 10.10.1.5 host 134.65.39.66
access-list 160 deny   53 any any
access-list 160 deny   55 any any
access-list 160 deny   77 any any
access-list 160 deny   pim any any
access-list 160 deny   udp any host 10.10.10.254 eq snmp
access-list 160 deny   udp any host 10.10.1.254 eq snmp
access-list 160 deny   udp any host 192.168.245.26 eq snmp
access-list 160 deny   udp any host 203.xxx.yyy.82 eq snmp
access-list 160 deny   udp any host 81.xxx.yyy.177 eq snmp
access-list 160 deny   udp any host 134.xxx.yyy.65 eq snmp
access-list 160 deny   tcp any host 10.10.10.254 eq telnet
access-list 160 deny   tcp any host 10.10.1.254 eq telnet
access-list 160 deny   tcp any host 192.168.245.26 eq telnet
access-list 160 deny   tcp any host 203.xxx.yyy.82 eq telnet
access-list 160 deny   tcp any host 81.xxx.yyy.177 eq telnet
access-list 160 deny   tcp any host 134.xxx.yyy.65 eq telnet
access-list 160 deny   tcp any any eq 135
access-list 160 deny   tcp any any eq 4444
access-list 160 permit ip host 255.255.255.255 any log
access-list 160 permit ip any host 255.255.255.255 log
access-list 160 permit ip any any
access-list 161 permit udp any any eq snmp
access-list 198 permit tcp any eq telnet any established
access-list 198 permit udp any any eq tftp
priority-list 5 protocol ip high tcp 1494
priority-list 5 protocol ip high udp 1604
```

```
priority-list 5 protocol ip high tcp telnet
priority-list 5 protocol ip high tcp 12680
priority-list 5 protocol ip medium tcp www
priority-list 5 protocol ip medium udp netbios-ns
priority-list 5 protocol ip medium udp netbios-dgm
priority-list 5 protocol ip medium tcp 135
priority-list 5 protocol ip medium tcp 137
priority-list 5 protocol ip low tcp 102
priority-list 5 protocol ip low tcp 139
priority-list 5 protocol ip low tcp uucp
priority-list 5 protocol ip low tcp cmd
priority-list 5 default low
dialer-list 1 protocol ip list 199
dialer-list 2 protocol ip list 198
route-map client-VPN permit 10
 match ip address client-VPN
!
tacacs-server host 129.xx.yy.20
tacacs-server key <removed>
snmp-server community <removed> RO 10
snmp-server community <removed> RW 10
snmp-server community <removed> RO 2
snmp-server trap-source Loopback10
snmp-server location ZEBRA
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps bgp
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server host 129.xx.yy.20 <removed>
radius-server host 10.10.1.1 auth-port 1645 acct-port 1646 key 7 <removed>
radius-server retransmit 3
banner login ^C
Access to this device is restricted to authorised users only.
Violators will be prosecuted to the fullest extent of the law.
^C
!
line con 0
 exec-timeout 30 0
 password 7 <removed>
 transport input none
 speed 115200
line 33 38
 modem Dialin
 transport input all
 flowcontrol hardware
line aux 0
 exec-timeout 15 0
 password 7 <removed>
```

```
line vty 0 4
 session-timeout 15
 exec-timeout 15 0
 password 7 <removed>
 login authentication vtymethod
!
ntp clock-period 17180080
ntp master 5
ntp server 10.100.1.1 prefer
end
```

List of References

The following documents or URLs are referenced in this paper:

[1] Standards Australia. HB 142–1999: A basic introduction to managing risk using the Australian and New Zealand Risk Management Standard AS/NZS 4360:1999

[2] David Hoelzer, SANS Track 7 Auditing Networks, Perimeters & Systems, 7.1 – Auditing Principles & Concepts, Class documentation Version 032304, (page 1-22), SANS Washington D.C. July 26 – 31, 2004. (referenced by Martinez, Yolanda in his paper "Auditing a Systems Security Consultant's Laptop Running Fedora Core 2", Dec 20, 2004. <http://www.giac.org/certified_professionals/practicals/gsna/0185.php>

[3] Standards Australia. AS/NZS 4360:2004 Risk Management. (modified version of figure 3.1)

[4] Standards Australia. AS/NZS 4360:2004 Risk Management

[5] International Standards Organisation. ISO/IEC 17799

[6] Insecure.Org - Nmap Free Security Scanner, Tools & Hacking resources <http://www.insecure.org/>

[7] Remote-exploit.org – Self contained auditing tool kit. <http://remote-exploit.org/>

[8] Nessus Open Source Vulnerability Scanner <http://www.nessus.org/>

[9] Anderson, Harry. Introduction to Nessus, October 28, 2003. <http://www.securityfocus.com/infocus/1741>

[10] Anderson, Harry. Nessus, Part 2: Scanning, December 16, 2003. <http://www.securityfocus.com/infocus/1753>

[11] Center for Internet Security Level-1 / Level-2 Benchmarks and Audit Tool for Cisco IOS Routers and PIX firewalls. <http://www.cisecurity.org/bench_cisco.html>

[12] Beck, Robert. Using RAT (Router Audit Tool) from CIS (Center for Internet Security) to Perform a Security Audit of the Configuration File of a Cisco Router at the Level-1 Benchmark. <http://www.giac.org/certified_professionals/practicals/gsna/0189.php>

[13] Microsoft Corporation. XFOR: Telnet to Port 25 to Test SMTP Communication <http://support.microsoft.com/kb/q153119/>

[14] Nessus Client for Win32 <http://nessuswx.nessus.org/>

[15] Stoll, Cecil. Nessus Primer with the NessusWX Client. June 26, 2004. <www.sans.org/rr/whitepapers/tools/1464.php>