Global Information Assurance Certification Paper

Auditing An Intranet Firewall From an ISO 17799 Perspective

GSNA Practical Version 3.1 Option 1

Richard Seiersen
04.29.2004

Abstract:
Security audits that focuses on technical means of securing an organization will likely ignore exposures caused by human means. Human error cannot be overlooked, and in fact may have more of an impact on security than employing the latest and greatest technology. In 2003 84% of security issues were caused by human error. (SysAdmin Magazine May 2004 • Volume 13 • Number 5). Is the trend of exposures created by human error more a function of better technical responses to security issues that only leave human error as the most likely path exposure? Or is this a trend associated with an excessive focus on technical means of securing the organization that leaves human concerns assessed as boring and or non-essential? Either way, as auditors, we need frameworks that will take both human and technical concerns into balanced consideration. We need a method of auditing that might force us to push beyond our own proclivities of technical obsession and push us to take a balanced look at security. This audit aims to do just that, by employing the ISO 17799 framework to an audit of an intranet firewall.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Table Of Contents

AUDITING AN INTRANET FIREWALL FROM AN ISO 17799 PERSPECTIVE 1

ASSIGNMENT 1: AUDIT, MEASUREMENT PRACTICE, AND CONTROL 4

A MENTION ON AUDIT FRAMEWORK 6

BENEFITS OF THE 17799 APPROACH TO THE ORGANIZATION 7

GENERAL INTERNAL NETWORK MAP 8

EVALUATE THE MOST SIGNIFICANT RISKS TO THE SYSTEM. 9

ENUMERATE AND DESCRIBE THREATS AND THEIR CAPACITY TO INFLICT DAMAGE... 9

PERSONNEL SECURITY 10
Section 6.2 :: User Training 10
Section 6.3:: Responding to security incidents and malfunctions 11
PHYSICAL AND ENVIRONMENTAL SECURITY 11
Section 7.2 :: Equipment Security 11
8. COMMUNICATIONS AND OPERATIONS MANAGEMENT 12
Section 8.3 :: Protection against malicious software 12
Section 8.4.1 :: Information Backup 12
Section 8.4.2 :: Operator Logs 13
INFORMATION ASSETS 13

THE CURRENT STATE OF PRACTICE 15

AUDIT CHECKLIST 16

1 SECURITY POLICY 16
2 PERSONNEL SECURITY 17
3 PHYSICAL AND ENVIRONMENTAL SECURITY 18
4 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 19
5 ACCESS CONTROL 20
6 BUSINESS CONTINUITY MANAGEMENT 21
7 SYSTEMS DEVELOPMENT AND MAINTENANCE ::CRYPTOGRAPHIC CONTROLS 22
8 COMPLIANCE 22

AUDIT CHECKLIST COMPLETED 24

1 SECURITY POLICY 24
2 PERSONNEL SECURITY 24
3 PHYSICAL AND ENVIRONMENTAL SECURITY 25
4 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 26
5 ACCESS CONTROL 27
6 BUSINESS CONTINUITY MANAGEMENT 31
7 SYSTEMS DEVELOPMENT AND MAINTENANCE ::CRYPTOGRAPHIC CONTROLS 32
8 COMPLIANCE 33

AUDIT EXECUTIVE SUMMARY: 37

MAJOR AUDIT FINDINGS DETAILS: 38

1. LACK OF EXECUTIVE MANAGEMENT APPROVED SECURITY POLICY 38
2. LACK OF TRAINING AND PROCEDURES FOR SUPPORT THE FLOPPY FIREWALL 38
3. UNENCRYPTED SERVICES USED FOR FIREWALL MAINTENANCE 39

AUDIT RECOMMENDATIONS: 39

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

POLICY 39
HUMAN RESOURCES 40
ENCRYPTION 41
ADDENDUM 42
GES ISO 17799 AUDITOR PORTAL 42

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Assignment 1: Audit, Measurement Practice, and Control

Preamble:
Note: Names and faces have been changed to protect the innocent; nonetheless, the facts herein are based entirely on a true story.

> *So how do you approach a firewall audit? The same way you approach the original design. First, review the security policy, and confirm that it's a good match for the organization's needs. Then review the design of the firewall system, confirming that it's a suitable choice for enforcing the security policy. Next review the configuration of the firewall, confirming that it's set up appropriately. Finally devise suitable spot-tests to confirm that the firewall is behaving as documented*. (10).

I will be auditing an intranet firewall, and related security practices, that safeguard the lifeblood of a high profile, multi national security consulting organization by the name of GIAC Enterprise Security (GES)*. This firewall not only helps to protect GES's intellectual property from prying eyes, it also protects all of the corporate subnets from each other's malicious activity. The major source of this malicious activity is the software development side of GES's intranet, which can be a quasi war zone of scanning, exploits, and general network commotion. This commotion makes GES's intranet a potentially cantankerous environment for those corporate white-collar workers seeking to work in peace. Therefore, this firewall is in place to make doubly sure that those portions of the network dedicated to high traffic of a dubious kind remain unto themselves, thereby not interfering with the 'business-side' of the house. Likewise, being that GES is a place that employs persons within the security space it was critical to make sure that GES's intellectual property was properly safeguarded.

Knowing that GES is one of the most sophisticated security firms on the globe, one would expect GES to have a top of the line firewall appliance to protect its intellectual property. One would expect this firewall to have all the bells and whistles money can buy. At the very least, one would expect the firewall to be stateful with in-depth packet inspection, after all it is the last border device used to protect the corporate file server, CRM system, CVS system, mail servers, and roughly thirty other key servers – not to mention all of the corporate desktop and workstations. (This is apart from host-based firewalls on key servers). But, alas, an auditor would be sorely disappointed if they were expecting something so glamorous as a hermetically sealed, costly, firewall appliance. What the auditor would actually see in terms of a firewall is a floppy drive and not much more, definitely no hard-drive. To the auditor's chagrin, they would discover that a crucial hub of defense for the GES corporate intranet is a simple floppy firewall.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

> "It boots a Linux kernel and comes with a minimal set of tools to get the job done. If you think about it, that's actually a feature. If a bad guy were to get into your firewall machine somehow, there won't be much for him to use against you. And since we're running completely on a RAM disk, a simple reboot from the floppy will restore the system to its original state." (*Andreas Meyer, Build a Floppy Firewall, Sys Admin January 2001*).

The little stripped down firewall boasts a Redhat 2.4 version kernel with hardware consisting of a Intel Celeron 466 with a 66 Mhz front side bus and with 256 Mb RAM. The firewall software is from http://www.zelow.no/floppyfw/ , version 2.0.4. The rule base is on the extreme side of generous, with roughly 17 pages of fine print dedicated to routing and security functions largely based on host identity and port/protocol. Also, while the particular version of floppy firewall software is stateful, this functionality has been turned off for this floppy firewall. This is due to the fact that at any given moment there is any number of scans impacting two of the three interfaces of the firewall. If state were used, the firewall would fall over in a matter of minutes due to the state tables overflowing. Not to worry though, all of the cutting edge appliances that are stateful and such are farther out toward the perimeter. In fact, the floppy firewall really sits within layers of security (a true example of defense in depth), and there really is slim advantage to a compromise of the server. This is largely due to the fact that there are scant services running on the floppy firewall due to lack of memory resources. Remember, the firewall runs completely in RAM. In fact, as stated in the above quote, any compromise is can be quickly thwarted by either a reboot, and or a wholesale swapping out of the server with one of its many cheap replacements.

This brings us the point of asking, 'why audit this firewall, sounds boring?'. While that assessment may or may not be true, the customer in question feels that they need beefing up in the broader areas of corporate security, particularly the procedural side of security. The customer's desire for a contextual audit of their floppy firewall begs for a style of audit that emphasizes human context as well as technical concerns. While this audit will not ignore the specific technical aspects of possible exploit to the firewall itself, it will largely look to help the IT department beef up security practices that revolve around the floppy firewall and can be applied broadly as a template throughout the organization.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

A Mention On Audit Framework
The ISO 17799 standard has been selected as a framework for this audit. The two main resource informing this audits view, particularly the audit checklist, is the 17799 Checklist found here:

http://www.sans.org/score/checklists/ISO_17799_checklist.pdf

Also, the ISO/IEC Information technology 17799:2000(E) Standard — Code of practice for information security management was heavily referenced.

The reason this particular framework has been selected is due to the auditor's background in ISO. The auditor's background includes roles as a an ISO 9000 coordinator and internal auditor for an ASP (application service provider), which plays a part in GES's service offering, as well as a contributing role to the OWASP (www.owasp.org) application of 17799 to web application security.

ISO Preamble
A preamble as to the nature of ISO is in order, as confusion abounds as to its true purpose. Having the nature of ISO clarified will also help to better explain the particular application of ISO to this audit. Its also hoped that this preamble will be of value to other SANS participants seeking to employ ISO and like standards in meaningful ways.

A basic tenant of ISO can be stated thusly, "*ISO is not particularly concerned with the 'how' of a particular activity, but more so the 'what' of that activity*". This can be better understood if we look closer at the term ISO itself. To the surprise of most people ISO does not stand for the 'International Standards Organization'. The organization actually is the 'International Organization of Standards' (IOS). ISO is a Greek term that can be loosely translated to mean same or equal. We see the term ISO showing up in the English language in such words as isosceles triangle, and or isometric.

All of the ISO standards share the same purpose at heart, to make practices same or equal across corporate, business, and international boundaries. It is this very emphasis on the equality of process that has made ISO such an excellent international standard. It allows a company to feel some semblance of assurance that if they enter into business with another ISO organization, perhaps a vendor, that the vendor will have certain processes that the purchaser can count on. Of course the existence of a particular practice is no guarantee that the practice is a 'good one'. The qualitative value of the practice really depends on how the organization interprets the standard.

Basically, this means that if ten companies states that they adhere to an ISO 17799 framework in terms of how they audit and maintain their perimeter security, you should expect to see similarities in the security policies and implementations of each of the ten organizations. It does not mean, for example, that all the organizations will necessarily have firewalls that implement iptables, or other standard firewall practices, but that their methodology for assessing what

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

types of perimeter defenses are needed, and how those defenses are maintained will look very similar.

In terms of a specific example of ISO as applied to security, it would be reasonable to expect that a company that adheres to the 17799 standard will have some form of policy on the use of cryptographic controls for protection of information (10.3.1). Whether those controls are 'good', which is a qualitative term, does not necessarily apply. Meaning, that one organization may interpret 10.3.1 as allowing you to connect to web servers with weak encryption – i.e. using

#openssl s_client -cipher LOW –connect <host>:<port>

while other organizations may specify only 128+ bit encryption (MED in terms of openSSL) is required across the board. The issue in terms of ISO boils down to whether or not you have procedures that are implemented in terms of 10.3.1, and that there is proof of your adherence to 10.3.1 as you have reasonably interpreted it. Meaning, an organization that goes through an audit in terms of ISO 17799 will have a finding if they do not have procedures, as well as proof of compliance, in relation to 10.3.1. An organization that states that all externally facing web severs only allow 128+ bit encryption for connection, yet you can connect with the command above, would have a finding as well. Conversely, if the organization has made a case for 10.3.1 not applying because the information accessible via their external web servers does not need to be encrypted, and they have stated this in their policy, will not have a finding when we connect with the command above. The hope of course would be that strong ciphers would be used where information needs to be protected from prying eyes.

What is important to consider is that if you are thinking of doing business with a company that adheres to ISO 17799, you could review their policy on cryptographic controls, and see proof that the practice is being carried out. You would then have to assess for yourself if you thought the level of implementation met your needs. For example, the policy may indicate that DES is adequate for all third party electronic communications. You, as that third party, may have your own policy that states that 3DES is adequate. ISO 17799 won't disagree, it only cares that the assessment occurred and that you are implementing based on the results of the assessment as you have interpreted and documented them. The issue of who has 'good' security in the particulars is left to other forms of assessment.

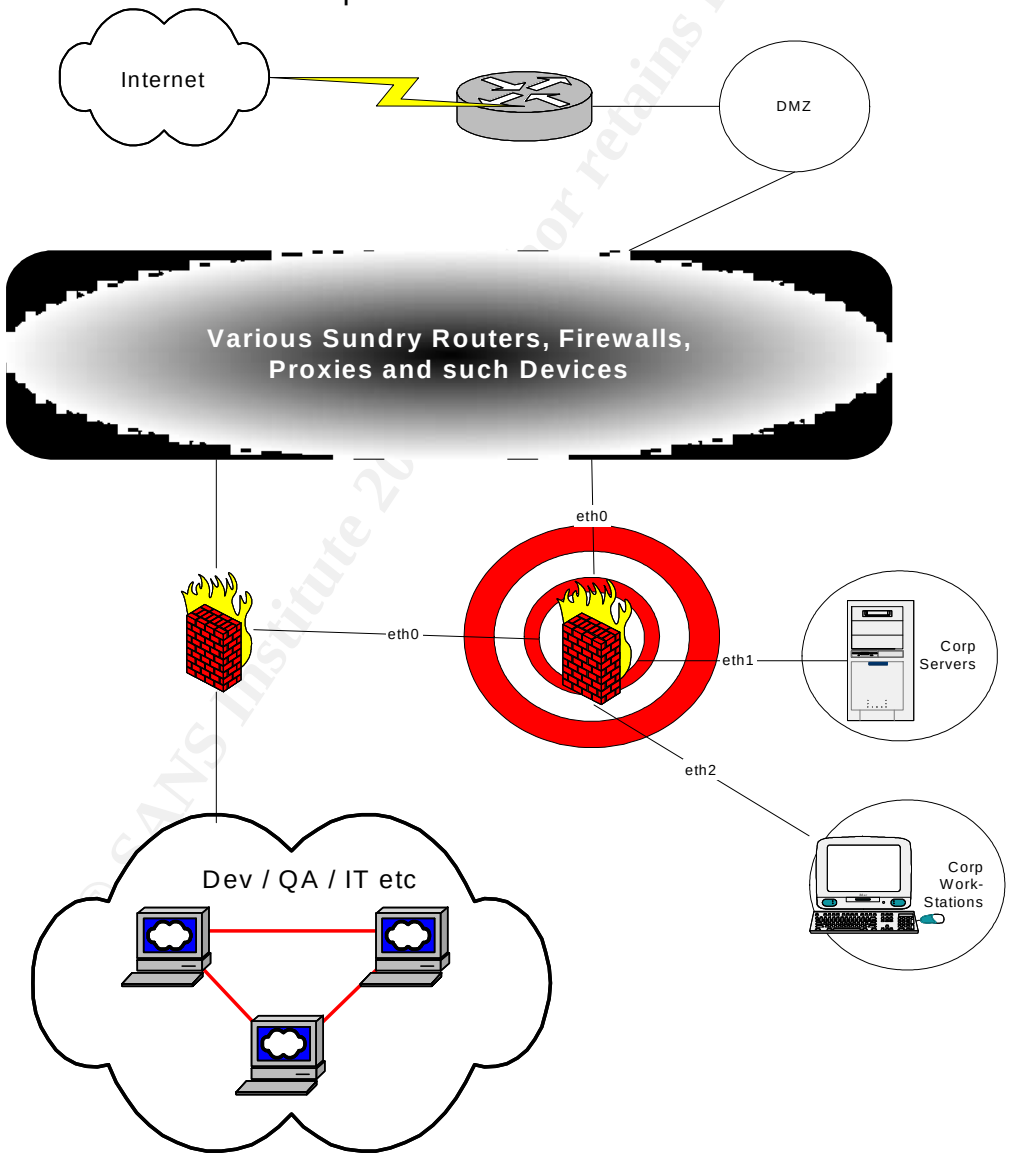
Benefits of the 17799 approach to the Organization

The specific benefit that an ISO 17799 framework will bring to this audit for this particular customer is that the '*methodology*' of audit can be applied to all their firewall systems as well as other corporate lines of defense. Methodology is emphasized because the particulars of each specific context will warrant different aspects of the ISO standard. Furthermore, with increased business in Europe and Asia, the practice of ISO 17799 could play a part in the increase of sales.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Note that of 100,000+ ISO registered organizations in the US (9000 standard), over 99% were contract based. This meant that US sales hinged on securing ISO registration before contracts were signed. Most of the organizations requiring the US firms to be ISO registered where European and Asian firms. (Statistic gathered from work done with Gregory Brower, ISO consultant and former VP Quality General Motors). The emphasis in all of these cases was on business process, particularly as it applied to manufacturing. Largely, these Asian and European firms were saying that they would only do business with organizations that wrapped ISO around their business processes. Being that data is increasingly the 'stuff' of business process as opposed to nuts, bolts, and various manufactured paraphernalia, would it not be reasonable to speculate that ISO 17799 would supercede ISO 9000 as the international standard dejour?

General Internal Network Map



*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

EVALUATE THE MOST SIGNIFICANT RISKS TO THE SYSTEM.

This section requires some definitions in order to be of impact. Definitions are chosen from the SANS glossary of security terms http://www.sans.org/resources/glossary.php

Risk: Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

Exposure: A threat action whereby sensitive data is directly released to an unauthorized entity.

Vulnerability: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Risk assessment: is defined in the SANS Institutes, track 7 book, Auditing Principles and Concepts as follows, "A risk assessment is an analysis of potential vulnerabilities and threats taken together to produce an overall picture of the potential for loss or harm to the organization." The ISO/IEC 17799-2000 Standard Document defines risk as, "Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence. "

Enumerate and describe threats and their capacity to inflict damage.
The assessment of threats will be viewed through the lens of ISO 17799, as applicable. This means that the various standard section the fit into a definition of threat for the audit of the floppy firewall will be used. It will be important to keep the scope of the audit tight, as firewall audits can quickly creep into network audits, which is out of scope for this process.

Threats:
Threats, as defined above, are distinct from vulnerabilities in that they are not system design flaws and or weaknesses, but a possibility of breach of security based on what can be called environmental factors. For example, in GES's environment, there is a fairly constant flow of scanning occurring at any given hour of the day. In the case of our floppy firewall, two of the interfaces are subject to this constant scanning. In this case, scanning could be classified as a threat. But, the nature of this threat is not so much in terms of the scanning for the purpose of reconnaissance, but in terms of scanning as a DOS attack on the floppy firewall. If the floppy firewall were running in a stateful mode, then it would be readily vulnerable to denial of service attacks caused by session overload.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

The occurrence of this phenomena would be daily if not hourly if it were not for the fact that this vulnerability has been resolved by the floppy firewall by turning off stateful functionality. The threat in this case actually shifts from a technical one, to more of a procedural one. Specifically, if an systems administrator was not trained in how to maintain the floppy firewall, he or she may inadvertently run the firewall in stateful mode. This type of threat, one or process, procedure, and training falls directly in line with what is considered a threat as well.

PERSONNEL SECURITY		
According to the results of the CompTIA survey, released on March 31st,2004 84 percent of the nearly 900 organizations surveyed "blamed human error either wholly or in part for their last major security breach" (www.SysAdminMag.com Vol 13, 5/1/04) Section 6 of the 17799 standard covers the area of 'Personnel Security'. The subsets of personnel security that are of particular concern for this audit revolve around training and related procedures. The reason this is a concern is two fold. First of all, the IT staff consists of two people. The system also is cobbled from the ground up. This includes hardware, OS modifications – specifically the kernel, and open source firewall software. There is no slick firewall GUI that makes the maintenance of the firewall simple and straightforward.		
ISO 17799 **Section 6.2 :: User Training**		
Objective: '*To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work*.'		
Risk	**Impact**	**Likelihood**
• Responsible staff does not have the requisite training in terms of policy as well as the technical skills to adequately configure the firewall.	• Critical infrastructure that management deems necessary to protect could be exposed to threats that the firewall was intended to filter out, according to policy.	Med
• Staff is not adequately trained in terms of OS hardening, particularly UNIX based OS hardening.	• The OS could be weakly hardened, for example it could be running services that create exposures, and or the kernel could be configured in a way that could further compromise systems that the firewall was suppose to be protecting.	Med

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

ISO 17799 **Section 6.3:: Responding to security incidents and malfunctions**		
Objective: '*To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents*.'		
Risk	**Impact**	**Likelihood**
• In the event of a compromise of the firewall itself and or a breakdown, procedures do not exist for brining the firewall back up to functional status.	• If a denial of service is created for the firewall, then all corporate systems, including workstations, cannot talk to the rest of the world. Or even worse, during the outage, someone pilfers the corporate systems the firewall was intended to protect.	Low

PHYSICAL AND ENVIRONMENTAL SECURITY		
Section 7 of the 17799 standard covers the area of 'Physical and environmental security'. The subsets of this area that is of particular concern has to do with how much physical access is given to the firewalls themselves, including the firewall 'media' (aka floppies) and the backup hardware.		
ISO 17799 **Section 7.2 :: Equipment Security**		
Objective: '*To prevent loss, damage or compromise of assets and interruption to business activities*.'		
Risk	**Impact**	**Likelihood**
• The firewall, while in a locked room, is itself not enclosed in a locked cage or other type of secure holding area.	• Firewall could be physically damaged either purposely or by accident, thereby creating a loss of service for the corporate network. • Malicious users could potentially alter the system, in particular firewall rules, allowing for easier exploit of corporate resources.	Med Med

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

• Backup firewall servers are out in the open, with potential of damage, malicious reconfiguring, and or server being stolen.	• Firewall downtime could be exacerbated and or exposure created by addition of a maliciously reconfigured firewall on to the network.	Med

8. Communications and operations management		
Objective: To ensure the correct and secure operation of information processing facilities.		
ISO 17799 **Section 8.3 :: Protection against malicious software**		
Risk	**Impact**	**Likelihood**
• Open source software used for the firewall is either faulty and or has been maliciously altered prior to download. Process for verifying authenticity is not in place or not followed. (8.3.1)	• Best-case scenario would be that the software just doesn't work. Worse case scenario is that a backdoor of sorts has been created allowing penetration of the firewall into a protected area.	Low
Housekeeping		
Objective: *To maintain the integrity and availability of information processing and communication services*.		
ISO 17799 **Section 8.4.1 :: Information Backup**		
Risk	**Impact**	**Likelihood**
• Firewall and routing rules are not backed up in a standardized method and in a known place.	• If the system goes down, there will be a need to reload software and rules to bring the system operational again. if the rule set was not adequately backed up, there is a significant delay until rules are re-written to meet policy. Note that there are roughly 3000 rules for both security filtering and associated routing.	Low

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

ISO 17799 Section 8.4.2 :: Operator Logs		
Risk	**Impact**	**Likelihood**
• Changes to the rule base were made in terms of filtering and or routing, but there isn't a record as to who made the change and to what end.	• Without some traceability it would be difficult to distinguish between friendly changes to rules and malicious changes that might leave corporate servers and workstations open to attack.	Low

Enumerate and describe the major information asset that is directly affected by the role of the audited device, system, or application.

There are two basic categories of assets that are protected by the floppy firewall. Those categories are corporate workstations and corporate servers. There are countless workstations and servers protected by this firewall, therefore, the focus will be on those corporate servers seen as most critical if they were compromised.

Information Assets		
Asset	**Description**	**Impact If Compromised**
• Corporate Workstations.	These workstations include all desktops in all departments: Finance, HR, Development, QA, IT, Support, Sales, Marketing, and etc. These workstations run the gamut from windows, *nix, and Macs.	Information pilfering is the worse case scenario. If an executives computer, and or a developers workstation were compromised then there could be a serious issue in terms of intellectual property leakage, if not sensitive customer data being exposed.
• NetApp	NetApp is a NFS appliance. It holds all corporate docs regarding IP (intellectual capital) – Product Marketing, Engineering Specs, not to mention a variety of financial docs.	Since the server is backed up, the worse case scenario would be ongoing covert data retrieval. A denial of service, while obnoxious, would not matter so much.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

• CRM System	This is a database driven system, SQL Server, with a web front-end. Its 100% windows based. All sales and customer support data is stored on this system.	The data in this system is highly sensitive as it holds all sales data as well as all customer related issues. If the system were compromised in terms of a denial of service, while this would be inconvenient, it pales in comparison to pilfering of information.
• Defect tracking system	This is a database and webserver used to track various product issues as well as for tracking various features	As above, information gathering is the most serious threat.
• Software repository and revision control system	This is a system for storing all product related code, include all current and historical versions/	The threat of a lack of confidentiality is the main concern regarding this system.

Enumerate and describe the major vulnerabilities of the audit subject.
In terms of vulnerabilities, ISO 17799 will be denoted where applicable, but the main path of organization will be that of the 5 steps in the path of attacks.

Vulnerability	Impact	Likelihood
System compromise	Potential of getting root on the firewall, but what then? You can perhaps crash the system, or negatively affect the routing rules, but replacement is simple, as is reboot. It would be more obnoxious then anything else. If the assessment finds this readily exposable, then is should be remedied.	Highly unlikely. Compromise most likely by sniffing UID/Pwd. Since telnet is used, password is in the clear. Requires local access to admin subnet.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Vulnerability	Impact	Likelihood
Denial Of Service	Corporate servers and workstations would not be able to reach the internet, nor each other	Apart from physically attacking the box, a denial of service would have to occur through arp poisoning. The filtering is very light in terms of packet inspection, mostly routing based on IP. All connections could be routed to nowhere. Not very likely.

THE CURRENT STATE OF PRACTICE

Below I have listed resource, largely web based, that I have used either in terms of quoting, or have been influence by in thought. Where I have done a direct quote, and or used someone else's thoughts I have made note by appending the number, which reverences back to here.

By in large, I am not aware of any white papers that take a look at auditing a firewall from an ISO 17799 perspective, let alone a floppy firewall used in an intranet. There is probably good reason for this:

1. ISO 17799 is an overall framework for security, as opposed to something that would be applied to a singular product. Nonetheless, in the event of an audit, it would not be out of the ordinary for auditors to ask for proof of compliance for the firewall in terms of a particular ISO 17799-audit item. For example, in terms of section 3.1, certainly it would be reasonable to expect that main corporate firewall's would have some mention in the executive endorsed security policy.
2. ISO 17799 is not a standard that one could be registered to as of the writing of this paper. Unlike ISO 9000:2000, or the BS7799 standard, this standard does not have registrars and third party audit groups that determine if a companies practices meet the standard, and hence can be registered as compliant by the IOS.

In terms of SANS GSNA papers, I found Alan Mercer's application of the BS 7799 standard (largely the same as the 17799 standard for this paper) highly instructive as applied to a specific technology in a specific context. I particularly liked the format of his checklist in terms page layout. Mr Mercer's content items largely follow the SANS requirements for checklist items, as well as the BS7799 items as applicable as they apply to his particular audit. I have largely adopted the same approach, which is appropriate in meeting SANS content requirements as well as 17799 requirements as they apply to auditing the floppy firewall. It is possible to make a case, with some effort, for every item in the standard to apply

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

to this audit. A decision has been made to limit the audit to those 17799 items that seem to particularly apply to the context of the audit of this floppy firewall. Lastly, the choice of items to include in the audit reflects the desire of IT management. They would like an audit that focuses more on process and procedure that can be applied broadly throughout the organization.

AUDIT CHECKLIST

(Note to the extent possible most text in terms of checklist questions, objective, compliance check are taken from the 17799 standard – see 3 above. Reference section points to sections used for text. This is not reproduced in the checklist that contains results, as it added considerable space to the audit document.)

1 Security Policy				
Objective: To provide management direction and support for information security.				
Reference: • First edition ISO/IEC 17799:2000(E) International Standard (1) o 3.1.1 Security Policy Document o 3.1.2 Review and evaluation • SANS: Avaya INDeX PBX Security Audit (4) • OWASP 17799 Draft Guide, Section 3.1 (Not available publicly) • Real World Linux Security (14)				
Risk: "The vast majority of users do not have the technical expertise, the time, or the interest to understand how to maintain security, but can be cajoled into following a policy, especially when failure to follow it has unpleasant consequences. " (14) Without a security policy to make clear managements general objectives in terms of what to secure and how, security is left in the hands of those with random motives and skills that may or may not be in line with business objectives.				
Test Nature:	Objective:	☒	Subjective:	☐
Compliance Check: A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization's approach to managing information security. (1)				

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Testing Procedure:

1. Is there a documented security policy that provides evidence that it is approved by management?

2. Can IT staff responsible for corporate 'intranet' security locate the security policy? Can they state management's general intent in terms of security, and the recommend approach as specified in the security policy?

3. Is there documented proof of management's review of corporate security as it is set forth in the security policy

4. Is there documented evidence that management, and its representative for security, update the security policy and its implementation based on such things as security assessments and incidents, policy effectiveness review, cost of controls, and effects on security due to change in technology?

2 Personnel Security

Objective: To ensure that users, particularly those responsible for the floppy firewall's maintenance, are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.

Reference:

- First edition ISO/IEC 17799:2000(E) International Standard (1)
    - 6.1.1 Security in job description
    - 6.2.1 Security Ed & Training
    - 6.3.1 Reporting security incidents
    - 6.3.2 Report security weaknesses
    - 6.3.3 Report software malfunctions

Risk: If personnel responsible for maintaining the firewall, and related security, do not have adequate IT security skills, then critical infrastructure that management deems necessary to protect could be unnecessarily exposed to threats.

Test Nature:	Objective: ☒	Subjective: ☐

Compliance Check: Security responsibilities should be addressed at the policy stage and within job descriptions. Adequate training should be provided to enforce the security policy where there are potential deficiencies. .

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Testing Procedure:

1. Are security responsibilities in terms of job functions documented in the security policy and job descriptions, particularly as they relate to the design and maintenance of custom built Linux firewalls?

2. Is there proof that relevant IT staff has received training in terms of the implementation and maintenance of the security policy, particularly as it relates to the corporate firewall?

3. Have relevant staff been trained to handle security incidents as it relates to the corporate firewall. This includes training in reporting security incidents including weaknesses, software malfunctions, breaches and threats. For example, if the floppy firewall need to be rebuilt, kernel configuration outward, can all relevant staff perform these operations?

3 Physical and Environmental Security

Objective: Objective: '*To prevent unauthorized access, damage and interference to business premises. To prevent likewise prevent information loss, damage or compromise of assets and interruption to business activities*.'

Reference:

- First edition ISO/IEC 17799:2000(E) International Standard (1)
    - 7.1.1 Physical security perimeter
    - 7.1.2 Physical entry controls
    - 7.2.1 Equipment siting and protection
    - 7.2.2 Power supplies
    - 7.2.3 Cabling security

Risk: The floppy firewall could be physically damaged either purposely or by accident, thereby creating a loss of service for the corporate network. Malicious users could potentially alter the system, in particular firewall rules, allowing for easier exploit of corporate resources.

Test Nature:	Objective: ☒	Subjective: ☐

Compliance Check: Critical or sensitive business information processing facilities should be physically protected from unauthorized access, damage and interference. The protection provided should be commensurate with the identified risks.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Testing Procedure:

1. Is the firewall removed from the general IT work area, for example behind a locked door?

2. Is there any form of authentication controls such as swipe cards and or bio-metric devices used to authenticate users and to create an audit trail?

3. Is there proof that access rights to the area where the firewall is kept are regularly reviewed and updated?

4. Is there firewall in a cabinet or other locked area that prevents it from being tampered with? Are the cables readily accessible? Are backup servers also locked down so that they cannot be tampered with?

5. Is there a power supply, such as a UPS, for the firewall?

4 Operational procedures and responsibilities

Objective: Objective: 'To ensure the correct and secure operation of the intranet floppy firewall.'

Reference:

- First edition ISO/IEC 17799:2000(E) International Standard (1)
  - 8.1.1-3 SOP's to Segregation of Duties
  - 8.3.1 Controls against malicious software
  - 8.4.1 Information back-up
  - 8.4.2-8.4.3 Log files (9.7.1)
  - 8.5.1 Network controls
  - 8.6.1 Management of removable computer media
  - 8.6.4 Security of system documentation

Risk: without adequate operational controls in place in terms of the assembling, deployment, and maintenance of the floppy firewall significant vulnerabilities may be introduced. The associated risks include, but are not limited to, such things as the introduction of corrupt software, lack of backups for recovery, lack of audit trail in terms of change management, and the loss of classified firewall documentation.

Test Nature:	Objective: ☒	Subjective: ☐

Compliance Check: Responsibilities and procedures for the management and operation of floppy firewall should be established.

Testing Procedure:

1. Are there documented operating procedures for firewall rebuild, restart and recovery?

2. Is there an audit log associated with changes to the floppy firewall system? This includes changes in rules, software, hardware, and identity and time or person accessing the firewall? Are there logs associated with tracking of faults and remediation?

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

3. Is there a formal approval procedure for proposed changes to firewall policy implementation?

4. Is there a procedure for addressing security incidents in relationship to the floppy firewall, and or related network security?

5. Is there a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium.

6. Is there any base lining done to the floppy firewall, and regular integrity checks against the baseline in terms of changes to rules or otherwise?

7. Any procedures in terms of addressing and recovering from virus attacks to the firewall, and or the floppy firewalls part in the quarantine of infected network segments?

8. Are the procedures in place in terms of the backup and secure storage of the firewall configuration files? Do these procedures include restoration procedures in terms of the firewall configuration file, and are they tested? Is the media physically protected during storage, and is disposal of old media (floppy with configs) done in a way that erases the data or renders it useless (see #1 above).

5 Access Control

Objective: Protection of networked services and detection of unauthorized activities.

Reference:

- First edition ISO/IEC 17799:2000(E) International Standard (1)
  - 9.4.1 Policy on use of network services
  - 9.4.2 Enforced Path
  - 9.7.1 Event Logging

Risk: Access should only be granted to services to users with specific authorization for those services.

Test Nature:	Objective: ☒	Subjective: ☐

Compliance Check: The floppy firewall provides adequate network controls as generally specified in the security policy.

Testing Procedure:

1. Is there a policy that defines procedures for determining who is allowed to access specific networks and networked services?

2. Are specific paths of network traffic enforced by the floppy firewall reflective of the above policy.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

3. Are there audit logs in relation to the floppy firewall that record exceptions and other security-relevant events? Facts collected should include such things and user Ids, dates and times for log-on and offs, terminal identity or location if possible, records of successful and reject system access attempts, records of successful and rejected data and other resource access attempts.

6 Business Continuity Management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

Reference:

- First edition ISO/IEC 17799:2000(E) International Standard (1)
  - 11.1.1 Business continuity management process
  - 11.1.2 Business continuity and impact analysis
  - 11.1.3 Writing and implementing continuity plans
  - 11.1.5 Testing, maintaining and re-assessing business continuity plans.

Risk: Without ensuring that the firewall systems can be made operational in a timely manner in the event of an outage, critical business processes could be subject to undue disruptions which can result in a result in revenue.

Test Nature:	Objective: ☒	Subjective: ☐

Compliance Check:

A business continuity management process should be implemented in relation to the floppy firewall to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls.

Testing Procedure:

1. Has there been an assessment in terms of the risk to the organization if there were a failure in terms of the floppy firewall?

2. Have acceptable risks been identified in terms of length of outage as applied to the business day, and how it applies to customers and related services for the organization?

3. Has there been a test to validate recovery in terms of an outage? Has the associated security policy been updated accordingly based on test results?

4. Has specific personnel been identified in terms of remediation if the firewall were to have an outage?

5. Has identified personnel been tested to ensure they can perform the requisite functions if the were an outage?

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

7 Systems Development and maintenance ::Cryptographic controls				
Objective: To protect the confidentiality, authenticity or integrity of information.				
Reference: • First edition ISO/IEC 17799:2000(E) International Standard (1) o 10.3.1 Policy on the use of cryptographic controls o 10.3.2 Encryption				
Risk: If data is not encrypted while traveling to the floppy firewall, it may be intercepted and used to gain access to the floppy firewall.				
Test Nature:	Objective: ☒		Subjective: ☐	
Compliance Check: Management of the floppy firewall should be done over encrypted connections.				
Testing Procedures: 1. Is there a policy on the corporate use of encryption in relation to network resources? 2. Are all means of connecting to the firewall for management purpose done using encryption?				

8 Compliance				
Objective: to ensure compliance of the floppy firewall to the security policy and related standards on an ongoing basis by conducting firewall system audits.				
Reference: • First edition ISO/IEC 17799:2000(E) International Standard (1) o 12.2.1 Compliance with security policy o 12.2.2 Technical compliance checking o 12.3.1 System audit controls • Lance Spitzner, Armoring Linux (12) • Jay Beale, How do I Tighten Security My System? (15) • Jay Beale, Shredding Access in the Name of Security: Set UID Audits (16) • Jay Beale, Anyone with a screwdriver can break in (17) • Steven Sipes, Why your switched network isn't secure. (18)				
Risk: Networks, software, and users are dynamic and prone to change. Policies should change to meet the demands of such a dynamic environment. Proof that the system adheres to policy changes on an ongoing basis is required to minimize the possibility of vulnerabilities being exploited.				
Test Nature:	Objective: ☒		Subjective: ☐	
Compliance Check: The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with security implementation standards, without disruption to business processes and systems.				

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Testing Procedure:

1. Has management with responsibility for security in relation to the floppy firewall ensured compliance to applicable security policies on an ongoing basis?

2. Is the Linux operating system associated with the floppy firewall configured (hardened) up to acceptable security standards?
    a. Check the partitioning, is there only one partition, therefore susceptible to a denial of service
    b. Are there any unnecessary services running?
    c. Check that all .rc scripts that are unnecessary are turned off.
    d. Are password files protected?
        i. /etc/shadow – use MD5, alert PAM
        ii. Removed default system accounts in /etc/passwd
    e. Since telnet is enabled (ssh to heavy for memory), make sure root cannot telnet in.
    f. Is /etc/host.deny and /etc/hosts.allow implemented appropriately.
    g. Have .rhosts, .netrc, and /etc/hosts.equiv been locked down?
    h. Remove history for commands
    i. Is password for BIOS, and /etc/lilo.conf
    j. Are patches implemented with regularity?
    k. Is set uid as root disabled where applicable.
    l. Are services that are running, running on standard ports?
    m. Are patches implemented with regularity?
    n. Is set uid as root disabled where applicable.

3. Is the firewall tested for the possibility of exploit, particularly in terms of system compromise and or denial of service? Is there proof of these tests, with results impacting implementation of the firewall and policy based on assessed risks to the system?
    a. Run a scanner against the firewall. Are there any known vulnerabilities that can be exploited.

    b. Try arp spoofing using ettercap http://ettercap.sourceforge.net to simulate a method of capturing admin traffic.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

AUDIT CHECKLIST COMPLETED
(Note that references are left for the checklist template, and removed here to conserve space)

1 Security Policy
Objective: To provide management direction and support for information security.
Compliance Check: A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization's approach to managing information security. (1)
Testing Procedure: 1. Is there a documented security policy that provides evidence that it is approved by management? **Findings:** There is a corporate IT policy. It is the type of document that has been emailed to management for review, but there is no signed confirmation of the IT policy. 2. Can IT staff responsible for security locate the security policy? Can they state management's general intent in terms of security, and the recommend approach as specified in the security policy? **Finding:** IT Staff can locate the corporate IT policy on the intranet. There is no overarching perspective on security, nothing that can be pointed to that is reflective of management's intent towards corporate security. 3. Is there documented proof of management's review of corporate security as it is set forth in the security policy **Finding:** There is no specified executive review of corporate security, particularly as it applies to the security policy. Management representative has proof of corporate IT policy change based on incidents. 4. Is there documented evidence that management, and its representative for security, update the security policy and its implementation based on such things as security assessments and incidents, policy effectiveness review, cost of controls, and effects on security due to change in technology? **Finding:** While the corporate IT group is very response to security related issues, there is not documentation trail in terms of specific policy changes or otherwise.
2 Personnel Security
Objective: To ensure that users, particularly those responsible for the floppy firewall's maintenance, are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Compliance Check: Security responsibilities should be addressed at the policy stage and within job descriptions. Adequate training should be provided to enforce the security policy where there are potential deficiencies. .

Testing Procedure:

1. Are security responsibilities in terms of job functions documented in the security policy and job descriptions?

   Finding: There is an outdated set of job descriptions. There also is a contact list that shows general responsibilities related to IT concerns. There also is a disaster recovery document that specifies certain responsibilities. There is no maintained description of security related job functions that are maintained in conjunction with the security policy document.
2. Is there proof that relevant IT staff has received training in terms of the implementation and maintenance of the security policy?

   Finding: No. Nonetheless, IT personnel have proven that they do have the requisite skills.

3. Have relevant staff been trained to handle security incidents. This includes training in reporting security incidents including weaknesses, software malfunctions, breaches and threats. For example, if the floppy firewall need to be rebuilt, kernel configuration outward, can all relevant staff perform these operations?

   Finding: There is no documented in terms of specific training, particularly as it relates to maintaining the corporate 'floppy' firewall.

3 Physical and Environmental Security

Objective: Objective: '*To prevent unauthorized access, damage and interference to business premises. To prevent likewise prevent information loss, damage or compromise of assets and interruption to business activities*.'

Compliance Check: Critical or sensitive business information processing facilities should be physically protected from unauthorized access, damage and interference. The protection provided should be commensurate with the identified risks.

Testing Procedure:

1. Is the firewall removed from the general IT work area, for example behind a locked door?

   Pass: Yes

2. Is there any form of authentication controls such as swipe cards and or bio-metric devices used to authenticate users and to create an audit trail?

   Pass: Yes

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

3. Is there proof that access rights to the area where the firewall is kept are regularly reviewed and updated?

   Pass: Yes, and there is proof of review. Logs are reviewed on a daily basis for access to the IT area.

4. Is the firewall in a cabinet or other locked area that prevents it from being tampered with? Are the cables readily accessible? Are backup servers also locked down so that they cannot be tampered with?
   Findings:
   a. No cabinet
   b. Cables are readily accessible
   c. Backups are not locked down

5. Is there a power supply, such as a UPS, for the firewall?

   Pass: There is a UPS

4 Operational procedures and responsibilities

Objective: Objective: 'To ensure the correct and secure operation of the intranet floppy firewall.'

Compliance Check: Responsibilities and procedures for the management and operation of floppy firewall should be established.

Testing Procedure:

1. Are there documented operating procedures for firewall rebuild, restart and recovery?

   Finding: No

2. Is there an audit log associated with changes to the floppy firewall system? This includes changes in rules, software, hardware, and identity and time or person accessing the firewall? Are there logs associated with tracking of faults and remediation?

   Pass: In terms of general auditing, syslog is enabled.
   Finding: There isn't a specific audit log in terms of faults and remediation.

3. Is there a formal, documented, approval procedure for proposed changes to firewall policy implementation?

   Finding: Changes do go through IT management, but there is no associated documentation.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

4. Is there a procedure for addressing security incidents? Is there anything particular to the firewall?

   Finding: Nothing documented, although there is an IT emergency contact list.

5. Is there a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium.

   Pass: Largely built in house, audited prior to being put into use. All scripts audited and cleaned up.

6. Is there any base lining done to the floppy firewall, and regular integrity checks against the baseline in terms of changes to rules or otherwise?

   Pass: There is a system that downloads the firewall rules on an hourly basis and checks differences between previous downloads, and alerts based on differences.

7. Any procedures in terms of addressing and recovering from virus attacks to the firewall, and or the floppy firewalls part in the quarantine of infected network segments?

   Findings:
   a. No documentation for firewall related virus handling
   b. Firewall has been used for quarantine, but no documented procedures.

8. Are the procedures in place in terms of the backup and secure storage of the firewall configuration files? Do these procedures include restoration procedures in terms of the firewall configuration file, and are they tested? Is the media physically protected during storage, and is disposal of old media (floppy with configs) done in a way that erases the data or renders.

   Pass: Backups happen regularly. Configuration files are in limited access area. All passwords for accessing are encrypted. Offsite storage with Iron Mountain. There is an overwrite process for the floppies.

5 Access Control

Objective: Protection of networked services and detection of unauthorized activities.

Reference:

- First edition ISO/IEC 17799:2000(E) International Standard (1)
  - 9.4.1 Policy on use of network services
  - 9.4.2 Enforced Path
  - 9.7.1 Event Logging

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Risk: Access should only be granted to services to users with specific authorization for those services.				
Test Nature:	Objective:	☒	Subjective:	☐
Compliance Check: The floppy firewall provides adequate network controls as generally specified in the security policy.				

Testing Procedure:

1. Is there a policy that defines procedures for determining who is allowed to access specific networks and networked services?

   Finding: There is no written policy that is specific, beyond the floppy firewall rule base. The expressed view of IT was to create subnets that are based on departmental and job functions. Control for ingress and egress is enforced for these groups via the firewall.

2. Are specific paths of network traffic enforced by the floppy firewall reflective of the above policy?
   Warning: As stated above, there is no written policy, but a dump of the firewall rules, and brief test of effectiveness reveal that serious consideration has been taken in terms of intent.

NOTE: A review of the 16+ pages of rules is out of scope for this paper. But, a brief description of the policy as implied by the iptables rules is shown below. Also, a quick spot check on the application within one particular departmental subnet is shown. All areas mentioned below represent grouped network resources, as the network is sub netted in terms of departmental and functional groups. So, while there are 16+ pages of rules, they are grouped in such a way as to make maintenance quite simple.

A. Departmental Groups: (ip ranges for groups and subgroups within each department).
   I. QA: This consists of all QA workstations and servers. In particular, it consists of several class B networks that are used for security testing.
   II. Support: support_net, support_wkstn: Support related networks
   III. CRM: consists of all systems related to the CRM system
   IV. DEV: All servers and workstations associated with development
   V. IT: All servers and work stations associated with IT
   VI. OPS: All servers and workstations associated with operations management.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Test: Auditor attached to the corporate workstations and was assigned a DHCP address. Access to network resources were largely non-existent. For example, auditor could not access operations intranet webserver via browser. Auditor, was give static ip within the support workstations, and in turn had access to the OPS web server via the following rule, which exemplifies GES's corporate infrastructure as expressed in the floppy firewall's iptables:

```
Iptables –A FORWARD –s $support_wkstn –d $ops_intranet $svc_Web –j accept
```

B. Invalid TCP/IP State Flag combos dropped:
Example for application of rule to IT servers (it_svrs):

I. All bits are cleared
II. SYN and FIN are both set
III. SYN and RST are both set
IV. FIN and RST are both set
V. FIN is the only bit set, without the expected accompanying ACK
VI. PSH is the only bit set, without the expected accompanying ACK
VII. URG is the only bit set, without the expected accompanying ACK

Test for tcp flag rules by scanning across firewall to adjacent network segment. NMAP 3.50 used in this case, as opposed to proprietary scanner. Auditor is scanning from the support network segment.

I. Ping Scan to prove host is up for testing:

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-04-28 06:46 PDT
Host corp2.corp.ges.com (10.100.1.22) appears to be up.
Nmap run completed -- 1 IP address (1 host up) scanned in 0.321 seconds
```

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

II. Send tcp connect scan for only first 100 ports, to see if normal traffic can get though to a more limited set of ports. This is a host the support can see:

```
nmap -sT -p 1-100 10.100.1.22
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-04-28 17:43 PDT
Interesting ports on corp2.corp.GES.com (10.100.1.22):
(The 98 ports scanned but not shown below are in state: filtered)
PORT   STATE SERVICE
53/tcp open  domain
88/tcp open  kerberos-sec
```

Result: **Pass**

III. Verify null scans are blocked:

a. Firewall Rule:

```
Iptables –A FORWARD –p tcp –d $it_svrs –tcp-flags AL NONE –j LOG –log-prefix “ILL TCP
ST: All bits” –log-ip-options –log-tcp-options
Iptables –A FORWARD –p tcp –d $it_svrs –tcp-flags ALL NONE –j DROP
```

b. nmap scan

```
nmap -sN -p 1-100 10.100.1.22
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-04-28 07:06 PDT
All 100 scanned ports on corp2.corp.foo.com (10.100.1.22) are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 6.535 seconds
```

Result: **PASS**

IV. Verify XMAS Scan Blocking

a. Fin, Urg, Psh Firewall Rule Apply individually, as well as to blocking an xmas scan.

```
Iptables –A FORWARD –p tcp –d $it_svrs –tcp-flags ACK,FIN FIN –j LOG –log-prefix “ILL TCP
ST: FIN no ACK” –log-ip-options –log-tcp options
Iptables –A FORWARD –p tcp –d $it_svrs –tcp-flags ACK,FIN FIN –j DROP
```

```
Iptables –A FORWARD –p tcp –d $it_svrs –tcp-flags ACK,URG URG –j LOG –log-prefix “ILL
TCP ST: URG no ACK” –log-ip-options –log-tcp options
Iptables –A FORWARD –p tcp –d $it_svrs –tcp-flags ACK,URG URG –j DROP
```

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

```
Iptables –A FORWARD –p tcp –d $it_svrs –tcp-flags ACK,PSH PSH –j LOG –log-prefix “ILL TCP
ST: FIN no ACK” –log-ip-options –log-tcp options
Iptables –A FORWARD –p tcp –d $it_svrs –tcp-flags ACK,FIN FIN –j DROP
```

b. Nmap XMAS scan test of firewall rule

```
nmap -sX -p 1-100 10.100.1.22
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-04-28 06:55 PDT
All 100 scanned ports on corp2.corp.foo.com (10.100.1.22) are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 6.506 seconds
```

Result: **Pass**

V. Verify that support cannot see network segments off limits.
   a. Ping to see if host is alive

```
nmap -sP  10.110.0.3
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-04-29 08:00 PDT
Host sw01.uk01.GES.com (10.110.0.3) appears to be up.
Nmap run completed -- 1 IP address (1 host up) scanned in 1.060 seconds
```

b. Run scan on all ports to see if tcp connect can occur

```
nmap -sT  10.110.0.3
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-04-29 07:55 PDT
All 1659 scanned ports on sw01.uk01.GES.com (10.110.0.3) are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 193.269 seconds
```

3. Are there audit logs in relation to the floppy firewall that record exceptions and other security-relevant events? Facts collected should include such things and user Ids, dates and times for log-on and offs, terminal identity or location if possible, records of successful and reject system access attempts, records of successful and rejected data and other resource access attempts. (Note example above in terms of logging commands):

Syslog related rules:

```
Iptables –A INPUT –p udp –sport 514 –d 0/0 –s $SYSLOG_SVR –j ACCEPT
Iptables –A OUTPUT –p udp –dport 514 –d $SYSLOG_SVR –s 0/0 –j ACCEPT
```

Result: **Pass**

6 Business Continuity Management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Compliance Check:
A business continuity management process should be implemented in relation to the floppy firewall to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls.

Testing Procedure:

1. Has there been an assessment in terms of the risk to the organization if there were a failure in terms of the floppy firewall?

   Pass: Yes, there is a written assessment.

2. Have acceptable risks been identified in terms of length of outage as applied to the business day, and how it applies to customers and related services for the organization?

   Pass: Yes, there is written documentation.

3. Has there been a test to validate recovery in terms of an outage? Has the associated security policy been updated accordingly based on test results?

   Finding: The process has been tested on the job, in real scenarios. It takes 5 minutes to bring it up. There is stand by hardware, and floppy. There has not been any organized test with any sort of regularity, an no documentation as proof of practice.

4. Has specific personnel been identified in terms of remediation if the firewall were to have an outage?

   Pass: Yes, generally based on the documented disaster recovery plan and emergency contact list.

5. Has identified personnel been tested to ensure they can perform the requisite functions if there were an outage?

   Finding: Personnel have been tested in real scenarios, but not in test scenarios.

7 Systems Development and maintenance ::Cryptographic Controls

Objective: To protect the confidentiality, authenticity or integrity of information.

Reference:

- First edition ISO/IEC 17799:2000(E) International Standard (1)
  - 10.3.1 Policy on the use of cryptographic controls
  - 10.3.2 Encryption

Risk: If data is not encrypted while traveling to the floppy firewall, it may be intercepted and used to gain access to the floppy firewall.

Test Nature:	Objective:	☒	Subjective:	☐

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Compliance Check: Management of the floppy firewall should be done over encrypted connections.

Testing Procedures:

1. Is there a policy on the corporate use of encryption in relation to network resources?
   Finding: There is not policy in terms of corporate use of encryption.
2. Are all means of connecting to the firewall for management purpose done using encryption?
   Finding: No, in terms of writing changes, telnet is used.

8 Compliance

Objective: to ensure compliance of the floppy firewall to the security policy and related standards on an ongoing basis by conducting firewall system audits.

Compliance Check: The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with security implementation standards, without disruption to business processes and systems.

Testing Procedure:

1. Has executive management with responsibility for security in relation to the floppy firewall ensured compliance to applicable security policies on an ongoing basis?

   Finding: While the IT manager does review policy with regularity executive management does not.

2. Is the Linux operating system associated with the floppy firewall configured (hardened) up to acceptable security standards?

   Note: many of the test/hardening considerations below do not apply due to the nature of the floppy firewall. Nonetheless presenting proposed tests, and the reason they are not considered or otherwise, will help to illustrate some of the intrinsic security features of a floppy firewall.

   a. Check the partitioning. Is there only one partition, therefore susceptible to a denial of service.

      Pass: Not applicable, creates a RAM drive which is a limited set of space. There is no disk, hence no writing to it.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

b. Are there any unnecessary services running?
   Pass: see netstat output below.

```
# netstat –an
Active Internet connections (servers and established)
Proto   Recv-Q  Send-Q  Local Address          Foreign Address        State
tcp     0       0       0.0.0.0:23             0.0.0.0:*              LISTEN
tcp     1       1       x.x.x.x:23             x.x.x.x:xxxx           ESTABLISHED
udp     0       0       0.0.0.0:161            0.0.0.0:*
Active UNIX domain sockets (servers and established)
Proto   RefCnt  Flags       Type            State           I-Node Path
```

c. Check that all .rc scripts that are unnecessary are turned off.
   Pass: There is one script that launches all the processes, which is proprietary.
d. Are password files protected?
   i. /etc/shadow – use MD5, alert PAM
      Pass: Telnet daemon, upon startup, grabs password from a clear text file (config file). In theory, the floppy disk could be accessed prior to load, and a new password applied by a malicious user.
   ii. Removed default system accounts in /etc/passwd
      Pass: Doesn't exist on system
e. Since telnet is enabled, make sure root cannot telnet in.
   Pass: There are no user accounts, not applicable
f. Is /etc/host.deny and /etc/hosts.allow implemented appropriately.
   Pass: Not used.
g. Have .rhosts, .netrc, and /etc/hosts.equiv been locked down?
   Pass: Not applicable.
h. Is password for BIOS
   Finding: No password
i. Are patches implemented with regularity?
   Pass: Yes, when critical kernel issues come out, kernel is patched and recompiled.
j. Is set uid as root disabled where applicable.
   Pass: No processes for anyone to run, no concept of root or user.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

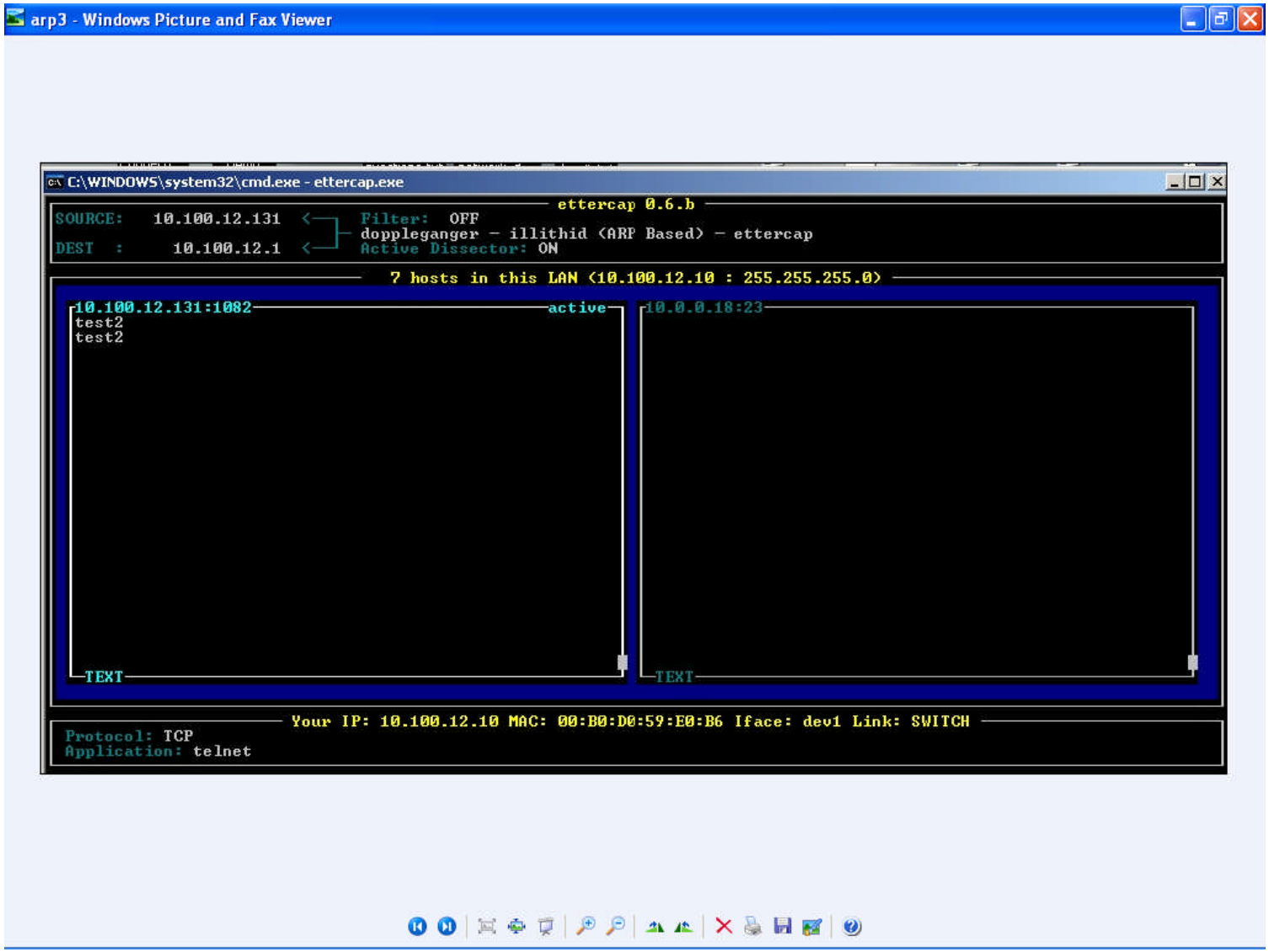
3. Is the firewall tested for the possibility of exploit, particularly in terms of system compromise and or denial of service? Is there proof of these tests, with results impacting implementation of the firewall and policy based on assessed risks to the system?
    k. Run a scanner against the firewall and see if there any known vulnerabilities that can be exploited.

Operating System Detected : (Stack Fingerprinting)		**There is no data available**	
Services Detected:		**There is no data available**	
Vulnerabilities Total:		**4**	
Vulnerabilities		**Type**	**Severity**
1.	ICMP Timestamp Request	Info Only (no vuln)	Minor
2.	ICMP Replies Received	Info Only (no vuln)	Minor
3.	Reachable Host List	Info Only (no vuln)	Minor
4.	Firewall Detected	Info Only (no vuln)	Minor

Pass: There aren't any glaring security holes from a scanning perspective. While telnet, for example, is seen to be open via netstat, one would need to be physically on the management network to access the server via telnet. Also, you would of course need the password, and short of social engineering to get it from one of two administrators. Basically, you would be limited to running a sniffer like tcpdump, and or arp spoofing, to recover the password. Again, this presupposes that you have physically have access to the management subnet.

l. Try arp spoofing so that admin telenet traffic to and from the firewall passes through your host so that you can sniff the UID and password which are in the clear. Ettercap was used for arp spoofing http://ettercap.sourceforge.net/
    i. Requires physical access to admin subnet
    ii. Requires knowledge of source and des in terms of admin console from which telnet connection would be made, and of course, ip of firewall.
    iii. Note that the actual IP of host, on bottom of image below
    iv. Note source IP and Dest IP in terms of telnet, and of course, captured ascii text in terms of username and password.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*



*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Finding: This whole issue of sniffing the uid and password would be largely null and void if ssh were used, which is available for the specific version of floppy firewall. Note that this version was not available at the time of original install, and would require kernel changes and other ancillary changes if telnet were completely removed. Nonetheless, it should be implemented to remove this relatively small possibility of attack.

Audit Executive Summary:

The main purpose of this audit was to expose areas needing strengthening along the lines of policy and procedure, particularly as they apply to securing the corporate intranet and related services. Using applicable parts of the ISO 17799 standard has allowed us to achieve this end. For example,

- We revealed that there was not an overarching security policy approved, enforced, and reviewed by executive management.
- There is no documentation in terms of firewall maintenance and recovery.
- IT staff, apart from the manager, has not been trained to bring the firewall back to an operational state in the event of a failure.
- Firewall rule set, and network design, is well thought out in terms of security, maintenance, and does match the 'verbal' policy as expressed by the IT manager.
- The auditor had zero access to subnets that he did not have explicit access to when he began his audit. With minimal effort, by simply giving the auditor a static ip in the support workgroup, the auditor had access to all support related items. Spot checking via scanning affirmed that rules were functioning as specified.
- The firewall itself is basically impermeable unless one was to have access to the IT subnet. Even so, scanning revealed scant information aside from basic icmp related phenomena.
- Netstat reveals only telent and syslog related services available on the firewall
- The threat of physical compromise of the firewall is moderate. The auditor verified that access logs to the room containing the firewall are checked daily to ensure only the limited user set authorized are actually accessing the room where the firewall is contained.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Major Audit Findings Details:
Below is a list of major findings. This of course is a relative term, as the system on whole is functioning as designed. That being said, from an ISO 17799 perspective this audit had many findings, as shown in the checklist, along the lines of policy and procedure. This audit would not have passed and ISO 17799 registration audit. (if one existed, a BS7799 audit would be the next best thing) This will not come as a surprise to the audited group, as their expressed desire was a beefing up in terms of the policy and procedure side of security.

1. Lack of Executive Management Approved Security Policy
(*audit checklist section 1*)
The auditor interviewed IT management in terms of applicable sections of ISO 17799, which a focus on section 3.1. This interview discovered that IT management has put much thought into network design and controls in terms of security. While this is considered 'good security', it still would be a finding in an ISO styled audit. That is because there is no documented proof of executive management endorsement for the current security implementation. Endorsement from corporate management helps to ensure that mission critical systems have appropriate controls. Also, executive support makes the policy more apt to be adopted by the organization as a whole. To that end, the goal of ISO is to make thing same and equal across the organization, and management backing would be key for such an endeavor.

Risk:
'*The firewall is a genuine policy enforcement engine, and like most policy enforcers, it is none too bright*.' (20)

Without a management policy, there is no way to determine if adequate defenses have been employed for the services management deems necessary to protect for its customers and other stake holders. For example, an IT manager may not realize the levels of importance between a corporate file server, software bug tracking system, revision control system for software development, CRM system for sales and customer support from a revenue generating perspective. They are all important, and the manager in question may know how to harden all the systems from the kernel to the perimeter, but do the controls reflect executive management's views? Again, which items deserves special attention in terms of protection for exploit, revenue and or natural disaster etc? This sort of assessment has not occurred formally, and strategically is a gapping hole in terms of corporate security.

2. Lack of training and procedures for support the floppy firewall
(*audit checklist section 2*)
During the interview, the auditor suggested that a test be contrived in which other IT personnel would be tested to see if they could rebuild the system if need be. IT management suggested that such a test would not prove fruitful. The manager stated that while other IT staff is capable of rebooting the

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

firewall, rebuilding from the kernel out would not happen. Currently only the IT manager has the skills to fully rebuild the system in the event of a complete loss. The manager did point out that there are other staff members within the operations and development groups that could probably rebuild the system, but this is not a proven fact, and would be outside the scope of the audit. Despite the prevalence of highly skilled security professionals, this would still be considered a major finding in a standard ISO audit.

Risk:
Short of a policy to determine the value of the resources the firewall protects, the IT manager states that the floppy firewall is a 'critical' system to protecting most corporate servers. There has been an assessment of acceptable downtime during production hours for the firewall. That down time had a max limit of four hours. If the firewall is down for four hours all customer support is largely brought to a halt, accept phone contact. The question becomes one of policy, does this downtime IT policy match with the corporate commitment of 24-7 support policy?

Is it reasonable to expect an IT manager to know that the 24-7 policy exists and that a four hour downtime may be unacceptable? Perhaps, but short of a policy supported and enforced by executive management this sort of concern along the lines of availability will slip through the cracks. In the end, if four hours is deemed unacceptable, then there may need to be training, testing, and procedures developed in terms of remediation to meet policy as authorized by senior management.

3. Unencrypted Services Used For Firewall Maintenance

(*audit checklist section 7*)
Telnet is used for the floppy firewall maintenance. Connecting to the firewall requires being on the same subnet, thus exploit is very difficult. Nonetheless, unless specifically stated otherwise in the security policy, encryption should be in use.

Risk: In theory a password could be sniffed, note the previous test doing just that using ettercap. A sniffed username and password could lead to system compromise. The best a compromise could probably do is create a DoS condition, which ties into meeting the corporate commitment to 24X7.

Audit Recommendations:

Policy

GES has two internal IT employees, one is the manager, and the other a staff person. All recommendations need to take into consideration the fact that there are only so many hours in the day for two people to work. This consideration

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

brings up the main area of remediation, which should help in focusing all other efforts,

> **GES needs an executive management endorsed and supported corporate security policy.**

To that end, the auditor is recommending that executive management look to the 17799 standard as a guide to developing a policy, and related procedures. Section 3.1 of the standard can provide the template for a policy that the executive team can then define. Section 3.1 has the following statement in terms of management's participation in the security policy development process:

> *Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.*

That statement is broad, and allows for some interpretation. The auditor thinks that a general statement from management about its views on security would be an ideal first step. This is typical of ISO, and in the event of an audit there would more than likely be a question asked of all IT personnel and management that would show up as such,

> '*Can you please tell me, in your own words, what the corporate security policy statement is*?'

While this may seem like an innocuous question, it is one of the main ways that an auditor can determine whether or not those with charge over security understand what their general marching orders are from executive management

A security policy statement could be something like the following,

> *'GES is committed to performing ongoing risk assessment and mitigation as it applies to providing service to our internal and external customers.'*

While this statement may seem like something straight out of Dilbert, it implies that risk assessments are being conducted, and that the results of the assessments are being directly applied to policy and procedure.

From such a 'security policy statement', other practices can also evolve. For example, an assessment of the various corporate IT servers can be made in terms of what value they bring to meeting customer needs. In such an assessment, there would need to be an evaluation of possible system compromise. If there were a compromise of said systems, what impact would it have on the customer? Note how the focus comes back to the customer. All policies and procedures would always need to be grounded in terms of a risk assessment and the impact of compromise upon the customer.

Human Resources

The above sort of practice should also extend into the practices associated with security and human resource, in particular, training. While the competency of the IT personnel was never in question, the lack of policy and procedure made their competence non-scalable. Meaning, if the two IT personnel were nowhere to be

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

found, and the firewall completely died, the organization would be at a veritable standstill in terms of providing service to its customer. But, the auditor believes that a cogent set of procedures would largely eliminate this problem.

If a thorough risk assessment were made of the various corporate server that are key to providing ongoing service to GES customers, and the assessment showed the floppy firewall's uptime as absolutely critical – which it would – then the staff responsible for maintaining the firewall would more than likely need procedures to assist in brining the firewall up from scratch in the event of a catastrophe. A risk assessment would point to the first sets of standard operating procedures that would need to be developed. Overtime, the set of procedures would expand to meet assessed risk.

Encryption

Simply put, use SSH. Beyond employing SSH, it is recommended to tighten up network alerting on the IT management subnet in which the firewall lives. Since this is a contained area, perhaps arpwatch can be employed, and also various checks for nics that have gone into promiscuous mode. Robert Graham's sniffing faq (21) provides a great overview of freely available tools and methodologies that can be combined to detect sniffing activity. Again, much of this would be a mute point if SSH were used for connection.

REFERENCES:

ISO 17799 Related:

1. ISO/IEC Information technology 17799:2000(E) Standard — Code of practice for information security management
2. http://www.sans.org/score/ISO_17799checklist.php (Main checklist resource) First edition ISO/IEC 17799:2000(E) International Standard
3. http://www.owasp.org There is an interpretation of ISO 17799 as applied to web application security, its in an early draft stage, and the author is a contributor to the current draft publication.

17799 Applied in SANS practical assignments:

4. Alan Mercer, Avaya INDeX PBX Security Audit: An Auditor's Perspective http://www.giac.org/practical/GSNA/Alan_Mercer_GSNA.pdf, Jan 24, 2004 GSNA Practical Assignment Version 2.1, Option 1

Floppy Firewall references:

5. http://www.samag.com/documents/s=1155/sam0101i/0101i.htm

Firewalls and Firewall Auditing in general:

6. Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman; Building Internet Firewalls, 2nd Edition, O'Reilly & Associates, Inc 2000. (723-741)
7. Sean Closson, A Review Of Floppy-Based Firewalls And Their Security Considerations, GSEC Practical 2002 http://www.sans.org/rr/papers/index.php?id=808,

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

8. Lance Spitzner, Auditing Your Firewall Setup ,12 December, 2000 http://www.spitzner.net/audit.html,
9. Lance Spitzner, Building Your Firewall Rulebase, http://www.spitzner.net/rules.html 12 December, 2000
10. Bennett Todd, Auditing Firewalls: A Practical Guide, 1998.http://www.itsecurity.com/papers/p5.htm,
11 Oskar Andreasson, IPTables Tutorial, 2001-2003 http://iptables-tutorial.frozentux.net

General Auditing Information

12 Lance Spitzner, Armoring Linux, 19 September, 2000. http://www.spitzner.net/linux.html
13. SANS, Linux Auditing Checklist http://www.sans.org/score/checklists/AuditingLinux.doc
14. Bob Toxen, Real World Linux® Security: Intrusion Prevention, Detection, and Recovery, Second Edition
15. Jay Beale, How do I Tighten Security My System?, 2000. http://www.bastille-linux.org/jay/how-do-I-tighten.html
16. Jay Beal, Shredding Access in the Name of Security: Set UID Audits, 2000. http://www.bastille-linux.org/jay/suid-audit.html
17. Jay Beal, Anyone with a screwdriver can break in, 2000. http://www.bastille-linux.org/jay/anyone-with-a-screwdriver.html
18. Steven Sipes, Why your switched network isn't secure, September 10, 2000. http://www.sans.org/resources/idfaq/switched_network.php
19. Northcutt, Zeltser, Winters, Frederick, Ritche. “Inside Network Perimeter Security”, New Riders, 2003.
20. Robert Graham, Sniffing FAQ, September 14, 2000. http://www.robertgraham.com/pubs/sniffing-faq.html

Addendum

Below is an item that is added as contribution to furthering ISO 17799 styled audits, and is going to be employed as an aspect of remediation for GES

GES ISO 17799 Auditor Portal

Below are screen shots of a web based ISO 17799 tool for implementing 17799 based audits that the auditor put together for use by GES. It is provided as an example of the sorts of items that might help an organization implement ISO 17799 with less pain. The tool consists of a GANTT charting tool for planning for a 17799 style audit, as well as a procedure creation and revision control tool for online ISO based documentation. Likewise, there is a searchable knowledge base for information only articles that would fall outside of ISO related audit for document control, but useful for ongoing security knowledge tracking. This tool will be made freely available via the OWASP web site www.owasp.org, as a part of their 17799 web security project.

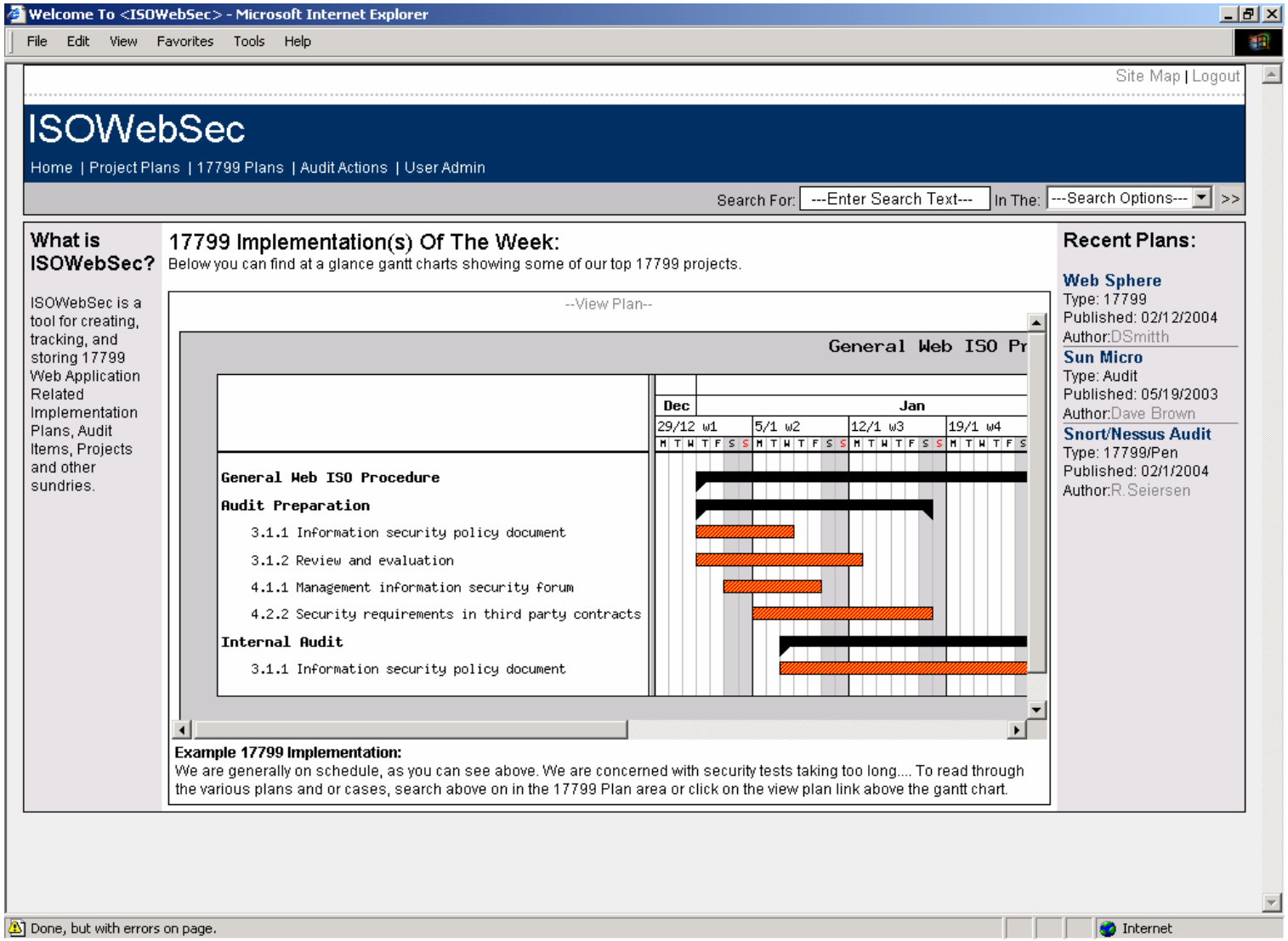
*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Page 1: Portal page, access to all tools, and marketing for recent audits and such. For example, see the left hand audits of various software components.

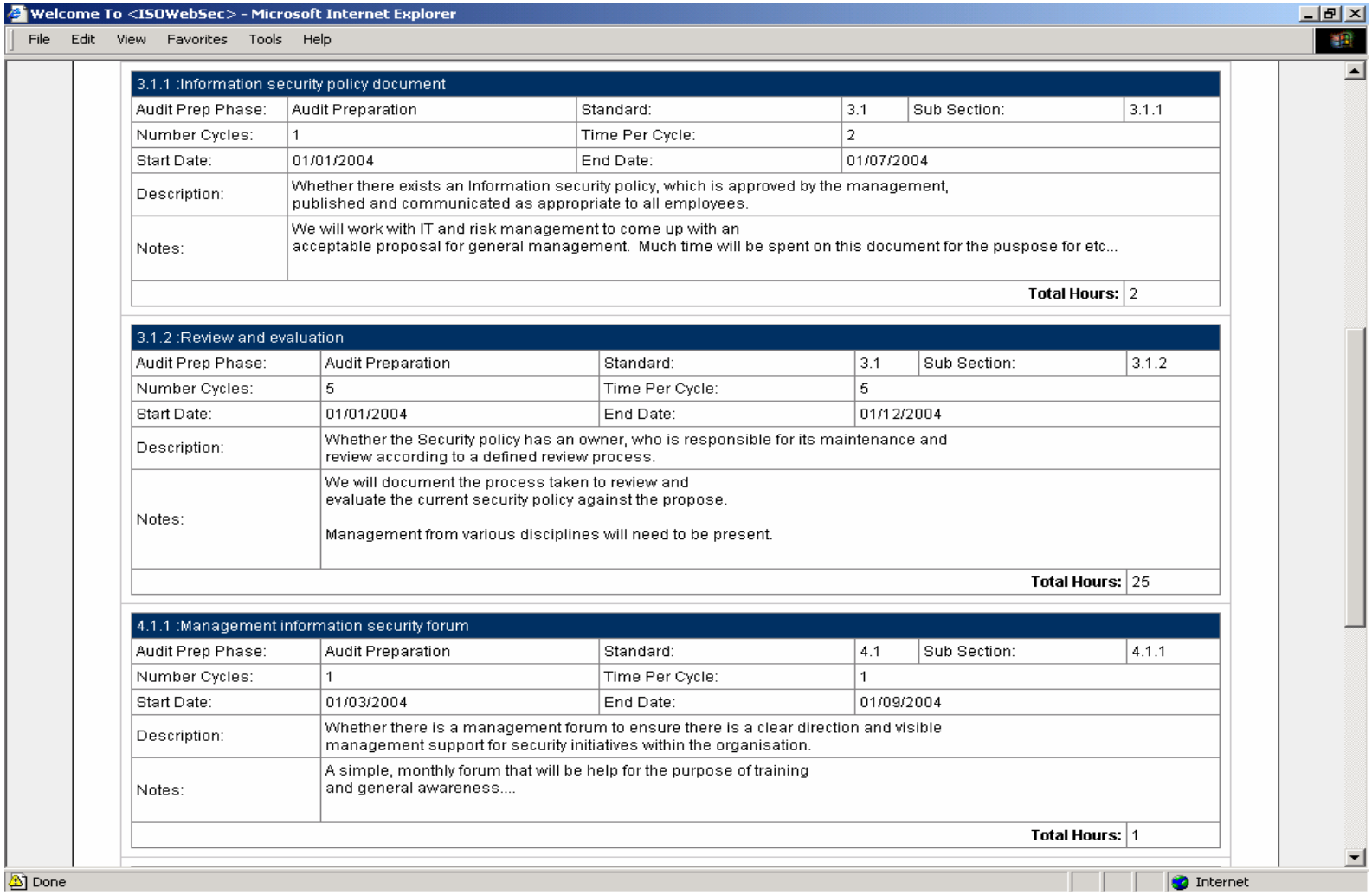
Page 2: Project management page, used for creating and documenting projects. All projects turn out dynamically generated web-based GANTT charts.

Page 3: Documents control page, used for creating procedures. The procedures creation tool includes revision control, which is a critical part of any ISO related documentation effort. Also includes checklists and information only docs.

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*



*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*



Welcome To <ISOWebSec> - Microsoft Internet Explorer

File Edit View Favorites Tools Help

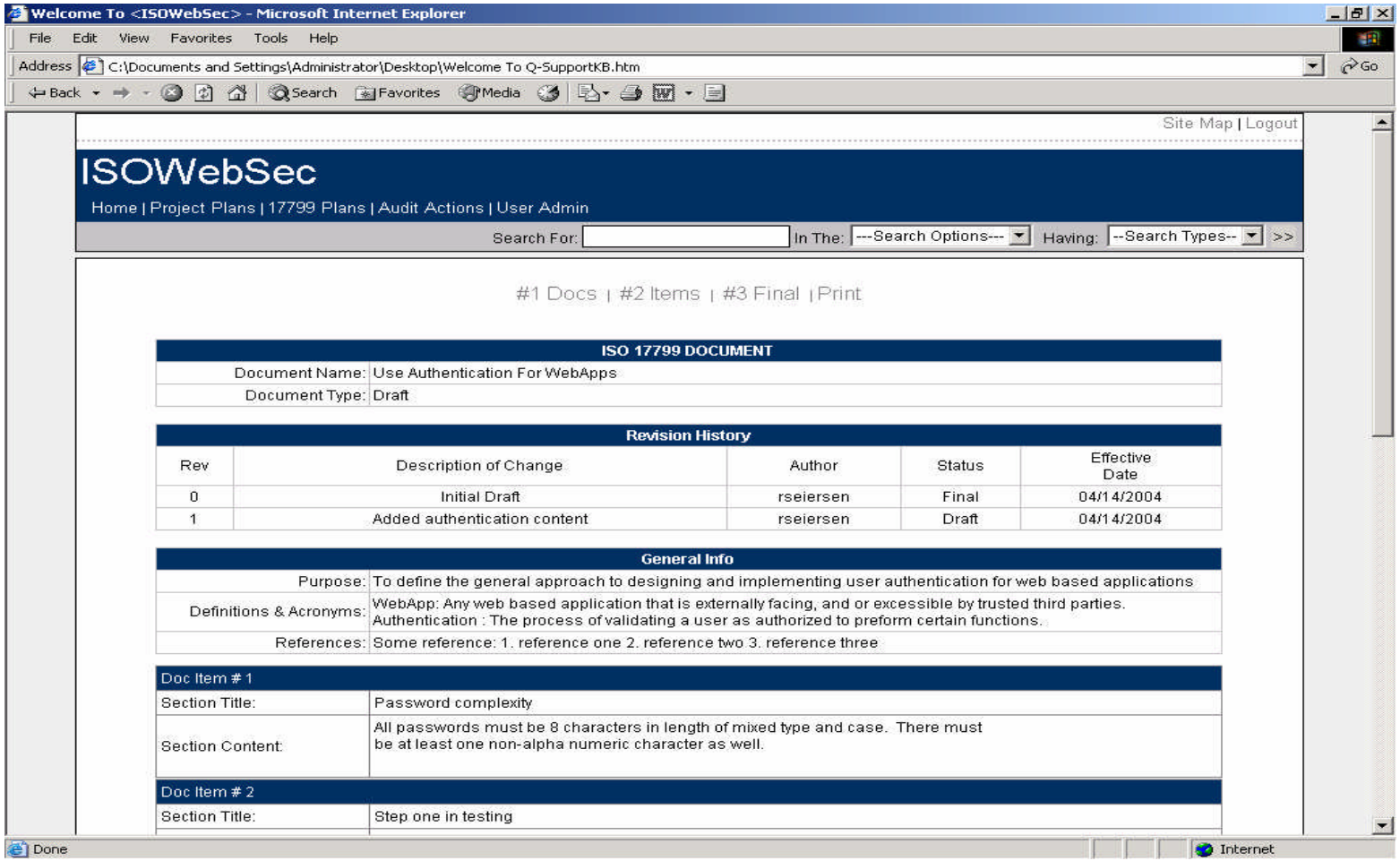
3.1.1 :Information security policy document					
Audit Prep Phase:	Audit Preparation	Standard:	3.1	Sub Section:	3.1.1
Number Cycles:	1	Time Per Cycle:	2		
Start Date:	01/01/2004	End Date:	01/07/2004		
Description:	Whether there exists an Information security policy, which is approved by the management, published and communicated as appropriate to all employees.				
Notes:	We will work with IT and risk management to come up with an acceptable proposal for general management. Much time will be spent on this document for the puspose for etc...				
				Total Hours:	2

3.1.2 :Review and evaluation					
Audit Prep Phase:	Audit Preparation	Standard:	3.1	Sub Section:	3.1.2
Number Cycles:	5	Time Per Cycle:	5		
Start Date:	01/01/2004	End Date:	01/12/2004		
Description:	Whether the Security policy has an owner, who is responsible for its maintenance and review according to a defined review process.				
Notes:	We will document the process taken to review and evaluate the current security policy against the propose. Management from various disciplines will need to be present.				
				Total Hours:	25

4.1.1 :Management information security forum					
Audit Prep Phase:	Audit Preparation	Standard:	4.1	Sub Section:	4.1.1
Number Cycles:	1	Time Per Cycle:	1		
Start Date:	01/03/2004	End Date:	01/09/2004		
Description:	Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organisation.				
Notes:	A simple, monthly forum that will be help for the purpose of training and general awareness....				
				Total Hours:	1

Done Internet

*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*



*GES is a wholly owned subsidiary *of GIAC Fortune Cookies*

Last Updated: July 22nd, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**