



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Auditing a Samba server from an administrator's perspective

Abstract

This paper describes the audit of a Samba server in a small office environment. This audit was performed by one of the administrators rather than by an independent auditor.

As part of the auditing process, the administrator documented the server and its environment, identified the company's information assets and performed a risk analysis.

Following on the risk analysis, the auditor researched and documented current practice before developing an audit checklist.

After performing the audit, the administrator reported his findings and recommended remedial actions.

Table of Content

1	DESCRIPTION OF SYSTEM AND ENVIRONMENT	3
1.1	DESCRIPTION OF COMPANY	3
1.2	DESCRIPTION OF NETWORK	3
1.3	DESCRIPTION OF SAMBA SERVER	4
2	RISK ASSESSMENT	5
2.1	GENERAL DISCUSSION OF INFORMATION ASSETS	5
2.2	THREATS, VULNERABILITIES, EXPOSURE AND RISK	6
2.3	RISK TABLE	9
3	CURRENT PRACTICE	12
3.1	POLICIES AND PROCEDURES	12
3.2	PHYSICAL SECURITY	12
3.3	BACKUPS	13
3.4	SOFTWARE PATCH/UPGRADE MANAGEMENT	13
3.5	ANTI-VIRUS SOLUTIONS	14
3.6	OPERATING SYSTEM HARDENING	14
3.7	AUDITING	15
4	AUDIT CHECKLIST	17
4.1	AUDIT STEPS	17
5	AUDIT	38
5.1	AUDIT CHECKLIST	38
5.2	ANALYSIS OF RESIDUAL RISK	57
5.3	ANALYSIS OF SYSTEM'S "AUDITABILITY"	58
6	RISK ASSESSMENT	59
6.1	SUMMARY	59
6.2	RISKS	59
6.3	SYSTEM CHANGES AND FURTHER TESTING	61
6.4	SYSTEM JUSTIFICATION	63
7	REFERENCES	64

Assignment 1

1 Description of system and environment

Samba is the bridge between the world of Microsoft Windows and the world of Linux/Unix; by all accounts it is one of the most often deployed open-source technologies. This paper will describe the audit of a Samba server running in a small company. The company details are fictitious but the environment described is a composite of a number of real environments.

1.1 Description of company

Fictitious Consultants is a small consultancy in a mid-size city. The company formed six months ago when four independent consultants decided to pool their resources and incorporate as a LLC. Aside from the consultants, the company has one additional employee who handles most of the administrative work for the company.

The majority of the company's work consists of IT project management work for local customers. This work has expanded into training and IT strategic consultancy. They have given themselves one year to see if they are more successful as a small partnership with an administrative assistant than as four individuals.

Fictitious operates out one floor in a 2 story building in a small business park, the building houses a number of different tenants. The office contains a reception area, which also houses the administrative assistant's desk, her desktop computer and the company's shared multifunction printer. There is a large room with four desks where the four consultants sit, as well as another large room used for meetings and training. The office also has a kitchen and a small "communications" closet containing an ADSL router, a patch panel, an Ethernet switch and a telephone switch.

1.2 Description of network

Fictitious Consultants operates a small network, using the cabling, network ports and the patch panel built into the office. There are eight ports in the conference room, eight ports in the office shared by the consultants and four ports in the reception area. At the moment, four ports from the office and two ports from the reception area are connected to the switch. One switch port is connected to the ADSL router and the rest is unused.

All the consultants have laptops that they connect to the network using standard Ethernet cables (RJ45 CAT5) running to the desks. The laptops are running Windows XP professional, are configured to use DHCP and are running personal firewalls. The DHCP server is configured to give specific addresses to each of the laptops.

The administrator's workstation runs Windows XP professional and is connected to the network by Ethernet cable. The workstation uses a static IP address that is reserved in the DHCP server.

The ADSL router connecting the network to the Internet has basic NAT and firewall capabilities and also serves as the DHCP server for the network. The router is owned and managed by Fictitious. The router's configuration is controlled by a management GUI (Graphical User Interface) only accessible from the local/internal network by using a web browser.

Fictitious has registered a domain name through their ISP and use the ISP to host a small static web site. The ISP provides Fictitious with POP3 accounts that are accessible over SSL as well as a SMTP server for outgoing mail.

1.3 Description of Samba server

The server is an spare desktop that belonged to one of the partners. Fictitious purchased and installed Red Hat 9.0 Professional Edition on the server. During install, Fictitious selected a server class install, using the default GRUB boot loader with a password. Fictitious also chose the "high" security setting for the firewall, but customized access to allow ssh (tcp/22), smb (tcp/139, udp/138) and nmb (tcp/137, udp/137). Fictitious also customized the packages to only install Samba. The version of Samba currently running on the system is 2.2.7a.

The server is configured as a domain controller for the "Fictitious" domain. Each laptop and the administrative desktop have accounts in the domain, each user has a Samba account authenticating on the domain. The Samba users do not have access to interactive shell (using /sbin/nologin). Two have Linux "admin" accounts to manage the server (root is blocked from logging in through ssh forcing the use of su).

The server provides each user with a personal share and allows all the consultants to store and retrieve documents in a common shared directory. In order to do this, the server does not use a [homes] share to automatically map users to shares; each user has a share mapping to their Linux home directory defined in the Samba configuration. The server does not use roaming profiles or logon scripts.

The server is located in the reception area behind the administrator's desk.

Originally all the shared files were stored on the office assistant's workstation, but as this workstation is also used to share a multifunction printer for the office, there were some performance issues. Curiosity was another key driver for implementing the Samba server; the consultants wanted to learn more about Linux and determined that running a Linux server in their office would be the perfect way to gain some insight.

2 Risk assessment

2.1 General discussion of information assets

The consultancy's main information assets are its employees, customer information, past & current project documents, internal documentation and internal records. Considering the scope of this audit, the employees were not included in the review of information assets.

Considering the size of the business, Fictitious decided to use a qualitative (High, Medium, Low) scale to classify and value their information assets.

2.1.1 Customer information

All current customers' corporate details are stored in a Microsoft Access database. The database resides on the Samba server in the shared folder.

Each consultant keeps customer contact information in Microsoft Outlook on their laptops; the consultants copy this data (.pst) to their personal folders as a backup.

Losing the customer information would impact the firm, but Fictitious only perceives it as a medium value asset. All of the consultants have long-established relationships with their customers and do not need to refer to the information in the database on a daily basis.

The customer information in the database is not confidential; this confirms the asset classification.

2.1.2 Project documentation

Each project Fictitious manages has a set of documents associated with it. These project documents are stored on the shared folder on the Samba server. The consultants also keep local copies on their individual laptops.

The loss of current project documentation would seriously impact the firm. In the great majority of cases, these documents are required for the projects and some take weeks of effort to assemble. Without them, days or even weeks of work could be lost.

Furthermore, in most cases, the documents are the deliverables purchased by their customers; without the documents, Fictitious cannot get paid. The value of this data is high, critical to the business.

The classification of the project documentation is confirmed by the fact that most of it is confidential data and is covered by Non-Disclosure Agreements (NDA) between Fictitious and its customers.

2.1.3 Internal documentation (know-how & best practices)

Over the years, each of the four consultants has accumulated knowledge and developed unique methodologies, techniques and document templates. When they established the partnership, the Fictitious partners spent time reviewing this know-how and documenting it. These documents are stored on the Samba server in the shared folder.

Fictitious valued these internal documents as medium. The consultants understand that while the knowledge captured in these documents is essential to their business, it is actually spread across the four consultants. Losing the documentation would not have an immediate impact on any given project.

2.1.4 Internal documentation (training curriculum)

In parallel with the work the consultants did to capture their know-how, they developed a training curriculum. This training curriculum is proprietary and is expected to generate new business for Fictitious.

Considering its revenue-generating potential, the training curriculum was valued as high.

2.1.5 Internal records

Fictitious has a number of internal records (e.g. financial record and legal documents). All of the hard-copies of the company's internal records are kept in the office in a fire-resistant file cabinet, but some of Fictitious's internal records are stored on the Samba server.

Based on the recommendations from an external accountant, Fictitious purchased a small business accounting package. This software package has been installed on the administrative workstation. The package has an automatic back-up function which stores a copy of the data on the shared folder on the Samba server. The paper documents generated by the accounting software (e.g. invoicing, expenses, cheques, payroll) are stored in the fire-resistant cabinet.

Once of Fictitious's main concern is to keep this data confidential; they do not want their customers to see other customer's contractual terms.

The value of the internal records is high. Note that Fictitious could have given more granular value to these assets, but settled for a rating that reflected the highest classification.

2.2 Threats, Vulnerabilities, Exposure and Risk

The Fictitious consultants also used a qualitative approach to determine the level of risk facing their information assets. The analysis consisted of identifying threats and vulnerabilities and then evaluating the exposure of their assets to given combinations of threats and vulnerability.

The consultants used a brainstorming session to identify the threats, vulnerabilities and exposure (when & how often). Following on the brainstorming session, they formalized their analysis, assigned qualitative ratings and captured the results of the analysis in a table. Note the brainstorm led the consultants to think in terms of threats first (see below), but the data in the Risk table is classified by risk to better identify control & audit requirements.

2.2.1 Hardware failure

Fictitious identified hardware failure as the biggest risk to the Samba server and the information residing on it. The specific threats were identified as power supply failure, electricity quality issues, and hard disk failure, both statistically common enough to have been experienced by a couple of the consultants.

These threats combined with the vulnerability of using a consumer desktop system with consumer desktop components, the lack of component redundancy, and the ad-hoc backup strategy (see 3.3) confirmed this as the highest risk to the business.

2.2.2 User error

Once again using previous experience, Fictitious identified user error as the second highest risk to their data. The main anticipated threats from user error were: overwriting a newer document with an older document, deleting a document by mistake, misconfiguring access rights on Samba, and misconfiguring network access restriction to the Samba server.

The identified vulnerabilities in this area were a lack of Linux/Samba knowledge, a lack of a document management system, and a lack of consistent backups (see 3.3). Fictitious identified user error as a high risk.

2.2.3 Software bug/malfunction

Fictitious identified software bugs as a risk to their data. Potential threats identified were bugs in OS (virtual memory management, ext3 filesystem), bugs in the Samba access control, buffer overflows in services (Samba, ssh) and incompatibilities between Microsoft & Samba versions of protocols.

The main vulnerability is, of course, the frequency of vulnerabilities discovered in widely deployed software. But since patches and upgrades can introduce bugs, the lack of a test platform was also considered vulnerability. Fictitious identified software bugs as a low risk.

2.2.4 Virus infection

Fictitious determined that they could expect to be infected by a virus once a year, but that damage would be limited by the anti-virus software deployed on all the Windows XP machines.

The threat of a new virus (unknown to their AV software) or a cross-platform virus that could infect the Samba server was considered remote. Yet these

remote threats combined with the more likely threat of common known windows viruses, the vulnerabilities stemming from old signature files on one of the Windows machine, the lack of anti-virus software on the Samba server(see 3.5) and the ad-hoc backups (see 3.3) still combined to present a medium risk to Fictitious.

2.2.5 Malicious insider on network

Fictitious, for the purpose of the risk assessment, defined insiders as anyone or any machine on their internal network. While they trusted themselves, the Fictitious consultants determined that one of their customers might try to get information while connected to their network.

Fictitious identified the following specific threats: IP spoofing, brute force password attack, network sniffing. The threat was corroborated by some of their customers admitting that they had read document that were “available” on 3rd party networks.

The vulnerability of a single, flat, accessible network, the lack of tools to monitor network activity, the use of NTLM and social engineering were all identified. The vulnerabilities were partly mitigated by the use of the switch and arpswatch. The risk from a malicious insider getting access to data was evaluated as medium (N.B. the specific risk of sniffing was rated as low).

2.2.6 Malicious outsider

Fictitious identified malicious outsider attacks low risk. The threats of a malicious outsider taking over the DLS router, sending a Trojan horse through email, or saturating Fictitious's LAN were all identified, but the vulnerabilities associated with these attack were mitigated by current firmware on the router, anti-virus software. The risk of a network-based attack by a malicious outsider affecting the Samba was evaluated as low.

2.2.7 Hardware damage/theft

Fictitious identified accidental damage and theft as risks to the server. The server's vulnerable location (see 3.2) increases the risk. The scenarios considered included coffee spills, storms, fires, theft of the hard drive and theft of the whole server. Considering the general environment (see 3.2), the consultants evaluated the risk as medium.

© SANS Institute

2.3 Risk Table

ID	Risk	Vulnerabilities	Threats	Exposure	Asset at risk	Risk Rating
I	Hardware failure makes data unavailable	Non-redundant hardware, ad-hoc backups	Disk failure, power supply failure, power surge	Permanent & high	Customer Information Project Documentation Internal Documentation Training Curriculum Internal Record (backup)	High
II	Physical destruction or removal of hardware make data permanently unavailable	Exposed location of Samba server, ad-hoc backups	Theft, accidental damage	Permanent & medium, mitigated by presence of Administrative assistant during working hours & building security	Customer Information Project Documentation Internal Documentation Training Curriculum Internal Record (backup)	Medium
III	Unauthorised user leverages physical access to access/modify/destroy data	Exposed location of Samba server	Theft of drive, boot to alternate OS, BIOS crack	Permanent & medium, mitigated by presence of Administrative assistant during working hours & building security	Customer Information Project Documentation Internal Documentation Training Curriculum Internal Record (backup)	Medium
IV	User error exposes data to unauthorized internal users	Lack of experience with Linux & Samba (user error)	Mis-configuration of Samba or firewall giving access to un-authorized party	Permanent & high but decreasing. As the consultants gain experience, the chances of errors decrease	Customer Information Project Documentation Internal Documentation Training Curriculum Internal Record (backup)	High

ID	Risk	Vulnerabilities	Threats	Exposure	Asset at risk	Risk Rating
V	User error makes data unavailable to authorized internal users	Lack of experience with Linux & Samba (user error)	Mis-configuration of samba or firewall, accidental deletion of files on Samba server	Permanent & high but decreasing. As the consultants gain experience, the chances of errors decrease	Customer Information Project Documentation Internal Documentation Training Curriculum Internal Record (backup)	High
VI	Software bug affects confidentiality, integrity or availability of data	Bug in software	Normal use causes bug to manifest itself.	Medium & Intermittent. Critical software bugs are not common and require specific conditions.	Customer Information Project Documentation Internal Documentation Training Curriculum Internal Record (backup)	Medium
VII	Software patch or upgrade corrupts data or makes it unavailable	Lack of test platform, ad-hoc backups	Bad/incompatible patch or update	Low (few patches to apply and even fewer bad patches)	Customer Information Project Documentation Internal Documentation Training Curriculum Internal Record (backup)	Low
VIII	Malicious agent uses vulnerability in exposed service to access/modify/destroy data	Exposed services (Samba, ssh), ad-hoc backups, lack of real-time monitoring, ad-hoc backups, flat network	New exploit + attack from malicious insider or cross-platform worm spreading through Win XP	Low (critical bug in Samba & ssh are well advertised and patched quickly + services accessible only from a limited set of IP addresses)	Customer Information Project Documentation Internal Documentation Training Curriculum Internal Record (backup)	Low

ID	Risk	Vulnerabilities	Threats	Exposure	Asset at risk	Risk Rating
IX	Virus or worm spreads to Samba server corrupting data or making it temporarily or permanently unavailable	Old signature on Win XP Laptop/desktop allowing worm/virus to spread to Samba server, ad-hoc backups	New virus or worm, old virus or worm	Medium (new malware appears every day but current policy is to update virus signatures once a week)	Customer Information Project Documentation Internal Documentation Training Curriculum Internal Record (backup)	Medium
X	Unauthorised user bypasses network protection to access/modify/destroy data	Single flat network, social engineering (for username & passwords), no real-time alerting mechanism	Malicious insider spoofing IP to get access or launch further attack (brute force/dictionary attacks against passwords, exploits against services)	Medium (trivial to spoof IP limited to period when guests are present on network). Could increase in future with increase in training courses.	Customer Information Project Documentation Internal Documentation Training Curriculum Internal Record (backup)	Medium
XI	Unauthorised user uses networks sniffing tools to access/modify/destroy data	Single flat network, NTLM version	Malicious insider sniffing data and passwords hashes	Low (Presence of the switch make sniffing difficult, but not impossible. Limited to period when guests present on the network). Could increase in future	Customer Information Project Documentation Internal Documentation Training Curriculum Internal Record (backup)	Low

3 Current practice

As part of the risk assessment, Fictitious researched best practices for management and auditing of the Samba server. They documented their current practices and benchmarked them against best practices.

Fictitious did not find any specific Samba security checklist or auditing guideline, but was able to use general Linux documentation & checklists that covered Samba as a base for their auditing checklist.

Two useful tools that came out of Fictitious's research are the Center for Internet Security's (CIS) Linux benchmarking tool and Bastille Linux. The CIS tool is a general linux benchmark that is simple to run and gives a detailed report as well as a score (www.cisecurity.org). Bastille Linux is a set of scripts that simplifies the secure configuration of a Linux server (www.bastille-linux.org).

3.1 Policies and Procedures

Fictitious has implemented a formal security policy. The policy was drafted using the information gathered during the risk assessment (see section 2).

Policy plays three major roles. First it makes clear what is being protected and why. Second, it clearly states the responsibility for that protection. Third, it provides a ground on which to interpret and resolve any later conflicts that might arise. [Garfinkel & Spafford 1996 p.35]

Fictitious's policy makes each individual responsible for his or her own data as well as the company's data (e.g updating anti-virus at least once a week and backing up shared data according to rota, being vigilant about social engineering).

3.2 Physical security

Fictitious used chapter 12 of [Garfinkel & Spafford 1996] to review the physical security of the server. The external security was in line with current accepted practices.

Fictitious's offices are on the first floor of the building, the door to the office is a solid wood door with two locks. Access to the stairs is secured by a door on the ground floor which can be opened by an electronic pass or from inside the building through an intercom. The intercom has a built-in camera. The building has four offices which share the ground floor door and stairwell. The landlord has contracted a private security company for the security of the building. The building has a sprinkler system, smoke detectors and fire alarms.

Prior to moving in, Fictitious contacted the occupiers of the other offices to get their opinion on the building and landlord, they also inquired about crime in

the area. None of the other occupiers of the building reported ever having any problems.

Within the office, the physical protection of the server was below accepted practice.

Simple common sense will tell you to keep your computer in a locked room. [Garfinkel & Spafford 1996 p. 369]

None of the key components of the server are resilient, it is easily accessible (including keyboard/screen, drives, ports and power/reset switch), and it is plugged straight into the wall socket. Network ports are also easily accessible once inside the office.

Fictitious believed that the size of their office and the lack of traffic mitigated the lack of internal physical security, but still acknowledged that the lack of physical security contributed to their highest risk (Hardware failure 2.2.1)

3.3 Backups

For backups, Fictitious used chapter 7 of [Garfinkel & Spafford] as a guideline and found itself far from implementing accepted best practices.

Fictitious has not implemented any traditional backup solutions (i.e. tape), but it has a manual process. Once a week, following a set rotation, one of the consultants uses their laptop's CD burner to backup the shared folder to 2 CD-Rs. The consultant then puts one of the CD-Rs in the fire resistant cabinet and takes the other one home. Data might be backed-up more frequently on an ad-hoc basis.

This method is not a reliable and efficient method of backing up the data on the Samba server. It does not offer any mean to restore the operating system and could lead Fictitious to lose a week's worth of data.

The Samba server itself is a repository for backups, the shared folder contains the backup of the accounting software data and the employees use their personal shares on the Samba server quasi-exclusively for backups (once again a manual ad-hoc process).

The lack of appropriate backups greatly increases the risk to Fictitious's data by making it more vulnerable. During risk analysis, the current backup strategy increased the risk rating of almost every risk scenario.

3.4 Software patch/upgrade management

Patch management is one the most important operational issues in IT and current practice is evolving rapidly. A variety of vendor solutions have emerged in the past few years, but none has yet emerged as a clear winner.

There is no centralized patch management at Fictitious. The individual windows machines are configured to use Windows Update.

For the Samba server, Red Hat updates and patches are packaged as RPMs, a format that is relatively easy to manage but:

One other critical issue is that there really isn't a good way to "back out" a patch if something goes wrong. [Pomeranz 2002:1-10]

To get around this issue and keep track of required patches, Fictitious is relying on the Red Hat Network (RHN) and up2date tool.

Red Hat Network is an Internet solution for managing a Red Hat Linux system or a network of Red Hat Linux systems. All Security Alerts, Bug Fix Alerts, and Enhancement Alerts (collectively known as Errata Alerts) can be downloaded directly from Red Hat. [Red Hat 2001-2003]

The Red Hat Network solution allows Fictitious to easily determine which patches and update are relevant to their system and the up2date tool has an undo option that allow patches to be rolled back.

Although Fictitious is using largely accepted solutions, the lack of a test platform still leaves an element of risk which was reflected in the rating.

3.5 Anti-virus solutions

Anti-virus in the Linux world is a relatively new development. A number of people still rely on safe computing practices and the fact that Linux has historically been less of a target. Most large anti-virus vendors now support Linux and some have products specifically tailored for Samba (e.g. Kaspersky, Bitdefender), but anti-virus on Linux still seems to be the exception rather than the rule.

Fictitious does not have a centralized anti-virus solution, but each individual Windows machines runs a commercial anti-virus with an automatic update feature. Fictitious's policy mandates that all employees must update their anti-virus signatures at least once a week.

The fact that the Samba server is not running anti-virus software makes Fictitious dependent on signature updates on each individual Windows machine and a single anti-virus vendor.

3.6 Operating system hardening

All of the references that Fictitious found mentioned server hardening in one way or another. After some research, and considering their lack of experience, Fictitious decided to use the Bastille Linux hardening scripts (<http://www.bastille-linux.org/>). Fictitious also relied on the SANS Security Essentials UNIX security Course book [Pomeranz 2002] and The Linux Security Cookbook [Barrett, Silverman and Byrnes 2003] as a source of best practices.

For specific Samba information, Fictitious relied on the “Doing the Samba” chapter of Real World Linux Security [Toxen 2001. 4.8].

3.6.1 Console access

As mentioned in the physical security section, the Samba server is easily accessible, Fictitious has taken some steps to mitigate this vulnerability by implementing BIOS and boot loader protection.

```
Password protection for the BIOS and the boot loader can
prevent unauthorized users who have physical access to
your systems from booting from removable media or
attaining root through single user mode. [Red Hat 2002a]
```

There are tools that can bypass BIOS and boot loader passwords, but their use requires time and effort.

3.6.2 Network access

With the help of the Bastille Linux script, Fictitious minimized the network services running on the server. Fictitious also implemented a firewall on the Samba server. Fictitious uses their router as a DHCP server, but all of the laptops and the administrator's workstation have their IP Addresses reserved by MAC address. This configuration should prevent guest on the network from accessing the Samba server.

Another key part of network access is to limit the use of clear-text or weakly encrypted password across the network.

The only network service available on the server aside from Samba is ssh.

3.6.3 Accounts & passwords

For accounts and password, current practice focuses on enforcing strong passwords as well as controlling and limiting the use of the root account. The configuration of PAM (Pluggable Authentication Manager) on Red Hat 9 enforces basic password strength. The Bastille Linux script helped to limit the ability to log in with the root account to the console.

3.7 Auditing

Fictitious based its auditing approach on accepted practice for the auditing of Linux Servers and added some auditing steps to deal specifically with Samba.

The general UNIX auditing references that Fictitious used were: SANS Institute Track 7 – Auditing Networks, Perimeters and Systems. 7.6 Advanced Systems Audit UNIX Course book [Green J. and Hoelzer D. 2003] and The Linux Security Cookbook [Barrett, Silverman and Byrnes 2003].

For specific Samba information, Fictitious relied on the “Doing the Samba” chapter of Real World Linux Security [Toxen 2001. 4.8].

Fictitious used the documentation section of the Red Hat website for Red Hat specific information.

Fictitious also used William Karwisch's Auditing a Corporate E-mail Gateway Running Postfix on Linux: an Administrator's Perspective [Karwisch 2003] as a template and source of ideas.

3.7.1 Auditing patches

For Red Hat systems, the current state of practice is simple: the system used for patch management can also be used for auditing patches. The up2date application, combined with the Red Hat Network and the rpm package management system can verify the patch level of a system.

3.7.2 System file integrity

The current practice to verify file integrity across most platforms is the use of the Tripwire application. Every Linux auditing reference mentions Tripwire and gives some details on how to use it. Fictitious has implemented Tripwire and tuned the policy.

3.7.3 Logging

Reviewing systems log is another standard practice. Most references highlight the need for tools to make the task easier. Red Hat comes pre-configured with the Logwatch tool.

3.7.4 Network scans

External network scans are the accepted practice to verify the presence and configuration of network services. Network scans also validate filtering (e.g. firewalls, tcpwrapper). The standard tools for network port audits are nmap and nessus.

3.7.5 Manual configurations checks

All of the above auditing checks are standard and applicable to all Linux machines. Fictitious used specific Samba references to create audit checks. Most of these Samba-specific checks are centred on the smb.conf file:

```
Because /etc/smb.conf is such a powerful tool for
configuring Samba, there are several parameters that are
very powerful. Each will be discussed in turn, including
discussion on why it is important, and how it could be
used to compromise security. [Toxen 2001, Chapter 4
Section 8.4]
```

Assignment 2

4 Audit Checklist

Following the risk assessment, Fictitious developed an audit checklist for the Samba server. The following details the checklist items.

Note that each audit item includes a full reference and that a complete list of references can be found at the end of this paper.

Note that commands that have to be typed verbatim at a command prompt are listed in courier font with additional elements in bold square brackets:

```
ls -l [home directory of user]
```

4.1 Audit Steps

AUDIT STEP	1 – Physical security
Reference	Garfinkel S. and Spafford G. 1996. <u>Practical Unix & Internet Security, 2nd Edition</u> . Chapter 12 Physical security. O'Reilly & Associates, Sebastopol, CA.
Risk	I - Hardware failure makes data unavailable II - Physical destruction or removal of hardware make data permanently unavailable III - Unauthorised user leverages physical access to access/modify/destroy data
Control Objective	Given that someone with physical access to the server and enough time will be able to access data on the server, it is important to limit access.
Testing Procedure	1. Evaluate using either interview or observation if a malicious insider could gain physical access to the server 2. If answer to above is yes estimate if a malicious outside could gain access for a period long enough to do arm
Compliance Criteria	The server is compliant if there is no window of opportunity for a malicious insider.
Test Type	Subjective.
Evidence	
Findings	

AUDIT STEP	2 – Verify BIOS and boot loader configurations
Reference	Red Hat. 2002a. <u>Red Hat Linux 9 Red Hat Security Guide. 4.2. BIOS and Boot Loader Security.</u> http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-wstation-boot-sec.html Last Accessed: 26 January 2004
Risk	III – Unauthorised user leverages physical access to access/modify/destroy data
Control Objective	Insure that it is not possible to bypass server OS protection features by booting the server to an alternative OS.
Testing Procedure	<ol style="list-style-type: none"> 1. Try to boot from a boot floppy (DOS 6.22) and a boot CD (FIRE) 2. Boot server 3. Try to access the setup/BIOS menu and change the boot priority (pressing F2 and navigating menu) 4. Reboot server 5. When server displays boot loader menu, try to use the GRUB command line (press c while grub menu is displayed)
Compliance Criteria	If the system can be booted to an alternative OS by using either boot media in the drives, changing the BIOS or using the boot loader, the system is non compliant.
Test Type	Objective. Stimulus-Response
Evidence	
Findings	

© SANS Institute 2004, Author retains full rights.

AUDIT STEP	3 – Verify Samba version and check for published vulnerabilities
Reference	<p>Pomeranz H. 2002. <u>SANS Institute Track 1 – SANS Security Essentials + CISSP CBK. 1.6</u> <u>SANS Security Essentials IV: UNIX Security v 1.4.</u> pp. 1-8, 1-7. SANS Institute.</p> <p>Personal experience</p>
Risk	<p>VI - Software bug affects confidentiality, integrity or availability of data VIII - Malicious agent uses vulnerability in exposed service to access/modify/destroy data</p>
Control Objective	Check that there are no published vulnerabilities/bugs for the Samba version that is currently running on the server.
Testing Procedure	<ol style="list-style-type: none"> 1. Log in to the Samba server & su to root 2. Check the location of the 2 Samba daemons <pre>which smbd which nmbd</pre> 3. Verify the version of Samba running on the server by logging on and typing the following commands: <pre>[path from output above] smbd -V [path from output above] nmbd -V</pre> 4. Search for reports of Samba vulnerabilities for this specific version in the following web locations: <p> http://www.cert.org/ http://www.samba.org/ http://www.securityfocus.com/ https://rhn.redhat.com/ (log in and check the profile of the server) </p>
Compliance Criteria	The compliance is subjective and will depend not only on the existence of vulnerabilities, but also on their relevance to the deployed system and on their severity.
Test Type	Subjective.
Evidence	
Findings	

AUDIT STEP	4 – Verify Tripwire configuration and run Tripwire
Reference	Barrett D J., Silverman R. E. and Byrnes R. 2003. <u>Linux Security Cookbook</u> , Chapter 1 Taking Snapshot with Tripwire. O'Reilly & Associates, Sebastopol, CA.
Risk	V - User error exposes data to unauthorized internal users VIII - Malicious agent uses vulnerability in exposed service to access/modify/destroy data. IX - Virus or worm spreads to samba server corrupting data or making it temporarily or permanently unavailable. X - Unauthorised user bypasses network protection to access/modify/destroy data
Control Objective	Verify that core binaries and configuration files have not been modified maliciously or accidentally. N.B. This control does not prevent any of the threats, but allows detection.
Testing Procedure	<ol style="list-style-type: none"> 1. Insure that you know Tripwire pass-phrase 2. Log in to server & su to root 3. Export the current tripwire policy file to plain text: <pre>cd /etc/triwire twadmin --print-polfile > twpol.txt</pre> 4. Search for key server components (/usr/sbin/smbd, /usr/sbin/nmbd, /etc/Samba/smb.conf, /etc/samba/smbusers) within the plain text policy file: <pre>grep smb twpol.txt grep nmb twpol.txt grep ssh twpol.txt</pre> 5. Verify that core files have not been modified by running a check: <pre>tripwire --check</pre> 6. Delete plain-text policy file: <pre>rm twpol.txt</pre>
Compliance Criteria	A key compliance point of this audit step is to verify that the core services binaries and supporting files have not been modified. But any discrepancy discovered by the Tripwire check should be investigated
Test Type	Subjective. The presence of the Samba configuration files is objective, but the analysis of any issue flagged by Tripwire is subjective.
Evidence	
Findings	

AUDIT STEP	5 – Verify RPM public keys
Reference	<p>Red Hat. 2003a.</p> <p><u>Red Hat Linux 9: Red Hat Linux Customization Guide. 32.3. Checking a Package's Signature.</u></p> <p><u>http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/s1-check-rpm-sig.html</u></p> <p>Last Accessed: 29 January 2004</p>
Risk	VII - Software patch or upgrade corrupts data or makes it unavailable
Control Objective	Insure that the system uses the correct public key to check the validity of rpm packages. This will prevent the installation of rogue packages.
Testing Procedure	<ol style="list-style-type: none"> 1. Log in to the server & su to root 2. Get Red Hat's public key signature from their web site (http://www.redhat.com/solutions/security/news/publickey.html) 3. Find the Red Hat public key in rpm: <pre>rpm -qa gpg-pubkey* [note exact name of key in output]</pre> 4. Export the key to a text file <pre>rpm -qi [exact name of key from above] > rh.key</pre> 5. Check the key with pgp by importing it (If the key already is in the key ring, pgp will indicate that the key has not changed). <pre>gpg --import rh.key</pre> 6. Use pgp to list the key's fingerprint and check the fingerprint against a good source (http://www.redhat.com/solutions/security/news/publickey.html) <pre>gpg -fingerprint</pre> 7. Delete text file <pre>rm rh.key</pre> 8. Check the signature of the key in the keyring used by up2date (N.B. the two lines bellow are a single line at the console): <pre>gpg --fingerprint --no-default-keyring --keyring /etc/sysconfig/rhn/up2date -keyring.gpg</pre>
Compliance Criteria	For the system to be compliant, both the fingerprint from the key found in rpm and the one used by up2date must match Red Hat's published key fingerprints.
Test Type	Objective.
Evidence Findings	

AUDIT STEP	6 – Verify Samba packages with rpm
Reference	Red Hat. 2003b. <u>Red Hat Linux 9: Red Hat Linux Customization Guide. 32.4. Impressing Your Friends with RPM.</u> http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/s1-rpm-impressing.html Last Accessed: 29 January 2004
Risk	VII - Software patch or upgrade corrupts data or makes it unavailable
Control Objectives	Verify that the elements of Samba installed on the server are the ones installed under rpm control.
Testing Procedure	1. Log in to the server & su to root 2. Use rpm to verify the Samba packages: rpm -V samba rpm -V samba-common
Compliance Criteria	For the system to be compliant, the verify commands should not return any modified files aside from: /etc/samba/smbusers /etc/samba/smb.conf
Test Type	Objective
Evidence	
Findings	

AUDIT STEP	7 – Verify that all relevant patches have been applied to the system
Reference	Red Hat. 2001-2003b. <u>Red Hat Network 2.8: Update Reference Guide. Chapter 2. Red Hat Update Agent</u> http://www.redhat.com/docs/manuals/RHNetwork/ref-guide/2.8/up2date-setup.html Last Accessed: 29 th January 2004
Risk	VI - Software bug affects confidentiality, integrity or availability of data VIII - Malicious agent uses vulnerability in exposed service to access/modify/destroy data
Control Objective	Check that there are no outstanding patches for the system.
Testing Procedure	1. Log in to the server & su to root 2. Use up2date to list available patches for yours system (N.B. you will need the root password) up2date -l
Compliance Criteria	The list of updates returned should not include any security update/errata for samba or ssh components. It might be necessary to read the description of certain updates such as libraries to determine if they have security implications for your system.
Test Type	Objective.
Evidence	
Findings	

AUDIT STEP	8 – Verify init levels and Samba startup scripts
Reference	Pomeranz H. 2002. <u>SANS Institute Track 1 – SANS Security Essentials + CISSP CBK. 1.6</u> <u>SANS Security Essentials IV: UNIX Security v 1.4.</u> pp. 2-19 to 2-24. SANS Institute.
Risk	IV - User error exposes data to unauthorized internal users V - User error makes data unavailable to authorized internal users
Control Objective	Check that the services required, and only the services required, are started automatically when the server boots up.
Testing Procedure	<ol style="list-style-type: none"> 1. Log in to the server & su to root 2. Check the default init level: <pre>grep initdefault /etc/inittab</pre> 3. List the service started at each run level <pre>chkconfig</pre> 4. Reboot server <pre>shutdown -r now</pre> 5. Log in 6. Check the services that are running <pre>ps -aux</pre>
Compliance Criteria	<p>The initdefault in inittab should be set to 3 and the following services should be set to start at initlevel 3:</p> <p>syslog, network, random, keytable, atd, sshd, crond, smb</p> <p>The ps command should return the following after boot (kernel omitted):</p> <pre> PID TTY STAT TIME COMMAND 1445 ? S 0:00 syslogd -m 0 1449 ? S 0:00 klogd -x 2280 ? S 0:01 smbd -D 2281 ? S 0:01 nmbd -D 2300 ? S 0:01 /usr/sbin/sshd 2429 ? S 0:00 crond 3479 ? S 0:00 /usr/sbin/atd 2586 tty2 S 0:00 /sbin/mingetty tty2 2587 tty3 S 0:00 /sbin/mingetty t ty3 2588 tty4 S 0:00 /sbin/mingetty tty4 2589 tty5 S 0:00 /sbin/mingetty tty5 2590 tty6 S 0:00 /sbin/mingetty tty6 2591 ? S 0:00 login -- root 2592 tty1 S 0:01 -bash 2614 pts/0 R 0:00 ps -aux </pre>
Test Type	Objective. Stimulus-Response (reboot)
Evidence	
Findings	

AUDIT STEP	9 – Verify Samba password encryption
Reference	Collier-Brown D., Eckstein R. and Ts J. 2003. <u>Using Samba, 2nd Edition</u> . Appendix B O'Reilly & Associates, Sebastopol, CA.
Risk	XI - Unauthorised user uses networks sniffing tools to access/modify/destroy data
Control Objective	Verify that Samba is configured to use the strongest form of password encryption available. For version 2 of Samba, the strongest encryption available is NTLM hash A.K.A. NTLM. Samba also supports the older, weaker LanManager hash; it should be disabled. This setting does not prevent passwords from being “sniffed” off the network, but it makes the passwords more difficult to crack.
Testing Procedure	1. Log in to the server & su to root 2. Check the Lan Manager authentication in the Samba configuration file: <code>grep lanman /etc/samba/smb.conf</code>
Compliance Criteria	The smb.conf file should have the following lanman config: lanman auth = no
Test Type	Objective.
Evidence	
Findings	

AUDIT STEP	10 – Verify file permissions on Samba password file (smbpasswd)
Reference	Toxen B. 2001. <u>Real world Linux security: Intrusion prevention, detection, and recovery</u> . Chapter 4.8. Prentice Hall PTR, Upper Saddle River, NJ. N.B. The Samba section of this book is credited to Larry Gee.
Risk	IV - User error exposes data to unauthorized internal users
Control Objective	The Samba password file contains password hashes, it should be protected by strict file permissions
Testing Procedure	1. Log in to the server & su to root 2. Check the file permission on the Samba password file: <code>ls -l /etc/samba/smbpasswd</code>
Compliance Criteria	The password file should be owned and only be readable by root.
Test Type	Objective.
Evidence	
Findings	

AUDIT STEP	11 – Verify Samba users configuration
Reference	Toxen B. 2001. <u>Real world Linux security: Intrusion prevention, detection, and recovery.</u> Chapter 4.8. Prentice Hall PTR, Upper Saddle River, NJ. N.B. The Samba section of this book is credited to Larry Gee.
Risk	IV - User error exposes data to unauthorized internal users X - Unauthorised user uses networks sniffing tools to access/modify/destroy data
Control Objective	Insuring that Samba users do not have interactive shell access limits their ability to perform actions on the server. It also prevents anyone from using password obtained from NTLM hashes from logging on to the server.
Testing Procedure	<ol style="list-style-type: none"> 1. Obtain list of users authorised to access the Samba server 2. Log in to the server & su to root 3. Check that the list of authorized users matches the users defined in /etc/samba/smbpasswd 4. Check that each samba user is configured to use /sbin/nologin as a shell by checking /etc/passwd 5. Verify that samba users cannot Log in to Linux by randomly choosing an account and attempting to Log in.
Compliance Criteria	<p>The users defined in smbpasswd must match the list of authorized users and each Samba user must have their shell set to /sbin/nologin in /etc/passwd.</p> <p>To be compliant the above setting must be validated by trying to Log in as one of the users and failing.</p>
Test Type	Objective. Stimulus–Response
Evidence	
Findings	

AUDIT STEP	12 – Verify password complexity requirements in Linux
Reference	<p>Garfinkel S. and Spafford G. 1996. <u>Practical Unix & Internet Security, 2nd Edition</u>. Chapter 3. O'Reilly & Associates, Sebastopol, CA.</p> <p>Red Hat. 2002b. Red Hat Linux 9 Red Hat Security Guide. 4.3. Password Security. http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-wstation-pass.html Last Accessed: 26 January 2004</p>
Risk	<p>X - Unauthorised user bypasses network protection to access/modify/destroy data</p> <p>XI - Unauthorised user uses networks sniffing tools to access/modify/destroy data</p>
Control Objective	Password complexity protects against dictionary attacks and slows down brute force attacks against passwords.
Testing Procedure	<ol style="list-style-type: none"> 1. Log in to Linux 2. Use passwd to attempt to set your password to a dictionary word: <pre>passwd</pre>
Compliance Criteria	The system must reject dictionary words as passwords for the system to be compliant.
Test Type	Objective. Stimulus–Response
Evidence	
Findings	

AUDIT STEP	13 – Verify password complexity requirements in Windows
Reference	<p>Garfinkel S. and Spafford G. 1996. <u>Practical Unix & Internet Security, 2nd Edition</u>. Chapter 3. O'Reilly & Associates, Sebastopol, CA.</p>
Risk	<p>X - Unauthorised user bypasses network protection to access/modify/destroy data</p> <p>XI - Unauthorised user uses networks sniffing tools to access/modify/destroy data</p>
Control Objective	Password complexity protects against dictionary attacks and slows down brute force attacks against passwords.
Testing Procedure	<ol style="list-style-type: none"> 1. From a Windows machine log in to the Domain 2. Press ctrl-alt-del to bring up the password change dialog box 3. Attempt to change the password to a dictionary word
Compliance Criteria	The system must reject dictionary words as passwords for the system to be compliant.
Test Type	Objective. Stimulus–Response
Evidence	
Findings	

AUDIT STEP	14 – Audit passwords
Reference	Barrett D J., Silverman R. E. and Byrnes R. 2003. <u>Linux Security Cookbook</u> . 9.1 Testing Login Passwords O'Reilly & Associates, Sebastopol, CA.
Risk	X - Unauthorised user bypasses network protection to access/modify/destroy data XI - Unauthorised user uses networks sniffing tools to access/modify/destroy data
Control Objective	Password complexity protects against dictionary attacks and slows down brute force attacks against passwords.
Testing Procedure	<ol style="list-style-type: none"> 1. Log in to Linux & su to root 2. "Unshadow" the password file: <pre>cd /var/lib/john umask 077 unshadow /etc/passwd /etc/shadow > mypasswords.txt</pre> 3. Run john: <pre>john mypasswords.txt</pre> 4. Delete the "mypasswords.txt" file: <pre>rm mypasswords.txt</pre> 5. Audit the Samba passwords: <pre>john /etc/smbpasswd</pre>
Compliance Criteria	For the system to be compliant, john should return the following message: 0 password cracked
Test Type	Objective.
Evidence	
Findings	

© SANS Institute, Author retains full rights

AUDIT STEP	15 – Verify Samba shares
Reference	Collier-Brown D., Eckstein R. and Ts J. 2003. <u>Using Samba, 2nd Edition</u> . 9.2 Controlling Access to Shares. O'Reilly & Associates, Sebastopol, CA.
Risk	IV - User error exposes data to unauthorized internal users V - User error makes data unavailable to authorized internal users
Control Objective	Insure that all the required shares are defined and that no additional shares are defined.
Testing Procedure	1. Obtain list of authorised Samba users 2. Log in to Linux & su to root 3. List Samba configuration: testparm
Compliance Criteria	The list of shares should match the list of authorized users with the addition of the shared directory and the netlogon share.
Test Type	Objective.
Evidence	
Findings	

AUDIT STEP	16 – Verify Samba share masks & permissions
Reference	Collier-Brown D., Eckstein R. and Ts J. 2003. <u>Using Samba, 2nd Edition</u> . 8.2 File Permissions and Attributes on MS-DOS and Unix. O'Reilly & Associates, Sebastopol, CA.
Risk	VI - Software bug affects confidentiality, integrity or availability of data IV - User error exposes data to unauthorized internal users
Control Objective	Samba translates file permissions and properties between Windows and Linux. Files on user directories should, by default, only be readable by the user and the root account.
Testing Procedure	1. From a Windows machine, Log in as a Samba user and write a test file to you home directory 2. Log in to the Samba server as a Linux user 3. Attempt to read the file created in step 1 cat /home/ [user] /testfile.txt
Compliance Criteria	No user on the Linux system should be able to read files in home directories of other users, even if these files have been written from Windows through Samba.
Test Type	Objective. Stimulus–Response
Evidence	
Findings	

AUDIT STEP	17 – Verify logging of failed log in attempts
Reference	Barrett D J., Silverman R. E. and Byrnes R. 2003. <u>Linux Security Cookbook</u> . 9.36 Summarizing Your Logs with logwatch. O'Reilly & Associates, Sebastopol, CA.
Risk	X - Unauthorised user bypasses network protection to access/modify/destroy data
Control Objective	Insure that failed log in are captured in the system's logs and by the logwatch tool.
Testing Procedure	<ol style="list-style-type: none"> 1. Attempt to log in to the Samba server using ssh with an invalid password 2. Attempt to log in to the domain from a Windows machine using an invalid password 3. Attempt to access a share using an invalid password. While logged in locally to a Windows machine, use Windows Explorer > Tools > Map network drive. Type UNC path to shared directory [\\Samba server\share], and click "Connect using a different user name". 4. Log in to Samba Server & su to root 5. Verify if failed log in attempts are captured by logwatch: <pre>logwatch -range all --print</pre>
Compliance Criteria	For the server to be compliant, the logwatch output must show all the failed log in attempts.
Test Type	Objective. Stimulus – Response
Evidence	
Findings	

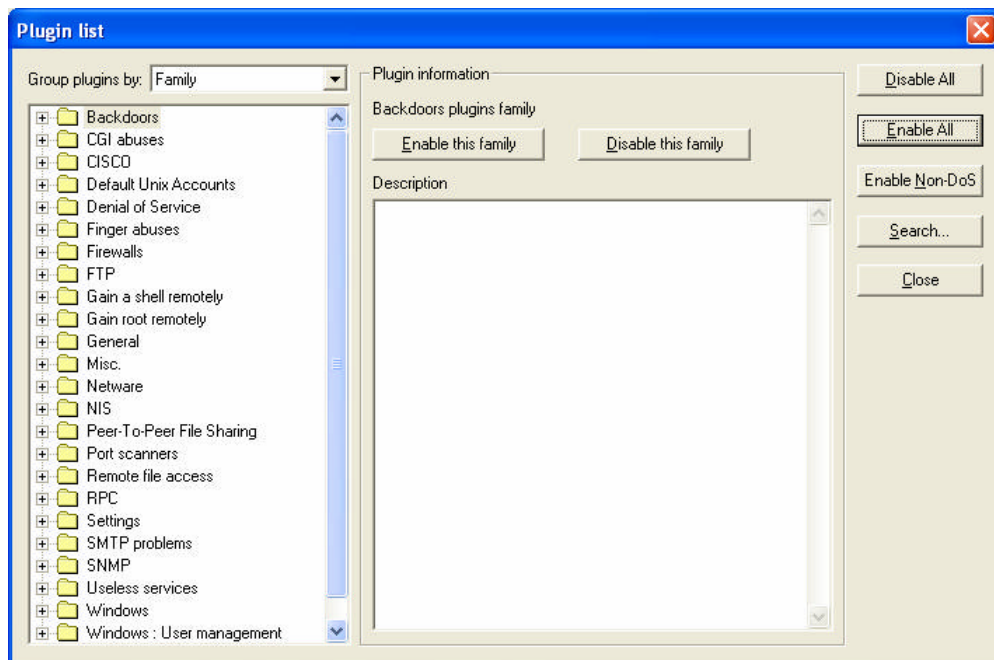
© SANS Institute 2004. All rights reserved.

AUDIT STEP	18 – Verify network access from authorised address
Reference	<p>Green J. 2002. <u>SANS Institute Track 7 – Auditing Networks, Perimeters and Systems. 7.4 Network Auditing Essentials v 4.1</u> pp. 6-17 to 6-66 SANS Institute.</p> <p>Fyodor. Nmap network security scanner man page. http://www.insecure.org/nmap/data/nmap_manpage.html Last Accessed: 28th February 2004</p>
Risk	<p>IV - User error exposes data to unauthorized internal users VIII - Malicious agent uses vulnerability in exposed service to access/modify/destroy data X - Unauthorised user bypasses network protection to access/modify/destroy data</p>
Control Objective	Insure that the only network services available on the server to authorised IP addresses are ssh and Samba.
Testing Procedure	<ol style="list-style-type: none"> 1. Identify an IP address authorised to connect to the Samba server 2. Connect scanning machine to network and configure it with Authorised IP address 3. Use nmap to scan Samba server for open TCP and UDP ports: <pre>nmap -sS -O [IP address of Samba server] nmap -sU [IP address of Samba server]</pre>
Compliance Criteria	<p>For the server to be compliant, the nmap scan must confirm that the only ports open on the server are:</p> <p>tcp 22 tcp 139 udp 137 udp 138</p>
Test Type	Objective. Stimulus-Response
Evidence	
Findings	

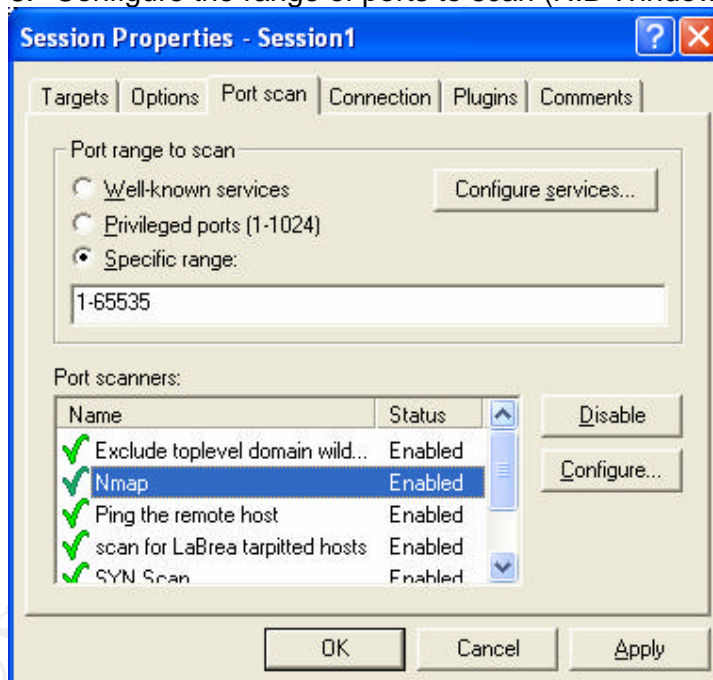
AUDIT STEP	19 – Verify network access from unauthorized address
Reference	<p>Green J. 2002. <u>SANS Institute Track 7 – Auditing Networks, Perimeters and Systems. 7.4 Network Auditing Essentials v 4.1</u> pp. 6-17 to 6-66 SANS Institute.</p> <p>Fyodor. Nmap network security scanner man page. http://www.insecure.org/nmap/data/nmap_manpage.html Last Accessed: 28th February 2004</p>
Risk	<p>IV - User error exposes data to unauthorized internal users VIII - Malicious agent uses vulnerability in exposed service to access/modify/destroy data X - Unauthorised user bypasses network protection to access/modify/destroy data</p>
Control Objective	Insure that no network services are available on the Samba server to unauthorised IP addresses.
Testing Procedure	<ol style="list-style-type: none"> 1. Identify an IP address not authorised to connect to the Samba server 2. Connect scanning machine to network and configure it with Authorised IP address 3. Use nmap to scan Samba server for open TCP and UDP ports: nmap -sS -O [IP address of Samba server] nmap -sU [IP address of Samba server]
Compliance Criteria	For the server to be compliant, the nmap scan must not return any open ports.
Test Type	Objective. Stimulus-Response
Evidence	
Findings	

© SANS Institute 2004

AUDIT STEP	20 – Network vulnerability scan from authorised address
Reference	Deraison Renaud http://www.nessus.org/documentation.html Last Accessed: 28 th February 2004
Risk	IV - User error exposes data to unauthorized internal users VIII - Malicious agent uses vulnerability in exposed service to access/modify/destroy data X - Unauthorised user bypasses network protection to access/modify/destroy data
Control Objective	The network vulnerability scan will verify that there are no known vulnerabilities in the services that Samba server exposes to the network. Note that during the nessus scan we check all ports (which was not done in the nmap scans of step 16 & 17). The nessus scan will also check for the presence of back-doors and Trojans on the server.
Testing Procedure	<ol style="list-style-type: none"> 1. Identify an IP address authorised to connect to the Samba server 2. Connect scanning machine to network and configure it with authorised IP address 3. Update Nessus with the latest plug-ins: <code>/usr/sbin/nessus-update-plugins</code> 4. Start the Nessus daemon on the scanning machines: <code>/usr/sbin/nessusd -D</code> 5. Start the Nessus GUI on the scanning machines or external machine (Using either the Linux client or NessuWX in Windows): <code>/usr/bin/nessus</code> 6. Set the Samba server as the target 7. Select all the plug-ins (N.B Windows screenshot):



8. Configure the range of ports to scan (N.B Windows screenshot):



9. Start the scan

10. Analyse the report:

Compliance Criteria	For the server to be compliant, there should be no serious vulnerabilities detected. Note that this test has a subjective element as the nessus report will require interpretation to determine the exact nature of each vulnerability.
Test Type	Subjective. Stimulus-Response

Evidence
Findings

© SANS Institute 2004, Author retains full rights.

AUDIT STEP	21 – Verify network share authentication & authorization
Reference	Collier-Brown D., Eckstein R. and Ts J. 2003. <u>Using Samba, 2nd Edition</u> . 8.2 File Permissions and Attributes on MS-DOS and Unix. O'Reilly & Associates, Sebastopol, CA.
Risk	IV - User error exposes data to unauthorized internal users V - User error makes data unavailable to authorized internal users
Control Objective	Insure that users cannot log in and access other user's personal shares
Testing Procedure	1. Log in to the domain from a Windows laptop 2. Attempt to connect to an other user's share, use Windows Explorer > Tools > Map network drive. Type UNC path to shared directory [\\Samba server\other user's share]
Compliance Criteria	For the server to be compliant, it should not be possible to connect to a user's share using any authentication other than the user's.
Test Type	Objective. Stimulus-Response
Evidence	
Findings	

© SANS Institute 2004, Author retains full rights.

AUDIT STEP	22 – Verify backups
Reference	Garfinkel S. and Spafford G. 1996. <u>Practical Unix & Internet Security, 2nd Edition</u> . Chapter 7. O'Reilly & Associates, Sebastopol, CA.
Risk	I - Hardware failure make data unavailable II - Physical destruction or removal of hardware make data permanently unavailable III - Unauthorised user leverages physical access to access/modify/destroy data VII - Software patch or upgrade corrupts data or makes it unavailable VIII - Malicious agent uses vulnerability in exposed service to access/modify/destroy data IX - Virus or worm spreads to Samba server corrupting data or making it temporarily or permanently unavailable X - Unauthorised user bypasses network protection to access/modify/destroy data XI - Unauthorised user uses networks sniffing tools to access/modify/destroy data
Control Objective	This test helps insure that required data can be restored from backups.
Testing Procedure	<ol style="list-style-type: none"> 1. Verify backup schedule and note the date and person responsible 2. Obtain both back-up CD-Rs 3. Verify that the backups were performed on the scheduled date 4. Select 2 files on the server that have not been modified since the last backup 5. Check the MD5 checksums of the 2 files above: <pre>md5sum [name of file]</pre> 6. Locate the 2 files from step 3 on the CD-Rs 7. Check the MD5 checksum of the 2 files on the 2 CDs (same as step 5) 8. Open the files using relevant software
Compliance Criteria	For the backups to be compliant, they must have been performed on the scheduled date, the MD5 sums of the files must match and it must be possible to open the files using the relevant software. Note that the tests must work for both CD-Rs.
Test Type	Objective.
Evidence	
Findings	

AUDIT STEP	23 – Verify arpswatch configuration
Reference	Leres Craig. arpswatch man page
Risk	X - Unauthorised user bypasses network protection to access/modify/destroy data IX - Unauthorised user uses networks sniffing tools to access/modify/destroy data
Control Objective	The arpswatch utility detects changes in MAC-IP relations highlighting potential attempts at MAC spoofing, IP spoofing and ARP poisoning.
Testing Procedure	1. Connect a tests machine to the network and obtain an IP address from the DHCP server 2. Manually change the IP address of the test machine 3. Check the logs for a warning from arpswatch
Compliance Criteria	For the server to be compliant, the logs must contain the arpswatch warnings.
Test Type	Objective. Stimulus-Response
Evidence	
Findings	

© SANS Institute 2004, Author retains full rights

Assignment 3

5 Audit

This audit of Fictitious's Samba server "ficsmb" was conducted on the 29th of January 2004

5.1 Audit Checklist

AUDIT STEP	1 – Physical security
Reference	Garfinkel S. and Spafford G. 1996. <u>Practical Unix & Internet Security, 2nd Edition.</u> Chapter 12 Physical security. O'Reilly & Associates, Sebastopol, CA.
Risk	I - Hardware failure makes data unavailable II - Physical destruction or removal of hardware make data permanently unavailable III - Unauthorised user leverages physical access to access/modify/destroy data
Control Objective	Given that someone with physical access to the server and enough time will be able to access data on the server, it is important to limit access.
Testing Procedure	1. Evaluate using either interview or observation if a malicious insider could gain physical access to the server 2. If answer to above is yes estimate if a malicious outside could gain access for a period long enough to do arm
Compliance Criteria	The server is compliant if there is no window of opportunity for a malicious insider.
Test Type	Subjective.
Evidence	An interview with the administrator confirmed that there had been a number of occasions when an outsider (e.g. customer, electrician, deliveryman) had been in the reception area unmonitored and could have gained access to the server for period of up to 15-20 min. The auditor also noted the absence of a surge protector.
Findings	The system is not compliant

AUDIT STEP	2 – Verify BIOS and boot loader configurations
Reference	Red Hat. 2002a. Red Hat Linux 9 Red Hat Security Guide. 4.2. BIOS and Boot Loader Security. http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-wstation-boot-sec.html Last Accessed: 26 January 2004
Risk	III – Unauthorised user leverages physical access to access/modify/destroy data
Control Objective	Insure that it is not possible to bypass server OS protection features by booting the server to an alternative OS.
Testing Procedure	<ol style="list-style-type: none"> 1. Try to boot from a boot floppy (DOS 6.22) and a boot CD (FIRE) 2. Boot server 3. Try to access the setup/BIOS menu and change the boot priority (pressing F2 and navigating menu) 4. Reboot server 5. When server displays boot loader menu, try to use the GRUB command line (press c while grub menu is displayed)
Compliance Criteria	If the system can be booted to an alternative OS by using either boot media in the drives, changing the BIOS or using the boot loader, the system is non-compliant.
Test Type	Objective. Stimulus-Response
Evidence	<ul style="list-style-type: none"> • When booted with the boot CD or floppy, the server still booted from the hard drive. • When F2 was pressed during boot, a password prompt appeared to access the BIOS. • When in the GRUB boot menu, the following message appeared: <pre>Use • and • keys to select which entry is highlighted. Press enter to boot the highlighted entry or 'p' to enter a password to unlock the next set of features.</pre> • Pressing c did not have any effect.
Findings	The server is compliant

AUDIT STEP	3 – Verify Samba version and check for published vulnerabilities
Reference	<p>Pomeranz H. 2002. <u>SANS Institute Track 1 – SANS Security Essentials + CISSP CBK. 1.6</u> <u>SANS Security Essentials IV: UNIX Security v 1.4.</u> pp. 1-8, 1-7. SANS Institute.</p> <p>Personal experience</p>
Risk	<p>VI - Software bug affects confidentiality, integrity or availability of data VIII - Malicious agent uses vulnerability in exposed service to access/modify/destroy data</p>
Control Objective	Check that there are no published vulnerabilities/bugs for the Samba version that is currently running on the server.
Testing Procedure	<ol style="list-style-type: none"> 1. Log in to the Samba server & su to root 2. Check the location of the 2 Samba daemons <pre>which smbd which nmbd</pre> 3. Verify the version of Samba running on the server by logging on and typing the following commands: <pre>smbd -V nmbd -V</pre> 4. Search for reports of Samba vulnerabilities for this specific version in the following web locations: <p> http://www.cert.org/ http://www.samba.org/ http://www.securityfocus.com/ https://rhn.redhat.com/ (log in and check the profile of the server) </p>
Compliance Criteria	The compliance is subjective and will depend not only on the existence of vulnerabilities, but also on their relevance to the deployed system and on their severity.
Test Type Evidence	<p>Subjective.</p> <pre>[root@ficsmb /]# which smbd /usr/sbin/smbd [root@ficsmb /]# /usr/sbin/smbd -V Version 2.2.7a-security-rollup-fix [root@ficsmb /]# which nmbd /usr/sbin/nmbd [root@ficsmb /]# /usr/sbin/nmbd -V Version 2.2.7a-security-rollup-fix</pre>
Findings	<p>The system is compliant.</p> <p>According to the sites consulted, Samba 2.2.8 fixes a number of vulnerabilities in Samba 2.2.7, but the version number indicates that the executables have are patched. It is a common practice for Red Hat to “backport” security patches, in this case the version of Samba running on the server has the security fixes, but none of the other features introduced in 2.2.8.</p>

AUDIT STEP	4 – Verify Tripwire configuration and run Tripwire
Reference	Barrett D J., Silverman R. E. and Byrnes R. 2003. <u>Linux Security Cookbook</u> , Chapter 1 Taking Snapshot with Tripwire. O'Reilly & Associates, Sebastopol, CA.
Risk	V - User error exposes data to unauthorized internal users VIII - Malicious agent uses vulnerability in exposed service to access/modify/destroy data. IX - Virus or worm spreads to samba server corrupting data or making it temporarily or permanently unavailable. X - Unauthorised user bypasses network protection to access/modify/destroy data
Control Objective	Verify that core binaries and configuration files have not been modified maliciously or accidentally. N.B. This control does not prevent any of the risk, but allows detection.
Testing Procedure	<ol style="list-style-type: none"> 1. Insure that you know Tripwire pass-phrase 2. Log in to server & su to root 3. Export the current tripwire policy file to plain text: <pre>cd /etc/triwire twadmin --print-polfile > twpol.txt</pre> 4. Search for key server components (/usr/sbin/smbd, /usr/sbin/nmbd, /etc/Samba/smb.conf, /etc/samba/smbusers) within the plain text policy file: <pre>grep smb twpol.txt grep nmb twpol.txt grep ssh twpol.txt</pre> 5. Verify that core files have not been modified by running a check: <pre>tripwire --check</pre> 6. Delete plain-text policy file: <pre>rm twpol.txt</pre>
Compliance Criteria	A key compliance point of this audit step is to verify that the core services binaries and supporting files have not been modified. But any discrepancy discovered by the Tripwire check should be investigated
Test Type	Subjective.
Evidence	<p>N.B. The output from the tripwire check has been edited for legibility.</p> <pre>[root@ficsmb tripwire]# twadmin --print-polfile > twpol.txt [root@ficsmb tripwire]# grep smb twpol.txt /sbin/mount.smb -> \$(SEC_CRIT) ; /sbin/mount.smbfs -> \$(SEC_CRIT) ; /var/lock/subsys/smb -> \$(SEC_CONFIG) ; /etc/samba/smb.conf -> \$(SEC_CONFIG) ; [root@ficsmb tripwire]# grep nmb twpol.txt [root@ficsmb tripwire]# tripwire --check</pre>

Parsing policy file: /etc/tripwire/tw.pol
 *** Processing Unix File System ***
 [...]

Wrote report file: /var/lib/tripwire/report/ ficsmb-20040129-231918.twr

Tripwire(R) 2.3.0 Integrity Check Report

Report generated by: root
 Report created on: Thu 29 Jan 2004 11:19:18 PM GMT
 Database last updated on: Thu 29 Jan 2004 10:37:57 PM GMT

Report Summary:

Host name: ficsmb
 Host IP address: 192.168.1.22
 Host ID: None
 Policy file used: /etc/tripwire/tw.pol
 Configuration file used: /etc/tripwire/tw.cfg
 Database file used: /var/lib/tripwire/ ficsmb.twd
 Command line used: tripwire --check

Rule Summary:

Section: Unix File System

Rule Name	Severity Level	Added	
Removed Modified			
-----	-----	-----	-----
--			
Invariant Directories	66	0	0
0			
Temporary directories	33	0	0
0			
Tripwire Data Files	100	0	0
0			
Critical devices	100	0	0
0			
User binaries	66	0	0
0			
Tripwire Binaries	100	0	0
0			
Libraries	66	0	0
0			
Critical system boot files	100	0	0
0			
File System and Disk Administration Programs	100	0	0
0			
Kernel Administration Programs	100	0	0
0			
Networking Programs	100	0	0
0			
System Administration Programs	100	0	0

0	Hardware and Device Control Programs	100	0	0
0	System Information Programs	100	0	0
0	Application Information Programs	100	0	0
0	Shell Related Programs	100	0	0
0	Operating System Utilities	100	0	0
0	Critical Utility Sym-Links	100	0	0
0	Shell Binaries	100	0	0
0	Critical configuration files	100	0	0
0	System boot changes	100	0	0
0	OS executables and libraries	100	0	0
0	Security Control	100	0	0
0	Login Scripts	1 00	0	0
0	* Root config files	100	2	0

Total objects scanned: 22785
Total violations found: 6

=====
Object Summary:
=====

Section: Unix File System

Rule Name: Root config files (/root)
Severity Level: 100

Added:
"/root/gpg"
"/root/rh.key"

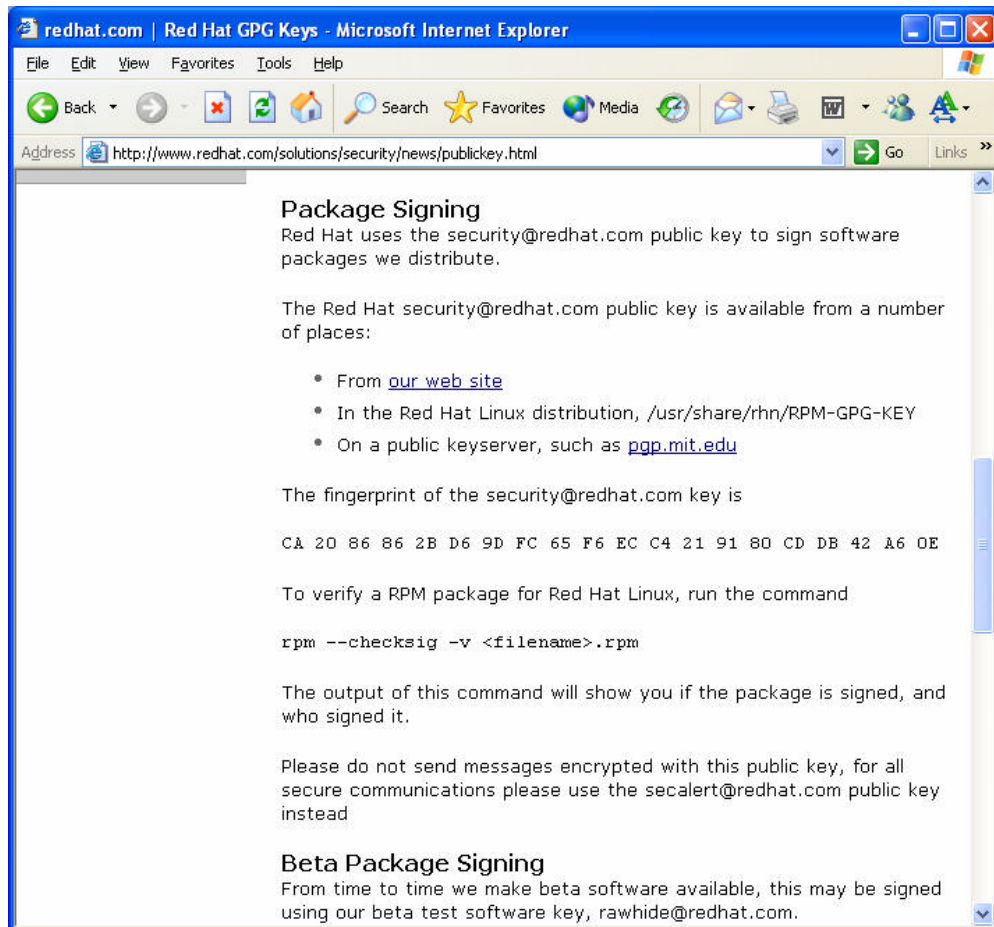
Modified:
"/root"
"/root/.gnupg"
"/root/.gnupg/pubring.gpg"
"/root/.gnupg/pubring.gpg~"

=====
Error Report:
=====

	<pre> Section: Unix File System ----- 1. File system error. Filename: /var/lock/subsys/autofs No such file or directory 2. File system error. Filename: /var/lock/subsys/identd No such file or directory 3. File system error. Filename: /var/lock/subsys/kprop No such file or directory 4. File system error. Filename: /var/lock/subsys/ripd No such file or directory 5. File system error. Filename: /etc/named.conf No such file or directory 6. File system error. Filename: /root/.esd_auth No such file or directory ----- *** End of report *** Tripwire 2.3 Portions copyright 2000 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY; for details use --version. This is free software which may be redistributed or modified only under certain conditions; see COPYING for details. All rights reserved. Integrity check complete. </pre>
Findings	<p>The server is non-compliant because a number of core Samba files are not monitored by tripwire:</p> <pre> /usr/sbin/smbd /usr/sbin/nmbd /etc/samba/smbusers /etc/samba/smbpasswd </pre> <p>There are a number of files in the policy that do not exist on the server, these should be removed from the Tripwire policy, note that the other violations reported were due to the audit and would not have caused the server to be non-compliant.</p>

AUDIT STEP	5 – Verify RPM public keys
Reference	<p>Red Hat. 2003a.</p> <p><u>Red Hat Linux 9: Red Hat Linux Customization Guide. 32.3. Checking a Package's Signature.</u></p> <p>http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/s1-check-rpm-sig.html</p> <p>Last Accessed: 29 January 2004</p>
Risk	VII - Software patch or upgrade corrupts data or makes it unavailable
Control Objective	Insure that the system uses the correct public keys to check the validity of rpm packages. This will prevent the installation of rogue packages.
Testing Procedure	<ol style="list-style-type: none"> 1. Log in to the server & su to root 2. Get Red Hat's public key signature from their web site (http://www.redhat.com/solutions/security/news/publickey.html) 3. Find the Red Hat public key in rpm: <pre>rpm -qa gpg-pubkey* [note exact name of key in output]</pre> 4. Export the key to a text file <pre>rpm -qi [exact name of key from above] > rh.key</pre> 5. Check the key with pgp by importing it (If the key already is in the key ring, pgp will indicate that the key has not changed). <pre>gpg --import rh.key</pre> 6. Use pgp to list the key's fingerprint and check the fingerprint against a good source (http://www.redhat.com/solutions/security/news/publickey.html) <pre>gpg -fingerprint</pre> 7. Delete text file <pre>rm rh.key</pre> 8. Check the signature of the key in the keyring used by up2date (N.B the two lines bellow are a single line at the console): <pre>gpg --fingerprint --no-default-keyring --keyring /etc/sysconfig/rhn/up2date -keyring.gpg</pre>
Compliance Criteria	For the system to be compliant, both the fingerprint from the key found in rpm and the one used by up2date must match Red Hat's published key fingerprints.
Test Type	Objective.

Evidence



```
[root@ficsmb root]# rpm -qa gpg-pubkey*
gpg-pubkey-db42a60e-37ea5438
[root@ficsmb root]# rpm -qi gpg-pubkey-db42a60e-37ea5438 > rh.key
[root@ficsmb root]# gpg --import rh.key
gpg: key DB42A60E: "Red Hat, Inc <security@redhat.com>" not
changed
gpg: Total number processed: 1
gpg: unchanged: 1
[root@ficsmb root]# gpg --fingerprints
/root/.gnupg/pubring.gpg
-----
pub 1024D/DB42A60E 1999-09-23 Red Hat, Inc <security@redhat.com>
   Key fingerprint = CA20 8686 2BD6 9DFC 65F6 ECC4 2191 80CD
DB42 A60E
sub 2048g/961630A2 1999-09-23

[root@ficsmb root]# gpg --fingerprint --no-default-keyring --
keyring /etc/sysconfig/rhn/up2date-keyring.gpg
-----
pub 1024D/DB42A60E 1999-09-23 Red Hat, Inc <security@redhat.com>
   Key fingerprint = CA20 8686 2BD6 9DFC 65F6 ECC4 2191 80 CD
DB42 A60E
sub 2048g/961630A2 1999-09-23
```

Findings

The server is compliant.

AUDIT STEP	6 – Verify Samba packages with rpm
Reference	Red Hat. 2003b. Red Hat Linux 9: Red Hat Linux Customization Guide. 32.4. Impressing Your Friends with RPM. http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/s1-rpm-impressing.html Last Accessed: 29 January 2004
Risk	VII - Software patch or upgrade corrupts data or makes it unavailable
Control Objectives	Verify that the elements of Samba installed on the server are the ones installed under rpm control.
Testing Procedure	1. Log in to the server & su to root 2. Use rpm to verify the Samba packages: rpm -V samba rpm -V samba-common
Compliance Criteria	For the system to be compliant, the verify commands should not return any modified files aside from: /etc/samba/smbusers /etc/samba/smb.conf
Test Type	Objective.
Evidence	[root@ficsmb root]# rpm -V Samba S.5....T c /etc/Samba/smbusers [root@ficsmb root]# rpm -V Samba-common S.5....T c /etc/Samba/smb.conf
Findings	The server is compliant; the only files that are different from the original rpm packages files are configuration files.

© SANS Institute 2004. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage or retrieval system, without the prior written permission of SANS Institute.

AUDIT STEP	7 – Verify that all relevant patches have been applied to the system
Reference	<p>Red Hat. 2001-2003b. <u>Red Hat Network 2.8: Update Reference Guide. Chapter 2. Red Hat Update Agent</u> http://www.redhat.com/docs/manuals/RHNetwork/ref-guide/2.8/up2date-setup.html Last Accessed: 29th January 2004</p>
Risk	<p>VI - Software bug affects confidentiality, integrity or availability of data VIII - Malicious agent uses vulnerability in exposed service to access/modify/destroy data</p>
Control Objective	Check that there are no outstanding patches for the system.
Testing Procedure	<ol style="list-style-type: none"> 1. Log in to the server & su to root 2. Use up2date to list available patches for yours system (N.B. you will need the root password) <pre>up2date -l</pre>
Compliance Criteria	The list of updates returned should not include any security update/errata for samba or ssh components. It might be necessary to read the description of certain updates such as libraries to determine if they have security implications for your system.
Test Type	Objective.
Evidence	<pre>[root@ficsmb /]# up2date -l Fetching package list for channel: redhat-linux-i386-9... ##### Fetching Obsoletes list for channel: redhat-linux-i386-9... ##### Fetching rpm headers... All packages are currently up to date [root@ficsmb /]#</pre>
Findings	The server is compliant

AUDIT STEP	9 – Verify Samba password encryption
Reference	Collier-Brown D., Eckstein R. and Ts J. 2003. <u>Using Samba, 2nd Edition</u> . Appendix B O'Reilly & Associates, Sebastopol, CA.
Risk	XI - Unauthorised user uses networks sniffing tools to access/modify/destroy data
Control Objective	Verify that Samba is configured to use the strongest form of password encryption available. For version 2 of Samba, the strongest encryption available is NT LanManager hash A.K.A. NTLM. Samba also supports the older, weaker LanManager hash; it should be disabled. This setting does not prevent passwords from being “sniffed” off the network, but it makes the passwords more difficult to crack.
Testing Procedure	1. Log in to the server & su to root 2. Check the Lan Manager authentication in the Samba configuration file: <code>grep lanman /etc/samba/smb.conf</code>
Compliance Criteria	The smb.conf file should have the following lanman config: lanman auth = no
Test Type	Objective.
Evidence	<code>[root@ficsmb /]# grep lanman /etc/Samba/smb.conf</code> <code>lanman auth = no</code>
Findings	The server is compliant

© SANS Institute 2004, Author retains full rights.

AUDIT STEP	12 – Verify password complexity requirements in Linux
Reference	<p>Garfinkel S. and Spafford G. 1996. <u>Practical Unix & Internet Security, 2nd Edition</u>. Chapter 3. O'Reilly & Associates, Sebastopol, CA.</p> <p>Red Hat. 2002b. Red Hat Linux 9 Red Hat Security Guide. 4.3. Password Security. http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-wstation-pass.html Last Accessed: 26 January 2004</p>
Risk	<p>X - Unauthorised user bypasses network protection to access/modify/destroy data</p> <p>XI - Unauthorised user uses networks sniffing tools to access/modify/destroy data</p>
Control Objective	Password complexity protects against dictionary attacks and slows down brute force attacks against passwords.
Testing Procedure	<ol style="list-style-type: none"> 1. Log in to Linux 2. Use passwd to attempt to set your password to a dictionary word: <pre>passwd</pre>
Compliance Criteria	The system should reject dictionary words as passwords for the system to be compliant.
Test Type	Objective. Stimulus–Response
Evidence	<pre>[alice_admin@ficsmb alice_admin]\$ passwd Changing password for user alice_admin. Changing password for alice_admin (current) UNIX password: New password: BAD PASSWORD: it is based on a dictionary word New password: BAD PASSWORD: it is too short New password: BAD PASSWORD: it's WAY too short passwd: Authentication token manipulation error [alice@ficsmb alice_admin]\$ passwd Changing password for user alice_admin. Changing password for alice_admin (current) UNIX password: New password: BAD PASSWORD: it is too simplistic/systematic New password: Retype new password: passwd: all authentication tokens updated successfully.</pre> <p>The passwords tested were: password, r2d2, bob and 12345678</p>
Findings	The server is compliant, the server rejected simple dictionary words as well as other easily cracked passwords.

AUDIT STEP	13 – Verify password complexity requirements in Windows
Reference	Garfinkel S. and Spafford G. 1996. <u>Practical Unix & Internet Security, 2nd Edition</u> . Chapter 3. O'Reilly & Associates, Sebastopol, CA.
Risk	X - Unauthorised user bypasses network protection to access/modify/destroy data XI - Unauthorised user uses networks sniffing tools to access/modify/destroy data
Control Objective	Password complexity protects against dictionary attacks and slows down brute force attacks against passwords.
Testing Procedure	1. From a Windows machine log in to the Domain 2. Press ctrl-alt-del to bring up the password change dialog box 3. Attempt to change the password to a dictionary word
Compliance Criteria	The system must reject dictionary words as passwords for the system to be compliant.
Test Type	Objective. Stimulus–Response
Evidence	<p>Not only was it possible to change the password to a dictionary word (“hello”) but the password synchronisation script also set the linux password of the account to “hello”. To validate the changes, the auditor ran john the ripper:</p> <pre>[root@scanner run]# unshadow /etc/passwd /etc/shadow > mypasswords.txt [root@scanner run]# ./john mypasswords.txt Loaded 8 passwords with 8 different salts (FreeBSD MD5 [32/32]) hello (alice) [root@scanner run]# ./john /etc/samba/smbpasswd Loaded 5 password (NT LM DES [24/32 4K]) HELLO (alice)</pre> <p>The auditor also managed to change passwords to dictionary words in Linux using smbpasswd.</p>
Findings	The server is non-compliant. The PAM is completely bypassed when changing Samba passwords.

AUDIT STEP	17 – Verify logging of failed log in attempts
Reference	Barrett D J., Silverman R. E. and Byrnes R. 2003. <u>Linux Security Cookbook</u> . 9.36 Summarizing Your Logs with logwatch. O'Reilly & Associates, Sebastopol, CA.
Risk	X - Unauthorised user bypasses network protection to access/modify/destroy data
Control Objective	Insure that failed log in are captured in the system's logs and by the logwatch tool.
Testing Procedure	<ol style="list-style-type: none"> 1. Attempt to log in to the Samba server using ssh with an invalid password 2. Attempt to log in to the domain from a Windows machine using an invalid password 3. Attempt to access a share using an invalid password. While logged in locally to a Windows machine, use Windows Explorer > Tools > Map network drive. Type UNC path to shared directory [\\Samba server\share], and click "Connect using a different user name". 4. Log in to Samba Server & su to root 5. Verify if failed log in attempts are captured by logwatch: logwatch -range all --print
Compliance Criteria	For the server to be compliant, the logwatch output must show all the failed log in attempts.
Test Type	Objective. Stimulus – Response
Evidence	<p>After a number of attempts, the log where checked through logwatch (edited for length & readability):</p> <pre> ----- pam_unix Begin ----- passwd: Unknown Entries: authentication failure; logname=cedric_admin uid=508 euid=0 tty= ruser= rhost= user=alice: 1 Time(s) su: Sessions Opened: cedric_admin(uid=500) -> root: 10 Time(s) Authentication Failures: cedric_admin(500) -> root: 1 Time(s) sshd: Authentication Failures: cedric_admin (192.168.1.102): 7 Time(s) Samba: Unknown Entries: session opened for user alice by (uid=0): 4 Time(s) session opened for user david by (uid=0): 1 Time(s) session closed for user david: 1 Time(s) session opened for user cedric by (uid=0): 6 Time(s) session closed for user alice: 4 Time(s) session closed for user cedric: 5 Time(s) </pre>

```

----- pam_unix End -----
[...]
----- SSHD Begin -----

SSHD Killed: 1 Time(s)

SSHD Started: 1 Time(s)

Failed logins from these:
    cedric_admin/password from 192.168.1.102: 4 Time(s)

Users logging in through sshd:
    cedric_admin logged in from 192.168.1.1 using password: 2
Time(s)
    cedric_admin logged in from 192.168.1.2 using password: 7
Time(s)
    alice logged in from 192.168.1.102 using password: 1 Time(s)

SFTP subsystem requests: 2 Time(s)

----- SSHD End -----

```

Findings

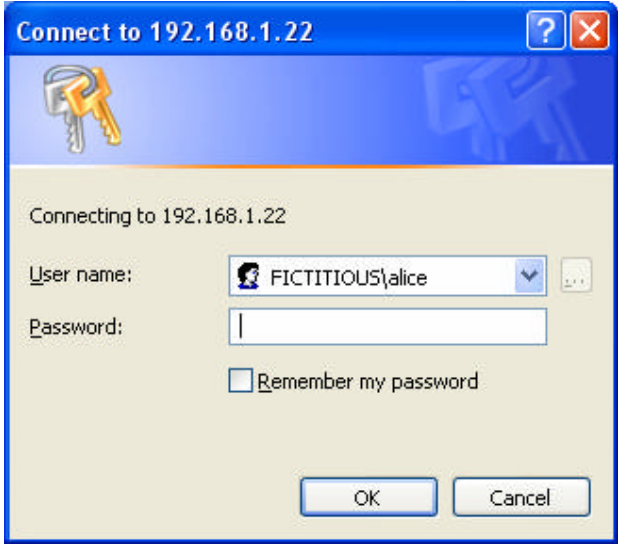
After a number of attempts, the log where checked through logwatch (extract):
The server is non compliant because the failed attempt to Log in to Samba shares do not appear in logwatch. Also note that the alice entry in the SSHD section was a login to /sbin/nologin, this is not clear from the output above.

© SANS Institute 2004, All rights reserved.

AUDIT STEP	18 – Verify network access from authorised address
Reference	<p>Green J. 2002. <u>SANS Institute Track 7 – Auditing Networks, Perimeters and Systems. 7.4 Network Auditing Essentials v 4.1</u> pp. 6-17 to 6-66 SANS Institute.</p> <p>Fyodor. <u>Nmap network security scanner man page.</u> http://www.insecure.org/nmap/data/nmap_manpage.html Last Accessed: 28th February 2004</p>
Risk	<p>IV - User error exposes data to unauthorized internal users VIII - Malicious agent uses vulnerability in exposed service to access/modify/destroy data X - Unauthorised user bypasses network protection to access/modify/destroy data</p>
Control Objective	Insure that the only network services available on the server to authorised IP addresses are ssh and Samba.
Testing Procedure	<ol style="list-style-type: none"> 1. Identify an IP address authorised to connect to the Samba server 2. Connect scanning machine to network and configure it with Authorised IP address 3. Use nmap to scan Samba server for open TCP and UDP ports: <pre>nmap -sS -O [IP address of Samba server] nmap -sU [IP address of Samba server]</pre>
Compliance Criteria	<p>For the server to be compliant, the nmap scan must confirm that the only ports open on the server are:</p> <p>tcp 22 tcp 139 udp 137 udp 138</p>
Test Type	Objective. Stimulus-Response
Evidence	<pre>[root@scanner /]# nmap -sS -O 192.168.1.22 Starting nmap V. 3.00 (www.insecure.org/nmap/) Interesting ports on (192.168.1.22): (The 1599 ports scanned but not shown below are in state: closed) Port State Service 22/tcp open ssh 139/tcp open netbios-ssn Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20 Uptime 0.1550 days (since Thu Jan 29 09:52:03 2004) Nmap run completed -- 1 IP address (1 host up) scanned in 43 seconds [root@scanner /]# nmap -sU 192.168.1.22 Starting nmap V. 3.00 (www.insecure.org/nmap/) Interesting ports on (192.168.1.22): (The 1466 ports scanned but not shown below are in state: closed) Port State Service 137/udp open netbios-sn 138/udp open netbios-dgm Nmap run completed -- 1 IP address (1 host up) scanned in 56 seconds</pre>

Findings	The server is compliant; the only ports open on the server are the Samba ports and ssh.
-----------------	---

© SANS Institute 2004, Author retains full rights.

AUDIT STEP	21 – Verify network share authentication & authorization
Reference	Collier-Brown D., Eckstein R. and Ts J. 2003. <u>Using Samba, 2nd Edition</u> . 8.2 File Permissions and Attributes on MS-DOS and Unix. O'Reilly & Associates, Sebastopol, CA.
Risk	IV - User error exposes data to unauthorized internal users V - User error makes data unavailable to authorized internal users
Control Objective	Insure that users cannot log in and access other user's personal shares
Testing Procedure	1. Log in to the domain from a windows laptop 2. Attempt to connect to an other user's share
Compliance Criteria	For the server to be compliant, it should not be possible to connect to a user's share using any authentication other than the user's.
Test Type	Objective. Stimulus-Response
Evidence	When trying to connect to another user's share (cedric) with the alice account, the server prompted for authentication despite using the correct password:
	
Findings	The server is compliant.

5.2 Analysis of residual risk

Overall the audit steps achieved the control objectives, but the control objectives still allowed for residual risks. The only notable control objective that could be better tested is password encryption, audit step 9 (Verify Samba password encryption) could use an external Stimulus-Response test such as sniffing with LophCrack.

5.2.1 Hardware failure

The principal residual risk to Fictitious's server is hardware failure. Given the nature of the hardware, the vulnerability cannot be addressed.

The risk of hardware failure is difficult to quantify, even with data such as mean time between failures on hard drives. Therefore the risk to the business is high.

5.2.2 DHCP

Fictitious is segregating its network between trusted and un-trusted users using DHCP, this is trivial to bypass and a more robust solution should be evaluated.

The use of arpwatch does give Fictitious a warning system, but relying on logs is not timely enough.

5.2.3 Red Hat Network Support

Fictitious's Red Hat Network contract is about to expire and is not renewable due to a change in Red Hat's strategy. Once the contract expires, Fictitious will have no means to automatically keep the server updated.

The solutions available to Fictitious are to migrate to the new Red Hat Enterprise product, or another Linux distribution such as Mandrake.

5.2.4 NTLM authentication

Although the server is compliant with audit step 9, the hash utilised is still weak. Microsoft has developed a stronger authentication (NTLMv2) and introduced it with Windows 2000.

New versions of Samba (3 and above) support this stronger authentication (force the use NTLMv2 with the option `ntlm auth = no`). Fictitious should consider upgrading.

5.2.5 Backups

By its nature, Fictitious's backup strategy puts the company at risk, the residual risk of losing a week's worth of data is always present.

The current system is too slow and labour-intensive to be used on a daily basis.

5.3 Analysis of system's "auditability"

The system is straightforward to audit, in great part due to the simplicity of the environment.

A number of audit steps would be much more difficult in an environment with more users; in particular audit steps 11 (Verify Samba users configuration) and 15 (Verify Samba shares) would have to be amended for a large user base. Audit step 14 (Audit passwords) would also be a time-consuming task with a large user base.

Audit steps 18 (Verify network access from authorized address) , 19 (Verify network access from unauthorized address) and 20 (Network vulnerability scan from authorised address) are somewhat redundant. It might be simpler to use 2 Nessus scans, or 1 Nessus scan from an authorised address and one nmap scan using the full port range from an un-authorised address.

© SANS Institute 2004, Author retains full rights

Assignment 4 (Risk Assessment)

6 Risk assessment

6.1 Summary

This audit has highlighted a number of failings with the Samba server. The principal issue remains the physical security of the server. As part of the initial risk assessment, we determined that the presence of the administrator helped counter the risks to the server, our audit proved that this is not the case (audit step 1). Tools do exist to bypass/reset BIOS password; such a tool combined with physical access could allow someone to access the data on the server. Theft of the server or a key component (Hard-drive) is also a potential risk.

The second most important issue detected by the audit was that the measures in place to insure password complexity on Windows clients were ineffective.

The audit also uncovered a non-compliant logging mechanism, the logwatch tool does not seem to capture failed Samba log in, this could leave a dictionary attack undiscovered: a guest on our network could brute-force a password and access data on the server without our knowledge.

The tripwire policy file did not include core Samba file (audit step 4). This could lead to corrupted/trojaned Samba executable running on the server

The residual risks are significant and should be addressed as well.

Before implementing any of the changes, Fictitious should review its justification for the system and seriously evaluate the costs and benefits of the current solution versus alternative solutions.

The administrator has performed a preliminary evaluation and believes that a small Network Attached Storage (NAS) solution such as the Linksys EFG80 will prove to be a better solution for Fictitious.

6.2 Risks

There were four non-compliances recorded during the audit. All of these, aside from Physical security exposed the server to risk X (Unauthorised user bypasses network protection to access/modify/destroy data).

Fictitious believes that the threats are currently low as they do not yet allow guests to connect to their network.

6.2.1 Audit Step 1 - Physical security

The non-compliance on Physical security leaves the server exposed to the following risks:

II - Physical destruction or removal of hardware make data permanently unavailable

III - Unauthorised user leverages physical access to access/ modify/destroy data

The lack of protection against power surges and electrical noises also exposes the server to:

I - Hardware failure makes data unavailable

The risks above have been rated as high and medium during risk analysis.

6.2.2 Audit Step 4 – Verify Tripwire configuration and run Tripwire

Since the core Samba binaries are not monitored, they could be modified without Fictitious being alerted:

X - Unauthorised user bypasses network protection to access/modify/destroy data

The risk above has been rated as medium during risk analysis.

6.2.3 Audit step 13 – Verify password complexity requirements in Windows

The non-compliance of the server in this case exposes Fictitious to the following risks:

X - Unauthorised user bypasses network protection to access/modify/destroy data

XI - Unauthorised user uses networks sniffing tools to access/modify/destroy data

The risks above have been rated as low and medium during risk analysis. (note that the specific risks of sniffing has been identified as low.

6.2.4 Audit step 17 – Verify logging of failed log in attempts

The non-compliance of the server would leave Fictitious unaware of attempted brute force attacks against the Samba account, exposing it to the following risk:

X - Unauthorised user bypasses network protection to access/modify/destroy data.

This risk was rated as medium during the assessment, but this non-compliance, in combination with the one above leaves the server very vulnerable to brute force attacks.

6.3 System changes and further testing

The audit highlighted the fact that Fictitious must implement some changes to protect their information assets before letting guest connect to their network.

6.3.1 Secure the system physically

The system should be secured physically, the “comms” closet might be a suitable location for it (see audit step 1).

Fictitious should also invest in an Uninterruptible Power Supply (UPS) to protect the server against power surges and interruptions. As a minimum precaution, Fictitious should purchase a surge protector.

Fictitious purchased a UPS and moved the server to the “comms” closet. The UPS will be used for the NAS solution if Fictitious decides to implement it.

6.3.2 Add Samba deamons to Tripwire policy file

The missing Samba files were added to the Tripwire policy:

```
[root@ficsmb tripwire]# twadmin --print-polfile > twpol.txt
[root@ficsmb tripwire]# grep smb twpol.txt
/usr/sbin/smbd -> $(SEC_CRIT) ;
/sbin/mount.smb -> $(SEC_CRIT) ;
/sbin/mount.smbfs -> $(SEC_CRIT) ;
/var/lock/subsys/smb -> $(SEC_CONFIG) ;
/etc/samba/smb.conf -> $(SEC_CONFIG) ;
/etc/samba/smbusers -> $(SEC_CONFIG) ;
/etc/samba/smbpasswd -> $(SEC_CONFIG) ;
[root@ficsmb tripwire]# grep nmb twpol.txt
/usr/sbin/nmbd -> $(SEC_CRIT) ;
```

6.3.3 Enforce strong passwords on Windows

Fictitious should implement system policies to enforce strong passwords on Windows. The current setup does not prevent users from choosing weak passwords.

The first step is for Fictitious to disable the password synchronization between Samba and Linux by setting the option unix password sync = no in smb.conf.

To implement system policies, Fictitious followed the instructions in [Collier-Brown D., Eckstein R. and Ts J. 2003 section 4.6 Windows NT Policies]:

- Use poledit.exe to create a policy
- Save the policy as ntconfig.pol
- Copy the ntconfig.pol file to the netlogon share on the Samba server

Fictitious will either implement system policies after migrating to the new OS, or implement the NAS solution.

6.3.4 Implement a custom Logwatch filter for failes Samba log ins

Fictitious will either wait for the migration to the new OS to implement the Logwatch filters or implement the NAS solution.

6.3.5 Migrate the system to a supported version of Linux

The system should be migrated to a new supported version of Red Hat or migrated to another distribution to insure the availability of patches (residual risk 5.2.3).

The easiest option for Fictitious is to migrate to either Red Hat Enterprise Linux WS or Mandrake Linux PowerPack; with either of these choices, the administrators will be able to use the skills they acquired on Red Hat 9.

Both options also give Fictitious access to automated online updates & patches tailored to their server which is the core reason for them to purchase a commercial, supported version of Linux.

Fictitious will use the remaining time in their RHN contract to evaluate the two options in parallel with the evaluation of the NAS solution.

6.3.6 Implement redundant hard drives

Fictitious should invest in redundant hard-drive solution (see residual risk 5.2.1). The simplest and most cost-effective way to implement a redundant drive solution is for fictitious to purchase a second hard drive and use software disk mirroring (built into Linux).

Fictitious will either wait for the migration to the new OS to implement the new drive or implement the NAS solution.

6.3.7 Implement a better backup mechanism

Fictitious should implement a backup solution that will insure that files are automatically backed-up on a daily basis and that copies of these backups are stored off-site.

A traditional tape solution will provide fictitious with the automation and portability required. The important caveat is to insure that the hardware is compatible with Linux.

Fictitious will either wait for the migration to the new OS to implement the new tape backup solution or implement the NAS solution.

6.3.8 Segregate the network with a firewall

By purchasing a firewall and a new switch, Fictitious could easily separate it network into a trusted and a un-trusted subnet without relying on reserved addresses in DHCP (see 5.2.2).

Fictitious has decided to implement a firewall to put the conference room on a separate subnet before they hold any training courses in their offices.

6.4 System Justification

Considering the results of the audit and the cost of the recommended changes, Fictitious should re-evaluate their use of the server.

Considering that the server was originally implemented to provide shared storage without impacting the administrator's workstation, we should evaluate other solutions in particular storage appliances and Internet-based storage services before committing to the changes described in 6.3. This evaluation should be based on security, cost and manageability.

Preliminary research shows that the cost of implementing the changes described in 6.2 will conservatively be 500 US dollars: (100 OS, 100 Hard drive, 300 backup solution). There are Network Attached Storage solutions available that will meet Fictitious's requirements, for 600 US dollars. The security and manageability of these solutions need to be researched further.

© SANS Institute 2004, Author retains full rights.

7 References

A note on references: A number of references used for this paper where located on the O'Reilly & Associate Safari web site. Since the site requires a subscription, and SANS's policy requires public web site references, I have referenced the original book using chapter and section.

Barrett D J., Silverman R. E. and Byrnes R. 2003. Linux Security Cookbook. O'Reilly & Associates, Sebastopol, CA.

Collier-Brown D., Eckstein R. and Ts J. 2003. Using Samba, 2nd Edition. O'Reilly & Associates, Sebastopol, CA.

Deraison Renaud
<http://www.nessus.org/documentation.html>
Last Accessed: 28th February 2004

Fyodor. Nmap network security scanner man page.
http://www.insecure.org/nmap/data/nmap_manpage.html
Last Accessed: 28th February 2004

Garfinkel S. and Spafford G. 1996. Practical Unix & Internet Security, 2nd Edition. O'Reilly & Associates, Sebastopol, CA.

Green J. 2002. SANS Institute Track 7 – Auditing Networks, Perimeters and Systems. 7.4 Network Auditing Essentials v 4.1 SANS Institute.

Green J. and Hoelzer D. 2003. SANS Institute Track 7 – Auditing Networks, Perimeters and Systems. 7.6 Advanced Systems Audit UNIX v 1.4. SANS Institute.

Karwisch W. 2003. Auditing a Corporate E-mail Gateway Running Postfix on Linux: an Administrator's Perspective.
http://www.giac.org/practical/GSNA/William_Karwisch_GSNA.pdf
Last Accessed: 28th February 2004

Leres Craig.
Arpwatch man page.
<http://www-nrg.ee.lbl.gov/>
Last Accessed: 28th February 2004

Pomeranz H. 2002. SANS Institute Track 1 – SANS Security Essentials + CISSP CBK. 1.6 SANS Security Essentials IV: UNIX Security v.1.4. SANS Institute

Red Hat. 2001-2003a. Red Hat Network 2.8: Update Reference Guide. Chapter 1. What is Red Hat Network?
<http://www.redhat.com/docs/manuals/RHNetwork/ref-guide/2.8/intro.html>
Last Accessed: 29th January 2004

Red Hat. 2001-2003b. Red Hat Network 2.8: Update Reference Guide. Chapter 2. Red Hat Update Agent
<http://www.redhat.com/docs/manuals/RHNetwork/ref-guide/2.8/up2date-setup.html>

Last Accessed: 29th January 2004

Red Hat. 2002a. Red Hat Linux 9 Red Hat Security Guide. 4.2. BIOS and Boot Loader Security.
<http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-wstation-boot-sec.html>

Last Accessed: 26 January 2004

Red Hat. 2002b. Red Hat Linux 9 Red Hat Security Guide. 4.3. Password Security.
<http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/security-guide/s1-wstation-pass.html>

Last Accessed: 26 January 2004

Red Hat. 2003a. Red Hat Linux 9: Red Hat Linux Customization Guide. 32.3. Checking a Package's Signature.
<http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/s1-check-rpm-sig.html>

Last Accessed: 29 January 2004

Red Hat. 2003b. Red Hat Linux 9: Red Hat Linux Customization Guide. 32.4. Impressing Your Friends with RPM.
<http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/custom-guide/s1-rpm-impressing.html>

Last Accessed: 29 January 2004

Toxen B. 2001. Real world Linux security: Intrusion prevention, detection, and recovery. Prentice Hall PTR, Upper Saddle River, NJ.
N.B. The Samba section of this book is credited to Larry Gee.

Zwicky E. D., Cooper S. and Chapman D. B. 2000. Building Internet Firewalls, 2nd Edition. O'Reilly & Associates, Sebastopol, CA.

© SANS Institute
Author retains full rights