An Audit of Samba File Sharing in a Home Office

GSNA Practical v4.0 Option 1, Topic 1 – “Testing”

Marc Bayerkohler

April 15, 2005

Table of Contents

Introduction

File Servers in SOHO Environments

For Small Office or Home Office (SOHO) environments, a basic reason to connect computers with a network is to easily share files and printers. These services are typically provided by a computer designated as the ‘File Server’.

File servers can be bought as appliances or built from parts. Many operating systems can be used to create a file server. They are generally flexible to meet various needs, and can be configured in many ways to integrate into any environment.

Because the purpose of the file server is to hold, share, and protect an organization’s data, the most important and confidential files will be stored on it. However, many SOHO situations do not have full-time Information Technology (IT) personnel, much less security experts. Therefore, the file server tends to be configured as simply as possible, with the goal of usability, not security.

An organization’s most valuable data is exposed to a number of risks involved with the file server. Properly managing the risk requires identifying the threats and vulnerabilities involved, and creating controls to eliminate or mitigate the exposure. An IT audit can help identify, define, and quantify those risks.

Pine Park Properties

Pine Park Properties is a home-based real-estate management company. As a two-person small business, the computing budget is small, with no IT staff. Pine Park Properties (PPP) has simple file-sharing requirements; they need to have separate storage for each user, a common file area, and a shared printer. The workstations use Microsoft Windows operating systems (XP Home and XP Professional), but to save money, a Linux server (requiring no license fees) was deployed to act as the file server.

Linux is a Unix-based operating system. However, it can provide file and printer sharing services to Windows and Unix clients using the Samba software package. Using a Samba-based Linux file server, the Windows clients can seamlessly access their files, folders, and printers via the network.

This paper analyzes risks to data stored on a Samba file server, provides an audit program to determine the vulnerabilities present in such a system, and presents the results of an audit done for Pine Park Properties. It fulfills the practical requirement of the SANS GIAC Systems and Network Auditor (GSNA) certification, and follows the format and restrictions of such.

Scope

The focus of this paper is on the Samba software as it is used as a file server. Samba provides file services when hosted on a server, and is dependent on other subsystems such as the underlying Operating System (OS), network, and hardware. In addition, the company data should be protected by processes such as encryption and regular backups. Controls are necessary to protect the company's electronic assets, and assure processing availability. The majority of these controls, while important, fall outside the domain of this document. The scope is the Samba software and configurations that provide file sharing for the company.

The Samba suite of software was created in 1992 by Andrew Tridgell[1]. He derived its name from the underlying protocol that it supports, Server Message Block (SMB). Originally developed by IBM as a part of NetBIOS (Network Basic Input Output System) for sharing files, SMB was used by Microsoft for network communication in Windows, and extended to its current form, called the Common Internet File System (CIFS).

Samba allows Unix systems, such as Linux, many of the abilities of a native Windows network server. Unix machines using Samba can participate in Windows networks, and can even replace Windows servers, acting as the Primary Domain Controller (PDC).

According to Chris Hertel in "Samba: An Introduction":

> The two key programs are `smbd` and `nmbd`. Their job is to implement the four basic modern-day CIFS services, which are:
>
> - File & print services
> - Authentication and Authorization
> - Name resolution
> - Service announcement (browsing)

While all these features are available, perhaps the most common use of Samba is for its ability to provide network disk space for files.

Pine Park Properties has limited IT requirements. The business requires email and web access for communication, research, and finances. Accounting is done with a small business financial package and various spreadsheets. Each property has contracts, notes, pictures, and various documents associated with it, and are stored in separate directories on disk. The company website is

[1] Hertel, http://www.samba.org/samba/docs/SambaIntro.html

hosted remotely. There are two users, two desktops, a laptop, and servers, all connected via LAN with firewalled access to the Internet. The users need separate private storage space, as well as a common area.

The scope of this document is reduced to the Samba system. To protect the integrity and availability of Pine Park's data, controls should be in place on many levels. Important concerns not in scope include:

- Use of encryption to protect sensitive data (for instance, bank account information) while stored or in transit
- Hardening of the server at the OS level
- Password procedures that require strong passwords (to protect against brute-force attacks)
- Firewalls
- Antivirus
- Physical security[2]

In addition, only the file serving functionality is addressed. Samba has many complex configurations with security implications for the company. The features regarding authentication and authorization, name resolution, printing, and service announcement are not analyzed.

The 'Risk Analysis' section has further statements limiting the scope of this paper.

[2] See d'Albis, 12 for such a discussion.

Risk Analysis

Risk is “the potential for harm or loss”[3]. For an organization to protect itself from harm or loss, it must understand and manage the risks that face it. Managing the risk requires identifying risks, then implementing and monitoring the internal controls that reduce risk to an acceptable level. The risks for an organization are detailed in its risk profile, the result of a risk analysis.

Risk analysis is “the process of analyzing a target environment and the relationships of its risk-related attributes”[3]. This process includes identifying the assets, threats, and vulnerabilities involved, their likelihood, and their impact.

For an audit to be meaningful and useful to an organization, it must address issues that are relevant and important to that organization. Therefore, an initial step in the auditing process is commonly a risk assessment of the entity to be audited. The analysis is used to focus the scope of the audit to areas of interest, i.e., of high or medium risk.

A full risk analysis of the Samba system at Pine Park Properties would describe all the relevant assets, potential impacts, threats, and vulnerabilities. The intention of this paper is to show the ability to perform a technical audit. The requirements for this paper dictate that only three high severity risks are analyzed, rather than performing a thorough, exhaustive risk analysis. The resulting controls and tests are limited to entries related to these three risks.

Assets

Pine Park Properties has many assets, physical, electronic, and financial. The assets affected by the Samba system, however, are limited. Because Samba controls access to electronic files, the assets at risk are the data in those files, and any assets put at risk by that information.

Computer files include copies of contracts, notes, pictures, and other documents associated with rental property. These documents, while confidential, would not lead to substantial loss if revealed. The financial accounting application, however, contains information critical to the operation of the business. The application and its data must be available on a monthly basis for billing to be completed properly. Most importantly, the financial information (bank accounts, names, balances, passwords) could be used to defraud the company or steal money directly. This information would be considered the ‘crown jewels’.

[3] Hansche, 12

Qualitative Assessment

The risk analysis will assess the risks in a qualitative, as opposed to quantitative, fashion. In a quantitative analysis, specific dollar amounts determine severity of loss, and accurate statistics are used for likelihood. In a qualitative analysis, more general terms (high, medium, low) are used to describe the terms.

The qualitative terms are based on the tables below, taken from the Centers for Medicare & Medicaid Services' "CMS Information Security Risk Assessment (RA) Methodology" [4] and modified to apply to this business.

Table 1. Likelihood of Occurrence Levels

Likelihood	Description
Low	Likely to occur two/three times every five years.
Medium	Likely to occur once every six months or less.
High	Likely to occur once per month or less.

Table 2. Impact Severity Levels

Impact Severity	Description
Minor	Will have some minor effect on the business. It will require minimal effort to repair or reconfigure the system.
Damaging	May cause moderate financial loss or damage to the reputation of the business. It will require expenditure of significant resources to recover/repair.
Critical	May cause major financial loss or the business to be permanently closed.

Table 3. Risk Levels

Likelihood of	**Impact Severity**		
Occurrence	Minor	Damaging	Critical
Low	Low	Moderate	Moderate
Medium	Low	Moderate	High
High	Moderate	High	High

[4] CMS, 8-10

Business Impact

Pine Park Properties relies on financial data stored on the file server. The significant risks to Pine Park Properties in regards to the Samba system involve the possibility of a loss of confidentiality of financial data (leading to theft), or a loss of availability (if system was damaged or controlled by an attacker).

For the purposes of this practical, three risks are examined. The greatest impact to the company would be a loss of funds due to theft or fraud, facilitated by the financial information kept in computer files, such as bank account numbers, balances, and passwords. Therefore, the risks analyzed all pertain to unauthorized access of data, or control of the system which leads to unauthorized access of data.

Three Major Risks

The three largest risks to Pine Park Properties are described in more detail. They are assigned qualitative assessments, and an explanation of the threats and vulnerabilities that combine to make the risk.

Risk R1 – Cleartext / Weakly Encrypted / Empty Passwords

R1	Password disclosure leads to unauthorized access of confidential data.	Likelihood:	Medium
		Severity:	Critical
		Risk Level:	High

Risk
Password disclosure leads to unauthorized access of confidential data.

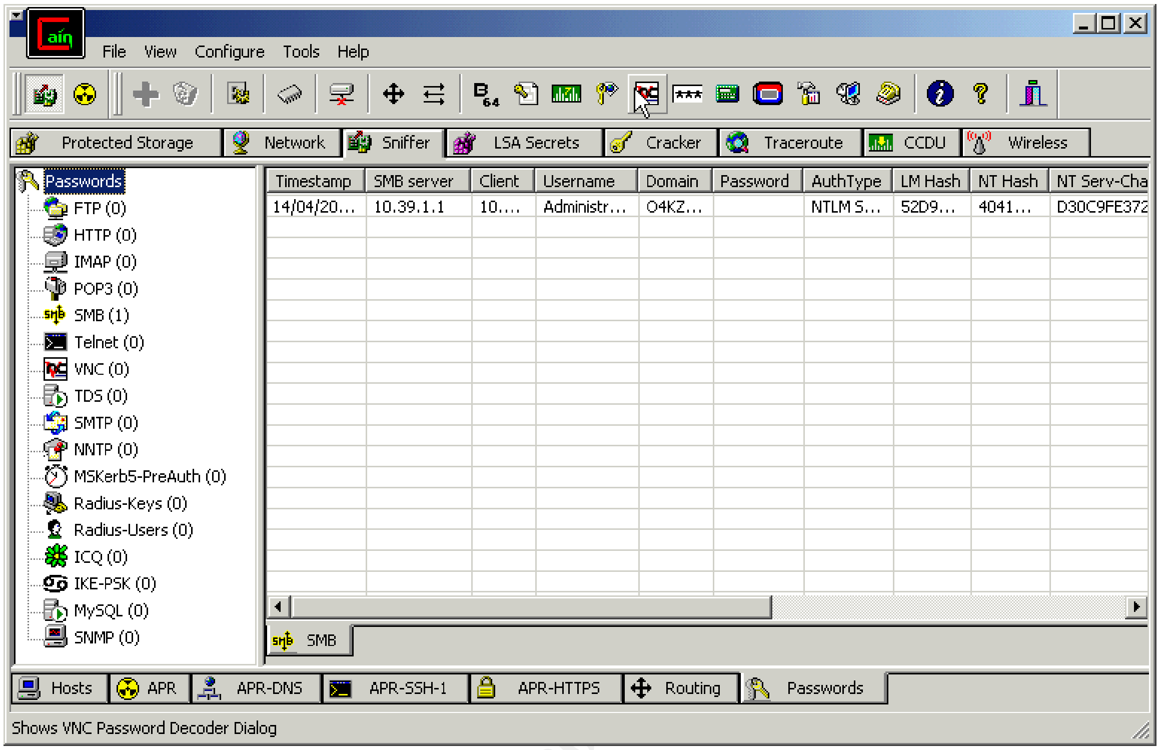
Threat
The threat comes from attackers on the local network 'sniffing' traffic for passwords, or users trying to connect with no password.

Samba provides access control to resources based on authenticating connections with a username and password. The SMB protocol supports sending this information across the network unencrypted, as 'cleartext', making it easy to intercept[5]. It also supports sending a hash of the password. The older LANMAN hashing algorithm is weak, and the password can be recovered in minutes or days using a brute-force tool. The newer MD4 hashing algorithm is much stronger, and could take years to brute-force.

There are numerous tools for capturing passwords from the network, and recovering passwords from hashes (e.g. Cain & Abel, dsniff, Ettercap). Below is a screenshot of Cain, a powerful tool that combines password sniffing, cracking, and ARP poisoning (a technique for sniffing traffic on a switched network).

[5] Vernooij, http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/ServerType.html#id2535830

Figure 1. Cain Password Sniffer/Cracker



Timestamp	SMB server	Client	Username	Domain	Password	AuthType	LM Hash	NT Hash	NT Serv-Cha
14/04/20...	10.39.1.1	10....	Administr...	O4KZ...		NTLM S...	52D9...	4041...	D30C9FE372

Shows VNC Password Decoder Dialog

Visitors to the office sometimes use the network, and could attempt access.

Vulnerabilities

Samba can be configured to accept cleartext passwords. Unless disabled, it also accepts LANMAN passwords, which are weak and easily broken with a brute-force attack[6][7]. Blank passwords allow access without requiring a password.

Risk R2 – Samba Exploits

R2	Server compromised via Samba exploit gives attacker full control.	Likelihood:	Low
		Severity:	Critical
		Risk Level:	Moderate

Risk

Server compromised via Samba exploit gives attacker full control and access to data.

[6] Mudge, http://www.insecure.org/sploits/l0phtcrack.lanman.problems.html

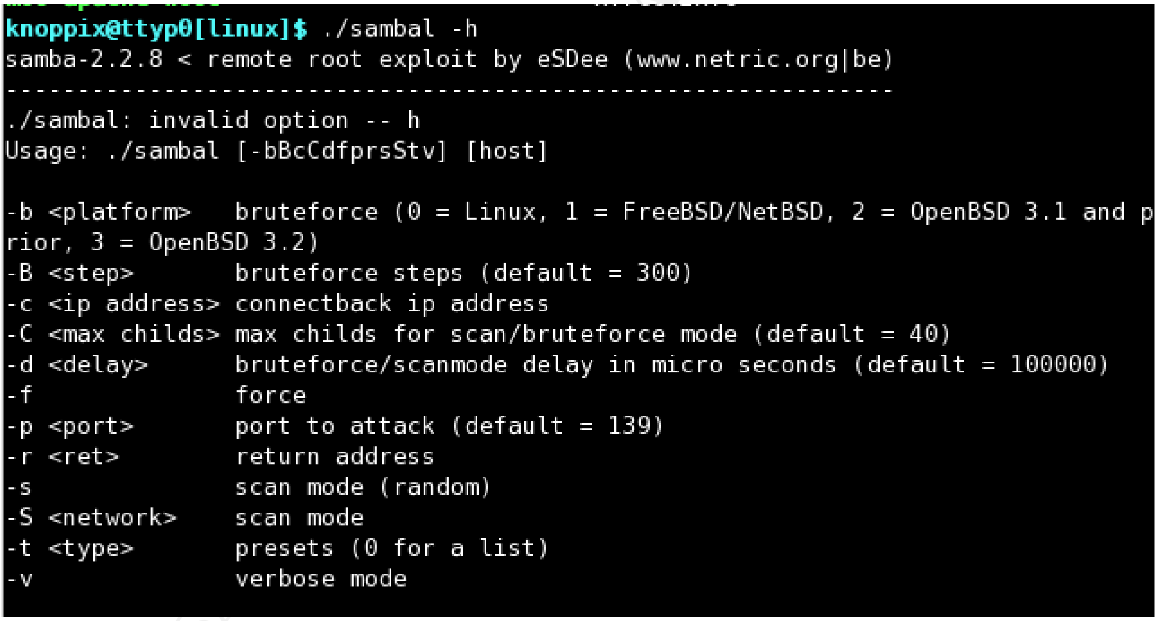
[7] Bogue, http://techrepublic.com.com/5100-6264_11-5427280.html?tag=LG#

Threat
Attackers on the local network could attempt unauthorized access using Samba exploits.

Samba accepts connections and data from the network, which has allowed attackers to create programs (exploits) that remotely take advantage of vulnerabilities in the Samba code to gain control of the server. Almost all programs have such weaknesses. Samba has a history of security issues which have been found and corrected with a patch or new release. Any Samba server that is not up-to-date on these patches is at risk.

Figure 2 shows the command line options for the sambal remote root exploit, by eSDee. Code such as this is available to attackers on the Internet, and is not difficult to find or use.

Figure 2. sambal Exploit Usage

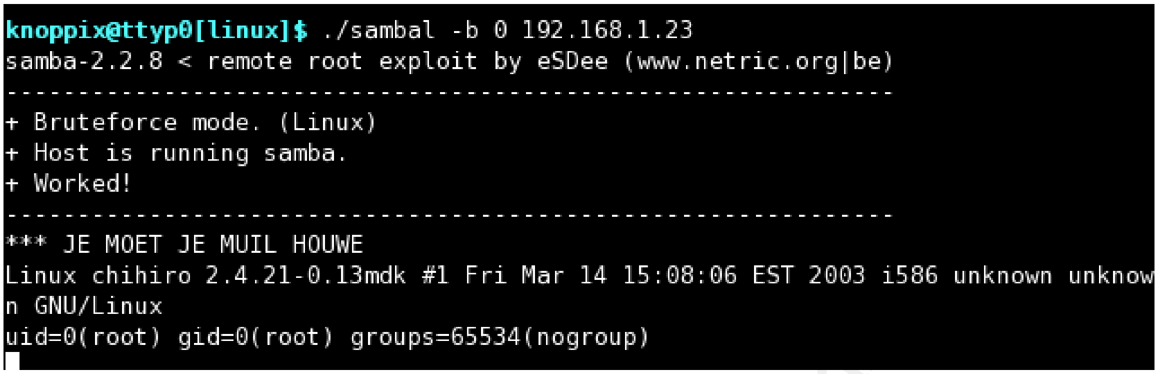


```
knoppix@ttyp0[linux]$ ./sambal -h
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
./sambal: invalid option -- h
Usage: ./sambal [-bBcCdfprsStv] [host]

-b <platform>   bruteforce (0 = Linux, 1 = FreeBSD/NetBSD, 2 = OpenBSD 3.1 and p
rior, 3 = OpenBSD 3.2)
-B <step>       bruteforce steps (default = 300)
-c <ip address> connectback ip address
-C <max childs> max childs for scan/bruteforce mode (default = 40)
-d <delay>      bruteforce/scanmode delay in micro seconds (default = 100000)
-f              force
-p <port>       port to attack (default = 139)
-r <ret>        return address
-s              scan mode (random)
-S <network>    scan mode
-t <type>       presets (0 for a list)
-v              verbose mode
```

The attacker specifies the architecture and IP address of the target server, and when run, the exploit provides an interactive connection to the target as root (see Figure 3).

Figure 3. sambal Exploit Successful



```
knoppix@ttyp0[linux]$ ./sambal -b 0 192.168.1.23
samba-2.2.8 < remote root exploit by eSDee (www.netric.org|be)
--------------------------------------------------------------
+ Bruteforce mode. (Linux)
+ Host is running samba.
+ Worked!
--------------------------------------------------------------
*** JE MOET JE MUIL HOUWE
Linux chihiro 2.4.21-0.13mdk #1 Fri Mar 14 15:08:06 EST 2003 i586 unknown unknow
n GNU/Linux
uid=0(root) gid=0(root) groups=65534(nogroup)
```

Visitors to the office sometimes use the network, and could attempt to use an exploit to gain control of the server, and access to the data.

Vulnerabilities
Exploits work on system with vulnerable code, such as buffer overflows. An unpatched Samba system, or a Samba system containing flaws the Samba Team has not fixed, creates a vulnerability.

Risk R3 – Misconfiguration

R3	Misconfiguration leads to compromise of the system or data.	Likelihood:	Medium
		Severity:	Critical
		Risk Level:	High

Risk
Misconfiguration leads to compromise of the system or data. Unauthorized access to confidential data results.

Threat
The threat comes from attackers on the local network attempting unauthorized access. Visitors to the office sometimes use the network, and could attempt access.

Vulnerabilities
A vulnerability is created when Samba is incorrectly configured in a way that decreases security. These could arise from:

- Technical errors, such as using an incompatible set of options, or a typo in the configuration file
- Access Control List (ACL) errors, such as not properly designing access restrictions to confidential data, or improperly implementing access

restrictions
- Security features left disabled, or not configured for the level of security necessary, such as logging passwords, or incorrect file permissions

Misconfiguration is a common cause of security vulnerabilities. The more complicated a system is to configure correctly, the more likely a misconfiguration will result in a vulnerability.

Although Samba is primarily configured from a single, well documented file (smb.conf), the Samba system itself, with its multitude of modes and options, makes misconfiguration easy. To address this issue, many GUI configuration tools such as SWAT and Webmin are available[8].

Use of GUI tools can still result in a technically correct configuration that allows incorrect access. For instance, if the access controls are not applied to data, or inappropriate users are in trusted groups, the data is at risk.

Samba's plethora of configuration options includes many related to security. Samba is flexible in allowing options that decrease security, but may be desired in some environments (such as displaying version information, or allowing .rhost authentication). Some options are strongly recommended by the Samba Team, but are not enabled by default.

Correctly Evaluating the Samba Configuration

The location of the Samba configuration file is set when compiled, but can be over-ridden on the command line. By default, it is in

```
/usr/local/samba/lib/smb.conf
```

but is often changed to

```
/etc/samba/smb.conf
```

or

```
/usr/samba/lib/smb.conf
```

The file is broken into 'sections' that describe the resources available (file shares, printers, etc.) and the options that apply to them. The '[global]' section contains options that will apply to all resources. The options in the shared resource sections (with exceptions like 'hosts allow') over-ride the global options. Therefore, to be effective, security options should be present in the global section, and not changed in other sections. When reviewing options, the

[8] Samba Team, http://samba.org/samba/GUI/

file must be searched for all instances of the option.

Options are set by assigning a value to them, using the format:

```
<option name> = <value>
```

For example:

```
server string = Samba Server %v
max log size = 50
```

Audit Program

An audit program is a structure to facilitate thorough, repeatable audits of a system. This program describes controls to address the risks identified in the previous section, and tests used to determine if a system is compliant with those controls. Some of the formatting and terms used are inspired by other's practicals[9].

1 Cleartext / Weakly Encrypted / Empty Passwords

Control 1.1

Control Objective
Samba passwords transmitted over the network are encrypted.

Risk Addressed
R1. Password disclosure leads to unauthorized access of confidential data.

Control Activity
Samba is configured to enable encrypted passwords during authentication, and reject unencrypted authentication attempts.

Type of Control: Preventive

Test 1.1.1
Inspect Samba configuration. Determine if options are used to prevent use of plaintext passwords.

Table 5. Password Encryption Configuration Options

Option Name	Default Value	Secure Value	Result
encrypt passwords	yes	yes	Encrypted passwords are accepted
lanman auth	yes	no	smbd does not use the weak LANMAN hash[10]
client lanman auth	yes	no	Samba client tools will not use the weak LANMAN hash

Compliance Criteria: Options must be set to secure value.

Type of Test: The test is objective; the options must be present to pass.

[9] Camac

[10] Note that older SMB clients, such as Windows98, are only capable of authenticating with LANMAN or cleartext, and will not be able to connect unless additional software is installed.

Test 1.1.2

Use a network ‘sniffer’ program to monitor network traffic for passwords or LANMAN password hashes. For a Windows system, Cain (http://www.oxid.it/cain.html) is an all purpose tool that can perform ARP-poisoning to sniff traffic even on a switched network. For Unix systems, the dsniff suite (http://www.monkey.org/~dugsong/dsniff/) or Ettercap (http://ettercap.sourceforge.net/) provide password sniffing and additional features.

Determine if the sniffer used was able to collect any passwords from the network. For Cain, if a password is collected, no encryption is used. If a ‘LM Hash” with no ‘NT Hash’ is collected, the weak LANMAN hash is being used.

Compliance Criteria: No unencrypted passwords or LANMAN hashes are collected.

Type of Test: Test is subjective, results depend on the sniffer used, how it is connected to the network, and network traffic.

Control 1.2

Control Objective

Blank passwords are not used.

Risk Addressed

R1. Password disclosure leads to unauthorized access of confidential data.

Test 1.2.1

Inspect the smbpasswd file, which stores hashes of passwords used for authentication.

Determine if any lines have the ‘N’ flag set to identify null (blank) passwords, or ‘NO PASSWORD’ in the hashes. For example:

```
snort:82:NO PASSWORDXXXXXXXXXXXXXXXXXXXXX:NO PASSWORDXXXXXXXXXXXXXXXXXXXXX:[NUX
]:LCT-425B065C:
```

Compliance Criteria: No blank passwords are found.

Type of Test: Test is objective, no blank passwords must be found.

2 Samba Exploits

Although not in scope, a detective control for exploits would be a Network Intrusion Detection System (NIDS) such as Snort, or a log watching script looking for errors acting as a Host-based Intrusion Detection System (HIDS).

Control 2.1

Control Objective

Minimize vulnerability to attackers using Samba exploits by using a non-vulnerable version.

Risk Addressed

R2. Server compromised via Samba exploit gives attacker full control.

Control Activity

Samba is kept up to date with the latest security patches.

The Samba Team addresses security issues by releasing either a new version of Samba, or a patch for source code. A list of these releases is kept on their web page at:

http://www.samba.org/samba/history/security.html

When a new version of Samba is released, the output of the –V version information is changed to match. This can be used to determine if a Samba installation is the correct version.

When a source code patch is issued, it must be applied to the Samba source, and recompiled, and the version output of –V is not changed. Therefore, it is difficult to determine if a given patch has been applied. The Samba Team does not provide a method to identify patched binaries. Two possibilities are 1) compiling a patched binary on an identical system, and comparing its md5sum to that of the target system 2) attempt to take advantage of the vulnerability by using exploit code against the target system. Neither method is guaranteed to determine if the vulnerability exists on all systems[11], and they are not appropriate for auditing purposes.

Type of Control: Preventive

Test 2.1.1

Use the version (-V) command line option to determine the version of Samba used.

```
$ /usr/sbin/smbd -V
Version 2.2.7a
```

Compare this to the Samba Team's 'Samba Security Releases' table and

[11] Md5sums may differ because of other patches or changes; failure of exploit code to succeed does not prove all exploit code would fail.

determine if a version with outstanding security issues is being used. If the version displayed is not sufficient (i.e., a patch release), inquire of the administrator if they can provide evidence that the version is not vulnerable (such as patched source code, and reperformance of a compile that results in a binary identical to that in use).

Compliance Criteria: A non-vulnerable version of Samba is used.

Type of Test: The test is subjective. The version output is verifiable and repeatable, but may not always be reliable. The system is complaint if the administrators can provide evidence that a vulnerable version has been patched to remove the vulnerability.

Control 2.2

Control Objective

Minimize vulnerability to attackers using Samba exploits by filtering connections to the server.

Risk Addressed

R2. Server compromised via Samba exploit gives attacker full control.

Control Activity

Samba is configured to accept connections only on appropriate interfaces from appropriate IP addresses.

If Samba is not or cannot be patched, there are still steps that can be taken to protect the server, described in "Protecting an unpatched Samba server.[12]" Filtering connections by network interface and IP address prevents exploits from untrusted networks.

Type of Control: Preventive

Test 2.2.1

IP filtering is configured to allow only connections from appropriate networks.

This is configured with the 'hosts allow' and 'hosts deny' options. For example, these lines deny all connections by default, and allow connections only from the trusted networks:

```
        hosts allow = 127.0.0.1 192.168.1.0/24
        hosts deny = ALL
```

Inspect the configurations and determine if the filtering options are used, and if

[12] Samba Team, http://www.samba.org/samba/docs/server_security.html

they are properly configured.

Compliance Criteria: The filtering options are enabled and configured with appropriate IP addresses.

Type of Test: Subjective. The appropriate IP addresses to allow/deny depend on the network topology, trust relationships, etc.

Test 2.2.2
Interface filtering is configured so Samba listens only on appropriate network interfaces.

Filtering is activated with the 'bind interfaces only' option, and configured with 'interfaces'. The loopback interface and address should always be included[13]. For example, these lines activate filtering, and instruct Samba to listen only to the first Ethernet interface (eth0) and the loopback interface (lo):

```
bind interfaces only = Yes
interfaces = eth0 lo
```

Inspect the configurations and determine if interface filtering is active, and properly configured.

Compliance Criteria: Interface filtering is active and configured with the appropriate interfaces.

Type of Test: Subjective. The appropriate interfaces to listen on depend on the server and network topology, trust relationships, etc.

3 Misconfiguration

Control 3.1

Control Objective
Samba configuration file is technically correct.

Risk Addressed
R3. Misconfiguration leads to compromise of the system or data.

Control Activity
Verify Samba configuration passes checks for technical errors.

Type of Control: Preventive (detective of errors so they may be resolved, preventing vulnerabilities)

[13] Harrison, http://www.linuxhomenetworking.com/linux-hn/samba-trouble.htm#_Toc92808931

Test 3.1.1

The Samba package includes the ‘testparm’ utility, which tests the Samba configuration file for errors[14]. Run this command and determine if any errors are detected.

```
$ testparm -s /etc/samba/smb.conf
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
…
```

Compliance Criteria: Testparm must run with no errors detected.

Type of Test: The test is objective; the utility must run clean to pass.

Control 3.2

Control Objective

Samba files are protected by adequate file permissions.

Risk Addressed

R3. Misconfiguration leads to compromise of the system or data.

Control Activity

Properly set file permissions on Samba files.

Type of Control: Preventive

Test 3.2.1

Inspect the file permissions for sensitive files.

Hashes of Samba passwords are stored by default in the ‘smbpasswd’ file. It must be protected to prevent an attacker from reading it and attempting a brute-force attack to recover the passwords[15].

Locate the smbpasswd file.

```
$ testparm -s | grep "passwd file"
      smb passwd file = /etc/samba/smbpasswd
$ ls -l /etc/samba/smbpasswd
-rw-------    1 root     root          206 Dec 26 02:10 /etc/samba/smbpasswd
```

[14] Harrison, http://www.linuxhomenetworking.com/linux-hn/samba-trouble.htm#_Toc92808925

[15] Blair, http://www.linuxjournal.com/article/2717

Determine if the file is owned by root, with read/write permissions only for root (-rw------- or 600).

When joining a domain, security identifiers are stored in 'secrets.tdb' (Trivial Database), which should be protected with the same permissions as smbpasswd[16]. Locate this file and determine its permissions.

Incorrect file permissions on the Samba binaries could allow them to be modified by at attacker. Binaries are stored in different directories, depending on the Operating System (OS) architecture and installation decisions. Locate the binaries (e.g. 'locate smbd') and determine if they are writeable only by root.

List of Samba binaries[17]:

smbd
nmbd
smbclient
testparm
testprns
smbstatus
nmblookup
make_smbcodepage
smbpasswd

The 'passwd program' option defines an alternate program to be executed when changing passwords. If the 'passwd program' option is used, locate the program and determine if it is only writable by root.

Compliance Criteria: File permissions must be correct.

Type of Test: The test is objective; the file permissions must be correct.

Control 3.3

Control Objective

High risk Samba configuration options are not used.

Risk Addressed

R3. Misconfiguration leads to compromise of the system or data.

Control Activity

Configure Samba without activating high risk options.

Type of Control: Preventive

[16] Eckstein, http://us1.samba.org/samba/docs/using_samba/ch04.html

[17] Samba Team, 'Samba' man page

Test 3.3.1

Some options available in the configuration are inherently riskier. Although there may be specific needs for some of these options, in general they reduce security and should not be used[18].

Table 5 describes the options, and the reason for not using them.

Table 5. High Risk Configuration Options

Option Name	Default Value	Secure Value	Risk
passwd chat debug	no	no	Passwords will be logged
null passwords	no	no	Null passwords are allowed
guest ok	no	no	Allows access without password
public	“	“	Synonym for ‘guest ok’
hosts equiv	# blank	# blank	Allows access without password
use rhosts	# blank	# blank	Allows access without password
server string	Samba %v	Samba	Version information assists attackers in identifying vulnerabilities

Inspect the configuration file and determine if these options are enabled.

Compliance Criteria: High risk options are set to the secure value.

Type of Test: The test is objective; the options must have the secure value. If any of the options are used, there may be other mitigating controls, but this control is not compliant.

Control 3.4

Control Objective

Samba and OS level access controls are correct.

Risk Addressed

R3. Misconfiguration leads to compromise of the system or data.

Control Activity

Samba share access controls and OS file permissions are configured to allow only authorized users access to resources.

Samba shares are configured with access controls that can allow or deny

[18] Eckstein, http://www.oreilly.com/catalog/samba/chapter/book/ch06_04.html/

access based on the account authenticated. In addition, the underlying OS file permissions provide access control. For an authenticated user to access a resource, the Samba permissions and the OS permissions must allow it.

The business owner of the data decides who is authorized to access it. Ideally, there is a written policy describing authorized use of the data. Otherwise, the business owner will have to review the access rights and decide if they are correct.

Type of Control: Preventive

Test 3.4.1
Inspect the Samba access control options for shares in the configuration file. Determine if there are any obvious conflicts or misconfigurations, using knowledge of the business, descriptions, or other information in the evaluation.

Capture the OS-level file permissions for the files and directories of the shares. How this is done may depend on the OS and system administration tools available.

One method is using the Unix ‘find’ command. Change into the directory the share is rooted in, and issue the following find command:

```
$ find . -exec ls -ld {} \;
…
drwxrwxr-x    3 nobody   users        4096 Feb 15 18:07 ./www
-rwxrw-r--    1 nobody   users       50407 Apr  9  2003 ./www/boxes4troops.jpg
-rwxrw-r--    1 nobody   users       18890 May  1  2003 ./www/dogbackpack08-
tiny.jpg
-rwxrw-r--    1 nobody   users       69076 May  1  2003 ./www/dogbackpack08.jpg
-rwxrw-r--    1 nobody   users        1180 Apr 20  2003 ./www/favicon.bmp
…
```

The output is a listing of every directory and file under the current directory. This listing could be quite voluminous. It can be viewed live, one page at a time (‘find . –exec ls –ld {} \; | more’), or redirected to a file (‘find . –exec ls –ld {} \; > file_listing_for_share.date.txt’) for further examination.

The following find commands may be helpful:

find . -perm -2	Find all world-writable files.
find . -perm -20	Find all group-writable files.
find . ! -user anne	Find all files whose owner is not anne.
find . ! -group anne	Find all files whose group is not anne.
find . ! -user nobody -a -exec ls -l {} \;	Find all files whose owner is not nobody, and print their permissions
find . ! -group nogroup ! -group users ! -group anne	Find all files whose group is not nogroup, users, or anne

One method to arrange the data is to import a text file of permissions listings into Microsoft Excel for sorting and formatting.

If there is an authorized use policy for the data, determine if the access controls correctly enforce this policy.

NOTE, SAMBA ACCESS CONTROLS ARE COMPLEX!

Samba access control options (such as ‘valid users’, ‘invalid users’, ‘read only’, ‘guest ok’, etc.) can be combined to create complex rights. Options in one section can negate the effects of previous options. The results of an option are not always intuitive. Because of these interactions, an auditor must be familiar with the subtleties of the options before performing the audit. These options are described in the Samba documentation and other documents, and a description of them is beyond the scope of this practical.

If there is no policy, interview the business owner of the data. Show them the access controls evidence, explain its meaning, and allow them to review the listings, paying attention to the accounts with access to sensitive data.

Compliance Criteria: Access controls do not permit unauthorized access to resources.

Type of Test: If no written authorized use policy exists, the test is subjective, based on the business owner’s evaluation of the access controls.

Audit Results

An audit of the Samba system used by Pine Park Properties was performed by Marc Bayerkohler on April 15, 2005. The results of the audit are recorded here, followed by a summary.

Testing

Test 1.1.1

Control Objective
Samba passwords transmitted over the network are encrypted.

Sample Selection Criteria
Configuration file for the Samba server.

Testing Procedure
The configuration file used was /etc/samba/smb.conf. The file was opened using vi, and searched for the option names specified in the test.

Evidence
smb.conf file tagged as 1.1.1-smb.conf.

Results

- ‘encrypt passwords’ option set to secure value of ‘Yes’
- ‘lanman auth’ option not present, therefore using using the default, nonsecure value of ‘yes’
- ‘lanman auth’ option not present, therefore using using the default, nonsecure value of ‘yes’

Exceptions Noted

Recommendation
Unless connectivity to unmodified, older SMB clients (such as Microsoft Windows98) is required, the LANMAN hash should be disabled. PPP currently has no older clients that require LANMAN, and should use the options listed.

Management’s Response
Administrator will enable the options by Q3 2005.

Test 1.1.2

Control Objective
Samba passwords transmitted over the network are encrypted.

Sample Selection Criteria
Sniffer attached to the network while authentication takes place.

Testing Procedure
Cain, a password sniffing tool, was connected to the network. ARP poisoning was used to intercept traffic while authentication was taking place.

Evidence
For security reasons, the hashes intercepted were not saved.

Results
Cain was able to intercept traffic, and identified authentication attempts of users connecting to file shares. No cleartext passwords were captured. The hashes it captured were NTLM hashes, not the weak LANMAN hashes, and were not broken with a brute-force attack.

No Exceptions Noted

Recommendation
None

Management's Response
N/A

Test 1.2.1

Control Objective
Blank passwords are not used.

Sample Selection Criteria
All accounts in the smbpasswd file are tested.

Testing Procedure
The password file used was /etc/samba/smbpasswd. The file was opened using vi, and searched for the 'N' flag or 'NO PASSWORD' string.

Evidence
smbpasswd file tagged as 1.1.2-smbpasswd.

Results
No blank passwords were found.

No Exceptions Noted

Recommendation
None

Management's Response
N/A

Test 2.1.1

Control Objective
Minimize vulnerability to attackers using Samba exploits by using a non-vulnerable version.

Sample Selection Criteria
The smbd daemon is tested.

Testing Procedure

```
# smbd -V
Version 2.2.7a
```

Evidence
See above.

Results
The version being used was released 10 Dec 2002. The most recent security patch listed on the Samba Security Releases page was released 16 December 2004. According to the release notes, there are four security vulnerabilities in 2.2.7a.

Exception Noted

Recommendation
Upgrade to the most recent release of Samba.

Management's Response
Administrator will upgrade Samba by Q3 2005.

Test 2.2.1

Control Objective
Minimize vulnerability to attackers using Samba exploits by filtering connections to the server.

Sample Selection Criteria
Configuration file for the Samba server.

Testing Procedure

The configuration file used was /etc/samba/smb.conf. The file was opened using vi, and searched for the option names specified in the test.

Evidence
smb.conf file tagged as 1.1.1-smb.conf.

Results
The IP filtering options are not present. No filtering is done.

Exception Noted

Recommendation
Configure the IP filtering options.

Management's Response
Administrator will configure IP filtering by Q3 2005.

Test 2.2.2

Control Objective
Minimize vulnerability to attackers using Samba exploits by filtering connections to the server.

Sample Selection Criteria
Configuration file for the Samba server.

Testing Procedure
The configuration file used was /etc/samba/smb.conf. The file was opened using vi, and searched for the option names specified in the test.

Evidence
smb.conf file tagged as 1.1.1-smb.conf.

Results
The interface filtering options are not present. No filtering is done.

Exception Noted

Recommendation
Configure the interface filtering options.

Management's Response
Administrator will configure interface filtering by Q3 2005.

Test 3.1.1

Control Objective
Samba configuration file is technically correct.

Sample Selection Criteria
Configuration file for the Samba server.

Testing Procedure
The configuration file used was /etc/samba/smb.conf.

```
# testparm -s /etc/samba/smb.conf > 3.1.1-testparm_output.txt
```

The file was opened using vi, and reviewed for errors.

Evidence
3.1.1-testparm_output.txt

Results
Two warnings were generated.

- WARNING: You have some share names that are longer than 8 chars These may give errors while browsing or may not be accessible to some older clients
- Invalid combination of parameters for service sumo. Level II oplocks can only be set if oplocks are also set.

Exception Noted

Recommendation
Resolve the issues so that testparm runs without warnings.

Management's Response

1. The long share names are not a concern because no older clients are used.
2. Service 'sumo' is a printer no longer connected to the server. The administrator will remove this entry by 1 May 2005.

Test 3.2.1

Control Objective
Samba files are protected by adequate file permissions.

Sample Selection Criteria
All sensitive files listed in the test description.

Testing Procedure
File owners and permissions for each sensitive file are captured and reviewed.

```
# ls -l /etc/samba/smbpasswd >> 3.2.1-file_permissions.txt
# ls -l /etc/samba/secrets.tdb >> 3.2.1-file_permissions.txt
…
```

Evidence
3.2.1-file_permissions.txt

Results
All files are owned by root:root. Only root has modify rights to the files.

No Exceptions Noted

Recommendation
None

Management's Response
N/A

Test 3.3.1

Control Objective
High risk Samba configuration options are not used.

Sample Selection Criteria
Configuration file for the Samba server.

Testing Procedure
The configuration file used was /etc/samba/smb.conf. The file was opened using vi, and searched for the option names specified in the test.

Evidence
smb.conf file tagged as 1.1.1-smb.conf.

Results
- 'guest ok' appears four times, three times for printers, and once for the 'public' file share.
- 'server string' is set to default value, displaying the version.

Exceptions Noted

Recommendation
1. Consider creating an account (with password) for visitors to use when

accessing the printers and 'public' share, and disabling all 'no password' access.
2. Remove the version from 'server string'.

Management's Response

1. Administrator will evaluate new account recommendation and consider implementation by Q3 2005.
2. Administrator will remove version by 1 May 2005.

Test 3.4.1

Control Objective

Samba and OS level access controls are correct.

Sample Selection Criteria

Access controls in the configuration file are tested. Files and directories in file shares (public, marc, and anne) are tested.

Testing Procedure

The configuration file used was /etc/samba/smb.conf. The file was opened using vi, and searched for the option names specified in the test.

Evidence

3.4.1-share_permissions.txt

Results

- Files writable by 'other' were found in the 'marc' file share.
- File group ownership on the 'public' is inconsistent, consisting of nogroup, users, and marc.

Exceptions Noted

Recommendation

1. Normalize the file permissions to a consistent standard.
2. Resolve configuration issue that allows these inconsistent permissions to occur.

Management's Response

1. Administrator will fix permissions by 1 May 2005.
2. Although inconsistent, no confidential files are at risk with the current configuration.

Summary of Results

Of the ten tests, exceptions were noted in seven, signifying non-compliance with the controls. The remaining three had no exceptions. Pine Park Properties' security posture is extremely weak. The highest priority should be to resolve the failure of Test 2.1.1, the vulnerable version of Samba. The version in use is antiquated, and could be compromised by an attacker with minimal effort.

Many of the issues can be resolved with configuration changes, meaning compliance is possible without purchasing additional software or hardware.

List of References

Blair, John. “Samba's Encrypted Password Support.” *Linux Journal* 1 Dec 1998. 11 Apr. 2005
http://www.linuxjournal.com/article/2717

Bogue, Robert. “Six easy ways to secure Samba.” 28 Oct. 2004. 11 Apr. 2005
http://techrepublic.com.com/5100-6264_11-5427280.html?tag=LG#

Camac, Brenton. “Auditing Borland‘s J2EE Application Server: An Auditor’s Perspective.” Mar. 2004
http://www.giac.org/certified_professionals/practicals/gsna/0136.php

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS). “CMS Information Security Risk Assessment (RA) Methodology.” Version 1.1 12 Sep. 2002.
http://www.cms.hhs.gov/it/security/docs/RA_meth.pdf

d’Albis, Cedric. “Auditing a Samba server from an administrator's perspective.” Mar. 2004. 11 Apr. 2005
http://www.giac.org/certified_professionals/practicals/gsna/0124.php

Eckstein, Robert, David Collier-Brown, Peter Kelly. Using Samba. 1st Edition November 1999 O’Reilly. 11 Apr. 2005
http://www.oreilly.com/catalog/samba/chapter/book/index.html

Hansche, Susan, John Berti, Chris Hare. Official (ISC)^2 Guide to the CISSP Exam. Boca Raton: Auerbach Publications, 2004

Harrison, Peter. “Samba Security & Troubleshooting.” Linux Home Networking. 11 Apr. 2005
http://www.linuxhomenetworking.com/linux-hn/samba-trouble.htm#_Toc92808925

Hertel, Chris, Samba Team, jCIFS Team. “Samba: An Introduction.” 27 Nov. 2001. 11 Apr. 2005
http://www.samba.org/samba/docs/SambaIntro.html

Mudge. “L0phtcrack 1.5 Lanman / NT password hash cracker.” 24 Jul. 1997 14 Apr. 2005.
http://www.insecure.org/sploits/l0phtcrack.lanman.problems.html

Samba Team. Samba Home Page. 14 Apr. 2005. http://samba.org

Samba Team. Samba man page, part of Samba software distribution.

Vernooij, Jelmer, John Terpstra, Gerald Carter, ed. The Official Samba-3

HOWTO and Reference Guide. Samba Home Page. 29 Jun. 2003 14 Apr. 2005. http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/