Global Information Assurance Certification Paper

Auditing Perimeter Defenses in a Home Office Environment with an OpenBSD Firewall/VPN Branch Tunnel Gateway - An Administrator's Perspective

GSNA Practical Version 2.1, Option 1

Author: Frank Sweetser
Date: February 19, 2004

Contents

1 Abstract **1**

2 Research in Audit, Measurement Practice, and Control **2**
2.1 System to be Audited . . . 2
2.2 Risk . . . 3
2.3 Current State of Practice . . . 4

3 Create an Audit Checklist **5**
3.1 Introduction . . . 5
3.2 Checklist . . . 5
3.2.1 Firewall Items . . . 5
3.2.2 Operating System Items . . . 7
3.2.3 Network Service Items . . . 9
3.2.4 Miscellaneous Tests . . . 11

4 Audit Evidence **13**
4.1 Introduction . . . 13
4.2 Checklist Results . . . 14
4.3 Residual Risk . . . 18
4.4 Auditability . . . 19

5 Risk Assessment **21**
5.1 Summary . . . 21
5.2 Background . . . 21
5.3 System Changes and Further Testing . . . 22
5.4 System Justification . . . 25

A OpenBSD Binary Update Check Script **i**

B Initial Nessus Scan Report **iii**

C Final Nessus Scan Report **viii**

List of Figures

1 Network Diagram . . . 3
2 Testing Network Diagram . . . 13

1 Abstract

This paper details an audit of an OpenBSD system providing internet gateway, firewalling, and persistent VPN functionality for a small number of end stations. The audit will focus primarily on operating system security, such as user accounts and unnecessary services, and network services, including proper filter rules and VPN tunnel operation. All work was performed from the point of view of the system administrator. All identifying information, including names of individuals, computers, and IP addresses have been altered for privacy and security reasons.

2 Research in Audit, Measurement Practice, and Control

2.1 System to be Audited

I am auditing an OpenBSD 3.4 router. This system provides internet connectivity through a DSL line, NAT, DHCP, and firewall services for a small number of end stations, typically one or two. In addition, it also maintains a persistent branch office VPN tunnel to the Pacific Tech University (PT) network. This tunnel is used by one of the school network administrators to securely perform various work related functions from home whenever required after normal office hours.

Best practice dictates that any unneeded services should be disabled to prevent any unknown vulnerabilities or misconfiguration in those services from being exploited. Since the VPN tunnel terminates behind the primary firewall of the PT netowrk, an exploit of this system would make it an ideal entry point into the PT network. This makes it extremely critical that it should provide no services that are not absolutely required for.

All software running on this system is provided with the OpenBSD distribution. OpenBSD is a freely available, multi-platform, open source Unix distribution modeled after 4.4BSD UNIX. Its major distinguishing characteristic is the projects emphasis on security, making it a suitable choice for firewall applications. The IP filtering, forwarding, and IPSec capabilities are part of the standard OpenBSD network stack. The `pfctl` utility controls forwarding, filtering, and NAT, and the `isakmpd` utility manages IPSec sessions.

The remote endpoint of the IPSec tunnel is a Nortel Networks Contivity 4500 VPN server. Since this sytem is outside of the scope of this audit, we will assume that it is secure, and that the IPSec tunnel is properly authenticated.

CPU	Intel Pentium II 266MHz
RAM	192MB
Network Card xl0	3Com 3c900 10Mbps-Combo
Network Card xl1	3Com 3c900 10Mbps-Combo
Hard Drive	Western Digital 6GB
Services Provided	Internet Gateway, NAT, DHCP Server

Due to political and administrative concerns at PT, highly restrictive firewalls are strongly discouraged. As a result, there is very little internal filtering done, including at the remote endpoint of the VPN tunnel. If any of the systems protected by the OpenBSD router were to be compromised, they could then be used as a point of entry into the PT network that is behind the firewall. This means the OpenBSD router must be at least as secure as the main campus internet connection.

Note that the subnet handled by the OpenBSD router is out of the larger subnet allocated to PT. The router also has split tunneling enabled to minimize unnecessary traffic over the VPN link, and uses many to one NAT for traffic that does not go over the VPN link. The entire PT subnet is only advertised through from the main campus ISP, not the OpenBSD firewall. As a result, the end stations are potentially reachable from the Internet at large, but only through the VPN link, which means they must go through the full campus firewall first. For the purposes of this audit, we will assume that the campus firewalls are secure.

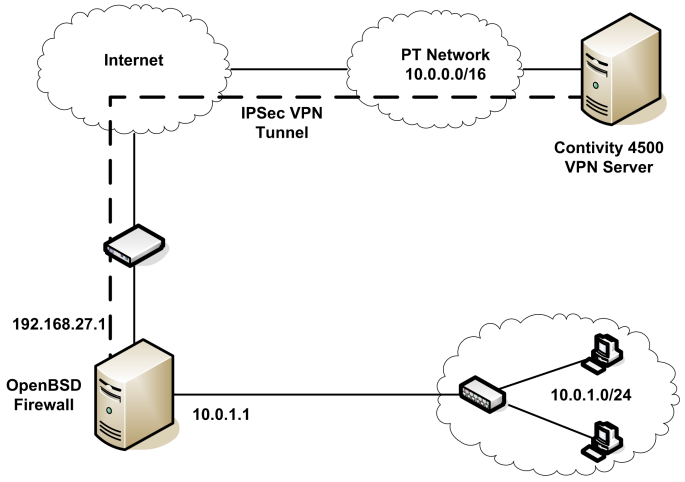

Figure 1: Network Diagram

2.2 Risk

This system is responsible for performing routing, firewall, and VPN endpoint functions. While it does not directly provide any service to any business critical systems, it frequently supports management of critical servers and network infrastructure by providing secure connectivity. This means that it will often be responsible for securing critical information in transit across the Internet that would otherwise be sent in clear text form, including passwords, SNMP community strings, and sensitive configuration files.

Category	Risk	Likelihood	Severity	Consequences
Denial of Service	Network is unable to communicate with Internet	Medium	Low	Since this system does not support any business critical functions, the consequences of being offline are minimal.
Tunnel Not Properly Encrypted	Any sensitive traffic transmitted over VPN tunnel will be vulnerable to sniffing	Moderate	High	Anyone with control over any intermediate networks can view potentially sensitive data.
Power Outage	All systems offline	Moderate	Low	None of the systems will be able to communicate with the Internet or PT. This is a low severity situation because none of the systems on this network are critical to the operation of PT.
System Compromise	Attacker is able to gain control of or execute arbitrary code on the firewall	Low	High	Attacker could use system for further attacks, including but not limited to password sniffing and launching attacks on PT network.

System Compromise	Attacker is able to intercept sensitive data to, from, or passing through the firewall	Low	High	Sensitive data passing through this firewall could potentially be used to gain further access on critical servers and network infrastructure.

2.3 Current State of Practice

There currently exists no written formal security policy for this system. Instead, the items here were gathered from general unwritten policy, best practice, and publicly available auditing checklists. Searching the web using Google revealed no checklists designed specifically for OpenBSD, so other more general checklists were adapted for use here.

Since no formal policy exists for this sytem, these general policy guidelines were used in selecting and creating the checklist items.

- All critical data must be backed up on a regular schedule.
- This system is intended to provide IP connectivity, a secure VPN tunnel, and DHCP for clients in the private network. Any ports not related to these services or management of the system itself should not be accessible.
- All management must be done through an encrypted, authenticated secure channel.
- All communication between the OpenBSD firewall or any systems behind it and the PT network must be securely encrypted.
- All security patches must be applied. New updates must be checked for an applied on a regular schedule.

Each item in the actual checklist references the source. Here are a few of the more useful sources, both for checklist items and examples for general policy.

Source	**Description**
An Administrator's Report on Auditing a LEAF (Linux Embedded Appliance Firewall) System. Credeur	GSNA Practical. Provided useful examples.
Auditing the S-Box Safe SOHO VPN/Firewall An Auditors Perspective. Skovfoged	GSNA Practical. Provided useful examples.
SANS Institute Top 20 Vulnerabilities. SANS	Provided several general checklist items.
Naval Surface Warfare Center	Provided firewall and UNIX specific checklists.

In addition to the operating system utilities such as `netstat` and `ps`, several useful auditing and analysis utilities were used.

Tool	**Description**	**URL**
Nessus	Network vulnerability scanner.	`http://www.nessus.org/`
John the Ripper	Cross platform password brute force cracking tool.	`http://www.openwall.com/john/`
nmap	Port scanning utility.	`http://www.insecure.org/nmap`
ngrep	Regular expression based network sniffer.	`http://ngrep.sourceforge.net`

3 Create an Audit Checklist

3.1 Introduction

Since no written security policy exists for this system, all tests described in this checklist are based upon other existing checklists or best practice. The tests are designed to be as objective as possible.

The majority of the operating systems tests were gathered from generic Unix checklists published by the Naval Surface Warfare Division, as no OpenBSD specific checklists were found to exist. This is most likely a result of the fact that the OpenBSD project takes a very proactive stance on ensuring that OpenBSD installs are by default secure. The OpenBSD projects security statement at `http://www.openbsd.org/security.html` states

> To ensure that novice users of OpenBSD do not need to become security experts overnight (a viewpoint which other vendors seem to have), we ship the operating system in a Secure by Default mode. All non-essential services are disabled.

Also extremely useful in the preparation of this checklist were the SANS Top 20 Vulnerabilities, and several previous GSNA Practical assignments, especially those by Skovfoged and Credeur. All checklist items specify the source when applicable.

3.2 Checklist

3.2.1 Firewall Items

1 **Test For Unnecessary Network Ports**

Reference	Naval Surface Warfare Center
Risk	Unnecessary open ports indicate that unnecessary services are available. These services represent potential vulnerabilities, and should be closed.
Compliance	All open ports must be identified as providing a service that is required.
Testing	Perform a scan with nmap.
Objectivity	Objective.

2 **Filter Illegal IP Traffic**

Reference	John Wack
Risk	Any such traffic is either an unintentional misconfiguration or an intentional spoof or attack. Not blocking this traffic may allow the intentional attacks to penetrate, or already compromised machines to continue to propagate attacks to external machines.
Compliance	All illegal traffic must be blocked. This includes any traffic with a source or destination address of the loopback network, any RFC 1918 network, directed broadcast, a multicast source address, or any source routing information.
Testing	Generate a sample of each instance of illegal traffic while a network sniffer is capturing. Verify that the traffic is not passed by the firewall.
Objectivity	Objective.

3 **Ingress Filter Private Network Source Addresses**

Reference	Best Practice
Risk	The private network addresses should only ever appear as a source in outgoing traffic, and a destination in outgoing traffic. Not blocking traffic from the external side that has the private network as a source may allow spoofed attacks to penetrate.
Compliance	Any traffic entering an external interface with a source address of the private network should not be forwarded.
Testing	For each external interface, from a machine connected to that interface, generate traffic with a source address and destination address in the private network range while a network sniffer is capturing. Examine the sniffer logs and verify that the traffic was not passed.
Objectivity	Objective.

4 **Ingress Filter Invalid Destination Addresses**

Reference	Best Practice
Risk	Any traffic with a destination address other than the firewall or a system in the private network range is invalid, and may be part of an attack. Not blocking this traffic may allow these attacks to penetrate.
Compliance	Any traffic entering an external interface with a destination address other than the firewall itself or the private network range must not be forwarded.
Testing	From an external machine, generate traffic with a destination address that is neither the firewall itself or in the private network range while a network sniffer is capturing. Examine the sniffer logs and verify that the traffic was not passed.
Objectivity	Objective

5 **Egress Filter Invalid Source Addresses**

Reference	Best Practice
Risk	Any traffic received on the internal interface with an address that is not in the private network range is the result of a misconfiguration or an attempted spoof or attack. Not blocking this traffic may allow these attacks to propagate to other networks.
Compliance	Any traffic received on the internal interface that does not have address within the private network range must not be forwarded.
Testing	Generate traffic from a machine connected to the internal network interface while a sniffer is capturing on the external interface. Examine the sniffer logs to verify that the traffic was not passed.
Objectivity	Objective.

6 **No Information is Leaked via ICMP**

Reference	SANS
Risk	ICMP messages can inadvertently leak information about the network, including but not limited to what network ports are explicitly filtered, what IP addresses are in use, and the network topology.
Compliance	All ICMP traffic that is not critical to normal operations must be blocked.
Testing	Send traffic that would normally generate an ICMP response, such as a ping request. No response should be generated.
Objectivity	Objective.

7 **All Blocked Traffic is Logged**

Reference	Best Practice
Risk	Records of unauthorized traffic act both as an indicator of attacks, and as an audit trail in the case of successful attacks. If logging is not properly enabled, this important information will be lost.
Compliance	All traffic that is blocked must be logged to the sytem log facility.
Testing	Generate traffic known to be blocked. Examine the system logs and verify that the traffic was logged, including at a minimum the source and destination IP, protocol type (UDP/TCP/ICMP), and (if applicable) source and destination ports.
Objectivity	Objective.

3.2.2 Operating System Items

8 **All Accounts Are Authenticated**

Reference	Naval Surface Warfare Center
Risk	An unauthenticated account would allow an attacker to gain access to a local account. Even if the account is restricted, such a break in would greatly increase exposure by allowing the attacker to execute arbitrary code on the system.
Compliance	All accounts must be disabled or require a password.
Testing	Examine the `/etc/password` and `/etc/master.passwd` files. All accounts must either be disabled or have a password set. If all accounts appear to be authenticated, continue by attempting to log in to each account with a blank password. All attempts should fail.
Objectivity	Objective.

9 **All Passwords Are Stored Encrypted**

Reference	Naval Surface Warfare Center
Risk	Any passwords stored unencrypted are vulnerable to being leaked to unauthorized parties, making break ins trivial.
Compliance	All passwords must be stored only in encrypted form, never in plain text.
Testing	Temporarily set the password of account to a known string. Examine the password store and verify that the string does not appear in plain text form anywhere.
Objectivity	Objective.

10 **Encrypted Passwords Are Not World Readable**

Reference	SANS
Risk	If an attacker is able to gain access to the encrypted passwords, they are vulnerable to being cracked through a brute force password guessing utility.
Compliance	The encrypted passwords must not be stored in the world readable `/etc/passwd` file, only in the protected `/etc/master.passwd` file.
Testing	Examine the `/etc/passwd` and `/etc/master.passwd` files. The `/etc/passwd` entry for each account should contain a simple placeholder for the password field, and the corresponding `/etc/master.passwd` entry should contain encrypted data for all non-disabled accounts. The `/etc/master.passwd` file must not be world readable.
Objectivity	Objective

11 **Trivial Passwords Are Rejected**

Reference	SANS
Risk	Trivial or easily guessable passwords increase the likelihood that an attacker will be able to guess the password and gain unauthorized access to the system.
Compliance	All passwords must be sufficiently complex that they are not easily guessable.
Testing	Attempt to set the password of a user account to several trivial passwords. They should be rejected.
Objectivity	Semi-objective. While it can objectively be determined that a specific example of a weak password was rejected, this does not guarantee that a different weak password could not have been picked.

12 **Existing Passwords Are Not Trivially Crackable**

Reference	SANS
Risk	Trivial or easily guessable passwords increase the likelihood that an attacker will be able to guess the password and gain unauthorized access to the system. While the system configuration should prevent users from setting trivial passwords, these restrictions can be bypassed either by the administrator or by using other password management utilities that do not obey these restrictions if installed. This test will attempt to verify this has not happened.
Compliance	All passwords must be sufficiently complex that they are not easily guessable.
Testing	Perform an analysis of the password file with the semi-intelligent brute-force password guessing utility John the Ripper.
Objectivity	Semi-objective. While it can objectively determined that a password is sufficiently strong as not to be guessed with this particular utility, this does not guarantee that another utility that does or will in the future exist can not easily guess the password.

13 **File Integrity Checker is Installed and Used**

Reference	Naval Surface Warfare Center
Risk	Without a file integrity checker, important modifications to system files may go unnoticed.
Compliance	Ensure that a strong file integrity checker, such as tripwire or AIDE, is installed and automatically run on a regular basis.
Testing	Demonstrate that a strong file integrity checker is installed, configured, and scheduled to run automatically on a regular basis.
Objectivity	Objective.

14 **All Vendor Security Patches are Regularly Applied**

Reference	Naval Surface Warfare Center
Risk	Any missing security patches from the vendor will leave a possibly exploitable security hole open.
Compliance	All available security patches from the sytem vendor must be installed.
Testing	The OpenBSD Project only releases security updates in source code form, never in binary. While this makes it easier to demonstrate that a given patch does not contain any trojan code, it also has the negative side effect of making it difficult to validate which patches are installed. Rather than attempting to prove a relationship between source code patches and binary releases, we will use the binary patch files from the Binpatch Project (Garrido) to compare against.
Objectivity	Objective.

15 **All Failed Login Attempts are Logged**

Reference	Naval Surface Warfare Center
Risk	Failed login attempts, particularly repeated ones, are often an indication of an attempted attack. By logging them, the administrator can be alerted to the threat.
Compliance	All failed login attempts must be logged.
Testing	Perform several login attempts. Examine the system logs and verify the attempts appear.
Objectivity	Objective.

16 **All User Login and Logout Events Are Logged**

Reference	Naval Surface Warfare Center
Risk	In the event that any valid user account is compromised, these login and logout events will form an audit trail that is essential to recreating the trail of an attacker. In some circumstances, they can even be the initial indication that an account has been compromised.
Compliance	All user login and logout events must be logged.
Testing	Perform successful login and logouts. Examine the sytem logs and verify the events appear.
Objectivity	Objective.

3.2.3 Network Service Items

17 **Account Authentication is Done in Such a Way as to Prevent Eavesdropping**

Reference	Naval Surface Warfare Center
Risk	If authentication is not secured, an eavesdropper could potentially gain unauthorized access to the system.
Compliance	All authentication must be encrypted.
Testing	Attempt a login with a specific username and password while a network sniffer is capturing. Examine the capture logs to ensure that neither the username nor password appear in plain-text in the data stream. This must be repeated once for each available login method.
Objectivity	Objective.

18 **Ensure VPN Tunnel is Properly Encrypted**

Reference	Best Practice
Risk	If the VPN tunnel is not encrypted, sensitive information may be exposed to potential eavesdropping.
Compliance	Ensure that data sent over the VPN tunnel is not visible in its plain-text form in transit.
Testing	Perform an action that will transmit known plain-text, such as retrieving a known URL, while a network sniffer is capturing. Examine the capture logs to ensure that the plain-text does not appear in the data stream.
Objectivity	Objective.

19 **No Anonymous Access Allowed**

Reference	Naval Surface Warfare Center
Risk	This sytem is not intended for any use by any individuals that are not explicitly authorized. Any anonymous access will allow unauthorized individuals access.
Compliance	All available services must be authenticated.
Testing	For each available service, attempt to log in or utilize the service using anonymous or unregistered credentials. Verify that the request is rejected.
Objectivity	Objective.

20 **No Open DHCP Pool**

Reference	Best Practice
Risk	A DHCP server can be configured either to hand out leases to all machines that request one, or to only hand out addresses to machines whose ethernet address have been registered with the server beforehand. While setting a DHCP server to the restricted mode will not prevent a rouge machine attached to the network from hard coding an IP address, leaving it in open mode will make it that much easier for the attacker.
Compliance	All DHCP pools must be configured to allow only known clients, and deny unknown clients.
Testing	Connect a machine with an ethernet address that has not been registered with the DHCP configuration. Attempt to get an address via DHCP. This should fail.
Objectivity	Objective.

21 **SSH Server Only Permits Version 2**

Reference	SANS
Risk	All 1 versions of the SSH protocol have known flaws which render them vulnerable to various attacks, including decryption of the session in transit. This could potentially lead to disclosure of any and all data transmitted over the SSH session, including sensitive data such as passwords and sensitive configuration files.
Compliance	The SSH server must be configured to refuse to negotiate a version 1 session, only a version 2 session.
Testing	The nessus vulnerability scanner includes a module that will identify all protocols versions supported by a given server. Only version 2 protocols should appear in the list. If the scan claims only version 2 protocols are supported, a connection will be attempted from an ssh client with version 1 specified on the command line will be attempted.
Objectivity	Objective

22 **No Clear-Text Services**

Reference	SANS
Risk	Any service which operates in plain text is inherently more vulnerable to a number of attacks. These include, at a minimum, sniffing, which could lead to disclosure of sensitive data, and man in the middle data injection attacks, which could lead to a remote attacker running arbitrary commands on the system.
Compliance	Whenever possible, all plain text service should be reconfigured to run encrypted or replaced with equivalents that run encrypted.
Testing	For each authorized service, run the service while a network analyzer is capturing. Review the sniffer logs to verify that no plain text is visible.
Objectivity	Mostly objective. While the determination of whether or not a service is running encrypted or plain text is objective, the decision to reconfigure an already established service to run encrypted, or to replace a service with an encrypted one, may be a subjective one.

23 **Sendmail Not Running in Daemon Mode**

Reference	SANS
Risk	There are two primary risks in running sendmail in daemon mode. The first, lesser risk is that a mis-configured sendmail can act as an open relay, allowing system resources to be stolen by spammers to send spam. Given the current extremely aggressive actions of spammers, this is a very likely risk. The second risk is less likely, but far more serious. While there are no pending vulnerabilities, sendmail history has been a large complex application, and has had many exploitable vulnerabilities. Not running sendmail in daemon mode makes any new vulnerabilities that may appear in the future much harder to exploit.
Compliance	Verify that sendmail is not running in daemon mode, listening on port 25.
Testing	Use the `netstat` command to ensure that no process is listening on TCP port 25.
Objectivity	Objective.

24 **SNMP is Disabled**

Reference	SANS
Risk	SNMP is a management protocol. Intended primarily for managing simple network devices, it has very weak authentication, defaults to poor passwords, and often has security holes. On servers, it is rarely even capable of actually performing management tasks without extensive configuration, and instead only services as a potential information leak to intruders at best, and as an exploitable vulnerability at worst.
Compliance	The system must not respond to any SNMP requests.
Testing	Use the `netstat` command to verify that no process is listening on any of the SNMP ports.
Objectivity	Objective.

3.2.4 Miscellaneous Tests

25 **Log Files Reviewed Regularly**

Reference	Naval Surface Warfare Center
Risk	If the log files are not monitored regularly, critical system events such as reports of hardware failures or suspicious events indicating an attack can go unnoticed for an indefinite length of time.
Compliance	Log file should be summarized and emailed or otherwise presented in an easily reviewable form on a daily basis.
Testing	Present a sample daily summary of the system logs.
Objectivity	Objective.

26 **System is Physically Secured**

Reference	Best Practice
Risk	If the system is not physically secured, it is vulnerable to theft. This will result in loss not only off the physical property, but also of any sensitive information stored on the machine, including but not limited to user credentials.
Compliance	The physical system must be in a facility that is adequately secured and monitored at all times.
Testing	Verify that the facility is monitored at all times, and locked whenever practical.
Objectivity	Subjective. Precisely what constitutes “adequate” will vary depending upon the cost of equipment, sensitivity of the data stored, and what resources are available.

27 **System Has Been Scanned With a Vulnerability Scanner**

Reference	Naval Surface Warfare Center
Risk	The total collection of known vulnerabilities is far too expansive to be reliably tested manually. Use of an automated scanner with an updated vulnerability list greatly reduces the possibility that one will be missed.
Compliance	The system has been thoroughly scanned with a vulnerability scanner, and any problems found by the scanner have been fixed or verified to be a false positive.
Testing	Perform a full scan of the system using the nessus vulnerability scanner.
Objectivity	Mostly objective. The verification of problems found by the scanner as false positives may be a subjective process in certain cases, depending upon the specific problem. There is also a possibility that a vulnerability may by list, no list of vulnerabilities can be guaranteed to be comprehensive

28 **System Has a Backup Power Source**

Reference	Best Practice
Risk	Without backup power, any loss of power - even a brief brownout - will mean a loss of connectivity until after power is restored. It also greatly increases the chance of data loss due to an unclean shutdown, and hardware damage due to fluctuations in power quality.
Compliance	The system power must be provided through a UPS with sufficient capacity to provide at least 10 minutes of run time.
Testing	Examine the hardware and verify that the system is plugged into a UPS. If the system is not, this is considered a failure. If the system is, proceed to simulate a power failure by disconnecting the UPS from its incoming power for at least ten minutes. The system should not lose power.
Objectivity	Objective.

29 **All Critical Data is Backed Up Regularly**

Reference	Best Practice
Risk	Unless a backup policy is in place and being followed, a system failure or could cause permanent data loss. In the best case, this requires that the system be reinstalled and reconfigured from scratch; in the worst case, critical data is permanently lost.
Compliance	A backup system, such as a tape drive or CD writer, must be available either locally or via network. Backups must be made and verified to this on a regular schedule.
Testing	Examine and manually verify at least one full cycle of backups.
Objectivity	Objective.

4 Audit Evidence

4.1 Introduction

For the purposes of auditing this system, three computers were placed at key points in the network infrastructure. Two computers were added to the local network. One was a RedHat 9 system installed behind the firewall, acting as a client. The second was a Windows XP machine, installed in front of the firewall, in the same ISP assigned IP address range. The third machine was also a RedHat 9 system installed in the PT network behind the Contivity firewall.

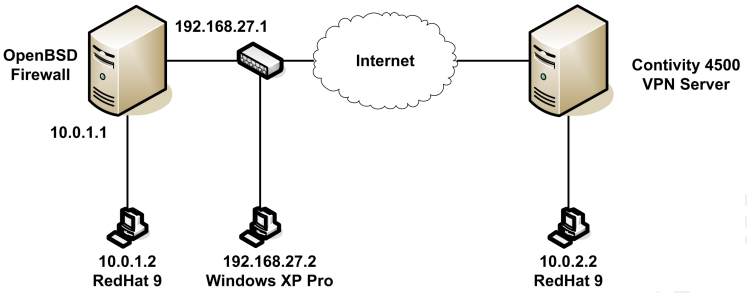

Figure 2: Testing Network Diagram

The two RedHat systems both had nmap, nessus, and ngrep installed for probing and analysis. The Windows XP system only had ngrep installed for passive analysis. It also had a route to 10.0.1.0/24 with a gateway of 192.168.27.1 added in attempt to bypass the PT campus firewall. The RedHat machine at PT was also used to run John the Ripper, as it had the most powerful CPU out of all available machines.

A very restricted list of services was used to determine the allowed ports list.

- Public Interface
  - SSH
  - IPSec
- Private Interface
  - SSH
  - DHCP Server
  - NAT

4.2 Checklist Results

1 **All Vendor Security Patches Applied Regularly**

Test	14

Test Results	The standard method of applying patches to an OpenBSD system is to download the full distribution source code, manually download and apply any patches that have not already been integrated, manually compile and then install the resulting updated binaries. While this method may appeal to those paranoid about what their vendor is putting into patches, it does not lend itself very well to auditing exactly what patches are installed on a given system. Even if a system administrator is diligent in keeping a logbook, there is still no way to provably show that the binaries have a particular source code patch applied without extensive analysis.
	As an alternative, this system is being patched with binary patches provided by the Binary Patches for OpenBSD project. This project takes the source code updates released from the main OpenBSD project, compiles them, and releases archives of only those files that have changed. This provides us with a relatively trusted source of binary updates that we can compare the installed files in the system against.
	The actual check was performed using the custom written `check-patches` script. The contents of the script are available in Appendix A. A transcript of the session follows.
	
	`bash-2.05b# ./check-patches -f -c`
	`Using arch -> i386 release -> 3.4`
	`Checking for and retrieving updates from http://www.openbsd.org.mx/pub/binpatch/`
	`Downloaded files - validating MD5 Checksums`
	`All checksums passed - extracting all patch files`
	`binpatch-3.4-i386-002.tgz`
	`binpatch-3.4-i386-003.tgz`
	`binpatch-3.4-i386-004.tgz`
	`binpatch-3.4-i386-005.tgz`
	`binpatch-3.4-i386-006.tgz`
	`binpatch-3.4-i386-007.tgz`
	`binpatch-3.4-i386-008.tgz`
	`binpatch-3.4-i386-009.tgz`
	`Files extracted - performing file comparison`
	`Done`
	
	In addition, the script is configured to run nightly as a cron job. An example of the nightly email report follows.
	
	`From: Charlie Root <root@bsdfw.pt.edu>`
	`To: root@bsdfw.pt.edu`
	`Subject: bsdfw.pt.edu check-patches output`
	
	`Using arch -> i386 release -> 3.4`
	`Checking for and retrieving updates from http://www.openbsd.org.mx/pub/binpatch/`
	`No new binpatch files found`
	`Done`

Conclusion	Pass. The output of the script does not show that files differ from those in the binpatch files, indicating all patches have been applied.

2 **Existing Passwords Are Not Trivially Crackable**

Test	11

Test Results	The password cracking utility John the Ripper was run on the password database. The first run was performed in "single" mode, in which the GECOS data was used to seed the guesses. This attempted to use strings such as the login, the users first or last name, plus other variations as the password. The following is a transcript of the session.
	
	`$ john -single passwd.1`
	`Loaded 2 passwords with 2 different salts (OpenBSD Blowfish [32/32])`
	`$ john -show passwd.1`
	`0 passwords cracked, 2 left`
	
	The second run was performed against a pre-existing word list. This word list was compiled in advance by the Openwall project. The following is a transcript of the session.
	
	`$ john -w:all passwd.1`
	`Loaded 2 passwords with 2 different salts (OpenBSD Blowfish [32/32])`
	`$ john -show passwd.1`
	`0 passwords cracked, 2 left`

Conclusion	Pass. Both sessions indicate that no passwords were successfully cracked.

3 **SNMP is Disabled**

Test	24

Test Results	The `netstat` command was used to list all open ports.
	
	`bash-2.05b# netstat -f inet | grep snmp`
	`bash-2.05b#`

Conclusion	Pass. The `netstat` command did not list any open ports listening associated with SNMP.

4 **System Has Been Scanned With a Vulnerability Scanner**

Test	27
Test Results	Several issues were found. Following is a brief summary. A full report of all items found by the nessus scan is attached in Appendix B. • SSH supports version 1 protocol • Daytime port is open • BIND port is open • Ident port is open • TCP Packets with SYN and FIN flags set are not discarded
Conclusion	Fail. While the majority of these items are not considered critical items by the nessus scan itself, they indicate failure of other test items, specifically tests 1 and 21.

5 **Test For Unnecessary Network Ports**

Test	1

Test Results	Two scans were performed with the `nmap` utility. One was directed at the public interface, the second at the private interface. All ports not included here were either in the closed state or filtered state (ie, blocked by the firewall rules).
	The results of the public interface scan were
	
	`Port State Service (RPC)`
	`13/tcp open daytime`
	`22/tcp open ssh`
	`37/tcp open time`
	`53/tcp open domain`
	`53/udp open domain`
	`113/tcp open auth`
	`123/udp open ntp`
	`500/udp open isakmp`
	
	The results of the private interface scan were
	
	`Port State Service (RPC)`
	`13/tcp open daytime`
	`22/tcp open ssh`
	`37/tcp open time`
	`53/tcp open domain`
	`53/udp open domain`
	`67/udp open dhcpserver`
	`113/tcp open auth`
	`123/udp open ntp`
	`500/udp open isakmp`

Conclusion	Fail. Both interfaces have open ports 13 (daytime), 37 (time), 53 (DNS resolution), 113 (ident), and 123 (ntp), none of which are considered necessary.

6 **Encrypted Passwords Are Not World Readable**

Test	10

Test Results	Under a non-privileged account, an attempt was made to read the encrypted passwords in the `/etc/master.passwd` file.
	
	`bash-2.05b$ id`
	`uid=1000(fs) gid=1000(fs) groups=1000(fs), 0(wheel)`
	`bash-2.05b$ ls -al /etc/master.passwd`
	`-rw-------  1 root  wheel  1319 Jul  1  2003 /etc/master.passwd`
	`bash-2.05b$ cat /etc/master.passwd`
	`cat: /etc/master.passwd: Permission denied`
	
	The command failed due to insufficient permissions.

Conclusion	Pass. Only the administrative account has permissions to read the `/etc/master.passwd` file.

7 **Account Authentication is Done in Such a Way to Prevent Eavesdropping**

Test	17

Test Results	The nessus scan (Appendix B) indicates that the only available login service is ssh. All other login services such as telnet and rlogin are disabled. Therefore, ssh is the only services that requires testing.
	To test this, a login was attempted using a username of “username” and a password of “password”. As this login was attempted, the `ngrep` network sniffer was also running on the OpenBSD system itself, searching all traffic between the two machines for either of those strings appearing in plaintext. The `ngrep` sniffer will print out any packets that meet the specified criteria.
	The login attempt was performed.
	`$ ssh -l username bsdfw-priv.pt.edu`
	`username@bsdfw-priv.pt.edu's password:`
	`Permission denied, please try again.`
	The `ngrep` session is shown here.
	`$ sudo ./ngrep username|password src or dst bsdfw-priv.pt.edu`
	`interface: eth0 (10.0.1.0/255.255.255.0)`
	`filter: ip and ( src or dst bsdfw-priv.pt.edu )`
	`match: username|password`
	`####################################exit`
	`43 received, 0 dropped`
	The lack of any packets being printed indicates that the strings never appeared in plaintext form in the data stream.

Conclusion	Pass. Neither username nor password are transmitted in plaintext.

8 **SSH Server Only Permits Version 2**

Test	21

Test Results	A full nessus scan was performed, including iterating all supported SSH protocol versions.
	`. Information found on port ssh (22/tcp)`
	`The remote SSH daemon supports the following versions of the SSH protocol :`
	`. 1.33`
	`. 1.5`
	`. 1.99`
	`. 2.0`
	The complete results of the nessus scan are available in Appendix B.

Conclusion	Fail. The test indicates that versions 1.33 and 1.5, both of which are known to have vulnerabilities, are enabled on the server.

9 **System Has a Backup Power Source**

Test	28
Test Results	The system was examined and verified to be plugged into an APC model Smart UPS 650. The power cord of the UPS was then removed from its wall outlet for a period of ten minutes while being observed for any signs of failure. The system stayed up for the full ten minutes and resumed normal operation when plugged back into the wall outlet.
Conclusion	Pass. The system proved capable of remaining operational for a full ten minute power outage

.

10 **All Critical Data is Backed Up Regularly**

Test	29
Test Results	Upon examination, not backup mechanism was found, either to a local storage medium or to a remote backup system.
Conclusion	Fail.

11 **System is Physically Secured**

Test	26
Test Results	The system is kept inside a locked residence. All inner and outer doors are locked unless someone is present, in which case the inner doors are unlocked, but the outer doors are still kept locked.
Conclusion	Pass. The system is kept in a reasonably secure area.

12 **File Integrity Checker is Installed and Used**

Test	13
Test Results	While the default OpenBSD installation does include a crude file integrity check system, it relies purely on non-verifiable data such as timestamps and comparing against unsecured previous versions of configuration files. No evidence was found of a more comprehensive integrity system, such as AIDE or tripwire.
Conclusion	Fail. No suitable system was in use.

13 **Ensure VPN Tunnel is Properly Encrypted**

Test	18

Test Results	To test this, the RedHat system behind the OpenBSD firewall sent known plain text traffic to another system in the PT network, specifically, an `index.html` file on a web server. While this request was sent, the Windows XP system was running the `ngrep` network monitor, looking for any instances of the string “html” in the data stream.
	
	`c:\temp>ngrep -i html`
	`interface: \Device\NPF_{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}`
	`match: html`
	`#######exit`
	`0 received, 0 dropped`

Conclusion	Pass. Since the request succeeded, but the string did not appear in the data stream, it must have been encrypted and sent over the VPN IPSec tunnel.

4.3 Residual Risk

Overall, there is relatively little residual risk. All valid communications channels appear to be properly authenticated and encrypted. All operating system patches are applied, so there are no known vulnerabilities, either from remote or via local accounts. Password security appears strong. There is still room for improvement, though. There are several areas where the control objectives are not met that should definitely be

addressed. In addition, there are always further changes above and beyond the polices used here that could be made to enhance the overall system integrity.

- Unneeded Services Still Enabled

  The nmap (result 5) and nessus (result 4) scans still indicate that there are a number of unneeded services enabled. These should be disabled if possible, or the ports firewalled if the services cannot be disabled or restricted to the private network only.

- No Backup Solution in Place

  There is currently no backup solution in place. However, there is no data on this system beyond configuration and the base operating system, both of which are practical to recreate in case of total system failure. Given that there is insufficient bandwidth to perform network based backups back to the available facilities on the PT campus, and the cost of adding an entire backup system including a drive and media would be prohibitive for backing up a single computer, it is highly unlikely that a backup system will be installed. This will require a strict policy that no important data reside solely on this machine - it must be treated as temporary data storage at most, never permanent.

- No Filesystem Integrity Checker Installed

  No evidence was found of any filesystem integrity checker, such as tripwire or AIDE. Without such a system, there is no reliable way to detect filesystem modifications due to any system attacks. Even if such an attack is detected via other means, there is no way to reliably detect which files were modified. Such a system should definitely be installed.

- Vulnerable SSH Protocols Enabled

  The SSH server has version 1 protocols enabled. This is a security risk because those protocols have known vulnerabilities which can lead to complete decryption of the data stream in transit, leading disclosure of sensitive information including passwords. The server should be reconfigured only to allow version 2 protocol sessions.

- Network Intrusion Detection System

  Although strictly outside the scope of this audit, a network intrusion system such as snort is recommended. This would gain the added benefit of providing monitoring not only for the host itself, but for all clients in the private network behind the host.

- Modem Link for Backup

  The PT network includes a limited modem pool. A modem could be installed and configured to autodial in case of network failure or denial of service attack. This would add redundancy for two scenarios. In case the local Internet link were lost, connectivity to the Internet, and more importantly the PT network, would still be available. Also, in case the PT network lost Internet, the modem could be used to log in for out of band management for troubleshooting.

4.4 Auditability

Overall this system is highly auditable. While there do not exist OpenBSD checklists with the same specificity and depth as, for example, Windows 2000, there is a wealth of general UNIX resources that readily apply to OpenBSD with little trouble. A complete list of all network and process states are readily available, unlike many “black box” router/firewall devices that do not offer a shell on the underlying operating system. All system configuration is in readily accessible standard formats and file locations. In addition, the OpenBSD ideal of minimizing the list of what is running on a default install greatly reduces the list of items that must be investigated.

In addition, the fact that OpenBSD is an open source operating system gives much greater transparency. A much wider community is readily available to search for bugs and security holes, fix those that are found, and watch for any attempts at inserting trojan code into the operating system itself. This last potential threat is not an unfounded one. Recently, an attacker managed to insert a subtle trojan into the code of the Linux

kernel (Andrews). The attempt was very nearly successful, but was quickly caught and removed before it could propagate. No attempt was made to cover up the facts of the attack, as would be the case with a large corporation with a reputation to project. Such events may or may not be happening with closed source commercial products - there is simply no way to tell either way.

There is one significant failing of OpenBSD with respect to auditability, though. The OpenBSD Project does not release any operating system patches in binary form, only in source code. While this does guarantee that it is very difficult for any malicious source code to slip in, this makes it impossible to examine an arbitrary system and discover what the patch level is without extensive additional infrastructure. Each system administrator must maintain his or her own trusted source tree, build environment, compiled binary files, and a secure authenticated binary update distribution system. Ideally, OpenBSD will start deploying software in a manner more similar to RedHat. All files on a RedHat system can be compared to a list of sizes and checksums in the local RPM database. If the database is suspect, the original RPM package files, which have been cryptographically signed by RedHat, can be used instead. OpenBSDs inability to identify the source of operating system binaries makes deploying OpenBSD in an environment requiring a strong audit policy very difficult without a lot of extra work.

,

5 Risk Assessment

5.1 Summary

The checklist of security items has been followed, and a representative selection of the results detailed in the previous section. This section will examine the risks found in the checklist results.

Out of the 29 total tests, 5 were found to be in an unacceptable state. Most of the tests were in the network services, plus one test regarding the status of regular backups. All of the network filtering rules were found to be working properly as outlined.

5.2 Background

1 **System Has Been Scanned With a Vulnerability Scanner**

Test 27 Result 4

Risk In addition to the SSH protocol version (addressed in item 2), there were several items listed in the Nessus scan (Appendix B).

- BIND port is open
  There are potential overflows in the BIND daemon. If an attacker were to exploit one, he could potentially take full control of the system, including intercepting all data going through it. Since providing DNS services is not a required function of this system, there is no reason for it to be running.

- Daytime port is open
  At a minimum, this represents and unnecessary information leak. While revealing the system time is not in and of itself a security risk, knowing the exact time stamp on the system can make certain malicious operations, such as guessing TCP sequence numbers, easier for an attacker. Requests to this port with a spoofed source address can also let an attacker use this system to launch a denial of service attack on a third party system.

- Ident port is open
  This daemon will reveal the user names of a user that has opened a given TCP connection. This will reveal the names of legitimate local user accounts, which will save an attacker the trouble of having to guess account names as well as passwords, thereby increasing the likelihood that an attempted break in be successful.

- TCP Packets with SYN and FIN flags set are not discarded
  By allowing these packets in, a scan from an outside machine that would normally be blocked by the firewall rules may be able to penetrate and gain privileged information about inside hosts in the private network.

2 **SSH Server Only Permits Version 2**

Test 21 Result 8	
Risk	The version 1 family of the SSH protocols are vulnerable to decryption of data while in transit (SANS 2003). This defeats the primary purpose of using SSH, which is to ensure that all data in the session is securely encrypted. Since this system is frequently used by a network administrator, decryption of this data by an eavesdropper could easily reveal highly sensitive data, including passwords and sensitive configuration files.

3 **File Integrity Checker is Installed and Used**

Test 13 Result 12	
Risk	Without a strong file integrity system, it is very difficult to reliably determine whether the contents of a filesystem are still in a known good state, or have been modified. This is important in detecting system break ins that often modify system binaries to add trojans and backdoors. After a break in has been detected, it is often the only way to determine the extent of the damage done by the attacker. Without such a system, the only reasonable way to ensure a system has been cleaned after a break in is to completely wipe and reinstall the operating system and all related software from a known good source.

4 **All Critical Data is Backed Up Regularly**

Test 29 Result 10	
Risk	Without regular backups, the system is vulnerable to data loss due to hardware failure, accidental deletion commands, and malicious hackers. All data must then be restored from the original installation source or manually recreated.

5 **Test For Unnecessary Network Ports**

Test 1 Result 5	
Risk	Each open network port indicates a service that is listening, and therefore a potential vulnerability. By closing any ports that are not required for the indented operation of this system, the risk can be minimized. Background item 1 includes more detailed information about the unnecessary network ports that were found open.

5.3 System Changes and Further Testing

1 **System Has Been Scanned With a Vulnerability Scanner**

Test 27 Result 4	
Risk	The nessus vulnerability scanner revealed several potential problems (see Appendix B).
Reccomendations	All extraneous services found should be disabled or filtered. All services that nessus found problems with should be reconfigured to close the specific problem.
Results	All extraneous services found in the nessus listing were disabled. The daytime, time, and auth services were disabled in the `inetd.conf` file. The DNS server was disabled in the `rc.conf` file. The SSH server was reconfigured only to disable version 1 sessions. The firewall ruleset was modified to explicitly discard any TCP packets with both the SYN and FIN flag bits set. The NTP daemon was reconfigured ignore all info packets. The full results of the repeated nessus scan are available in Appendix C.
Conclusion	The list of open services has been reduced to an acceptable list. Those services still open (ssh, ntp) have been adequately secured.

2 **SSH Server Only Permits Version 2**

Test 21 Result 8	
Risk	Version 1 of the SSH protocol is known to have several flaws, including being vulnerable to having a session decrypted in transit.
Reccomendations	Configure the SSH server to only accept version 2 sessions.
Results	The configuration file `/etc/ssh/sshd_config` was modified. The line `Protocol 2` was added to restrict the permitted SSH protocol versions. The nessus scan was repeated, including the SSH protocol check.

```
. Information found on port ssh (22/tcp)


   The remote SSH daemon supports the following versions of the
   SSH protocol :

     . 1.99
     . 2.0
```

This indicates that only the 1.99 protocol is enabled from the version 1 suite. This version is an early version of what is currently the version 2 protocol, and does not share the same vulerabilities as versions 1.3 and 1.5. An attempt was then made to connect to the SSH server with version 1 protocol to ensure that actual connection attempts are rejected.

```
$ ssh -1 bsdfw.pt.edu
Protocol major versions differ: 1 vs. 2
```

Conclusion	The SSH server is now properly restricted to version 2 sessions only.

3 **Test For Unnecessary Network Ports**

Test 1 Result 5	
Risk	Unnecessary open ports increase the number of potential vulnerabilities.
Reccomendations	Any ports not related to a service required for the operation of this system should be closed, either by disabling the relevant service or adding a firewall rule to filter the port.
Results	All extraneous services were disabled, and the `nmap` scan was repeated with the following results, on the private interface

```
Port       State       Service (RPC)
22/tcp     open        ssh
67/udp     open        dhcpserver
123/udp    open        ntp
500/udp    open        isakmp
```

and on the public interface

```
Port       State       Service (RPC)
22/tcp     open        ssh
123/udp    open        ntp
500/udp    open        isakmp
```

While the NTP port is still open, the nessus scan (result 4) showed that it does not respond to information request packets anymore.

Conclusion	All ports still open are required for services intended to be operating on this system.

4 **File Integrity Checker is Installed and Used**

Test 13 Result 12	
Risk	The lack of a strong file integrity verification system makes it extremely difficult to be sure that the important files on a given system have not been compromised. Such a system is very important both in detecting the results of a successful attack, and determining the extent of damage during a forensic analysis.
Reccomendations	A file integrity verification package should be installed, configured, and scheduled to run at regular intervals. Good choices include AIDE or tripwire.
Results	The AIDE integrity system was installed from the OpenBSD ports tree. The database was initialized using the default configuration.

```
bash-2.05b# aide --init

AIDE, version 0.10

### AIDE database initialized.
bash-2.05b# mv /var/db/aide.db.new /var/db/aide.new
bash-2.05b# aide --update
...
bash-2.05b# rm -f /var/db/aide.db
bash-2.05b# mv /var/db/aide.db.new /var/db/aide.db
bash-2.05b# aide --check

AIDE, version 0.10

### All files match AIDE database.  Looks okay!
```

To test that AIDE is properly operating, a new file `/sbin/badfile` was created. Since the `/sbin/` directory is being monitored by AIDE, this new file should be detected and flagged.

```
From: Charlie Root <root@bsdfw.pt.edu>
To: root@bsdfw.pt.edu
Subject: bsdfw.pt.edu aide output

AIDE found differences between database and filesystem!!
Start timestamp: 2004-02-15 19:19:36
Summary:
Total number of files=101211,added files=1,removed files=0,changed files=1

Added files:
added:/sbin/badfile
Changed files:
changed:/sbin
Detailed information about changes:

Directory: /sbin
  Mtime    : 2004-02-15 16:23:02              , 2004-02-15 18:42:58
  Ctime    : 2004-02-15 16:23:02              , 2004-02-15 18:42:58
```

Conclusion	AIDE correctly found the added file in the scheduled nightly run, and appears to be properly installed and operating.

5.4 System Justification

Only a single item was left in an unsatisfactory state, specifically, the lack of a backup solution, checklist item 29. As shown in result 10, this system currently has no backup solution of any kind installed. In the case of any kind of hardware failure, accidental deletion commands, or filesystem compromise from a system break in, the data loss would be far more difficult to recover from. All files would have to be reinstalled from the original source, or recreated manually.

Installing a backup solution would involve either adding hardware, such as a tape drive, or increasing the bandwidth of the DSL link to handle performing backups to a system on the PT network. Given the effort that would be involved in rebuilding this system from scratch, without any backups to restore from, versus purchasing and maintaining a backup system, it has been determined to be more cost effective to leave the system without backups. Note that this means that a strict policy of not using this system as primary storage of any important or non reproducible data. At most, it should be used as temporary storage for unimportant data.

A OpenBSD Binary Update Check Script

```
#!/bin/sh

force="no"
copy="no"

cd /var/spool/binpatches || exit 255

if ! [ -d root ] ; then
        mkdir root || exit 255
fi
if ! [ -d patches ] ; then
        mkdir patches || exit 255
fi

set -- `getopt fc $*`
          if test $? != 0
          then
                  echo 'Usage:'
                echo " -f   force check even if no new patches are found"
                echo " -c   automatically copy out of date files"
                  exit 2
          fi
          for i
          do
                  case "$i"
                  in
                          -f)
                                  force="yes"; shift;;
                          -c)
                                  copy="yes"; shift;;
                          --)
                                  shift; break;;
                  esac
          done

URL=http://www.openbsd.org.mx/pub/binpatch/ #3.4/i386/
REL=`uname -a | awk '{print $3}'`
ARCH=`uname -a | awk '{print $5}'`

echo "Using arch -> ${ARCH} release -> ${REL}"

cd patches
echo "Checking for and retrieving updates from ${URL}"
wget -o wget.log -mirror -nH -np --cut-dirs=4 ${URL}/${REL}/${ARCH}/

if [ ${force} = "yes" ] || grep -i saved wget.log | grep -v .listing | grep -q binpatch- ; then
        echo "Downloaded files - validating MD5 Checksums"
        if md5 -c MD5 | grep -v -q FAILED ; then
                echo "All checksums passed - extracting all patch files"
                for file in `echo binpatch-${REL}-${ARCH}*.tgz | sort` ; do
                        echo "    ${file}"
                        tar xpzf ${file} -C ../root
```

```
                done

                echo "Files extracted - performing file comparison"
                cd ../root
                for file in `find . -type f -print` ; do
                        if ! cmp -s ${file} /${file} ; then
                                echo "    ${file} out of date"
                                if [ ${copy} = "yes" ] ; then
                                        echo "        copying ${file}"
                                        cp -fp ${file} /${file}
                                fi
                        fi
                done
        else
                echo "MD5 checksum failed"
        fi
else
        echo "No new binpatch files found"
fi

echo "Done"
```

B Initial Nessus Scan Report

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 0
 - Number of security warnings found : 4
 - Number of security notes found : 12



TESTED HOSTS

 bsdfw.pt.edu (Security warnings found)



DETAILS

+ bsdfw.pt.edu :
 . List of open ports :
   o ssh (22/tcp) (Security warnings found)
   o daytime (13/tcp) (Security warnings found)
   o time (37/tcp) (Security notes found)
   o domain (53/tcp) (Security notes found)
   o auth (113/tcp) (Security warnings found)
   o general/tcp (Security warnings found)
   o domain (53/udp) (Security notes found)
   o ntp (123/udp) (Security notes found)
   o general/udp (Security notes found)

 . Warning found on port ssh (22/tcp)



    The remote SSH daemon supports connections made
    using the version 1.33 and/or 1.5 of the SSH protocol.

    These protocols are not completely cryptographically
    safe so they should not be used.

    Solution :
     If you use OpenSSH, set the option 'Protocol' to '2'
     If you use SSH.com's set the option 'Ssh1Compatibility' to 'no'

    Risk factor : Low

 . Information found on port ssh (22/tcp)
```

An ssh server is running on this port

. Information found on port ssh (22/tcp)

The remote SSH daemon supports the following versions of the
SSH protocol :

. 1.33
. 1.5
. 1.99
. 2.0

. Information found on port ssh (22/tcp)

Remote SSH version : SSH-1.99-OpenSSH_3.7.1

. Warning found on port daytime (13/tcp)

The remote host is running a 'daytime' service. This service
is designed to give the local time of the day of this host
to whoever connects to this port.

The date format issued by this service may sometimes help an attacker
to guess the operating system type of this host, or to set up
timed authentication attacks against the remote host.

In addition to that, the UDP version of daytime is running, an attacker
may link it to the echo port of a third party host using spoofing, thus
creating a possible denial of service condition between this host and
a third party.

Solution :

- Under Unix systems, comment out the 'daytime' line in /etc/inetd.conf
  and restart the inetd process

- Under Windows systems, set the following registry keys to 0 :
  HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime
  HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime

Then launch cmd.exe and type :

   net stop simptcp
   net start simptcp

To restart the service.

Risk factor : Low
CVE : CVE-1999-0103

. Information found on port time (37/tcp)

A time server seems to be running on this port

. Information found on port domain (53/tcp)

BIND 'NAMED' is an open-source DNS server from ISC.org.
Many proprietary DNS servers are based on BIND source code.

The BIND based NAMED servers (or DNS servers) allow remote users
to query for version and type information. The query of the CHAOS
TXT record 'version.bind', will typically prompt the server to send
the information back to the querying source.

The remote bind version is :

Solution :
Using the 'version' directive in the 'options' section will block
the 'version.bind' query, but it will not log such attempts.

. Information found on port domain (53/tcp)

A DNS server is running on this port. If you do not use it, disable it.

Risk factor : Low

. Warning found on port auth (113/tcp)

The remote host is running an ident (also known as 'auth') daemon.

The 'ident' service provides sensitive information to potential
attackers. It mainly says which accounts are running which services.
This helps attackers to focus on valuable services (those
owned by root). If you do not use this service, disable it.

Solution : Under Unix systems, comment out the 'auth' or 'ident'
line in /etc/inetd.conf and restart inetd

Risk factor : Low

```
   CVE : CAN-1999-0629

. Information found on port auth (113/tcp)


   An identd server is running on this port

. Warning found on port general/tcp



   The remote host does not discard TCP SYN packets which
   have the FIN flag set.

   Depending on the kind of firewall you are using, an
   attacker may use this flaw to bypass its rules.

   See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html
              http://www.kb.cert.org/vuls/id/464113

   Solution : Contact your vendor for a patch
   Risk factor : Medium
   BID : 7487

. Information found on port general/tcp


   Remote OS guess : OpenBSD 2.9-beta through release (X86)

   CVE : CAN-1999-0454

. Information found on port domain (53/udp)



   A DNS server is running on this port. If you do not use it, disable it.

   Risk factor : Low

. Information found on port domain (53/udp)


   The remote name server could be fingerprinted as being : ISC BIND 8.2




. Information found on port ntp (123/udp)


   It is possible to determine a lot of information about the remote host
   by querying the NTP (Network Time Protocol) variables - these include
   OS descriptor, and time settings.
```

```
    It was possible to gather the following information from the remote NTP host
     :

    version='ntpd 4.1.1c-rc1@1.836 Thu Nov  6 20:09:30 EST 2003 (1)',
    processor='i386', system='OpenBSD3.4', leap=0, stratum=3, precision=-17,
    rootdelay=67.125, rootdispersion=52.988, peer=37892,
    refid=128.194.254.9, reftime=0xc3d222f5.d9bd2fa0, poll=10,
    clock=0xc3d22350.b3f3e037, state=4, offset=26.778, frequency=-125.331,
    jitter=8.145, stability=0.104



    Quickfix: Set NTP to restrict default access to ignore all info packets:
     restrict default ignore

    Risk factor : Low

--------------------------------------------------
This file was generated by the Nessus Security Scanner
```

C Final Nessus Scan Report

```
Nessus Scan Report
------------------



SUMMARY

 - Number of hosts which were alive during the test : 1
 - Number of security holes found : 0
 - Number of security warnings found : 0
 - Number of security notes found : 5



TESTED HOSTS

bsdfw.pt.edu (Security notes found)



DETAILS

+ bsdfw.pt.edu :
 . List of open ports :
   o ssh (22/tcp) (Security notes found)
   o general/tcp (Security notes found)
   o general/udp (Security notes found)

 . Information found on port ssh (22/tcp)


    An ssh server is running on this port

 . Information found on port ssh (22/tcp)


    The remote SSH daemon supports the following versions of the
    SSH protocol :

      . 1.99
      . 2.0




 . Information found on port ssh (22/tcp)


    Remote SSH version : SSH-2.0-OpenSSH_3.7.1

 . Information found on port general/tcp
```

```
    Remote OS guess : OpenBSD 2.9-beta through release (X86)

    CVE : CAN-1999-0454

------------------------------------------------------
This file was generated by the Nessus Security Scanner
```

Works Cited

Address Allocation for Private Internets [online]. Available from World Wide Web: http://www.faqs.org/rfcs/rfc1918.html.

Google Web Search Engine [online]. Available from World Wide Web: http://www.google.com.

John the Ripper [online]. Available from World Wide Web: http://www.openwall.com/john/.

Nessus Vulnerability Scanner [online]. Available from World Wide Web: http://www.nessus.org/.

Nmap Network Scanner [online]. Available from World Wide Web: http://www.insecure.org/nmap/.

OpenBSD Project [online]. Available from World Wide Web: http://www.openbsd.org/.

OpenSSH Security [online]. Available from World Wide Web: http://www.openssh.org/security.html.

Openwall Project [online]. Available from World Wide Web: http://www.openwall.org/.

Snort Intrusion Detection System [online]. Available from World Wide Web: http://www.snort.org/.

Andrews, Jeremy. Linux: Kernel "Back Door" Attempt [online]. Available from World Wide Web: http://kerneltrap.org/node/view/1584.

Credeur, Brian. 2002 “An Administrator’s Report on Auditing a LEAF (Linux Embedded Appliance Firewall) System.”. Available from World Wide Web: http://www.giac.org/practical/GSNA/Brian_Credeur_GSNA.pdf.

Garrido, Gerardo Santana Gomez. Binary patches for OpenBSD [online]. Available from World Wide Web: http://www.openbsd.org.mx/~santana/binpatch.html.

John Wack, Jamie Pole,Ken Cutler. 2002 “Guidelines on Firewalls and Firewall Policy.”. Available from World Wide Web: http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf.

Naval Surface Warfare Center. Naval Surface Warfare Center Information Assurance Office [online]. Available from World Wide Web: http://www.nswc.navy.mil/ISSEC/.

Naval Surface Warfare Center. Generic Accreditation Form [online]. 1999. Available from World Wide Web: http://www.nswc.navy.mil/ISSEC/Form/AccredForms/acc_part2_generic.html.

Naval Surface Warfare Center. Risk Assessment for Firewalls [online]. 2001. Available from World Wide Web: http://www.nswc.navy.mil/ISSEC/Form/AccredForms/acc_part4_firewall.html.

Naval Surface Warfare Center. Unix Accreditation [online]. 2002. Available from World Wide Web: http://www.nswc.navy.mil/ISSEC/Form/AccredForms/acc_part2_unix.html.

Ritter, Jordan. Network Grep [online]. Available from World Wide Web: http://ngrep.sourceforge.net/.

SANS. SANS Top 20 Vulnerabilities [online]. 2003. Available from World Wide Web: http://www.sans.org/top20/.

Skovfoged, Erik. 2003 “Auditing the S-Box Safe@ SOHO VPN/Firewall An Auditors Perspective.”. Available from World Wide Web: http://www.giac.org/practical/GSNA/Erik_Skovfoged_GSNA.pdf.

Solar Designer. “Complete John the Ripper Wordlist.”. Available from World Wide Web: ftp://ftp.kaizo.org/pub/openwall/wordlists/all.gz.