The 60 Minute Network Security Guide

(First Steps Towards a Secure Network Environment)

Systems and Network Attack Center (SNAC)

Updated: May 15, 2006
Version 2.1

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

SNAC.Guides@nsa.gov

Change Control

Version	Date	Details
1.1	18 February 2002	Updated UNIX Section which starts on page 35. These updates where to fixes grammar and syntax
1.2	12 July 2002	Clarify reference of shareware product: Tripwire ASR, page 40
2.0	29 March 2006	Nearly all sections of the document were updated to reflect new releases and to remove references to deprecated versions.
2.1	15 May 2006	Format & grammatical changes.

Table of Contents

Introduction

During the last seven years the National Security Agency's Systems and Network Attack Center has released Security Guides for operating systems, applications, and network components that operate in the larger IT network. These security guides can be found on our web site at http://www.nsa.gov/snac. Many organizations across the Department of Defense have used these documents in the development of new networks and in securing existing IT infrastructures. This Security Guide addresses security a bit differently. Instead of focusing on a single product or component it covers a wide range of network elements with the notion of providing a terse presentation of those most critical steps that should be taken to secure a network. While intentionally not as complete as the totality of our other guides, our goal is to make system owners and operators aware of key actions that are especially useful as "force multipliers" in the effort to secure their IT network.

Security of the IT infrastructure is a complicated subject, usually addressed by experienced security professionals. However, as organizations increase their dependence on IT, a greater number of people need to understand the fundamentals of security in a networked world. This Security Guide was written with the less experienced System Administrator and Information Systems Manager in mind, to help them understand and deal with the risks they face.

Opportunistic attackers routinely exploit the security vulnerabilities addressed in this document. Information Systems Managers and System Administrators perform risk management as a counter against the multitude of threats and vulnerabilities present across the IT infrastructure. The task is daunting when considering all of their responsibilities. Security scanners can help identify thousands of vulnerabilities, but their output can quickly overwhelm the IT team's ability to effectively use the information to protect the network. This Security Guide was written to help with that problem by offering a focused presentation reflecting the experience gained via our research and our operational understanding of the DoD and other US Government IT infrastructures. It is intended that one can read this "60 Minute Network Security Guide" in around an hour.

This Security Guide should not be misconstrued as containing anything other than recommended security "best practices" and as such must be considered in the context of an organization's security policies. We hope that this document will equip the reader with a wider perspective on security in general and a better understanding of how to reduce and manage network security risk.

We welcome your comments and feedback. SNAC.Guides@nsa.gov

General Guidance

The following section discusses general security advice that can be applied to any network.

Security Policy

(This section is an abstract of the security policy section of RFC 2196, Site Security Handbook. Refer to this RFC [10] for further details.)

A security policy is a formal statement of the rules that people who are given access to an organization's technology and information assets must abide. The policy communicates the security goals to all of the users, the administrators, and the managers. The goals will be largely determined by the following key tradeoffs: services offered versus security provided, ease of use versus security, and cost of security versus risk of loss.

The main purpose of a security policy is to inform the users, the administrators and the managers of their obligatory requirements for protecting technology and information assets. The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization.

A good security policy must:

- Be able to be implemented through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods
- Be able to be enforced with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible
- Clearly define the areas of responsibility for the users, the administrators, and the managers
- Be communicated to all once it is established
- Be flexible to the changing environment of a computer network since it is a living document

Operating Systems and Applications: Versions and Updates

As much as possible, use the latest available and stable versions of the operating systems and the applications on all of the following computers on the network: clients, servers, switches, routers, firewalls and intrusion detection systems. Keep the operating systems and the applications current by installing the latest updates (e.g., patches, service packs, hotfixes), especially updates that correct vulnerabilities that could allow an attacker to execute code. Note that some updates may not be applied to the computer until a reboot occurs. The following applications should be given particular attention because they have been frequently targeted (e.g., by CodeRed, Melissa virus, Nimda): IIS, Outlook, web browsers (e.g. Internet Explorer, Mozilla Firefox), Adobe Acrobat, database servers (e.g. SQL Server, Oracle), media players (e.g. Windows Media Player, RealPlayer), BIND and Sendmail.

Know Your Network

Developing and maintaining a list of all hardware devices and installed software is important to the security of the IT infrastructure. Understanding software applications that are installed by default is also important (e.g., IIS is installed by default by SMS and SQL Server on Windows platforms). Although not thorough, a quick method for taking inventory of services running on the network is to port scan.

TCP/UDP Servers and Services on the Network

Scan the network for all active TCP/UDP servers and services on each computer in the network. Shut down unnecessary servers and services. For those servers that are necessary, restrict access to only those computers that need it. Turning off functional areas, which are seldom used but potentially have vulnerabilities, prevents an attacker from being able to take advantage of them. An application may install sample CGI scripts or other applications, which sometimes contain problems. As a general rule do not install sample applications in production systems.

Passwords

Passwords are a primary method used to control access to resources. Because authenticated access is seldom logged, a compromised password is a way to explore a system without causing suspicion. An attacker with a compromised password can access any resource available to that user.

Poor passwords or blank passwords are still a common occurrence on many networks. Many users still use dictionary words, hybrids, names, and default passwords. Additionally passwords less than 8 characters and passwords that are the same as the username are also frequently used. These types of passwords can be cracked within minutes or even seconds using any number of publicly available password crackers.

General guidelines for password security include:

- Passwords should be 12 or more characters in length on Windows systems.
- In older releases of some UNIX operating systems, a maximum of 8 characters was the maximum number of characters allowed. However, on more modern day UNIX systems passwords length is based upon the available algorithm (MD5, Blowfish, etc) residing on the systems. This gives the added benefit of maximizing the password length to 255 characters on some systems.
- Users should never share their passwords nor keep written passwords in an easily-accessible place (e.g. under a keyboard, on the computer monitor).
- Passwords should be difficult to guess and include uppercase, lowercase, special (e.g., punctuation and extended character set), and numeric characters. They should not include dictionary words or names.
- Users should not transmit passwords in cleartext (e.g. via Telnet or FTP)
- System administrators should crack passwords monthly to identify problems with weak passwords and to determine if the password policy is being followed. Password-guessing programs (e.g. “John the Ripper,'' “L0phtCrack,” and “Crack”) identify those users having easily guessed passwords. Because password cracking programs are very CPU intensive and can slow down the system on which it is running, it is a good idea to transfer the encrypted passwords (the dumped SAM database for Windows and the /etc/passwd and /etc/shadow files in UNIX) to a stand-

alone (not networked) system. Also, by doing the work on a non-networked machine, any results found will not be accessible by anyone unless they have physical access to that system. NOTE: Always obtain explicit and preferably written permission from the organization before running any password scanner/cracker.

- Passwords should be changed regularly (every 30 to 90 days). Set up password aging via Account Policy for Windows systems or the /etc/default/passwd file in SOLARIS. Some Linux releases use the 'charge' command to set up and modify the password aging requirements for users.

UNIX Password Recommendations

The following are UNIX-specific password recommendations:

- Passwords should be encrypted and stored in the /etc/shadow file (for some UNIX systems) with permissions set to 400 with ownership by root and group sys. The /etc/passwd file should have permissions 644 with owner root and group root.
- Lock the following accounts by placing a *LK* in encrypted password field in /etc/shadow: adm, bin, daemon, listen, lp, nobody, noaccess, nuucp, smtp, sys, uucp. These accounts should not have login shells, rather they should be set to /dev/null.

Windows Password Recommendations

Passwords for Windows operating systems and domains should adhere to the policy detailed in the table below. Additionally, NSA has written an enhanced password filter (**ENPASFLT.DLL)** that enforces password minimum length of 8 characters, 4 character sets, and does not allow the password to include the username. This password filter is available to government customers upon request. Also, various third-party tools (e.g. PPE) can serve as excellent password enforcers, allowing customizable password restrictions across an enterprise.

The following settings can be configured via Local Security Policy or a Group Policy Object (GPO). Note that password and account policies for a domain MUST be configured in a domain-level GPO.

Password Policy Options	**Recommended Settings**
Enforce Password History	24 Passwords
Maximum Password Age	90 days
Minimum Password Age	1 day
Minimum Password Length **NOTE: It is recommended for privileged accounts such as administrator to have a password of at least 14 characters.**	12 characters
Passwords must meet complexity requirements **NOTE: If using NSA's ENPASFLT.DLL this option should be set to Disabled to avoid conflict with Microsoft's PASSFLT.DLL**	Enabled
Store password using reversible encryption for all users in the domain	Disabled

Account Lockout Policy Options	Recommended Settings
Account Lockout Duration	15 minutes
Account Lockout Threshold	3-5 invalid logon attempts
Reset account lockout counter after	15 minutes

In addition to the password policy described in the table, several other practices should be followed.

- Services should be run under their own Non-privileged accounts, as opposed to using the built-in SYSTEM or Administrator accounts. These service accounts should also have strong passwords.
- Passwords for privileged accounts should be at least 14 characters long and contain at least four different types of characters.
- The Guest account should be disabled. Ensure that all accounts (service and user) have passwords regardless if the account is enabled or disabled.
- To prevent LM hashes being stored in the SAM or Active Directory, the creation of LM hashes can be turned off with a registry control on Windows 2000, 2003, and XP. The following registry key can be set on Windows 2000 SP2 or later: HKLM\System\CurrentControlSet\Control\LSA\NoLMHash. This prevents LM hashes from being generated. Existing LM hashes will remain until the next time the user changes his or her password. See the Windows Configuration section later for more detailed information on configuring this security option.

Do Not Run Code From Non-Trusted Sources

For the most part, software applications run in the security context of the person executing them without any consideration to source. A PKI infrastructure may help, but when not available remember that spoofing the "From" line of an e-mail message and disguising URLs are trivial. DO NOT OPEN E-MAIL ATTACHMENTS OR RUN PROGRAMS UNLESS THE SOURCE AND INTENT ARE CONFIRMED AND TRUSTED. Always run Outlook so that it executes in the restricted zone and disable all scripting and active content for that zone. For more specific details, reference "*E-mail Client Security in the Wake of Recent Malicious Code Incidents" Reference [* 2]

Read E-mail as Plain Text

Outlook 2002 and Outlook 2003, as well as some email clients from other sources, have a highly recommended security feature that will strip out HTML from incoming messages. This is to prevent HTML scripting attacks that have been known to take advantage of Windows vulnerabilities by a simple preview of a message. To enable this feature in Outlook 2002, create the following registry key:

Key: [HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Options\Mail]
Value Name: ReadAsPlain
Data Type: REG_DWORD
Value: 1 [enable]
0 [disable]

Outlook 2003 does not support this key. Instead, the option is exposed via *Tools/Options/Preferences*. Click on *E-mail Options* and enable ***Read all standard mail in plain text*** **and** ***Read all digitally signed mail in plain text*****.**

Later versions of Outlook Express include the ability to read messages as plain text as well. It is accessed under *Tools/Options/Read*.

Other Malicious Code Countermeasures

Scanning for malicious code at both the perimeter and desktop is recommended as a fundamental counter to a highly prevalent attack vector. Most virus scanning products function by scanning for known malicious code signatures; therefore, they can be ineffective against new or uncharacterized attacks. They can, however, be effective at preventing reoccurrences of past attacks. Some products also allow the definition of attachment types that are then blocked from entry onto the network - a "black list." Populating the black list can be problematic in that determining all the attachment types that represent unacceptable risk is a difficult problem given the plethora of file types. To assist with such an effort, Reference [1] offers a list of file types that can be used as a starting point; however, it can be much easier, and potentially more secure, to utilize products that enforce the acceptance of only those attachment types allowed by the organization's security policy -- a "white list." A combination of both techniques is attractive as well. Assume that a hypothetical file extension .xyz is allowed via the organization's security policy but a known attack uses a file attachment entitled "open_me_please.xyz". Placing the .xyz file extension on the white list but blocking that specific file with a black list entry would be effective in this instance. Unfortunately there are few products which support a white list; black list support is much more common.

Some email clients also support the notion of blocking potentially dangerous file types. For example, Microsoft Outlook releases starting with Outlook 2000 with Microsoft Office Service Pack 2 include attachment blocking. The specific file types that are blocked depend upon the version of the software being run and are included in Reference [1].

Follow The Concept Of Least Privilege

Least privilege is a basic tenet of computer security that means users should be given only those rights required to do their job. Malicious code runs in the security context of the user launching the code. The more privileges the user has, the more damage the code can do. Recommendations pertaining to the least privilege principle include:

- Keep the number of administrative accounts to a minimum.
- Administrators should use a regular account as much as possible instead of logging in as administrator or root to perform routine activities such as reading mail.
- Set resource permissions properly. Tighten the permissions on tools that an attacker might use once he has gained a foothold on the system. Tools or utilities that should be restricted are operating system configuration editing tools, network and domain information gathering tools, Windows Resource Kit and Support Tools, debuggers, compilers, and scripting languages such as gcc, perl, etc.
- The least privilege concept also applies to server applications. Where possible, run services and applications under a non-privileged account.

Application Auditing

Most server-level applications have extensive auditing capabilities. Auditing can be of value in tracking down suspected or actual intrusions. Enable auditing for server applications and audit access to key files (such as those listed above) that an attacker might use once he has gained a foothold on a compromised server.

Network Printers

Today's network printers contain built-in FTP, WEB, and Telnet services as part of their OS. Enabled network printers can be readily exploited and are often overlooked by system administrators as a security threat. These network printers can and are often exploited as FTP bound servers, Telnet jump-off platforms, or exploited via web management services. Change the default password to a complex password. Explicitly block the printer ports at the boundary router/firewall and disable these services if not needed.

Simple Network Management Protocol (SNMP)

SNMP is widely used by network administrators to monitor and administer all types of computers (e.g., routers, switches, printers). SNMP uses an unencrypted "community string" as its only authentication mechanism. Attackers can use this vulnerability in SNMP to possibly gather information from, reconfigure or shut down a computer remotely. If an attack can collect SNMP traffic on a network, then he can learn a great deal about the structure of the network as well as the systems and devices attached to it.

Disable all SNMP servers on any computer where it is not necessary. However, if SNMP is a requirement, then consider the following:

- Allow read-only access and not read-write access via SNMP.
- Do not use standard community strings (e.g., public, private).
- If possible, only allow a small set of computers access to the SNMP server on the computer.
- Alternately, SNMPv3 does include security features; however, this version is not widely available in products which may make implementing it impractical today.

Network Security Testing

Test regularly the security of all of the following devices on the network: clients, servers, switches, routers, firewalls and intrusion detection systems. Also, do this after any major configuration changes on the network.

Perimeter Routers and Firewalls

The following section addresses recommendations for securing network perimeter routers and firewalls. These devices remain a first line of defense that can serve to limit the access a potential adversary has to an organization's network. While the passing of legitimate operational traffic does represent a risk (e.g., malicious emails, attacks delivered via the web browser) tightening these critical devices can offer substantial security benefits.

Host Security

Recommendations for improved host security include:

- Shut down unneeded TCP/UDP servers (e.g., bootps, finger) on the router or the firewall. Servers that are not running cannot break. Also, more memory and processor slots are available with fewer servers running.
- For TCP/UDP servers on the router or the firewall that are necessary, make sure that access to them is limited only to the administrators.
- Shut down unneeded services (e.g., source routing, remote configuration) on the router or the firewall.
- Disable any unused interface on the router or the firewall. Protect each and every active interface on the router or the firewall from information gathering and attacks.
- Protect each and every management port on the router or the firewall from attacks. Disable any unused management port.
- Configure durable passwords on the router or the firewall. . . in accordance with the suggestions offered on page 7.

Example: Cisco IOS Routers

The following scenario steps through the recommendations listed above.

- The `show processes` command can help to show active information about the servers on the router. The following commands show how to disable the following servers: TCP/UDP small servers (echo, discard, daytime, chargen), bootps, finger, http, identd and snmp.

```
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
Router(config)# no ip bootp server
Router(config)# no service finger
Router(config)# no ip http server
Router(config)# no ip identd
Router(config)# no snmp-server community <community string>
```

- If SNMP on the router is required, use the following commands to clear out any SNMP servers with default community strings.

```
Router(config)# no snmp-server community public
Router(config)# no snmp-server community private
```

- Then set up the SNMP server with a community string that is difficult to guess. Also, if possible, allow only read-only access to the server; do not allow read-write access to the server. Apply an access-list to the server. Refer to the following section on TCP/IP Filters for discussion of an access-list for SNMP in more detail. The following command is an example.

```
Router(config)# snmp-server community S3cr3t-str1n9 ro 10
```

- The following commands disable the following services: Cisco Discovery Protocol (CDP), remote configuration downloading, source routing and zero subnet.

```
Router(config)# no cdp run
Router(config)# no service config
Router(config)# no ip source-route
Router(config)# no ip subnet-zero
```

- The following command disables a router interface.

```
Router(config-if)# shutdown
```

- Secure each and every active interface on the router from Smurf attacks, ad-hoc routing and access-list queries with the following commands.

```
Router(config-if)# no ip directed-broadcast
Router(config-if)# no ip proxy-arp
Router(config-if)# no ip unreachables
```

- Configure the console line () and the virtual terminal lines () on the router to time out a session, to require a password at login and to allow only telnet traffic. If the auxiliary line () is not needed, then it should be disabled. Use the following line configuration commands to configure the lines.

```
Router(config)# line con 0
Router(config-line)# exec-timeout 5 0
Router(config-line)# login
Router(config-line)# transport input telnet
Router(config)# line aux 0
Router(config-line)# no exec
```

```
Router(config-line)# exec-timeout 0 5
Router(config-line)# no login
Router(config-line)# transport input none
Router(config)# line vty 0 4
Router(config-line)# exec-timeout 5 0
Router(config-line)# login
Router(config-line)# transport input telnet
```

- Configure the Enable Secret password, which is protected with an MD5-based algorithm. The following global configuration command is an example.

```
Router(config)# enable secret 0 2manyRt3s
```

- Configure passwords for the console line, the auxiliary line and the virtual terminal lines. Use a different password for the console line and the auxiliary line versus the virtual terminal lines. The following line configuration commands are examples.

```
Router(config)# line con 0
Router(config-line)# password Soda-4-jimmY
Router(config)# line aux 0
Router(config-line)# password Popcorn-4-sara
Router(config)# line vty 0 4
Router(config-line)# password Dots-4-georg3
```

- Provide a basic protection for the line passwords by using the following global configuration command.

```
Router(config)# service password-encryption
```

TCP/IP Filters

Carefully consider which TCP/IP services will be allowed through and to the perimeter routers and firewalls (inbound and outbound). The guiding principle should be that services not explicitly permitted are prohibited. In other words, the administrator should create filters focusing on what services and hosts are permitted and denying everything else. This method means that one may not need to block each service individually; however if an organization has a need to individually list services the following tables present common services to restrict because they can be used to gather information about the protected network or they have weaknesses that can be exploited against the protected network.

- **Table 1** lists those TCP or UDP servers that should be completely blocked at the perimeter router or firewall. These services should not be allowed across the router or the firewall in either direction. Also, they should not be allowed to the router or the firewall.

- **Table 2** lists those TCP or UDP servers on the protected network, on the router, or on the firewall that should not be accessible by external clients.

- **Table 3** lists the common TCP or UDP servers on the protected network, on the router or on the firewall that may need some access by internal or external clients and servers. Many of these services can be filtered to the few authorized computers (e.g., ftp server, mail server, domain name server, web server) on the protected network or on the DMZ subnet.

- **Table 4** lists the ICMP message types that can be allowed outbound from the protected network, while all other message types should be blocked.

- **Table 5** lists the ICMP message types that can be allowed inbound to the protected network, while all other message types should be blocked.

Finally, use an intrusion detection system on the protected network to monitor the TCP/IP traffic that is allowed past the perimeter routers and firewalls.

Table 1:
TCP or UDP Servers to Completely Block at the Perimeter Router/Firewall

Port(s) (Transport)	Server	Port(s) (Transport)	Server
1 (TCP & UDP)	tcpmux	1807 (TCP)	SpySender
7 (TCP & UDP)	echo	1981 (TCP)	Shockrave
9 (TCP & UDP)	discard	1999 (TCP)	BackDoor
11 (TCP & UDP)	systat	2001 (TCP)	Trojan Cow
13 (TCP & UDP)	daytime	2023 (TCP)	Ripper
15 (TCP & UDP)	netstat	2049 (TCP & UDP)	nfs
17 (TCP & UDP)	qotd	2115 (TCP)	Bugs
19 (TCP & UDP)	chargen	2140 (TCP)	Deep Throat
37 (TCP & UDP)	time	2222 (TCP)	Subseven21
43 (TCP & UDP)	whois	2301 (TCP & UDP)	compaqdiag
67 (TCP & UDP)	bootps	2565 (TCP)	Striker
68 (TCP & UDP)	bootpc	2583 (TCP)	WinCrash
69 (UDP)	tftp	2701 (TCP & UDP)	sms-rcinfo
93 (TCP)	supdup	2702 (TCP & UDP)	sms-remctrl
111 (TCP & UDP)	sunrpc	2703 (TCP & UDP)	sms-chat
135 (TCP & UDP)	loc-srv	2704 (TCP & UDP)	sms-xfer
137 (TCP & UDP)	netbios-ns	2801 (TCP)	Phineas P.
138 (TCP & UDP)	netbios-dgm	3268 (UDP)	msft-gc
139 (TCP & UDP)	netbios-ssn	3269 (TCP)	msft-gc-ssl
177 (TCP & UDP)	xdmcp	4045 (UDP)	lockd
445 (TCP & UDP)	microsoft-ds	5800 - 5899 (TCP)	winvnc web service
512 (TCP)	rexec	5900 – 5999 (TCP)	winvnc
513 (TCP)	rlogin	6000 – 6063 (TCP)	X11 Window System
513 (UDP)	who	6665 - 6669 (TCP)	irc
514 (TCP)	rsh, rcp, rdist, rdump, rrestore	6711 - 6712 (TCP)	Subseven
515 (TCP)	lpr	6776 (TCP)	Subseven
517 (UDP)	talk	7000 (TCP)	Subseven21
518 (UDP)	ntalk	12345 – 12346 (TCP)	NetBus
540 (TCP)	uucp	16660 (TCP)	Stacheldraht
593 (TCP & UDP)	MS-RPC	27444 (UDP)	Trinoo
1024 (TCP)	NetSpy	27665 (TCP)	Trinoo
1045 (TCP)	Rasmin	31335 (UDP)	Trinoo
1090 (TCP)	Xtreme	31337 – 31338 (TCP & UDP)	Back Orifice
1170 (TCP)	Psyber S.S.	32700 – 32900 (TCP & UDP)	RPC services
1234 (TCP)	Ultors Trojan	33270 (TCP)	Trinity V3
1243 (TCP)	Backdoor-G	39168 (TCP)	Trinity V3
1245 (TCP)	VooDoo Doll	65000 (TCP)	Stacheldraht
1349 (UDP)	Back Orifice DLL		
1492 (TCP)	FTP99CMP		
1600 (TCP)	Shivka-Burka		
1761 – 1764 (TCP & UDP)	sms-helpdesk		

Table 2:
TCP or UDP Servers to Block at the Perimeter Router/Firewall from External Clients

Port(s) (Transport)	Server
79 (TCP)	finger
161 (TCP & UDP)	snmp
162 (TCP & UDP)	snmp trap
514 (UDP)	syslog
550 (TCP & UDP)	new who

Table 3:
TCP or UDP Servers to Allow Limited Access at the Perimeter Router/Firewall

Port(s) (Transport)	Server
20 (TCP)	ftpdata
21 (TCP)	ftp
22 (TCP)	ssh
23 (TCP)	telnet
25 (TCP)	smtp
53 (TCP & UDP)	domain
80 (TCP)	http
88 (TCP)	kerberos
110 (TCP)	pop3
119 (TCP)	nntp
123 (TCP)	ntp
143 (TCP)	imap
179 (TCP)	bgp
389 (TCP & UDP)	ldap
443 (TCP)	ssl
1080 (TCP)	socks
3128 (TCP)	squid
8000 (TCP)	http (alternate)
8080 (TCP)	http-alt
8888 (TCP)	http (alternate)

Table 4:
ICMP Message Types to Allow Outbound at the Perimeter Router/Firewall

Message Types	
Number	**Name**
4	source quench
8	echo request (ping)
12	parameter problem

Table 5:
ICMP Message Types to Allow Inbound at the Perimeter Router/Firewall

Message Types	
Number	**Name**
0	echo reply
3	destination unreachable
4	source quench
11	time exceeded
12	parameter problem

This section describes methods using filters to defend the router, the firewall and the protected network from information gathering and attacks. Note that one needs to be careful with combining the below recommendations together in any filter in order to prevent contradictions or other problems.

- When creating a TCP/IP filter always delete any previous filter.
- Set logging for each statement in the filter that blocks access. This feature will provide valuable information about what types of packets are being denied and can be used in intrusion detection against one's network. Refer to the following section on Logging and Debugging for discussion of logging configuration in more detail.
- Provide IP address spoof protection for the protected network. For inbound traffic do not allow any IP packet that contains an IP address in the source IP address field from the following: the protected network, any local host address (127.0.0.0 – 127.255.255.255), any reserved address (10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, 192.168.0.0 – 192.168.255.255), or any multicast address (224.0.0.0 – 239.255.255.255). For outbound traffic allow IP traffic from the protected network and do not allow IP traffic that contains an external IP address in the source IP address field.
- Protect the router or the firewall from the Land Attack. This attack involves sending a packet to the router with the same IP address in the source address and destination address fields and with the same port number in the source port and destination port fields. This attack can cause a denial of service.
- Protect the router or the firewall from the TCP SYN Attack. The TCP SYN Attack involves transmitting a volume of connections that cannot be completed at the destination. This attack causes the connection queues on the router or the firewall to fill up, thereby denying service to legitimate TCP traffic.
- Protect the router, the firewall or the protected network from unnecessary ICMP traffic. There are a variety of ICMP message types, and some are associated with programs. Some message types are used for network management and are automatically generated and interpreted by network devices. For example, the ping program works with message type Echo. With Echo packets an attacker can create a map of the protected networks behind the router or the firewall. Also, he can perform a denial of service attack by flooding the router, the firewall or the hosts on the protected network with Echo packets. With Redirect packets the attacker can cause changes to a host's routing tables.

  For outbound ICMP traffic, one should allow the message types Echo, Parameter Problem and Source Quench. Otherwise, block all other ICMP message types going outbound. With Echo packets users will be able to ping external hosts. Parameter Problem packets and Source Quench packets improve connections by informing about problems with packet headers and by slowing down traffic when it is necessary. For inbound ICMP traffic, one should allow the following message types: Echo Reply, Destination Unreachable, Source Quench, Time Exceeded and Parameter Problem. Otherwise, block all other ICMP message types coming inbound.
- Protect the router, the firewall or the protected network from inbound traceroute. Traceroute is a utility that prints the IP addresses of the routers that handle a packet as the packet hops along the network from source to destination. On UNIX operating systems traceroute uses UDP packets and causes routers along the path to generate ICMP message types Time Exceeded and Unreachable. Similar to ICMP Echo

packets, an attacker can use traceroute to create a map of the protected network behind the router or the firewall.

- Apply a filter to the router or the firewall to allow only a small set of computers (e.g., those used by the administrators) Telnet access to the router or the firewall. Log all successful and unsuccessful connections.
- If an SNMP server is necessary on the router or the firewall, then apply a filter to the router or the firewall to allow only a small set of computers (e.g., those used by the administrators) SNMP access to the router or the firewall. Log all successful and unsuccessful connections.

Example: Cisco IOS Routers

The following scenario steps through the recommendations listed above.

- The following commands show an example of how to clear out a previous version of an access-list before creating a new access-list.

```
Router(config)# no access-list 100
Router(config)# access-list 100 permit ip 10.2.9.0 0.0.0.255 any
Router(config)# access-list 100 permit ip 10.55.1.0 0.0.0.255 any
```

- The following commands show an example of how to set logging on an extended IP access-list statement.

```
Router(config)# access-list 102 permit tcp 10.4.6.0 0.0.0.255 any eq 80
Router(config)# access-list 102 deny ip any any log
```

Note that there is an implicit `deny` statement at the end of every access list on a Cisco router. This implicit statement blocks all other packets not permitted by the rest of the access-list. However, it does not log these packets. Thus, add the following statements at the end of each extended IP access-list. These statements will guarantee that the router will log the values for the source and destination ports for TCP and UDP traffic being denied.

```
Router(config)# access-list 106 deny udp any range 0 65535 any range 0
                65535 log
Router(config)# access-list 106 deny tcp any range 0 65535 any range 0
                65535 log
Router(config)# access-list 106 deny ip any any log
```

- Below are two example access-lists that provide IP address spoof protection. The first example is for inbound traffic to the protected network (e.g., 14.211.150.0).

```
Router(config)# access-list 100 deny ip 14.211.150.0 0.0.0.255 any log
Router(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
Router(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
Router(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
```

```
Router(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
Router(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any log
Router(config)# access-list 100 permit ip any 14.211.150.0 0.0.0.255
Router(config)# interface Ethernet1/2
Router(config-if)# description "external interface"
Router(config-if)# ip address 25.73.1.250 255.255.255.248
Router(config-if)# ip access-group 100 in
```

The second example is for outbound traffic from the protected network (e.g., 14.211.150.0).

```
Router(config)# access-list 102 permit ip 14.211.150.0 0.0.0.255 any
Router(config)# access-list 102 deny ip any any log
Router(config)# interface Ethernet0/1
Router(config-if)# description "internal interface"
Router(config-if)# ip address 14.211.150.17 255.255.255.240
Router(config-if)# ip access-group 102 in
```

Note that you can apply two access-lists to any interface on the router, one for network traffic leaving the interface and the other for network traffic entering the interface.

- The following commands show how to protect the router from the Land Attack.

```
Router(config)# access-list 101 deny ip host 198.26.171.178 host
                198.26.171.178 log
Router(config)# access-list 101 permit ip any any
Router(config)# interface serial2/1
Router(config-if)# description "external interface"
Router(config-if)# ip address 198.26.171.178 255.255.255.248
Router(config-if)# ip access-group 101 in
```

- Protect the router against the TCP SYN Attack for the following two scenarios: blocking external access and limited external access. Below is an example for blocking external access on a Cisco router. The access list blocks packets from any external network that have only the SYN flag set. Thus, it allows traffic from TCP connections that were established from the protected network (e.g., 14.2.6.0), and it denies anyone coming from any external network from starting any TCP connection.

```
Router(config)# access-list 100 permit tcp any 14.2.6.0 0.0.0.255
                established
Router(config)# access-list 100 deny ip  any any log
Router(config)# interface serial0/0
Router(config-if)# description "external interface"
```

```
Router(config-if)# ip access-group 100 in
```

Below is an example for allowing limited external access on a Cisco router. Using the TCP intercept feature, the access list blocks packets from unreachable hosts; thus, it only allows reachable external hosts to initiate connections to a host on the protected network (e.g., 14.2.6.0). In intercept mode the router intercepts a TCP connection and determines if a host is reachable. If successful, the router establishes the connection; otherwise, it prevents the connection. This protection does not stop reachable hosts from performing this attack against the router or the protected networks.

```
Router(config)# ip tcp intercept list 100

Router(config)# access-list 100 permit tcp any 14.2.6.0 0.0.0.255

Router(config)# access-list 100 deny ip  any any log

Router(config)# interface e0/0

Router(config-if)# description "external interface"

Router(config-if)# ip access-group 100 in
```

- The following commands show how to allow outbound from the protected network (e.g., 14.2.6.0) only the following ICMP message types: Echo, Parameter Problem and Source Quench.

```
Router(config)# access-list 102 permit icmp 14.2.6.0 0.0.0.255 any echo

Router(config)# access-list 102 permit icmp 14.2.6.0 0.0.0.255 any
                parameter-problem

Router(config)# access-list 102 permit icmp 14.2.6.0 0.0.0.255 any
                source-quench

Router(config)# access-list 102 deny icmp any any log
```

- The following commands show how to allow inbound to the protected network (e.g., 14.2.6.0) only the following ICMP message types: Echo Reply, Destination Unreachable, Source Quench, Time Exceeded and Parameter Problem.

```
Router(config)# access-list 100 permit icmp any 14.2.6.0 0.0.0.255
                echo-reply

Router(config)# access-list 100 permit icmp any 14.2.6.0 0.0.0.255
                unreachable

Router(config)# access-list 100 permit icmp any 14.2.6.0 0.0.0.255
                source-quench

Router(config)# access-list 100 permit icmp any 14.2.6.0 0.0.0.255
                time-exceeded

Router(config)# access-list 100 permit icmp any 14.2.6.0 0.0.0.255
                parameter-problem

Router(config)# access-list 100 deny icmp any any log
```

- The following command shows how to block inbound traceroute from a UNIX computer.

```
Router(config)# access-list 111 deny udp any any range 33434 33534 log
```

- The following commands show how to allow Telnet access from certain computers on the protected network (e.g., 14.4.4.0) to the router via an extended IP access-list. The administrator can telnet to any interface IP address on the router. However, the router converts any interface IP address to 0.0.0.0. Thus, the unusual destination IP address 0.0.0.0 must be used in the access-list.

```
Router(config)# access-list 105 permit tcp host 14.4.4.10 host 0.0.0.0 eq
                23 log
Router(config)# access-list 105 permit tcp host 14.4.4.11 host 0.0.0.0 eq
                23 log
Router(config)# access-list 105 permit tcp host 14.4.4.12 host 0.0.0.0 eq
                23 log
Router(config)# access-list 105 deny ip any any log
Router(config)# line vty 0 4
Router(config-line)# access-class 105 in
```

- The following commands show how to allow SNMP access from certain computers on the protected network (e.g., 14.4.4.0) to the router via a standard IP access-list.

```
Router(config)# access-list 10 permit 140.4.4.10
Router(config)# access-list 10 permit 140.4.4.11
Router(config)# access-list 10 permit 140.4.4.12
Router(config)# snmp-server community snmp72str1ng64 ro 10
```

Logging and Debugging

Logging on a router or a firewall offers several benefits. It informs the administrator if the router or the firewall is working properly or has been compromised. It can also show what types of attacks are being attempted against the router, the firewall or the protected network.

The following are recommendations for logging and debugging:

- Send the most serious level of logs to the console on the router or the firewall in order to alert the administrator.
- Send the logs to a log host, which should be a dedicated computer on the protected network whose only job is to receive logs. The log host should have all unnecessary servers and accounts disabled except for syslog.
- Configure the router or the firewall to include more specific time information in the logging and in the debugging. Direct the router or the firewall to at least two different, reliable network time protocol (NTP) servers to ensure accuracy and availability of time information. Set all NTP messages with the same IP source address of an interface on the internal network. This configuration will allow the administrator to create a TCP/IP filter that allows time information only from the internal IP address of the router or the firewall to the external NTP servers. This filter will help to prevent

spoofing or flooding NTP messages to the router or the firewall. Include a more specific timestamp in each log message and each debug message. This will allow an administrator to trace network attacks more credibly.

- By default, a log message contains the IP address of the interface it uses to leave the router or the firewall. Instead, set all log messages with the same IP source address of an interface on the internal network, regardless of which interface the messages use. This configuration will allow the administrator to create a TCP/IP filter that allows logs only from the internal IP address of the router or the firewall to the logging host. This filter will help to prevent spoofing or flooding log messages to the logging host.
- Finally, consider also sending the logs to a dedicated printer to deal with worst-case scenarios, e.g., failure of the log host.

Example: Cisco IOS Routers

The following scenario steps through the recommendations listed above.

- Enable the router's logging capability with the following command.

```
Router(config)# logging on
```

- Set the syslog level of logs to be sent to the router console and to the terminal lines (monitor connections). The following commands are examples.

```
Router(config)# logging console errors
Router(config)# logging monitor errors
```

- Set the IP address of the log host. Set the syslog level to be sent to the log host. Set the syslog facility type in which log messages are sent. The following commands are examples.

```
Router(config)# logging 10.1.1.200
Router(config)# logging trap debugging
Router(config)# logging facility local7
```

Note that the effect of the `log` keyword with the IP extended access-list statements depends on the setting of the logging console command. The `log` keyword takes effect only if the logging console syslog level is set to 6 (informational) or 7 (debugging). If the level is changed to a value less than 6 and if the `log` keyword is used within an IP extended access-list command, then no information is logged to the log host or displayed to the console. Refer to the previous section on TCP/IP Filters for discussion of access-lists in more detail.

- The following commands show an example of how to set time information for the logging and for the debugging.

```
Router(config)# ntp server 192.168.41.40
Router(config)# ntp server 192.168.41.41
Router(config)# ntp source Ethernet0/1
```

```
Router(config)# service timestamps log datetime localtime show-timezone
Router(config)# service timestamps debug datetime localtime show-timezone
Router(config)# clock timezone EST –5
Router(config)# clock summer-time EDT recurring
```

- The following command shows an example of how to set all log messages with the same IP source address of a router interface.

```
Router(config)# logging source-interface e0/1
```

General Recommendations

It is highly recommended that the configuration files for the router or the firewall be created, stored and maintained on a computer offline in ASCII format. These files will contain any comments that can help give perspective to the configuration settings and the filters. Also, changes to the filters can be done with much more ease and accuracy. Then the file can be transferred from the computer to the router or the firewall. This is invaluable for diagnosing suspected attacks and recovering from them. Finally, protect the contents of the configuration files from unauthorized individuals.

Windows 2000 and Above Operating Systems

Service Packs And Security Patches

A service pack is a periodic update to the operating system that contains fixes to vulnerabilities and bugs. Updates addressing specific vulnerabilities and bugs discovered between service packs are called hotfixes or patches.

It is important to install Service Packs and hotfixes in a timely manner. Service packs are cumulative, meaning they include all patches from previous service packs as well as new fixes, many of which can be security related. As the time between the discovery of a vulnerability and the appearance of corresponding attacks shrinks, hotfixes will often address current attacks that are proliferating throughout networks. Too often, administrators only choose to install "critical" patches, or those their organizations are mandated to apply (e.g. via Information Assurance Vulnerability Alerts, or IAVAs). However, depending on current network configuration, vulnerabilities addressed by other patches may be very relevant. Also, although the initial effects of exploiting the vulnerability may not appear to be as devastating as those deemed critical, they nonetheless may provide an inroad into the network and lead to further exploitation. Therefore, it is recommended that all security-related hotfixes be installed immediately after installation of the latest service pack. Note that if a service pack is reapplied at any time, the hotfixes must also be re-installed.

Patch Management

A major challenge for network administrators is identifying missing security patches and pushing patches to machines on the network. In addition to numerous third party tools, Microsoft has developed free tools that will assist in these areas.

Windows Server Update Services (WSUS) is Microsoft's latest patch management technology. WSUS allows for deployment of patches and new software versions for Microsoft Windows Server 2000, Windows Server 2003, and Windows XP operating systems. See Microsoft's web site for more information on this patch management technology.

Microsoft Baseline Security Analyzer (MBSA) is a tool that scans for common system misconfigurations and missing security patches. MBSA 2.0, the latest version of the tool, is built on the Windows Update Agent and Microsoft Update infrastructure. MBSA is compatible with other Microsoft management products including Microsoft Update (MU), WSUS, SMS, and Microsoft Operations Manager (MOM). MBSA 2.0 can conduct local or remote scans and is for use on systems with the following software baselines:

- Windows 2000 SP3 or higher, Windows XP, Windows Server 2003
- Microsoft SQL Server 2000 with Service Pack 4 (SP4) or higher
- Microsoft Exchange 2000 with SP3 or higher
- Microsoft Office XP, Microsoft Office 2003

For users with older software versions, MBSA 1.2.1 can be used. Note that this version can only scan for Office updates on a local machine and is only compatible with Software Update Services (SUS). Refer to Microsoft Knowledge Base Article 895660 for additional information on both versions of MBSA. For additional information on Microsoft's MSBA and downloads see: http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Regardless of the choice in patch management software, a documented patch management process should be established, and patches should be pushed out in a regular, timely manner. Periodic scans of the network should be conducted in order to identify machines not up-to-date on patches or versions.

Active Directory and Group Policy

Active Directory is a hierarchical directory service for Windows 2000 and above operating systems. Administrators should become very familiar with Active Directory and how to organize and manage their domains using this powerful service. Within Active Directory, configurations can be pushed down to domain members via Group Policy Objects (GPOs). The following section discusses several best practices for implementing security settings via Group Policy.

Domain Group Policy

The domain level Group Policy Object should contain settings common to all computers in the domain. With respect to the Windows security settings portion of Group Policy (Computer Configuration → Windows Settings → Security Settings), typically the domain level GPO should only include:

- Account Policies (password policy, account lockout policy, Kerberos policy)
- “Add workstations to the domain” user right
- Three security options:
  - “Network Security: Force logoff when logon hours expire”
  - “Microsoft network server: Disconnect clients when logon hours expire”
  - “Network Access: Allow anonymous SID/NAME translation.”

Note that the security options listed above are the wording for Windows XP/Server 2003 GPOs and may differ slightly for Windows 2000 GPOs.

Organization and Group Policy Based on Computer Roles

It is recommended to push down security settings through the Security Settings portion of Group Policy including user rights, security options, restricted groups, and file permissions based on computer roles. Organizational Units (OUs) should be created for each computer role (e.g. Domain Controllers, Member Servers, Workstations), with child OUs if necessary (e.g. Exchange Servers and Web Servers under Member Servers and Laptops under Workstations). For example, suppose there exists an OU for Windows XP workstations with a child OU under it for Windows XP laptops. A comprehensive GPO for all Windows XP workstations can be implemented at the workstation OU level and a GPO with laptop-specific settings different from normal workstations could be implemented at the laptop OU level.

Windows Configuration Recommendations

The following recommendations of Windows configuration-related security measures are by no means exhaustive. It should also be understood that alleviating one's network of these vulnerabilities does not render the network "secure,” rather these recommendations are part of a defense in depth strategy that should be implemented in concert with the organization's security policy.

Security Policy Recommendations

The items in this section describe critical problems commonly found in Windows 2000 and above operating systems that can be mitigated via security policies (Group Policy or Local Security Policy) by expanding Windows Settings → Security Settings → Local → Security Options.

Anonymous Connections

The anonymous user, also known as the null connection, allows an unauthorized user to connect to a system with no credentials and enumerate system information such as user accounts and SIDs, shared resources, policies, and services. This type of information can be used as a basis for system exploitation.

Disallow anonymous access to critical system information. The steps to do this are different depending on whether the system is Windows 2000 or Windows XP/2003.

For Windows 2000:

Set the following registry key, preferably via Group Policy:

Security Attribute	Recommended Settings
Additional restrictions for anonymous connections HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous = 1	Do not allow enumeration of SAM accounts and shares.

Note: Setting the RestrictAnonymous key = 2 (No access without explicit permissions), is the most secure option; however, compatibility issues may occur depending on the type of operating system on clients/servers and what applications and services are running. If the most secure setting is desired, try setting the key to 2 in a non-production environment first to ensure that operation will continue. See Microsoft Knowledge Base Article 246261 “How to Use the RestrictAnonymous Registry Setting in Windows 2000” for more information.

For Windows XP and Windows Server 2003:

Windows XP and Windows Server 2003 have the ability to remove the anonymous user from membership in the Everyone group. This is done in a default installation and removes much of the risk associated with the null connection.

By default, the anonymous user-related keys are set to the recommended values. Ensure via Group Policy that the following are configured:

Security Attribute	Recommended Settings
Network access: Do not allow anonymous enumeration of SAM accounts HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymousSAM = 1	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares HKLM\System\CurrentControlSet\Control\Lsa\RestrictAnonymous = 1	Enabled
Network access: Let Everyone permissions apply to anonymous users HKLM\System\CurrentControlSet\Control\Lsa\EveryoneIncludesAnonymous = 0	Disabled

LAN Manager Passwords

LAN Manager (LM) is a type of challenge/response network authentication included in recent Windows operating systems for compatibility with pre-Windows NT systems. Client authentication to Windows servers using LM is weaker than the Windows NT challenge/response (NTLM) and the enhanced version (NTLMv2).

By default, Windows authentication sessions send the LM hash along with the NTLM or NTLMv2 hash. LM authentication sessions can be easily sniffed and cracked, revealing a user name and password. In fact, most Windows password crackers, such as L0phtCrack, specifically target the LM hash due to the relative quickness in brute-forcing LM passwords.

It is recommended that the LM hash not be passed during network authentication. To accomplish this, set the following registry key, preferably via Group Policy:

Security Attribute	Recommended Settings
LAN Manager authentication level HKLM\System\CurrentControlSet\Control\Lsa\LMCompatibilityLevel = 4	Send NTLMv2 response only\refuse LM

Microsoft has released a Directory Services Client that allows pre-Windows 2000 clients to take advantage of features, including NTLMv2, provided by the Active Directory service. Refer to Microsoft Knowledge Base article 288358 for more information.

An additional safeguard can be made by disabling the storage of the LM hash in the local SAM database or Active Directory if the system is a domain controller. Refer to Microsoft Knowledge Base Article 299656 “How to Prevent Windows from Storing a LAN Manager Hash of Your Password in Active Directory and Local SAM Databases” for additional information on this issue.

For Windows 2000 Service Pack 2 and higher:

- Start Registry Editor (Regedt32.exe).
- Locate and then click the following key:

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
- On the **Edit** menu, click **Add Value**, and add the following value:

- NoLMHash = 1

- Restart the computer, and then change the password to make the setting active.
- NOTE: This setting change must be performed on all domain controllers in the Active Directory.

For Windows XP and Windows Server 2003:

Via Group Policy configure the following security option:

Security Attribute	Recommended Settings
Network security: Do not store LAN Manager hash value on next password change HKLM\System\CurrentControlSet\Control\Lsa\NoLMHash = 1	Enabled

File and Shared Resource Permissions

Poor access control lists (ACLs) on resources such as files, folders, and shares pose a major vulnerability to Windows systems. Poor ACLs make it easy to elevate a user's privileges or view and manipulate data that should be off-limits. In general, Windows 2000 and above operating systems have default ACLs superior to those of Windows NT 4.0. However, a few recommendations for improving security are in order:

- Ensure that the file system is NTFS versus FAT. NTFS allows file access control to be set; FAT does not.
- Restrict the Power Users group to have no members. This will ensure that non-administrative users cannot modify critical system files and registry keys. Power Users membership can be restricted via a Group Policy Object under the Restricted Groups security setting.
- Windows 2000 default permissions for the operating system partition (usually the C drive) allow users Full Control privileges over files in the root directory. This may enable users to add Trojan programs and files to the partition. It is recommended that the permissions for the system drive FOLDER ONLY be set to allow Administrators and SYSTEM Full Control, Authenticated Users Read/Execute, and CREATOR OWNER Full Control. Ensure that these permissions DO NOT propagate to sub folders.
- When creating a new partition, the default permissions are Everyone Full Control over the entire partition. Ensure that appropriate permissions are then explicitly set on the partition's folders and files.
- Lock down operating system executable files within the %SystemRoot%\System32\ folder that could be used for network information gathering and exploitation. The following files should all be given the permissions Administrators: Full Control, System: Full Control:

regedit.exe	arp.exe	at.exe
attrib.exe	cacls.exe	debug.exe
edlin.exe	eventcreate.exe	eventtriggersxe
ftp.exe	nbtstat.exe	net.exe

net1.exe	netsh.exe	netstat.exe
nslookup.exe	ntbackup.exe	rcp.exe
reg.exe	regedt32.exe	regini.exe
regsvr32.exe	rexec.exe	route.exe
rsh.exe	sc.exe	secedit.exe
subst.exe	systeminfo.exe	telnet.exe
tftp.exe	tlntsvr.exe	

- Create only those shared resources that are necessary and restrict permissions on existing network shares. When a share is created, the default access control is Everyone having Full Control. Restrict the share permissions to only those groups that need access. Note that share permissions work in conjunction with file permissions, with the more restrictive of the two applying.

Auditing

Most server-level applications have extensive auditing capabilities. Auditing can be of value in tracking down suspected or actual intrusions. If concerned about attackers executing particular applications or files, auditing can be enabled for these. In summary, auditing recommendations include:

- Enable auditing, preferably via Group Policy.
- At a minimum, for all servers and any systems within a DMZ, audit logons and logoffs, failed attempts at exercising user privileges, and system events such as shutdowns.
- Develop an audit management process that includes procedures for regular reviewing and archiving of audit logs.

Windows Firewall

Included in Windows XP Service Pack 2 and Windows Server 2003 is Windows Firewall, a host-based firewall used to restrict unsolicited in-bound traffic to a computer. Windows Firewall settings can be configured locally on a host, or, preferably via Group Policy. The following are recommendations regarding the use of Windows Firewall:

- Enable Windows Firewall.
- Windows Firewall configurations should be pushed down via Group Policy within a domain if possible. In general, do not allow local administrators to disable/enable the firewall or make changes.
- Within the Group Policy settings for Windows Firewall, exceptions are allowed for local ports, programs, file and print sharing, and remote desktop. Typically the firewall is configured to allow these exceptions from any IP address in the local network. It is recommended to evaluate whether all machines need these accesses to all other machines. If not, exceptions based on IP addresses can be configured to restrict what machine can send certain types of network traffic through Windows Firewall. Periodically review port and program exceptions to re-evaluate whether they are still needed.

Additional Windows 2000 Security Measures

- Block Windows ports susceptible to attack (e.g., 88, 135, 137, 138, 139, 389, 445, 3268, and 3269) either at the perimeter router or firewall. These ports are usually needed in an internal network, but not externally. Blocking these ports will stop many attacks against Windows systems. In general, take a "deny all" approach for network routers and firewalls initially, then add ports as necessary. Microsoft Knowledge Base Article 832017 "Port Requirements for the Microsoft Windows Server System" gives a listing of port assignments.
- Remove all services and protocols that are not required (e.g., Telnet, FTP, Web). Ensure proper placement of services on the network (e.g. RAS or Web service should not be on a Domain Controller).
- Review Trust Relationships between domains. Remove unnecessary trusts. Trusted domains with poor security could pose a substantial risk.

Data Execution Prevention (DEP)

DEP is a new feature included in Microsoft's Windows XP (SP2) or later and Windows 2003 (SP1) or later operating systems. DEP will help prevent execution of malicious code as a result of certain attacks such as buffer overflows. By default, DEP is enabled for "essential windows programs and services only". It is recommended that this be changed to "all programs and services except those I select".

Open System Properties, click **Start**, click **Control Panel**, click **Performance and Maintenance**, and then click **System**.

Click the **Advanced** tab and, under **Performance**, click **Settings**.

Click the **Data Execution Prevention** tab.

Select "Turn on DEP for all programs and services except those I select"

DEP can also be set by modifying the boot.ini file on a machine. The boot.ini setting is: **/NoExecute**=*policy_level*

Note *policy_level* is defined as AlwaysOn, AlwaysOff, OptIn, or OptOut.

Configuration	Description
OptIn	This setting is the default configuration. On systems with processors that can implement hardware-enforced DEP, DEP is enabled by default for limited system binaries and programs that "opt-in." With this option, only Windows system binaries are covered by DEP by default.
OptOut	DEP is enabled by default for all processes. You can manually create a list of specific programs that do not have DEP applied by using the **System** dialog box in Control Panel. Information technology (IT) professionals can use the

		Application Compatibility Toolkit to "opt-out" one or more programs from DEP protection. System compatibility fixes, or shims, for DEP do take effect.
AlwaysOn		This setting provides full DEP coverage for the whole system. All processes always run with DEP applied. The exceptions list to exempt specific programs from DEP protection is not available. System compatibility fixes for DEP do not take effect. Programs that have been opted-out by using the Application Compatibility Toolkit run with DEP applied.
AlwaysOff		This setting does not provide any DEP coverage for any part of the system, regardless of hardware DEP support. The processor does not run in PAE mode unless the **/PAE** option is present in the Boot.ini file.

When using the recommended setting, **/NoExecute** is set to **OptOut**.

Note: DEP is implemented in both software and hardware. In order for Windows to take full advantage of DEP, the processor of the machine must support “execution prevention”. To determine if your processor supports hardware based DEP, refer to Microsoft Knowledge Base article **KB912923**.

Microsoft Web Server

Internet Information Server (IIS)

IIS security can be critical to an organization. While recent releases have shown remarkable improvement, early versions of the Windows operating system enabled IIS by default along with many of it options. This had the effect of increasing the attack surface available to an adversary -- an avenue that was taken advantage of in various Internet based attacks.

This section offers security configuration guidance for Microsoft IIS web servers. Consistent with the theme of this document, this list is by no means a complete security guide. More complete guidance can be found at [4] and [9] :

- Ensure the web server computer is dedicated. It should not have other uses, e.g., client workstation or print server.
- Ensure the server is kept up-to-date on OS and web server related patches (as noted on page 6).
- Do not perform development work on the operational web server. Ensure all applications are thoroughly tested and in final form prior to their transfer onto the operational server. Create a secondary mirror of the server for all development services and experimentation. Do not use insecure communications, such as unprotected FTP or telnet, for data transfer particularly if the data would pass over a less trusted network or unnecessarily open up access to the server.
- Remove/disable all unnecessary services on the web server.
- Isolate the web server physically and logically to the maximum extent practical. Suggestions include the following:
    - If possible, limit physical access to the web server to the fewest number of people.
    - Place the web server close to the administrator, the web engineer, or the webmaster.
    - Keep the web server on a LAN segment separate from the rest of the IT infrastructure.
    - Do not mount or share services to and from the server.
- Remove all unnecessary ISAPI script mappings from the Master properties page and propagate to all web sites. This will help prevent any potential vulnerability in those .dll files, such as buffer overflows, from affecting the security of your web server.
- Separate content and place in proper directories (e.g. static files, scripts and executables).
- Use NTFS permissions, along with user groups, to set the restrictive ACL's on the content, script, publishing and all other web-related directories on the web server - [4] contains specific recommendations. Also, create a special WebUsers group for the IUSR account and remove IUSR from the Guests group. This will prevent users from accessing areas and content that they should not have access to.
- Set proper IIS permissions on web sites, virtual directories, and files. Permissions set here need to match NTFS permissions. If they do not match, the more restrictive of the two will be enforced. Set these permissions as *Read* for static content and *Scripts only* for script content. Do not enable the directory browsing option.

- Enable OS level auditing as noted on page 30 and consider auditing access to critical system files that an attacker might leverage in an attack such as listed on page 29. Also enable logging on the web server. Recording the following is recommended:
    - Date and Time event occurred
    - IP Address of the client
    - Username (this is likely to be IUSR_machinename) accessing your site – this is very useful because this data does not appear in the NT log files
    - HTTP method used to access your site
    - URI Stem - the resource accessed by the client (HTML page, script, or ISAPI application)
    - URI Query - the query the client was making
    - Status of the request
    - Time taken to process the request
    - URL of the last site visited by the client
- Disable or block all protocols and services (ports) not required for the web server to function. This will minimize the malicious user's ability to attack vulnerable services and add a layer of protection in the event other security measures fail.
- Remove all samples installed by the web server. Often samples contain scripts that can be used by malicious users to elevate privileges or gain access to sensitive system/user information.
- Run URLSCAN. URLSCAN, a free tool provide by Microsoft [11], allows administrators to restrict servers to help ensure that they only respond to legitimate requests. URLSCAN is easy to configure and is especially important for IIS 5.0. IIS 6.0 has integrated a lot of URLSCAN's functionality directly into the web server; however, it still offers some additional benefit as described in [11].
- Make certain the operating system is adequately protected. The guidance contained within this document is intended to offer the fundamental steps, but additional safeguards should be considered. For Windows 2000 and IIS 5.0, use of the HISECWEB.inf policy provided by Microsoft [9] offers additional protections, but the highest level of protection is available via the NSA's operating system guides [8]. For Windows Server 2003 and IIS 6.0, a range of additional operating system settings are available in the associated guide [5]. The High Security Member Server Baseline with the supplemental WebServer.inf offers the highest level of protection. Whichever guidance is used, it is important to remember that it must be tailored to the situation and in accordance with the security policy of the organization.

UNIX Systems and Networks

The following recommendations can be implemented to improve the security of UNIX systems and networks.

Startup and Login Scripts

Improper use and/or configuration of system startup and user login scripts may allow an avenue of attack into the system. To help mitigate this risk:

- Check the permissions and ownership of files accessed or executed upon system startup and user login. If these files allow world-access, browse scripts to see if any unusual process or script is started, especially if in user directories.
- System files and directories should be owned by root/root or root/sys without world write or execute permissions so that they cannot be modified or exploited by unauthorized users.
- User startup files should be owned by the individual user and should not allow world access.
- In each user's directory, check for Trojan commands or entries in hidden files (e.g. .login, .profile, .netrc, .forward) as well as files that have extensions such as .old or .backup or begin with ".." and "...".

Services and Ports

Many UNIX services have well known security vulnerabilities associated with them which allow root access. In order to detect and minimize potential vulnerabilities, perform the following actions:

- Run a port scanner, such as nmap (available at http://www.insecure.org/nmap) to list open ports and services. In addition, run netstat –a to view the status of all socket and routing table entries.
- All unnecessary services (e.g., rexd, rquotad, talk, sadmind, kcmsd, rstatd, fs, exec, daytime, walld, fingerd, systat, rusersd, sprayd, uucpd, chargen, time, echo, display, tftp, comsat and discard) should be disabled so they do not start at boot time. In addition, these ports should be blocked at the perimeter router or firewall.

System Trust

There are various ways for UNIX systems to allow access to a machine or an account without providing a password. Through the use of *.rhosts, .forward, .netrc, hosts.lpd,* and *hosts.equiv* files, it is possible for a user on one system to access or utilize another system without providing authentication. This practice should be reviewed for necessity. An intruder breaking into an authorized user's account can use that same trust to reach multiple machines with little effort. Additional safeguards include:

- Do not use plus signs (+) in the files mentioned above as they allow global access (to users and/or machines).
- Prohibit root from logging directly into a remote system through proper configuration in files such as /etc/ttys, /etc/ttytab, /etc/securetty and /etc/default/login.

Network Communication

Network communications programs like *telnet, ftp,* and the *"r commands"* (*rlogin, rcp, rsh* and *rexec*) may transmit the username and password across the network in the clear making it easy for a sniffer to capture this information. Some administrators feel that the use of trust relationships that allow a user to access a remote system without supplying a password via *rlogin* and *rsh*, eliminate the risk of password sniffing. However, if an attacker gains control of any machine in such a trusted network, access can be gained to all other machines that trust the hacked machine. If these remote services are not required, they should be disabled. If similar functionality is still required, SSH (available at http://www.openssh.com) or a similar virtual private networking solution should be installed to provide the necessary connectivity while encrypting all session-traffic (including the password) to reduce the threat of password sniffing and TCP session hijacking.

Network Configurations

Ensure that network configuration files (such as /etc/*hosts, /etc/defaultdomain, /etc/defaultrouter,* and */etc/netmasks*) are owned by root/root and have permissions of 644.

Patches

Ensure that recommended and system security patches are installed and are up-to-date and that each system is rebooted after patch installation.

User Accounts

The following are recommended practices for securing user accounts:

- Review all user accounts on a regular basis to ensure relevance.
- Configure each account to have a unique user ID number.
- Check to make sure each shell field is set to a valid shell to prevent malicious code from being executed and granting root access.
- Delete unneeded default system accounts (like nobody4, uucp).
- Ensure every line in /etc/passwd is properly formatted.
- Always make sure each user has a strong, valid password.
- Set permissions for home directories to 750.
- For accountability purposes, system administrators should not directly log in as root, but rather as themselves and then switch user (su) to root.
- An administrative group (e.g. wheel) should be created in the /etc/group file and each administrative user should belong to that group. Once the administrative group has been created, the "su" program should have its ownership, group, and permissions changed (root/wheel, 4750) so that only authorized users have access to the "su" program.

Permissions

The following are recommendations for ensuring directory and file permissions are secure:

- Look for setuid or setgid files and programs.
- Disable unnecessary setuid/setgid programs by deleting the suid and/or sgid bits with the chmod command.

- Look for world-writable directories and files and eliminate world access if not needed. This prevents unauthorized access or the insertion of malicious code.
- Also check for files and directories owned by root that are world-writable. These files may indicate a potential symbolic link attack or a recursive copy/modify/re-copy directory attack.
- World writable directories (like /tmp) should have the sticky-bit set. (e.g. chmod 1777 /tmp)
- Check umask values. Most user umasks should be set to 022 at login.

Cron and At Jobs

Cron and at jobs allow tasks to be scheduled for execution at a later time. To ensure the security of these jobs, perform the following actions:

- Check permissions on cron and at job configuration file cron.allow, cron.deny, at.allow and at.deny files. They should be 644, root/sys. The cron.allow and at.allow files permit users to use crontab and at jobs. The cron.deny and at.deny files restrict these users from access. If .allow files do not exist, then the system checks the .deny files.
- Check to make sure that all cron and at jobs have valid users associated with them. Crontab files should be owned by the specific user associated with them and have permissions of 600.
- Make sure that all cron or at jobs use absolute paths (full path names).

Core Dumps

Check for *core* files. Many reside in the "/" directory, but others may be located elsewhere. Core files may contain sensitive system data and/or user passwords. Remove core files from the system via a regularly scheduled cron job. Configure the system so that when core files are created, they automatically have a zero byte size.

Stray system files

Regularly search for stray system files like old versions *of /etc/passwd* and */etc/shadow* that have been inadvertently copied to temporary locations with insecure permission modes. Some entries in a stray *shadow* file may still contain valid user passwords that can be cracked and used to gain entry to additional accounts or systems.

Network Services

NIS

NIS has the reputation of being extremely insecure and should only be used when absolutely necessary. If the use of NIS is required,, ensure NIS maps do not contain system accounts. Establish a *securenets* file to specify the machines allowed to connect to the NIS server. NIS+, the successor to NIS, is a better alternative, but still can be exploited when improperly configured.

NIS +

Check to see if NIS+ is running in NIS compatibility mode. If the "-YP" argument is used, the server is in NIS emulation mode and is vulnerable to all NIS attacks. Permissions on NIS+

tables should be reviewed after initial installation as NIS+ is far too lax when using the default installation settings.

NFS

The Network File System (NFS) allows computers to share files in a networked environment. To better secure NFS:

- Ensure the NFS environment is not exporting sensitive file systems to the world (like /, /usr, or /etc).
- Never share critical file systems to the world with read-write access.
- Share exported file systems only with specific hosts, and not globally.
- Do not export files to "localhost".
- Share files with the "nosuid" designator, unless set-user-id execution is required.
- Ensure that file systems exported with root access are limited to only those systems that require it. This is set through the use of “anon=0” and “root=hostname” entries in the configuration file.
- Check all clients and servers to see which file systems are being mounted locally or remotely.
- Check automount directories for unauthorized automount maps. All maps should be protected with permissions 755 and owned by root/root.

DNS

The Domain Name System is the mechanism that Internet hosts use to determine the IP address that corresponds to a given hostname. Attackers often attempt zone transfers in order to gather information about a local network. The following are recommendations to greater secure DNS:

- To prevent zone transfers, filter traffic from untrusted addresses to TCP port 53 on the DNS server. This can be done via firewall or router access filters.
- Disable the BIND name daemon (named) on systems not authorized to be DNS servers.
- On the servers, upgrade to the latest version of BIND and run it as a non-privileged user in a chrooted environment.
- Hide the version string using the version option in named.conf.

Sendmail

Sendmail is an oft-targeted service. Therefore, special attention must be taken to ensure mail can be sent in a secure fashion. The following are security best practices for Sendmail:

- Upgrade to the latest version of Sendmail.
- Do not display the version number through sendmail banners by modifying the “DZ” line in the sendmail.cf file and by changing the version name in the source code before compilation.
- Ensure that the decode alias is not available. Decode should be removed or commented out of the /etc/aliases file so that it does not pipe to the 'uudecode' command and allow an attacker to overwrite system files.

- Check for non-standard entries in all users' .forward files as this can open up the system to attacks. Remove if not needed.
- Permissions on .forward files should be 640 and owned by the user.
- Run sendmail in queue mode as a root cron job on machines that are not mail servers or relays.
- If the system is not a server or does not have to listen for incoming mail, rename the sendmail startup script, binaries, and configuration files and change their permissions to 000.

Logs

System logging is crucial for troubleshooting and tracking unauthorized user accesses. Ideally, logs should be kept locally as well remotely on a central log host that does nothing but accept and store log messages. Network security policy should help dictate which events need to be audited. *Logcheck* and *swatch* are open source tools that system administrators can use to examine log files for unusual activity, based on key phrases or specially set string patterns. They can also send email to the system administrators, alerting them to possible unauthorized activity.

X-Window Environments

Since most servers do not require the use of windowing packages, remove the X Windowing environment on all servers to avoid introducing unnecessary vulnerabilities.

Distributed Server Functions

It is a good security practice to distribute the server functions of a network among separate systems. For instance, the DNS server should be separate from the mail server, which should be separate from the firewall, etc. A number of products include the software to run a web server, mail server, DNS server and other server functions all from the firewall. However, this presents a single point of failure for the network and therefore an avoidable vulnerability. Ideally, network servers should be set apart from the user segment in a secure DMZ or secure server network. Most firewalls allow this. It can also easily be accomplished by using routers behind the firewall.

Chroot Environments

chroot is a UNIX command used to run a command or interactive shell with a special root directory. This command can also be used to create virtual file systems and directory trees. If possible, configure applications like DNS, sendmail, web and ftp servers to run in a chrooted environment. In the event that the application is compromised, the adversary would then be limited to a subset of the file system and would not have access to the real root file system.

Interesting Files

Check for files that have no permissions or have invalid owners or groups. Sometimes administrators will have files that have no permissions assigned to them. These files are generally executed by a script, cron job, or other application that temporarily changes the permissions during the execution of the program, then resets the program back to the original state. Look for stray copies of password or shadow files, files with names beginning with a ".", and setuid root programs in world-writable directories and home directories.

Peripheral Devices

Malicious code can be introduced into secure networks through their peripheral devices. Therefore, care should be taken when allowing and configuring devices.

- Consider removing or restricting access to local or network peripheral devices. If an external device is not required for a specific client or server, have it removed. If the device cannot be removed, disable access to it via the hardware or software.
- Configure the systems so they cannot be booted into single-user mode via floppies or CD-ROM drives.
- Make sure floppy devices do not allow setuid programs on the floppy disk to execute as a privileged user.

Buffer Overflows

Ensure that Solaris systems have a non-executable stack environment enabled. This will help prevent buffer overflow attacks from successfully executing code on the stack. Keeping the security patches up-to-date on all UNIX systems will eliminate many well-known buffer overflow attacks.

System Utilities and Commands

Restrict access or remove system utilities such as compilers and debuggers, as well as utilities like network traffic analyzers and security scanners, that can be used to compromise other systems on the local network.

Current OS Packages

Ensure that the system packages are current. Most, if not all, UNIX systems provide the ability to check the status of system packages.

Rootkits

There are several scripts for UNIX systems that will detect rootkits. Checking the integrity of system files against a master backup known not to be altered by malicious code is also a good practice.

Security Tool

To ensure and maintain the integrity of the network servers, it is important to constantly monitor them for signs of malicious activity. There are a number of tools that can aid an administrator in this task. One tool which is commonly implemented is TCP Wrappers.

TCP Wrappers

TCP wrappers allow the administrator to log connections to TCP services -- primarily those launched by the inet daemon. It also can restrict incoming connections to these services from systems via two files, *hosts.allow* and *hosts.deny*. Both of these features can be very useful when tracking or controlling unwanted network connection attempts.

UNIX Web Servers

This section describes security configuration for UNIX web servers. The example described is an Apache web server running on Linux. This discussion assumes the Apache web server has been installed from the Apache website with default security parameters.

General Guidance

- Ensure the computer that runs the web server is a dedicated server. Do not support other services on the web server, e.g., client workstation or print server. Always upgrade to the latest production version of the web server.
- Do not perform development work on the operational web server. All data and applications should be in final form and simply copied into place on the operational server (ensure directory/file permissions are set appropriately). Create a secondary mirror of the server for all development activities and experimentation. Transfer data to the web server by tape, disk, or CD. Do not use FTP or telnet for data transfer, particularly if the data would pass over a less trusted network or unnecessarily open up access to the server. If remote access is required, use SSH or SSL services.
- Secure the host operating system as much as possible. Apply guidance from this document and others, e.g., Center for Internet Security Benchmarks, to secure the operating system. In general, remove all unnecessary services on the web server; including FTP, telnet, mail, and X Windows. If possible, use command line interfaces instead of X Windows. Using an X-windowed interface opens up ports that cannot be effectively closed and still have full system functionality. Since the server should be in production mode only, a command line is all that is required to update the site. Perform site testing from a separate client.
- Isolate the web server physically and virtually. If possible, allow local web server access to the fewest number of users. Locate the web server close to the administrator, web engineer, or webmaster. Place the web server on a LAN segment separate from the rest of the IT infrastructure. Do not mount or share services to and from the server.

Example: Apache

Apache HTTP Server 2.2.0 is the latest version, as of 25 January 2006, and is available at [1]. Please reference the CIS “Apache Benchmark for Unix” at [3] for more complete instructions on securing an Apache installation.

- Clean the Apache root directory by deleting all directories and files not needed to run the production web server. For most servers, the important directories are bin, cgi-bin, conf, error, htdocs, lib, and logs. If modules are used, which are loaded at run time, the modules directory is also needed (which should only contain the modules required). Also, remove preinstalled test scripts (like printenv and test-cgi) and html content before adding your own web server.

- Create a unique user and group for running the Apache HTTP Server in the Operating System. Lock down the user so it can only be used by a server (e.g., no interactive login). Then, remove any interactive login files that are left in the web user directory.

  Example – to create the user and group:

  groupadd web

  useradd –d /usr/local/apache2/htdocs –g web –c “Web Server Account” –m web

  Example – method to lock down the user account:

  passwd –l web

  usermod –s /bin/false web

  Example – remove login files from web user directory:

  rm .bash_logout .bash_profile .bashrc

- Ensure the web administrator (in this case root) owns all the files within the Apache root directory. Example:

  chown –R root:root /usr/local/apache2

- Set permissions on the web server directories.

  In general, only the web administrator requires the ability to write to files in any apache directory. Therefore, ensure that this capability is limited to only the web administrator. In our example, all files are under the /usr/local/apache2 directory, so this can be done with one command:

  chmod –R o-w /usr/local/apache2

  Now, set the permissions on the sub-directories. There is no need for “world” to have access to the bin, conf, error, lib, or logs directories, so remove the other access. Example:

  chmod –R o-rwx /usr/local/apache2/bin

  chmod –R o-rwx /usr/local/apache2/conf

  chmod –R o-rwx /usr/local/apache2/error

  chmod –R o-rwx /usr/local/apache2/lib

  chmod –R o-rwx /usr/local/apache2/logs

  There should be no executables located in the htdocs directory structure; therefore, remove the executable flags from all files within the htdocs sub-directory. Example:

  chmod –R 664 /usr/local/apache2/htdocs

  chmod –R +X /usr/local/apache2/htdocs

  Finally, no data should be written into the cgi-bin directory; therefore, ensure all write permissions are removed. If a cgi script needs to write data to a file, create a new directory, e.g., /usr/local/apach2/cgi-data.

  Example - for removing write permission from cgi-bin:

  chmod –R -w /usr/local/apache2/cgi-bin

- Modify the Apache configuration file.

  Ensure the user running the Apache web server and its group are unique. Modify the lines in the `httpd.conf` file in the `/usr/local/apache2/conf` directory that relate to this. Example:

  User web

  Group web

  Configure the ServerName. Example:

  ServerName www.myserver.org:80

  Configure the root directory for the web server. Make sure all options are off and the directory is not accessible through the web interface.

  <Directory />

  Options None

  AllowOverride None

  Order deny,allow

  deny from all

  </Directory>

  Configure the web content directory. Do not turn on any options that are not needed. In particular, there is no need for Indexes, which provide access to directories that have no explicit web content. `FollowSymLinks` should also be disabled, if possible. The server will follow any symlink in the directory with the permissions of the web server. If symlinks are required, consider using a chroot jail for the web server (see CIS “Apache Benchmark for Unix” for more details). The Example below explicitly disables all options. Keep all ExecCGI scripts in their own directory structure; do not incorporate CGI scripts within content directories. Limit web methods to GET (HEAD requests are included with GET when using the LimitExcept directive) and POST. Only allow additional access types if you are explicitly using them.

  <Directory "/usr/local/apache2/htdocs">

  <LimitExcept GET POST>

  deny from all

  </LimitExcept>

  Options –Indexes –Includes –FollowSymLinks -MultiViews

  AllowOverride None

  Order allow,deny

  Allow from all

  </Directory>

- For additional security mechanisms, consider using chroot or mod_security. A discussion of these is beyond the scope of this document. A discussion on chroot and mod_security is included in the “Apache Benchmark for Unix” at www.cisecurity.org. The code and documentation for mod_security can be found at www.modsecurity.org.

- Another important part of security is logging. By default, Apache's log level is set to warning, which is acceptable for most situations. By default, Apache logs web accesses to the access_log and server information (errors, etc) to the error_log file, located in the /usr/local/apache2/logs directory. It is important to back up these files periodically for forensics reasons and to prevent the logs from filling up the disk.
- Additional information can be found at:

  http://www.apache.org/docs - Apache Documentation (choose correct release). This site includes a Security Tips page.

Intrusion Detection Systems (IDS)

This section of *The 60 Minute Network Security Guide* departs from the explicit detail of previous sections and provides a brief overview of Intrusion Detection Systems, describing in general terms the steps to be taken when deploying IDS in your environment.

Generally, there are two types of IDS: host based and network based. Host based IDS monitor security within a network component, such as a server or a workstation. Network based ID systems monitor the traffic between network components and networks. Some IDS are strictly network based, whereas others are a combination of network and host based.

Most IDS are comprised of two components: sensors and managers. Depending on the IDS type, sensors can be either network based or host based.

The following are steps to be taken when deploying an IDS.

Step 1 - Identify what needs to be protected

To maximize the utilization of IDS, the organization must first determine in order of priority what needs to be protected. For many organizations, the various servers (e.g.., application, database, file and domain controllers) contain mission-critical resources. Furthermore, depending on the organization, some departments may be more critical than others or must enforce different trust relationships. All of this must be defined in a priority list prior to deploying any IDS.

Step 2 - Determine what types of sensors are required

The types of sensors that are required are dependant on the priority list defined in Step 1. A host sensor would be used to monitor a critical server, whereas a network sensor would be used to monitor network entry points and critical network segments.

Another important issue to consider is how many sensors the organization can afford to buy. This number will influence how the sensors are deployed throughout the network, as the number of critical resources must be balanced against how many sensors can be acquired and maintained.

Step 3 - Configure host system securely

Prior to loading any IDS, the host that the IDS will reside on must be configured securely. Often, the vendor of the IDS will supply its own host to run the IDS sensor, in which case, the vendor should supply guidelines on how to secure that host. Otherwise, the IDS typically reside on UNIX and Microsoft Windows NT/2000 hosts. The guidelines for securing UNIX and Microsoft Windows NT/2000 systems are well documented elsewhere in this document.

Step 4 - Keep signature database current

The majority of IDS that are currently available for use are signature based. Because new vulnerabilities and attacks are being discovered daily, the signature database must be kept current. The respective vendors should supply the latest signatures for their IDS.

Step 5 - Deploy IDS sensors

The final phase is to actually deploy the IDS. The following scenarios are based on how many sensors are available for deployment versus what is deemed critical.

Scenario 1

If the organization can only afford to purchase and monitor one sensor of any type, then it should be a network sensor. As described earlier, a network sensor is much better suited to monitoring large segments of a network, whereas a host sensor is limited to monitoring the system that it resides on. In this scenario, the ideal location to place the sole network sensor is in the DMZ, between the external router and the firewall, as shown in Figure 1. In spite of having only one sensor, this design allows the IDS to be used for maximum effectiveness. By placing the IDS sensor between the external router and the firewall, the sensor can monitor all network traffic going to and coming from the Internet.

Furthermore, because the router can filter all incoming traffic from the Internet, the IDS sensor can be tuned to ignore certain types of attacks, thereby allowing the sensor to operate with maximum efficiency.

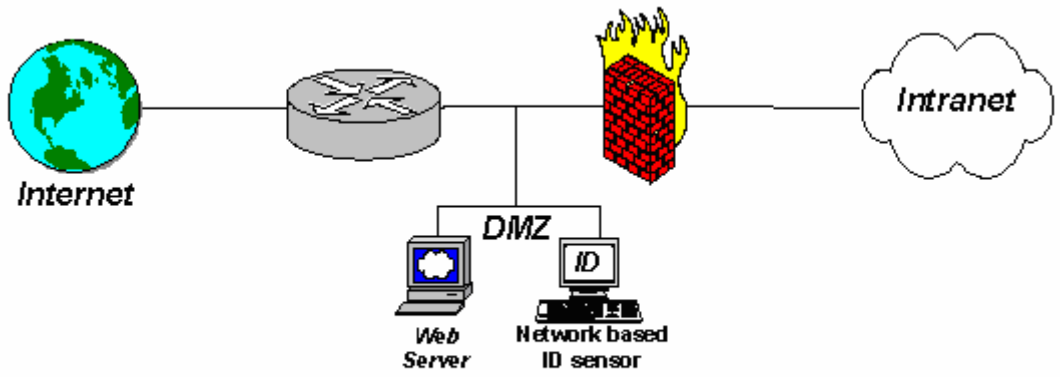

Figure 1 - Deploying 1 ID system

Scenario 2

In the case where only two sensors of any type can be acquired and maintained, then they should be network sensors. Like the previous scenario, one of the sensors should be placed in the DMZ, between the external router and the firewall. The second sensor should then be placed between firewall and the intranet, as shown in Figure 2. The second sensor can indicate what attack breached the firewall. By strategic placement of these two sensors, all access points from the Internet will be monitored.

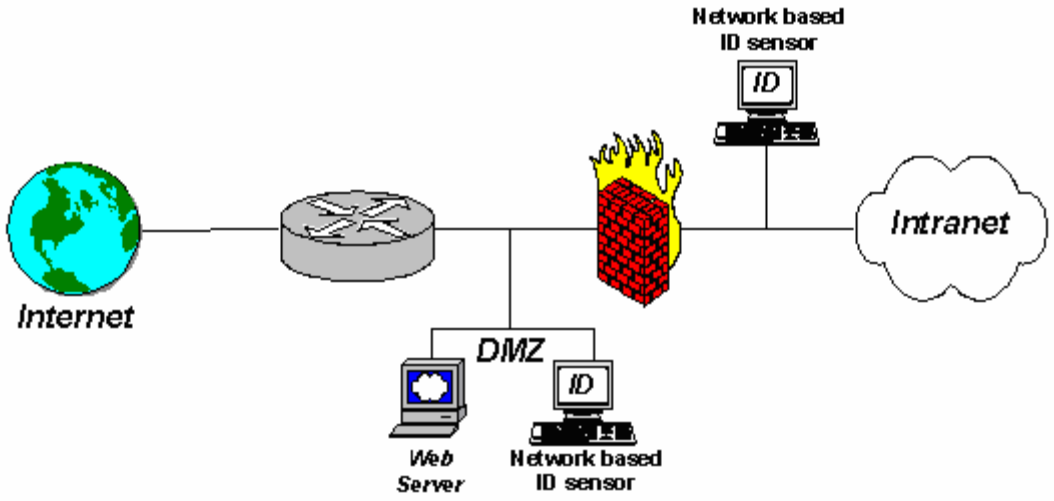

Figure 2 - Deploying 2 ID systems

Scenario 3

If more than two sensors of any type can be acquired and maintained, then at least two should be network sensors. Those sensors should be deployed as described in Scenario 2. If a critical LAN within the intranet needs to be protected, then a network sensor should be placed at the entry point to that LAN. The remaining sensors should be host sensors that are loaded onto critical servers, such as domain controllers, file servers, web servers, and mail servers. The order of what is deemed critical is determined by the organization, as directed in Step 1.

Step 6 - Management and Configuration

The other component of IDS, the manager, should be centrally located where dedicated security staff can monitor the health of the systems and network. Many organizations have a Network Operations Centers (NOC) that fulfills the role of a central location to place the manager. IDS sensors could then report all alerts to the NOC, thereby allowing the security staff to respond quickly to attacks and to notify the appropriate authorities, such as CERT technicians.

The other issue to consider is how to configure the sensors. Careful configuration of the sensors can increase the effectiveness of IDS and all unnecessary signatures should be disabled. For example, if the network is entirely composed of Microsoft Windows systems, then the sensors can be configured to ignore any attacks that are directed against UNIX systems (however, it would be prudent to monitor for the unexpected presence of a UNIX service). An organization can see great benefit in an IDS with the combination of a priority list as defined in Step 1 and a careful analysis of the proper configuration.

References

1. Apache HTTP Server Project. http://httpd.apache.org/

2. Bartock, Paul and Pitsenbarger, Trent. *Outlook E-mail Security in the Midst of Malicious Code Attacks*. Available at http://www.nsa.gov/snac/downloads_docs.cfm?MenuID=scg10.3.1

3. Center for Internet Security Level-1 & 2 Benchmark and Scoring Tool for the Apache Web Server. http://www.cisecurity.org/bench_apache.html

4. Christman, Sheila M. and Walker, William E. IV. *Guide to Secure Configuration and Administration of Microsoft Internet Information Services 5.0* Available at: http://www.nsa.gov/snac/downloads_miis.cfm?MenuID=scg10.3.1.4

5. *Microsoft Security Baseline Analyzer 2.0. A Microsoft,* Technet description and download link available at: http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx

6. *Microsoft Windows Server 2003 Security Guide*. Available at: http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx

7. *Microsoft Windows XP Security Guide*. Available at: http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.mspx.

8. The National Security Agency's System Network Attack Center's security configuration guide series, available via HTTP at http:\\www,nsa.gov\snac.

9. *Secure Internet Information Services 5 Checklist,* Available from Microsoft at: http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/iis/tips/iis5chk.mspx

10. *Site Security Handbook*, available via ftp at ftp://ftp.rfc-editor.org/in-notes/fyi/fyi8.txt

11. *UrlScan Security Tool*. A Microsoft Technet description and download link available at: http://www.microsoft.com/technet/security/tools/urlscan.mspx

12. *Windows Server Update Services.* A Microsoft description and download link available at: http://www.microsoft.com/windowsserversystem/updateservices/default.mspx