

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

SANS GCNT Practical Assignment

© SANS Institute 2000 - 2002, Author retains full rights.

Securing/Auditing Windows NT 4.0 Web Server Bastion Hosts in the DMZ

Kerry Steele

4/4/2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

EXECUTIVE SUMMARY 4
BASTION HOST DEFINITION 5
DMZ ENVIRONMENT CONFIGURATION 5
DMZ FIREWALL POLICIES EXAMPLE 5
DMZ NETWORK ENVIRONMENT CONFIGURATION DIAGRAM EXAMPLE 6
HACKER POINT-OF-VIEW 7
NETWORK FIREWALL 8
RESTRICT PHYSICAL ACCESS TO SERVERS 8
VIRUS PROTECTION 8
DNS AND WINS SERVERS 8
INCIDENT HANDLING GUIDE 8
C2 SECURITY 8
EMERGENCY REPAIR DISK – ERD 9
DRIVE IMAGING 9
REMOVABLE DRIVE CARTRIDGES 9
SPARE SERVER 9
BACKUPS 9
VERIFYING THE DMZ WEB SERVER BASTION HOST SECURITY USING COMMERCIAL VULNERABILITY ANALYSIS TOOLS 10
NETWORK-BASED INTRUSION DETECTION SYSTEM – AUTOMATED PROTOCOL ANALYZERS 11
HOST-BASED INTRUSION DETECTION SYSTEM – AUTOMATED EVENT LOG ANALYZERS 11
HOST AND DATA INTEGRITY 12
HOST AVAILABILITY AND MONITORING 12
SECURITY UPDATES – STAY UP TO DATE WITH SECURITY EXPLOITS AND VULNERABILITIES 13
INSTALLATION 14
IIS INSTALLATION 14
INSTALL THE LATEST SERVICE PACK AND HOTFIXES 15
THIRD PARTY TOOLS TO MANAGE HOTFIXES 16
IIS CONFIGURATION – DELETE ADMIN AND SAMPLE SCRIPTS 18
MOVE COMMON ADMINISTRATIVE TOOLS 19
IIS – DISABLE ABILITY TO CALL THE COMMAND SHELL WITH #EXEC 19
IIS – REMOVE UNUSED APPLICATION MAPPINGS 20
IIS – DISABLE PARENT PATHS 21
IIS – VIRTUAL DIRECTORY PERMISSIONS 22
IIS – SCRIPTED AND EXECUTABLE CONTENT 22
IIS – LOGGING OPTIONS 22
COM SECURITY 22
MODIFICATION OF HIGH SECURITY TEMPLATE FOR AN IIS SERVER 23
MICROSOFT SECURITY CONFIGURATION EDITOR 24
SECEDIT OVER THE NETWORK USING A BATCH SCRIPT 24
SECEDIT LOCALLY USING A FLOPPY DISK 25
THIRD PARTY SECURITY TEMPLATES 25
REMOVE OR DISABLE NON-ESSENTIAL SERVICES AND DRIVERS 26
TCP/IP INTERNALS 27
PORT NUMBER ASSIGNMENTS 27
TCP/IP PARAMETERS 28
SYN FLOODS 29
DISABLE NETBIOS 30
BLOCK NON-ESSENTIAL PORTS 31
REMOVE THE OS/2 AND POSIX SUBSYSTEMS 32
PROTECT USER ACCOUNTS AND PASSWORDS 33
ENCRYPT THE SAM DATABASE WITH SYSKEY 34

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SYSKEY – METHOD OF STORAGE 35
APPLY THE SYSKEY HOTFIXES 35
ADMINISTRATOR ACCOUNT PASSWORD 36
ENFORCING COMPLEX PASSWORDS WITH A PASSWORD FILTER 36
ADMINISTRATOR ACCOUNT LOCKOUT AND COMPLEX PASSWORDS 36
WEB-BASED USER ACCOUNTS (AND OTHERS) 37
RENAME ADMINISTRATOR ACCOUNT 38
GUEST ACCOUNT 38
REMOVE THE "ACCESS THIS COMPUTER FROM THE NETWORK" RIGHT FROM THE ADMINISTRATORS GROUP 38
SERVICE ACCOUNTS 39
SERVICE ACCOUNT MANAGEMENT 39
NT USER MANAGER ACCOUNT AND PASSWORD POLICY 40
RESTRICTING NULL USER SESSIONS 41
DISABLE NULL SESSION ACCESS TO SHARES 42
DISABLE NULL SESSION ACCESS TO NAMED PIPES 42
RESTRICT REMOTE NETWORK ACCESS TO THE REGISTRY 43
REGISTRY MANIPULATION UTILITIES 43
RESTRICT REGISTRY ACCESS TO PREVENT KNOWN TROJANS 44
RESTRICT GUEST ACCESS TO EVENT LOG 45
SECURE ACCESS TO THE EVENT LOG FILES 45
EVENT LOG SETTINGS 46
SERVER CRASH WHEN SECURITY LOG FILLS - CRASHONAUDITFAIL 46
TOOLS TO MANAGE EVENT LOGS 46
REGISTRY AUDITING – BEST PRACTICES 47
SECURE NTFS PERMISSIONS 48
USER MANAGER AUDIT POLICY 50
TOOLS TO MANAGE NTFS PERMISSIONS AND AUDITING 51
ADVANCED USER RIGHTS ASSIGNMENT 52
DISABLE CACHED LOGONS 53
DISABLE ADMINISTRATIVE SHARES 53
DISABLE 8.3 FILE NAME CREATION 53
HIDE THE LAST LOGON USER NAME 53
SECURE PRINTER DRIVERS 54
CONTROL ACCESS TO THE SCHEDULE SERVICE 54
DISABLE BOOT TO ANOTHER OPERATING SYSTEM USING THE FLOPPY DRIVE 54
PREVENT EXPLOIT OF TROJAN NOTIFICATION PACKAGES AND SUB-AUTHENTICATION PACKAGES 55
REFERENCES 56
NTLMV2 AUTHENTICATION 58
SMB MESSAGE SIGNING 59
SECURING THE NETLOGON CHANNEL 60
AUDIT TAPE BACKUPS AND ADDITIONAL USE OF USER RIGHTS 61
FILE ENCRYPTION ON NTFS 4 VOLUMES 61

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Executive Summary

This guide was developed with the goal to include many of the means available to secure a Windows NT 4.0 Web Server running Internet Information Server 4.0 to be configured as a bastion host and placed in the DMZ, and to meet the practical assignment requirement for the SANS GCNT certification.

This will be accomplished by addressing methods to prevent a hacker from exploiting known vulnerabilities of Windows NT Server 4.0 and Internet Information Server 4.0.

This guide can be used to audit existing servers, plan for deployment of new servers, or to secure existing servers in the DMZ. Justifications should be provided for each deviation from these guidelines. This document should be used in conjunction with other guidelines available such as:

- Microsoft Internet Information Server 4.0 Security Checklist http://www.microsoft.com/technet/security/iischk.asp
- Securing Windows NT, Step-by-Step by Jason Fossen
- Securing Windows NT/2000 Servers for the Internet by Stefan Norberg

The steps in this guide should not be applied directly to a production web server, as they may break certain functionality of the server. The actions outlined in this document should first be applied to a web server in a mock production environment (or the security administrators themselves may be the cause of a Denial of Service). Once the functionality of the server has been verified, then it would be appropriate to perform the same steps on a production server.

Throughout this document, I will be following the concept of defense in depth, which will entail hardening the system at multiple levels to minimize the possibility of intrusion. With defense in depth, a single device alone will not enforce the security policy. The network will be compartmentalized, and each compartment will be fortified against intrusion.

Following these concepts, deploying a hardened firewall alone will not suffice, as the avid hacker will ultimately find ways past this front-line measure of defense, and many exploits occur on ports that are usually open on the firewall such as HTTP (80) and DNS (53). Attention will be given to several areas, since attackers will try many different techniques in their attempt to exploit vulnerabilities in the DMZ. If a hacker is serious about breaking into a system, the additional hurdles may provide time to track down the hacker or to stop the attack before it occurs.

Honey pot tactics, such as honey pot servers and marked files, although quite useful, will not be discussed in this document in great detail. I will note that it is useful to implement honey pot tactics through the careful implementation of registry and file permissions and auditing on known targets of the host in order to detect intrusion attempts. This technique works well in conjunction with a Host-Based Intrusion Detection System.

I have included many tools that come to mind for each topic.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

DMZ Definition – Demilitarized Zone

A DMZ is a perimeter network that is configured as a "neutral zone" between a company's private internal network and the Internet.

Bastion Host Definition

A bastion host is an application server that is placed in a company's perimeter network. These servers are configured to provide one single application service, such as Web/HTTP services or Proxy services, and other unnecessary services and operating system features are removed or disabled. The process of securing a bastion host is commonly referred to as "hardening".

DMZ Environment Configuration

Although each DMZ environment will differ slightly, a secure perimeter configuration may have common characteristics including (based on the examples provided in Securing Windows NT/2000 Servers for the Internet):

- No direct traffic is allowed between the Internet and the internal network.
- If one component in the DMZ is compromised, the entire DMZ should not be compromised. This is achieved by configuring the components of the DMZ on separate segments, and compartmentalizing the servers based upon the services they provide.
- If one component in the DMZ is compromised, the internal network should not be compromised. This is achieved by isolating the internal network from the DMZ network.

DMZ Firewall Policies Example

(Based on the examples provided in Securing Windows NT/2000 Servers for the Internet):

Inbound HTTP traffic (TCP/80) is allowed to the DMZ web servers only.

Outbound HTTP (TCP/80), HTTPS (TCP/443), and FTP (TCP/21) are allowed from the DMZ proxy server only.

Inbound SMTP traffic (TCP/25) is allowed to the DMZ mail gateway only.

Outbound SMTP (TCP/25) is allowed from the DMZ mail gateway only.

The DMZ mail gateway is allowed to relay incoming mail to an internal mail server, and the internal mail gateway is allowed to relay outgoing mail to the DMZ mail gateway.

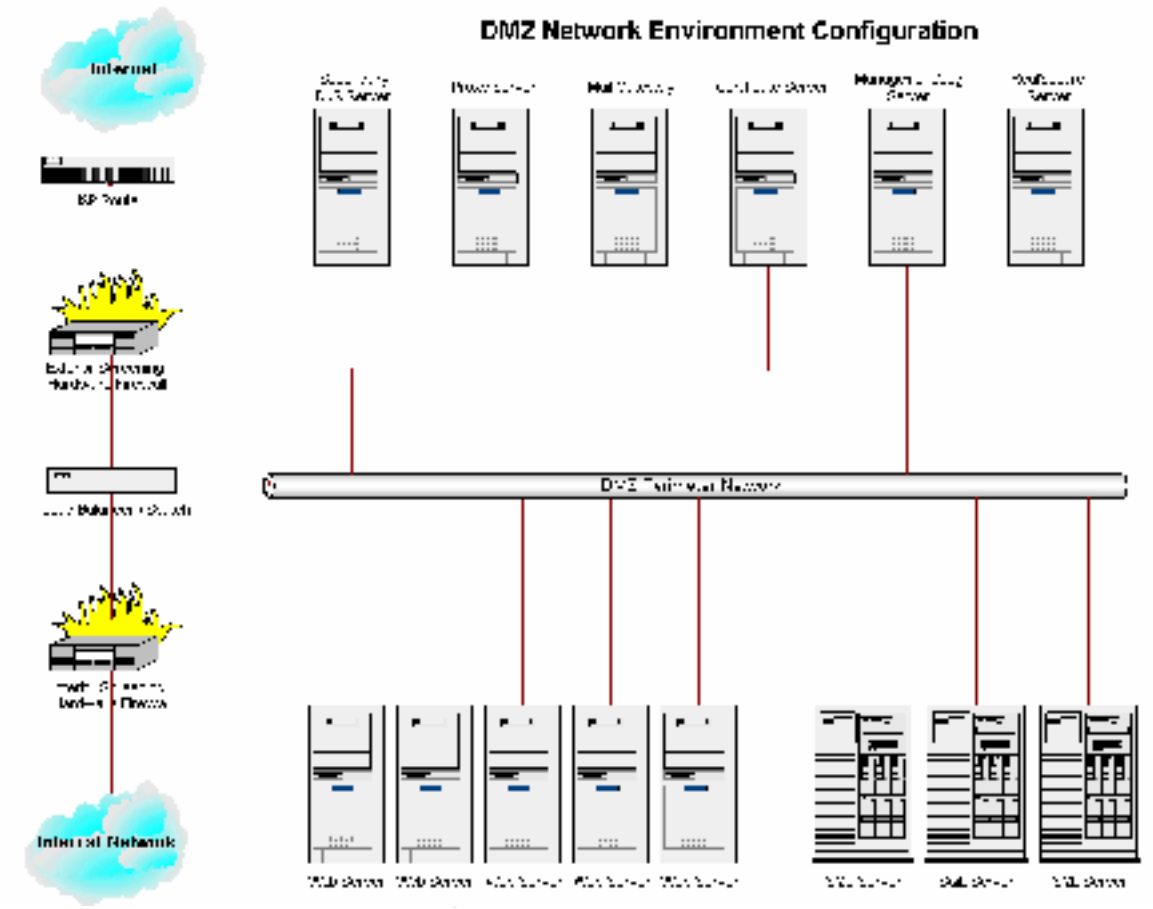
DNS queries (UDP/53) are allowed from the DMZ proxy server and DMZ mail gateway only.

The internal network is allowed to use the DMZ proxy server only.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

DMZ Network Environment Configuration Diagram Example



© SANS Institute

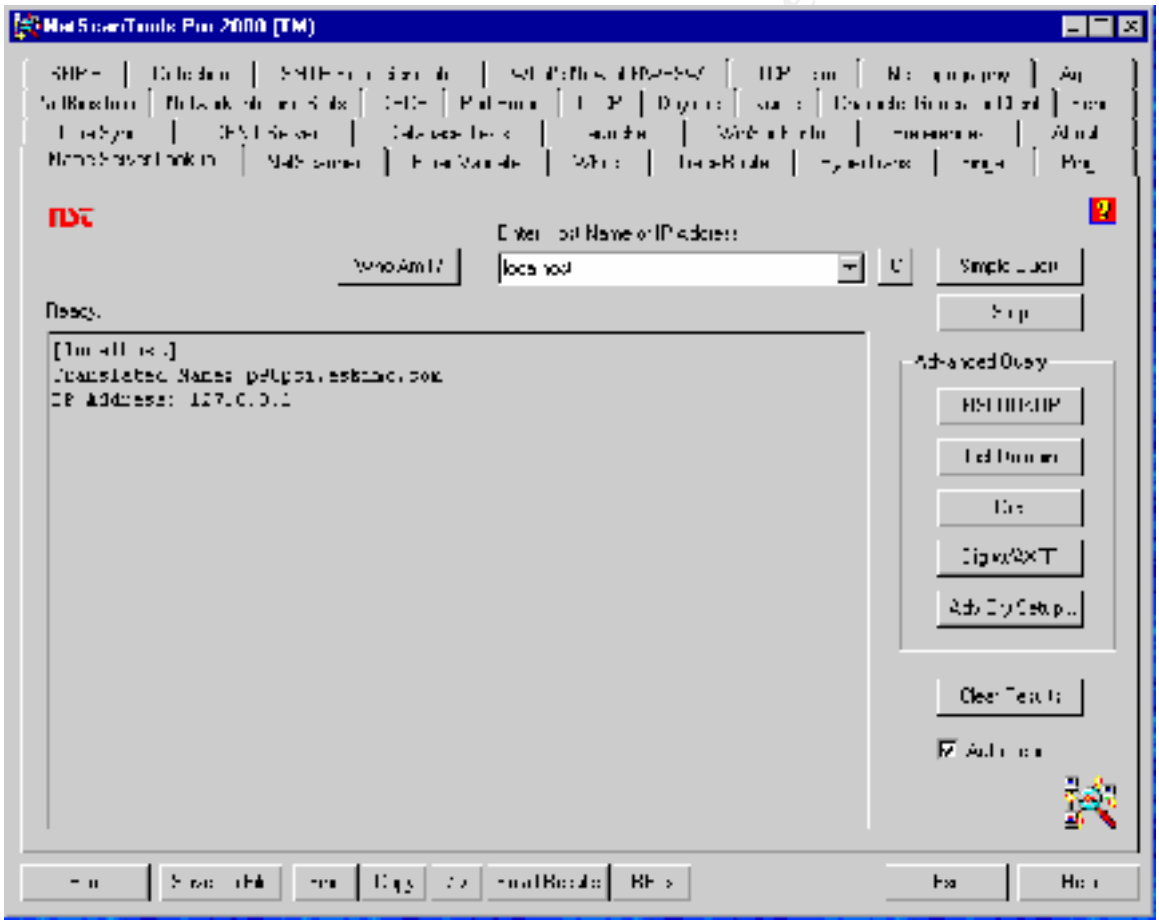
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Hacker Point-of-View

Use hacker tools to analyze the bastion hosts in the DMZ. Common hacker tools include:

- Netcat – http://www.l0pht.com/~weld/netcat/
- @stake (list of tools) – http://www.atstake.com/research/tools/index.html
- Port Scanners – Ostrosoft Internet Tools – http://www.ostrosoft.com/index.html
- NETBIOS Name and share scanners – Legion from Rhino9 and NBTSTAT
- Administrator and hacker tools – http://www.nttoolbox.com
- NMAP – http://www.eeye.com/html/Research/Tools/nmapnt.html
- Whisker – http://www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2nmap
- Rhino9 Grinder – http://hackersclub.com/km/files/hfiles/index.html
- Enum – http://razor.bindview.com/

- NetScan Tools Pro 2000 – http://www.nwpsw.com



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network Firewall

Deploy a network firewall with stateful packet-filtering capabilities. A best practice is to configure the firewall to DENY ALL, making exceptions for necessary services. For example:

- Nokia/CheckPoint FireWall-1 – http://www.checkpoint.com/products/firewall-1/index.html
- Cisco PIX – http://www.cisco.com/warp/public/cc/pd/fw/sqfw500

Restrict Physical Access to Servers

The bastion hosts in the DMZ network should be located in a physically secured location with monitored access.

Virus Protection

Install on all servers and workstations (including firewalls, proxy servers, email gateways, etc.), and configure the software to automatically update the virus definition lists on a regular basis. For example:

- Network Associates NetShield for NT – http://www.mcafeeb2b.com/products/netshieldnt/default.asp

DNS and WINS Servers

Configure DNS Server in the DMZ to prohibit unauthorized zone transfers.

WINS servers should not be installed in the DMZ unless absolutely necessary.

Incident Handling Guide

For more information about how to handle computer security incidents:

- Computer Security Incident Handling: Step-by-Step – SANS http://www.sans.org/newlook/publications/incident_handling.htm

C2 Security

For information about C2 Security, see the Windows NT C2 Configuration Checklist: http://www.microsoft.com/TechNet/security/c2config.asp

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Emergency Repair Disk – ERD

Update the emergency repair disk after changes are made to a server.

Use the RDISK /S- command to make a copy of the current SAM database and the registry files in the %SystemRoot%\repair folder. As the SAM database may not fit on a floppy, copy these files to a central secured location for archive.

Drive Imaging

Use Ghost to create a binary drive image of the server. In the event of a disaster, restore the server from the binary drive image.

Removable Drive Cartridges

Install a drive caddy so that a new drive can be swapped out in the event of a disaster. By far, this is the quickest method of recovery since the drive is preconfigured. Using drive-imaging software such as Ghost in addition to the drive caddies provides a quick and easy way to recover from a disaster.

Spare Server

Keep a fully configured spare test server for use in the event of a disaster.

Backups

Implement disaster recovery using commercial tape backup software.

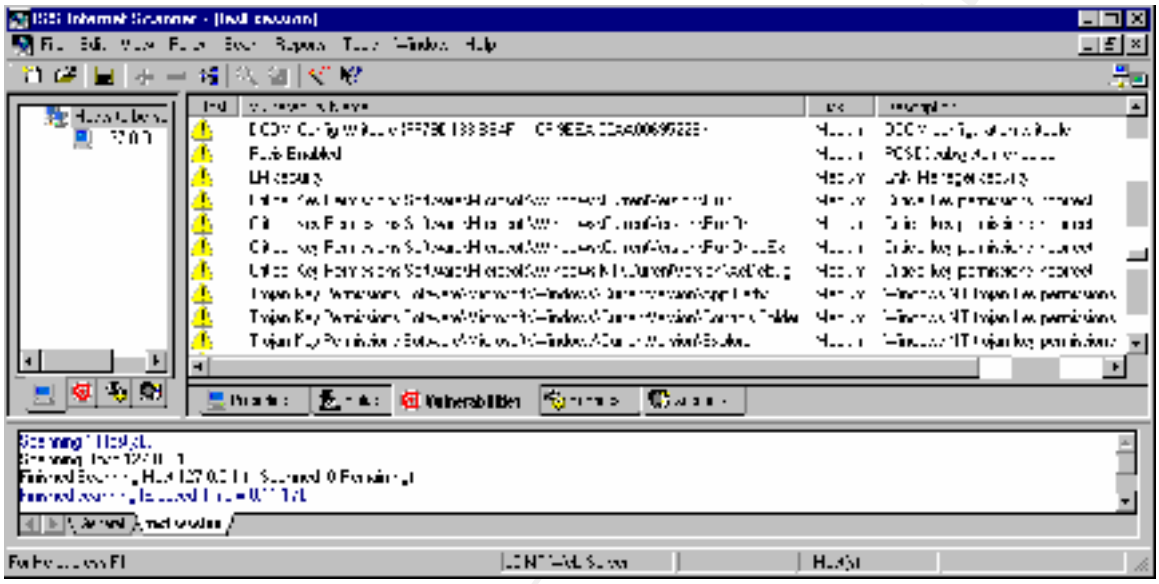
© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Verifying the DMZ Web Server Bastion Host Security Using Commercial Vulnerability Analysis Tools

Using a Vulnerability Analysis tool to assess the security of corporate web servers is an essential task to validate the security of the bastion hosts in the DMZ. For example:

- Internet Security Systems Internet Scanner – http://www.iss.net – http://documents.iss.net/literature/InternetScanner/is_ps.pdf



- bv-Control for Internet Security – http://www.bindview.com/products/bvControl/internetsec/index.cfm?Area=6&Product=14
- eEye Retina – http://www.eeye.com/html/Products/Retina/index.html
- WebTrends Security Analyzer – http://www.webtrends.com/products/wsa/default.htm
- System Scanner from Internet Security Systems – http://www.iss.net – a utility to locally verify the security on a DMZ Web Server (and it's included with the Windows 2000 Resource Kit in the apps\systemscanner directory):
- CyberCop Scanner– http://www.pgp.com/products/cybercop-scanner/default.asp
- CyberSafe Centrax – http://www.cybersafe.com/centrax
- STAT – http://www.statonline.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Network-Based Intrusion Detection System – Automated Protocol Analyzers

A network-based intrusion detection system analyzes network traffic in real-time and takes the appropriate action to stop an attack before damage occurs by modifying the firewall to block the attackers IP address, launching custom programs, killing the TCP session of the attacker, or notifying security administrators.

"Network-based IDS (Intrusion Detection Systems) form their attack detection upon the comparison of parameters of the user's session and the users commands to a rule-base of techniques used by attackers to penetrate a system" (known attack/intrusion signatures) (Paller, 111). Network-based IDS detect potential attacks. For example:

- Internet Security Systems – RealSecure – http://www.iss.net
  http://documents.iss.net/literature/RealSecure/rs_ps.pdf
  http://www.iss.net/customer_care/resource_center/product_lit/

- Cisco NetRanger – http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml

- NFR Network Intrusion Detection – http://www.nfr.com/products/NID

Host-Based Intrusion Detection System – Automated Event Log Analyzers

A host-based intrusion detection system analyzes a hosts event logs (including database, web, application, system, security, etc.) in real-time and takes defensive action in response to suspicious activity or actual intrusions. As it is impossible to manually sift through event logs, a third party tool is critical in this situation. The tools can be configured to watch for specific events or patterns, attempted or successful actions, and will log off and disable intruder accounts, shut down the system, notify security administrators, etc. when suspicious or malicious activity is detected. Host-based IDS detect actual attacks. For example:

- Internet Security Systems – RealSecure – http://www.iss.net
  http://documents.iss.net/literature/RealSecure/rs_ps.pdf
  http://www.iss.net/customer_care/resource_center/product_lit/

- CyberSafe Centrax – http://www.cybersafe.com
  http://www.cybersafe.com/centrax/index.html

- Symantec Intruder Alert –
  http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48&PID=3460023

Host-based intrusion detection systems are an excellent combination with honey pot tactics.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Host and Data Integrity

In order to detect tampering with the configuration, file system and registry of a web server bastion host, a third party tool is needed to monitor file content integrity and system and registry attributes. By taking a snapshot of the system before it is placed in the DMZ, it is possible to later identify if the file system or registry has been compromised or tampered with.

- Tripwire for Servers – Host and Data Integrity Verification
  http://www.tripwire.com/products/servers

  Takes a digital snapshot of the system, including core operating system files, using a cryptographic hashing technique. Files are routinely tested for tampering.

- Pedestal Software – INTACT
  http://www.pedestalsoftware.com/intact/index.htm

  Intact detects changes to the system by taking a snapshot of system objects and then comparing the snapshot to the active system in real-time.

- File Comparison Utility – compare the tampered file with the original
  http://www.componentsoftware.com/csdiff

Host Availability and Monitoring

To monitor the availability of the bastion hosts in the DMZ, a third party tool is needed. For example:

- Prognosis for Windows – server, network, application, and database availability monitoring and management utility
  http://www.prognosis.com/prognosis_nt.asp

- IP Sentry – Host Availability Monitoring
  http://www.ipsentry.com

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Security Updates – Stay up to date with Security Exploits and Vulnerabilities

Windows NT security vulnerabilities circulate throughout the hacker community quickly. When a new hotfix is released, quickly determine if the bastion hosts are vulnerable to the exploit, and apply the appropriate hotfix.

The best way to stay on top of these new developments is to subscribe to security bulletins available at:

- http://www.microsoft.com/technet/security/notify.asp
- http://www.microsoft.com/technet/security/current.asp
- http://www.securityfocus.com
- http://www.win2000mag.com
- http://www.ntbugtraq.com
- http://www.sans.org
- http://www.cert.org

Some other useful security-related sites include:

- http://www.phrack.com
- http://packetstorm.securify.com
- http://www.2600.com
- http://www.attrition.org
- http://www.l0pht.com
- http://www.packetfactory.net
- http://www.ntsecurity.net
- http://www.nttoolbox.com
- http://www.somarsoft.com
- http://www.winternals.com
- http://www.sysinternals.com
- http://www.hackersclub.com
- http://www.atstake.com
- http://www.ussrback.com
- http://www.rootshell.com
- http://www.hackingexposed.com

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Installation

- Install Windows NT Server 4.0 as a Stand Alone Server.
- Create two partitions – one for the operating system (C:), and one for IIS (D:).
- Use only NTFS file systems for file storage, as the security features of NTFS such as auditing and permission level protection are not available on the FAT file system.
- Update the server to SP6a 128 bit (see the section "Install the Latest Service Pack and Hotfixes" on the next page).
- Install Internet Explorer 5 from the MSDN (Install only the web browser component).
- Install only the TCP/IP protocol with a static IP address.
- Do not install miscellaneous services such as the Network Monitor Agent unless necessary.
- Place a paging file for virtual memory on both partitions.
- Install the post Service Pack hotfixes from http://www.microsoft.com/technet/security/current.asp

IIS Installation

Using the Windows NT 4.0 Option Pack, install IIS on a separate partition from the operating system (the D drive in this case).

When prompted during the installation, perform a Custom Installation, and install only the needed components. Deselect:

- Front Page 98 Server Extensions
- Documentation – load this on your mock production server or workstation
- File Transfer Protocol (FTP) Server – dedicate a separate server to FTP
- Internet Service Manager (HTML) – this forces you to sit at the console
- SMTP Service
- World Wide Web Sample Site
- Microsoft Index Server – unless your site uses Index Server
- Microsoft Script Debugger
- Transaction Server Core Documentation
- Remote Data Service 1.5 (RDS/ADC)
- ADO Documentation

Start with a minimal configuration, and add components as they are needed.

The only components that you should have selected are:

- Internet Service Manager
- World Wide Web Server
- Data Sources
- MDAC Core files
- Microsoft Management Console
- NT Option Pack Common Files
- Transaction Server Core Components
- Windows Scripting Host

When prompted, configure MTS for Local Administration.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Install the Latest Service Pack and Hotfixes

Install the Domestic version (128-bit) of the latest service pack, Service Pack 6a
http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/128bitX86/default.asp

To avoid having to reapply the service pack after making modifications to a system, extract the service pack to the i386 folder by using the "/x" switch.

Hotfixes are updates that are later bundled into a Service Pack. To ensure that corporate servers are not exposed to the vulnerabilities patched by the hotfix, apply the appropriate hotfixes after you have determined that your system is in fact exposed to the vulnerability. For example, if a Hotfix for DNS is released and you are not running the DNS Service, you do not need to apply that particular hotfix. Remember to apply the hotfixes in the order of release date.

Service Pack 6a is the final Service Pack for NT 4.0, so it is essential to apply the appropriate Hotfixes for your system.

Hotfixes should not be applied to production servers without first being tested on a mock production server. Apply the hotfix to the mock production server, test and verify functionality of your applications, and then apply the hotfix to the production server

To stay up to date with Security patches, subscribe to the Microsoft Security Notification Service:
http://www.microsoft.com/technet/security/notify.asp

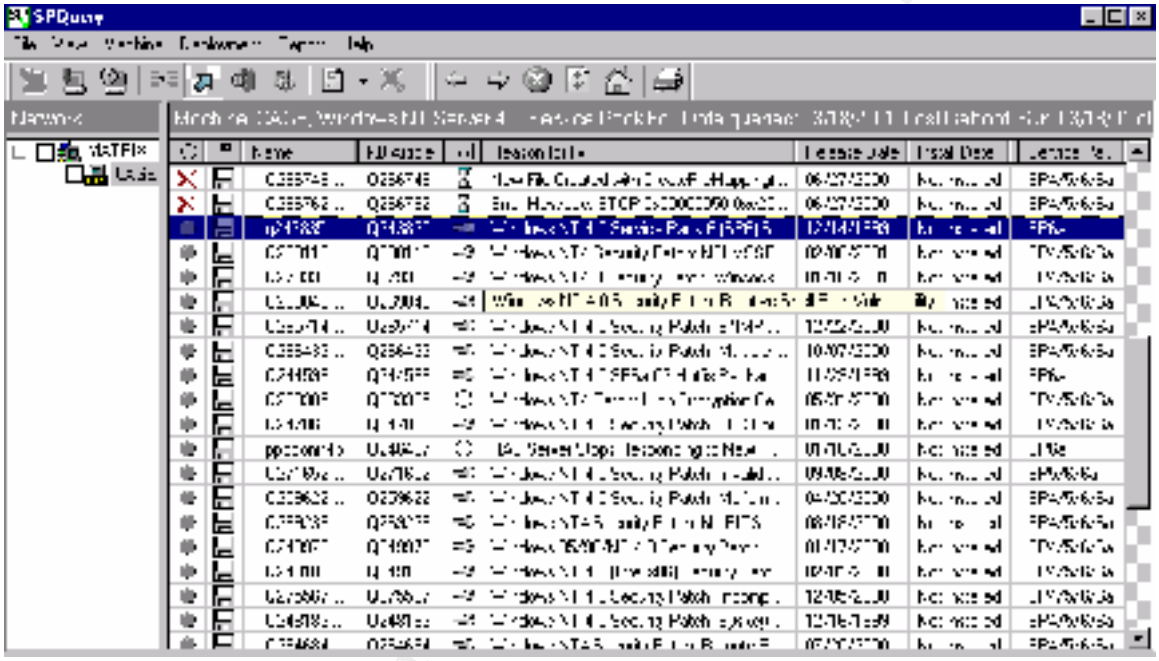
© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Third Party Tools to Manage Hotfixes

An excellent tool to keep systems up to date with the appropriate hotfixes and service packs is SPQuery from St. Bernard Software – http://www.stbernard.com/products_spquery.asp SPQuery allows administrators to remotely check which hotfixes are applied on servers, research hotfixes on Microsoft's website, and download and apply the hotfixes to remote servers.

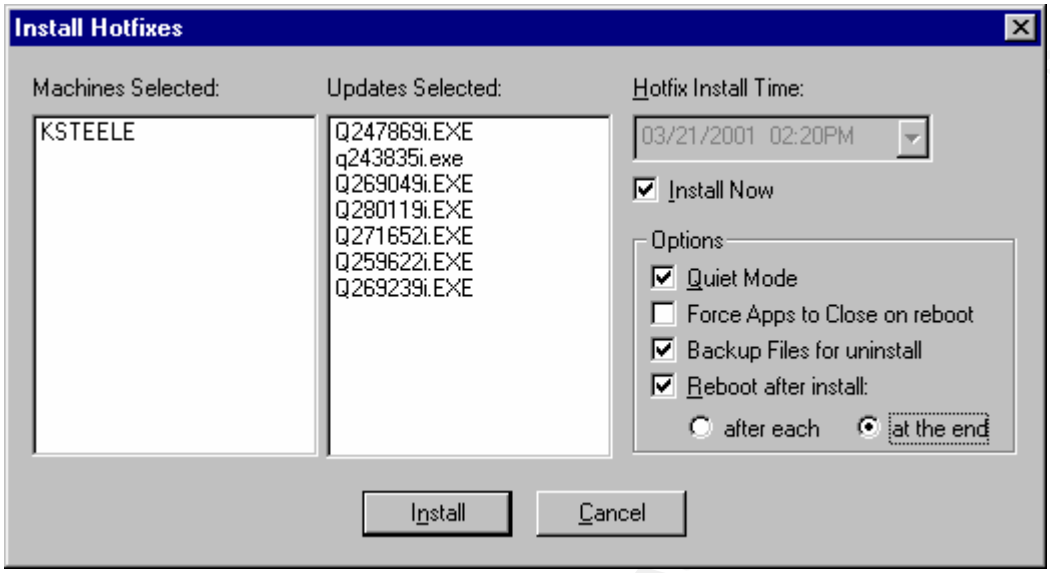
Although it is not recommended to install miscellaneous software on a production web server in the DMZ, this would be a perfect scenario to justify the expense of a mock production environment. Install this utility on your mock production web server, test and verify functionality, and then burn a CD with the appropriate hotfixes to install on your bastion hosts in the DMZ.



© SANS Institute

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SPQuery includes a feature that allows for hotfixes to be uninstalled. SPQuery also provides an option to roll up multiple hotfixes for simultaneous installation, forcing a reboot after completion of installing all of the hotfixes instead of after each individual one.



Other tools include:

Service Pack Manager – Gravity Storm Software http://home.san.rr.com/gravitystorm

Design of scripts to perform Windows Update using Logon scripts or Group Policy – http://corporate.windowsupdate.com

NOTE – These tools include support for NT 4.0 and Windows 2000 – including Internet Information Server 5.0. As of this writing, these tools do not include support for Internet Information Server 4.0 or Internet Explorer related security hotfixes, unless they are determined to be critical by the vendors. According to the vendors of SPQuery, the next version of this product will include support for IIS 4.0, Internet Explorer, SQL Server, Exchange Server, and other BackOffice Products.

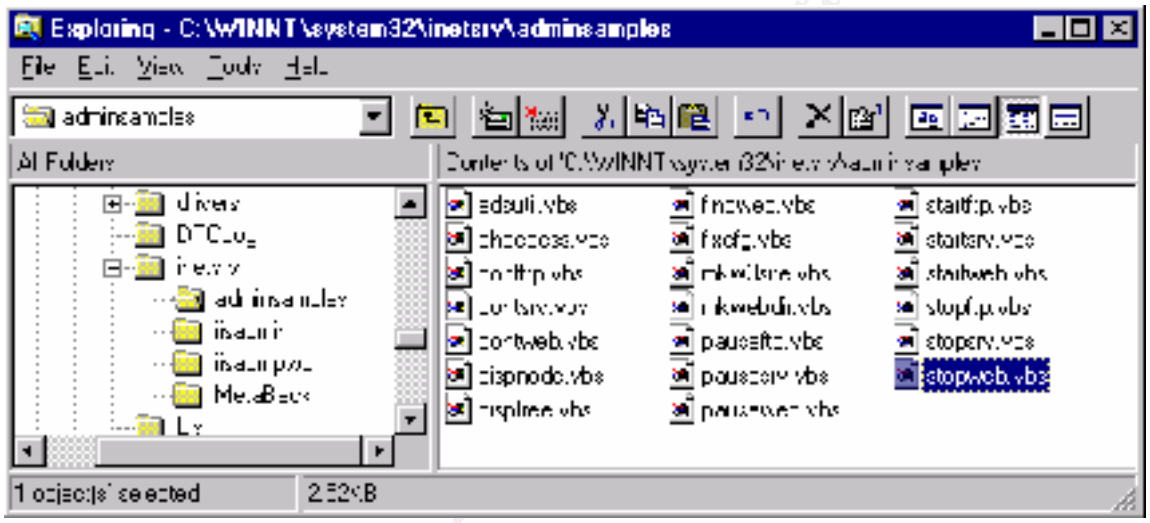
© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

IIS Configuration – Delete Admin and Sample Scripts

Once the installation is complete, delete all of the sample scripts (or use them in conjunction with honey pot tactics).

- Delete the IISSAMPLES Virtual Directory and Rename/Move/Delete/Secure the contents D:\Inetpub\iissamples*.*
- Delete the IISADMPWD Virtual Directory (contains a utility to change the Administrators password) and Rename/Move/Delete/Secure the contents C:\Winnt\System32\inetsrv\iisadmpwd*.*
- Rename/Move/Delete/Secure dangerous sample administrative scripts at C:\Winnt\System32\inetsrv\adminsamples*.*



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Move common Administrative tools

Move common administrative tools located in the %SystemRoot% (C:\Winnt) and the %SystemRoot\System32 (C:\Winnt\System32) directories to a secure directory such as C:\CommonTools.

- Implement NTFS Access Control Lists (ACL) on the directory so that only the Administrators have Read Access.
- Implement Auditing on the directory so that Everyone is audited for Failures

ARP.EXE	DEBUG.EXE	NBTSTAT.EXE	QBASIC.EXE	ROUTE.EXE
AT.EXE	EDIT.COM	NET.EXE	RCP.EXE	RSH.EXE
ATSVC.EXE	EDLIN.EXE	NETSTAT.EXE	RDISK.EXE	RUNONCE.EXE
CACLS.EXE	FINGER.EXE	NSLOOKUP.EXE	REGEDIT.EXE	SECFIXUP.EXE
CMD.EXE	FTP.EXE	PING.EXE	REGEDT32.EXE	SYSKEY.EXE
CSCRIPT.EXE	IPCONFIG.EXE	POSIX.EXE	REXEC.EXE	TELNET.EXE

IIS – Disable ability to call the command shell with #exec

The following registry value allows arbitrary shell commands to be called from within an HTML page. By default, IIS disables this capability. When the value is set to 1, remote shell commands can be executed on the web server. Verify that the following registry value is set to zero:

Hive:	HKEY_LOCAL_MACHINE
Key:	\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters
Value Name:	SSIEnableCmdDirective
Value Type:	REG_DWORD
Value Data:	0

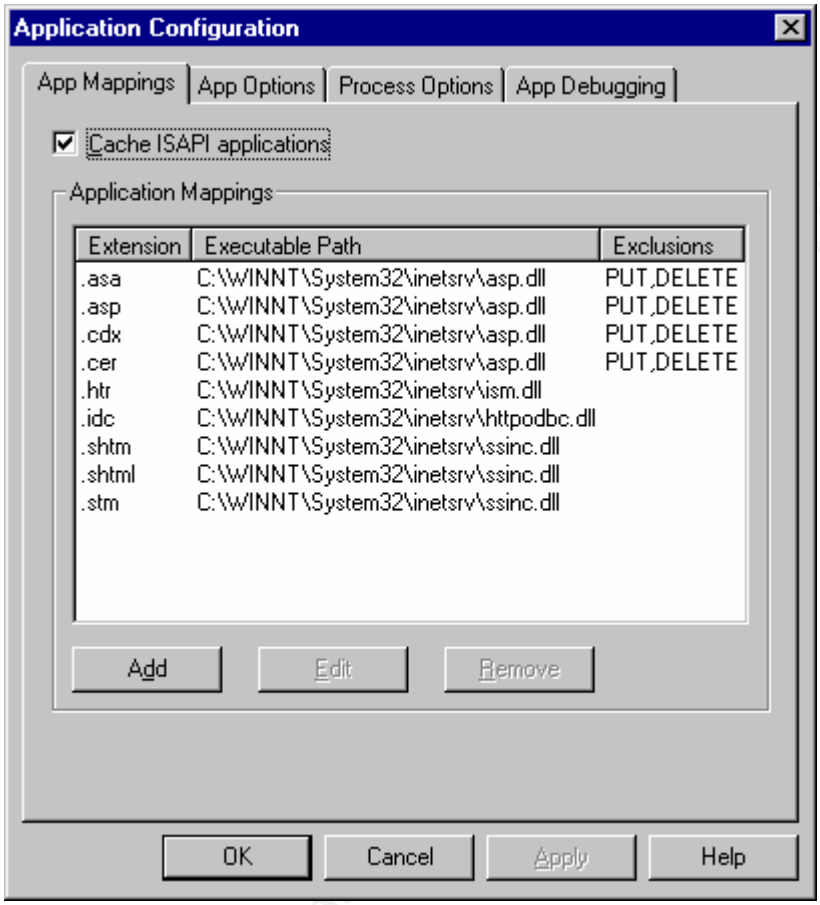
© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

IIS – Remove Unused Application Mappings

Remove application mappings that are not needed on the web server bastion host. For example, remove all application mappings except .asp.

The following screen shot shows the application mappings that exist by default on the web server bastion host:



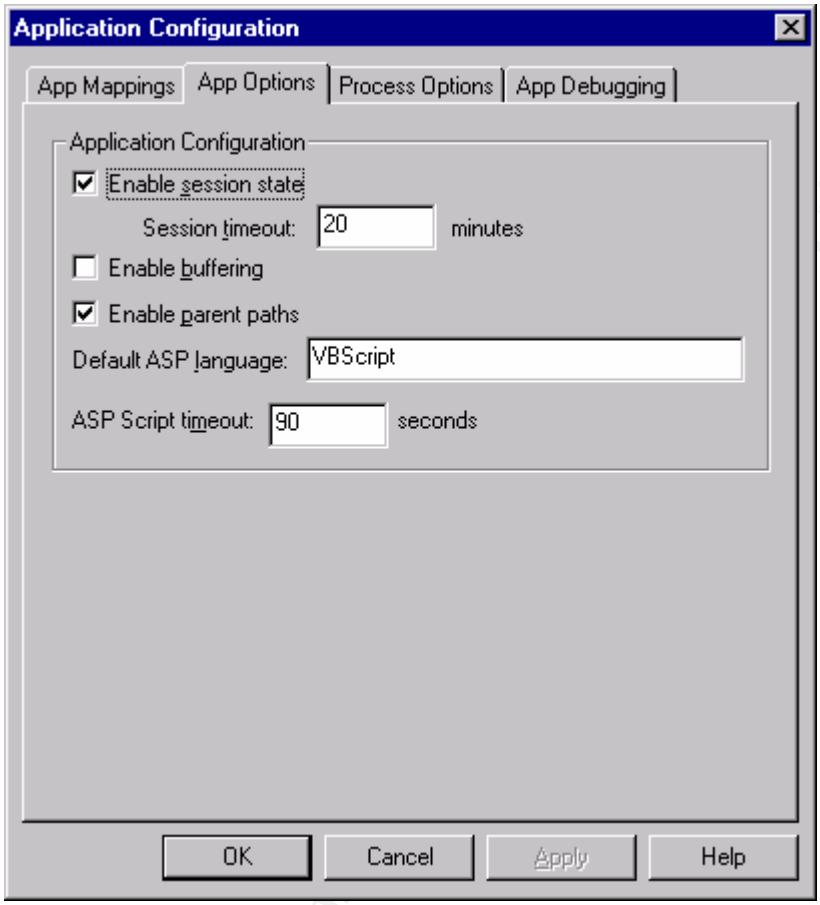
The following descriptions were provided in "Securing Internet Information Server 5.0," by Jason Fossen (Fossen, 148).

Filename Extension:	Purpose:
ASA	ASP files to declare scripts/objects with session or application scope, such as the Global.asa file
ASP	Active Server Pages
CDX	Scripts to declare Channel Definition Files
CER	Scripts to handle digital certificates from Certificate Server
HTR	Remote password change scripts
IDC	Internet Database Connector files, used with HTX files
SHTM	Server Side Includes
SHTML	Server Side Includes
STM	Server Side Includes

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

IIS – Disable Parent Paths

Parent Paths enable the ability to use relative file system paths. This ability provides a method for malicious scripts to be used to access any file located in the same partition as IIS. As shown in the following screen shot, Parent Paths are enabled by default. If possible, Parent Paths should be disabled. Disabling Parent Paths will force the use of absolute paths in scripts, which may require a rewrite of ASP/HTML code.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

IIS – Virtual directory Permissions

When configuring Virtual Directories on the bastion host, grant the following NTFS Permissions:

User Account:	Permission:
Administrator	Full Control
System	Full Control
IUSR_BASTION	Read
IWAM_BASTION	Read

IIS – Scripted and Executable Content

Since executable files need the Script and Execute permissions, while scripts need only the Script permission, create separate directories for this type of content.

IIS – Logging Options

Configure IIS W3C Extended Logging Properties to include the following options:

- Client IP Address
- User Name
- Method
- URI Stem
- HTTP Status
- User Agent
- Server IP Address
- Server Port

COM Security

The MSDN is an excellent resource for COM Security. For more information, see the MSDN Article COM Security in Practice:
http://msdn.microsoft.com/library/techart/msdn_practicom.htm

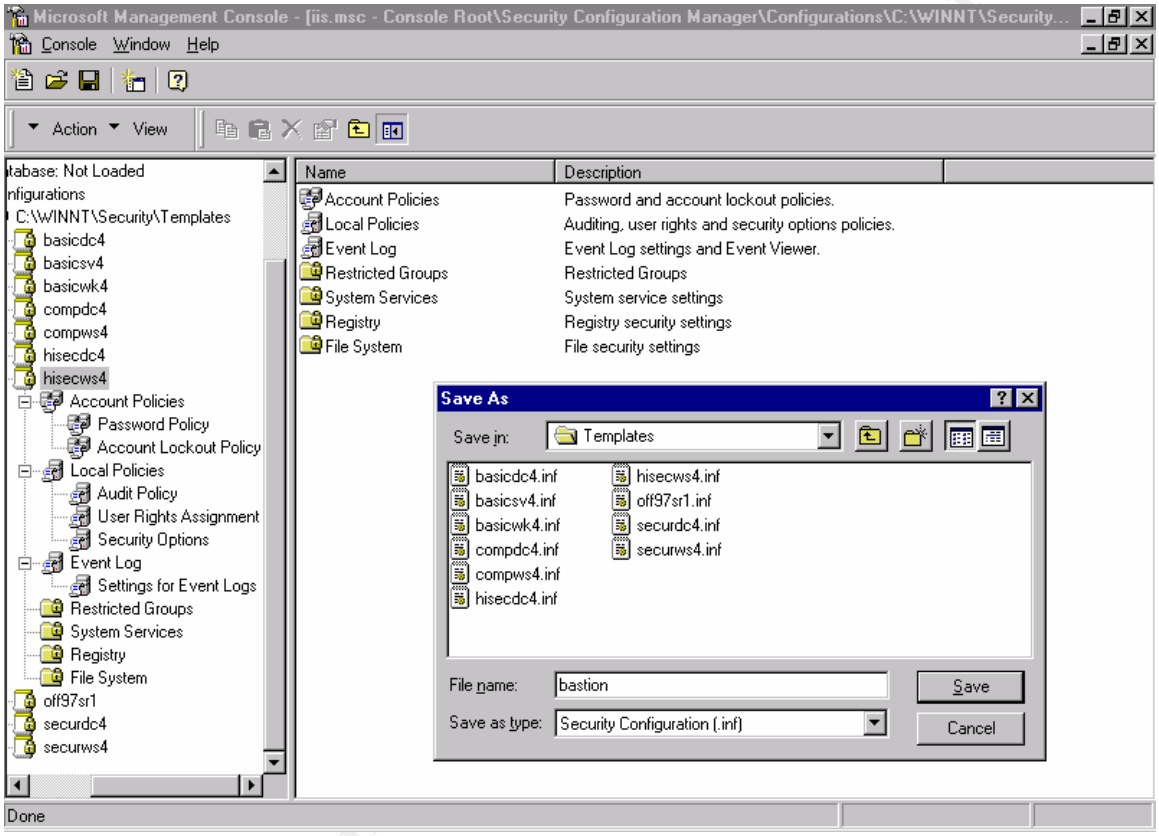
© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Modification of High Security Template for an IIS Server

Many of the changes that will be made throughout this guide are most easily and quickly applied through the use of a security policy template management tool such as the Microsoft Security Configuration Editor or Security Expressions from Pedestal Software.

In this case, a Microsoft Security Configuration template will be made by copying the HISECWS4 template and choosing Save As → BASTION.INF.



© SANS Institute 2000 - 2002

As part of GIAC practical repository. Author retains full rights.

Microsoft Security Configuration Editor

Download from: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm

The Microsoft Security Configuration Editor (SCE) is used to perform three tasks:

1. Define a template of security configuration settings.
2. Compare the local machine's security settings with a security template.
3. Configure the local machine's security settings to match a security template

The SECEDIT utility provides a method to define a security policy template for the bastion hosts in the mock production environment, which can be reapplied to other machines. Use the graphical utility to define a policy for the bastion hosts, and then apply the policy to other machines using the SECEDIT utility via a batch script or manually using a floppy disk.

SECEDIT Over the Network Using a Batch Script

The policy can be applied remotely using a batch script that connects to a network share containing the SECEDIT utility files (secedit.exe, scedll.dll, and esent.dll) and the appropriate security template files (bastion.inf in our case). Execute the batch file by using the UNC path to the script.

- To configure a system – \\%COMPUTERNAME%\template\configure.bat

  ```
  net use x: \\%COMPUTERNAME%\template

  (All one line)
  x:\secedit.exe /configure
  /cfg bastion.inf
  /db x:\%COMPUTERNAME%\secedit.sdb
  /log x:\%COMPUTERNAME%\scelog.txt /verbose

  net use x: /d
  ```

- To analyze a system – \\%COMPUTERNAME%\template\analyze.bat

  ```
  net use x: \\%COMPUTERNAME%\template

  (All one line)
  x:\secedit.exe /analyze
  /cfg bastion.inf
  /db x:\%COMPUTERNAME%\secedit.sdb
  /log x:\%COMPUTERNAME%\scelog.txt /verbose

  net use x: /d
  ```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SECEDIT Locally Using a Floppy Disk

Another method to apply the template to a bastion host is to copy the secedit utility (secedit.exe, scedll.dll, and esent.dll) and the security template file (bastion.inf in our case) to a floppy disk.

- To apply the security template:

  (All one line)
  A:\secedit /configure
  /cfg bastion.inf
  /db %TEMP%\secedit.sdb
  /verbose
  /log %TEMP%\scelog.txt

  Review the log file and then delete the files from the %TEMP% directory.

- To analyze and compare a system to a security template:

  (All one line)
  A:\secedit /analyze
  /cfg bastion.inf
  /db %TEMP%\secedit.sdb
  /verbose
  /log %TEMP%\scelog.txt

Third Party Security Templates

Security Expressions – Apply security policy to multiple machines
http://www.pedestalsoftware.com/secexp/index_sxcom.htm

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Remove or Disable Non-essential services and Drivers

If it's not needed, remove it or disable it. This will limit exposure to potential vulnerabilities, and will improve performance. Configure services using the following table on an IIS server used as a web server only:

Service	Startup
Alerter	Disabled
Clip Book Server	Disabled
Computer Browser	Disabled
DHCP Client	Disabled
Directory Replicator	Disabled
Event Log	Automatic
IIS Admin Service	Manual
License Logging Service	Disabled
Messenger	Disabled
MSDTC (Distributed Transaction Coordinator)	Automatic
Net Logon	Disabled
Network DDE	Disabled
Network DDE DSDM	Disabled
NT LM Security Support Provider	Manual
Plug and Play	Automatic
Protected Storage	Automatic
Remote Procedure Call (RPC) Locator	Disabled
Remote Procedure Call (RPC) Service	Automatic
Schedule	Disabled
Server	Disabled
Spooler	Disabled
TCP/IP NetBIOS Helper	Disabled
Telephony Service	Disabled
UPS	Automatic
Workstation	Disabled
World Wide Web Publishing Service	Automatic

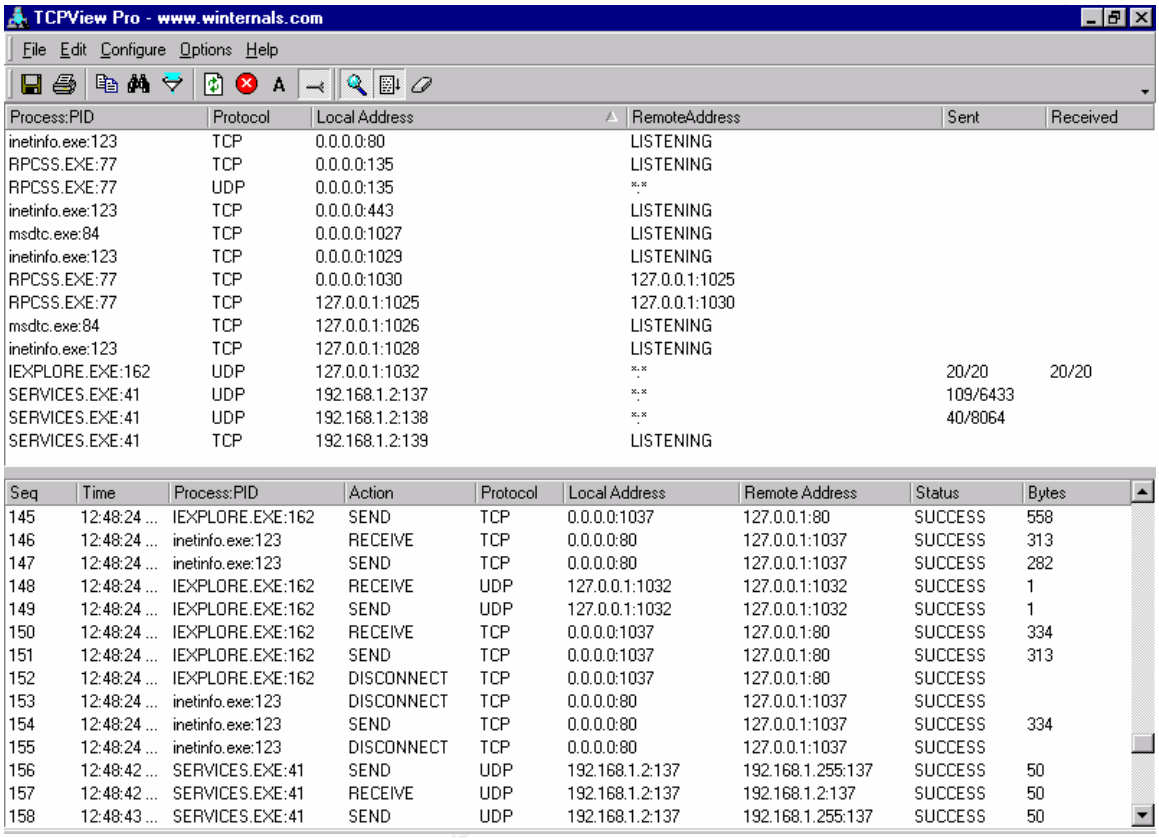
On a Windows NT 4.0 Server running Internet Information Server 4.0, the following services are required:

- Event Log
- IIS Admin Service
- NT LM Security Support Provider
- MSDTC (Distributed Transaction Coordinator)
- Protected Storage
- Remote Procedure Call (RPC) Service
- World Wide Web Publishing Service

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

TCP/IP Internals

An excellent utility to see which services and processes are running on which port is TCP View Pro from Winternals Software – http://winternals.com/products/monitoringtools/tcpviewpro.shtml



Process:PID	Protocol	Local Address	RemoteAddress	Sent	Received
inetinfo.exe:123	TCP	0.0.0.0:80	LISTENING		
RPCSS.EXE:77	TCP	0.0.0.0:135	LISTENING		
RPCSS.EXE:77	UDP	0.0.0.0:135	*:*		
inetinfo.exe:123	TCP	0.0.0.0:443	LISTENING		
msdtc.exe:84	TCP	0.0.0.0:1027	LISTENING		
inetinfo.exe:123	TCP	0.0.0.0:1029	LISTENING		
RPCSS.EXE:77	TCP	0.0.0.0:1030	127.0.0.1:1025		
RPCSS.EXE:77	TCP	127.0.0.1:1025	127.0.0.1:1030		
msdtc.exe:84	TCP	127.0.0.1:1026	LISTENING		
inetinfo.exe:123	TCP	127.0.0.1:1028	LISTENING		
IEXPLORE.EXE:162	UDP	127.0.0.1:1032	*:*	20/20	20/20
SERVICES.EXE:41	UDP	192.168.1.2:137	*:*	109/6433	
SERVICES.EXE:41	UDP	192.168.1.2:138	*:*	40/8064	
SERVICES.EXE:41	TCP	192.168.1.2:139	LISTENING		

Seq	Time	Process:PID	Action	Protocol	Local Address	Remote Address	Status	Bytes
145	12:48:24 ...	IEXPLORE.EXE:162	SEND	TCP	0.0.0.0:1037	127.0.0.1:80	SUCCESS	558
146	12:48:24 ...	inetinfo.exe:123	RECEIVE	TCP	0.0.0.0:80	127.0.0.1:1037	SUCCESS	313
147	12:48:24 ...	inetinfo.exe:123	SEND	TCP	0.0.0.0:80	127.0.0.1:1037	SUCCESS	282
148	12:48:24 ...	IEXPLORE.EXE:162	RECEIVE	UDP	127.0.0.1:1032	127.0.0.1:1032	SUCCESS	1
149	12:48:24 ...	IEXPLORE.EXE:162	SEND	UDP	127.0.0.1:1032	127.0.0.1:1032	SUCCESS	1
150	12:48:24 ...	IEXPLORE.EXE:162	RECEIVE	TCP	0.0.0.0:1037	127.0.0.1:80	SUCCESS	334
151	12:48:24 ...	IEXPLORE.EXE:162	SEND	TCP	0.0.0.0:1037	127.0.0.1:80	SUCCESS	313
152	12:48:24 ...	IEXPLORE.EXE:162	DISCONNECT	TCP	0.0.0.0:1037	127.0.0.1:80	SUCCESS	
153	12:48:24 ...	inetinfo.exe:123	DISCONNECT	TCP	0.0.0.0:80	127.0.0.1:1037	SUCCESS	
154	12:48:24 ...	inetinfo.exe:123	SEND	TCP	0.0.0.0:80	127.0.0.1:1037	SUCCESS	334
155	12:48:24 ...	inetinfo.exe:123	DISCONNECT	TCP	0.0.0.0:80	127.0.0.1:1037	SUCCESS	
156	12:48:42 ...	SERVICES.EXE:41	SEND	UDP	192.168.1.2:137	192.168.1.255:137	SUCCESS	50
157	12:48:42 ...	SERVICES.EXE:41	RECEIVE	UDP	192.168.1.2:137	192.168.1.2:137	SUCCESS	50
158	12:48:43 ...	SERVICES.EXE:41	SEND	UDP	192.168.1.2:137	192.168.1.255:137	SUCCESS	50

Port Number Assignments

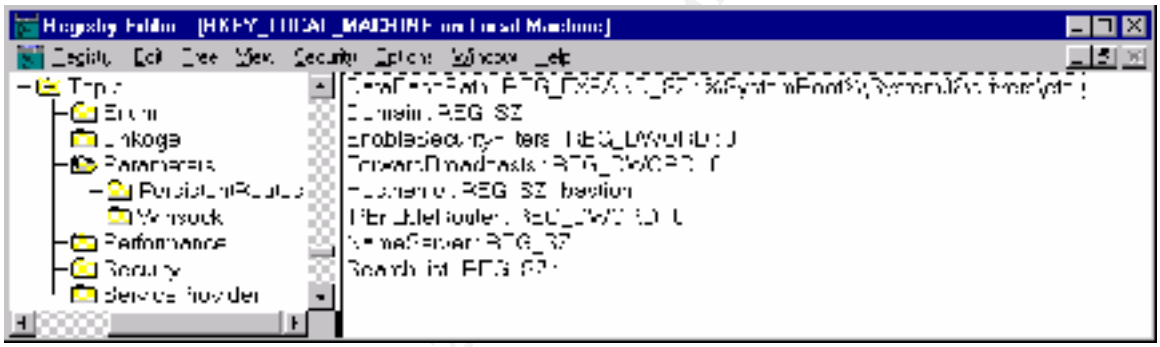
- Official Listing of Port Numbers: http://www.isi.edu/in-notes/iana/assignments/port-numbers
- Common Microsoft Port Numbers: http://www.microsoft.com/WINDOWS2000/library/resources/reskit/samplechapters/cnfc/cnfc_por_zqyu.asp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

TCP/IP Parameters

In the HKLM\System\CurrentControlSet\Services\Tcpip\Parameters registry key, many parameters exist that can be modified for performance and security purposes including:

- TcpMaxHalfOpen
- TcpMaxHalfOpenRetried
- EnablePMTUDiscovery
- NoNameReleaseOnDemand
- EnableDeadGWDetect
- KeepAliveTime
- PerformRouterDiscovery
- EnableICMPRedirects
- BacklogIncrement
- MaxConnBackLog
- EnableDynamicBacklog
- MinimumDynamicBacklog
- MaximumDynamicBacklog
- DynamicBacklogGrowthDelta



For more information on TCP/IP see:

- TCP/IP Illustrated, Volumes 1 - 3 (W. Richard Stevens, Addison-Wesley Publishing)
- Building a Highly Available and Scalable Web Farm
  http://msdn.microsoft.com/library/default.asp?URL=/library/techart/d5nlb.htm
- TCP/IP & NBT Configuration Parameters for Windows NT and Windows 2000
  Article ID: Q120642
  http://support.microsoft.com/support/kb/articles/Q120/6/42.asp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SYN Floods

(Based on the information available in Securing Windows NT, Step-by-Step).

Windows NT will set aside memory for each new request to the operating system. This can be used to cause a denial of service attack by depleting all of the resources on the target machine by initiating these requests without fully completing them.

A SYN Flood occurs when thousands of TCP session request packets (with the SYN flag set) are sent to a target with spoofed source IP addresses.

To manually determine if your site is under a SYN Flood attack (intrusion detection systems do this more efficiently), go to a command prompt and enter:

netstat -a -n|find /i "syn"

By default, Windows NT 4.0 does not provide protection to SYN Floods. However, starting with Service Pack 5, a registry key can be set to limit exposure to these SYN floods. On a Windows NT 4.0 Web Server running IIS, this is essential.

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\Tcpip\Parameters
Value Name:	SynAttackProtect
Value Type:	REG_DWORD
Value Data:	2

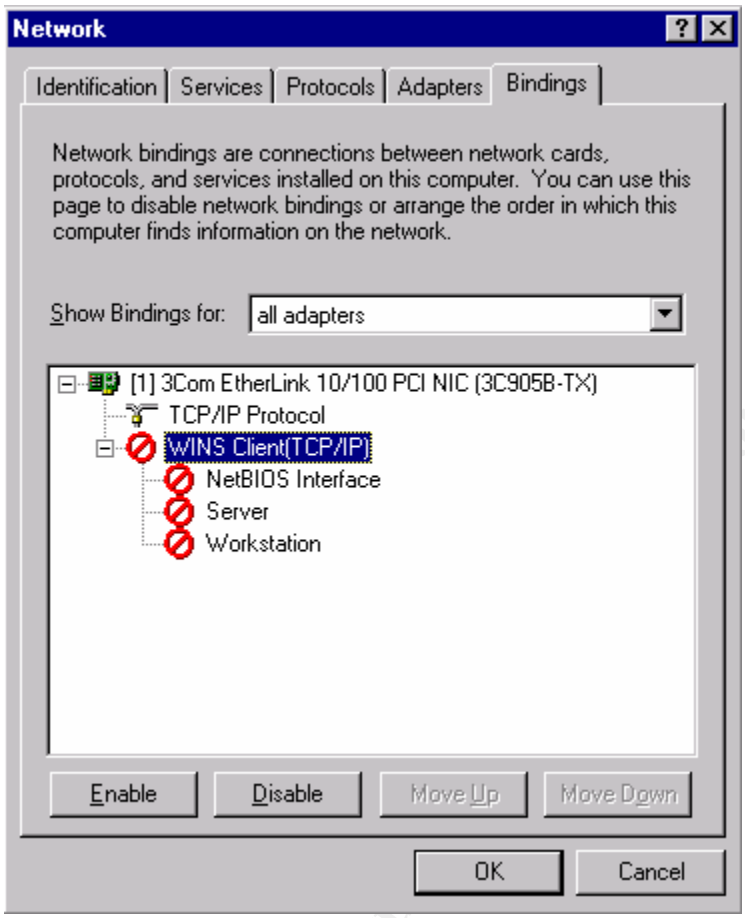
Setting this value to 2 will reduce the retransmission of SYN-ACK retries, and the full three-way TCP handshake must complete before the afd.sys driver commits additional resources.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Disable NetBIOS

On a NT server that is configured solely as a web server, the NetBIOS interface, Server service, and Workstation Service are not needed, and should be disabled.



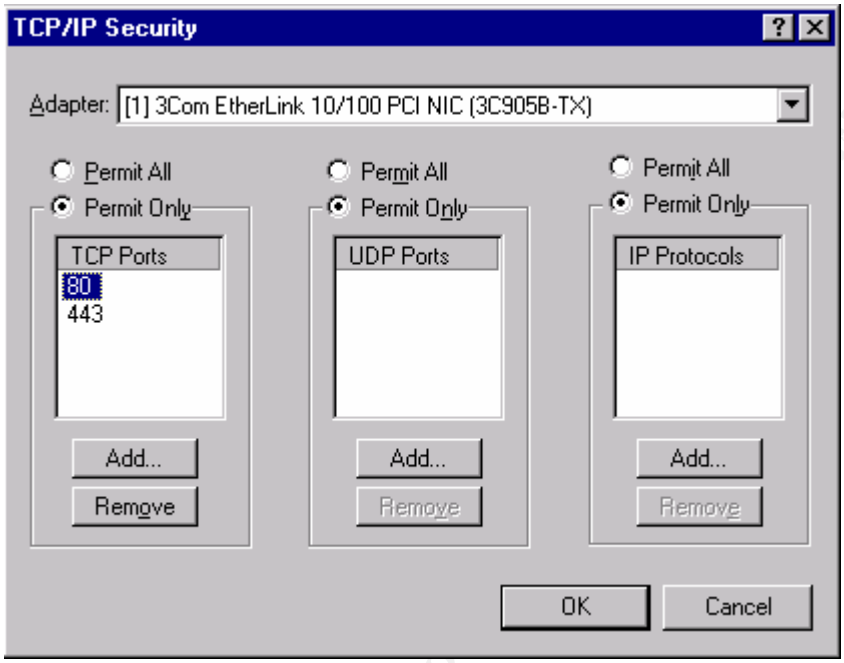
On a dual-homed web server connected to both the external and internal networks, install both the NetBeui protocol and TCP/IP. Bind only the TCP/IP protocol to the adapter on the external interface, and bind the WINS client over NetBeui (including the Server, Workstation, and NetBIOS interfaces services) to the adapter on the internal interface.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Block Non-essential ports

Deny access to all ports except the necessary ports. On a web server, disable all ports except TCP ports 80 and 443 (if SSL will be used on the web server).

Configure this by going to the Network settings applet in the Control Panel, select the Protocols tab, double-click on the TCP/IP Protocol, select the Advanced button, Check the Enable Security Box, click on the Configure button, and configure the protocol to permit only TCP port 80 and 443 as shown in the following screenshot.



An alternative to the native TCP/IP filtering in Windows NT is the:

- Routing and Remote Access Services (RRAS) available from Microsoft: http://www.microsoft.com/NTServer/nts/downloads/winfeatures/rras/rrasdown.asp

  The RRAS Service is integrated into Windows 2000.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Remove the OS/2 and POSIX Subsystems

These subsystems provide support for legacy applications and should not be needed on a web server. Removing these subsystems will also slightly improve performance.

To remove the OS/2 and POSIX Subsystems:

1. Delete the following folder and all of its contents: %systemroot%\System32\os2

2. Delete all the subkeys underneath:
   HKEY_LOCAL_MACHINE\Software\Microsoft\OS/2 Subsystem for NT

3. Delete value Os2LibPath in:
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\Environment

4. Remove the "Os2" and "Posix" values from the multistring value named "Optional" in the Registry
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\SubSystems

   (Leave the value named Optional itself in place)

5. Delete the Os/2 and Posix subkeys in
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SubSystems

6. Reboot.

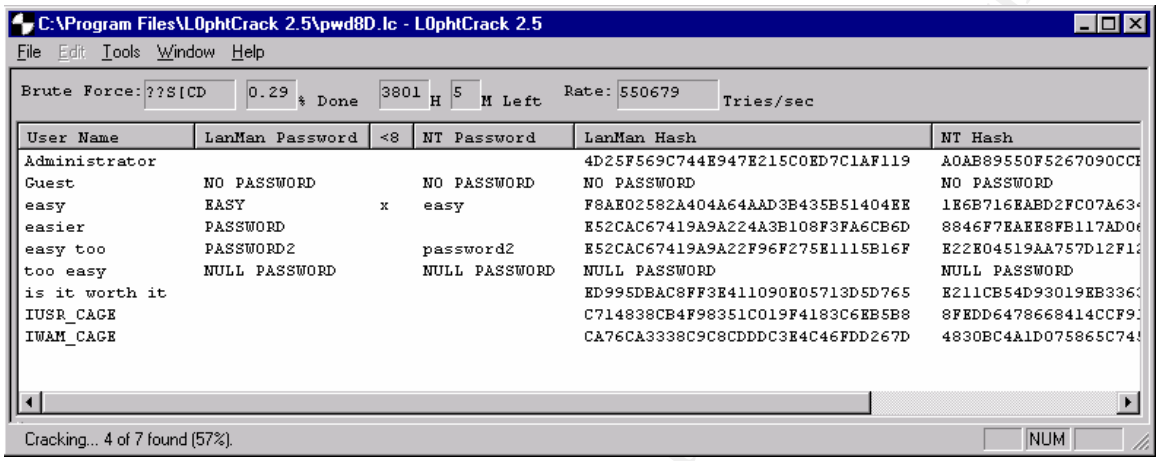
© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Protect User Accounts and Passwords

In order to prevent password cracking tools from breaking passwords, it is essential to enforce complex passwords and complex password policies:

L0phtCrack – http://www.securitysoftwaretech.com/l0phtcrack



© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

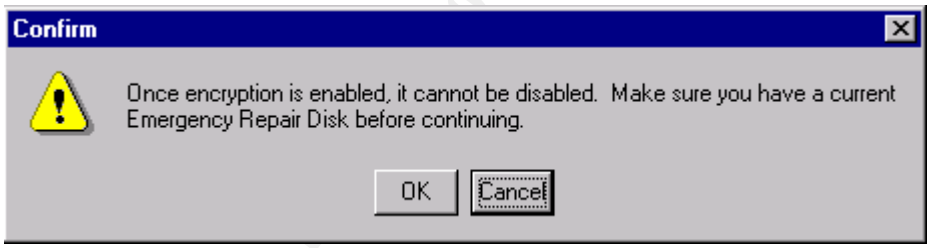
Encrypt the SAM database with SYSKEY

To prevent a utility such as L0phtCrack from deciphering password hashes and learning user passwords, the passwords in the SAM database can be strongly encrypted using the SYSKEY utility.

The SYSKEY utility generates a 128-bit random key with which to encrypt the password hashes in the SAM database. This random key is then encrypted with a second key (the System Key) and stored on the server locally, on a floppy disk, or a System Key password can be created that must be entered during the boot process. The decryption of the password hashes is performed during the boot process, so overall performance will not be degraded. However, the boot process may take longer on servers with large SAM databases.



Start → Run → Syskey



NOTE – This is not entirely true.

Search the security and hacker websites and newsgroups for methods of reversing SYSKEY on Windows NT 4.0 and Windows 2000 such as:
http://home.eunet.no/~pnordahl/ntpasswd/

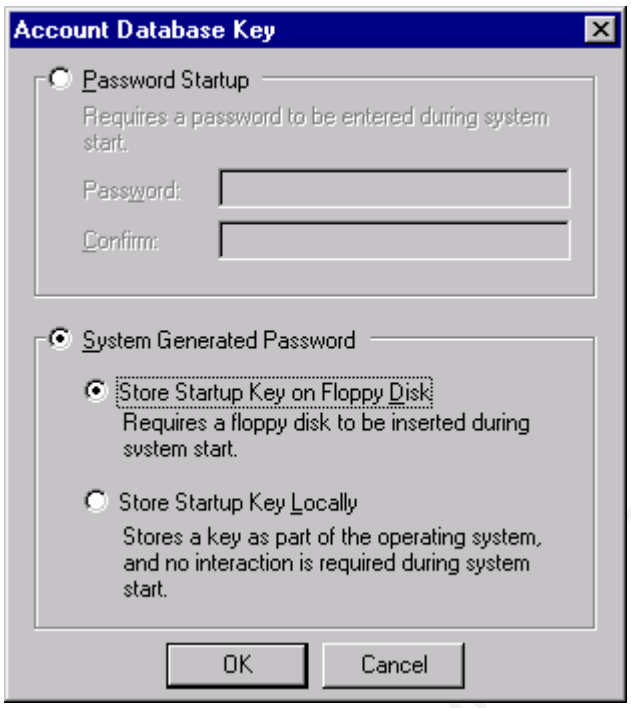
For more information on SYSKEY:

- Windows NT System Key Permits Strong Encryption of the SAM:
  http://support.microsoft.com/support/kb/articles/q143/4/75.asp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SYSKEY – Method of Storage

The most secure method of storing the key is on a floppy disk, and we will assume that the server room is already secure. If you do not want to be required to enter a startup password and do not want to store the key locally in the registry, choose the option to store the system key on a floppy disk, make a backup of the disk, store the backup in a secure location, and disable the BIOS option to boot from the floppy drive.



For a production web server bastion host, our only choice is store the key on a floppy disk or locally in the registry, since this situation will require unattended reboots in the event of failure.

Apply the Syskey Hotfixes

Microsoft Support Article Q248183 reported a vulnerability with the SYSKEY utility: "A cryptographic error in the Syskey tool makes offline password attacks easier than previously believed. Syskey reuses keystream when encrypting certain elements in the Security Accounts Manager (SAM) database, making the tool vulnerable to an attack using a known cryptanalytic method. This vulnerability could allow offline password attacks to be mounted against a Syskey-protected SAM database." (Q248183)

Apply the appropriate patch for the web server bastion host below. For more information see:

- Microsoft's knowledge base article regarding the vulnerability:
  "Syskey Tool Reuses Keystream" – Article ID: Q248183
  http://support.microsoft.com/support/kb/articles/q248/1/83.asp
- Microsoft's hotfix page for this vulnerability:
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=16798

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Administrator Account Password

The most important account on a web server bastion host is the Administrator account. For the administrator account, assign a complex password that consists of 14 uppercase letters, lowercase letters, numbers, symbols, and extended ASCII characters, such as:

- Alt-1-4-5 = æ (Use the numeric keypad)
- Alt-2-2-2 =
- Alt-0-1-3 = equivalent of Carriage Return, Line Feed (this particular character is virtually unbreakable by password crackers such as L0phtCrack)

Enforcing Complex Passwords with a Password Filter

A modification must be made to the registry in order to enforce complex passwords on the web server bastion host. To enable password filtering, add an additional line to the following value in the registry:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\Lsa
Value Name:	Notification Packages
Value Type:	REG_MULTI_SZ
Value Data:	PASSFILT

The password filter will require that changed passwords (not existing passwords) be at least six characters long, not contain any part of the user's full name, and contain at least three out of the four following categories of characters:

- Uppercase letters
- Lowercase letters
- Numbers
- Non-alphanumeric symbols

Third party password filters include:

- Password Padlock – http://www.quakenbush.com

Administrator Account Lockout and Complex Passwords

By default, the Administrator account cannot be locked out due to bad logons attempts.

Use the Passprop utility from the Windows NT 4.0 Server Resource Kit to enable the Administrator account to be locked out from network logons due to bad password attempts. This will still allow the Administrator account to log on locally to the console. Use the following command:

Passprop /complex /adminlockout

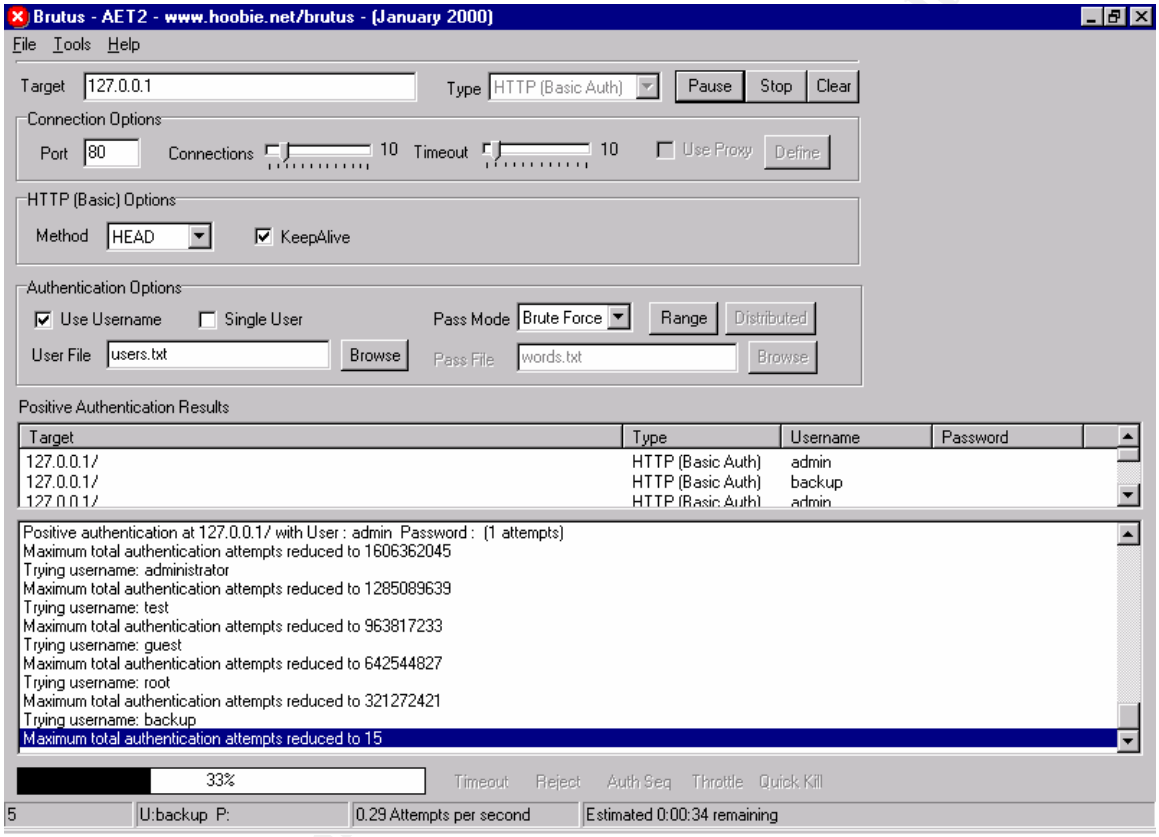
- /complex = forces passwords to be complex, requiring passwords to be a mix of upper and lowercase letters and numbers or symbols.
- /adminlockout = allows the Administrator account to be locked out.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Web-Based User Accounts (and others)

NT User Accounts are usually not the only usernames and passwords that we find on a web server bastion host. Password complexity is just as important (if not more) for web-based applications that maintain their own usernames and/or passwords as it is for NT user names and passwords.

Brutus – http://www.hoobie.net/brutus/ – is especially useful for cracking web-based applications.



© SANS Institute 2000 - 2002

As part of GIAC practical repository. Author retains full rights.

Rename Administrator Account

Despite the fact that there are methods of determining the name of the built-in Administrator account using its SID (which always ends with a RID of 500), the account should still be renamed to provide another method of deterring hackers.

A honey-pot Administrator account can be created by copying the renamed Administrator account (to get its description field), naming the copy Administrator, disable the account, strip it of all user rights such as group memberships file and registry permissions, etc.

Once you have created the honey-pot Administrator account, change the renamed account's description field to something other than the default description "Built-in account for administering the computer/domain."

Use a logon script to take action in the event that a hacker does gain access with the account, such as sending an alert or page, make an entry into a log file, etc.

Search the security websites and other sources for more information about a honey-pot Administrator account.

Guest Account

Ensure that the Guest account is disabled, and assign the account a password.

Remove the "Access this Computer from the Network" Right from the Administrators Group

This will prevent hackers from gaining administrative level access to the web server bastion host over the network, and will force Administrators to log on locally when performing administrative duties.

- Navigate to User Manager → Policies → User Rights → Access This Computer Over Network → remove the Administrators group.
- Navigate to User Manager → Policies → User Rights → Log on Locally ensure that Administrators is in the list of allowed users.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Service Accounts

If you are adding a new custom service to the bastion host web server, run the service under the System Account if possible. Running under the System account, the service cannot log onto other computers over the network, but it can access resources shared to the Everyone group or to null sessions.

When using a local (or domain) user account as a Service Account, the account can be used to log in to the server, and the service account password is stored in the registry, which opens an opportunity for hackers.

In order of preference, run the service under a:

1. System Account – attack is contained to the local computer
2. Local User Account – attack is contained to the local computer
3. Domain User Account – attack is not contained to the local computer and can access network resources
4. Domain User Account (member of the Domain Administrators group) – worst-case scenario – will have administrative access on all members of the domain.

If a service requires to be run under the context of a local or domain user account, assign it a complex password, and restrict its rights so that it only has the necessary permissions to run.

For example, start with a local user account, assign it the appropriate NTFS permissions for the service, and give it the right in User Manager to "Log On As A Service." Add rights until you have a functioning service. If the service does not need to be a member of the Local Administrators group, do not grant the account this permission. The account should also not need the right to "Take Ownership Of Files And Other Objects." Test this in your mock production environment until the service is functioning.

In addition, assign NTFS permissions to the executable files that are used by the service, and audit failed access to the executables.

Service Account Management

An excellent utility to manages service accounts across multiple machines or networks is:

- NT Service Account Manager – http://www.lanicu.com

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

NT User Manager Account and Password Policy

User Manager is used to set account policies (determine when accounts should be locked out) and password policies (place restrictions on passwords).

Use the following as a guide for these settings on a web server bastion host.

Maximum Password Age	60 days
Minimum Password Age	1 day
Minimum Password Length	9 characters
Password Uniqueness	10 passwords
Account Lockout After	3 bad logins
Account Reset After	1 hour
Account Lockout Duration	Forever
Users must logon to change password	Disable

Third party tools to enforce password policies include:

- Quakenbush Password Appraiser – http://www.quakenbush.com

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Restricting Null User Sessions

Null user sessions can be used against a target to extract the following information: user account names, groups, shared folders and printers, list of users with dial-in permission, password policy, list of assigned user rights, running services, share permissions, NTFS permissions, NTFS audit settings, etc.

- Pedestal Software's NTUSER utility – http://www.pedestalsoftware.com
- SomarSoft's DumpSec – http://www.somarsoft.com

To create a null user session, go to a command prompt and type the following:

net use \\yourIPaddress\ipc$ "" /user:""

To prevent null user sessions, a registry change must be made on the bastion host:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\LSA
Value Name:	RestrictAnonymous
Value Type:	REG_DWORD
Value Data:	1

NOTE – This modification to the registry will break the functionality to remotely view the list of users on the machine when assigning permissions. For a web server bastion host, this restriction should not be a problem.

As with all of the changes in this guide, first make this change on a mock production server and verify functionality of services before making the change on a production server. In this case, ensure that this does not break the functionality of tape backup software.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Disable Null Session Access to Shares

Setting the following registry value will prevent null session users from accessing shared folders:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\LanmanServer\Parameters
Value Name:	RestrictNullSessAccess
Value Type:	REG_DWORD
Value Data:	1

Values in the following registry key will make an exception to the above setting on a per share basis:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\LanmanServer\Parameters
Value Name:	NullSessionShares
Value Type:	REG_MULTI_SZ
Value Data:	(one or more share names)

Disable Null Session Access to Named Pipes

The following registry key contains a list of the named pipes, which are accessible to null user sessions:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\LanmanServer\Parameters
Value Name:	NullSessionPipes
Value Type:	REG_MULTI_SZ
Value Data:	(remove one or more named pipe names from this list)

NullSessionPipes include:

- COMNAP
- COMNODE
- SQL\QUERY
- SPOOLSS
- LLSRPC
- EPMAPPER
- LOCATOR

Remove named pipes from this list to block anonymous access. This may break the functionality of an application, so test this in a mock production environment.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Restrict Remote Network Access to the Registry

To prevent remote users from accessing the registry with utilities such as Registry Editor, System Policy Editor, and DumpReg from Somarsoft – http://www.somarsoft.com, appropriate permissions should be set on the following registry key.

Using REGEDT32.EXE, assigning permissions to the Winreg key specifies the accounts that have the permission to access the entire registry remotely (on the Windows NT Server bastion host the default is set to Administrators – Full Control).

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\SecurePipeServers\Winreg

AllowedPaths exceptions to the above setting reside in the following location:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths
Value Name:	Machine or Users
Value Type:	REG_MULTI_SZ
Value Data:	(registry locations)

Registry Manipulation Utilities

- Small Wonders Software Security Explorer – http://www.securityexplorer.com
- DumpReg from Somarsoft – http://www.somarsoft.com
- NTSEC from Pedestal Software – http://www.pedestalsoftware.com/ntsec/index.htm
- NT Resource Kit – REGINI.EXE
- Multi-Remote Registry Change Utility – http://www.systemtools.com/reg

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Restrict Registry Access to Prevent Known Trojans

To prevent the exploit of known Trojan programs, set permissions on the following keys to:

User Account:	Permissions
Administrators	Full Control
System	Full Control
Creator Owner	Full Control
Authenticated Users	Read

User Account:	Audit:
Everyone	All Auditing

Hive:	HKEY_LOCAL_MACHINE
Key:	\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Hive:	HKEY_LOCAL_MACHINE
Key:	\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Hive:	HKEY_LOCAL_MACHINE
Key:	\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

Hive:	HKEY_LOCAL_MACHINE
Key:	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug

Hive:	HKEY_LOCAL_MACHINE
Key:	\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Restrict Guest Access to Event Log

To control guest access to the NT Event logs, set the following values in the registry:

Hive:	HKEY_LOCAL_MACHINE
Key:	\SYSTEM\CurrentControlSet\Services\EventLog\%LogName%
Value Name:	RestrictGuestAccess
Value Type:	REG_DWORD
Value Data:	1

(%LogName% = Application, Security, and System)

Secure Access to the Event Log Files

To secure access to the Event Log files, configure NTFS Permissions and auditing on files: %SystemRoot%\System32\Config – C:\Winnt\System32\Config

Event Log:	File:
Application	AppEvent.evt
Security	SecEvent.evt
System	SysEvent.evt

User Account:	Permissions:
Administrators	Full Control
System	Full Control

User Account:	Auditing:
Administrators	Success and Failure
Everyone	Failure

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Event Log Settings

Configure the Event Log with the following settings:

Log:	Size (K):	Wrapping:
Application	16384 - 524288	Overwrite Events Older than 14 Days
Security	32768 - 1048576	Overwrite Events Older than 14 Days
System	16384 - 524288	Overwrite Events Older than 14 Days

Server Crash when Security Log Fills - CrashOnAuditFail

To cause a server to crash when the Security log fills to its maximum capacity, add the following value to the registry:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\Lsa
Value Name:	CrashOnAuditFail
Value Type:	REG_DWORD
Value Data:	1

Tools to manage Event Logs

- bv-Control for Windows 2000/NT – a complete Enterprise Management System that includes an excellent tool for managing event logs – http://www.bindview.com/products/bvControl/win2000nt/index.cfm?Area=6&Product=70
- Microsoft Windows NT Resource Kit – DUMPEL.EXE
- SomarSoft's DumpEvt – http://www.somarsoft.com
- Event Log Monitor – TNT Software http://www.tntsoftware.com/products/emon22/Default.asp
- Event Archiver – Dorian Software Creations, Inc. http://www.doriansoft.com/eventarchiver
- Event Analyst – Dorian Software Creations, Inc. http://www.doriansoft.com/eventanalyst
- NTLast – NTOBJECTives, Inc. http://www.foundstone.com/rdlabs/proddesc/ntlast.html

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Registry Auditing – Best Practices

Microsoft Windows NT 4.0 Security, Audit, and Control recommends auditing these permissions on the following three registry keys and their subkeys:

- HKEY_LOCAL_MACHINE\System
- HKEY_LOCAL_MACHINE\Software
- HKEY_CLASSES_ROOT

Recommended Registry Auditing Options:

Query Value	None
Set Value	Success and Failure
Create Subkey	Success and Failure
Enumerate Subkeys	None
Notify	None
Create Link	Success and Failure
Delete	Success and Failure
Write DAC	Success and Failure
Read Control	None

For more information about recommended Registry permissions, see the GCNT paper by Daniel A. Boss "Registry Key Security."

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Secure NTFS Permissions

As a general rule, when assigning NTFS permissions, use the Authenticated Users group instead of the Everyone group, since null user sessions are a member of the everyone group.

Following the principle of least privilege, assign users the minimum rights, permissions, group memberships, etc. so that they can access only exactly what they need to perform their job. For exampled, assign the Change permission rather than Full Control when granting permissions to users other than Administrators, System or Creator Owner.

For more information about NTFS Permissions, see "Windows NT Security Guidelines: Considerations & Guidelines for Securely Configuring Windows NT in Multiple Environments" from Trusted Systems Services – http://www.trustedsystems.com

At a minimum, apply the following NTFS permissions. Do NOT apply these permissions to all subdirectories unless specifically stated.

Path	Rights
Root of C: and D:	Administrators = Full Control System = Full Control Authenticated Users = Read
BOOT.INI (C:\boot.ini) NTDETECT.COM (C:\ntdetect.com) NTLDR (C:\ntldr)	Administrators = Full Control System = Full Control
AUTOEXEC.BAT (C:\autoexec.bat) CONFIG.SYS (C:\config.sys)	Administrators = Full Control System = Full Control Authenticated Users = Read
IO.SYS (C:\io.sys) MSDOS.SYS (C:\msdos.sys)	Administrators = Full Control System = Full Control Authenticated Users = Read
%SystemRoot% (C:\Winnt)	Administrators = Full Control Creator Owner = Full Control System = Full Control Authenticated Users = Read
%SystemRoot%\System32 (C:\Winnt\System32)	Administrators = Full Control Creator Owner = Full Control System = Full Control Authenticated Users = Read
%SystemRoot%\System (C:\Winnt\System)	Administrators = Full Control Creator Owner = Full Control System = Full Control Authenticated Users = Read
%SystemRoot%\Repair (C:\Winnt\Repair)	Administrators = Full Control
%SystemRoot%\System32\Config (C:\Winnt\System32\Config)	Administrators = Full Control System = Full Control Creator Owner = Full Control Authenticated Users = List
%SystemRoot%\System32\drivers (C:\Winnt\System32\Config) (Including all subdirectories)	Administrators = Full Control System = Full Control Authenticated Users = Read
%SystemRoot%\Config	Administrators = Full Control

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

(C:\Winnt\Config)	System = Full Control Authenticated Users = Read
%SystemRoot%\inf (C:\Winnt\inf)	Administrators = Full Control System = Full Control Authenticated Users = Read
%Temp% (C:\Temp)	Administrators = Full Control System = Full Control Creator Owner = Full Control Authenticated Users = Read, Write, and Execute
%SystemRoot%\System32\Spool (C:\Winnt\System32\Spool) (and all subdirectories)	Administrators = Full Control System = Full Control Creator Owner = Full Control Authenticated Users = Read
%SystemRoot%\System32\LogFiles (and all subdirectories) (C:\Winnt\System32\LogFiles)	Administrators = Full Control System = Full Control Authenticated Users = List
%SystemRoot%\System32\Inetsrv\Metabase.bin (IIS Metabase) (C:\Winnt\ System32\Inetsrv\Metabase.bin)	Administrators = Full Control System = Full Control
%SystemRoot%\System32\Inetsrv\Metaback (ISS Metabase Backup) (C:\Winnt\ System32\Inetsrv\Metaback)	Administrators = Full Control System = Full Control
C:\Common Tools (this is where we will later relocate administrative tools)	Administrators = Read
%SystemRoot%\Cookies (C:\Winnt\Cookies) %SystemRoot%\Temporary Internet Files (C:\Winnt\Temporary Internet Files	Administrators = Full Control
%SystemRoot%\Web C:\Winnt\Web	Administrators = Full Control System = Full Control

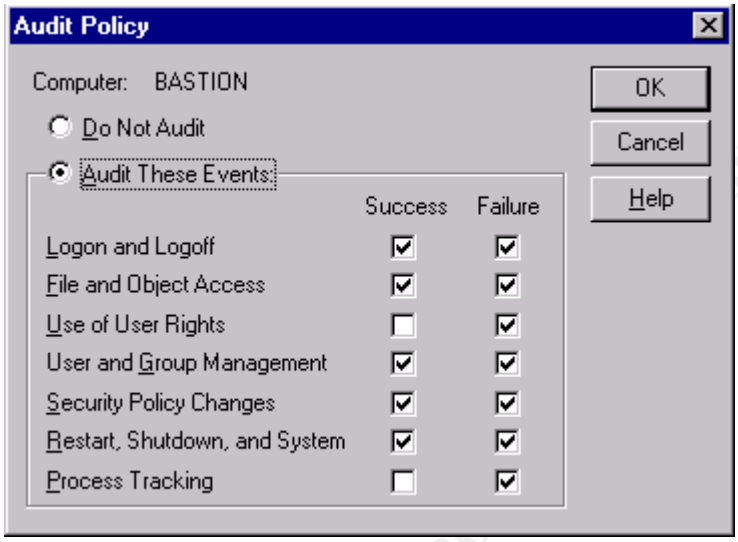
© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

User Manager Audit Policy

Configure the Audit Policy in User Manager by selecting Policies → Audit.

Event:	Audit:
Logon and Logoff	Success, Failure
File and Object Access	Success, Failure
Use of User Rights	Failure
User and Group Management	Success, Failure
Security Policy Changes	Success, Failure
Restart, Shutdown and System	Success, Failure
Process Tracking	Failure

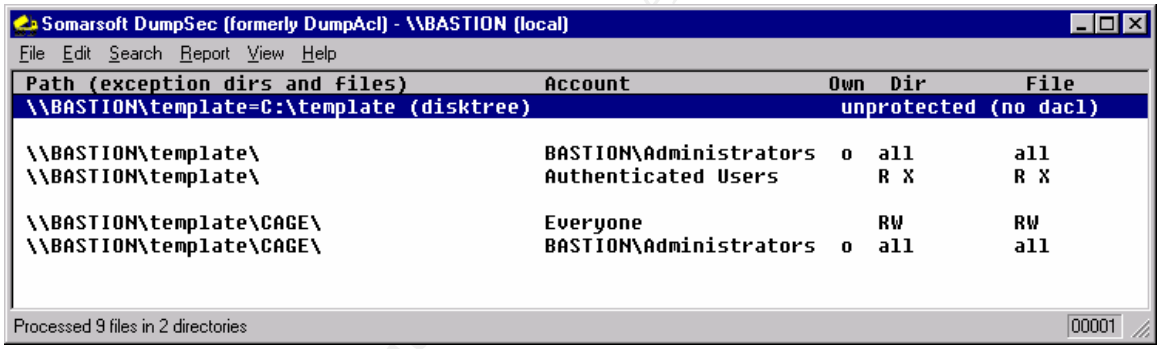


NOTE – Enabling successful logging of File and Object Access will result in excessive entries into the Event Logs. Disable successful logging if the log files become unmanageable.

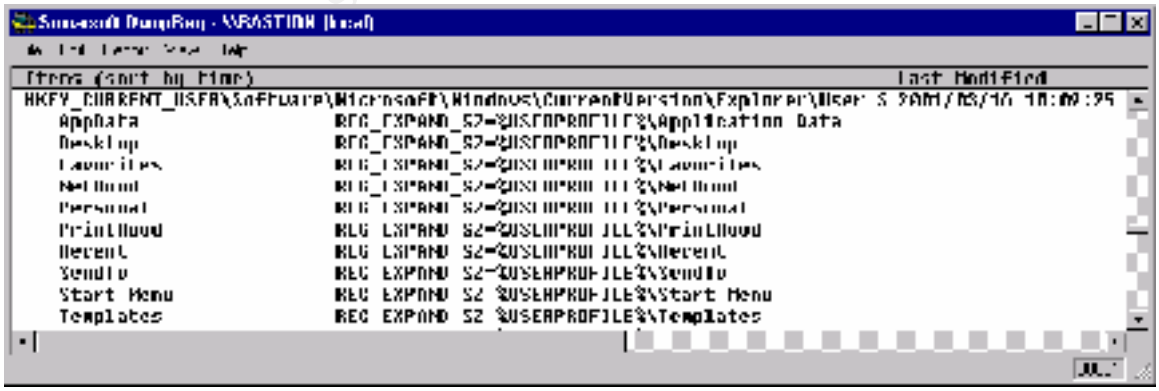
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Tools to manage NTFS Permissions and Auditing

- Small Wonders Software Security Explorer – http://www.securityexplorer.com
- CACLS.EXE – built in Windows NT utility for managing NTFS permissions on files
- Microsoft Windows NT 4.0 Server Resource Kit:
  PERMCOPY.EXE – copies share permissions from one share to another
  SECADD.EXE – changes permissions on registry keys
  RMTSHARE.EXE – manages shared folders and printers on remote systems, including permissions
  SHAREUI.DLL – manage shared folders (hidden and visible) on remote systems via Windows Explorer
  Net Watch – manage and monitor hidden and visible shares on multiple systems
- Trusted System's SuperCACLS – http://www.trustedsystems.com
- Pedestal Software's NT Command Line Security Tools – http://www.pedestalsoftware.com
- SomarSoft DumpSec – http://www.somarsoft.com



- DumpReg from Somarsoft – http://www.somarsoft.com



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Advanced User Rights Assignment

Open User Manager and navigate to Policies → User Rights → check the Show Advanced User Rights checkbox.

User Right:	User Accounts:
Access this computer from the network	IUSR_BASTION IWAM_BASTION Don't add Administrators as a security measure!
Act as part of the operating system	None
Add workstations to the domain	None
Back up files and directories	Administrators Backup Operators
Bypass traverse checking	Authenticated Users
Change the system time	Administrators
Create a pagefile	Administrators
Create a token object	None
Create permanent shared objects	None
Debug programs	Administrators or None!!!
Force shutdown from a remote system	Administrators or None!!!
Generate security audits	None
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	None
Log on as a batch job	None (unless specifically needed)
Log on as a service	None (unless specifically needed)
Log On Locally	Administrators Backup Operators IUSR_BASTION IWAM_BASTION
Manage auditing and security log	Administrators
Modify firmware environment variables	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Replace a process level token	None
Restore files and directories	Administrators Backup Operators
Shut down the system	Administrators
Take ownership of files or other objects	Administrators

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Disable Cached Logons

By default, Windows NT stores the last 10 users logon credentials. To disable the caching of logon information, add the following value to the registry:

Hive:	HKEY_LOCAL_MACHINE
Key:	\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon
Value Name:	CachedLogonsCount
Data Type:	REG_DWORD
Value:	0

Disable Administrative Shares

To disable Administrative shares (such as C$, D$, and ADMIN$) on the bastion host server, add the following registry value:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\LanmanServer\Parameters
Value Name:	AutoShareServer
Value Type:	REG_DWORD
Value Data:	0

Disable 8.3 File Name Creation

To disable the automatic generation of 8.3 file names, add the following registry value:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\FileSystem
Value Name:	NtfsDisable8dot3NameCreation
Value Type:	REG_DWORD
Value Data:	1

Hide the Last Logon User Name

Set the following value in the Registry to hide the name of the last user that logged on:

Hive:	HKEY_LOCAL_MACHINE
Key:	\Software\Microsoft\Windows NT\Current Version\Winlogon
Value Name:	DontDisplayLastUserName
Value Type:	REG_SZ
Value Data:	1

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Secure Printer Drivers

To prevent the installation of a Trojan printer driver, restrict the installation of printer drivers to Administrators by setting the following value in the registry:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers
Value Name:	AddPrintDrivers
Value Type:	REG_DWORD
Value Data:	1

Control Access to the Schedule Service

By default, only Administrators and Power Users can submit jobs to the Schedule service. However, to control who can LIST the jobs that have been submitted to the Schedule Service, set the permission on the following registry key to:

User Account:	Permissions:
Administrators	Full Control
System	Full Control

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\Schedule

Disable Boot to another Operating System using the Floppy Drive

To prevent a malicious user from booting the server to another operating system using a floppy disk, modify the BIOS to boot from the hard drive first, and set a password on the BIOS to prevent this setting from being modified.

For example, a Linux boot floppy disk can be used to reset the Administrator's password, even if SYSKEY has been used to secure the SAM database on the server:
http://home.eunet.no/~pnordahl/ntpasswd

NOTE – Password protecting the BIOS will disable unattended reboots.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Prevent Exploit of Trojan Notification Packages and Sub-Authentication Packages

Sub-authentication packages are loaded if they are listed as Auth# values in the following key:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\Lsa\MSV1_0
Value Name:	Auth1, Auth2, Auth3, etc.
Value Type:	REG_SZ
Value Data:	(the name of the sub-package DLL file)

Notification packages are listed in a multi-string value named Notification Packages.

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\Lsa
Value Name:	Notification Packages
Value Type:	REG_MUTLI_SZ
Value Data:	(zero or more package DLL filenames)

To defend against any malicious notification or sub-authentication packages, make the following changes:

1. If the File and Print Services for NetWare or the Directory Service Manager for NetWare are not required, then delete the FPNWCLNT entries from the Notification Packages and Auth# values listed in the above registry locations.

2. Configure permissions and auditing of the registry keys above to the following:

User Account:	Permission:
Administrators	Full Control
System	Full Control
Authenticated Users	Read

User Account:	Auditing:
Everyone	All Auditing

Full Auditing = Everyone

3. Configure NTFS permissions and auditing for:
FPNWCLNT.DLL (C:\Winnt\System32\fpnwclnt.dll) and
PASSFILT.DLL (C:\Winnt\System32\passfilt.dll)

User Account:	Permission:
Administrators	Full Control
System	Full Control
Authenticated Users	Read

User Account:	Auditing:
Everyone	All Auditing

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

1. Fossen, Jason. Securing Windows NT, Step-by-Step. The SANS Institute, 2001.

2. Fossen, Jason. Securing Internet Information Server 5.0. The SANS Institute, 2001.

3. Paller, Alan. Choosing and Justifying the Right Intrusion Detection and Vulnerability Analysis Tools. The SANS Institute, 2001.

4. Norberg, Stefan. Securing Windows NT/2000 Servers for the Internet. O'Reilly Press, 2001.

5. Schultz, E. Eugene. Windows NT/2000 Network Security. Macmillan Technical Publishing, 2000.

6. Scanbray, Joel, et. al. Hacking Exposed – Second Edition: Network Security Secrets & Solutions. Osborne/McGraw-Hill, 2001.

7. Jumes, James G., et. al. Microsoft Windows NT 4.0 Security, Audit, and Control. Microsoft Press, 1999.

8. Microsoft Corporation. Windows NT Server 4.0 Resource Kit. Microsoft Press, 1996.

9. Microsoft Corporation. Internet Information Server Resource Kit. Microsoft Press, 1998.

10. "Windows NT Security Guidelines: Considerations & Guidelines for Securely Configuring Windows NT in Multiple Environments – A study for NSA Research by Trusted Systems Services." http://www.trustedsystems.com

11. "MS Security Configuration Manager for Windows NT 4." http://www.microsoft.com/technet/winnt/Winntas/technote/scmnt4.asp

12. "Step by Step Guide to Using the Security Configuration Tool Set." http://www.microsoft.com/WINDOWS2000/library/planning/security/secconfsteps.asp

13. "Windows NT 4.0 Member Server Configuration Checklist." http://www.microsoft.com/technet/security/mbrsrvcl.asp

14. "Microsoft Internet Information Server 4.0 Security Checklist." http://www.microsoft.com/technet/security/iischk.asp

15. "Designing and Planning Windows NT External Security." http://www.microsoft.com/technet/winnt/winntas/technote/Planning/ntextsec.asp

16. Windows NT Security Website. http://www.microsoft.com/TechNet/security/winntsec.asp

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SANS GCNT Practical References – http://www.sans.org/giactc/gcnt.htm

1. Moses, David. "IT Services Security Plan – Hardening and Managing IIS 4 servers for the Internet."
2. Dean Farrington. "Windows NT Web Server Auditing."
3. Yeo, Lisa. "Configuring and Auditing Windows NT With Security Configuration Manager."
4. McClelland, Alan. "Securing Windows 2000 on the Internet."
5. Michael Hom. "Practical Assignment for GIAC NT."
6. Millott, Robert. "Security Configuration for Windows 2000 Server Acting as an IIS 5.0 Web Server."
7. LaRoche, Mary. "Audit Guidelines for Microsoft IIS with Windows 2000."
8. Brig, Otis. "SANS Practical."

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

NTLMv2 Authentication

Setting this value on a web server bastion host may not be needed, and is included for informational purposes only since it is one of the top methods to secure a Windows NT Network (based on the information available in Securing Windows NT, Step-by-Step).

NTLMv2 is only needed for secure communication of NT password hashes over the network between clients and domain controllers. Password cracking utilities such as L0phtCrack cannot sniff password hashes over the wire when using NTLMv2 authentication.

Setting the value to 1 will provide the widest compatibility. Setting the value to 5 on both client and server will provide the most secure authentication method. Setting this value will break communication with all clients not configured with the appropriate client setting for the server authentication setting and will break communication with all non-Microsoft clients.

Authentication and session security options are set in a registry value named LMCompatibilityLevel on both Windows NT and Windows 9x clients.

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\Lsa
Value Name:	LMCompatibilityLevel
Value Type:	REG_DWORD
Value Data:	0 to 5

Level Number	Results of setting LMCompatibilityLevel for authentication.
0	This is the default behavior if the value is not defined. The client will authenticate exactly as it did before and not use NTLMv2. Domain controllers will accept NTLMv2 if a client requests it.
1	Clients will attempt to negotiate NTLMv2, but will fall back to LM and NTLMv1 authentication when necessary. Domain controllers will accept NTLMv2 authentication if the client requests it.
2	Clients will use NTLMv1 authentication only. Clients will not use LM or NTLMv2 responses. Domain controllers will accept NTLMv2 authentication if the client requests it.
3	Clients will use NTLMv2 authentication only. Domain controllers will accept NTLMv2 authentication if the client requests it.
4	Clients will use NTLMv2 authentication only. Domain controllers will refuse LM authentication, and accept NTLMv1 or NTLMv2 authentication if the client requests it.
5	Clients will use NTLMv2 authentication only. Domain controllers will refuse LM and NTLMv1 authentication and accept only NTLMv2.

For more information, see the following Microsoft articles:

- Q239869: "How to Enable NTLMv2 for Windows 95/98 Clients" http://support.microsoft.com/support/kb/articles/Q239/8/69.ASP
- Q147706: "How to Disable LM Authentication on Windows NT" http://support.microsoft.com/support/kb/articles/Q147/7/06.asp

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SMB Message Signing

Windows NT uses the Server Message Block (SMB) protocol to access shared folders, printers and named pipes over the network (based on the information available in Securing Windows NT, Step-by-Step). To prevent SMB sessions from being hijacked, modify the registry of the server and client with the following values:

To ENABLE SMB message signing on a Windows NT system running the SERVER service, add the following registry value:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\LanManServer\Parameters
Value Name:	EnableSecuritySignature
Value Type:	REG_DWORD
Value Data:	1

To REQUIRE SMB message signing on a Windows NT system running the SERVER service, add the following registry value:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\LanManServer\Parameters
Value Name:	RequireSecuritySignature
Value Type:	REG_DWORD
Value Data:	1

To ENABLE SMB message signing on a Windows NT system running the WORKSTATION service, add the following registry value:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\Rdr\Parameters
Value Name:	EnableSecuritySignature
Value Type:	REG_DWORD
Value Data:	1

To REQUIRE SMB message signing on a Windows NT system running the WORKSTATION service, add the following registry value:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\Rdr\Parameters
Value Name:	RequireSecuritySignature
Value Type:	REG_DWORD
Value Data:	1

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Securing the NetLogon Channel

The NetLogon Channel allows communication, like pass-through authentication and synchronization of user accounts, to occur within a Windows NT domain. Unsecured NetLogon Channel communication is vulnerable to packet sniffing and man-in-the-middle attacks. If a computer is a member of a domain, when it boots up, the NetLogon Service establishes communication with a domain controller (based on the information available in Securing Windows NT, Step-by-Step).

Making this change is not necessary on a web server bastion host that is installed as a stand-alone server, as it is not a member of a domain and does not run the NetLogon service, and is included for informational purposes only.

Encryption and integrity checking of the NetLogon channel is enabled in the registry by adding the following values:

Hive:	HKEY_LOCAL_MACHINE\SYSTEM
Key:	\CurrentControlSet\Services\Netlogon\Parameters

Value Name	Value Type	Effects
SignSecureChannel	REG_DWORD	When set to 1, all outgoing NetLogon channel packets will be digitally signed for integrity checking.
SealSecureChannel	REG_DWORD	When set to 1, all outgoing NetLogon channel traffic will be encrypted. This option also forces digital signing.
RequireSignOrSeal	REG_DWORD	When set to 1, all outgoing NetLogon channel traffic must at least be digitally signed, but may also be encrypted. These options will be negotiated. Should a remote system support neither option, the NetLogon connection to it will fail. Enable this value only if all domain controllers have been upgraded to SP4. This includes domain controllers in trusted domains.

© SANS Institute 2000 - Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Audit Tape Backups and Additional Use of User Rights

By default, the following User Rights are not audited, even when the option to Audit Successful Use of User Rights has been enabled in User Manager:

- Backup Files and Directories
- Bypass Traverse Checking
- Create A Token Object
- Debug Programs
- Generate Security Audits
- Replace A Process Level Token
- Restore Files and Directories

To enable auditing of these additional user rights, add the following value to the registry:

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\Lsa
Value Name:	FullPrivilegeAuditing
Value Type:	REG_BINARY
Value Data:	1

NOTE – Adding this additional auditing will create a massive amount of entries in the log during normal operations, and especially during the Backup and Restore procedures. Enabling Full Privilege Auditing will decrease performance on the server.

File Encryption on NTFS 4 volumes

Windows NT 4.0 does not include any file encryption capabilities integrated into the operating system (although Windows 2000 does). To perform file encryption on NT 4.0, a third party product must be used. These utilities can be found at:

- http://www.pgp.com
- http://www.rsasecurity.com

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.