



Building a Windows NT bastion host in practice

*Stefan Norberg (stnor@sweden.hp.com)
HP Consulting*

Version 1.01

Abstract

This paper presents a checklist for converting a default Windows NT installation to a bastion host. This document makes no or little attempt to explain or discuss the features it implements. Therefore I suggest that you read all the Knowledge Base articles in Appendix A and the referenced documents in Appendix C. If there is something you don't understand after having read these articles, DO NOT CONTINUE. Read them again or look for additional assistance.

What is a Bastion Host?

A bastion host is a computer system that is exposed to attack, and may be a critical component in a network security system. Special attention must be paid to these highly fortified hosts, both during initial construction and ongoing operation. Bastion hosts can include:

- Firewall gateways
- Web servers
- FTP servers
- Name servers (DNS)
- Mail hubs
- Victim hosts (sacrificial lambs)

The American Heritage Dictionary defines a bastion as:

1. A projecting part of a rampart or other fortification. 2. A well-fortified position or area. 3. Something regarded as a defensive stronghold.

Marcus Ranum is generally credited with applying the term bastion to hosts that are exposed to attack, and its common use in the firewall community. In [1] he says:

Bastions are the highly fortified parts of a medieval castle; points that overlook critical areas of defense, usually having stronger walls, room for extra troops, and the occasional useful tub of boiling hot oil for discouraging attackers. A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Generally, bastion hosts will have some degree of extra attention paid to their security, may undergo regular audits, and may have modified software.

Bastion hosts are not general purpose computing resources. They differ in both their purpose and their specific configuration. A victim host may permit network logins so users can run untrusted services, while a firewall gateway may only permit logins at the system console. The process of configuring or constructing a bastion host is often referred to as hardening. The effectiveness of a specific bastion host configuration can usually be judged by answering the following questions:

- How does the bastion host protect itself from attack?
- How does the bastion host protect the network behind it from attack?

Extreme caution should be exercised when installing new software on bastion hosts. Very few software products have been designed and tested to run on these exposed systems. See [2] for a thorough treatment of bastion hosts.

Install NT

Start with a clean system. The machine should not be attached to a public network while doing the installation/configuration. If you have to have a network connection, make sure it's an isolated trusted network segment. Do not have any other operating systems installed on your bastion host. Install Windows NT 4.00 US-ENGLISH. Use only NTFS. If installing NT Server, make it a "stand-alone" member server. This server will not be able to participate in a domain environment. Do not install IIS 2.0. If you want to run IIS, install it from the NT option pack.

As for network protocols and services, install only TCP/IP and do not install additional network services.

Install software

Install any third party software. This might be a web server like IIS 4.0. To install IIS 4.0 you have to have SP3 or SP4 already on the system. This doesn't change the fact that you have to re-install SP4 afterwards.

(Re-)Install the latest service pack

Install the latest service pack for Windows NT 4.00. At the time of writing, this is Service Pack 4.

Install available hotfixes

Install all available hotfixes. The hotfixes are available from <ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40>.

This is a list of fixes included in the roll-up patch bundle (post-SP4) as of April 4th 1999:

Q192296 Specially-Malformed GET Requests Can Create Denial of Service
Q195540 Windows NT 4.0 Does Not Recognize ATAPI Iomega Clk 40! Drive
Q195725 Intermediate Network Driver Causes STOP 0x0000001E on MP PC
Q195733 Denial of Service in Applications Using RPC over Named Pipes
Q196270 SNMP Agent Leaks Memory When Queried
Q214802 WinNT Lets You Paste Text into Unlock Workstation Dialog Box
Q214840 MSV1_0 Allows Network Connections for Specific Accounts

Date	Time	Version	Size	File name	Platform
11/20/98	06:11p		247,056	advapi32.dll	(x86)
11/06/98	12:47p		13,744	class2.sys	(x86)
12/16/98	01:08p		130,320	infocomm.dll	(x86)
01/18/99	04:06p		124,176	msgina.dll	(x86)
02/02/99	03:47p		47,376	msvl_0.dll	(x86)
11/20/98	06:11p		29,456	perfctrs.dll	(x86)
11/12/98	01:38p		12,048	rpclts1.dll	(x86)
11/16/98	05:29p		17,680	snmp.exe	(x86)
11/17/98	03:21p		8,976	tapiperf.dll	(x86)
11/11/98	12:13p		147,664	tcpip.sys	(x86)
12/16/98	01:11p		113,936	w3svc.dll	(x86)
11/20/98	06:11p		188,176	winlogon.exe	(x86)

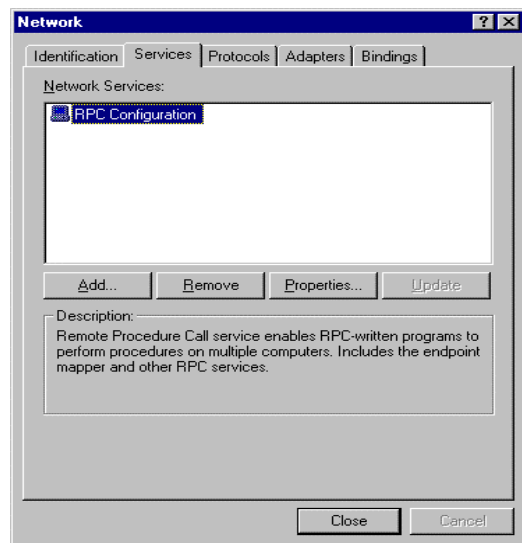
Remove unused network services

Remove all unused services with the Network application in the Control Panel. This should leave you with a configuration looking like the picture to the right.

Only the RPC configuration for the port mapper (RpcSs) is left. IIS will not start without it.

Note that when you remove the Workstation service, you will get a message every time you start the Network application in Control Panel: "Windows NT Networking is not installed. Do you want to install it now?" Ignore this question by answering NO.

Another caveat is that User Manager for Domains (usrmgr.exe) stops working when the Workstation service is not running. Replace it with User Manager (usrmgr.exe) from NT Workstation.



Disable NETBIOS

By unbinding the WINS Client in the Network application from all adapters, we get rid of all listeners on the NETBIOS ports. Network -> Bindings -> All protocols -> WINS Client -> Disable.

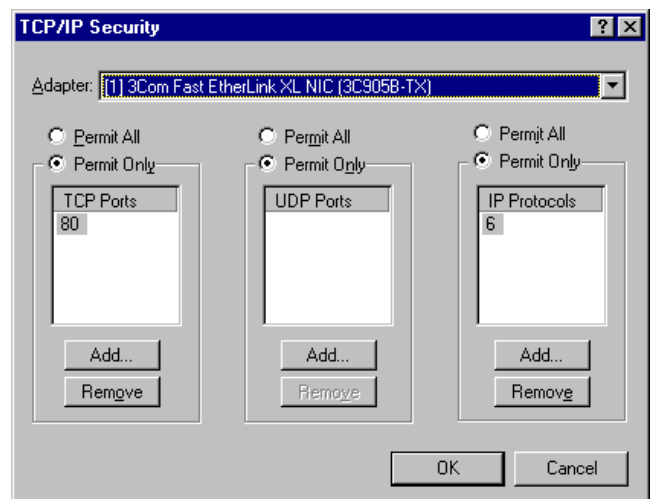
Also disable the WINS Client driver in Control Panel -> Devices -> WINS Client -> Disable.

Configure TCP/IP filters

Configure TCP/IP-security by specifying what ports are allowed inbound (TCP or UDP) on each network adapter. This is done in the Network application -> Protocols -> TCP/IP -> Advanced -> Enable Security -> Configure.

Example: Web-server

The configuration shown to the right allows only connections to tcp/80.



No UDP is accepted. IP protocol 6 is TCP.

Disable unused services

Everything should be disabled but the following (excluding any applications we want running on the system of course).

Disable all but the services below is a good idea.

- EventLog
- NT LM Security Support Provider
- Plug and Play
- Protected Storage
- Remote Procedure Call (RPC) Service

The processes that should be running are these:

smss.exe Session Manager

csrss.exe	Client Server Subsystem
winlogon.exe	The logon process
services.exe	The main service handler process
pstores.exe	Protected storage
lsass.exe	Local Security Authority
rpcss.exe	The RPC end-point mapper
explorer.exe	The Explorer GUI
loadwc.exe	Explorer related
nddeagnt.exe	Explorer related

Encrypt the system accounts database

Run the syskey.exe utility (with the key on disk option). This will provide protection against password cracking tools like L0pht Crack (<http://www.l0pht.com/>).

Apply policies and ACLs

Run the Microsoft Security Configuration Editor (SCE) in command line mode. This tool is included in the same archive as this document. This tool is a part of the service pack 4 CD. Our configuration file is called bastion.inf. This file is an ASCII text file. You can take a look at it in your favorite editor, but it's best viewed with the SCE Microsoft Management Console snap-in.

```
C:> secedit /configure /cfg bastion.inf /db %TEMP%\secedit.sdb /verbose /log %TEMP%\scelelog.txt
```

This will make a number of changes to your configuration. Here is a summary of the most significant changes:

Account policies

Password policy

Enforce password uniqueness by remembering last passwords	6
Minimum password age	2
Maximum password age	42
Minimum password length	10
Complex passwords (passfilt.dll)	Enabled
User must logon to change password	Enabled

Account lockout policy

Account lockout count	5
Lockout account time	Forever
Reset lockout count after	720 mins

Local policies

Audit policy

Audit account management	Success, Failure
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success, Failure

User rights assignment

SeAssignPrimaryTokenPrivilege	No one
SeAuditPrivilege	No one
SeBackupPrivilege	Administrators
SeCreatePagefilePrivilege	Administrators
SeCreatePermanentPrivilege	No one
SeCreateTokenPrivilege	No one

SeDebugPrivilege	No one
SeIncreaseBasePriorityPrivilege	Administrators
SeIncreaseQuotaPrivilege	Administrators
SeInteractiveLogonRight	Administrators
SeLoadDriverPrivilege	Administrators
SeLockMemoryPrivilege	No one
SeNetworkLogonRight	No one
SeProfileSingleProcessPrivilege	Administrators
SeRemoteShutdownPrivilege	No one
SeRestorePrivilege	Administrators
SeSecurityPrivilege	Administrators
SeShutdownPrivilege	Administrators
SeSystemEnvironmentPrivilege	Administrators
SeSystemProfilePrivilege	Administrators
SeSystemTimePrivilege	Administrators
SeTakeOwnershipPrivilege	Administrators
SeTcbPrivilege	No one
SeMachineAccountPrivilege	No one
SeChangeNotifyPrivilege	Everyone
SeBatchLogonRight	No one
SeServiceLogonRight	No one

Event log settings

The Application, System and Security logs are configured to be up to 100MB each. They will overwrite events as needed, but only entries older than 30 days. Anonymous access to the logs is disabled.

Registry Values

The policy will also apply the following changes to the registry.

KEY	Type	Value
MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\AddPrintDrivers	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnablePlainTextPassword	REG_DWORD	0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoDisconnect	REG_DWORD	15
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoShareWks	REG_DWORD	0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\AutoShareServer	REG_DWORD	0
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\RequireSecuritySignature	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\EnableSecuritySignature	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel	REG_DWORD	1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous	REG_DWORD	1
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode	REG_DWORD	1
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilityLevel	REG_DWORD	2
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText	REG_SZ	This is a private system. Unauthorized use is prohibited.
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption	REG_SZ	Hardened by HP Consulting
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName	REG_SZ	1
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAuditFail	REG_DWORD	1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown	REG_DWORD	1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\CachedLogonsCount	REG_SZ	0
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateFloppies	REG_SZ	1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AllocateCDRoms	REG_SZ	1
MACHINE\System\CurrentControlSet\Control\Lsa\AuditBaseObjects	REG_DWORD	1
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl	REG_DWORD	0
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing	REG_BINARY	1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon	REG_SZ	1

File system and Registry Access Control Lists

The ACLs applied to the file system and the registry are identical to what Microsoft ships as the "Highly secure workstation" template in SCE. For details check the bastion.inf file with the SCE snap-in in MMC.

Administrator account

The bastion.inf policy renames the Administrator account to "root". This should be changed to something unique for your environment. Make sure to have a strong password on the Administrator account as well.

Remove unused and potentially dangerous components

If an attacker gains access to the bastion host it is crucial that the attacker doesn't get extra help to establish a back door or gain access to other systems. Therefore it's good practice to remove unused binaries from the bastion host. The downside of doing this is that it may slow down the administrators as well. Use your judgement here.

To remove DOS, Win16, OS/2 and Posix sub systems

KEY	Type	Value
MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Optional	REG_BINARY	00 00
MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Os2	N/A	REMOVE THIS KEY
MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems\Posix	N/A	REMOVE THIS KEY
MACHINE\SYSTEM\CurrentControlSet\Control\WOW	N/A	REMOVE THIS KEY

Delete the following files:

```
%SystemRoot%\system32\ntvdm.exe
%SystemRoot%\system32\krnl386.exe
%SystemRoot%\system32\psxdll.dll
%SystemRoot%\system32\psxss.exe
%SystemRoot%\system32\posix.exe
%SystemRoot%\system32\os2.exe
%SystemRoot%\system32\os2ss.exe
%SystemRoot%\system32\os2srv.exe
%SystemRoot%\system32\os2 (directory)
```

Other potential dangerous tools

```
%SystemRoot%\system32\nbtstat.exe
%SystemRoot%\system32\tracert.exe
%SystemRoot%\system32\telnet.exe
%SystemRoot%\system32\tftp.exe
%SystemRoot%\system32\rsh.exe
%SystemRoot%\system32\rcp.exe
%SystemRoot%\system32\rexec.exe
%SystemRoot%\system32\finger.exe
%SystemRoot%\system32\ftp.exe
%SystemRoot%\system32\lpq.exe
%SystemRoot%\system32\lpr.exe
```

Open Ports

It's not possible to make Windows NT stop listening on some ports and have a supported environment. For example it's not supported to stop the RPC end-point mapper service (RpcSs.exe on TCP and UDP port 135). Even more annoying is the fact that the RpsSs fires up an undocumented TCP-listener on a high port (usually port tcp/1027). Another port that shows in netstat is tcp/1028, but it does not seem to respond on connection attempts.

Output of netstat on my test system:

```
C:\>netstat -an

Active Connections
```

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING (IIS)
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING (RpsSs)
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING (RpcSs)
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING (IIS)
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING (???)
TCP	0.0.0.0:1028	0.0.0.0:0	LISTENING (???)
TCP	127.0.0.1:1025	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1025	127.0.0.1:1028	ESTABLISHED
TCP	127.0.0.1:1026	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1028	127.0.0.1:1025	ESTABLISHED
UDP	0.0.0.0:135	*:*	(RpcSs)

C:\>

We will have to live with this. The TCP/IP security filters should deny any connection attempts made to those ports.

Test of TCP/IP security filters

Let's try the TCP/IP security filters. First I configured the filters to allow only tcp/80 and udp/1111. Then I fired up listeners with netcat (<http://www.l0pht.com/~weld/netcat/>) on tcp/80,81 and udp/1110,1111. To test I used netcat to try to connect to the server on the listener ports.

The tcpdump output below shows the behavior of the filter function.

UDP packets to port 1110 (blocked) shows no output on the listener.

```
22:54:14.041112 arp who-has 10.0.0.43 tell 10.0.0.5
22:54:14.041171 arp reply 10.0.0.43 is-at 0:10:5a:e6:cf:74
22:54:14.041240 10.0.0.5.1252 > 10.0.0.43.1110: udp 10
22:54:16.909514 10.0.0.5.1252 > 10.0.0.43.1110: udp 11
```

UDP packets to port 1111 (unblocked) shows output on the listener.

```
22:58:30.045340 10.0.0.5.1254 > 10.0.0.43.1110: udp 10
22:58:32.807513 10.0.0.5.1254 > 10.0.0.43.1110: udp 11
```

UDP packets to port 1111 (unblocked) with no listener sends ICMP udp port unreachable.

```
23:00:39.497178 10.0.0.43 > 10.0.0.5: icmp: 10.0.0.43 udp port 1111 unreachable
23:00:39.725978 10.0.0.5.1255 > 10.0.0.43.1111: udp 2
23:00:39.726038 10.0.0.43 > 10.0.0.5: icmp: 10.0.0.43 udp port 1111 unreachable
23:00:39.979497 10.0.0.5.1255 > 10.0.0.43.1111: udp 5
```

TCP connect to port 80 (unblocked) shows output on the listener.

```
23:03:05.220808 10.0.0.5.1264 > 10.0.0.43.http: S 52482:52482(0) win 8192 <mss 1460> (DF) [tos 0x10]
23:03:05.220922 10.0.0.43.http > 10.0.0.5.1264: S 61918:61918(0) ack 52483 win 8760 <mss 1460> (DF)
23:03:05.221044 10.0.0.5.1264 > 10.0.0.43.http: . ack 1 win 8760 (DF) [tos 0x10]
23:03:07.289221 10.0.0.5.1264 > 10.0.0.43.http: P 1:7(6) ack 1 win 8760 (DF) [tos 0x10]
23:03:07.395725 10.0.0.43.http > 10.0.0.5.1264: . ack 7 win 8754 (DF)
23:03:11.146798 10.0.0.5.1264 > 10.0.0.43.http: P 7:8(1) ack 1 win 8760 (DF) [tos 0x10]
23:03:11.301110 10.0.0.43.http > 10.0.0.5.1264: . ack 8 win 8753 (DF)
23:03:11.960993 10.0.0.5.1264 > 10.0.0.43.http: R 52490:52490(0) win 0 (DF) [tos 0x10]
```

TCP connect to port 81 (blocked) shows no output on the listener. NT sends RST.

```
23:23:43.669792 10.0.0.5.1286 > 10.0.0.43.81: S 52552:52552(0) win 8192 <mss 1460> (DF) [tos 0x10]
23:23:43.669857 10.0.0.43.81 > 10.0.0.5.1286: R 0:0(0) ack 52553 win 0
23:23:44.168936 10.0.0.5.1286 > 10.0.0.43.81: S 52552:52552(0) win 8192 <mss 1460> (DF) [tos 0x10]
23:23:44.168995 10.0.0.43.81 > 10.0.0.5.1286: R 0:0(0) ack 1 win 0
23:23:44.669639 10.0.0.5.1286 > 10.0.0.43.81: S 52552:52552(0) win 8192 <mss 1460> (DF) [tos 0x10]
23:23:44.669697 10.0.0.43.81 > 10.0.0.5.1286: R 0:0(0) ack 1 win 0
23:23:45.170337 10.0.0.5.1286 > 10.0.0.43.81: S 52552:52552(0) win 8192 <mss 1460> (DF) [tos 0x10]
23:23:45.170392 10.0.0.43.81 > 10.0.0.5.1286: R 0:0(0) ack 1 win 0
```


Conclusion

The TCP/IP security filters works well on Windows NT 4 .0 SP4.

If the filters are enabled, NT will ignore UDP-packets and TCP connection attempts will be reset on the denied ports.

Secure the application

The last step is to make a security review of the application that is going to run on the system. This might include NTFS ACLs/Auditing and checking with application vendor for known holes and workarounds or patches.

Summary

Now your system is reasonably secured. The only way of breaking into it over the network (as far as I can tell) is by exploiting a vulnerability in the applications running on the host (or the MS IP-stack possibly) to run arbitrary code that opens up the system.

What we've done here is basically rendered our system inoperable from a management perspective. Windows NT does not provide us with remote logging. NT based remote administration tools like the Event Viewer and Server Manager is based on NETBIOS and the problem with NETBIOS is that it's considered a no go in perimeter networks. This is because everything runs in NETBIOS (SMB/CIFS, management and other applications based on named pipes) which means you cannot limit traffic to a host in router access control lists in a granular way. Hence we have to find other - preferably standardized - ways of administering and monitoring the Windows NT host.

HP Consulting has world-class security consultants experienced in building perimeter networks in a secure, manageable and highly available manner. Contact us if you are interested in our services. Send an email to Mikael Johansson (mijo@sweden.hp.com).

Disclaimer

HEWLETT-PACKARD DOES NOT WARRANT THE ACCURACY OR COMPLETENESS OF THE INFORMATION GIVEN HERE. ANY USE MADE OF, OR RELIANCE ON, SUCH INFORMATION IS ENTIRELY AT USER'S OWN RISK.

Copyright

This paper, and all contents, are Copyright ©1999 by Stefan Norberg and Hewlett-Packard. Do not duplicate, republish, mirror, or reprint without permission.

Appendix A: Relevant MS Knowledge Base articles

Microsoft Support Knowledge Base is available on the Internet at <http://support.microsoft.com/support/search>. Use "Search for a specific article ID number" and type in the PSS ID number.

<i>PSS ID Number</i>	<i>Name of article</i>
Q93362	C2 Evaluation and Certification for Windows NT
Q101063	Windows NT Logon Welcome, Displaying Warning Message
Q114463	Hiding the Last Logged On Username in the Logon Dialog
Q114817	No Shutdown Button in Windows NT Server Welcome Screen
Q140058	How To Prevent Auditable Activities When Security Log Is Full
Q142641	Internet Server Unavailable Because of Malicious SYN Attacks
Q143164	INF: How to Protect Windows NT Desktops in Public Areas
Q143474	Restricting Information Available to Anonymous Logon Users
Q143475	Windows NT System Key Permits Strong Encryption of the SAM
Q146906	How To Secure Performance Data in Windows NT
Q147706	How to Disable LM Authentication on Windows NT
Q151082	HOWTO: Password Change Filtering & Notification in Windows NT
Q153094	Restoring Default Permissions to Windows NT System Files
Q155363	HOWTO: Regulate Network Access to the Windows NT Registry
Q161372	How to Enable SMB Signing in Windows NT
Q161990	How to Enable Strong Password Functionality in Windows NT
Q166992	Standard Security Practices for Windows NT
Q172925	INFO: Security Issues with Objects in ASP and ISAPI Extensions
Q172931	Cached Logon Information
Q174840	Disabling Buttons in the Windows NT Security Dialog Box
Q176820	Differences Between 128-bit and 40-bit versions of SP3 & SP4
Q187506	List of NTFS Permissions Required for IIS Site to Work
Q195227	SP4 Security Configuration Manager Available for Download
Q214752	Adding Custom Registry Settings to Security Configuration Editor

Appendix B - List of Ports Used by Windows NT version 4.0

<i>Function</i>	<i>Static ports</i>
Windows NT	
Browsing	UDP:137,138
DHCP Lease	UDP:67,68
DHCP Manager	TCP:135
Directory Replication	UDP:138 TCP:139
DNS Administration	TCP:135
DNS Resolution	UDP:53
Event Viewer	TCP:139
File Sharing	TCP:139
Logon Sequence	UDP:137,138 TCP:139
NetLogon	UDP:138
Pass Through Validation	UDP:137,138 TCP:139
Performance Monitor	TCP:139
PPTP	TCP:1723 IP Protocol:47 (GRE)
Printing	UDP:137,138 TCP:139
Registry Editor	TCP:139
Server Manager	TCP:139
Trusts	UDP:137,138 TCP:139
User Manager	TCP:139
WinNT Diagnostics	TCP:139
WinNT Secure Channel	UDP:137,138 TCP:139
WINS Replication	TCP:42
WINS Manager	TCP:135
WINS Registration	TCP:137
Convoy Clustering (WLBS)	
Convoy	UDP:1717
WLBS	UDP:2504
Exchange	
Client/Server Comm.	TCP:135
Exchange Administrator	TCP:135
IMAP	TCP:143
IMAP (SSL)	TCP:993
LDAP	TCP:389
LDAP (SSL)	TCP:636
MTA - X.400 over TCP/IP	TCP:102
POP3	TCP:110
POP3 (SSL)	TCP:995
RPC	TCP:135
SMTP	TCP:25
NNTP	TCP:119
NNTP (SSL)	TCP:563
Terminal Server	
RDP Client (Microsoft)	TCP:3389 (Pre Beta2:1503)
ICA Client (Citrix)	TCP:1494

DCOM RPC high ports

By default DCOM dynamically allocates one high port (>1023) per process. There is a way to limit the port mapper to only a specific range of ports. You must decide how many ports you want to allocate, which is equivalent to the number of simultaneous DCOM processes through the firewall. You must open all of the UDP and TCP ports corresponding to the port numbers you choose. In addition, you must open TCP/UDP 135, which

is used for RPC End Point Mapping, among other things. In addition, you must tell DCOM which ports you reserved using the following registry key:

```
HKEY_LOCAL_MACHINES\Software\Microsoft\Rpc\Internet
```

You probably will have to create this key.

Here is an example of how to restrict DCOM to a range of 10 ports:

```
Named value: Ports
Type: REG_MULTI_SZ
Setting: Range of port. Can be multiple lines such as: 3001-3010 135.
```

```
Named value: PortsInternetAvailable
Type: REG_MULTI_SZ
Setting: "Y"
```

```
Named value: UseInternetPorts
Type: REG_MULTI_SZ
Setting: "Y"
```

Appendix C – References

#	Document	Author(s)	Where
1	Thinking About Firewalls V2.0: Beyond Perimeter Security	Marcus J. Ranum	http://www.clark.net/pub/mjr/pubs/think/index.htm
2	Building Internet Firewalls	D. Brent Chapman and Elizabeth D. Zwicky	O'Reilly & Associates ISBN: 1-56592-124-0
3	Securing Windows NT Installation	Microsoft Corporation	http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp
4	Building a Bastion Host Using HP-UX 10	Kevin Steves	http://people.hp.se/stevesk/security/bastion.html

Appendix D – Acknowledgements

This white paper would not have been published without the help of the following people:

Hans Jönsson (HP Support) for assisting me with practical tests and being supportive in a UNIX-loving environment.

Kevin Steves (HP Consulting) for writing an excellent paper on making a bastion host of HP-UX [4] and correcting my confused attempts to write about this subject in English.

Appendix E – Files included in this archive

This document is available for free as an Adobe Acrobat PDF. It's available from

<http://people.hp.se/stnor>

Additional files included are:

<i>File name</i>	<i>Description</i>	<i>MD5 hash</i>
bastion.inf	The security template	1c3865586837e6e6a8f1f182d ea261fd
secedit.exe	Microsoft Security Configuration Manager – command line version	e2c64f52418f90212999930a3 39fd342
scedll.dll	The SCE core DLL	1bd8ce63c98b97b2b5769dff3 9b71801
esent.dll	Extensible Storage Engine DLL – required to run SCE	6a07e37421e03ca3bdf5983f0 a73ce69

Appendix F – About the author

Stefan Norberg has been working as technical consultant for six years with UNIX and Windows NT infrastructure. He mainly works with security related consulting in Internet environments. Stefan holds a MCSE+Internet certification and is a Microsoft Certified Trainer. You can reach him at stnor@sweden.hp.com.