Securing Windows NT

Careful configuration and monitoring of NT, especially Internet-facing NT machines, can make the difference between a secure system and one which is open to security breaches. We explain the steps you need to take.

By Justin S Kapp

Windows NT has become a popular choice as a platform for providing Internet services. As a result it is becoming more and more important that the Windows NT machine is secure from attack.

In order to keep Windows NT secure while on the Internet or on a private network it is important that you have a baseline starting point for a secure system. This starts with the installation and continues through to the live system monitoring.

When securing Windows NT it is important to decide what role the machine is to undertake. There is a core set of tasks that should be undertaken for any machine and some specific tasks for different machine roles. It is also important to limit the machine to a limited set of roles, as this reduces the possible exposure of the machine to security breaches.

There are a few things you need to have before you start:

- Windows NT Server CD (for server installs).
- Windows NT Workstation CD (required for Workstation installs, plus some Server installs).
- Latest Windows NT Service Pack (more than one service pack may be required), and required Windows NT hot fixes.
- Microsoft Security Configuration Manager (SCM), which is part of the NT Service Pack 4 CD or is available from the Microsoft Web site.
- Any hardware drivers (network, SCSI card etc) for your specific machine configuration.

Installation

Firstly determine the requirements for the machine. Make sure you have all the pre-requisite items to hand before you start the installation. The instructions given here are geared towards the US English Windows NT; however, they are equally valid for other language versions. Some of the system configuration may leave certain system elements unusable, and note that configuration should not be attempted at all if you are not familiar with installing and configuring Windows NT.

During the various stages of the machine configuration it is a good idea to perform a backup of the machine settings using RDISK, which allows you to restore the machine to a known configuration should there be a problem.

Another way to preserve the machine is to create a machine image using a product like Norton Ghost or PowerQuest ServerMagic, and cut the image to CD. If restoring from the image to more than one machine, make sure each machine has a unique Security Identifier (SID) created using a tool like NewSID from System Internals (**www.sysinternals.com**).

Firstly you should install the system onto a disk partitioned to use only the NTFS file system, since only NTFS supports NT's access control lists for files. When installing an Internet-based Server or Enterprise Server, make the machine a "standalone" member server. This server will not participate in a domain environment.

You should create a system partition of around 1 GB, and partition the rest of the disks so you have separate partitions for your data, such as your Web server root directories and extra applications that are not part of the operating system.

Keeping the machine system files separate from data and other applications is good practice to avoid some security issues. Some applications (such as ftp servers and Web servers) try to enforce a sandbox for users to operate within. Sometimes, if there is an implementation issue and, as a result, aa compromise in the sandbox, it would mean the user may have access outside this sandbox. Thus separating this sandbox from the system files reduces the risk of compromise to system files. It is also a good idea to keep the log files for such services separate, too - this makes it easier to maintain them.

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

Figure 1 - Account policies.

"The process of intrusion detection is something of a black art. However, there are various tools that can be used to assist the administrator, but remember that these tools do not provide full cover!"

When installing on a machine you should start with the minimum required and add any other components you need later. You should not install any of the following:

- Any games.
- Any accessories.
- Any communications.
- Any multimedia options.
- Any Windows messaging.
- Internet Information Server (IIS) Version 2.0.

You should only install TCP / IP networking protocols; do not install any other network services unless explicitly required - for instance DNS or WINS if they are required for the machine's role.

Software

Install any third-party software as required, but be aware that some software may require installing once other items (such as the NT Service Pack) have been installed.

The next step is to install the latest NT service pack and hot fixes. The current NT service pack at the time of writing is SP6. It is important that, should you create a backup during the service pack installation, this backup is removed before the machine is made live on a public network. This is simply because, if someone should gain access to the machine, they could use the older files from the backup as a means to enable further weaknesses that could be exploited.

In between service packs, Microsoft releases the latest fixes as hot fixes. These fixes are available from **ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/nt40**. It may not be necessary to install all the available fixes; however, a minimum subset including all security-relevant fixes for the machine configuration must be installed.

Many applications that would be installed on the machine will have their own updates. Some fixes for some of the Microsoft Back Office applications (SQL Server, Exchange, IIS) are released separately to those for Windows NT, and these will require installing once the relevant application is installed.

Application software such as Office and Internet Explorer will also require updating. These applications are not usually installed on Internet-facing servers, but they are used on many Workstation installations and as such they do present issues, which the updates resolve.

Securing The SAM

The next step is to secure the system accounts database (SAM). This is performed by executing the application SYSKEY.EXE. This provides some pro-

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

Figure 2 - Local policies.

Security NT

tection against password-cracking tools such as L0phtcrack. Password-cracking applications such as L0phtcrack need to extract information from the SAM in order to attack the passwords of users, and encrypting the database makes it harder for these tools to extract this information.

It is also important to remove the directory %SystemRoot%\Repair before the machine is made live because this also contains a copy of the SAM that is placed on a repair disk.

Configuration Steps

Some of the following steps may be skipped as required; however, this depends on exactly the intended use and environment the host will be operating within. Sample environments are described later.

Remove Unused Network Services

In the Network applet in Control Panel go to Services and remove any unused services. Depending on the use of the machine you should remove everything except RPC Configuration. Other services may be required, depending on the role of the machine. For example, RPC services are required for Internet Information Server (IIS) to operate.

When the Workstation service is removed you will get a message every time you re-enter the Network applet: "Windows NT Networking is not installed. Do you want to install it now?" Ignore this by entering "No". On Windows NT Server, once the Workstation service is removed, User Manager For Domains (USRMGR.EXE) will stop working. This can be fixed by replacing it with the User Manager from NT Workstation (MUSRMGR.EXE).

Certain components may need to be disabled, such as NETBIOS. This can be achieved by unbinding the WINS client in the Network applet from all network interfaces. This is performed by Network->Binding->All protocols->WINS Client->Disable. Also disable the WINS Client driver in Control Panel->Devices->WINS Client->Disable.

Disable Unused Services

In the Services applet in Control Panel disable any services that are not in use. The following services should not be disabled.

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

Key	Type	Value
MACHINE\System\CurrentControlSet\Control\Print\Provide rs\LanMan Print Services\AddPrintDrivers	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\Enabl ePlainTextPassword	REG_DWORD	0
MACHINE\System\CurrentControlSet\Services\LanMan Server\Parameters\AutoDisconnect	REG_DWORD	15
MACHINE\System\CurrentControlSet\Services\LanMan Server\Parameters\AutoShareWks	REG_DWORD	0
MACHINE\System\CurrentControlSet\Services\LanMan Server\Parameters\AutoShareServer	REG_DWORD	0
MACHINE\System\CurrentControlSet\Services\LanMan Server\Parameters\EnableForcedLogOff	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\LanMan Server\Parameters\RequireSecuritySignature	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\LanMan Server\Parameters\EnableSecuritySignature	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\Requi reSecuritySignature	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Rdr\Parameters\Ena bleSecuritySignature	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Netlogon\Paramete rs\RequireSignOrSeal	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Netlogon\Paramete rs\SealSecureChannel	REG_DWORD	1
MACHINE\System\CurrentControlSet\Services\Netlogon\Paramete rs\SignSecureChannel	REG_DWORD	1
MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonym ous	REG_DWORD	1
MACHINE\System\CurrentControlSet\Control\Session Manager\ProtectionMode	REG_DWORD	1
MACHINE\System\CurrentControlSet\Control\Lsa\LmCompatibilit yLevel	REG_DWORD	2
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText	REG_SZ	Warning.
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption	REG_SZ	Hardened
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\DontDisplayLastUserName	REG_SZ	1
MACHINE\System\CurrentControlSet\Control\Lsa\CrashOnAudi tFail	REG_DWORD	1
MACHINE\System\CurrentControlSet\Control\Session Manager\Memory Management\ ClearPageFileAtShutdown	REG_DWORD	1
MACHINE\Softw are\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\Audit BaseObjects	REG_DWORD	1
MACHINE\System\CurrentControlSet\Control\Lsa\SubmitContr ol	REG_DWORD	0
MACHINE\System\CurrentControlSet\Control\Lsa\FullPrivile geAuditing	REG_BINARY	1
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ShutdownWithoutLogon	REG_SZ	1

Figure 3 - Registry changes recommended to harden a machine.

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

Figure 4 - Registry entries which should be removed.

Use TCP/IP Filters

Windows NT does have some packet-filtering features that can be configured within the Network applet properties for the TCP / IP protocol advanced options. These are set on a per-interface basis and should only be implemented if required. This can be skipped if packet filtering is performed by another application such as a firewall.

However, if the packet filtering is provided by an application it will not become active until the application has started. Some Windows NT service packs have been known to break the TCP / IP filters, and as a result these cannot always be relied on.

Security Configuration

Service Pack 4 includes a tool called the Security Configuration Manager (SCM). SCM allows the administrator to automate the process of performing various configuration tasks, such as configuring audit settings for system objects, password policy etc.

Files To Remove
%SystemRoot%\system32\ntvdm.exe
%SystemRoot%\sy stem32\krnl386.exe
%SystemRoot%\system32\psxdll.dll
%System Root%\system32\psxss.exe
%SystemRoot%\system32\posix.exe
%Sy stemRoot%\system32\os2.exe
%SystemRoot%\system32\os2ss.exe
% SystemRoot%\system32\os2srv.exe
%SystemRoot%\system32\os2 (directory)

Other Potentially Dangerous Tools
%SystemRoot%\system32\nbtstat.exe
%SystemRoot%\sy stem32\tracert.exe
%SystemRoot%\system32\telnet.exe
%System Root%\system32\tftp.exe
%SystemRoot%\system32\rsh.exe
%Syste mRoot%\system32\rcp.exe
%SystemRoot%\system32\rexec.exe
%Sys temRoot%\system32\finger.exe
%SystemRoot%\system32\ftp.exe
% SystemRoot%\system32\lpq.exe
%SystemRoot%\system32\lpr.exe

Figure 5 - Dangerous files.

"During the various stages of the machine configuration it is a good idea to perform a backup of the machine settings using RDISK, which allows you to restore the machine to a known configuration should there be a problem."

SCM uses a script file that performs the configuration of the machine, and comes as a command-line tool and a Management Console plug-in. The SCM MMC plug-in can be used to edit the script file to implement the change you wish to make. The SCM also comes with some common machine configurations, for machines in different roles such as a Workstation, or a PDC. So the configurations supplied can be used to secure both Internet-facing and non-Internet-facing systems.

The configurations that come with the SCM are:

- Basic (default) Windows NT Domain Controller 4.0.
- Basic (default) Windows NT Server 4.0.
- Basic (default) Windows NT Workstation 4.0.
- Compatible Windows NT Domain Controller 4.0.
- Compatible Windows NT Workstation\Server 4.0.
- High Security configuration for Windows NT 4.0 Domain Controllers.
- High Security Windows NT Workstation\Server 4.0.
- Specific file system settings for MS Office 97-SR1. Append to compatible configuration.
- Secure configuration for Windows NT 4.0 DCs.
- Secure Windows NT Workstation\Server 4.0.

With the SCM you can set up your policies and ACL requirements easily. When you are hardening a machine you need to implement various policies and Access Control List (ACL) settings. The policies listed in Figure 1 and Figure 2 are a good starting point for securing a machine; these settings are based loosely around the High Security Workstation / Server script included with the SCM.

When securing the file system and registry, the settings provided in the sample script included with the Security Configuration Manager for a High Security Workstation / Server are an optimal choice. Some applications may require that some files or directories can be accessed by a certain user or group; any change in permissions to these files or directories may result in the application failing to work properly.

Using the SCM you can also set the properties of the Application, System and Security logs. It is good practice to have the logs set for a maximum size

Key	Type	Value
MACHINE\Software\Microsoft\RPC\ClientProtocols\nca cn_ip_tcp	N / A	REMOVE THIS KEY
MACHINE\Software\Microsoft\RPC\ClientProtocols\nca cn_ip_udp	N / A	REMOVE THIS KEY
MACHINE\Software\Microsoft\RPC\ServerProtocols\nca cn_ip_tcp	N / A	REMOVE THIS KEY
MACHINE\Software\Microsoft\RPC\ServerProtocols\nca cn_ip_udp	N / A	REMOVE THIS KEY

Figure 6 - Remove these registry entries in order to disable RPC.

Security NT

of approximately 100 MB, and so that the system overwrites events as required, but only those events older than 30 days. Also set it so that only Administrators can access the logs. In some applications it may be advantageous to have the logs manually rotated and to machine halt if the logs become full, to ensure the full audit trail.

There are also a number of registry changes that are recommended to harden a machine. These are shown in Figure 3.

Accounts

Before the machine is placed on a public network rename the system Administrator account to something obscure. The Administrator account is one of two accounts that cannot be deleted; it also provides a known account that can be used as a target for attack.

Also give this account a complex password that is difficult to guess using a dictionary, with a minimum length of 10 characters; however, one of 14 characters is preferable, for instance 345EdHd.T4Q-4j. Using a password that includes symbols as well as numbers and letters makes it much harder for someone to determine the password using brute force with a dictionary or randomly-generated characters.

It is sometimes useful to disable Administrator access from over the network; however, this is often impractical if the server is held on a remote co-location site.

To act as a decoy for would-be attackers, create a new account named Administrator, then disable this account and make sure it does not have any rights to access the system. Also make sure that the built-in Guest account is disabled and remove any rights this account has to the system.

If any user accounts are required for the machine, then create them and make sure these accounts only have access rights required for operation of the services or user using that account, and nothing more than required.

If an attacker gains access to the machine it is important that the attacker is able to cement any intrusion by establishing a back door or gaining access to other systems. Therefore it's good practice to remove unused or potentially dangerous applications from the system. This will have the side-effect of slowing down site administrators, too. Any removal of files should be made on individual judgement.

Remove Subsystems

The removal of DOS, Win16, OS/2 and Posix sub-systems will remove possibly dangerous elements. However, removal of Win16 or DOS may cause problems. Many Win32 applications still have installation programs that are Win16 applications (such as Installshield). If one of these applications is executed, the system will claim the executable isn't a valid Windows NT application. The registry entries should be removed as shown in Figure 4.

Figure 5 shows a number of other files which should also be removed, and other potentially dangerous tools.

Open Ports

It is possible to stop Windows NT listening on all ports. However, this

```
C:\>netstat -an
Active Connections
Proto      Local Address          Foreign Address    State
TCP        0.0.0.0:80             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        0.0.0.0:1026           0.0.0.0:0          LISTENING (???)
TCP        0.0.0.0:1029           0.0.0.0:0          LISTENING (???)
TCP        127.0.0.1:1025         0.0.0.0:0          LISTENING
TCP        127.0.0.1:1036         0.0.0.0:0          LISTENING
UDP        0.0.0.0:135            *:* (RpcSs)
C:\>
```

Figure 7 - Sample output from the NETSTAT.EXE command.

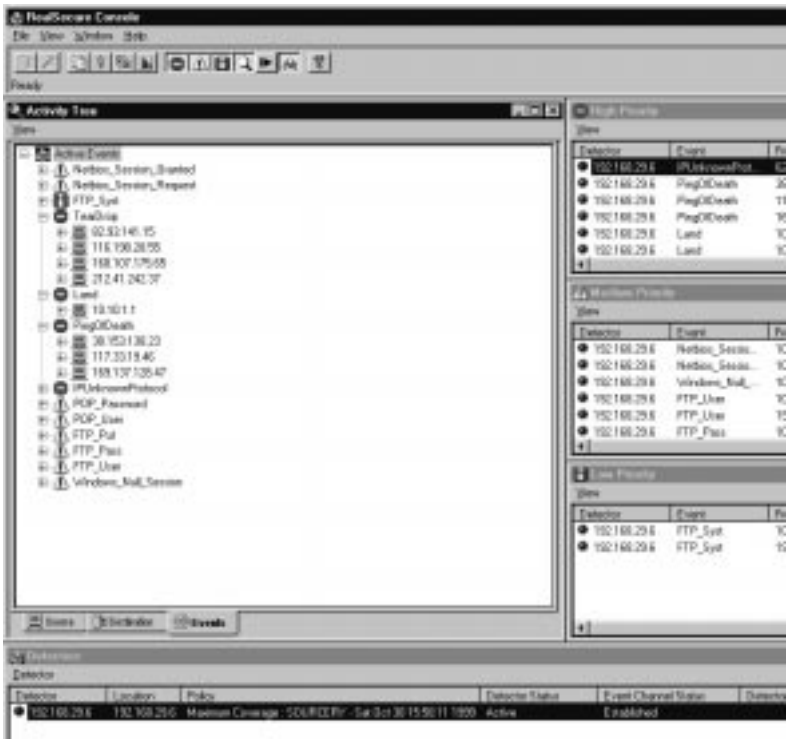

Figure 8 - The RealSecure Console after a possible attack.

"Once the system is up and running it is important to provide a means of monitoring the system's day-to-day activity - for both accounting purposes and, more importantly, intrusion detection."

isn't very useful and many applications rely on RPC loopback communication. For instance, Microsoft Internet Information Server (IIS) and other Microsoft products will stop working if the RPC client or Server is disabled. To disable RPC, remove the registry entries shown in Figure 6.

Configurations

Firewall machines are frontline machines, and will often come under scrutiny from external and internal threats. As such the firewall machine needs to be heavily protected.

Most firewall machine configurations are machines with two network interfaces. The machine will sit between two networks, one network per interface. When this machine is in place, if penetrated it can form a starting point for the attacker into the internal network. The goal is to make this event as hard as possible. This configuration is known as a Bastion Host.

Another common machine configuration is a Web Server which, like the firewall, is a frontline machine. It is a public-facing machine and can often come under attack. This type of configuration will again need to be a Bastion Host.

Once the basic Windows NT configuration is complete you should perform all the use-specific configuration changes mentioned previously in order to make a Bastion Host.

Workstation Hardening

The user workstations are often hidden behind a firewall, but hardening of these is still useful. The requirements of a workstation are completely different to those of a server. During the installation most of the time you will need to leave in place items such as Microsoft Networking and keep the DOS and Win16 sub-systems in place.

However, make sure the latest service packs and hot fixes are installed - and it is important to install the service packs or releases for applications installed on the workstation. Applications such as Internet Explorer, Outlook and Office all have numerous issues, which can affect the security of the workstation. Installing anti-virus measures is also a must for an Internet-connected workstation.

Intrusion Index

There are four levels of severity of penetration of security of any computer system.

Level One

Level One is simply attacks such as mail bombing, Denial of Service attacks, and other attacks that would take on average about 30 minutes to resolve. This level of attack is easily resolved - mail bombing and similar attacks can usually be dealt with using the server software banning access from the perpetrator's domain.

Denial of Service attacks can become a little tricky if the attack is unknown to the software vendor. However, in most cases the attack will be known, and to resolve the issue you would need to obtain the relevant patch from the vendor and apply it to the system.

Unknown attacks would require more time to resolve. You would need to gather as much information about the attack as possible, then pass this information onto the software vendor and/or CERT. Then wait for the vendor to release a fix. Some attacks may be prevented by configuring an upstream firewall or screening router to filter the offending packets if applicable to the type of attack.

Level Two

Level two attacks include attacks which result in locally gaining read and write access to files which the attacker shouldn't have access to. This also depends to some extent on the type of file to which access is gained.

The severity of this level also depends on whether the user is able to gain write access, which can often follow on from gaining read access. This type of issue is usually resolved internally; it may include actions such as disabling the user's accounts, and disciplinary action being brought against the user. Also gather evidence of the attacks just in case there are any issues later.

Level Three

Level three usually revolves around an external user being able to gain access to internal files, or to

execute a limited number of commands. A high proportion of level three issues are the result of problems with machine configuration, bad CGI and buffer overflow problems.

Level Four

Finally, level four is a situation that should never occur. This final level of intrusion is a fatal condition, where the attacker has full access to the system with rights to achieve anything. This type of intrusion is rare - however, it is still possible.

Resolving Attacks

Level three and four attacks are a serious problem, so you need to take a number of steps to resolve the situation and to gather information about the attacker.

Isolate the system so that activity can be monitored without impacting on the surrounding systems. Allow the activity to continue. Log ALL activity heavily. Make every effort to trace the source or sources of attack.

Security NT

Also contact your local law enforcement body responsible for computer-related crime. This should be done early on, since they will be able to advise you and maybe assist by explaining what information they require and the procedures involved in order to make a case for arrest. Remember that the person committing a level three or four attack is now a criminal; if you catch that criminal, gathering the evidence to convict the person will take some time, so take all the help you can get.

Sometimes the situation may not warrant pursuing further if the attack is very minor. It is also important to remember that if your system is being used as a staging point for an attack on another party, this could result in possible legal issues if you allow continued access. When you contact your local law enforcement body they will be able to advise you regarding this.

These levels of attack define various levels of severity; a simple attack where the attacker steals the password database may be quite minor at first, and is difficult to prove unless the attacker uses the information stolen to gain entry again. Continuing attacks are more serious and are easier to prove, whereas one-off attacks are often harder to prove.

Intrusion Detection

Once the system is up and running it is important to provide a means of monitoring the system's day-to-day activity - for both accounting purposes and, more importantly, intrusion detection.

The process of intrusion detection is something of a black art. However, there are various tools that can be used to assist the administrator, but remember that these tools do not provide full cover! It is important to remember that a human is required to view the output of the intrusion detection systems and also to provide a personal review of the system on a regular basis.

Intrusion detection systems are only as good as the information they use as rules to perform checks. If a new attack comes along it is likely your intrusion detection system will be unable to detect or prevent the attack. So using your common sense is an important tool. However, automated detection systems do make the process a lot easier.

"With Windows NT Server you get the tool Netmon, which is a basic packet sniffer. This tool can be used for real-time monitoring of network traffic and also to look at protocol-based attacks such as Teardrop UDP attack."

When monitoring Windows NT you need to know what to look at and what things to look for. You first need to watch for known attacks; most Intrusion Detection Systems do this today. The next thing to look for is any event that affects your system security. This sounds a bit vague - however, here are some examples of what to look for:

- A new user being added to your system.
- Administrator logins or logouts.
- An administrator establishing a trust relationship.
- Someone deleting a system file.
- Someone changing another user's profile.
- Someone taking ownership of another user's file.
- Remote login attempts from unknown machines or networks.

Two very important event categories to monitor on Windows NT are privilege changes and impersonation, both of which are means to gain additional privileges.

Keep a close watch on the various vulnerabilities mailing lists and Web sites for information on new attacks. They will often provide details on how to detect the attack, or provide sample code to demonstrate the attack, and you can use this to test your systems or use in a controlled environment to evaluate the attack and develop a means to detect the attack.

Microsoft Tools

Windows NT comes as standard with a number of tools to help the system administrator monitor system usage. The main repository into which Windows NT logs information is the Event Log; the Windows NT security providers all log information into the Security Log within the Event Log system. However, it will only log what you have configured the system to log, and the SCM scripts contain sections that set up the auditing for common events so that they are logged.

Other tools, which are very useful for determining the real-time system usage, are the Performance monitor and the Windows NT Task Manager; these provide a real-time look at what processes are running on the system, which is a valuable tool for locating processes that shouldn't be running on the system.

Another tool which is very useful is NETSTAT. This provides a real-time look at which TCP/IP ports are open and in use on the machine. This tool will help you find such things as the backdoor Trojans such as Back Orifice or NetBus. Most of these backdoor Trojans open up TCP or UDP ports, usually above port 1024, to allow the attacker to penetrate the system.

During the installation of the system it is a very good idea to run the NETSTAT tool at various stages of the configuration to determine the ports open on the system in its clean state, so that this information can be used as a reference point when checking the system later for possible intrusion. See Figure 7 for a sample output from the

Windows NT NETSTAT.EXE command.

If the relevant port is not required for normal operation of the machine, it should be removed or filters used to deny any connection attempts to it. If a process on the machine opens listening ports, the purpose of the ports should be determined since this can be a sign of unwelcome activity on the machine.

With Windows NT Server you get the tool Netmon, which is a basic packet sniffer. This tool can be used for real-time monitoring of network traffic and also to look at protocol-based attacks such as Teardrop UDP attack.

Microsoft Server software such as Internet Information Server (IIS) provides logging features. The range of products for IIS all output logging information in one of three possible formats. There are tools available to read these log files. It is important with these log files that you are able to spot suspicious activity.

Third-Party Tools

When attempting to keep an NT machine secure it is important to monitor the machine for possible intrusions, and whilst the various logs provided by the OS can help, for certain things these logs can fall short. There are a number of third-party intrusion detection systems available for Windows NT which can be used to provide an alternative source of information to detect attack.

ISS (**www.iss.net**) produces the RealSecure product. This product is designed to detect common attacks as they occur and provides a means of tracking where they originated. This is performed by a series of rules that the detection engine employs during runtime in order to isolate attacks. Figure 8 shows a section of sample output from RealSecure after what appears to be several failed Denial of Service attacks on a Windows NT server.

CyberSafe Corporation produces a product called Centrax (**www.cybersafe.com**), which is another intrusion detection system. There is also Network Associates' (**www.nai.com**) CyberCop product line, and RSA Data Security's Kane Security Analyst and Kane Security Monitor (**www.rsa.com**).

Other third-party tools include Tripwire for NT (**www.tripwiresecurity.com**); once configured, this popular Unix tool for detecting change in the system can be used to detect changes in the configuration of the machine, which can be useful for detecting successful attacks on the system. The Windows NT product includes all of the features available to Unix users and some features specific to Windows NT.

The tools filemon and regmon from System Internals are also valuable tools for determining the usage of the system. Filemon is used to determine which files are open or being opened by processes on the system. Regmon is used to determine registry activity - which processes opened which keys and what information was changed or viewed.

Further Information

There are a number of sources of information that are extremely important to the Administrator. Remember that there are both "Black Hat" sites (underground) and "White Hat" sites that contain security information, and they are both equally useful. Some of the more useful starting points:

PacketStorm Security is a very good source of the latest security issues and can be found at **packetstorm.security.com.**

Bugtraq is a mailing list for the discussion and announcement of computer security vulnerabilities. Details of how to subscribe and access archives of the mailing list can be found at **www.securityfocus.com.**

NTBugtraq is the Windows platform version of the Bugtraq mailing list. NTBugtraq can be found at **www.ntbugtraq.com.**

COAST (Computer Operations, Audit and Security Technology) is a research project into computer security in the Computer Science Department at Purdue University. COAST also boasts a large catalogue of security and audit-related applications in their ftp archive. COAST can be found at **www.cs.purdue.edu/coast/coast.html**.

CERT (Computer Emergency Response Team) provides information regarding many security issues, including advisory information. CERT is located at **www.cert.org.**

L0pht is a "Black Hat" group that performs testing of commonly used tools for security issues. L0pht also produces a number of useful tools for testing system security, and can be found at **www.l0pht.com.**

PCNA

Copyright ITP, 2000

The Author

Justin S Kapp (justin.kapp@itp-journals.com) is an IT security consultant. He specialises in cryptography and Windows platform security, and is the original author of the RSAEuro Cryptographic Library.

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.