Global Information Assurance Certification Paper

GIAC ADVANCED INCIDENT HANDLING AND HACKER EXPLOITS
By George Cruz

Preventing

Detecting

And

Responding

To

Intrusion

For

Windows NT

Introduction 6

The Threat 6

Deter the Intrusion 7
Detect the Intrusion 8
Approach 9
Passive Intrusion Detection *10*
Active Intrusion Detection *10*
Investigating User Accounts 11
Monitoring Active Processes 11
Examining System Logs 11
Network and Configuration 12
Examining Services 12
Locating Intruder Modifications 12
Searching 12
Comparisons 12
Sorting 12
Proactive Intrusion Detection *13*
Wrappers 13
Network Traffic Monitor (Sniffer) 13
Determine the Penetration Technique 14
Account Compromise *14*
Brute Force 14
Really weak passwords 15
Dictionary attacks 15
Snooping 15
Hole creation 15
Buffer overflows 15
Physical Intrusion 16
Network 16
Non-technical 16
Social Engineering 16
Exploits *17*
Remote 17
Local 17
Administrator 17
Hacker Tools *17*
System Crashes and Denial of Service *18*
System Security Problems *18*
Determine the Extend of Penetration 18
Administrator *18*
Users other than Administrator *19*
Determine Intruders signature and any attempts to conceal its signature 19
Outsiders *19*
Insiders *19*
Trojan Files *20*

Back Doors 20
Intrusion outside your system 20
Modification or Destroying Of Logs Files 21
Evaluate the findings and determine best course to resolve and prevent further penetration. 21

Passive Intrusion Detection **22**

Symptom: The system is unresponsive to commands and displays the blue crash screen 22
Symptom: Windows NT displays an error message upon system startup. 22
Possible Causes 23
Evidence 23
Symptom: Your system disk storage capacity has dramatically decreased in size to the point that the disk is dangerously low on free space. 23
Symptom: The system is running sluggishly for an unknown reason. 23
Possible Causes 24
Evidence 24

Active Intrusion Detection **25**

Investigating User Accounts Information 25
Methods: User Manager (Local Machine) User Manager for Domains (Domain Machine) 25
Method: Windows NT Explorer (Used to verify Directory/File permissions) 25
Method: Windows NT Explorer (used view directory/file auditing) 25
Monitoring Active Processes 26
Method: Task Manager, Performance Monitor (Application) 26
Method: Net (Command) 26
Method: SET 27
Method: Devices 27
Method: Services 27
Examining System Logs 28
Method: System Logs 28
Method: Security Logs 28
Method: Application Logs 28
Network Traffic and Configuration 29
Method: Netstat 29
Method: nbtstat 29
Method: Windows NT Diagnostics (Network) 30
Locating Intruder Modifications 30
Method: Find all Directory/file within the last xx days 30
Method: Install/Uninstalled Program 31
Method: Locate all files containing specific string syntax. 31
Usage: To find files and folders 31
Method: fc (File Compare) 31
Method: Registry Editor (regedit) 32
Method: Registry Editor (regedt32) 32

Proactive Intrusion Detection **33**

Vulnerabilities **33**

Brute Force 33

Exploit: Password Guessing/Cracking 33
Exploit: Lophtcrack 34
Prevention from Brute Force Attack: 34
Snooping 35
Exploit: nbtstat 35
Prevention 36
Exploit: Sniffers 36
Prevention 36
Exploit: Scanners 37
Prevention 37

Network Exploits **37**

Denial Of Service Attack Exploit 37
Exploit: Ping Of Death 37
Prevention 38
Exploit: SYN Attack 38
Prevention 38
Exploit: CPU Attacks (Telnet to Port XXX) 38
Prevention 39
Exploit: Crashing NT's LSA 39
Prevention 40
Exploit: Invalid IGMP Header DoS Vulnerability 40
Prevention 40
Exploit: NT Null Session Admin Name Vulnerability 41
Prevention 41
Exploit: NT Telnetd Vulnerability 41
Prevention 42
Exploit: NT Services.exe Denial of Service 42
Prevention 43
Man In The Middle Exploits 43
Exploit: Microsoft Windows IP Source Routing Vulnerability 43
Prevention 44
Exploit: SMB sessions can be hijacked 44
Prevention 45
Exploit: NT Predictable TCP Sequence Number Vulnerability 45
Prevention 45
Exploit: NT LSA DoS (Phantom) Vulnerability 45
Prevention 46
Local Attacks 46
Exploit: NT RASMAN Privilege Escalation Vulnerability 46
Prevention 47
Exploit: NT Unattended Installation File Vulnerability 47
Prevention 48
Exploit: NT DCOM Server Vulnerability 48
Prevention 48
Exploit: NT Master File Table Corruption Vulnerability 48
Prevention 49
Exploit: NT Malformed Dialer Entry Vulnerability 49

Prevention 49
Exploit: NT IOCTL Console DoS Vulnerability 50
Prevention 50
Exploit: NT Malformed Image Header DoS Vulnerability 50
Prevention 51
Exploit: NT Login Default Folder Vulnerability 51
Prevention 51
Exploit: NT Performance Counters Memory Leak Vulnerability 52
Prevention 52
Exploit: NT RAS Phonebook Buffer Overflow Vulnerability 52
Prevention 53
Exploit: NT Help File Buffer Overflow Vulnerability 53
Prevention 53
Exploit: NT Trojan Profile Vulnerability 53
Prevention 54
Exploit: NT CSRSS Worker Thread Exhaustion Vulnerability 54
Prevention 55
Exploit: NT Screensaver Vulnerability 55
Prevention 56
Exploit: NT Blank Password SP4 Vulnerability 56
Prevention 56
Exploit: NT Anonymous Users Can Obtain The Password Policy Under Windows NT 4.0 Vulnerability 56
Prevention 57
Exploit: NT RAS Dial-up Networking "Save Password" Vulnerability 57
Prevention 57
Exploit: NT Spoolss.exe Buffer Overflow Vulnerabilities 58
Prevention 58

WEB Server Attacks (IIS) 59

Exploit: Microsoft IE Setupctl ActiveX Control Buffer Overflow Vulnerability 59
Prevention 59
Exploit: Microsoft IE Registration Wizard Buffer Overflow Vulnerability 59
Prevention 60
Exploit: Microsoft IE5 Download Behavior Vulnerability 60
Prevention 61
Exploit: Microsoft IIS 4.0 Domain Resolution Vulnerability 61
Prevention 62
Exploit: Microsoft IIS FTP NO ACCESS Read/Delete File Vulnerability 62
Prevention 63
Exploit: Microsoft IE Import/Export Favorites Vulnerability 63
Prevention 64
Exploit: Microsoft IE Virtual Machine Sandbox Vulnerability 64
Prevention 65
Exploit: NT IE5 FTP Password Storage Vulnerability 65
Prevention 65
Exploit: Microsoft IE5 ActiveX "Eyedog" Vulnerability 66
Prevention 66

Exploit: Microsoft IE5 ActiveX "Object for constructing type libraries for scriptlets" Vulnerability 66
Prevention 67
Exploit: NT IIS Malformed HTTP Request Header DoS Vulnerability 67
Prevention 68
Exploit: NT IIS MDAC RDS Vulnerability 68
Prevention 69
Exploit: NT IIS SSL DoS Vulnerability 69
Prevention 70
Exploit: NT IIS Double Byte Code Page Vulnerability 70
Prevention 70
Exploit: NT IIS4 Buffer Overflow Vulnerability 71
Prevention 71
Exploit: NT IIS Showcode ASP Vulnerability 72
Prevention 72
Exploit: NT IIS ISAPI Extension Vulnerability 73
Prevention 73
Exploit: NT Using ASP And FSO To Read Server Files Vulnerability 73
Prevention 74
Exploit: NT IIS4 Shared ASP Cache Vulnerability 74
Prevention 74
Exploit: NT IIS and Perl - Enumerate Root Web Server Directory Vulnerability 74
Prevention 75
Exploit: NT IIS4 DoS - ExAir Sample Site Vulnerability 75
Prevention 75
Exploit: NT IIS FTP DoS / Buffer Overflow Vulnerability 75
Prevention 76
Exploit: NT IIS4 Log Avoidance Vulnerability 76
Prevention 76
Exploit: NT IIS4 Remote Web-Based Administration Vulnerability 76
Prevention 77

Application Attacks **77**

Exploit: Microsoft Excel SYLK Macro Execution Vulnerability 77
Prevention 77
Exploit: Microsoft Excel File Import Macro Execution Vulnerability 77
Prevention 78
Exploit: Microsoft JET Text I-ISAM Vulnerability 78
Evidence: None during the development of this document 79
Prevention 79

Windows NT Resource Kit **80**

Trojan Port Numbers **95**

References 98

Introduction

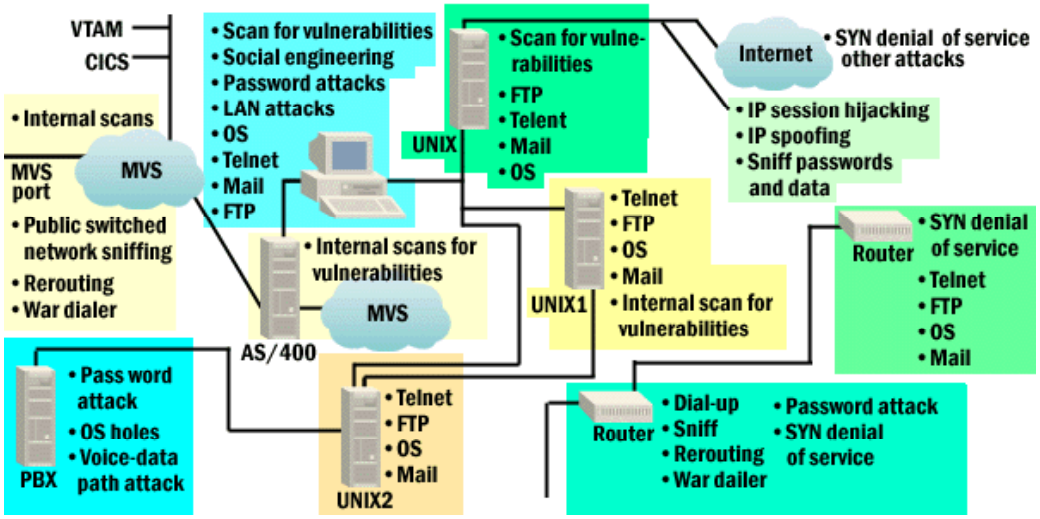
Network intrusions have become common and sophisticated. Attacking a system through a network provides the attacker with advantages that are not available when attacking a host. For example, network attacks often do not re-quire any previous access to the attacked system and may be totally invisible from the audit trail produced by the attacked host. In addition, the use of firewalls to protect enterprise networks from the external Internet has often sup-ported the design of open, efficient, and *insecure* internal networks. These networks are open to insider attacks. Although networks give the attacker additional advantages, networks, by their very nature, have some characteristics that intrusion detection systems (IDSs) can take advantage of. For instance, networks can provide detailed information about computer system activity, and they can provide this information regardless of the installed operating systems or the auditing modules available on the hosts. In addition, network auditing can be performed in a nonintrusive way, without notching the performance of either the monitored hosts or the network itself, and network audit stream generation cannot be turned off. Finally, network traffic has more precise and timely timing information than the audit records produced by the standard OS auditing facilities.

Effective enterprise security is all about managing risk. An effective enterprise security program is based on a multi-layered security policy that recognizes and addresses the complexity of the operational risks associated with any information system.

Protecting an information system is, in large measure, based on providing essential services while isolating the information system from those risks that would damage the system or the information it stores, processes, or transmits. Should the isolation measure fails, and an event occur that could damage a system, a prudent security policy provides that means to detect that failure and report the event to an assigned person/persons for resolution.

The Threat

A key challenge presented in protecting interconnected networks, intranets, and extranets, is to maintain isolation from individuals with no legitimate need to access the system: “outsiders”. Internetworking, particularly with the Internet, has grossly increased the number of outsiders with potential to access internal networks. This potential has been interpreted as a challenge by a significant number of those individuals, motivating them to develop techniques for penetrating system security.



This guide is design to prevent or deter penetration, although complete security is not achievable on Windows NT OS this guide will present some procedure to determine if and when a penetration has taken place and how to determine the extend of the penetration. The following methods should be followed to prevent penetration of network systems;

- Deter the Intrusion
- Detect the Intrusion
- Determine penetration techniques
- Determine the extend of penetration
- Determine Intruders signature and any attempts to conceal its signature
- Evaluate the findings and determine best course to resolve and prevent further penetration.

Deter the Intrusion

Capturing an accurate, reliable, and complete record of your systems and data when they are first created, and as they evolve, establishes the expected state against which to compare your current systems and data. The information to be captured includes a known, expected state for all assets -- your data (system and user), systems (hardware and software), networks (hardware and software), workstations (hardware, software), applications, and user environments. It should also include information that characterizes past process and user behavior derived from system and network transaction logs, once you have been operational for some period of time. This information is periodically compared with your current systems and data to determine if anything has been altered in an unexpected way.

Approaches to detecting signs of intrusion are usually based on identifying differences between your current operational state and a previously captured expected state. You need to know where each asset is located and what information you expect to find in each location. You need to be able to verify the correct or expected state of every asset. Without this information, you cannot adequately determine if anything has been added, deleted, modified, lost, or stolen. You may not be able to rebuild a critical component that has been compromised. Creating up to date records that are reliable and secure is the only way to address these requirements.

The Microsoft Windows NT Operating System (OS) provides several security features. However, the default COTS configuration is relaxed, especially on the NTW product. Because of the higher availability of NTW to an average home user, using the product in a static/isolated environment, the default configuration has few of the security features enabled. NTS, a higher-end product intended for corporate use, has many features enabled, but not all. Many of the features that can be set require undocumented and manually edited changes of the Registry or the use of utilities found only in the Resource Kits. **Please refer to NT Lockdown Document for a detail procedure for locking and securing Windows NT.** The following items listed below are basic outline for securing NT;

- **Install the Latest Service Pack and Hot-Fixes**
- **Secure the Registry**
- **Secure the Directory and File Structure**
- **Secure the Security Account Manager Database**
- **Secure Client/Server Communications**
- **Secure Event Log Viewing**

- **Secure Performance Data**
- **Secure Print Driver Installation**
- **Secure Services for an Internet or Firewall Server**
- **Secure Unnecessary Network Bindings**
- **Restrict Access to the Schedule Service**
- **Restrict Anonymous Network Access**
- **Restrict Anonymous Network Access from Listing Account Names and Network Shares**
- **Restrict Default Access Controls on Registry Keys**
- **Restrict Client-Side LanManager Password Authentication**
- **Disable Automatic Administrative Shares**
- **Disable Caching of Logon Credentials**
- **Disable Display of Last User Name**
- **Disable Guest Account**
- **Disable Removable Disk Access from Network**
- **Disable Shutdown Without Logon**
- **Rename the Administrator Account**
- **Wipe the Page File at a Clean System Shutdown**
- **Enforce Strong User Passwords**

The above outline is explained in detail in Appendix A of this document.

One particular installation's requirements can differ significantly from another. Therefore, it is necessary for administrators to individually evaluate their particular environments and requirements before implementing any of the security configurations suggested within this document. Implementing security settings can affect system configurations already in use or effect requirement variations in the future. Certain applications installed on Windows NT require more relaxed settings to function properly than others because of the nature of the product. Administrators are strongly advised to carefully evaluate recommendations in the context of their system configurations and environment.

Detect the Intrusion

Intruders are always looking for new ways to break into systems. They may attempt to breach your network's perimeter defenses from remote locations, or physically infiltrate your organization to gain direct access to its information resources. Intruders seek and take advantage of newly discovered vulnerabilities in operating systems, network services and protocols. They actively develop and utilize sophisticated programs to rapidly penetrate systems. As a result, intrusions, and the damage they cause, are achieved in a matter of seconds.

This means that even if your organization has implemented comprehensive information security measures, it is essential that your information resources, and transactions involving them, be watched closely for signs of intrusion. Doing so may be complicated, since intruders often cover their tracks by changing the systems they break into to hide their activities. In other words, an intrusion may have already taken place but you may not have noticed anything wrong because everything seems to be operating normally.

A general security goal is to prevent intrusions. But because no prevention measures are

perfect, you also need a strategy for handling intrusions that includes preparation, detection, and response. This module focuses on detection. The practices recommended below are designed to help you detect intrusions by looking for the "fingerprints" of known intrusion methods.

These practices are intended primarily for system and network administrators, managers of information systems, and security personnel responsible for networked information resources.

These practices are applicable to your organization if your networked systems infrastructure includes:

- Host systems providing services to multiple users (file servers, timesharing systems, database servers, Internet services, and so forth)
- Internal local-area or wide-area networks
- Direct connections, gateways, or modem access to and from external networks, such as the Internet

Approach

The general approach to detecting intrusions is

1. Observe your systems, networks, and user activities for anything unusual.

2. Investigate anything you find to be unusual.

3. If your investigation finds something that isn't explained by authorized activity, immediately initiate your intrusion response procedures.

While this process sounds simple enough, implementing it is a resource-intensive activity that requires continuous, automated support and daily administrative effort. Furthermore, the scale of intrusion-detection practices may need to change as threats, system configurations, or security requirements change. In all cases, however, there are five areas that must be addressed:

- Integrity of the software you use to detect intrusions
- Integrity of your file systems and the program and data files they contain
- Operations of your systems and the traffic on your networks
- Physical forms of intrusion to your computer systems, offline data storage media, and output devices
- Investigation of reports by users and other reliable sources (such as incident response teams) of unusual activities associated with your networked information resources

As you look for signs of intrusion, keep in mind that information from one source may not appear suspicious by itself. Inconsistencies among several sources can sometimes be the best indication of suspicious activities or intrusions.

Detection of Intrusions to your Systems or Network can be a difficult process, so a fundamental guideline should be in place to handle such an occurrence. If a intrusion is suspected on a system than an initial investigation should be performed prior to implementing a full intrusion investigation. If the initial investigation determines that the system has been

compromise than a full investigation is necessary to determine the extend of the intrusion.

Intrusion detection can be categorized into three types of methods:

- **Passive Intrusion Detection** – Intrusion detection occurs due to noticeably abnormal system behavior that is cause by the intruder directly or indirectly.
- **Active Intrusion Dectection** – An intrusion is detected examining Performance Logs, Audit Logs, Event Viewer, File Logs, and Network Logs.
- **ProActive Intrusion Detection** – An intrusion is detected by the information that Intrusion Detection Software and other detections methods that is not part of the Operating system. For example; Port scanners, Software Scanners, Internet Scanners, and Third party Monitoring/Auditing software.

Passive Intrusion Detection

In this method, the system can or may display abnormal circumstances that seem unusual or irregular. Warning signals could include such things as unexplainable system activity that you did not perform, data that appears to be of questionable accuracy, and unexpected or incorrect processing results or anything of a questionable nature.

The difficulties of this method are that the system user must be able to recognize the abnormal behavior of the system. Once the abnormal behavior is detected the system administrator or user must then categorized as to the type of intrusion that has taken place. The system administrator/user must also determine what part of the system data or operating system are operating abnormally, to include the number of systems effected by this intrusion. The Passive Intrusion Detection is listed this document.

Active Intrusion Detection

Active Intrusion detection can be divided into six major categories;

- **Investigating Users Accounts** – Examining user account information with User Manager within Administrative Tools.
- **Monitoring Active Processes** – Determine and examining what processes/software is running on the system.
- **Examine System Log Files** – Examine all system log files before, during and after the Intrusion has been detected.
- **Network Traffic and Configuration** – Detecting/Monitoring suspicious activity on the network and any changes in network configuration.
- **Examine Services** – Verify that all services running within the O/S are valid.
- **Locate Intruder Modification** – Located changes made to files, disk, or software.

Because all six types of active intrusion detection involves using the Windows NT Commands, the information they yield can be altered by Trojans, see Hiding The Intrusion. Unless the integrity of the commands is verified, the information reported is suspected.

An intruder can also modify data files that many commands depend on to give information " *.dll files". Modification of data files is a very effective method for hiding an intruder's tracks in a system. Information that such commands give can be false, even if the command itself has not been altered or replaced. When using command the are dependent on log files, remember that the intruder may also modify the information in the

log files.

The information revealed by each type of active intrusion detection is not unique. To increase the probability of the information being accurate, use all six type of active intrusion to cross-verify the information. They should give different prospective to the same scenario. If there are some inconsistencies, that may indicate an attempt to hide the intrusion.

Investigating User Accounts

Investigating the User Accounts is the most direct way to get a list of suspects who could have penetrated your system. Windows NT doesn't give much information by user. There are no user history files, so examining System Log files and Audit files should be performed as well. The Investigating User Accounts in Appendix B shows various method to perform this type of Active Intrusion.

Monitoring Active Processes

By monitoring active processes, you can determine what types of processes are running on your system. This information may give a *clue* about any unauthorized program that are running (such as IRC, ICQ, Scanners, and Sniffers). Unauthorized programs poses a danger, since they could be Trojans that employees downloaded from the Internet or receive via e-mail attachment. The Monitoring Active Processes section in **this document** list various methods to perform this type of Intrusion detection.

Examining System Logs

System/Auditing Logs record various activities in the system. Log files are often the only record of suspicious behavior. Failure to enable the necessary mechanisms to record this information and use it to initiate alert mechanisms will greatly weaken and possibly even eliminate your ability to determine whether or not an intrusion has been attempted and has indeed succeeded. This also applies to having the necessary procedures and tools in place to process and analyze your log files. The Examining System Logs section in **this document** lists various methods to perform Intrusion detection. Look for activities involving a user that are unusual for that user.

You may need your logs to:

- Alert you that an intrusion is occurring
- Help recover your systems
- Conduct an investigation
- Give testimony
- File insurance claims

Network and Configuration

Examining the network will give information about the connection made to your systems and any connections taking place and who is connected to the network. This method is use for detecting many remote exploits such as, SYN Attacks, ICMP Floods, UDP Floods, Null Session Connection, Suspicious Port Connections, and suspicious IP addresses. The Network Traffic and Configuration in **this document** list various methods to perform this type of detection.

Examining Services

This method is use to determined if the intruder has place addition services on you system. Creation of additional services on your system may impact the performance and integrity of your system and other systems that may be connected to you via the network. Keep a listing of services running on your machine to verify if in fact an intruder has place a malicious service on you machine. The Examining Services in **this document** list various methods to perform this type of detection.

Locating Intruder Modifications

This method is the most extensive active detection method. It involves looking at the entire content of a system. A system typically contains massive amounts of files of many types, thus trying to find changes made by the intruder would be difficult but not impossible. A simpler way to go about finding changes is to first find the files that changed during the suspected time period and then examine the exact changes in those files.

Searching

Searching involves finding the files that have been changed directly or indirectly by the intruder. Looking only at files that have changed narrows the search. The Searching for Intruder Modification section in **this document** show various methods to find such files.

Comparisons

Another method is comparing files structure and size with an existing Backup File structure. This method can only be performed if you have a properly backup system.

Sorting

Sorting involves finding the changes made in the changed files, this includes looking for suspicious strings that might be compromising commands or words that should not exist in the system “such as You Suck”. The Sorting for Intruder Modification section in **this document** list various methods to perform this type of detection.

Proactive Intrusion Detection

Proactive Intrusion Detection involves installing and using specialized software on the system to monitor intrusion detection. There is a variety of IDS (Intrusion Detection Software) within the IT industry. For this guides purpose we will cover two notable IDS for detecting remote attacks.

Wrappers

Wrappers are small programs that protect a system's services from an attack. Especially, TCP/IP services are protected from Denial Of Service Attack, due to a wrapper's relatively small execution time. A service that is protected by a wrapper is said to be wrapped. When such services are requested, the wrapper checks the request and logs any important information, and then it gives the request to the service. Since services correspond to ports that appear to the network, and request indicates the service they want by a port, wrappers are configured by ports.

If an attack is made against a system with wrappers, the wrappers' logs can examined to determine what ports were used in the attack, how long the attack lasted, and from where the attack came.

Network Traffic Monitor (Sniffer)

Network Traffic Monitors are computer systems that are dedicated to being legitimate packet sniffers. All network traffic is monitored and can be logged. More sophisticated monitors can look for connections to uncommonly used ports, failed connection, and suspicious pattern of connection.

If an attack occurs against a system in the network that contains a Sniffer, the sniffer logs can be check for connections to the attack.

Intruders often begin attack by running a port scanner against the target machine. Port scanners try to connect to ports that are used by common services (such as Telnet, FTP, HTTP, SMTP, NetBios etc..). Network Monitors should be configured to detect scans to multiple ports on the same system and for scan to the same port on multiple systems. See the "Hacker Tools" section in **this document** for a list of commonly used hacker tools.

Ports used by hacker tools should be monitored as well as ports used by the following services.

- FTP
- IRC
- HTTP
- SMTP
- LINK
- LOGIN
- NETBIOS
- KRCMD
- RSH
- TFTP

- TELNET

Determine the Penetration Technique

Upon discovery of a valid intrusion, it is important to determine how the intruder gain unauthorized access to the system. Unauthorized access to a system can be obtained using the following methods;

- **Account Compromise**
- **Exploits**
- **Hacker Tools**
- **System Crashes and Denial of Services**

Account Compromise

Compromise of user accounts can be achieved by using various utilities, such as, Packet sniffing, password file cracking, and surfing. Unlike exploits, these methods will allow an intruder to logon as the normal users instead of having to exploit some other methods of security vulnerability. Account compromise can fall into several categories;

- Brute Force
- Snooping
- Social Engineering

Brute Force

Passwords are computed using 2 different methods. The first, a dictionary lookup, called dictionary cracking, uses a user supplied dictionary file. The password hashes for all of the words in the dictionary file are computed and compared against all of the password hashes for the users. When there is a match the password is known. This method is extremely fast. Thousands of users can be checked with a 100,000-word dictionary file in just a few minutes on a PPro 200. The drawback to this method is that only finds very simple password.

The second method is the brute force computation. This method uses a particular character set such as A-Z or A-Z plus 0-9 and computes the hash for every possible password made up of those characters. This method will always compute the password if it is made up of the character set you have selected to test. The only downside to this method is time. It is a very computation intensive and the larger the character set the longer it takes. The character set A-Z takes about 24 hours on a Ppro 200. A-Z and 0-9 takes about 10 days.

The Brute Force section in **this document** lists various brute force methods.

Really weak passwords

Most people use the names of themselves, their children, spouse/SO, pet, or car model as their password. Then there are the users who choose "password" or simply nothing. This gives a list of less than 30 possibilities that intruders can type in for themselves.

Dictionary attacks

Failing the above attack, the intruder can next try a "dictionary attack". In this attack, the intruder will use a program that will try every possible word in the dictionary. Dictionary attacks can be done either by repeatedly logging into systems, or by collecting encrypted passwords and attempting to find a match by similarly encrypting all the passwords in the dictionary. Intruders usually have a copy of the English dictionary as well as foreign language dictionaries for this purpose. They all use additional dictionary-like databases, such as names and lists of common passwords.

Snooping

Snooping involves finding information to gain a level of access on a system without manipulating a system. This can be done via the network or the conventional non-technical snooping.

Hole creation

Virtually all programs can be configured to run in a non-secure mode. Sometimes administrators will inadvertently open a hole on a machine. Most administration guides will suggest that administrators turn off everything that doesn't absolutely positively need to run on a machine in order to avoid accidental holes. Note that security-auditing packages can usually find these holes and notify the administrator.

Buffer overflows

Almost all the security holes you read about in the press are due to this problem. A typical example is a programmer who sets aside 256 characters to hold a login username. Surely, the programmer thinks, nobody will ever have a name longer than that. But a hacker thinks, what happens if I enter in a false username longer than that? Where do the additional characters go? If they hackers do the job just right, they can send 300 characters, including code that will be executed by the server, and voila, they've broken in. Hackers find these bugs in several ways. First of all, the source code for a lot of services is available on the net. Hackers routinely look through this code searching for programs that have buffer overflow problems. Secondly, hackers may look at the programs themselves to see if such a problem exists, though reading assembly output is really difficult. Thirdly, hackers will examine every place the program has input and try to overflow it with random data. If the program crashes, there is a good chance that carefully constructed input will allow the hacker to break in. Note that this problem is common in programs written in C/C++, but rare in programs written in Java.

Physical Intrusion

If an intruder has physical access to a machine (i.e. they can use the keyboard or take apart the system), they will be able to get in. Techniques range from special privileges the console has, to the ability to physically take apart the system and remove the disk drive (and read/write it on another machine). Even BIOS protection is easy to bypass: virtually all BIOSes have backdoor passwords.

Network

A hacker can use various methods to achieve the required results to obtain information about your system. The most common method is the use of scanning utilities. A scanner can obtain network configuration information (IP address, routing table, etc…) that can be useful for many exploits. This type of snooping is why network packet encryption and network proxying are important. The Snooping via network section in **this document** list various methods to gain information from the network.

Non-technical

This technique deals more with the physical aspect of snooping. There are a variety of ways an intruder can gather information to compromise your system, such as, Dumpster snooping, which involves searching trash can for information that a users discards without the thought that this could be valuable information. An intruder can also walk into your area and gather information required to gain access to your system. This type of snooping is why Paper Shredders, doors and Drawer locks, and displaying passwords as series of "*" are important.

Social Engineering

Social Engineering is the only method that involves the intruder making human contact with the users; thus, social engineering is difficult to recognize as a cracking method. The intruder tries to gather information from the user that will help them gain access to one or more systems. Common methods of Social Engineering includes tricking the user into:

- Revealing a username and password
- Downloading and executing a Trojan Horse program
- Executing a command on the system
- Allowing the intruder physical access to a system
- Revealing any information about a system; Firewall software, IP Addresses, O/S version, etc…

Exploits

This document will define the types of exploits that a Windows NT system. The word Exploits is defined as, security vulnerabilities to gain access and/or privileges to a computer system and its files. System software and hardware invariably have security vulnerabilities due to their complexity. The Microsoft Windows NT Operating System (OS) provides several security features. However, the default COTS configuration is relaxed, especially on the NTW product. Because of the higher availability of NTW to an average home user, using the product in a static/isolated environment, the default configuration has few of the security features enabled. NTS, a higher-end product intended for corporate use, has many features enabled, but not all.

Remote

A Remote exploit occurs when an intruder exploits a system that is connected to a network. This method involves snooping for network addresses, Denial of Service attacks, IP Spoofing attacks, SYN Attacks, or attacking other computers with which the remote system has a trust relationship. The Remote Exploits section in **this document** list these exploits.

Local

A Local Exploit occurs when an intruder exploits a system on which they are physically using the console. This often involves physically altering the system, the system control files, using alternative boot media. The Local Exploits section in **this document** list these exploits.

Administrator

Administrative exploits are exploits that the intruder utilizes specifically to gain administrative privileges. Usually, such exploits make the intruder a member of the administrative group, which allows easy access to the system files and processes. Administrative exploits can be implemented physically on the system or from access via the network.

Hacker Tools

This document will concentrate on tools that hackers use to install and execute programs within your system. Viruses, Trojans, and worms are also types of hacker tools, but will not be discussing because these tools must be install physically or executed by a users from either an e-mail attachment.

Hacker Tools are use to scan for vulnerabilities in systems, get information about the system, and exploit existing vulnerabilities. Many hacker tools are Free Software that is used in Proactive Intrusion Detection.

System Crashes and Denial of Service

A denial of service attack is a malicious attack against a computer system. Most denial of service attacks are attacks that cause a computer to work very hard so that it cannot perform any of its normal tasks. The intent with a denial of service attack is either to harass or to actually destroy data.

Many denial of service attacks just take advantage of existing services and thus the only defense against many attacks is to simply turn the service off. Some exploits, however, take advantage of bugs in a program and for some attacks there are patches and fixes available for downloading:

Intruders often use such exploits as means to gain access or to impersonate a user or system. The System Crashes and Denial of Service section in Appendix B list these exploits.

System Security Problems

System security vulnerabilities that exist are cause by improper installation/configuration of the operating system and its application software. Examining the software configuration will give clues to what security vulnerabilities exist in the system and which one the intruder may have exploited. The System Security Problems section list various methods to configure and secure your system.

Determine the Extend of Penetration

Upon determination that the intruder has gain-unauthorized access to the system, the level of penetration/access that was gained must be determine. Sometimes, the method that was used to gain penetration indicates the level of access that was gained. For example if the intruder was able to gain administrative rights this should indicate the level of penetration the intruder will have and the damage to the system that intruder can perform.

In Windows NT, there is only distinct level of access; it is called “administrator”. The majority of access rights or privileges can be given to any user or group of users. Windows NT has built-in user accounts and groups, but their access rights are adjustable and more accounts can be added. The number of actual access levels depends on how Windows NT and the network are configured.

There is no single way to determine the level of access gained by the intruder. Security vulnerabilities can allow intruders more access than the user account they used allows.

Administrator

Use separate accounts for administrative activity and general user activity. Individuals who do administrative work on the computer should each have two user accounts on the system: one for administrative tasks, and one for general activity. To avoid accidental changes to protected resources; the account with the least privilege that can do the task at hand should be used. For example, viruses can do much more damage if activated from an account with administrator privileges.
It is a good idea to rename the built-in Administrator account to something less obvious. This powerful account is the one account that can never be locked out due to repeated failed log on attempts, and consequently is attractive to hackers who try to break in by repeatedly guessing passwords. By renaming the account, you force hackers to guess the

account name as well as the password.

If, on a system, accounts exist that the legitimate administrator did not create, indicates that the intruder definitely has administrative rights.

Users other than Administrator

Users that are not administrator can have all the rights and access of an administrator (based on how the administrator configured that particular account) except the rights to change account information, access rights, and creation of additional users. It is important to note that members of the administrator group have the same privileges that of the administrator has.

Determine Intruders signature and any attempts to conceal its signature

There are two words to describe the intruder: **hacker** and **cracker**. A hacker is a generic term for a person who likes getting into things. The benign hacker is the person who likes to get into his/her own computer and understand how it works. The malicious hacker is the person who likes getting into other people's systems. The benign hackers wish that the media would stop bad-mouthing all hackers and use the term 'cracker' instead. Unfortunately, this is not likely to happen. In any event, the word used is 'intruder', to generically denote anybody trying to get into your systems.

Intruders can be classified into two categories.

Outsiders

Intruders from outside your network, and who may attack you external presence (deface web servers, forward Spam through e-mail servers, etc.). They may also attempt to go around the firewall to attack machines on the internal network. Outside intruders may come from the **Internet**, **dial-up** lines, **physical break-ins**, or from **partner** (vendor, customer, reseller, etc.) network that is linked to your corporate network.

Insiders

Intruders that legitimately use your internal network. These include users who **misuse privileges** (such as the Social Security employee who marked someone as being dead because they didn't like that person) or who **impersonate** higher privileged users (such as using someone else's terminal). A frequently quoted statistic is that insiders commit 80% of security breaches.
There are several types of intruders **Joy riders** hack because they can. **Vandals** are intent on causing destruction or marking up your web pages. **Profiteers** are intent on profiting from their enterprise, such as rigging the system to give them money or by stealing corporate data and selling it.

Intruders will attempt to conceal their presence. They often use the same technique and tools for hiding their presence with the tools used for gaining access. The following listed below are some of the most commonly used techniques for concealing their presence.

Trojan Files

- An unauthorized program contained within a legitimate program. This unauthorized program performs functions unknown by the user.
- A legitimate program that has been altered by the placement of unauthorized code within it; this code performs functions unknown by the user.

- Any program that appears to perform a desirable and necessary function but that (because of unauthorized code within it that is unknown to the user) performs functions unknown to the user.

Trojans files can appear almost anywhere, on any operating system or platform. They can be distributed if many forms or fashion; software downloads, e-mail attachments, file attachments, and may also be placed by an intruders that has gained access to your system.

Trojan files can replace critical system files such as *.dll's .exe's or any other files that a user may execute during a normal operating environment.
Trojan files are transparent to the users and are often difficult to detect, but using precautionary measures and techniques may allow you to detect the installation and concealment of Trojans. An example of this technique is to compare previous backup files with the current file structure to determine if in fact the files have been altered. They are also various software vendors that can provide tools to just this sort of comparison, such as, Tripwire.

Back Doors

Back doors are security vulnerabilities that allow intruders to access your system. Back Doors can be installed in a form of a Trojan, it allows intruders access to your system, network information, and files access. Some Trojans open new vulnerabilities to allow access to your system in the future, even if the original methods was discovered and fixed. Since these Trojans allow a different access point logging in with a specific user name is not required.

Intrusion outside your system

If an intruder has gained access to your system it is then possible for the intruder to access other systems within your network, based on your topology (Trusted Domains). This type of access can and will allow the intruders to place Trojans, sniffers, scanners, and other utilities to gather information or to have back door access at a later time. Implementation of a strong security policy can deter access to other system upon intrusion of your system (strong password generation, user specific shared resources that are pass worded). **This document** contains a list of tools and Trojans used by intruders.

Modification or Destroying Of Logs Files

As a precautionary measure, an intruder may try to remove evidence of the intrusion by either modifying or deleting your system log files. So with this in mind, you must ensure that privileges to all your log files are as independent of each other. You can use the registry to further secure you logs files within Windows NT. **this document** lists exploits the can modify log files.

Use NTFS instead of FAT. NTFS allows permissions to be set on a per-file/per-directory basis. NTFS also allows auditing on a per-file/per-directory basis. Note that many people recommend using FAT as the boot drive and NTFS for all other drives (due to the ease-of-use in using DOS to fix things on a FAT drive). However, using NTFS for all drives is definitely more secure.

Evaluate the findings and determine best course to resolve and prevent further penetration.

Digital information retrieval systems are wonderful things. With hardly any effort at all, it is possible to extract specific data from an archive, manipulate it to solve a problem, and commit the changes back in to the archive, all from the same terminal. It is this ability to manipulate data that makes proving a computer attack so difficult.

Proper logging is therefore a procedural issue; there must be clear policy (preferably in written form) describing what is 'interesting' and should be recorded, and why.

There is not a single method to determine the level of access the intruder has achieved. If it is determine that the intruder could have gained administrative access, then a reinstallation of the software should be performed.

To ensure that nothing was missed throughout the investigation the following items should be answered;

- Determine and record the length of time spent on the system by the intruder
- Determine and record the services/ports the intruder use to gain access
- Determine and record the methods used by the intruder to gain access
- Determine and record if the intruder gained administrative access
- Determine and record if the system has any known security vulnerabilities
- Determine and record any attempt by the intruder to hide its signature
- Determine and record if files and data have been modified
- Determine and record if the intruder gained access to other systems via the attacked system

This document is design to give the users/administrators a basis for discovering and preventing intrusion from inside/outside intrusion. The information contain within this document will be updated when other methods of intrusion are discovered.

Passive Intrusion Detection

Symptom: The system is unresponsive to commands and displays the blue crash screen

Explanation: When Windows NT encounters a problem that it cannot or will not recover from without a system restart or cold boot. When a Windows NT system crashes, it produces a screen of information that strikes fear into the hearts of any system administrator or user--the infamous blue screen, also known as "The Blue Screen Of Death" (BSOD).

While a blue screen and the seemingly garbled text that accompanies it is rather intimidating, it also is a very effective troubleshooting tool created to help determine what caused the crash. It is a snapshot of memory at the time the crash occurred, with some insights as to the possible cause.

Since a blue screen cannot tell the complete tale of a crash, a file called MEMORY.DMP also is created. It is, as its name implies, a dump of the entire contents of memory when the crash occurred, giving much more useful information as to what happened.

Possible Causes: An intruder had the Kernel operate an instruction that the system cannot execute, either due to machine instruction set limitations or kernel operation limitation.

Evidence: The Blue Screen Of Death lists a program or process that was the offending process when it crashed. If a BSOD appears, it may be due to a Denial of Service (DoS) attack, such as the PING OF DEATH against the TCP/IP stack. The following listed below are some example of the BSOD;

Error: STOP 0xc0000218...UNKNOWN_HARD_ERROR
Error: STOP 0x0000000A (in Ntoskrnl.exe at logon to NT 4.0)

If an executable file with a specially-malformed image header is executed, it will cause a system failure and you may receive the following STOP error message on a blue screen:

```
STOP 0x0000000A IRQ_not_less_or_equal

or

STOP 0x00000050 PAGE_FAULT_IN_NON_PAGED_AREA
```

Symptom: Windows NT displays an error message upon system startup**.**

Explanation: Windows NT displays the following error message upon startup; *"At least one of your services/drivers failed at system startup"* Use the Event Viewer to examine the event logs for detail, typically these failure will be logged in the System Event Log in Event Viewer. Please refer to Appendix B "Examining System Log" for details on viewing these log files.

Possible Causes

- The hacker make system alterations, such as modifying Registry settings, replacing or modifying ***.dll** files that are required and dependent within Windows NT, and modifying or replacing system drivers with Trojan files.

- The hacker added services to your system, such as, Sniffer, Scanner, and monitoring devices to gather information about you system/network.
- The Hacker may have disable certain services required by Windows NT to operate correctly, such as RAS, NetBIOS, Workstation.

Evidence

- Services/devices have been added or altered or incorrectly configured.
- Additional devices installed on you system, System hardware configuration has been modified.

Symptom: Your system disk storage capacity has dramatically decreased in size to the point that the disk is dangerously low on free space.

Explanation: Windows NT will display a message informing you that you disk storage capacity is at a critical low state. Use the Windows Event Viewer to view details about your system drive condition. Please refer to the Examining System Log in the Appendix of this document.

Possible Causes:

- A Trojan was installed on your system that creates bogus files to fill up your disk space.
- A Trojan process is running in the background causing your system to create large log files.
- The intruder is using your system to store files for later use, such as, Network Sniffer trace data, Port Scanning Data and Network/system configuration data.

Evidence:

- Evidences of unknown directories and files installed within you drive structure
- Large portion of data are owned by an unknown user
- Log files exist on the system that should not.
- Windows NT alerts you of a low drive space condition.
- Identify any missing files or directories.
- Identify any new files and directories
- Investigate any unexpected changes among those you have identified.

Symptom: The system is running sluggishly for an unknown reason.

Explanation: Programs executing on your networked systems typically include a variety of operating system and network services, user-initiated programs, and special-purpose applications such as database servers. Every program executing on a system is represented by one or more processes. Each process executes in an environment with specific privileges that govern what system resources, programs, and data files it can access, and what it is permitted to do with them.

The execution behavior of a process is represented by the operations it performs while running, the manner in which those operations execute, and the system resources it uses

while executing. Operations include computations, transactions with files, devices, and other processes, and communications with processes on other systems via your network.

The goal is to verify that the processes executing on your systems are attributed only to authorized activities of users, administrators, and system functions, and are operating only as would be expected.

A process that exhibits unexpected behavior may indicate that an intrusion into a system has occurred. Intruders may have disrupted the execution of a program or service, causing it to fail, or to operate in a way other than the user or administrator intended. For example, if intruders were to successfully disrupt the execution of access-control processes running on a firewall system, they may be able to gain access to your organization's internal network in ways that would normally be blocked by the firewall. Unexpected processes may also indicate that an intruder is using the system covertly for unauthorized purposes, including attempts to attack other systems within and external to your network, or running network sniffer programs.

Possible Causes

- The hacker is running software that consumes a large amount of processing time.
- The hacker has inserted a Trojan, such as CPU HOG, BackOrifice.
- The Hacker is accessing your system through the use of Trojan programs, such as, NetBus.

Evidence

- missing processes
- extra processes
- unusual process behavior or resource utilization
- processes that have unusual user identification associated with them
- unexpected volume or types of resource usage on a system
- attempts to log into systems with privileged (e.g., administrator) access
- attempts to access sensitive system data files or restricted resources
- unexpected volume and types of network traffic
- network interfaces operating in promiscuous mode
- other unexpected changes to hardware configuration settings

Active Intrusion Detection

Investigating User Accounts Information

Methods: User Manager (Local Machine) User Manager for Domains (Domain Machine)

Description: A Windows NT Workstation tool used to manage the security for a workstation. Administers user accounts, groups, and security policies.

A Windows NT Domain tool used to manage security for the domain.

Usage: *Start/ Programs/ Administrative Tools/ User Manager*

Evidence:

- Check for user accounts or groups that should not exist.
- Ensure that all disable accounts are **Disabled.**
- Ensure that users or group accounts have not changed.

Method: Windows NT Explorer (Used to verify Directory/File permissions)

Description: Windows NT Explorer may be use to verify Directory and file permission for specific users/groups and the amount of access rights they have.

Usage: *Start/ Programs/ Windows NT Explorer.* Highlight/select the directory/file that you would verify for changes; *Highlight the directory or file that you want to check, right click mouse/ Properties/ Security tab/ permission button/ username* shows access rights to this directory or file.

Evidence:

- Rights have changed for a user on a specific file or directory
- A unknown user exist for the file or directory
- A user was given additional rights to a file or directory

Method: Windows NT Explorer (used view directory/file auditing)

Description: Directory/File Auditing have been modified from its original configuration.

Usage: *Start/ Programs/ Windows NT Explorer.* Highlight/select the directory/file that you would verify for changes; *Highlight the directory or file that you want to check, right click mouse/ Properties/ Security tab/ Audit button/* Shows what auditing features are selected and who will receive the alerts.

Evidence:

- The Security Event logs shows that the auditing of directories/files have been modified from its original settings
- A user was removed from the auditing feature to receive alerts.
- Audit logs no longer show accesses to directories/files that are being monitored.

Monitoring Active Processes

Method: Task Manager, Performance Monitor (Application)

Description: Task Manager – Displays status or processes, applications, and Memory usage.

Performance Monitor – Displays real time logging of system events ie; Processes, disks usages, memory usage and application running. Can also be use to monitored multiple functions and log events selected for these functions.

Usage: <CTRL><ALT><DEL> Task Manager.
Start/ Programs/ Administrative Tools/ Start/ Programs/ Administrative Tools/ Performance Monitor.

Evidence:

- Unknown programs running
- Unknown process running consuming large amount of CPU time
- Unknown file or command executable
- Process/executable that should be running is pause/stop.
- missing processes
- extra processes
- unusual process behavior or resource utilization
- processes that have unusual user identification associated with them

Method: Net (Command)

Description: Many Windows NT networking commands begin with the word net. The Net command has various option associated with the command, we will cover only those command associated with the Active Intrusion Detection.

Usage: *Start/ Run/ Command.exe/ "net Options"*

- **Net Files** - Displays the names of all open shared files on a server and the number of file lock, if any, on each file. This command also closes individual shared files and removes file locks. **net file [id [/close]**
- **Net Config Workstation -** Displays or changes settings for the Workstation service while the service is running. Type **net config workstation** to display the current configuration for the local computer.
- **Net User -** Adds or modifies user accounts or displays user-account information. Type **net user** without parameters to view a list of the user accounts on the computer.

Evidence:

- Suspicious or unknown shared files (net file)
- System configuration has changed from it original state. (net config workstation)
- Unknown users logged on to the system. (Net users)

Method: *SET*

Description: Displays system's environment variables.

Usage: *Start/ Run/ Command.exe/ "set"*

Evidence:

- Suspicious or unknown environment variable name
- Suspicious or unknown environment variable setting.

Method: Devices

Description: Lists all available devices. This option will allow you to view and/or stop/start various Windows NT Devices.

Usage: *Start/ Settings/ Control Panel/ Devices*

Evidence:

- Unknown device driver running
- Device Driver(s) stop when it should be running
- Device driver(s) startup configuration has been altered

Method: Services

Description: Displays current services running within Windows NT environment. Default services are installed during installation and additional services can be added. It is recommended that a list of services running on your system be recorded.

Usage: *Start/ Settings/ Control Panel/ Services*

Evidence:

- Unknown services running.
- Known Services stopped or paused.
- Services startup configuration has been altered.

Examining System Logs

Method: System Logs

Description: The System log records events logged by the Windows NT system components. For example, the failure of a driver or other system component to load during startup is recorded in the System log.

Usage: *Start/ Programs/ Administrative Tools/ Event Viewer/ Logs/ System*

Evidence:

- Inappropriate Driver errors, a failure to load a needed system driver
- Unknown driver loaded within your system

Method: Security Logs

Description: The Security log records security events. These helps track changes to the security system and identify any possible breaches to security. For example, attempts to log on the system may be recorded in the Security log, depending on the Audit settings in User Manager. You can view the Security log only if you are an Administrator for a computer.

Usage: *Start/ Programs/ Administrative Tools/ Event Viewer/ Logs/ Security*

Evidence:

- Failed log on attempts
- Unusual Logons time. User logon after normal operating hours.
- Unknown logon user name
- Unknown authentication process name.
- Security events that have discrepancies with the logs of servers to which the system has access.
- Suspicious changes to registry keys. Auditing of registry keys must be set.

Method: Application Logs

Description: The Application log records events logged by applications. For example, a database application might record a file error in the Application log.

Usage: *Start/ Programs/ Administrative Tools/ Event Viewer/ Logs/ Application*

Evidence:

- Suspicious or Unknown Application error.
- Suspicious or Unknown Application event.
- Multiple application errors or events for a particular application.

Network Traffic and Configuration

Method: Netstat

command is available only if the TCP/IP protocol has been installed.

Usage: *Start/ Programs/ Command Prompt/ Netstat –options*

- **-a** Displays all connections and listening ports; server connections are normally not shown.
- **-e** Displays Ethernet statistics. This may be combined with the -s option.
- **-n** Displays addresses and port numbers in numerical form (rather than attempting name look-ups).
- **-s** Displays per-protocol statistics. By default, statistics are shown for TCP, UDP, ICMP, and IP; the -p option may be used to specify a subset of the default.
- **-p** protocol Shows connections for the protocol specified by proto; proto may be tcp or udp. If used with the -s option to display per-protocol statistics, proto may be tcp, udp, icmp, or ip.
- **-r** Displays the contents of the routing table.

Evidence:

- An unknown FQDN is shown that does not correspond to any legitimate FQDN that you know.
- An unknown session is established to Ports 135, 136, 137, 138, or 139.
- You have multiple open SYS_RECEIVED state waiting for a connection.
- You see multiple failed connection attempt on your TCP statistics.
- You have an unknown IP Address or FQDN in the routing table.
- You have an unknown connection to ports that not legitimate for use within your system.
- You have an enormous amount of ICMP packets received to your system.

Method: nbtstat

Description: This diagnostic command displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP). This command is available only if the TCP/IP protocol has been installed.

Usage: *Start/ Run/ Command.exe/ "nbtstat Options"*

- **-a remotename**
  Lists the remote computer's name table using its name.
- **-A IP address**
  Lists the remote computer's name table using its IP address.
- **-c**
  Lists the contents of the NetBIOS name cache giving the IP address of each name.
- **-n**
  Lists local NetBIOS names. Registered indicates that the name is registered by broadcast (Bnode) or WINS (other node types).
- **-R**
  Reloads the LMHOSTS file after purging all names from the NetBIOS name cache.
- **-r**
  Lists name resolution statistics for Windows networking name resolution. On a Windows NT computer configured to use WINS, this option returns the number of

names resolved and registered via broadcast or via WINS.

- **-S**
  Displays both client and server sessions, listing the remote computers by IP address only.
- **-s**
  Displays both client and server sessions. It attempts to convert the remote computer IP address to a name using the HOSTS file.

Evidence:

- An unknown NetBIOS connection is display in the NetBIOS Connection table.
- A foreign IP Address shows a NetBios Connection.
- Shows multiple Unknown Inbound NetBIOS connection.

Method: Windows NT Diagnostics (Network)

Description: Shows configuration and activity statistics of the system's network connection. This program has the significant advantage of being functional for whatever network type to which the system is connected.

Usage: *Start/ Programs/ Administrative Tools/ Windows NT Diagnostics/* Network Tab

Evidence:

- Unusually high activity statistics.
- Suspicious change (s) in the network configuration.

Locating Intruder Modifications

Method: Find all Directory/file within the last xx days

Description: Locate and display all files that have been modified in the last xx days.

Usage: *Start/ Find/ Files or Folders/ name & location, Date Modified or modified: during the previous x days,/ Find now.*

Evidence:

- Unusual file modification times.
- Unusual files size.
- Unauthorized modification of system/registry files.

Method: Install/Uninstalled Program

Description: Displays a listing of programs installed on your system. You can also uninstall any program you desire using this function.

Usage: *Start/ Settings/ Control Panel/ Add/Remove Programs/* install/uninstall tab.

Evidence:

- Suspicious, unusual, or unauthorized software/programs installed on your computer.

Method: Locate all files containing specific string syntax.

Description: Locate and display all files containing specific string syntax.

Usage: To find files and folders

1. Click the **Start** button, point to **Find**, and then click **Files or Folders**.
2. In the **Named** box, type all or part of the file's name.

   If you do not know the name of a file or you want to refine the search, click the **Date** or **Advanced** tab.

   If you want to specify the location from which to start the search, click one in the **Look in** list, or click **Browse**.
3. Click **Find Now**.

Evidence:

- Locates and displays suspicious files text/size in KB. The intruder may have replaced a known file with a Trojan.

Method: fc (File Compare)

Description: Compares two files and displays the differences between them.

Usage: *Start/ Programs/ Command Prompt/ fc [/a] [/b] [/c] [/l] [/lbn] [/n] [/t] [/u] [/w] [/nnnn] [drive1:][path1]filename1 [drive2:][path2]filename2*

- **/b**
  Compares the files in binary mode. Fc compares the two files byte by byte and does not attempt to resynchronize the files after finding a mismatch. This is the default mode for comparing files that have extensions of .EXE, .COM, .SYS, .OBJ, .LIB, or .BIN.
- **/l**
  Compares the files in ASCII mode. Fc compares the two files line by line and attempts to resynchronize the files after finding a mismatch. This is the default mode for comparing files that do not have extensions of .EXE, .COM, .SYS, .OBJ, .LIB, or .BIN.
- **/u**
  Compares files as Unicode text files.

Evidence:

- Files that have been changed either in size or content. Most importantly verify that these are not important system files.

Method: Registry Editor (regedit)

Description: REGEDIT.EXE is the registration editor for 16-bit Windows, which is used to modify the Windows registration database. The database is located in the Windows

directory as REG.DAT. The database contains information about 16- bit applications, and is used by File Manager for opening and printing files. It is also used by applications that support Object Linking and Embedding (OLE). REG.DAT is used and maintained by Windows on Windows (WOW) and 16-bit Windows applications. The WOW layer resides on top of the Virtual DOS Machine (VDM).

REGEDIT.EXE is a 16-bit application that is included in Windows NT for compatibility with previous 16-bit applications. Regedit provides a method for examining REG.DAT under Windows NT. You can migrate the REG.DAT database file to the Windows NT registry during the first logon to an initial installation of Windows NT.

Usage: *Start/ Run/ Regedit*

Evidence:

- Unknown registry key/value name.
- Unknown registry data content.

Method: Registry Editor (regedt32)

Description: REGEDT32.EXE is the configuration editor for Windows NT, which is used to modify the Windows NT configuration database, also known as the Windows NT Registry. This editor allows you to view or modify the Windows NT Registry. The editor provides views of windows that represent sections of the registry, called hives. Each window displays two sections. On the left side, there are folders that represent registry keys. On the right side, there are the values associated with the selected registry key. Regedt32 is a powerful tool, which you must use with extreme caution when changing registry values. Missing or incorrect values in the registry can render the Windows NT installation unusable.

Usage: *Start/ Run/ Regedt32*

Evidence:

- Registry key value permission has changed from their original configuration.
- Unknown registry key/value
- Unknown account added within the registry

Proactive Intrusion Detection

Vulnerabilities

Brute Force

Exploit: Password Guessing/Cracking

Description: The term *password cracker* can be misinterpreted, so I want to define it here. A password cracker is any program that can decrypt passwords or otherwise disable password protection. A password cracker need not decrypt anything. In fact, most of them

don't. Real encrypted passwords, as you will shortly learn, cannot be reverse-decrypted.

A more precise way to explain this is as follows: encrypted passwords cannot be decrypted. Most modern, technical encryption processes are now one-way (that is, there is no process to be executed in reverse that will reveal the password in plain text).

Passwords are computed using 2 different methods. The first, a dictionary lookup, called dictionary cracking, uses a user supplied dictionary file. The password hashes for all of the words in the dictionary file are computed and compared against all of the password hashes for the users. When there is a match the password is known. This method is extremely fast. Thousands of users can be checked with a 100,000 word dictionary file in just a few minutes on a PPro 200. The drawback to this method is that it only finds very simple passwords.

The second method is the brute force computation. This method uses a particular character set such as A-Z or A-Z plus 0-9 and computes the hash for every possible password made up of those characters. This method will always compute the password if it is made up of the character set you have selected to test. The only downside to this method is time. It is a very computation intensive and the larger the character set the longer it takes. The character set A-Z takes about 24 hours on a PPro 200. A-Z and 0-9 takes about 10 days.

Version Affected:

- Windows NT Workstation 3.5, 3.51, 4.0
- Windows NT Server 3.5, 3.51, 4.0

Evidence:

- If Successful/Unsuccessful logon attempts are audited, the security event log will show evidence of a password guessing attack on the system.
- An unknown program or process running on your system.

Exploit: Lophtcrack

Description: L0phtCrack is designed to recover passwords for Windows NT. NT does not store the actual passwords on an NT Domain Controller or Workstation. Instead it stores a cryptographic hash of the passwords. L0phtCrack can take the hashes of passwords and generate the cleartext passwords from them. Many of L0phtCracks features are designed to make these long brute force computations feasible. It takes advantage of multiprocessor machines and runs with lower than normal priority so you can use it on servers that have idle CPU. It can save and restore its state during a brute force computation so that previously computed work is not lost. L0phtCrack will automatically save its state every 5 minutes in case of power loss or reboots. The saved .LC file is in ASCII so it can be inspected over the network to check on progress.

Network sniffing requires that you be on a physical segment of the user or the resource they are accessing. The sniffer, readsmb.exe, included with L0phtCrack 2.0 will only work on Windows NT 4.0.

Version Affected:

- Windows NT Workstation 3.5, 3.51, 4.0
- Windows NT Server 3.5, 3.51, 4.0

Evidence:

- If Successful/Unsuccessful logon attempts are audited, the security event log will show evidence of a password guessing attack on the system.
- An unknown program or process running on your system.

Prevention from Brute Force Attack:

The best prevention against a brute-force attack is to require all users to have passwords that are at least four characters in length, and perhaps longer. The time required guessing a password increases geometrically with the length of the password. Where possible, set password software to require a password of a minimum length, such as eight or ten characters. Force all users with shorter passwords to select new, longer passwords.

You can take several measures to make passwords more secure and to increase the use of passwords:

- Use passwords that the computer generates. Then have each user choose a memorable password from a list of generated passwords. If, for some reason, you can't do this, use passwords generated from memorable phrases. A user who can remember *Now Is The Time For All Good Men To Come To The Aid Of Their Party,* also can remember *NITTFAGMTCTTAOTP.*
- Many users who choose guessable passwords (such as the name of their cat) do so out of fear that they will forget a tougher password. Who can blame them? Why not let the computer train the user in password entry until the user has memorized the computer-generated, unguessable password?
- Some users post passwords on bulletin boards, tape them to the PC, or write them on a slip of paper that they place in their wallets or desk drawers. Inspect user areas for evidence of posted passwords. Require that passwords never be stored in login scripts or batch files. Regularly use some program to look for the word *login* in files throughout the server, to determine whether passwords are stored in any files. Similarly, sweep user machines for the word *login* -- before an attacker does.
- Train users in the consequences of security violations.
- Make entry to the system as simple as possible for authorized users.
- Make individuals responsible for security violations that occur under their passwords.
- Convince users to not enter their passwords when someone else can observe either their hands or the screen.
- Force periodic password changes (monthly or weekly, depending on your security needs). Then if a password gets out, its period of validity limits its usefulness.
- Show users how to change their password if they think it may have been compromised.
- Use dialback modems. Such modems receive the password and the user ID and then disconnect and dial the site for which this password is authorized. This precaution prohibits unauthorized use at unauthorized sites, which is likely to be more destructive than unauthorized use at an authorized site.

Snooping

Exploit: nbtstat

Description: 'Nbtstat -a *nodename*' or 'Nbtstat -A *ipaddress*' will display much information about a remote node. This command will display:

- Active User
- Services running
- NT Domain name
- Nodename
- Ethernet Hardware address

This give a hacker doing password guessing two of the three pieces of information required to mount shares on a remote system, 'Domain name' and 'Username'.
The local and remote systems must be able to communicate via ports 137, 138, 139.

Version Affected:

- Windows NT Workstation 3.5, 3.51, 4.0
- Windows NT Server 3.5, 3.51, 4.0

Evidence:

- The use of Windows NT NetStat –a command will display any connection to these ports.
- The use of the Freeware program NukeNabber will also monitor and display the connections to these ports.

Prevention

Use a Port Monitoring Utility to monitor and gather information about your port or Null Session connection. You may also use Performance Monitor Alert Chart to configure and monitor Network and NBT connection to alert you for a specific connection.

Exploit: Sniffers

Description: Plaintext and binary information can be copied from the network. Network sniffers have allowed users to record network traffic for a long time, however their primary limitation is the vast amount of traffic that is recorded. Sniffers, which have been recovered from several hackers' toolkits, have simplistic schemes to limit the amount of recorded data either by expiring after a certain amount of time, or after a certain amount of traffic has been exchanged over individual connections.

Version Affected:

- Windows NT Workstation 3.5, 3.51, 4.0
- Windows NT Server 3.5, 3.51, 4.0

Evidence:

- An administrator suspects a sniffer has been installed and looks for large files on his

file system.
- Unusual amount of CPU usage from an unknown processes

Prevention

While malicious use of IP-Watcher and similar tools renders a great deal of the currently considered "most secure" software, and hardware vulnerable, there are steps which can be taken to prevent the malicious use of active sniffers.

- Force all incoming connections from the outside world to be fully encrypted. Attackers outside of your network will have a **much** more difficult time if passwords aren't sniffable, and sessions not hijackable.
- Force all connections to critical machines to be fully encrypted. The latest telnet package allows administrative policies like this to be enforced. Kerberos doesn't allow policies to be enforced, but will allow encrypted communications, as will SRA telnet/FTP (sometime soon) and the new STEL (which is currently in beta test) from CERT-IT.
- Force all traffic on your network to be encrypted. Again, Kerberos will help somewhat, but won't solve all problems (especially not denial of service). Newer systems such as SKIP will help a great deal, but they are in their infancy.

Unfortunately, there are no easy steps, *yet*, that can be taken to secure your network from active sniffing. Although, by simply becoming aware that this threat exists, we feel that most people are better prepared to make intelligent security decisions for their network than those who are uninformed. That is why we make this information availible; not to scare people away from the Internet, but to better prepare them for the risks. Forewarned is forearmed.

Exploit: Scanners

Description: Port scanning is a technique to check TCP/IP ports to see what services are available. For example port 80 is typically a web server, port 25 is SMTP used by Internet mail and so on. By scanning and seeing what TCP/IP ports are listening at the end of a TCP/IP address, you can get an idea as to what type of box the target might be, what services are available, and possibly plan an attack if you are aware of an exploit involving a particular service.

Version Affected:

- Windows NT Workstation 3.5, 3.51, 4.0
- Windows NT Server 3.5, 3.51, 4.0

Evidence:

- Suspicious ports are open when they should be closed.
- Logs Files indicates an unusual amount of connections logged.

Prevention

You can set your system log files to alert you of unusual amount port connection. You can also install third party intrusion detection software to alert you of any form of intrusion within your system.

Network Exploits

Preventing, Detecting, and Responding to Intrusion Detection for Windows NT

Denial Of Service Attack Exploit

Exploit: Ping Of Death

Description: A denial of service attack can be effectively launched against Windows operating systems using similar tactics to the older Ping-of-Death problem - thus we name this bug "Ping-of-Death 2".

Instead of sending a *single* 64k ICMP packet, which becomes fragmented, as done in the Ping-of-Death attack, Ping-of-Death 2 is accomplished by sending a *flurry of 64k packets*, which also become fragmented. This flurry of packets causes Windows systems to completely lock up cold without warning.

Version Affected:

- Windows NT Workstation 3.5, 3.51, 4.0
- Windows NT Server 3.5, 3.51, 4.0

Evidence:

- Unusual amount of ICMP packet being received.
- System performance will decay or stop.

Prevention

Apply all necessary Service pack. Remember, if you install a service using the Windows NT CD-Rom you must reapply the Current Service Pack. Refer to the Microsoft Site located *at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/* for the current fixes and patches for your system.

Exploit: SYN Attack

Description: Multiple TCP connection requests (SYN) are sent to the target computer with an unreachable source IP address. On receiving the connection request, the target computer allocates resources to handle and track the new connection, then responds with a "SYN-ACK" to the unreachable address. A default-configured Windows NT 3.5x or 4.0 computer will retransmit the SYN-ACK 5 times, at 3, 6, 12, 24, and 48 seconds. After the last retransmission, 96 seconds are allowed to pass before the computer gives up on receiving a response, and deallocates the resources that were set aside earlier for the connection. The total elapsed time that resources are in use is 189 seconds.

Version Affected:

- Windows NT Workstation 3.5, 3.51, 4.0
- Windows NT Server 3.5, 3.51, 4.0

Evidence:

- The System will respond with the following error message; "The connection has been reset by the remote host."
- Use the command C:/> netstat -n -p tcp . It will display multiple SYN packets.

Prevention

Apply all necessary Service pack. Remember, if you install a service using the Windows NT CD-Rom you must reapply the Current Service Pack. Refer to the Microsoft Site located *at* ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ for the current fixes and patches for your system.

Exploit: CPU Attacks (Telnet to Port XXX)

Description: Multiple service ports (53, 135, 1031) are vulnerable to 'confusion'. Which results in a target host CPU utilization of 100%, though at a lower priority than the desktop shell. Multiple services, which are confused, can result in a locked system.
When launched against port 135, NT Task manager on the target host shows RPCSS.EXE using more than usual process time. To clear this the system must be rebooted.
The above also works on port 1031 (inetinfo.exe) where IIS services must be restarted.
If a DNS server is running on the system, this attack against port 53 (dns.exe) will cause DNS to stop functioning.

Version Affected:

- Windows NT Workstation 3.5, 3.51, 4.0
- Windows NT Server 3.5, 3.51, 4.0

Evidence:

- High CPU Utilization for Process RPCSS.EXE and INETINFO.EXE
- A Telnet session to the above listed ports should not be present.

Prevention

Apply all necessary Service pack. Remember, if you install a service using the Windows NT CD-Rom you must reapply the Current Service Pack. Refer to the Microsoft Site located *at* ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ for the current fixes and patches for your system.

Exploit: Crashing NT's LSA

Description: a remote attacker can crash The Windows NT LSA. The problem pointed out in this advisory affects systems running Windows NT by crashing the Local Security Authority, rendering the target machine unusable after some period of time. The problem stems from a failure to verify the input to LsaLookupNames. It is made worse by the fact that it can be anonymously exploited. The RestrictAnonymous (1) registry key does not prevent this problem from being exploited.

The LSA is the system component responsible for authenticating users to the system, and deciding what access and privilege the users are entitled to. The same process that contains the LSA also contains the SAM (Security Accounts Manager), as well as elements of the RPC subsystem, particularly those responsible for launching DCOM servers. Those components will also be unavailable as a result of the crash. Once the LSA has died, new authentication tokens can no longer be created. Anything that requires creating new

authentication tokens will no longer function.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0 Workstation
- Microsoft Windows NT 4.0 Server
- Microsoft Windows NT 4.0 Server, Terminal Server Edition, 4.0
- Windows 2000 Beta 3

Evidence:

- Valid User requiring access to a system resource will be denied.
- RPC subsystems will not be available.
- An Unknown Null Session is established from a foreign IP Address or NetBIOS Name.

Prevention

- These symptoms can be delayed by disabling the automatic debug option in the Registry. To disable this, set the "Auto" value of the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug key to "0". In this configuration, the debugger will prompt the user to continue. The symptoms of the attack will not appear until this dialog box has been cleared.
- As documented in MS Knowledgebase article Q143474, setting the following key value can help restrict many of the anonymous (null) SMB connections.

  Hive: HKEY_LOCAL_MACHINE\SYSTEM
  Key: System\CurrentControlSet\Control\LSA
  Name: RestrictAnonymous
  Type: REG_DWORD
  Value: 1
- Microsoft has issued a Post Service Pack 5 hotfix to correct this vulnerability. This hotfix can be downloaded at:

  ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/LSA3-fix/

Exploit: Invalid IGMP Header DoS Vulnerability

Description: The Windows 98 and Windows 2000 TCP/IP stacks were not built to reliably tolerate malformed IGMP headers. When one is received, the stack will sometimes fail with unpredictable results ranging from a Blue Screen to instantaneous reboot.

VERSIONS EFFECTED

- Microsoft Windows 98
- Microsoft Windows 95
- Microsoft Windows NT 4.0

- Microsoft Windows NT 2000.0

Evidence: None During the Development of this Document.

Prevention

Microsoft has released a series of patches, available at::

Windows NT Workstation 4.0; Windows NT Server 4.0; Windows NT Server, Enterprise Edition:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/IGMP-fix/

Windows NT Server 4.0, Terminal Server Edition:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40TSE/hotfixes-postSP5/IGMP-fix/

Exploit: NT Null Session Admin Name Vulnerability

Description: By establishing a Null session with an NT host, an intruder can gain the name of even a renamed Administrator account. This is because even Null sessions are added to the Everyone group for the duration of the connection. This was done so that hosts not in the domain could still use MS Networking's browser functions.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence:

- Suspicious or unknown Null Session connection to Ports 135, 137, 138, 139

Prevention

Establishing a null session in Windows NT opens a variety of flaws, but can be easily prevented. By setting the registry properly, anonymous connections are restricted. The registry setting for this is:

HKLM\System\CurrentControlSet\Control\Lsa
Name: RestrictAnonymous
Type: REG_DWORD
Value: 1

While this has not been tested against this specific code, It has been tested against other information gathering techniques that use a null connection to IPC$. With this registry setting enabled, you are still able to connect to IPC$, but cannot gain any further data about a domain.

Exploit: NT Telnetd Vulnerability

Description: Vulnerability exists within Microsoft's Telnetd daemon, which allows a denial of service condition. The popular scanning tool, Nmap 2.01 or later can crash telnetd services when using the SYN scanning flag (-sS).

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0
- Microsoft Windows NT 3.5.1SP5
- Microsoft Windows NT 3.5.1SP4
- Microsoft Windows NT 3.5.1SP3
- Microsoft Windows NT 3.5.1SP2

Evidence: None During the Development of this Document.

Prevention

Remove the NT telnetd service. The telnetd, which ships with NT, is not a supported product but a part of the resource kit.

Exploit: NT Services.exe Denial of Service

Description: A specially crafted packet can cause a denial of service on an NT 4.0 host, rendering local administration and network communication next to useless. This attack will crash the "services" executable, which in turn, disables the ability for the machine to perform actions via 'named pipes'. As a consequence, users will be unable to remotely logon, logoff, manage the registry, create new file share connections, or perform remote administration. Services such as Internet Information Server may also fail to operate as expected.

The problem lies within the manner that srvsvc.dll makes calls to services.exe. Certain MSRPC calls will return NULL values, which are not correctly interpreted by services.exe. This, in turn, may lead to a crash of Services.exe.

If this denial of service is combined with a number of other exploits, it may be possible to have this attack spawn a Debugger (ie Dr Watson) call on the host, which, if trojaned, may execute malicious code on the target host.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1

- Microsoft Windows NT 4.0

Evidence: RFPoison.zip, by .rain.forest.puppy, will reboot (NT) or crash (9x) the target system, and includes only a windows executable. rfpoison.py is an open source 'implementation' of the above exploit written in python by nas <nas@adler.dynodns.net>. It has only been tested against NT targets.

/data/vulnerabilities/exploits/RFPoison.zip
/data/vulnerabilities/exploits/rfpoison.py

Prevention

Workarounds posted to Bugtraq on November 4, 1999 by rfp:

#1 Enable 'RestrictAnonymous'

Go to (in the registry):

\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Current\Lsa

If you don't have it, you need to create a DWORD key named 'RestrictAnonymous', with a value of '1'. This will restrict anonymous SMB connections (which RFPoison uses). This should not affect legitimate users of the system. Suggested by David LeBlanc.

#2 Unbind NetBIOS from TCP/IP

TCP/IP can be unbound from NetBIOS, which will prevent this attack. On a dual-homed host, it is also possible to unbind NetBIOS from TCP/IP on only the 'outside' NIC, which will diable Windows netwroking services to the Internet, but maintain their availablity to the internal TCP/IP network. Suggested by Scott G. Danahy.

#3 Stop the Server service

Stopping the Server service will make the computer nearly unusable from the network (except for FTP and http services) but will prevent this and a myriad of other attacks. Suggested by Glitch.

Man In The Middle Exploits

Exploit: Microsoft Windows IP Source Routing Vulnerability

Description: A vulnerability in the Windows 95/98 and NT TCP/IP stacks allows specially crafted IP packets to perform source routing functions, even when source routing has been specifically disabled (NT SP5 Registry Setting:

(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting)

The vulnerability lies within the stack's inability to properly process source routed packets where the offset value is set greater than the specified route length. In this case, the data in the packet will get passed to the application layer of the host for further processing (instead of being dropped by the stack.) Should the attacker spoof the source address and, instead, use a source address of a known host on an internal network (assuming the Windows host is dual-homed), the datagram reply will be sent to the host on the internal network (accessible via the second NIC).

In addition to being susceptible to various tunneling attacks, the vulnerable host may be used to aid an attacker in locating other non-Windows hosts that have source routing enabled and/or perform port scans against other Windows hosts.

VERSIONS EFFECTED

- Microsoft Windows 98.0se
- Microsoft Windows 95.0b
- Microsoft Windows 95.0a
- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0
- Microsoft Windows NT Terminal Server

Evidence: None During the Development of this Document.

Prevention

Microsoft has released a post Service Pack 5 hotfix for Windows NT. It is available at:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/Spoof-fix

Exploit: SMB sessions can be hijacked

Description: SMB sessions can be hijacked. Having the correct frame numbers at the transport level, the correct TID at the redirector level, and the correct UID at the server level allow you to impersonate an administrator or other user.

Regedit/regedt32 and other RPCs, which use named pipes, also use SMB UIDs for authentication and can be taken over via this method.

This requires the use of an application that combines a combination of Sequence attack and UID/TID spoofing.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0
- Microsoft Windows NT 3.51
- Microsoft Windows NT 3.5

Evidence:

- The source IP address of the forged packets is an unknown or non-authorized address.
- The Intruder forged a field that is being logged, but was not needed to impersonate. For example, the intruder gave their real IP address as the source IP field and the IP source address was not part of the authentication information needed. The suspicious IP address would be a clue to an impersonation.

Prevention

Apply all necessary Service pack. Remember, if you install a service using the Windows NT CD-Rom you must reapply the Current Service Pack. Refer to the Microsoft Site located *at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/* for the current fixes and

patches for your system.

Exploit: NT Predictable TCP Sequence Number Vulnerability

Description: Windows NT 4 uses predictable TCP sequence number generating algorithms that could allow an attacker to set up connections to other machines with a spoofed source address of the NT host.

Windows NT4.0 until and including SP3 used a predictable means of generating initial TCP sequence numbers, incrementing it by one every millisecond. Alerted to this problem, they changed the method in SP4. However, the new method is in fact easier to predict than the previous one: Now there only 8 possible increments, (0, 2, 4, 6, 8, 10, 12, and 14) and the fact that most TCP/IP stacks will ignore invalid sequence numbers makes this easy to exploit - obtain a valid sequence number, and send 8 packets to the target, each with one of the possible next sequence numbers.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None During the Development of this Document.

Prevention

Apply all necessary Service pack. Remember, if you install a service using the Windows NT CD-Rom you must reapply the Current Service Pack. Refer to the Microsoft Site located *at* ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ for the current fixes and patches for your system.

Exploit: NT LSA DoS (Phantom) Vulnerability

Description: NT hosts are subject to a Denial of Service attack against the Local Security Authority (LSA) subsystem. Sending invalid data to the LsaLookupNames function of the LSA API can crash the LSA system, as well as the Security Accounts Manager and certain MSRPC processes.

In order for this exploit to occur, the user must first establish a null session connection to the target host.

Once a host has been impacted by this exploit, the NT system will begin to exhibit "strange behavior". Remote users will be unable to connect to the host's shares or resources, users may not be able to change their passwords, console logon to a domain will be unavailable, systems management tools such as User Manager and Server Manager will not function, and RPC dependant services using integrated security (IIS, SQL Server) will not function. Users will be unable to shutdown the server - they will receive a message stating that the current user does not have privileges to perform that function. Users connected to resources prior to the attack will still be able to access these resources.

These symptoms can be delayed by disabling the automatic debug option in the Registry. To disable this, set the "Auto" value of the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug key to "0". In this configuration, the debugger will prompt the user to continue. The symptoms of the attack will not appear until this dialog box has been cleared.

This Denial of Service attack requires the machine to be "hard-booted" to reset the system to normal operation. Upon reboot, the system will function normally.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None During the Development of this Document.

Prevention

Microsoft has issued a Post Service Pack 5 hotfix to correct this vulnerability. This hotfix can be downloaded at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/LSA3-fix/

Local Attacks

Exploit: NT RASMAN Privilege Escalation Vulnerability

Description: Any authenticated NT user (ie domain user) can modify the pathname for the RASMAN binary in the Registry. The next time the RAS Service is started, the (trojan) service referenced by the RASMAN pathname will be executed with system privileges. This trojan service may allow the User to execute commands on the target server as an administrator, including elevating the privileges of their own account to that of Administrator. A modified (UNC) pathname may be used to point to an executable existing on another host on the network.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence:

BertzHole.exe <binary pathname> will modify the RASMAN/ImagePath key in the Registry with the service executable to be run in its place. BertHole.exe (author supplied) is a sample

trojan service that may be run. This executable runs a service, which launches a netcat listener on tcp port 123. (nc -d -L -p 123 -e cmd.exe). (This service may or may not run with errors.)

- /data/vulnerabilities/exploits/BertzHole.exe
- /data/vulnerabilities/exploits/BertzSvc.exe

Prevention

Microsoft has released a tool that will set proper permissions over the HKEY_Local_Machine/SYSTEM/CurrentControlSet/Services/RASMan key

The Post SP6 Rasman-fix tool can be downloaded from ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP6/Security/Rasman-fix/

This tool may be executed against any NT host, regardless of the current Service Pack level. The tool may be executed against a remote machine using the syntax: "fixrasi \\machinename" (without the quotes).

Exploit: NT Unattended Installation File Vulnerability

Description: When an unattended installation of Windows NT4 is performed, the configuration details are read from the Unattend.txt file. The contents of this file are copied to one of two locations, depending on the type of installation: %windir%\system32\$winnt$.inf for a normal unattended installation, or %windir%\system32\$nt4pre$.inf for an installation using Sysprep. This file is not deleted after the installation, and can be read by any Interactive User. In certain circumstances, this file may include the administrative password in plain-text.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence:

- The files described in the above description exist on your system.

Prevention

If the files exist on your system delete these files.

Exploit: NT DCOM Server Vulnerability

Description: It is possible for a local user to modify how DCOM servers are run, thereby escalating his/her privilege level. The Interactive User has write permissions to the DCOM registry entries. By editing the registry keys associated with DCOM server applications, they can change which services are started to handle specific events. They can then overwrite the services EXE file, trigger the event, and have their code run as SYSTEM.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence:

This exploit will cause the System Event Notification service or SENS service to start when a VBScript calls for the creation of a new Wordpad Document. The SENS service is installed during an installation of IE5, but is not started. The default permissions allow Everybody write access to the EXE.

Prevention

Restrict write permission to all DCOM registry keys and, using NTFS, service EXEs.

Exploit: NT Master File Table Corruption Vulnerability

Description: The Master File Table (MFT) of an NT 4 host may show signs of corruption after it has grown larger than 4 Gig. Corruption may include: presence of formerly deleted files, disappearance of non-deleted files, and warning messages about corruption that recommend running CHKDSK. The MFT may grow larger than 4 Gig if there are more than 4 million files on the host.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: See description for evidence

Prevention

Microsoft has issues a post-SP5 hotfix to correct this problem. It can be obtained at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/NTFS-fix

Exploit: NT Malformed Dialer Entry Vulnerability

Description: Dialer.exe has an unchecked buffer in the part of the program that reads dialer

entries from %systemroot%\dialer.ini. A specially formed entry could cause arbitrary code to be run on the machine. By default, the %systemroot% folder is world-writeable. Dialer.ini is Dialer runs in the security context of the user, so an attacker would have to have a higher authority user dial the entry to gain any escalated priveleges.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence:

The following code will create a trojaned dialer.ini file that when read in by dialer will cause it to run a batch file called code.bat - this is hidden from the desktop by calling the equivalent of WinExec("code.bat",0); - and then ExitProcess(0); is called to shutup dialer.exe. Once the dialer.ini has been trojaned the attacker would create a batch file called code.bat and place in there any commands they wished to be run. Needless to say that if a user with admin rights runs dialer any commands placed in this batch file are likely to succeed.

- /data/vulnerabilities/exploits/dialer.c

Prevention

Microsoft has released a Post-SP5 patch to address this issue. It is available at:

Windows NT Server; Windows NT Server 4.0, Enterprise Edition; and Windows NT Workstation 4.0:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/Dialer-fix
Windows NT Server 4.0, Terminal Server Edition:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40tse/hotfixes-postSP4/Dialer-fix

Exploit: NT IOCTL Console DoS Vulnerability

Description: In Windows NT, device driver services are requested through objects known as IOCTLs. User-level programs can invoke the keyboard and mouse IOCTLs. By using specific, legitimate calls malicious code could disable the keyboard and mouse, forcing a reboot to re-establish their usability. On NT Terminal Server, the keyboard and mouse on the remote server could be disabled, forcing a reboot of that machine.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2

- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

Microsoft has issued a post-SP5 (post-SP4 for Terminal Server) hotfix to correct this vulnerability. This hotfix can be downloaded at:
Windows NT Server and Workstation 4.0:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/IOCTL-fix/
Windows NT Server 4.0, Terminal Server Edition:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40tse/Hotfixes-PostSP4/IOCTL-fix/

Exploit: NT Malformed Image Header DoS Vulnerability

Description: The system will crash and will need to be rebooted if an executable file with a specific type of malformed image header is run. The machine will BSOD with the error message:

STOP 0x0000000A IRQ_not_less_or_equal or 0x00000050
PAGE_FAULT_IN_NON_PAGED_AREA

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

Upgrade to SP5. If this is not acceptable, Microsoft has made a Post-SP4 hotfix publicly available for download at:
NT 4.0:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP4/Kernel-fix/
NT Terminal Server 4.0:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40tse/Hotfixes-PostSP4/Kernel-fix/

Exploit: NT Login Default Folder Vulnerability

Description: When a user logs into an NT machine, there are a few processes that are started automatically, including explorer.exe. These programs are normally in %winroot% or %winroot%\system32. The problem is that NT will look for these programs first in the user's home directory. If no user folder is specified, it will look in the root of the system drive. Only if the program it is looking for is not found in that location will it look in the 'normal' location. This allows any user to rename any executable and have it run at login, effectively bypassing many policy restrictions. The list of currently known filenames that will work is: explorer.exe, nddeagnt.exe, taskmgr.exe and userinit.exe .

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence:

Verify the integrity of the following files, to ensure they have the proper date and time stamp that is conducive to the operating system.

explorer.exe, nddeagnt.exe, taskmgr.exe and userinit.exe .

Prevention

There are several possible workarounds including:

Using NTFS permissions to remove write access to the root of the system drive and home directory.
Removing any instances of the executables from the home directory via the login script.
Using NTFS permissions to remove write access to the root of the system drive and disabling user home directories.

Exploit: NT Performance Counters Memory Leak Vulnerability

Description: A memory leak exists in the NT performance counters that may cause an NT host to stop functioning and/or need to be rebooted. Specifically, when a request is made to monitor a counter that does not exist on a machine, the memory leak may occur. For example, Healthmon.exe, from Microsoft Systems Management Server 2.0, requires SNMP to be loaded on the host. If SNMP is not installed, memory may not be deallocated from looking for a performance counter that does not exist. This condition may cause the computer to stop functioning or responding to future requests.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

Microsoft has issued a Post SP5 hotfix for this memory leak. It is available at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/Perfctrs-fix/

Exploit: NT RAS Phonebook Buffer Overflow Vulnerability

Description: Microsoft Windows NT RAS Service contains multiple buffer overflows that allow the execution of arbitrary code resulting in elevated privileges by local users.

The RAS Service allows users to dial and connect to RAS servers, or other dial-up servers. The RAS API function RasGetDialParams performs no bounds checkings, which leads to an exploitable buffer overflow. The RAS RASMAN.EXE components implement the RAS Autodial Manager and RAS Connection Manager services which are used to dial out. RASMAN.EXE is a system process and is run in the security context of the LocalSystem account. RASMAN.EXE uses the RasGetDialParams function to read in things such as the telephone number from the Phonebook (rasphone.pbk) when is tries to dial out. This leads to a vulnerability that can be exploited by creating a phonebook entry with executable code inserted in the phone number parameter. If the phone number is over 299 bytes in length the process's saved return address will be overwritten.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

Install the patches available at:

- ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/RAS-fix/

Exploit: NT Help File Buffer Overflow Vulnerability

Description: The Windows NT Help utility parses and displays help information for selected applications. The help files are stored in the %SystemRoot%\help directory. The default permissions in this directory allow any user to add new files.

A buffer overflow exists in the Help utility when it attempts to read a .cnt file with an overly long heading string. Content tab informaton files (".cnt") are generated when rich text format files (".rtf") are translated to help files (".hlp"). If the string is longer than 507 bytes winhlp32 truncates the entry and the buffer overflow does not occur.

A malicious user can create a custom .cnt help file with executable code in an entry string which when stored in the help directory and viewed by an unsuspecting user can grant them that users privileges.

The vulnerability is not limited by the permissions of the help file directory as the Help utility will search for a .cnt file first in its execution directory before looking in the help file directory.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

Apply the patches found at:

- X86 version: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP5/winhlp32-fix/winhlp-i.exe

Exploit: NT Trojan Profile Vulnerability

Description: Lax permission in Windows NT's ProfileList registry key allows malicious users to install trojan profiles for other users, including administrator, which may lead to a system compromise.
When a new user logs onto a Windows NT workstation or server a new subkey is written to the registry key "HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList". The name of this key is the user's Security Identifier (SID). One of the values of the new key is "ProfileImagePath" which points to the location of the user's profile directory.

The default permission on the ProfileList registry key grants the Everybody group the SetValue permission. This means any user can edit the information in this key or any of its subkeys. This allows a malicious user to modify another user's ProfileImagePath making them load a trojan profile which contains entries in the Start Up folder that will execute the next time the user logos to the machine.

Registry editing can be acomplished locally or across a network. Although access to the registry via the network can be controlled by the applying ACL permissions over the winreg key, by default, the path "HKLM\Software\Microsoft\Windows NT\CurrentVersion" is an AllowedPath. This allows a remote user to edit any subkey of that path regardless of the permission on the winreg key.

Tools such as Regedit.exe and Regedt32.exe may have problems editing AllowedPath keys whether or not they are allowed to.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

Since the winlogon process creates the new subkey when a new user logs on in the context of the SYSTEM account, only the SYSTEM account needs write access to the ProfileList key and Everyone should only be given read access.

Exploit: NT CSRSS Worker Thread Exhaustion Vulnerability

Description: Worker threads in CSRSS.exe (the Client Server Runtime Subsystem, aka the Win32 Subsystem) that are waiting for user input remain occupied until they get that input. If all threads (default 16) are simultaneously waiting for input, the system will hang until it is received. This condition will lead to a Denial of Service, and could be caused by malicious or defective code in a service or program.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

Microsoft has released a post-SP5 hotfix. It is available for download at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP5/Csrss-fix/

Exploit: NT Screensaver Vulnerability

Description: When the computer is idle for the set time period (user definable) Winlogon.exe starts the screensaver. The screen saver process is selectable by the user. Winlogon.exe uses the CreateProcessAPI call to start the screen saver and immediately suspends it. At this point the screen saver is running with the security context of Winlogon.exe (system). Winlogon obtains the process handle, changes the primary security token of the screen saver to match the current user, and resumes the screen saver. Winlogon never verifies that the token change was successful. Therefore, a user could create an executable, set it as the screen saver, and should the security change fail it will run with full system-level privileges.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: The simulation consists of one 32-bit application say BEADMIN.EXE and one MS-

DOS based application, say SCRNSAVE.EXE. The BEADMIN.EXE when started does the following Creates one event in 'not-signal'ed state Sets up the screen saver. The screen saver executable is specified as SCRNSAVE.EXE and the timeout is set to minimum. . BEADMIN.EXE now waits on the event. After some time, the screen saver is triggered. This results in Winlogon.Exe spawning SCRNSAVE.EXE. Since the CreateProcess call returns junk handle to Winlogon.Exe, the setting of primary token fails. Hence the SCRNSAVE.EXE application (NTVDM.EXE) runs in System Context. This SCRNSAVE.EXE again spawns BEADMIN.EXE application. Now this second copy of BEADMIN.EXE inherits the security context of NTVDM which is System Context. This application adds the logged in user to admin group and signals the event on which first instance of BEADMIN.EXE is waiting. In response to this the first copy of BEADMIN.EXE resets back the Screen Saver settings and quits. The logged in user name is passed between the first and second copy of BEADMIN.EXE using shared section.

- /data/vulnerabilities/exploits/beadmin.zip

Prevention

Microsoft has issued a Post Service Pack 4 hotfix to correct this vulnerability. This hotfix can be downloaded at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP4/ScrnSav-fix/

Exploit: NT Blank Password SP4 Vulnerability

Description: Windows NT 4.0 SP4 introduced a logic error in the network authentication process for "downlevel" clients. When a user changes his or her password (on an NT 4.0 SP4 server) from a Windows for Workgroups, OS/2, or Macintosh client, the LanMan hash is properly updated, however, the NT hash is reset to a null value. This vulnerability would allow a user to logon to the host or domain from a Win9x or NT machine by presenting the username and a blank password.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

Microsoft has release a Post SP4 hotfix for this vulnerability. This fix was originally released at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP4/Msv1-fix/

however, it has been moved and included in the Post SP4Roll-up fix located at:
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP4/Roll-up/

The original fix is now located at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP4/archive/Msv1-fix/

Exploit: NT Anonymous Users Can Obtain The Password Policy Under Windows NT 4.0 Vulnerability

Description: Service Pack 3 added the ability to restrict anonymous users from obtaining information about the system. Even with SP3 installed anonymous users are able to retrieve the systems password policy.

Normally Windows NT uses anonymous access to the password policy to provide users with meaningful error message such as in the case of when an user changes his password before login in.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

To fix this vulnerability, apply the lsa2-fix hotfix from Microsoft

Exploit: NT RAS Dial-up Networking "Save Password" Vulnerability

Description: Windows NT allows users to save their RAS (and/or RRAS) credentials by using the 'Save Password' checkbox when making a dial-up connection. Credentials saved in this manner are stored in the HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets\RasCredentials!SID#0 registry key.

These credentials can be enumerated using the LSA secrets code, as published by Paul Ashton.

If a user does not check the 'save password' checkbox to prevent the password from being stored, RAS will STILL save the successful connection information. This information includes the Dial-up username, phone number, and password, and is stored in the HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets\RasDialParams!SID#0 registry key.

This infromation can be enumerated using the LSA secrets code.

NOTE: Administrator privileges are needed to execute the LSA secrets code.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3

- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: See Description.

Prevention

Microsoft has released a hotfix for NT 4.0 SP3 machines that prevents enumeration of the LSA secrets. This hotfix can be found at: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postSP3/lsa2-fix/

This hotfix has been included in Service Pack 4.

However, the LSA-2 patch does not prevent the username, phone number, and password from being saved in the Policy\Secrets\RasDialParams!SID#0 registry key. Microsoft has released a post SP5 hotfix that prevents these credentials from being cached. This hotfix can be found at

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/RASPassword-fix/ or

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/RRASPassword-fix/

Exploit: NT Spoolss.exe Buffer Overflow Vulnerabilities

Description: Spoolss.exe, AKA the spooler service, which handles all print requests for the NT operating system, has a number of APIs with unchecked buffers. Some of these an only be executed by Power Users or Administrators, but some are accessible to all authenticated users. Many of the overflows will write directly into the EIP register, meaning that an exploit could be created to run arbitrary code as SYSTEM.

VERSIONS EFFECTED

- Microsoft Windows NT 4.0SP6
- Microsoft Windows NT 4.0SP5
- Microsoft Windows NT 4.0SP4
- Microsoft Windows NT 4.0SP3
- Microsoft Windows NT 4.0SP2
- Microsoft Windows NT 4.0SP1
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

Microsoft has released patches for this issue for NT4.0 Server and Workstation machines that are at SP5 or SP6. Other SP levels will be supported at a later date. The patches are available for download at:

X86:

http://download.microsoft.com/download/winntsrv40/Patch/Spooler-fix/NT4/EN-US/Q243649.exe

Alpha:
http://download.microsoft.com/download/winntsrv40/Patch/Spooler-fix/ALPHA/EN-US/Q243649.exe

WEB Server Attacks (IIS)

Exploit: Microsoft IE Setupctl ActiveX Control Buffer Overflow Vulnerability

Description: There is a buffer overflow in the setupctl ActiveX control that used to ship with some versions of Microsoft's Internet Explorer. This ActiveX control is used to link to an update site at Microsoft and is marked 'Safe for Scripting' . Arbitrary commands may be executed if the ActiveX control is run in a malicious manner.

VERSIONS EFFECTED

- Microsoft Internet Explorer 4.0 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 4.0 for Windows 98
- Microsoft Windows 98
- Microsoft Internet Explorer 4.0 for Windows 95
- Microsoft Windows 95

Evidence: None during the development of this document.

Prevention

Microsoft has released a patch for this vulnerability:

Internet Explorer 4.01 for Intel:
ftp://ftp.microsoft.com/peropsys/ie/ie-public/fixes/usa/IE401/ImportExportFavorites-fix/x86/q241361.exe
Internet Explorer 5 for Intel:
ftp://ftp.microsoft.com/peropsys/ie/ie-public/fixes/usa/IE50/ImportExportFavorites-fix/x86/q241361.exe

Exploit: Microsoft IE Registration Wizard Buffer Overflow Vulnerability

Description: There is a buffer overflow in the Internet Explorer Registration Wizard control (regwizc.dll). This control is marked 'Safe for Scripting'. Arbitrary commands may be executed if the control is run in a malicious manner.

VERSIONS EFFECTED

- Microsoft Internet Explorer 5.0 for Windows NT 4.0
- Microsoft Internet Explorer 4.0 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 4.0 for Windows 98
- Microsoft Windows 98
- Microsoft Internet Explorer 4.0 for Windows 95
- Microsoft Windows 95

Evidence: None during the development of this document.

Prevention

Microsoft has released a patch for this vulnerability:

Internet Explorer 4.01 for Intel:
ftp://ftp.microsoft.com/peropsys/ie/ie-public/fixes/usa/IE401/ImportExportFavorites-fix/x86/q241361.exe

Internet Explorer 5 for Intel:
ftp://ftp.microsoft.com/peropsys/ie/ie-public/fixes/usa/IE50/ImportExportFavorites-fix/x86/q241361.exe

Exploit: Microsoft IE5 Download Behavior Vulnerability

Description: The "download behavior" feature of Microsoft's Internet Explorer 5 may allow a malicious web site operator to read files on an IE5 client computer or on a computer that is in the client's 'Local Intranet' web content zone.

IE5 introduced a new feature called DHTML Behaviors. DHTML Behaviors allow web developers to encapsulate methods, properties and events that can then be applied to HTML and XML elements. IE5 comes with set of built-in DHTML behaviors. One of them is the "#default#download" behaviors. This behavior defines a new Javascript method called "startDownload" that takes two parameters, the file to download and a function to call once the file has been downloaded.

By default the "startDownload" method checks that the file to be downloaded is in the same web content zone as the file calling the method. When both the file to be downloaded and the file executing the behavior are in the same security zone, the client will safely download the requested file and subsequently perform the specified function.

A malicious web site owner may bypass this security restriction and force an IE5 client to both read and perform a follow-up action on the contents of a local file or files in other security zones. This action may include sending the contents of the file back to the malicious web site operator.

VERSIONS EFFECTED

- Microsoft Internet Explorer 5.0 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 5.0 for Windows 98
- Microsoft Windows 98
- Microsoft Internet Explorer 5.0 for Windows 95
- Microsoft Windows 95

Evidence:

Here's how it works:

1: An IE5 client visits a malicious website and loads a web page containing a client side scripting that makes use of the "#default#download" behavior.

2: The client side script calls the "startDownload" method and passes it the URL of a file to download and a function to call with the contents of the file once the file is finished downloading.

3. The startDownload method verifies that the URL is in fact in the same zone as the malicious web server.

4: The startDownload method begins the download, requesting the URL specified in step 2 from a malicious web server.

5: The malicious web server send an HTTP redirect to some other file in any security zone including local files on the IE5 client machine (for example: c:\winnt\repair\sam._).

6: startDownload reads the file and executes the function specified in step 2 on that file's content.

The malicious web server has now bypassed the security restrictions outlined earlier by successfully forcing the client to load and act upon a file that resides in a web content zone different than that of the malicious web server. This can all be done transparently to the end user.

This vulnerability cannot be used to delete or modify files on the vulnerable IE5 client. The vulnerability can only retrieve text files or small parts of binary files.

Prevention

Microsoft has developed a patch for this problem. It is available at either of the following locations
- http://windowsupdate.microsoft.com
- http://www.microsoft.com/msdownload/iebuild/dlbhav/en/dlbhav.htm

Exploit: Microsoft IIS 4.0 Domain Resolution Vulnerability

Description: IIS 4.0 and CIS 2.5 allow an administrator the option to restrict access by specifying a domain or an IP address If a domain is restricted, but a machine in that domain that cannot be resolved makes an HTTP request, the IIS server will respond as usual. Any subsequent requests will be denied.

Restricted hosts with an IP address that can be resolved to a domain name will be denied access from the first request.

VERSIONS EFFECTED

- Microsoft Commercial Internet System 2.5
- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

Microsoft has released a hotfix, available at:
IIS 4.0:
ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/IIS40/hotfixes-postSP6/security/IPRFTP-fix/
MCIS 2.5:
ftp://ftp.microsoft.com/bussys/mcis/mcis-public/fixes/usa/mcis25/security/ftpsvc-fix/

Exploit: Microsoft IIS FTP NO ACCESS Read/Delete File Vulnerability

Description: IIS 4.0 FTP servers, which have installed a specific post SP5 FTP hotfix, are vulnerable to an exploit whereby FTP clients may download. and/or delete files (on the FTP server) that have been specifically marked as 'No Access' (via NTFS file or directory permissions). Web browser FTP clients may be able to view and/or download these files, while specially crafted requests from non-browser based FTP clients may be able to delete these files.

This vulnerability only affects IIS 4.0 servers running NT 4.0 SP5 with a specific post SP5 hotfix for an FTP get error as described in <http://support.microsoft.com/support/kb/articles/Q237/9/87.ASP >. Microsoft states there are no negative ramifications to applying this hotfix to SP4 or SP5 hosts who have not installed the previously referenced FTP hotfix.

VERSIONS EFFECTED

- Microsoft Commercial Internet System 2.5
- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5
- Microsoft Windows NT 4.0

Evidence:

To see if you are vulnerable, check the file version for Ftpsvc.dll. Versions 0718 through 0722 are thought to be vulnerable, although Microsoft documentation is unclear as to whether the vulnerable versions start with 0718 or 0719. Version 0724 represents the version installed by the latest hotfix.

The hotfix designed to correct this problem was not released in time for the upcoming NT 4.0 Service Pack 6. Service Pack 6 contains the "buggy" hotfix and will be vulnerable to this error when it is released. It will be necessary to install the corresponding hotfix after installing Service Pack 6, regardless of whether or not the Service Pack 5 installation was vulnerable.

Prevention

Microsoft has released a hotfix for this vulnerability. This hotfix was too late to be included in NT 4.0 SP6 (as yet unreleased), so it has been released as an IIS Post -SP6 hotfix for IIS and

a fix for CIS.
The patches can be found at
IIS 4.0:
ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/IIS40/hotfixes-postSP6/security/IPRFTP-fix/
MCIS 2.5:
ftp://ftp.microsoft.com/bussys/mcis/mcis-public/fixes/usa/mcis25/security/ftpsvc-fix/

Microsoft states there are no negative ramifications to applying this hotfix to SP4 or SP5 hosts who have not installed the previously referenced FTP hotfix.

The hotfix designed to correct this problem was not released in time for the upcoming NT 4.0 Service Pack 6. Service Pack 6 contains the "buggy" hotfix and will be vulnerable to this error when it is released. It will be necessary to install this hotfix after installing Service Pack 6, regardless of whether or not the Service Pack 5 installation was vulnerable.

Exploit: Microsoft IE Import/Export Favorites Vulnerability

Description: The ImportExportFavorites() method, used to import and export favorites to/from a file in IE5, can be made to write to any file on the system, in some cases from an email or remote webpage.

VERSIONS EFFECTED

- Microsoft Internet Explorer 5.0 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 5.0 for Windows 98
- Microsoft Windows 98
- Microsoft Internet Explorer 5.0 for Windows 95
- Microsoft Windows 95
- Microsoft Internet Explorer 5.0 for Windows 2000
- Microsoft Windows NT 2000.0
- Microsoft Internet Explorer 4.0.1 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 4.0.1 for Windows 98
- Microsoft Windows 98
- Microsoft Internet Explorer 4.0.1 for Windows 95
- Microsoft Windows 95

Evidence: None during the development of this document.

Prevention

Microsoft has released patches for this vulnerability. From the Microsoft Advisory (MS99-037):

Internet Explorer 4.01 for Intel:
ftp://ftp.microsoft.com/peropsys/ie/ie-public/fixes/usa/IE401/ImportExportFavorites-fix/x86/q241361.exe

Internet Explorer 5 for Intel:
ftp://ftp.microsoft.com/peropsys/ie/ie-public/fixes/usa/IE50/ImportExportFavorites-fix/x86/q241361.exe

Exploit: Microsoft IE Virtual Machine Sandbox Vulnerability

Description: The Microsoft Virtual Machine (VM) that ships with Win9X, NT and Internet Explorer 4.X and 5.0 contains a vulnerability that may allow a hostile Java applet to escape the bounds of its "sandbox" and perform malicious activities on the victim host. These activities may result in a privilege escalation or other harmful activities including, under certain circumstances: adding, modifying or deleting user accounts and groups, deleting files, formatting the hard drive, and copying data off of the victim host.

This vulnerability may occur when a Microsoft IE client visits a web site that hosts a hostile java applet. Disabling the execution of java applets from within the IE client may prevent this vulnerability from occurring.

VERSIONS EFFECTED

- Microsoft Internet Explorer 5.0 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 5.0 for Windows 98
- Microsoft Windows 98
- Microsoft Internet Explorer 5.0 for Windows 95
- Microsoft Windows 95
- Microsoft Internet Explorer 4.1 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 4.1 for Windows 95
- Microsoft Windows 95
- Microsoft Internet Explorer 4.0 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 4.0 for Windows 98
- Microsoft Windows 98
- Microsoft Internet Explorer 4.0 for Windows 95
- Microsoft Windows 95
- Microsoft Visual Studio 6.0
- Microsoft Windows NT 4.0

Evidence: None during the development of this document.

Prevention

Microsoft has released a patch for this vulnerability. It is located at http://www.microsoft.com/java/vm/dl_vm32.htm

Microsoft recommends disabling java applets until this patch has been applied.

Additional Microsoft VM components may be impacted by the vulnerability. To see if you're vulnerable, type JVIEW from a command prompt. Evaluate the last four digits of the VM version number. Versions at or below 1520 are NOT vulnerable. Versions above 1520 ARE vulnerable. The patch referenced above is version 3186. This version is SAFE from this vulnerability.

Exploit: NT IE5 FTP Password Storage Vulnerability

Description: FTP usernames and passwords for sites accessed via Internet Explorer 5.X are stored (cleartext) in history files stored under \Winnt\Profiles\[Username]\History\History.IE5\index.dat and \Winnt\Profiles\[Username]\History\History.IE5\MSHist<date>..\index.dat. By default, the \Winnt\Profiles\[Username]\History directories are secured with ACLs to allow Full Control for System, the Administrators group, and the given Username. The index.dat files, however, are created with Everyone:Full Control permissions.

Because the "Bypass Traverse Checking" right is assigned by default to the Everyone group, any user with access to the host can read any other user's index.dat files.

VERSIONS EFFECTED

- Microsoft Internet Explorer 5.0 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 5.0 for Windows 2000
- Microsoft Windows NT 2000.0

Evidence:

To bypass traverse checking and access another user's index.dat files, reference the absolute filename. For example, to search for all index.dat files belonging to the "administrator" account, issue the following command from a command prompt:

find "//"<\winnt\profiles\administrator\history\history.ie5\index.dat

Prevention

a) remove "Bypass Traverse Checking" for everyone except administrators

b) set the permissions on all directories and files in each user's profile, to allow only the owner (and possibly an administrator) to access them

c) disable URL histories if the URLs contain sensitive information like passwords

d) use the FTP client, rather than IE, in cases where it is unacceptable

to pass the password as part of the URL

Exploit: Microsoft IE5 ActiveX "Eyedog" Vulnerability

Description: The Eyedog ActiveX control is marked 'safe for scripting' although it permits registry access and other information gathering methods to be used. It also contains a buffer overflow error. These weaknesses can be exploited remotely via a malicious webpage or email.

VERSIONS EFFECTED

- Microsoft Internet Explorer 5.0 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 5.0 for Windows 98
- Microsoft Windows 98
- Microsoft Internet Explorer 5.0 for Windows 95
- Microsoft Windows 95
- Microsoft Internet Explorer 5.0 for Windows 2000
- Microsoft Windows NT 2000.0
- Microsoft Internet Explorer 4.0 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 4.0 for Windows 98
- Microsoft Windows 98
- Microsoft Internet Explorer 4.0 for Windows 95
- Microsoft Windows 95

Evidence: None during the development of this document.

Prevention

Microsoft has released a patch, available at:
Windows 95/98:
ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/Eyedog-fix/x86/q240308.exe
Windows NT:
ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/Eyedog-fix/

Exploit: Microsoft IE5 ActiveX "Object for constructing type libraries for scriptlets" Vulnerability

Description: The ActiveX Control "scriptlet.typlib" can create, edit, and overwrite files on the local disk. This means that an executable text file, such as an .hta file, can be written to the startup folder of a remote machine and will be executed the next time that machine reboots. This vulnerability can be exploited via a malicious web page or an email message.

VERSIONS EFFECTED

- Microsoft Internet Explorer 5.0 for Windows NT 4.0
- Microsoft Windows NT 4.0
- Microsoft Internet Explorer 5.0 for Windows 98
- Microsoft Windows 98

- Microsoft Internet Explorer 5.0 for Windows 95
- Microsoft Windows 95

Evidence: None during the development of this document.

Prevention

Microsoft has released a patch, available at:
Windows 95/98:
ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/Eyedog-fix/x86/q240308.exe
Windows NT:
ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/Eyedog-fix/

Exploit: NT IIS Malformed HTTP Request Header DoS Vulnerability

Description: Microsoft IIS and all other products that use the IIS web engine have a vulnerability whereby a flood of specially formed HTTP request headers will make IIS consume all available memory on the server and then hang. IIS activity will be halted until the flood ceases or the service is stopped and restarted.

VERSIONS EFFECTED

- Microsoft Commercial Internet System 2.5
- Microsoft Commercial Internet System 2.0
- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5
- Microsoft Site Server 3.0 Commerce Edition
- Microsoft Site Server 3.0
- Microsoft Site Server 3.0 Commerce Edition

Evidence:

Simple play. I sent lots of "Host:aaaaa...aa" to IIS like...

GET / HTTP/1.1
Host: aaaaaaaaaaaaaaaaaaaaaa....(200 bytes)
Host: aaaaaaaaaaaaaaaaaaaaaa....(200 bytes)
...10,000 lines
Host: aaaaaaaaaaaaaaaaaaaaaa....(200 bytes)

I sent twice above request sets. Then somehow victim IIS got memory leak after these requests. Of course, it can not respond any request any more. If you try this, you should see memory increase through performance monitor. You would see memory increase even after those requests finished already. It will stop when you got shortage of virtual memory. After that, you might not be able to restart web service and you would restart computer. I tried this against Japanese and English version of Windows NT.

Prevention

Microsoft released a patch for this vulnerability on August 11, 1999. However, on August 12, 1999 they retracted it due to an error that made IIS hang whenever the logfile was an exact

multiple of 64KB. Microsoft re-released the bulletin on August 16, 1999. The new patches are available at:
ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/HDBRK-fix/

Exploit: NT IIS MDAC RDS Vulnerability

Description: MDAC (Microsoft Data Access Components) is a package used to integrate web and database services. It includes a component named RDS (Remote Data Services). RDS allows remote access via the internet to database objects through IIS. Both are included in a default installation of the Windows NT 4.0 Option Pack, but can be excluded via a custom installation.

RDS includes a component called the DataFactory object, which has a vulnerability that could allow any web user to:
--Obtain unauthorized access to unpublished files on the IIS server
--Use MDAC to tunnel ODBC requests through to a remote internal or external location, thereby obtaining access to non-public servers or effectively masking the source of an attack on another network.

The main risk in this vulnerability is the following:
--If the Microsoft JET OLE DB Provider or Microsoft DataShape Provider are installed, a user could use the shell() VBA command on the server with System privileges. (See the Microsoft JET Database Engine VBA Vulnerability for more information). These two vulnerabilities combined can allow an attacker on the Internet to run arbitrary commands with System level privileges on the target host.

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5
- Microsoft Windows NT 4.0
- Microsoft IIS 3.0
- Microsoft Index Server 2.0
- Microsoft MDAC 2.1UPGRADE
- Microsoft MDAC 2.1CLEAN
- Microsoft MDAC 2.0
- Microsoft MDAC 1.5
- Microsoft Site Server 3.0
- Microsoft Site Server 3.0 Commerce Edition
- Microsoft Commercial Internet System 2.0

Evidence: None during the development of this document.

Prevention

If you have MDAC 1.5 or 2.x installed on the IIS server and DO NOT need MDAC functionality, perform the following:
--Delete the /msdac virtual directory in IIS, or
--Remove the following registry keys and all of their subkeys on the IIS server:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\AdvancedDataFactory
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls

If you need MDAC capabilties, you should:
--Install the latest version of MDAC 2.1.2.4202.3 (GA) (also known as MDAC 2.1 SP2) from:
http://www.microsoft.com/data/download.htm
--Disable Anonymous Access to the /msdac virtual directory
--Create a Custom Handler to filter incoming requests. More information on this is available at:
http://www.microsoft.com/Data/ado/rds/custhand.htm
these changes have been placed in a registry file:
http://www.microsoft.com/security/bulletins/handsafe.exe
this file implements the following Registry keys:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory]

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo
"handlerRequired"=dword:00000001
"DefaultHandler"="MSDFMAP.Handler"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo\safeHandlerList
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo\safeHandlerList\MSDFMAP.Handler
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo\safeHandlerList\MSDFMAP_VB.Handler
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory\HandlerInfo\safeHandlerList\MSDFMAP_VC.Handler

Exploit: NT IIS SSL DoS Vulnerability

Description: NT Servers running IIS with SSL security enabled are susceptible to a DoS attack due to the server's inability to differentiate between pages that require SSL and those that don't. Therefore, by replacing the 'http' string in the URL with 'https' the server can be forced to encrypt any content in the web site, including high-bandwidth pages. An attacker could, with carefully planned https requests, drive the processor utilization to 100% resulting in extreme slowdown or even failure of the server.

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5
- Microsoft IIS 3.0

Evidence: None during the development of this document.

Prevention

Currently the only work around for this issue is to separate the secure content

onto different servers. Microsoft has been notified and has passed the information to the IIS Security and IIS Development teams.

Exploit: NT IIS Double Byte Code Page Vulnerability

Description: This vulnerability could allow a web site viewer to obtain the source code for .asp and similar files if the server's default language (Input Locale) is set to Chinese, Japanese or Korean. How this works is as follows:

IIS checks the extension of the requested file to see if it needs to do any processing before delivering the information. If the requested extension is not on it's list, it then makes any language-based calculations, and delivers the file. If a single byte is appended to the end of the URL when IIS to set to use one of the double-byte language packs (Chinese, Japanese, or Korean) the language module will strip it as invalid, then look for the file. Since the new URL now points to a valid filename, and IIS has already determined that this transaction requires no processing, the file is simply delivered as is, exposing the source code.

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5
- Microsoft IIS 3.0

Evidence:

Request a URL of a known-good file that requires server processing, then append a hex value between x81 and xfe to the URL. For example: <http://myhost/main.asp%81>. If your server is vulnerable you will receive back the source code of your .asp file.

Prevention

Microsoft has re-issued the patch to correct this vulnerability. The original hotfix was found to have a regression error. This patch can be downloaded from the original location, in the following languages at:
English:
ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/fesrc-fix
Simplified Chinese:
ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/chs/security/fesrc-fix
Traditional Chinese:
ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/cht/security/fesrc-fix
Japanese:
ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/jpn/security/fesrc-fix
Korean:
ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/kor/security/fesrc-fix

The patch fixes the problem by checking for single bytes before determining whether any processing is required.

Exploit: NT IIS4 Buffer Overflow Vulnerability

Description: A buffer overflow vulnerability in the way IIS handles requests within .HTM

extensions allows remote attackers to execute arbitrary code on the target machine.

IIS supports a number of file extensions that require futher processing (i.e. .ASP, .IDC, .HTR). Whe a request is made for one of this file types a specific DLL processes it. A stack buffer overflow vulnerability exists in ISM.DLL while handling .HTR, .STM or .IDC extensions. The ISM.DLL filter is installed by default with IIS.

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5

Evidence

Use the following script to test your site:

```
#!/usr/bin/perl
use LWP::Simple;
for ($i = 2500; $i <= 3500; $i++) {
warn "$i\n";
get "http://$ARGV[0]/".('a' x $i).".htr";
}
```

Prevention

Microsoft has made the following fix available:

ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/ext-fix/

Microsoft recommends disabling the script mapping for .HTR files as a workaround:

* From the desktop, start the Internet Service Manager by clicking Start | Programs | Windows NT 4.0 Option Pack | Microsoft Internet Information Server | Internet Service Manager
* Double-click "Internet Information Server"
* Right-click on the computer name and select Properties
* In the Master Properties drop-down box, select "WWW Service", then click the "Edit" button .
* Click the "Home Directory" tab, then click the "Configuration" button .
* Highlight the line in the extension mappings that contains ".HTR", then click the "Remove" button.
* Do the same for .STM and .IDC extensions.
* Respond "yes" to "Remove selected script mapping?" say yes, click OK 3 times, close ISM

eEye has made available a filter patch that will limite .htr request to 255 bytes yet allow normal request to continue to work. The filter and source are available at:

http://www.eeye.com/database/advisories/ad06081999/ad06081999-ogle.html

Exploit: NT IIS Showcode ASP Vulnerability

Description: A sample Active Server Page (ASP) script installed by default on Microsoft's Internet Information Server (IIS) 4.0 gives remote users access to view any file on the same volume as the web server that is readable by the web server.

IIS 4.0 installs a number of sample ASP scripts including one called "showcode.asp". This script allows clients to view the source of other sample scripts via a browser. The "showcode.asp" script does not perform sufficent checks and allows files outside the sample directory to be requested. In particular, it does not check for ".." in the path of the requested file.

The script takes one parameter, "source", which is the file to view. The script's default location URL is:

http://www.sitename.com/msadc/Samples/SELECTOR/showcode.asp

Similar vulnerabilities have been noted in ViewCode.asp, CodeBrws.asp and Winmsdp.exe.

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5
- Microsoft Site Server 3.0
- Microsoft Site Server 3.0 Commerce Edition
- Microsoft Commercial Internet System 2.0

Evidence: None during the development of this document.

Prevention

Do not install the sample code on production servers. If you have installed the sample code remove it or install the patches found at:

- Internet Information Server:
ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/Viewcode-fix/

- Site Server:
ftp://ftp.microsoft.com/bussys/sitesrv/sitesrv-public/fixes/usa/siteserver3/hotfixes-postsp2/Viewcode-fix/

Exploit: NT IIS ISAPI Extension Vulnerability

Description: IIS and potentially other NT web servers have a vulnerability that could allow arbitrary code to be run as SYSTEM. This works because of the way the server calls the GetExtensionVersion() function the first time an ISAPI extension is loaded. Any user able to put a CGI script in the web structure can insert code that will be run as SYSTEM during this window.

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0

- Microsoft BackOffice 4.5
- Microsoft IIS 3.0
- Microsoft IIS 2.0

Evidence: None during the development of this document.

Prevention

Do not allow users to use ISAPI extensions and their own CGI on the same server.

Exploit: NT Using ASP And FSO To Read Server Files Vulnerability

Description: The File System Object (FSO) may be called from an Active Server Page (ASP) to display files that exist outside of the web server's root directory. FSO allows calls to be made utilizing "../" to exit the local directory path.

An example of this syntax would be: http://www.server.foo/showfile.asp?file=../../global.asa

This vulnerability could be used to view the source code of ASP files or stream data into other ASP files on the web server.

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5
- Microsoft IIS 3.0

Evidence: None during the development of this document.

Prevention

Applying appropriate NTFS permissions to limit the access to given to the IUSR_machinename account. For multiple virtual web servers, run each virtual server under a different user account.

Disable the "Allow Parent Paths" option via Internet Services Manager.

Exploit: NT IIS4 Shared ASP Cache Vulnerability

Description: Two separate web servers may be configured to share the same physical directory on an IIS directory. There may be instances where ASP information containing confidential information (from site A) is presented in ASP information served to a user from site B.

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5

Evidence: None during the development of this document.

Prevention

Microsoft has released a patch for this problem:
http://support.microsoft.com/support/kb/articles/q197/0/03.asp?FR=0

As a workaround, Microsoft recommends:

1. Right-click on the virtual directory and select Properties.

2. Select the Home Directory Property Page.

3. Check Run in Separate Memory Space (isolated process).

4. Stop and the restart the Web Sites.

Exploit: NT IIS and Perl - Enumerate Root Web Server Directory Vulnerability

Description: IIS web sites configured to interpret Perl requests can give up the file directory structure of the web server. Create a URL with a bogus perl file ex. www.domain-name.com/scripts/bogus.pl. If this file does not exist, the web server will return an error message listing the directory root of the web server:

CGI Error
The specified CGI application misbehaved by not returning a complete set of HTTP headers. The headers it did return are:
Can't open perl script "C:\InetPub\scripts\bogus.pl": No such file or directory

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5
- Microsoft IIS 3.0
- Microsoft IIS 2.0

Evidence: None during the development of this document.

Prevention

Use the ISAPI version of Perl - perlis.exe. In IIS4, configure IIS to check for the existence of this file before giving the error message.

Exploit: NT IIS4 DoS - ExAir Sample Site Vulnerability

Description: An IIS4 sample site "ExAir" has three ASP pages, that if called directly without having the sample site dlls running, will cause the server CPU to increase to 100%. These pages include:

Exair - root/search/advsearch.asp
Exair - root/search/query.asp
Exair -root/search/search.asp

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5

Evidence: None during the development of this document.

Prevention

Do not install sample sites when creating an IIS server. Delete all files and directories that contain sample site pages.

Exploit: NT IIS FTP DoS / Buffer Overflow Vulnerability

Description: There is a Denial of Service / Buffer Overflow condition in Microsoft IIS4 FTP service when using the NLST command. A user having user or anonymous access to the FTP server may initiate this attack.

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5
- Microsoft IIS 3.0

Evidence:

Connecting to the FTP server and issuing an ls command with 316 characters will cause the inetinfo.exe service to crash (and the connection to be reset). Passing more than 316 characters will cause the stack to be overwritten. Up to 505 characters may be passed.

Prevention

For IIS 4.0, install the following Post SP4 hotfix: ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/ftpls-fix/Ftpls4i.exe

For IIS 3.0, install the following Post SP4 hotfix: ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/ftpls-fix/Ftpls3i.exe

Exploit: NT IIS4 Log Avoidance Vulnerability

Description: An http get request against an IIS4 server will not be logged if the request is longer than 10150 bytes long.

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5

- Microsoft IIS 3.0

Evidence: None during the development of this document.

Prevention

None

Exploit: NT IIS4 Remote Web-Based Administration Vulnerability

Description: Web-based administration for IIS 4.0 is, by default, limited to the local loopback address, 127.0.0.1. In instances where IIS4.0 was installed as an upgrade to IIS 2.0 or 3.0, a legacy ISAPI DLL (ISM.DLL) is left in the /scripts/iisadmin directory. An attacker may call this DLL via the following syntax:

http://www.server.com/scripts/iisadmin/ism.dll?http/dir

This URL prompts the user for a username/password to access the remote administration console. Although approved access does not permit the user to commit changes to the IIS server, it may allow them to gather sensitive information about the web server and its configuration.

VERSIONS EFFECTED

- Microsoft IIS 4.0
- Microsoft Windows NT 4.0
- Microsoft BackOffice 4.5

Evidence: None during the development of this document.

Prevention

Delete the ISM.DLL from the /scripts/iisadmin directory.

Application Attacks

Exploit: Microsoft Excel SYLK Macro Execution Vulnerability

Description: When a symbolic link (SYLK) file containing a macro is opened by Excel 97 or Excel 2000, the user is not warned that a macro will be executed upon opening the file (as is customary when Excel opens other spreedsheet files containing macros.) SYLK files are basic ascii files that can be read by a variety of applications, including word processors and other spreadsheet applications. SYLK files can be created using the "Save As" function in Microsoft Excel.

VERSIONS EFFECTED

- Microsoft Excel 97 SR2
- Microsoft Excel 97 SR1
- Microsoft Excel 97
- Microsoft Excel 2000
- Microsoft Office 97
- Microsoft Office 2000

Evidence

See Discussion

Prevention

Microsoft has released a patch for this vulnerability. It is available at:

- Excel 97:
http://officeupdate.microsoft.com/downloadDetails/Xl8p7pkg.htm
- Excel 2000:
http://officeupdate.microsoft.com/2000/downloadDetails/XL9p1pkg.htm

Exploit: Microsoft Excel File Import Macro Execution Vulnerability

Description: When Excel 97 opens a Lotus 1-2-3 or Quattro Pro file containing a macro, the user is not warned that a macro will be executed upon opening the file (as is customary when Excel opens other spreedsheet files containing macros.)

VERSIONS EFFECTED

- Microsoft Excel 97 SR2
- Microsoft Excel 97 SR1
- Microsoft Excel 97
- Microsoft Office 97

Evidence

See Discussion

Prevention

Microsoft has released a patch for this vulnerability. It is available at:

- Excel 97:
http://officeupdate.microsoft.com/downloadDetails/Xl8p7pkg.htm
- Excel 2000:
http://officeupdate.microsoft.com/2000/downloadDetails/XL9p1pkg.htm

Exploit: Microsoft JET Text I-ISAM Vulnerability

Description: Microsoft's JET database engine includes functionality referred to as Text I-ISAM. This allows the JET driver to write to a text file for another application to read later. This was implemented to allow data sharing between JET applications and other applications that don't support Dynamic Data Exchange. A vulnerability exists in that any text file can be written to, including system files. A database query could be created that adds destructive commands to a startup file or script.

VERSIONS EFFECTED

Microsoft JET 4.0
+ Microsoft Access 2000
Microsoft JET 3.51

+ Microsoft Excel 97
  - Microsoft Windows 98
  - Microsoft Windows 95
  - Microsoft Windows NT 4.0

Microsoft JET 3.5

+ Microsoft Access 97
  - Microsoft Windows 98
  - Microsoft Windows 95
  - Microsoft Windows NT 4.0

Evidence: None during the development of this document

Prevention

Microsoft has released a patch for this issue. To quote Microsoft advisory MS99-030:

- http://officeupdate.microsoft.com/articles/mdac_typ.htm

NOTES:
The above web site provides separate pages for Office97 and Office2000. This is done in order to provide specific information about the vulnerabilities affecting the products. The patch for Office97 and Office2000 (and indeed for all affected products) is exactly the same, and both pages link to exactly the same patch. The patch will determine what version(s) of Jet are present on the machine and apply all of the needed corrections. The patch is suitable for use by all language packs. The patch applies to Jet 3.5 and all subsequent versions. Older versions of Jet are no longer supported, and we recommend that affected customers upgrade to a supported version. The patch is suitable for widespread deployment via Microsoft(r) Systems Management Server(r). Users who wish to manually apply patches for specific versions of Jet should consult the FAQ for information on how to do this.

Windows NT Resource Kit

The following are Microsoft sanctioned utilities that install with the Windows NT 4.0 Resource Kits. This following should be used as a quick overview of the utilities available, and a brief description of their functionality. The Windows NT 4.0 Resource Kit contains a variety of utilities that can be use to help prevent, deter, and detect intrusion into your system. Always read and understand the respective documentation for a full explanation of features before attempting to use them.

Program	Usage	Location
3DPAINT.EXE	3DPAINT is a paint utility that enables you to create three-dimensional bitmap graphics.	GUI
ADDUSERS.EXE	Add Users for Windows NT is a 32-bit administrative command-line tool used to create or write user accounts to a comma-delimited file. Add Users is most beneficial when the file is maintained in a spreadsheet, such as Microsoft Excel, that will work with comma-delimited files. Typical use includes the batch creation of multiple NT user accounts.	COMMAND-LINE
ANIEDIT.EXE	Microsoft Animated Cursor Editor. Use the animated cursor creator to draw and edit frames to create animated cursors.	GUI
APIMON.EXE	This command-line tool enables the user to monitor the API calls a process is making. APIMON incorporates the functionality of Application Profiler, which is being dropped from the Windows NT 4.0 Resource Kit.	COMMAND-LINE
ASSOCIATE.EXE	This command-line utility enables you to register or un- register a filename extension with the Registry. "File extension, executable program" associations enable the Windows NT 4.0 shell to start the correct executable program when a file with the associated extension is opened from the command line or from Explorer.	COMMAND-LINE
ATANLYZR.EXE	ATANLYZR performs an AppleTalk lookup for registered AppleTalk devices on an AppleTalk network. The user can perform a lookup of all AppleTalk devices, specific Net, Name, Type, or partial Name, and Types in the selected zone(s).	
AUDITCAT.HLP	This Windows Help file displays information on seven categories of audit events.	HELP FILE
AUTOEXNT.EXE	The AutoExNT service allows you to start a batch file, AUTOEXNT.BAT, at boot time without having to log on to the computer on which it will run.	COMMAND-LINE
AUTOLOG.EXE	Windows NT Auto Logon Setter is a simple GUI utility, which configures a Windows NT Workstation to automatically log on a particular user at bootup. This enables you to bypass the CTRL+ALT+DEL logon dialog box.	GUI

BREAKFTM.EXE	This command-line utility was designed to be used with Windows NT Server 4.0 Unattended Upgrade. Windows NT computers that have the system drive mirrored cannot be upgraded, as a mirrored system drive will cause the Unattended Upgrade to fail. The mirror must therefore be broken before upgrading. BREAKFTM breaks the system mirror before the Windows NT Server 4.0 upgrade, and then recreates the mirror once the upgrade is finished. The tool has no effect on computers that do not have a system mirror.	COMMAND-LINE NT SERVER ONLY
BROWMON.EXE	The Browser Monitor is a Windows-based utility that monitors the status of browsers on selected domains. Browsers are shown on a per-domain and per-transport basis.	GUI
BROWSTAT.EXE	BrowStat is a general purpose, character-based browser diagnostic. Use BrowStat to find whether a browser is running and to find active Microsoft Windows for Workgroups 1.0 (WFW) browsers in Windows NT domains. This utility provides information about the state of the browser in a workgroup, including the name of the master browser.	COMMAND-LINE
C2CONFIG.EXE	The Windows NT C2 Configuration Manager displays the various C2 security parameters and their current configuration. Selecting one of these items will display more information on the configuration of that item and allow you to change the configuration as desired.	GUI
CAT.EXE	Posix utility that reads files sequentially, writing them to the standard output.	COMMAND-LINE
CHMOD.EXE	Posix utility that modifies the file mode bits of the listed files as specified by the mode operand.	COMMAND-LINE
CHOICE.EXE	CHOICE prompts the user to make a choice in a batch program by displaying a prompt and pausing for the user to choose from among a set of keys. You can use this command only in batch programs.	COMMAND-LINE
CHOWN.EXE	Posix utility to change the owner of a file.	COMMAND-LINE
CLIP.EXE	CLIP.EXE dumps STDIN to the Windows NT Clipboard. Run any program that prints text to STDOUT and pipe the results through Clip. Clip will read from its STDIN and copy the text to the Clipboard.	COMMAND-LINE
COMPREG.EXE	A Win32 character-based/command-line "Registry DIFF" that enables you to compare any two local and/or remote Registry keys in both Windows NT and Windows 95.	COMMAND-LINE
COMPRESS.EXE	This command-line utility can be used to compress one or more files.	COMMAND-LINE
CP.EXE	Posix command to copy files.	COMMAND-LINE
Crystal Reports for NT Resource Kit	Windows-based WYSIWYG report writer for formatting reports from the NT Event Log. Included are a number of sample reports that can be refreshed with data from the local machine.	MULTI-FILE APPLICATION
DATALOG.EXE	The Performance Monitor Service, invoked by the MONITOR.EXE utility. This service runs on the computer on which it is started. Alerts are watched locally on that computer, so no data needs to travel across the network.	COMMAND-LINE

dbWeb	dbWeb is a gateway between Microsoft Open Database Connectivity (ODBC) data sources and the Internet Information Server (IIS). You can use dbWeb to publish data from an ODBC data source and provide familiar World Wide Web (WWW) hypertext navigation. While allowing users to create queries, dbWeb enables you to filter the data and sources users can access and display.	GUI
DELPROF.EXE	This command-line utility deletes user profiles on Windows NT computers.	COMMAND-LINE
DELSRV.EXE	This command-line utility un-registers a service with the service control manager.	COMMAND-LINE
Designed for Windows NT and Windows 95 Logo Handbook (WINLOGO.DOC)	The "Designed for Windows NT and Windows 95 Logo Handbook for Software Applications" describes the technical requirements that must be satisfied by an application in order to receive the Designed for Windows NT and Windows 95 logo	
Desktop Themes	Desktop Themes include a variety of visual, sound, and symbolic components that can enhance the look and feel of your Windows NT 4.0 desktop. Each desktop theme includes a background wallpaper, a screen saver, a color scheme, and a set of sounds, cursors, icons, and fonts.	UI ENHANCEMENTS
DESKTOPS.EXE	This desktop-switching application for Windows NT 4.0 enables you to customize desktop wallpaper and colors and separate executing programs into new deskspaces.	GUI
DFLAYOUT.EXE	This layout tool for document files enables you to optimize compound files for better performance on the World Wide Web.	GUI
DH.EXE	This command-line utility enables your to lock heaps, tags, stacks, and objects.	COMMAND-LINE
DHCPCMD.EXE	The command-line DHCP Administrator's Tool is an auxiliary method of administering DHCP servers.	COMMAND-LINE
DHCPLOC.EXE	DHCPLOC.EXE displays the DHCP servers active on the subnet. It beeps and sends out alert messages if it detects any unauthorized DHCP servers. It also displays packets it detects from DHCP servers; you can specify whether it displays packets from all DHCP servers, or only from unauthorized servers.	COMMAND-LINE
DIRUSE.EXE	This utility will traverse the named directory and it's subs to give you disk space usage for the specified directory tree.	COMMAND-LINE
DISKMAP.EXE	This command-line utility produces a detailed report on the configuration of the hard disk that you specify. It provides information from the Registry about disk characteristics and geometry, and reads and displays data about all of the partitions and logical drives defined on the disk.	COMMAND-LINE

DSKPROBE.EXE	DiskProbe is a sector editor for Windows NT Server and Workstation. It allows a user with local Administrator rights to directly edit, save and copy data on the physical hard drive that is not accessible in any other way. You can use DiskProbe to replace the Master Boot Record, repair damaged partition table information and to repair or replace damaged Partition Boot Sectors or other file system data. The program can also save Master Boot Records and Partition Boot Sectors as files. They can then be replaced if the sectors become damaged at a later time. These on-disk data structures are not accessible through the file system, and so are not saved by any backup programs currently available.	GUI
DISKSAVE.EXE	DISKSAVE allows you to save the Master Boot Record and Partition Boot Sector as binary image files. Once these critical disk structures have been saved, they can be easily restored if they become corrupted later on. This tool also enables you to disable fault tolerance on the Boot Drive, which can be useful when Windows NT will not boot from a mirrored system drive.	COMMAND-LINE
DNSSTAT.EXE	This command-line utility provides a dump of DNS server statistics (queries and responses, database size, caching, memory consumption) on a computer running Microsoft DNS Server.	COMMAND-LINE
DOMMON.EXE	Domain Monitor is a Windows-based utility that monitors the status of servers in a domain and the secure channel status to the domain controller and to domain controllers in trusted domains. Domain Monitor displays various status errors, plus the domain controller name and a list of trusted domains.	GUI
DRIVERS.EXE	The Drivers tool displays character-based information about the installed device drivers. There are no command-line arguments.	COMMAND-LINE
DSKPROBE.EXE	DiskProbe is a sector editor for Windows NT Server and Workstation. It allows a user with local Administrator rights to directly edit, save and copy data on the physical hard drive that is not accessible in any other way.	GUI
DUMPEL.EXE	Dump Event Log is a command-line utility that can be used to dump an event log for a local or remote system into a tab-separated text file. This utility can also be used to filter for certain event types or to filter out certain event types.	COMMAND-LINE
EM2MS.EXE	This command-line utility converts verbose descriptions of files stored on NT-based EMWAC (European Microsoft Windows NT Academic Centre) Gopher Servers to the Microsoft Internet Information Gopher Server content format. EM2MS.EXE is useful for EMWAC Gopher Server administrators who want to begin using the Microsoft Internet Information Gopher Server. It allows them to easily convert their EMWAC-based content descriptions to the Microsoft Gopher tag-file format.	COMMAND-LINE

EMWAC Server CGI Gateway Scripts	A gateway script is an executable program that uses the CGI protocol, Common Gateway Interface, to communicate with a server on the World-Wide Web. Gateway scripts add custom features to a Web server, increasing the diversity of services that a Web server can provide to the Web browser. The example gateway script provided in the Resource Kit demonstrates how to provide access to the Microsoft SQL Server. The script accepts a single SQL statement, which it passes on to SQL Server. The results, including any error messages, are returned to the browser for display to the user.	COMMAND-LINE
ENUMPRN.EXE	Windows utility to display installed printer drivers.	GUI
EXCTRLST.EXE	This utility provides information on the Extensible Performance Counter DLLs that have been installed on a Windows NT computer, listing the services and applications that provide performance information via the Windows NT Registry. You can use these performance counters for optimizing and troubleshooting.	COMMAND-LINE
EXETYPE.EXE	ExeType is an MS-DOS-based application that identifies the operating system environment and processor required to run a particular executable file.	COMMAND-LINE
EXPNDW32.EXE	You can use the File Expansion Utility to expand one or more compressed files from the Windows NT CD. EXPNDW32.EXE is a 32-bit utility that provides a fully graphical interface for ease of use.	COMMAND-LINE
FIND.EXE	Find recursively descends the directory tree for each file listed, evaluating an expression (composed of a rich set of arguments) in terms of each file in the tree.	COMMAND-LINE
FINDGRP.EXE	The Find Group utility finds all direct and indirect group memberships for a specified user in a domain. This helps determine a particular users access to Windows NT Domain Controllers in a domain by listing the groups in which the user is a member.	COMMAND-LINE
FLOPLOCK.EXE	FloppyLock is a service that controls access to the floppy drives of a computer. When the service is started on Windows NT Workstation, only members of the Administrators and Power Users groups can access the floppy drives. When the service is started on Windows NT Server, only members of the Administrators group can access the floppy drives. Install via INSTSRV.EXE.	SERVICE
FORFILES.EXE	This command-line utility can be used in a batch file to select files in a folder or tree for batch processing. FORFILES enable you to run a command on or pass arguments to multiple files. For example, you could run the TYPE command on all files in a tree with the *.TXT extension. Or you could execute every batch file (*.BAT) on the C:\ drive with the filename "MYINPUT.TXT" as the first argument.	COMMAND-LINE
FREEDISK.EXE	This command-line utility checks for free disk space, returning a 0 If there is enough space and a 1 if there isn't.	COMMAND-LINE BATCH/SCRIPT

FTEDIT.EXE	FTEDIT.EXE is a new GUI utility that allows you to create, edit, and delete fault tolerance sets for disk drives and partitions of local and remote computers. It improves on the functionality of the command-line utility SHOWDISK.EXE.	GUI
FTPCONF.EXE	Windows-based utility to configure your Microsoft FTP Server.	GUI
GETMAC.EXE	Command-line utility to display network transports and address information.	COMMAND-LINE
GETSID.EXE	This utility which returns the SID information for any two system accounts.	COMMAND-LINE
GLOBAL.EXE	This command-line utility displays members of global groups on remote servers or domains.	COMMAND-LINE
GREP.EXE	Posix utility (Global Regular Expression Print) to search one or more files for lines that match a regular expression.	COMMAND-LINE
GRPCOPY.EXE	This GUI utility enables users to copy the usernames in an existing group to another group in the same or another domain or on a Windows NT computer. It is included in the Windows NT Server Resource Kit only.	GUI
GRPTOREG.EXE	This tool creates group files for Program Manager and converts them to the Registry for use in Windows NT.	COMMAND-LINE
HCL40.HLP	Hardware Compatibility List in Windows Help format.	HELP FILE
HEAPMON.EXE	This command-line tool enables the user to view system heap information.	COMMAND-LINE
IFMEMBER.EXE	IfMember is a command-line utility that checks whether the current user is a member of a specified group. It is typically used in Windows NT Workstation and Windows NT Server logon scripts and other batch files.	COMMAND-LINE
IMAGEDIT.EXE	The Image Editor allows you to create and edit cursors and icons for VGA, monochrome, and other display devices. The Image Editor is also used with aniedit.exe to create custom animated cursors.	GUI
Index Server	Index Server is the Microsoft content-indexing and searching solution for Microsoft Internet Information Server (IIS), which is included with Windows NT Server 4.0, and Peer Web Services (PWS), which is included with Windows NT Workstation 4.0. An add-on module for IIS and PWS, Index Server is designed to index the full text and properties of documents on an IIS or PWS-based server. Index Server can index documents for both corporate intranets and for any drive accessible through an uniform naming convention (UNC) path on the Internet. Clients can formulate queries by using any World Wide Web (WWW) browser to fill in the fields of a simple Web query form. The Web server forwards the query form to the query engine, which finds the pertinent documents and returns the results to the client formatted as a Web page. Unlike many content indexing systems, Index Server can index the text and properties of formatted documents, such as those created by Microsoft® Word or Microsoft® Excel. This feature lets you publish existing documents on your intranet Web without converting them to HyperText Markup Language (HTML).	MULTI-FILE APPLICATION NT SERVER ONLY

INET.EXE	INET is a network command that works like the Windows NT NET command, except that UNC names are assumed to be Internet Domain Name Server (DNS) names and translated accordingly. Inet works on TCP/IP services rather than on SMB.	COMMAND-LINE
INSTALL.CMD	INSTALLD.CMD installs NTDETECT.CHK, the debug or checked version of NTDETECT.COM, from the Windows NT CD.	See related topic NTDETECT.COM
INSTSRV.EXE	INSTSRV.EXE: Service Installer is a command-line utility that installs and uninstalls executable (.EXE) services and assigns names to them.	COMMAND-LINE
KERNPROF.EXE	This command-line utility provides counters for and profiles of various functions of the Windows NT operating system Kernel. With Kernel Profiler, you can monitor details and frequency for each function the Kernel calls, how often a process switches from User mode to Kernel mode, and, on a multi-processor computer, display information for each processor.	COMMAND-LINE
KILL.EXE	KILL.EXE is a command-line utility you can use to end one or more tasks, or processes. When using KILL.EXE, you can specify a process by its process ID number, any part of its process name, or its window title, if it has a window. You can use the TLIST.EXE utility, also included with this Resource Kit, to find the process names and process IDs of currently running processes.	COMMAND-LINE
KIX32.EXE	KiXtart 95 is a logon script processor and/or enhanced batch language for Windows NT and Windows 95 workstations in a Windows Networking environment.	BATCH/SCRIPT
LAYOUT.DLL	This utility is a shell extension that saves and restores the icon positions on a desktop.	EXPLORER EXTENSION
LN.EXE	Posix utility which allows you to create pseudonyms (links) for files, allowing them to be accessed by different names.	COMMAND-LINE
LOCAL.EXE	This command-line utility displays members of local groups on remote servers or domains.	COMMAND-LINE
LOGEVENT.EXE	LogEvent enables entries to be made to the Windows NT Event Log on either the local or a remote machine from the command line or a batch file.	COMMAND-LINE
LOGTIME.EXE	A command-line tool that logs the start or finish of command-line programs from a batch file. This can be useful for timing and tracking batch jobs such as mail-address imports.	COMMAND-LINE
LS.EXE	Posix utility to list files.	COMMAND-LINE
Mail Server	Mail Server is an SMTP and POP server for Windows NT. The intermediate files and the mailboxes are all spooled securely (when using the NTFS file system) on the computer running Windows NT server, and can be accessed by any POP-compliant public-domain (PD) or commercial client.	MULTI-FILE APPLICATION
MIBCC.EXE	MIB (Management Information Base) compiler for SNMP (Simple Network Management Protocol).	COMMAND-LINE
MKDIR.EXE	Posix utility to create one or more directories.	COMMAND-LINE

MONITOR.EXE	Command-line interface to the Performance Monitor service. The activity being monitored is described in a workspace settings file that you create using Performance Monitor. You use monitor.exe to start, stop, and to establish a particular workspace settings file describing the measurement. You can run monitor.exe from a remote computer, so complete control of all your Performance Monitor services is available from any Windows NT computer on the network.	COMMAND-LINE
MUNGE.EXE	This utility provides a convenient way to search for and replace strings in a file.	COMMAND-LINE
MV.EXE	Posix utility to move file and directories or to rename them.	COMMAND-LINE
NETCLIP.EXE	NetClip is a GUI utility that enables you to view the contents of another computer's clipboard, and to Drag & Drop (or Cut & Paste) any data, in any format, to and from the other computer.	GUI
NETSVC.EXE	Command-line utility which remotely controls and displays status of a specified service on a given computer.	COMMAND-LINE
NetTime for Macintosh	This Macintosh program synchronizes the local Macintosh clock to a given AppleShare server on the network. It requires ResEdit or another resource editor to change the zone and server name for the tool to synchronize to.	MACINTOSH
NETWATCH.EXE	Windows-based utility, which provides general system, user, share and file information on local and remote resources.	GUI
NLMON.EXE	This command-line utility can be used to list and test many aspects of Trust relationships.	COMMAND-LINE
NLTEST.EXE	This command-line tool helps perform administrative tasks such as forcing a user-account database into sync, getting a list of PDC's, forcing a shutdown, querying and checking on the status of trust.	COMMAND-LINE
NOW.EXE	Similar to ECHO, this command will display date and time stamp information followed by the given string argument. Useful in batch file debugging or possibly batch performance monitoring.	COMMAND-LINE
NTCARD40.HLP	Windows NT Adapter Card Help was created by Microsoft Product Support to assist you in the setup of network adapters, SCSI adapters, and sound cards for Windows NT 4.0. This file provides IRQ, I/O base, RAM base address, and other settings, along with illustrations that show the location for jumper settings on the cards.	HELP FILE
NTDETECT.COM	INSTALLD.CMD installs NTDETECT.CHK, the debug or checked version of NTDETECT.COM, from the Windows NT CD.	
NTUUCODE.EXE	NTUUCODE is a 32-bit GUI program that you can use to encode or decode files according to the UUEncoding standard.	GUI
OLEVIEW.EXE	This administration and testing tool for Microsoft Component Object Model (COM) classes is oriented towards developers and power users. The user interface, however, offers both "Expert" and "Novice" modes. OLE/COM Object Viewer enables you to browse, configure, activate, and test all of the COM classes installed on your computer. You can also configure system-wide COM settings, including enabling or disabling Distributed COM, and activate COM classes remotely. The new Component Categories specification is fully supported.	GUI

OS2API.TXT	The OS2API.TXT file contains information for developers describing which APIs for the OS/2 operating system are supported by Windows NT 4.0 and which are not supported.	DEVELOPER DOC
PASSPROP.EXE	This command-line tool can be used to set two domain policy flags: whether passwords have to be complex and whether the administrator account can be locked out. These domain password and security properties cannot be set by any other tool, including the NET command and User Manager.	COMMAND-LINE
PATHMAN.EXE	This command-line tool enables you to add or remove components of both the system and user paths. It can modify any number of paths in a single call and includes error checking that can handle path abnormalities such as repeated entries, adjacent semicolons, and missing entries.	COMMAND-LINE
PERF2MIB.EXE	Using PERF2MIB.EXE: Performance Monitor MIB Builder Tool, developers can create new ASN.1 syntax MIBs for their applications, services, or devices that use Performance Monitor counters. Administrators can then track performance of these components using any system-management program that supports SNMP.	COMMAND-LINE
PerfLog Data Log Service	This tool logs data from performance counters to tab or comma-separated variable files. It lets you choose which performance counters you want to log, and starts new log files automatically at intervals you select. The text files to which PerfLog logs data can be used as input to spreadsheets, databases, and other applications, as well as to Performance Monitor. Unlike Performance Monitor logs, which store data in a compact, multi-dimensional C-language data format, PerfLog logs can be used as direct input without reformatting. PerfLog uses the same objects and counters as Performance Monitor (included with the Windows NT operating system), but it lets you select which counters you want to log for each instance of an object. You can also select the level of detail you need on an instance and let PerfLog select a set of counters for you.	SERVICE
PERFMTR.EXE	Command-line performance monitor which displays CPU, memory, cache, and I/O usages, VdM and server statistics until user terminates the display.	COMMAND-LINE
Performance Tools	The \PERFTOOL folder of the installed Resource Kit contains tools for monitoring and optimizing the performance of a computer running Windows NT or a Windows NT application. Several of these tools are also covered in separate topics in this Help file. The Performance Tools are grouped into folders by function. A few of these tools are listed in more than one sub-folder. The \EXAMPLES folder is not installed by default because it contains over 20 MB of files.	
PERL	Practical Extraction and Report Language. Perl is an interpreted language optimized for scanning arbitrary text files, extracting information from those text files, and printing reports based on that information. It's also a good language for many system management tasks.	
PERMCOPY.EXE	This command-line utility copies file- and share-level permissions.	COMMAND-LINE

PERMS.EXE	Command-line utility which displays specified users' permissions for a given file.	COMMAND-LINE
PFMON.EXE	This utility enables you to monitor the page faults that occur as you run an application. Page Fault Monitor produces a running list of hard and soft page faults generated by each function call by the application.	COMMAND-LINE
PMON.EXE	Command-line utility which displays process statistics. Useful in troubleshooting system resource problems, etc..	COMMAND-LINE
POLEDIT.EXE	This utility sets administrative policies to override user behavior.	GUI
PSTAT.EXE	Version 0.2 of this command-line utility displays process statistics. Useful for debugging problems.	COMMAND-LINE
PULIST.EXE	This command-line tool tracks what processes are running on local or remote computers. It can list the names and process IDs of all processes running on one or more remote systems. If run against the local computer (with no arguments specified), PULIST will also try to list the user name associated with each process.	COMMAND-LINE
PVIEWER.EXE	Windows-based process management tool, which allows for process termination and priority boosting and downgrading.	GUI
QSLICE.EXE	Windows-based tool which shows the amount of CPU used by each process in the system.	GUI
QUICKRES.EXE	This tool enables you to change the visible screen area, resolution (DPI), bit depth, and color palette settings from the taskbar, without restarting Windows NT.	GUI
QUICKRUN.EXE	This utility provides a convenient method of launching Windows applications.	GUI
RASLIST.EXE	This command-line utility displays RAS server announces from a network.	COMMAND-LINE
RASUSERS.EXE	RasUsers lets you list all user accounts that have been granted permission to dial in to the network via Remote Access Service (RAS).	COMMAND-LINE
RCMD.EXE	Remote Command allows a user to execute a single command on a remote server from within a command shell. If the command is supplied then the shell executes the command once before exiting the shell. If command is not supplied, it leaves the user in an interactive session until explicitly exited or session is otherwise broken.	COMMAND-LINE
REGBACK.EXE	Allows user with SeBackupPriviledge the ability to back up a servers'registry hives (without the use of tape) while they are in use. Options are available to back up a single hive or all at once. Error exit codes reflect success, failure or other. Recommended use prior to any changes to the registry.	COMMAND-LINE
REGCHG.EXE	This command-line utility makes changes to the Registry on the local or a remote system.	COMMAND-LINE
REGDEL.EXE	This command-line and batch utility removes Registry keys remotely or on the local computer.	COMMAND-LINE
REGENTRY.HLP	his tool provides a database of Windows NT Registry entries in the form of a Help file. You can use this Help file while working in Registry Editor to find ranges, minimum-maximum values, and instructions for setting specific values in the Registry.	HELP FILE

Regina REXX	Regina REXX is a full scripting language with Registry access, event log functions, and OLE automation support.	BATCH/SCRIPT
REGINI.EXE	Command-line utility which makes changes to the Registry based on a script. Good for Setup programs.	COMMAND-LINE
REGKEY.EXE	Supports interactive setting of Logon and FAT file system settings including parsing of AUTOEXEC.BAT for SET/PATH commands.	COMMAND-LINE
REGREAD.EXE	This command-line utility reads the Registry, parses out values, and outputs them to the screen.	COMMAND-LINE
REGREST.EXE	Used in conjunction with regback.exe, this command-line utility will restore registry hives from backup files and is effective upon system reboot. User must have SeRestorePriviledge to execute this command.	COMMAND-LINE
REGSEC.EXE	This command-line utility removes the Everyone group from a Registry key. Removing the Everyone group can enable you to implement stricter and more specific security.	COMMAND-LINE
REGTOGRP.EXE	Creates a Windows NT specific .GRP file in the current directory for each of your Program Manager groups. This file is not compatible with MS-DOS Windows. (Must be used with GRPTOREG.EXE.)	COMMAND-LINE
Remote Access Manager	Remote Access Manager, by virtual motion, enables network managers to manage Remote Access Service (RAS) on a per-user, RAS server, or port basis. You can control RAS resources via LAN or dial-up access. With Remote Access Manager, you can: display RAS server and port status. Disconnect RAS sessions from any port. enable or disable RAS privileges for any user.	MULTI-FILE APPLICATION
Remote Console	Remote Console is a client/server application that enables you to run a command-line session remotely, within which you may launch any other application.	
REMOTE.EXE	Command-line utility to provide remote command-line access to start either the Client or Server end of Remote.	COMMAND-LINE
Remote Kill	This service (RKILLSRV.EXE) with both GUI (WRKILL.EXE) and command-line (RKILL.EXE) clients allows a user to enumerate and kill processes on a remote computer. To kill a process remotely with this tool, you must be member of the Administrators group.	COMMAND-LINE /GUI
RESTKEY.EXE	This command-line utility enables you to restore a Registry key from a file.	COMMAND-LINE
RIPROUTE.WRI	This Microsoft Write document explains how you can use Windows NT Server, along with Windows NT Server Multi-Protocol Routing, to connect local area networks (LANs) together or local area networks to wide area networks (WANs) without needing to purchase a dedicated router.	DOCUMENT NT SERVER ONLY
RM.EXE	POSIX command-line utility for file deletion or removal.	COMMAND-LINE
RMDIR.EXE	POSIX command-line utility for directory deletion or removal.	COMMAND-LINE
RMTSHARE.EXE	RMTSHARE.EXE is a command-line utility that allows you to set up or delete shares remotely.	COMMAND-LINE

ROBOCOPY.EXE	A robust file copy command which includes switches for including populated and unpopulated subdirectories, adjusting attributes, setting date and time stamps, establishing wait and retry intervals, establishing exclusion clauses, and moving subdirectories after copy.	COMMAND-LINE
RREGCHG.EXE	This command-line and batch utility creates or changes Registry settings on a remote computer. It is useful for making global Registry changes over a network.	COMMAND-LINE
RSHSVC.EXE	RSHSVC.EXE is the server side for the TCP/IP utility rsh.exe. It works the same way as the UNIX remote Shell Service. RSH clients can access this service from both NT and UNIX machines.	SERVICE
SAVEKEY.EXE	This command-line utility enables you to save a Registry key to a file.	COMMAND-LINE
SC.EXE	This tool provides a way to communicate with the Service Controller (the SERVICES.EXE process) from the command prompt.	COMMAND-LINE
SCANREG.EXE	A Win32 character-based/command-line "Registry GREP" that enables you to search for any string in keynames, valuenames, and/or valuedata in local or remote Registries keys in both Windows NT and Windows 95.	COMMAND-LINE /GUI
SETUPMGR.EXE	Creates an answer file of system and licensing information for unattended product installation/upgrade.	COMMAND-LINE
SCLIST.EXE	This command-line tool can show currently running services, stopped services, or all services on a local or remote computer.	COMMAND-LINE
SCOPY.EXE	Command-line utility which copies files to and from NTFS partitions while keeping file permissions intact. User must have Backup and Restore file security rights on both the source and destination directories. Not compatible with FAT, HPFS or any other non-secured file system.	COMMAND-LINE
SECADD.EXE	This command-line utility enables you to add user permissions to a Registry key.	COMMAND-LINE
SECEDIT.EXE	This GUI security-context editor allows you to modify security privileges of the logged-on user and running processes, and to list the security contexts that are in use.	GUI
SETX.EXE	A command-line utility that offers a batch method for setting environmental variables in the user or machine environment from a variety of sources, without any programming or scripting. Besides taking both the variable and value from the command line, it can also take values from Registry keys and offsets into text files.	COMMAND-LINE
SH.EXE	POSIX utility for creation of a command shell.	COMMAND-LINE
ShareUI	This stand-alone extension of Explorer makes it easier to manage network shares. ShareUI is a special shell folder that allows you to view, add, remove, and configure the properties of network shares for any local or remote machine that you have permission to administer. Network shares are objects that represent shared directories on a computer.	EXPLORER EXTENSION
SHOWACLS.EXE	This command-line utility enumerates access rights for files, folders, and trees. It allows masking to enumerate only specific ACLs.	COMMAND-LINE

SHOWDISK.EXE	This command-line utility reads and displays the Registry Subkey HKEY_LOCAL_MACHINE\SYSTEM\DISK. This Subkey contains information about each of the primary partitions and logical drives defined on the computer. It also identifies which of the primary partitions and logical drives are members of volume sets, stripe sets, mirror sets, and stripe sets with parity.	COMMAND-LINE
SHOWGRPS.EXE	This command-line tool displays group information for a specified user.	COMMAND-LINE
SHUTDOWN.EXE	Third-party utility, which allows a user to shutdown a local or remote server with command-line, options support.	COMMAND-LINE
SHUTGUI.EXE	SHUTGUI.EXE allows you to remotely shut down or reboot a computer running Windows NT. It can be run either with command-line parameters or without.	COMMAND-LINE /GUI
SLEEP.EXE	Command-line utility which executes a pause for a specified amount of time in seconds. Useful in batch processing.	COMMAND-LINE
SMBTRACE.EXE	Executes an SMB packet trace from the server or redirector. Includes command-line option support.	COMMAND-LINE
SNMPMON.EXE	SNMP Monitor is a utility that can monitor any SNMP MIB variables across any number of SNMP nodes. It can then optionally log query results to any ODBC data source (such as SQL Server), automatically creating any necessary tables. Logging can be enabled for all queries or limited to particular thresholds, and thresholds can be either edge or level triggered.	GUI
SNMPUTIL.EXE	Command-line browsing utility which allows you to get SNMP information from an SNMP host on your network.	COMMAND-LINE
SOON.EXE	SOON.EXE is a command scheduling utility which runs an AT command in the near future. The delay is set in seconds and can run commands locally or remotely.	COMMAND-LINE
SRVANY.EXE	This utility allows running Windows NT applications as services.	COMMAND-LINE
SRVCHECK.EXE	This command-line utility lists the non-hidden shares on an computer running Windows NT and enumerates the users on the ACL's for that share.	COMMAND-LINE
SRVINFO.EXE	This command-line utility displays information about a remote server.	COMMAND-LINE It is included in the Windows NT ServerResource Kit only.
SRVINSTW.EXE	The Service Installation Wizard provides an easy method of installing or deleting services and device drivers. It can connect to and configure services on both local and remote computers.	GUI
SRVMGR.EXE	Windows-based remote server administration tool.	GUI

SU.EXE SYSDIFF.EXE	SU lets you start a process running as an arbitrary user. It is named after the SU (Switch Users) utility of the UNIX family of operating systems. This utility enables you to pre-install applications, including those that do not support scripted installation, as part of an automated setup.	COMMAND-LINE COMMAND-LINE It is included in the Windows NT ServerResource Kit only.
TDISHOW.EXE	Menu-driven command-line utility which allows a user to capture and display TDITRACE buffer information.	COMMAND-LINE
Telnet Server Beta (TELNETD.EXE)	Telnet Server has two components: the service itself (TELNETD.EXE) and an underlying component, the Remote Session Manager (RSM.EXE). The Telnet Server service operates by connecting to the Remote Session Manager component. Remote Session Manager (RSM) is responsible for initiating, terminating, and managing the character-oriented remote telnet session on a given system. RSM affects only the services provided in the Telnet Server service; it does not affect Microsoft's Remote Access Service (RAS), or other layered products.	COMMAND-LINE
TEXTVIEW.EXE	TextViewer provides a graphical interface for quickly viewing text files on local or shared drives. While it provides basic editing and searching capabilities, it is primarily intended for viewing similar files within multiple sub-folders.	GUI
TIMEOUT.EXE	Similar to the DOS "pause" command, timeout.exe will wait a period of time denoted in seconds and then continue running without a key press.	COMMAND-LINE
TIMESERV.EXE	This service sets the system time accurately and keeps Windows NT workstations and servers synchronized with a primary or secondary timesource that you specify. TIMESERV always keeps the computer in sync, even when no one is logged on. The service can be run from either the Services Control Panel or the command prompt.	SERVICE
TIMETHIS.EXE	Executes the command specified by it's arguments and reports its run time in HH:MM:SS.TTT format.	COMMAND-LINE
TIMEZONE.EXE	This command-line utility updates the daylight savings information for a timezone in the Registry.	COMMAND-LINE
TLIST.EXE	The Task List Viewer is a command-line utility that displays a list of tasks, or processes, currently running on the local computer. For each process, it shows the process ID number, process name, and, if the process has a window, the title of that window.	COMMAND-LINE
TLOCMGR.EXE	Telephony Location Manager was written for laptop computer users who use telephone applications, such as Dial-Up Networking, from several locations. It is useful for anyone who changes Telephony API (TAPI) locations-for example, taking a laptop from the office to home, where the computer no longer has to dial a "9" prefix. For a laptop user with a hot-docking setup, this utility will automatically change the TAPI location.	EXPLORER EXTENSION

TOPDESK.EXE	This command along with topdesk.hlp presents a small representation of the virtual desktop showing your current desktop, the home desktop, all visible windows, and optionally, all ghost windows. TopDesk lets you manipulate all of these objects with various keyboard and mouse actions.	GUI
TOUCH.EXE	POSIX utility used to change date and/or time of a file.	COMMAND-LINE
TZEDIT.EXE	Time Zone editor.	GUI
UPTOMP.EXE	A performance and system monitoring utility which upgrades a single-processor system to a multiprocessor system.	COMMAND-LINE
USRMGR.EXE	The Windows NT User Manager utility which provides for the management of accounts, group membership and access permissions.	GUI
USRSTAT.EXE	This command-line utility displays username, fullname, and last login date and time for each user in a given domain.	COMMAND-LINE
USRTOGRP.EXE	Using a text file containing a Domain name on line 1, a Local or Global group name on line 2, and user names on successive lines, this utility will add users to groups in batch.	COMMAND-LINE
VDESK.EXE	VDESK.EXE is a simple desktop switcher that enables you to maintain multiple desktops on a computer running Windows NT Workstation.	GUI
VI.EXE	POSIX text file editor.	COMMAND-LINE
WC.EXE	POSIX utility for 'word count'.	COMMAND-LINE
Web Administration of Windows NT Server	This ISAPI DLL allows limited remote administration of Windows NT Server via HTML browsers (including Internet Explorer 2.0 and later) from Windows, Macintosh and UNIX platforms. Web Administration of Microsoft Windows NT Server is included in the Windows NT Server Resource Kit only and is also available for download from the Microsoft World Wide Web site. This tool does not replace existing administrative tools for Windows NT Server, but rather assists administrators when they do not have access to existing tools-for example, when they are away from their normal administrative workspace. This tool will be particularly useful for Windows NT administrators who are already experienced with the current administrative tools on Windows NT Server 3.51 and 4.0.	MULTI-FILE APPLICATION
WHOAMI.EXE	POSIX utility for identifying active session.	COMMAND-LINE
WINAT.EXE	Command Scheduler can be used to schedule commands on a local or remote computer to occur once or regularly in the future. The Workstation service must be started to use this application.	GUI
WINDIFF.EXE	Windows-based utility showing the differences between two named files or directories.	GUI
WINEXIT.SCR	WINEXIT is a screen saver that logs the current user off after the specified time has elapsed. It is similar to other screen savers and can be configured and tested using the Desktop icon in Control Panel.	SCREEN SAVER
WINMSDP.EXE	WinMsdP is a command-line version of WINMSD.EXE. It provides information about your system configuration and status.	COMMAND-LINE

WINSCHK.EXE	This command-line utility checks name and version- number inconsistencies that may appear in Windows Internet Name Service (WINS) databases, monitors replication activity, and verifies the replication topology in an enterprise network. It is particularly useful for WINS administrators.	COMMAND-LINE
WINSCL.EXE	Command-line utility providing limited NT server administration capabilities via TCP/IP or a named pipe.	COMMAND-LINE
WINSDMP.EXE	Tool which has been designed to take a dump from the WINS database and provide this output in a fixed record file format	COMMAND-LINE
WNTIPCFG.EXE	WNTIPCFG is a graphical version of the IPConfig utility that is shipped with the Windows NT operating system. Use this utility to manage the Internet Protocol (IP) addresses and view IP information for computers that run the TCP/IP protocol.	GUI

Trojan Port Numbers

Port number	Protocol	Name of Trojan(s)
21	TCP	Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, WinCrash
23	TCP	Tiny Telnet Server
25	TCP	Antigen, Email Password Sender, Haebu Coceda, Shtrilitz Stealth, Terminator, WinPC, WinSpy, Kuang2 0.17A-0.30
31	TCP	Hackers Paradise
80	TCP	Executor
456	TCP	Hackers Paradise
555	TCP	Ini-Killer, Phase Zero, Stealth Spy
666	TCP	Satanz Backdoor
1001	TCP	Silencer, WebEx
1011	TCP	Doly Trojan
1095, 1097, 1098, 1099		Rat
1170	TCP	Psyber Stream Server, Voice
1234	TCP	Ultors Trojan
1243, 6711, 6776	TCP	Sub 7
1245	TCP	VooDoo Doll
1349	UDP	Back Ofrice DLL
1492	TCP	FTP99CMP
1600	TCP	Shivka-Burka
1807	TCP	SpySender
1981	TCP	Shockrave
1999	TCP	BackDoor 1.00-1.03
2001	TCP	Trojan Cow
2023	TCP	Ripper

2115	TCP	BUGS
2140, 3150, 6670 & 6771	TCP/UDP	Deep Throat
2140 & 3150	TCP	The Invasor
2801	TCP	Phineas Phucker
3024 & 5742	TCP	WinCrash
3129	TCP	Masters Paradise
3700, 9872, 9873, 9874, 9875, 10067 & 10167	TCP	al of Doom
4092	TCP	WinCrash
4567	TCP	File Nail 1
4590	TCP	ICQTrojan
5000	TCP	Bubbel
5000, 5001	TCP	Sockets de Troie
5321	TCP	Firehotcker
5400, 5401, 5402	TCP	Blade Runner 0.80 Alpha
5569	TCP	Robo-Hack
6969	TCP	GateCrasher, Priority
7000	TCP	Remote Grab
7300, 7301, 7306, 7307, 7308	TCP	NetMonitor
7789	TCP	ICQ Killer
9989	TCP	iNi-Killer
10607	TCP	Coma 1.0.9
11000	TCP	Senna Spy
11223	TCP	Progenic trojan
12223	TCP	Hack´99 KeyLogger
12345, 12346	TCP	NetBus 1.20-1.70, GabanBus
12361 & 12362	TCP	Whack-a-mole

16969	TCP	Priority
20001	TCP	Millennium
20034	TCP	NetBus 2.0 Beta-NetBus 2.01
21544	TCP	GirlFriend 1.0 Beta-1.35
22222	TCP	Prosiak
23456	TCP	Evil FTP, Ugly FTP
26274	TCP	Delta
30100, 30101, 30102	TCP	NetSphere 1.27a
30100, 30101, 30102 & 30103 3010330103	TCP UDP	NetSphere 1.31
31337	UDP	BackOfrice 1.20
31338	UDP	DeepBO
31339	TCP	NetSpy DK
31666	UDP	BOWhack
31785, 31787, 31789 & 31791 31789 & 31791	TCP UDP	Hack Attack
33333	TCP	Prosiak
34324	TCP	BigGluck, TN
40412	TCP	The Spy
40421, 40422, 40423 & 40426	TCP	Masters Paradise
47262	TCP	Delta
50505	TCP	Sockets de Troie
50766	TCP	Fore
53001	TCP	Remote Windows Shutdown
54321	TCP	SchoolBus .69-1.11
61466	TCP	Telecommando

65000	TCP	Devil 1.3
69123	TCP	ShitHeep

References

Computer Operations, Audit, and Security Technology (COAST). "Introduction to Intrusion Detection."
http://www.cs.purdue.edu/coast/intrusion-detection/introduction.html

"On Computer and Network Security." *NetSurfer Focus*, Volume 1, Number 1: April 1995.
http://www.netsurf.com/nsf/v01/01/nsf.01.01.html

Cisco Systems, Inc. NetRanger Product Information.
http://www.cisco.com/warp/public/cc/cisco/mkt/security/nranger/

Cisco Systems, Inc. NetSonar Product Information.
http://www.cisco.com/warp/public/cc/cisco/mkt/security/nsonar/

Computer Security Institute. "The Cost of Computer Crime."
http://www.gocsi.com/losses.htm

Computer Security Institute. Intrusion Detection Resources.
http://www.gocsi.com/intrusion.htm