
# Microsoft Windows 2000 Security

*An Overview and Evaluation of Windows 2000 Security*

## Introduction

In today's digital economy, an organization's success may depend on its ability to adapt to e-business. In this model, transparent online supply chains connect offices, employees, customers, partners and suppliers through new, innovative and quickly evolving business practices. This massive shift to e-business demands more protection of an organization's vital information assets and the systems that manage them. In this environment, your organization's information security depends in large part on the security infrastructure provided by the network operating system you use.

ISS is committed to helping customers protect their networks. Part of that commitment is to keep you up-to-date with advances in security technology and what those advances can mean for your network.

Microsoft® Windows® 2000, the successor to Microsoft® Windows® NT, is sure to be a core technology in the fabric of enterprise computing around the world. For this reason, ISS has studied the security services available in Windows 2000 and is offering the findings of that work in this white paper.

This paper will focus on answering the following three questions:

- What's new in Windows 2000 security?
- How is management easier and more secure in Windows 2000?
- What attacks and vulnerabilities are addressed by Windows 2000?

Overall, ISS believes that Microsoft has made a significant leap forward in security with Windows 2000. It has done so by using tried-and-true industry standards as well as by incorporating a large number of enhancements to address known vulnerabilities in previous versions of Windows NT.

ISS appreciates Microsoft's contributions, review, and input to this paper.

Note: Readers wanting to learn more about the technologies discussed in this paper can find online Help for Windows 2000 and reference materials delving into Windows 2000 directory and security technologies at www.microsoft.com/windows2000/library.

## What's New in Windows 2000 Security?

The Windows 2000 security infrastructure integrates four important technologies: Kerberos v5 for network authentication, the Active Directory® service for centralized network management, the IPSec Internet security protocol for secure communications, and Public Key Infrastructure used for user authentication and data encryption. The integration of these features provides end-to-end security, from clients to back-end servers, making Windows 2000 to be one the most secure and flexible operating system platforms in the market.

## Kerberos

Windows 2000 implements a default network authentication mechanism within the Windows 2000 (Active Directory) domains based on Kerberos v5 with extensions. A domain is a security boundary consists of security principals such as computers and users that are part of a network and share a common directory database. Kerberos v5 (RFC 1510), is an Internet standard security protocol for handling authentication of user or system identity. Kerberos is a mature and well-established Internet standard that provides high security network communication capability, cross platform interoperability, efficient authentication, and simplified trust management. Kerberos is a significant improvement over NTLM in terms of protocol security practice, performance, and administration. Note: Windows 2000 supports NTLM (NT LAN Manager authentication is used in Windows NT 4.0) for compatibility with legacy Windows NT machines.

### *Password Protection*

One of the major features of Kerberos is its ability to provide strong password protection. Kerberos performs network authentication without ever transmitting passwords on the wire. In the Windows 2000 implementation of Kerberos, a user's password, once entered on a local machine, is hashed and subsequently protected under LSA process memory and is never written to non-volatile storage. This helps ensure that unauthorized parties cannot obtain a user's password by either monitoring network transmissions or gaining access to the domain controller. Windows 2000 does not implement the Kerberos replication protocol, rather, Windows 2000 keeps an encrypted copy of each client's password in the Active Directory account database. This database is replicated between domain controllers via a Microsoft secure-channel protocol.

### *Internet Standard*

Windows 2000 authentication is based on Kerberos v5 (RFC 1510) with extensions. Kerberos is a well-established security protocol for network authentication. Supporting a security standard such as Kerberos allows applications that demand higher security to take advantage of Kerberos authentication. Kerberos support also allows these applications to be more portable across different operating system platforms.

### *Efficient Authentication*

Windows 2000 servers, unlike their Windows NT counterparts, no longer need to contact a domain controller to authenticate clients. A Windows 2000 server checks a client's identity by verifying the content of the client's Kerberos authentication ticket. A Windows 2000 client only needs to contact a domain controller to receive a server ticket, the client then presents the ticket to the server in order to access server resources. Once a Kerberos ticket is obtained for a particular server, a client can reuse the same ticket until the ticket expires, without any further authentication from domain controller.

## Active Directory

### *Fine-grain Access Control*

In Active Directory, access permission can be granted at the object and individual properties level to enable more flexible administrative control. Every object in the directory has a unique security descriptor. The access control list (ACL) in the security descriptor contains a list of access control entries (ACE) that store specific access rights granted or denied with different levels of scope on the object. Unlike Windows NT 4.0, Windows 2000 account objects such as Users and Groups are objects in the Active Directory. This enables control of more restrictive access to sensitive account properties

### *Multi-master Support*

Active Directory account updates can take place at any domain controller instead of just the primary domain controller (PDC), which is generally considered a bottleneck in NT 4.0. Replication between Windows 2000 domain controllers is done over a secure channel, and Windows 2000 administrator has greater controller in terms of scheduling, and the replication mechanism.

### *Easy Domain Trust Management*

The Active Directory domain model mimics the standard Kerberos realm structure. To simplify domain trust management, two-way transitive trust is set up automatically when a domain is created and added to an Active Directory domain tree. The old-style one-way trust can still be used with down-level NT domains.

### *Better Account Management Capability*

The Active Directory has a much larger capacity than the registry-based account database in Windows NT 4.0, which only supports a flat name space that can contain a limited number of objects. Active Directory can contain more than one million account objects, efficiently arranged in a hierarchical structure. This makes Active Directory more flexible, scalable, and easier to manage than the Windows NT 4.0 account database.

### *Delegation*

Administrators can organize users, groups, and computer account objects in the Active Directory into containers called Organizational Units. To achieve distributed management, administrative control of Organizational Units can be delegated to particular users or groups at any level of an Active Directory tree. Active Directory also allows specific access permission to be delegated at the container, object, and object properties level.

### *Strong Password Authentication*

The Windows 2000 implementation of the secure channel security protocol (SSL/TLS) supports strong client authentication by mapping user credentials in the form of public-key certificates to existing Active Directory user accounts. Similar to the SSL/TLS public key certificate mapping, Windows 2000 supports smart card interactive logon in addition to the traditional Kerberos shared-secret key such as password, thus enabling strong authentication from the desktop to the domain.

### *Group Policy*

Domain-wide security policy such as strong password requirements, restricted groups, and user rights, can be centrally managed via Group Policy. Group Policy enables security policies to be maintained and enforced consistently for all computers in the Windows 2000 domain based on inheritance.

## IPSec

### *Internet Standards*

The Windows 2000 implementation of IPSec is based on IETF standards RFC 2402 (IP Authentication Header, AH), RFC 2406 (IP Encapsulating Security Payload, ESP), RFC 2408 (Internet Security Association and Key Management Protocol, ISAKMP) and RFC 2412 (The Oakley Key Determination Protocol). The Windows 2000 implementation of these standards ensures interoperability across different vendor platforms and network components.

### *Authentication*

The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams and to provide protection against replays.

### *Confidentiality*

The IP Encapsulating Security Payload (ESP) is used to provide confidentiality, data origin authentication, connectionless integrity, anti-replay service, and limited traffic flow confidentiality.

### *Transparency*

IPSec provides secure end-to-end communication silently at the IP layer. Applications, users and higher layer protocols gain the benefit of secure communication without the need to deal with any complicated setup issues.

### *IPSec Policy*

The Windows 2000 implementation of IPSec takes advantage of the Group Policy mechanism in Active Directory for policy dissemination. The administrator defines the IPSec policy as part of the Group Policy that can be applied to any computers in the domain. The IPSec policy agent, running on a Windows 2000 computer as one of the system services, retrieves the active IPSec policy from the domain controller to ensure the domain-wide IPSec policy is consistently enforced.

## Public Key Infrastructure

Windows 2000 comes with an integrated Public Key Infrastructure (PKI). This means that Windows 2000 provides a development and management platform for public-key enabled applications such as secure email systems, virtual private networking hardware and software and document encryption and signing products. Windows 2000 PKI is integrated with Active Directory to provide a single store for all network information and credentials. Certificates, certificate revocation lists, and policy information all are stored in Active Directory, meaning that they can be replicated, mirrored, and partitioned using native features of the Active Directory. In addition, Windows 2000 PKI-related data are just like any other objects in the Active Directory subject to the built-in fine-grained

access control facility. The PKI in Windows 2000 provides authentication, encryption, and non-repudiation capabilities for secure communication.

### *Kerberos Integration*

Windows 2000 security infrastructure bridges PKI and Kerberos to provide flexible deployment scenarios. For example, Windows 2000 provides certificate mapping which enables a PKI certificate to be mapped to a user account in the Active Directory for extranets. In addition, Windows 2000 implements a standard called PKinit that permits initial authentication using a certificate stored on a smart cards. When a smart card is used in place of a password, a private/public key pair stored on the user's smart card is substituted for the shared secret key derived from the user's password.

### *Smart Cards*

Windows 2000 supports smart cards as a password alternative to achieve strong network authentication. Smart cards, which use a tamper-resistant storage for protecting private key and personal information, use public key-based technology that Windows 2000 supports as a password alternative to achieve strong network authentication. A smart card can be used to authenticate to a Windows 2000 domain for services such as SSL/TLS, interactive logon, and secure email. A smart card adds another level of security because it stores the private key on the card, protected by a PIN. In order to compromise the private key, both the user's smart card and the PIN will be needed.

### *IPSec*

PKI can be used as one of the IPSec authentication methods for situations, such as Internet access and remote access to protected resources, to provide transparent and automatic encryption of network communication.

## Core Operating System Security Features

In addition to the features above, Microsoft has incorporated a number of low-level operating system technologies that greatly improve the security and reliability of Windows, including system file protection, driver verification and signing, heap memory management and kernel-mode write protection.

### *System File Protection*

System File Protection (SFP) is a feature of Windows 2000 that prevents the replacement of essential system files. SFP runs as a background process on Windows 2000 and monitors core operating system files. When SFP detects that a protected file has been changed, it restores the original.

### *Driver Verification and Signing*

To assure customers that device drivers loading on their systems are certified production grade products, or notify them if such is not the case, Microsoft provides cryptographic signing on the binary driver code. Microsoft digitally signs drivers that pass the Windows Hardware Quality Labs (WHQL) verification tests. WHQL certification proves to users that the drivers they employ are identical to those Microsoft has tested, and flags any changes after a product is put on the Hardware Compatibility List.

### *Heap Memory Management*

A common problem in application development is heap corruption. This typically occurs when an application allocates a block of heap memory of a given size and then writes to memory addresses beyond the requested size of the heap block. Another common cause of heap corruption is writing to a block of memory that has already been freed. These memory corruptions can then be exploited by malicious applications and result in security vulnerabilities.

To help developers find heap corruption problems faster and more reliably, the PageHeap feature has been built into the Windows 2000 heap manager. When the PageHeap feature is enabled for an application, all heap allocations in that application (including heap allocations from all .dlls in that process) are placed in memory such that the end of the heap allocation is aligned with the end of a virtual page of memory. The page of virtual memory following the allocation is set to NO_ACCESS in Windows 2000 to protect against memory-based attacks.

### *Kernel Mode Write Protection*

Microsoft Windows 2000 benefits from the stability provided by kernel-mode write protection, which uses the Windows 2000 memory manager to provide write-protection for code and read-only subsections of the kernel and device drivers, just as it always has been for user-mode programs and dynamic link libraries (.dll files). This protects each part of the operating system from bugs in other sections.

## How is security management easier and more secure with Windows 2000?

Active Directory is a core technology of Windows 2000, and serves as central point of network management. The access methods at the programming level supported by Active Directory are Lightweight Directory Access Protocol (LDAP) and the Active Directory Service Interface (ADSI). Customized security applications can be created to directly access objects in the Active Directory via these program interfaces. In addition, certain important security-related tools that come pre-packaged with Windows 2000 are noted below.

### *Users and Computers Management Tools*

In terms of Windows 2000 domain operation, Kerberos setup and authentication in general is transparent to users and administrators. The login process and password maintenance are very similar to previous Windows NT environment. The Active Directory Users and Computers Management Microsoft Management Console (MMC) is the main tool in Windows 2000 for account management.

### *Kerberos Interoperability Tools*

This set of tools includes the Domain and Trust Management MMC for managing Kerberos trust relationship across different platforms, the ktpass tool for managing Kerberos keytab file for clients on different platforms, and the ksetup tool for managing Kerberos realm association and Kerberos principal mapping for Windows 2000 clients.

### *Public Key Certificate Tools*

Several new tools are introduced in Windows 2000 for management of public key certificate related tasks. The Certificates MMC is used for management of certificates for users, services, and computers. The Certification Authority MMC lets administrators configure the certificate service, browse the certificate database, and revoke previously issued certificates. To enable strong authentication, the Windows 2000 administrator may use the Active Directory User and Computer Management MMC to create explicit mapping between a certificate and a user account.

### *Group Policy Editor*

The Group Policy Editor is the tool that is used to configure the group policy technology in Active Directory to disseminate computer and user security configuration information to domain computers. Group policy follows the Active Directory hierarchy for inheritance and the group policy object ACL for access permission. Numerous security configuration parameters are available thru this tool.

**IPSec Policy Editor** – This tool is part of the Group Policy Editor. Windows 2000 provides three pre-packaged IPSec policies, i.e., client, server, and secure server for customers to start with. Administrators can create additional IP filters, filter actions, and IPSec policies using the IPSec Policy Editor.

## What attacks and vulnerabilities are addressed by Windows 2000?

Over the years a number of vulnerabilities have been identified in Windows NT and are fixed by applying hot-fixes and service packs from Microsoft. Windows 2000 brings all of these fixes together into a uniform initial installation, avoiding the need and risk of performing a base installation and applying multiple hot-fixes and service packs. One of the gravest risks to security is the lack of resources to track hot-fixes and service packs dating back years. Consequently, attackers have broken into sites using exploits for problems that were fixed for over a year and a half. Windows 2000 resets the baseline on these problems by incorporating solutions and advances to those fixes in a new robust platform.

Windows 2000 significantly raises the bar on security by incorporating and improving fixes from previous service packs and hot-fixes and advancing the over all robustness of the operating system. It is clear that Microsoft has learned a considerable amount about how earlier versions of Windows NT have been compromised and has rolled that knowledge into Windows 2000. While not nearly a complete list of the thousands of security enhancements made in Windows 2000, the following documents what ISS considers to be the most important improvements for enterprise computing.

In situations where fixes for vulnerabilities have existed for some time, Windows 2000 incorporates improvements on those fixes. The sequence number predictability in earlier versions of Windows NT is addressed by some service packs, but the TCP/IP sequence predictability in Windows 2000 is addressed using a superior method among the best approaches available.

Windows 2000 default security installation settings (“out of the box”) are improved. Windows NT default registry settings raise security issues that are addressed in Windows 2000 default registry settings. Windows 2000 improves the over all security that the user can expect from a new installation.

The vulnerabilities and attacks that Windows 2000 addresses are organized into four categories: on-the-wire attacks, information disclosure, denial of service, and elevation of privilege.

### On-the-Wire Attacks Addressed by Windows 2000

Windows 2000 incorporates fixes for a number of on-the-wire attacks in the areas of identity spoofing, data tampering, and reputability using Kerberos network authentication, the encrypted file system, dynamic DNS, and IPSec.

#### *Spoofing User Identity*

Spoofing threats are associated with a hacker being able to impersonate a valid system user or resource to get access to the system and thereby compromise system security. In this case, the hacker has obtained the user's personal information or something that enables him or her to replay the authentication procedure.

### *Data Tampering*

An unauthorized change to stored or in-transit information, formatting a hard disk, a malicious intruder introducing an undetectable network packet in a communication, and making an undetectable change to a sensitive file are all data tampering threats.

### *Repudiability*

The ability of a user to perform an action or transaction (malicious or otherwise) and later deny their responsibility for it is termed repudiation. Repudiation threats are associated with users (malicious or otherwise) who can deny a wrongdoing without any way to prove otherwise.

**nt-ssl-fix (SSL patch not installed)**
An unpatched version of the Secure Sockets Layer (SSL) allows an attacker to formulate a complex structured attack that could potentially decode an Internet transaction encrypted using SSL. This knowledge would not give the attacker an advantage in decoding any other transactions that had been made by the server, nor would it necessarily give the attacker an advantage in decoding any other transactions performed by the user. A web site operator could detect an attack through observations, such as abnormal network activity or high CPU utilization.
http://support.microsoft.com/support/kb/articles/q148/4/27.asp

**nt-rras (RRAS patch not installed)**
The machine has an unpatched version of the Routing and Remote Access Service (RRAS). This patch includes an enhancement to TCP/IP that will improve the performance of TCP-based applications over high latency networks, demand dial filtering to better control dialing interfaces, fragmented IP packet filtering to drop malformed or unauthorized packets, and other security fixes.
http://support.microsoft.com/support/kb/articles/Q177/6/70.asp

**Q177670 (RRAS does not enforce strong encryption for Dial-Up Networking clients)**
When a Dial-Up Networking (DUN) client connects to a 40-bit or 128-bit Routing and Remote Access Server that is configured to "Require Data Encryption" or "Require Strong Data Encryption", the client is not disconnected if the selected data encryption negotiation fails to converge.
The following error may be logged in Event Viewer in the System Log on the server after the client has successfully established its connection:
Event ID : 20073
Source : Router
Description: The following error occurred in the %protocol_name% module on port %port_name%. The PPP control protocol for this network protocol is not available on the server.
http://support.microsoft.com/support/kb/articles/q177/6/70.asp

**Q170534 (FTP client echoes gateway password)**
Firewalls can be configured to request a password (sometimes referred to as a firewall account) independent of the FTP logon sequence, in order to provide stronger security and to audit traffic going through the firewall. The Microsoft FTP client echoes the entered gateway password on screen when connecting to a host across a firewall.
http://support.microsoft.com/support/kb/articles/q170/5/34.asp

**nt-pptp3-fix (PPTP patch not installed)**
The machine has an unpatched version of the Point to Point Tunneling Protocol (PPTP). Microsoft has made improvements to the native Virtual Private Networking (VPN)

capabilities that significantly improve the performance and security of PPTP-based VPN connections via the Internet, especially for remote access or high-latency networks.
http://support.microsoft.com/support/kb/articles/q189/5/95.asp

**nt-netbios-nullsession (Shares enumerated through a nullsession)**
Users or shares were detected using a null session. A null session is a NetBIOS connection established with a zero length string as user, password, and domain name, which is designed to enable enumeration of shares and users. This capability has always been present in Windows NT, but was discovered to allow access to the registry with the same level of permissions as the Everyone group. It is a medium risk vulnerability (similar to finger) that allows users and shares to be enumerated.
http://support.microsoft.com/support/kb/articles/q143/4/74.asp

## Information Disclosure Attacks Addressed by Windows 2000

Information disclosure threats expose information to individuals who are not supposed to see it, thus compromising private or business-critical information. A user's ability to read a file that she or he was not granted access to, as well as an intruder's ability to read the data while in transit between two computers, are both disclosure threats. Note that this threat differs from a spoofing threat in that here the perpetrator gets access to the information directly rather than by having to spoof a legitimate user.

Key security technologies in Windows 2000 that address information disclosure attacks include Active Directory, Kerberos network authentication, the encrypted file system, and IPSEC.

**L0phtcrack**
L0phtcrack used weaknesses in the NTLM cryptographic hashes to crack NT passwords. Depending on the complexity of the passwords it may take minutes or weeks to crack a password. The hashes are obtained from the registry, file system, or the network.
Attack: The tool compromises passwords. It can be used for undetectable attacks after an Elevation of Privilege attack. The attacker gets a copy of the hashes, erases all evidence of the entry, and then goes home to crack the passwords.
http://www.l0pht.com

**nt-sp4-auth-error**
A vulnerability was introduced in Windows NT 4.0 SP4 (Service Pack 4) that could allow some users to access resources by supplying a null password. The problem exists when clients other than Windows NT/95/98 change their passwords causing certain fields in the SAM (Service Account Manager) to be left null. The next time this account is accessed from a Windows NT machine no password will be required for authentication. This vulnerability only affects sites that have deployed machines with DOS, Windows 3.1, Windows for Workgroups, OS/2 or Macintosh clients.
http://support.microsoft.com/support/kb/articles/q214/8/40.asp

**nt-gina-clipboard**
A flaw has been found in Windows NT that allows anyone to view the contents of the first line from the clipboard of a user who has locked their terminal, by pasting into the console login username field.
http://support.microsoft.com/support/kb/articles/q214/8/02.asp

**Q193689**
Internet Database Connector (IDC) could be used to gain information. If the IDC file returns an error, the error returned displays the full physical path of the IDC file that caused the error.

http://support.microsoft.com/support/kb/articles/Q193/6/89.ASP

**Q193793**
Accessing the :$DATA data stream of a file displays the source (script code) of the file.
http://support.microsoft.com/support/kb/articles/Q193/7/93.ASP

**Q194341**
Sending a specific UDP packet to a server using the Simple TCP/IP services will cause the Simple TCP/IP services to drive the processor usage up to 100 percent..
http://support.microsoft.com/support/kb/articles/Q194/3/41.ASP

**http-iis-aspsource, http-iis-dot**
This version of Microsoft Internet Information Server (IIS) displays the source to active server pages (.asp files), if a period is appended to the URL. Scripting information, in addition to other data in the file, is visible.
Potentially proprietary web server files (such as .ASP, .HTX, and .IDC file name extensions) may contain sensitive information (such as user IDs and passwords) embedded in the source code but not normally available to remote users.
http://support.microsoft.com/support/kb/articles/q163/4/85.asp

## Denial of Service Attacks Addressed by Windows 2000

A Denial of Service (DoS) attack prevents legitimate users from using a service. The effectiveness of a DoS attack is measured three ways:

**Effort**
A measure of the effort required for the attack to be successful. The least effort is a single packet that crashes a computer. Many large packets, possibly sent by multiple attackers, represent the greatest effort.

**Severity**
A measure of how much the service has been degraded. A severe attack will prevent all legitimate users from accessing the service. A mild attack may slow down access, but not shut it down completely.

**Persistence**
An attack is persistent if its affects continue after the attack stops. The strongest attacks persist even if the attacker is blocked from accessing the service. Some attacks persist until the server is rebooted. The negative affects of a weak attack end as soon as the attack itself ends.

ISS considers the following list of vulnerabilities and attacks to be among the most critical that have been addressed by Windows 2000.

**Q132470**
When you use PING similar to "PING -l 65527 -s 1 <target computer>" (without quotes) in Windows NT 3.51, the target computer stops responding (hangs) and one of the following STOP messages may appear on your computer:
STOP: 0X0000001E
KMODE_EXCEPTION_NOT_HANDLED - TCPIP.SYS
-or-
STOP: 0x0000000A
IRQL_NOT_LESS_OR_EQUAL - TCPIP.SYS
http://support.microsoft.com/support/kb/articles/Q132/4/70.asp

**Q162927**

A Windows NT 4.0 Domain Name Service (DNS) server produces the following event error 454:
DNS Server select() Function failed. The data is the error.
Besides the event error, CPU usage is high, the DNS server is unstable, and it sometimes crashes.
CAUSE: The possible cause of this problem is when an unknown user telnets to the DNS server port 53. When this is done, and a few characters are typed, the above behavior is seen on the Windows NT 4.0 DNS server.
http://support.microsoft.com/support/kb/articles/Q162/9/27.asp

**Q163196**
When you use the Windows NT 4.0 version of the Ping utility (Ping.exe) to test IP communication to a network resource, the networked computer or other device may experience symptoms including one or more of the following:
- The system may hang.
- A Panic error may be displayed.
- Other errors may occur.

CAUSE: Under some circumstances it is possible for the Windows NT Ping utility to send an IP packet which is interpreted as an invalid IP datagram.
http://support.microsoft.com/support/kb/articles/Q163/1/96.asp

**Q163620**
When you use Windows NT to access a file with an extremely long file name that is nested in a long path, the following blue screen STOP error message may occur:
STOP 0x00000050 (0xff737000 0x00000001 0x00000001 0x00000000)
Note: The first parameter will vary, but the last three should always be the same.
CAUSE: The Redirector (Rdr.sys) does not check the path name before sending a Query_Information server message block (SMB).
http://support.microsoft.com/support/kb/articles/Q163/6/20.asp

**Q164491**
A Winsock application may cause a Stop 0x00000050 PAGE_FAULT_IN_NONPAGED_AREA error in Afd.sys.
CAUSE: The application passes a socket address length that is larger than the maximum socket address length in the TDI buffer in Afd.sys. The socket address data that goes beyond the MaxSockaddrLength overwrites the stack.
http://support.microsoft.com/support/kb/articles/Q164/3/52.asp

**Q164491**
When you start a computer running Windows NT 4.0, you may experience a Stop 0x0000000A in Rdr.sys if one of the first three mailslot messages received is over 512 bytes in size.
CAUSE: The browser mailslot overran its buffer.
http://support.microsoft.com/support/kb/articles/Q164/4/91.asp

**Q174465**
Computers running Windows NT will blue screen with a Stop 0x0000000A shortly after the Logon Screen appears or if the computer was removed from the network during startup, it will blue screen approximately 10 seconds after being put back on the network.
Stop screen:
Stop 0x0000000A (0xFFB94000, 0x00000002, 0x00000001, 0xFF5A98C5)
The blue screen will show Afd.sys, Nwlnkipx.sys, and Ntoskrnl.exe on the stack.
The first and last BugCheck parameters will vary.
This will be most evident if there are many computers running the SAP Agent.
CAUSE: A faulty network interface card (NIC) is broadcasting bad SAP packets on the network with a large value for Bytes Remaining. The computer has to have SAP Agent

loaded for this to occur. It does not matter if the computer is using the Gateway Services for NetWare (GSNW) or intraNetWare client redirector but must have either redirector loaded. The SAP Agent is allowing the packet to be passed up the stack.
http://support.microsoft.com/support/kb/articles/q174/4/65.asp

**smtp-exchangedos**
Microsoft Exchange Server 4.0 and 5.0 contain a buffer overflow in multiple commands (HELO, RCPT TO, and MAIL FROM) that could allow a remote attacker to crash the server and under some circumstances possibly execute arbitrary code on the system. The attack itself does not directly have any impact on the integrity of data stored by the Exchange Server.
http://support.microsoft.com/support/kb/articles/q169/1/74.asp

**nt-kernvers**
This system was found to have an outdated Windows NT kernel version. Windows NT can allow a user to start a high priority process that cannot be killed from the Task Manager. It is extremely difficult to cause this behavior to occur remotely.
http://support.microsoft.com/support/kb/articles/Q135/7/07.asp

**nt-35, nt-351**
A version of Windows NT was detected as vulnerable to the Samba. bug. Windows NT 3.51 prior to Service Pack 3 is vulnerable to the Samba “cd..” bug. If a Samba client attaches to a file system share on a Windows NT 3.5 or 3.51 machine and executes a “cd ..” command from the root directory of the share, it causes a kernel exception. Depending on the configuration of the machine, it may automatically reboot or require manual intervention. If a Windows 95 share is accessed, this bug allows anyone to gain access to the entire hard drive.
http://support.microsoft.com/support/kb/articles/q140/8/18.asp

**nt-dnsver**
This version of Windows NT 4.0 DNS is vulnerable to denial of service and spoofing attacks. These attacks can allow an attacker to access sensitive information.
http://support.microsoft.com/support/kb/articles/Q142/0/47.asp
http://support.microsoft.com/support/kb/articles/Q169/4/61.asp

**synflood**
SYN flooding is an attack based on sending numerous session connection requests to a server and never completing the entire handshake. In some systems, this behavior depletes the new connection buffer space and records all the new connections, which results in a denial of service for clients wishing to make legitimate connections.
http://support.microsoft.com/support/kb/articles/q142/6/41.asp

**http-iis-cgi**
The Microsoft Internet Information Server (IIS) 2.0 and 3.0 contain a vulnerability that crashes the server if a very large client request is received. The attack can be embedded in many requests, such as headers and CGI requests, and requires a length between 4 KB and 8 KB to be transmitted, which never happens in normal HTTP traffic.

**http-iis-longurl**
Microsoft Internet Information Server (IIS) can crash if a formatted URL of about 8 KB is sent to the server.
http://support.microsoft.com/support/kb/articles/q143/4/84.asp

**land**

The land exploit consists of a forged packet sent to a target machine, with identical source and destination addresses, and identical source and destination ports. This type of packet is known to crash many machines.

**land-patch**
An outdated version of TCP/IP has been detected. An attacker can cause a high CPU load by sending a spoofed packet to a port that claims to have originated from that port. Variations on this attack can cause machines to lock up.
http://support.microsoft.com/support/kb/articles/q165/0/05.asp

**win-oob**
The machine is vulnerable to the Out of Band (OOB) attack. Sending out of band data to port 139 will cause Windows NT to stop and Windows 95 to lose networking and possibly crash. Other systems have also been shown to be vulnerable to this attack.

**nt-syncstormpatch**
This machine was found to be vulnerable to a Sync Storm denial of service attack due to an unpatched TCPIP.SYS file.
http://support.microsoft.com/support/kb/articles/q179/1/29.asp

**nt-logondos**
Windows NT servers (including those with Service Pack 3 when all hotfixes applied) are vulnerable to a denial of service attack. When a logon request is initiated to access the SMB/CIFS service and the SMB logon packet is incorrectly processed, memory corruption results in the Windows NT kernel. When this happens, a blue screen error message appears and the machine has to be rebooted.
http://support.microsoft.com/support/kb/articles/Q180/9/63.asp

**nt-ssping**
An unpatched version of Windows NT has been found. It is possible for an attacker to cause the host to crash by sending improperly formed ICMP packets.
http://support.microsoft.com/support/kb/articles/Q154/1/74.asp

**chargen-patch**
An unpatched version of Windows NT Simple TCP/IP services has been detected. It is possible for an attacker to cause a network denial of service by sending broadcast UDP packets to the Windows NT chargen service.
http://support.microsoft.com/support/kb/articles/q154/4/60.asp

**nt-wins-patch**
An unpatched version of Windows NT WINS has been found. It is possible for an attacker to cause WINS to fail by sending invalid UDP packets.
http://support.microsoft.com/support/kb/articles/Q155/7/01.asp

**nt-rpc-ver**
Prior to installation of the Windows NT 4.0 post-SP2 rpc-fix, an attacker can telnet to port 135 and cause the system to become extremely slow. As a result of this denial of service attack, the RPC locator process will use nearly 100% of the processor.
http://support.microsoft.com/support/kb/articles/q162/5/67.asp

**nt-lsasp3**
An unpatched version of the Local Security Authority (LSA) subsystem exists, allowing an attacker to display sensitive security information. In addition, account lockout events, as a result of exceeding the Bad Logon Attempts limit, are not logged at Domain Controllers. Although the latter is not a vulnerability, it does create an inconvenience for administrators wanting to locate the computer originating the bad password attempts.

http://support.microsoft.com/support/kb/articles/q182/9/18.asp

**iis-remote-ftp**
This could allow a remote attacker to crash the FTP server and allow a carefully constructed list request to execute arbitrary code on the server. The attacker is required to have a valid login (such as "anonymous") to the server before exploiting this hole.
http://support.microsoft.com/support/kb/articles/q188/3/48.asp

**ftp-pasv-dos**
A vulnerability exists in many FTP server packages that allows an attacker to endlessly request PASV (passive) connections to the server. Eventually, this attack depletes all the ports on the system, denying legitimate traffic to the machine.
http://support.microsoft.com/support/kb/articles/q189/2/62.asp

**snork-dos**
A vulnerability has been identified in Windows NT 4.0 up to SP4 that allows a remote attacker with minimal resources to cause the system to consume all available processor and network bandwidth resources for an indefinite length of time. The attack induces a storm of packets much like the smurf and fraggle attacks and has been referred to as the snork attack.
http://support.microsoft.com/support/kb/articles/q193/2/33.asp

**nt-nprpc-dos**
A vulnerability in the RPC services of Windows NT 4.0 through SP4 could allow a remote attacker to cause the machine to consume all available memory and processor resources, and eventually hang the machine. The attack is exploited by connecting to either the SPOOLSS.EXE and LSASS.EXE service over a named pipe and sending random data.
http://support.microsoft.com/support/kb/articles/q195/7/33.asp

**nt-snmpagent-leak**
A memory leak exists in the Windows NT 4.0 SNMP agent when it is queried multiple times. The program erroneously uses a memory buffer that it then never frees, which, in theory, could be exploited by a remote attacker to deplete a machine's memory resources.
http://support.microsoft.com/support/kb/articles/q196/2/70.asp

**nt-rras-incoming**
The Routing and Remote Access Server (RRAS) computer may stop responding to incoming calls when it is placed under heavy loads.
http://support.microsoft.com/support/kb/articles/q221/3/31.asp

**nt-ras-bo**
The portion of the Remote Access Service (RAS) client for Windows NT 4.0 that processes phone book entries contains a buffer overflow condition that could allow a local user to cause a denial of service or possibly execute arbitrary code with system privileges.
http://support.microsoft.com/support/kb/articles/q230/6/77.asp

**msrpc-lsa-lookupnames-dos**
A potentially serious denial of service attack on the Windows NT Local Security Authority (LSA) service could allow a remote attacker to crash this service by making a malformed request to LsaLookupNames. In most cases, the system will have to be rebooted to regain normal functionality. There is no capability to use this vulnerability to obtain unauthorized services from LSA.
http://support.microsoft.com/support/kb/articles/q231/4/57.asp

**nt-csrss-dos**
The Microsoft Windows NT CSRSS.EXE Client Server Runtime Subsystem service can be used to launch a denial of service attack against hosts accepting interactive logins. CSRSS provides Windows NT services to client processes running on the local computer. When all worker threads (by default, a maximum of 16) within the CSRSS service are awaiting user input, no new connections can be made, effectively hanging the system.
http://support.microsoft.com/support/kb/articles/q233/3/23.asp

**nt-malformed-image-header**
It is possible to crash a Windows NT machine if the user executes a file with a specially malformed image header. Every executable file contains an image header that is produced as part of the link process and describes how the program will use system resources; where it will reside in memory, how big the stack is, and so on. The system will require a reboot to become functional again.
http://support.microsoft.com/support/kb/articles/q234/5/57.asp

**dns-Netbtsys-dos**
Windows NT 4.0 computers configured to use DNS for Windows name resolution could display a blue screen error when a query DNS for a computer name and receive 0.0.0.0 as the IP address.
http://support.microsoft.com/support/kb/articles/Q188/5/71.ASP

**tcpipsys-icmp-dos**
Windows NT 4.0 generates the following blue screen STOP error in Tcpip.sys when it processes an ICMP Subnet Mask Address Request packet:
STOP 0x0000000A (0xA0033000, 0x00000002, 0x00000000, 0xf381329B)
http://support.microsoft.com/support/kb/articles/Q192/7/74.ASP

**win-redirects-freeze**
A flaw in the way Windows 9x and NT handle ICMP redirect packets allows a remote attacker to spoof packets from a router and cause the Windows machine to modify its routing tables. This attack will effectively freeze the machine during the duration of the attack. Exploit information and source code has been made widely available.
http://support.microsoft.com/support/kb/articles/Q225/3/44.ASP

## Elevation of Privilege Attacks Addressed by Windows 2000

In an elevation of privilege attack, an unauthorized user gains privileged access sufficient to completely compromise or destroy the entire system. The more dangerous aspect of such threats is compromising the system in undetectable ways, whereby the user is able to take advantage of the privileges without the knowledge of system administrators. Elevation of privilege threats include those situations where an attacker is allowed more privilege than should properly be granted, completely compromising the security of the entire system and causing extreme system damage. Here the attacker has effectively penetrated all system defenses and become part of the trusted system itself and can do nearly anything.

Windows 2000 incorporates fixes for a large number of known escalation of privilege vulnerabilities in previous versions of NT and has included system file protection, support for driver signing and verification, heap management, kernel-mode write protection, Kerberos, and IPSEC to address this type of attack.

### *Remote Escalation of Privilege Attacks*

**nt-getadmin**
The version of Windows NT is vulnerable to the GetAdmin exploit, allowing a local user to obtain administrator privileges by running getadmin.

**nt-getadmin-present**
The getadmin exploit has been run. Problems in Windows NT kernel functions allowed a flag to be set inside the operating system that allows any user to gain administrator privileges. Getadmin leaves a Software\AntiShut key in the registry, and this key has been detected. An early workaround to getadmin developed by ISS was to create that key and deny non-administrators access. If this key is present but is not writable by non-administrators, it is not considered to be a vulnerability.
http://support.microsoft.com/support/kb/articles/q146/9/65.asp

**http-iis-cmd**
The Microsoft Internet Information Server (IIS) 1.0 contains a vulnerability that allows a remote attacker to execute commands on the server via .BAT and .CMD files. It is believed this hole affects other servers, in addition to IIS. Contact your vendor for more information.
http://support.microsoft.com/support/kb/articles/q148/1/88.asp

**nt-iis-rds**
Implicit remoting is enabled via the Microsoft Internet Information Server (IIS) web server. RDS allows an unauthorized user access to ODBC databases via IIS.
http://support.microsoft.com/support/kb/articles/q184/3/75.asp

**iis-rds-odbc**
The system is configured to allow Remote Data Services (RDS) DataFactory objects to be invoked. RDS is part of the Data Access Components installed by default with Windows NT 4.0 Option Pack and Internet Information Server (IIS) 4.0. With RDS, web clients can issue client-based SQL queries to OLE database data sources hosted on the web server.
http://support.microsoft.com/support/kb/articles/Q184/3/75.ASP

**iis-remote-ftp**
This could allow a remote attacker to crash the FTP server and allow a carefully constructed list request to execute arbitrary code on the server. The attacker is required to have a valid login (such as "anonymous") to the server before exploiting this hole.
http://support.microsoft.com/support/kb/articles/q188/3/48.asp

**tcp-seq-predict**
The TCP sequence was found to be predictable. When the TCP sequence is predictable, an attacker can send packets that are forged to appear to come from trusted machines. These forged packets can compromise services, such as rsh and rlogin, because their authentication is based on IP addresses. The percentage guessed is the likelihood that an attacker could predict the sequence and compromise the system.
http://support.microsoft.com/support/kb/articles/q192/2/92.asp

**ldap-exchange-overflow**
A buffer overflow exploit against Microsoft Exchange's LDAP (Lightweight Directory Access Protocol) server allows read access to the Exchange server directory by using an LDAP client. This buffer overflow consists of a malformed bind request that overflows the buffer and can execute arbitrary code. This attack can also cause the Exchange LDAP service to crash. This vulnerability exists in Microsoft Exchange Server version 5.5.

http://www.microsoft.com/security/bulletins/ms99-009.asp

**nt-helpfile-bo**
The Windows NT 4.0 help file utility could allow a malformed help file to overflow buffers inside the program. Help files are typically started by pressing the F1 key or by choosing options from the Help menu in programs. This hole could possibly be manipulated to execute arbitrary code on affected systems.
http://support.microsoft.com/support/kb/articles/q231/6/05.asp

**iis-htr-overflow**
Internet Information Server 4.0 contains the ability to perform various server-side processing via specific file types. A vulnerability exists in the way that .HTR, .STM, and .IDC files are processed. Requests for files ending with these file name extensions are passed to the appropriate external DLL for processing. These DLLs contain unchecked buffers that could allow a long request to overflow these buffers and crash the IIS service. This hole has also been demonstrated to allow remote execution of arbitrary code and exploits have been made widely available.
http://support.microsoft.com/support/kb/articles/q234/9/05.asp

**win2k-dns-cachepollution**
Microsoft DNS server may cache non-secure data in response to DNS query. The non-secure data can be used to redirect queries to a rogue DNS server and can be malicious in nature.
http://support.microsoft.com/support/kb/articles/Q241/3/52.ASP

**nt-rras-dun-cache**
When Routing and Remote Access Service (RRAS) is installed on your computer and you are using the Dial-Up Networking client software to connect to a server, a dialog box requests the user's User ID and password for the server. In the same dialog box is the Save Password check box, which is intended to provide the user with the option to cache their security credentials if desired. However, the implemented client functionality actually caches the user's credentials regardless of whether the check box is selected or not. In general, caching security credentials on a computer is not a good security practice. Cache files can easily be decrypted, or users with access to the machine can access unauthorized systems without authentication.
http://support.microsoft.com/support/kb/articles/q233/3/03.asp

**nt-ras-pwcache**
A bug exists in the Remote Access Service (RAS) and Routing and Remote Access Service (RRAS) clients installed on Windows NT 4.0 SP5 and below that saves the user's password regardless of whether or not the "Save Password" option is disabled. The password is, however, stored in a registry key with strict permissions and the option of being strongly encrypted.
http://support.microsoft.com/support/kb/articles/q230/6/81.asp

**url-asp-av**
A very long Uniform Resource Locator (URL) with hundreds of forward slashes (/) is passed to an ASP page on the Web serve could cause an access violation (AV) to occur.
http://support.microsoft.com/support/kb/articles/q187/5/03.asp

### *Local Escalation of Privilege*

**nt-gina-lockout**
Windows NT gina flaw allowed locked-out users to log in. A vulnerability in Windows NT allows users to use a password on a locked terminal even if that account has been

locked out. This action opens up the possibility for users to make endless brute force attempts to guess passwords at the console.
http://support.microsoft.com/support/kb/articles/Q188/7/00.asp

**nt-privilege-elevation**
This exploit can potentially allow a non-administrative user to gain local administrative access to the system and thereby elevate their privileges on the system. In order to perform this attack, the user has to have a valid local account on the system and be able to run arbitrary code on the system. Normally this means they must have physical access to the computer in order to log in locally to the system. Sensitive systems, such as the Windows NT Domain Controllers, where non-administrative users do not have any local log on rights by default are not susceptible to this threat. The attack cannot be used over the network get domain administrative privileges remotely.
http://support.microsoft.com/support/kb/articles/q190/2/88.asp

**nt-priv-fix**
The sechole.exe utility circulated on the Internet can allow a non-administrative user to gain debug-level access on a system process. Using this utility, the non-administrative user may run some code in the system security context and acquire local administrative privileges on the system.
http://support.microsoft.com/support/kb/articles/q190/2/88.asp

**nt-knowndlls-list**
Windows NT implements a feature that keeps the most used DLL's in memory to improve performance and memory usage. A flaw exists in the permissions normal users have to this KnownDLLs list that allows them to load malicious code in the list and point applications at this Trojan horse code, which will then be executed with administrative privileges.
http://support.microsoft.com/support/kb/articles/q218/4/73.asp

**nt-screen-saver**
A vulnerability in the Windows NT screen saver could allow local administrator privileges to be compromised. The hole exists because under some circumstances the screen saver will fail to drop its elevated privileges and can then be tricked into running arbitrary commands with administrative rights.
http://support.microsoft.com/support/kb/articles/q221/9/91.asp

**nt-ras-bo**
The portion of the Remote Access Service (RAS) client for Windows NT 4.0 that processes phone book entries contains a buffer overflow condition that could allow a local user to cause a denial of service or possibly execute arbitrary code with system privileges.
http://support.microsoft.com/support/kb/articles/q230/6/77.asp

**Q142615**
When you use Event Viewer to examine the Security log file, the Event Log service does not examine the "Manage auditing and security log" privilege as the Concepts and Planning manual states. It does examine the Administrators membership.
http://support.microsoft.com/support/kb/articles/Q142/6/15.asp

## Conclusion

Windows 2000 represents a great leap forward for the security of Microsoft products. In addition, it raises the bar for the entire industry by integrating leading-edge security technologies, as well as addressing the lessons learned from one of the world's most

prolific operating systems. This combination of innovation and experience makes Windows 2000 the most secure operating system Microsoft has ever shipped, and certainly one of the most secure in the industry today.

True enterprise security is a combination of technology and policy. Windows 2000 provides a tremendous infrastructure for secure computing, but requires proper configuration and management to ensure enterprise security. ISS has studied Windows 2000 and can provide the tools and experience to make sure that you can get the most out of this new operating system.

## About ISS

ISS is a leading global provider of security management solutions for e-business. By offering best-of-breed SAFEsuite security software, comprehensive ePatrol monitoring services and industry-leading expertise, ISS serves as its customers' trusted security provider protecting digital assets and ensuring the availability, confidentiality and integrity of computer systems and information critical to e-business success. ISS' security management solutions protect more than 5,000 customers including 21 of the 25 largest U.S. commercial banks, 9 of the 10 largest telecommunications companies, and over 35 government agencies.
Founded in 1994, ISS is headquartered in Atlanta, GA, with additional offices throughout North America and international operations in Asia, Australia, Europe, and Latin America. For more information, visit the ISS Web site at www.iss.net or call 800-776-2362.

IssDoc3/27/2000