Global Information Assurance Certification Paper

Providing Defense in Depth Security for a Windows 2000 Environment

Mr. Dana J. Willis, MCSE, CCA
GSEC Practical Version 1.4, Option 1
January 15, 2005

Abstract

Windows 2000 has emerged as the premier desktop and server operating system of major and minor corporations throughout the world. This emergence requires these corporations to plan, coordinate, implement, and support a "defense in depth" secure environment. To achieve true "defense in depth" security for a Windows 2000 environment, it is critical that all security components of Windows 2000 be understood.

Objective

This paper will uncover security considerations, layers, strategies, and solutions to allow for an organization to provide and master a defense in depth secure environment for their Windows 2000 client/server environment.

Defining "Defense in Depth"

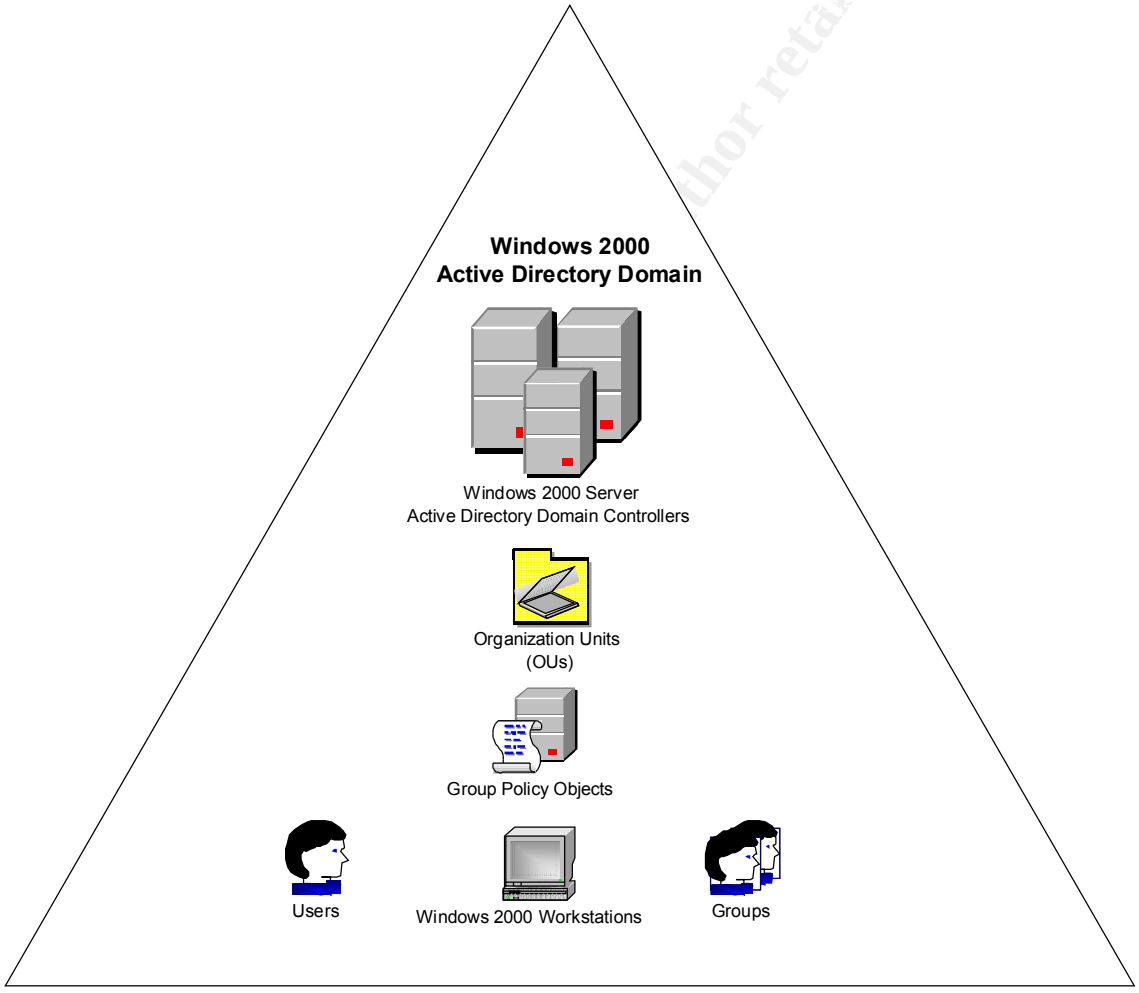
Defense in depth is a security model in which you implement barriers at multiple layers to provide a more secure enterprise. Multiple security layers prevent direct attacks against critical systems and make network reconnaissance more difficult for potential intruders. By deploying multiple layers of security, you help ensure that if one layer is compromised, the other layers will provide the security needed to protect your resources. In essence, you are not allowing a single point of failure. For example, the compromise of an organization's firewall should not provide an attacker unchallenged access to the organization's most sensitive data. Ideally each layer should provide different forms of countermeasures to prevent the same exploit method from being used at multiple layers. This paper will apply this security model towards a Windows 2000 infrastructure.

Assumptions

This paper will focus on a fictitious organization that is utilizing Windows 2000 on both the desktop/client and server side for their daily operations.

For the purpose of this paper, I will only focus on security related to the Windows 2000 base operating system and Active Directory Domain. The server resources of the domain will be made up of Windows 2000 Servers. The fictitious organization will utilize an Active Directory Domain Controller for end-user authentication and resource access.

To clearly identify the Windows 2000 and Active Directory infrastructure of this organization, please refer to the diagram below.



Windows 2000 Security Threats - (Vulnerabilities and Exploits)

The three primary attributes of traditional security are confidentiality, integrity and availability. To provide these attributes in a Windows 2000 environment, an organization must be aware of different categories of vulnerabilities and exploits. This section of the paper will outline some of the more common threats to the security of a Microsoft Windows 2000 environment.

Threats are anything that cause unwanted or unauthorized modification, disclosure, or the unavailability of data. Understanding where these threats can come from is primary to providing a Defense in Depth strategy for a Windows 2000 environment. Windows 2000 security threats come from numerous sources. These sources are identified as follows:

The Internal Threat

Employees or trusted users of an organization who have authorized access to a Windows 2000 environment should be recognized as the biggest threat. Their activity within a Windows 2000 environment can be in the form of malicious or non-malicious. Some examples of malicious threats are users seeking revenge, stealing sensitive information or taking unsupported advantage of their authorization. Non-malicious threats can be taken by trusted users who are unknowingly, passing along viruses via e-mail and/or file transfer, and verbally giving another user credentials to access a sensitive data store. Industry analysts agree that this type of internal activity is the most important to be aware of.

Mobile and Remote Users

Allowing network logon services to your Windows 2000 environment for mobile and remote users poses another significant threat. The number of these authorized users via mobile or remote access has greatly increased. The remote user exposes a Windows 2000 environment to potential security problems in a number of ways. Some of these ways are in the form of:

- A remote user in a public place being monitored as they login to the Windows 2000 environment.
- The public telephone lines being monitored by attackers who are watching for trusted user logon activity.
- Portable systems being stolen, which in-turn leads to that system being in the hands of an un-trusted person who can therefore access unauthorized data.
- A remote system may be accessible to an attacker who can attack the system for hours without being disturbed by security personnel.

The Internet and TCP/IP

The Internet and TCP/IP protocol play a big role in an environment utilizing Windows 2000 for their client/server/application resources. Because the internet is accessible to anyone, an attacker can gain unwarranted access to a Windows 2000 system by gathering TCP/IP packet information via a protocol sniffer. The information within the packets can contain user IDs or passwords, which could allow an attacker to launch an attack upon a Windows 2000 system.

Physical

Although electronically securing a Windows 2000 system is of utmost importance, physically securing a Windows 2000 system should be a primary objective. An attacker with physical access to a Windows 2000 system could easily obtain unauthorized access via a boot disk, boot password or file system permissions. The simple truth here is that if a Windows 2000 system is not physically secure, then any other steps an organization takes can be bypassed.

Phone Attacks

Windows 2000 supports phone line access to its resources via its embedded Remote Access Service (RAS), which can be attacked by a war-dialer service launched by an outside person. With RAS enabled on a Windows 2000 system, an organization is left open even to the public telephone system.

Knowing these threats and potential targets is key for an organization to implement a Defense in Depth strategy for their Windows 2000 environment. The next area of concern is, understanding the multiple attack methods that arise from the aforementioned threats. The following table identifies Windows 2000 common vulnerabilities and attack methods.

Windows 2000 Common Vulnerabilities and Attack Methods

Vulnerability or Attack Method	Description
Authentication Compromises	Intruder acquisition of user account and password
Hacking User Accounts and Passwords	Intruder gathering account and password through network sniffers or easily guessed or cracked passwords.
Default Configurations	Windows 2000 out of the box is not locked down
SNMP	Community string is typically set to public which an intruder can easily interrogate and gather info of that system.
Files and Directories	Default permissions on Windows 2000 File System are not locked down out of the box.
Default Service Installations	Windows 2000 out-of-the box loads many unnecessary services which can be interrogated by intruder.
Buffer Overflows	Buffer area becomes full and other processes can be run against the system without being traced via buffer.
HTTP Form Variables	Similar to buffer overflow but using get or post inputs to a web server. Additional commands can be appended to carry out intruder activity.
Compromised Trusted Systems	Intruder takes advantage of Windows 2000 transitive trusts where he can access data via trust to another system.
Session Hijacking	Intruder takes over TCP connection to system via a DenialofService (DoS), takes affected system offline and then synchronizes his system with affected one.
DNS Cache Poison	Intruder compromising DNS information with bad DNS entries, which affect all Windows 2000 systems requesting DNS information.
Sniffers	Network packet data is captured and interrogated for use to access systems.
Applications and Services	Intruders attack via 1) highly vulnerable services such as Telnet, E-mail, FTP, and DNS., 2) scripting with VB, Java, or ActiveX, or 3) TCP/UDP port stealing.
Denial of Service/DDoS	Intruder removes a Windows 2000 resource from the network via a continuous flood of data from either a single point or multi-node source.
Viruses, Worms, and Trojans	Intruder infects, spreads, and or hides code inside of the Windows 2000 system to cause damage, downtime, or way to gain backdoor access.
Physical Access	Intruders can obtain access of Windows 2000 laptops, workstations or servers via theft or them being unattended and unlocked.

Other Windows 2000 Client/Server Security Vulnerability Considerations

Consideration	Description
System backups	Organizations fail to adequately back up important system data. Of the few that actually perform back ups, not many take the time to restore a file or otherwise validate the success of each back up operation. This can lead to situations where entire sets of backup media have gone bad and cannot be used to restore data lost to an attack or catastrophic failure.
Vendor updates and patches	All software and hardware has vulnerabilities and is in a continuous state of development. Feature improvements, design improvements, and bug fixes will generally be released until the software is no longer useful. Because software and (to a lesser extent) hardware is constantly changing, it is imperative that the IT staff stay current on patches, updates and fixes to their systems. Failure to remain current puts the attacker at an advantage.
Existing security controls	Users often attempt to disable virus protection in hopes of faster processing speeds. Additionally, to achieve greater convenience, they lower or remove macro security protection on productivity applications such as Microsoft Word, Microsoft Excel, and so on. It is important to educate users on the importance of maintaining security controls.
Installation of unapproved software	Users prone to installing unauthorized or unapproved software place the organization at risk by potentially executing applications containing Trojan Horses or other vehicles of security compromise.
Exposure of personal information	Sharing names of children, full birthdates, and so on, enables attackers more opportunity to either guess passwords or acquire unauthorized access by means of social engineering. Information may be shared directly—verbally to the attackers over the phone, through e-mail, or passively by what is stored in the work area (pictures of children, information containing their social security number, health cards, and so on.)
Untrained users and IT staff	Many incidents could be mitigated or avoided if users were properly trained to recognized signs of attack, mis-configuration, virus, or other incidents. They also must be trained to properly respond once they have recognized an attack.
Unnecessary Windows 2000 services	Default installations often enable more services than necessary for operation. These additional services provide more avenues for potential attacks and must be disabled. Only necessary services should be running. Services should periodically be audited to ensure need for them still exists.
Windows 2000 services privileges	Services need a certain level of access in order to perform their specific tasks within the context of the system. When installing or troubleshooting these services, it may be tempting to grant more access than necessary in order to achieve functionality quickly. Services must have the least amount of privilege possible in order to maintain system security. You should ensure that this is enforced by both system administrators who configure service privileges, and application developers who create service dependencies.
Internal security threats	A natural tendency is to focus security efforts and resources towards attacks from outside the organization. Sometimes this tendency results in a lack of focus on the bigger potential threat—people inside your organization. Whether intentional or unintentional, people on the inside of your organization have the most access and therefore pose the greatest potential threat for damage.
Enforcement of	An excellent security policy only loosely enforced will have little

security policy	benefit to the organization. Loosely enforcing security policy also has the dangerous side effect of creating apathy among employees towards security.
Defense-in-depth strategy implementation	While it is important to implement and correctly configure a firewall and an intrusion detection system, security countermeasures must not stop there. For example, your defense-in-depth strategy should specify administrative and personnel-level controls. Many companies fail to adequately train public facing individuals such as receptionists and telephone operators to recognize and protect sensitive information. Failure to adequately protect against all layers of potential attack is a common mistake that leads to a false sense of security

Overview of Windows 2000 Security and Native Components

Active Directory

Because they are so closely intertwined, understanding how security services work in Windows 2000 requires a basic understanding of the Active Directory architecture. Active Directory consists of trees and forests. The tree contains multiple domains and network objects while domains contain network objects. The forest is a collection of trees joined together. Active Directory allows the security to be managed from the top down allowing for a consistent security policy throughout the organization.

Authentication

Authentication is a fundamental aspect of system security. It is used to confirm the identity of any user trying to log on to a domain or access network resources. The Windows 2000 authentication process is part of what enables single sign-on to all network resources. With single sign-on, a user can log on to the domain once, using a single password or smart card, and authenticate to any computer in the domain.

Each user that logs into Active Directory is granted a security access token for authentication. This token consists of an individual Security Identifier (SID), a group SID for each group the user belongs to and user rights. When the user tries to access any AD object this token is compared to an Access Control List (ACL) to verify the user has authority to access the object.

The administrator has several options for user authentication within AD. The default authentication method is Kerberos. This method provides better security, efficiency and interoperability than Windows NT authentication. AD also provides for authentication by Public Key Infrastructure (PKI), smart cards and the older Windows NT standard NTLM. All of the available authentication methods can be used at the same time, by using policies in AD you can specify which type of login that is required for individual users or groups of users according to your security needs.

Kerberos

This is an industry standard authentication. This authentication method not only verifies the clients right to access the network it authenticates the server to the client. When a client Windows 2000 workstation requests authentication to a server the request goes to the Key Distribution Server (KDC), the KDC responds to the client with the requested servers key, the client sends this key along with its request to the intended server, the server then authenticates the user. All of this communication is encrypted for use over an unprotected network.

PKI

PKI authentication is normally done to authenticate external users. The external user must have a certificate, this can be from a trusted certificate authority or can be issued from the certificate server that comes with Windows 2000. The certificate of the external user is mapped to a user account setup for external users, AD uses these mappings to allow access to resources that the user is entitled to use.

Access Control

Windows 2000 implements access control by letting administrators assign security descriptors to objects, such as files, printers, and services. An object's security descriptor includes an access control list (ACL), which defines which users (either by individual or by group) have permission to perform particular actions with that object. An object's security descriptor also specifies the various access events to be audited for that object, such as all write activities to a secured file. By managing properties on objects, administrators can set permissions, assign ownership, and monitor user access.[1]

Not only can administrators control access to a specific object, they can also control access to a specific attribute of that object. For example, through proper configuration of an object's security descriptor, a user could be allowed to access a subset of information, such as employees' names and phone numbers, but not their home addresses.[2]

Using an object's ACL, Windows 2000 compares information about the client and the information about the object to determine whether the user has the desired access rights (for example, read/write permission) to that object (for example, a file). The access check is done in kernel mode within the security subsystem of Windows 2000. Depending on the outcome of this comparison, the service will respond to the client, either serving the object or returning an access-denied failure. [3]

Windows 2000 protects securable resources from unauthorized access by employing discretionary access control, which is implemented through discretionary access control lists (DACLs). DACLs, usually abbreviated to ACLs, are a series of access control entries (ACEs). Each ACE lists a principal and contains information about the principal and the operations that the principal can perform on the resource. Some people may be granted read access, and others may be granted full control. The type of ACE depends on the type of securable object.
A securable object is any object that has a security descriptor containing security information, such as the owner's SID and ACL data, about the object. Examples of securable objects include the following:

- NTFS files and directories
- Named and anonymous pipes
- Processes and threads
- Services
- Network shares

An ACL is a simple data structure. It contains a series of owner information and zero or more ACEs. Each ACE contains a SID and access information pertaining to that SID, such as read, write, open, create, and so on. ACLs are applied to resources requiring protection and are

[1] Microsoft Corporation. "Windows 2000 Server Technical Overview", p. 13.
[2] Microsoft Corporation. "Windows 2000 Server Technical Overview", p. 13
[3] Microsoft Corporation. "Windows 2000 Server Technical Overview", p. 13

referred to as discretionary, because deciding who has what degree of access to the object is at the discretion of the object owner. [4]

Windows 2000 also includes support for explicitly denying access to an object by using deny permissions. For example, if all users (Everyone) except for Tommy must have access to a file, the following permissions would be set: Everyone (Read) and Tommy (Deny Full Control). Because deny permissions are always checked before allow permissions, Tommy will always be denied access to this object. For this reason, the Everyone account should never be denied access to an object; the Windows shell issues a warning if this is attempted. [5]

Different objects have different permission types, for example:

- Files can have their permissions set and can be written to, read from, and created.
- Active Directory objects can have specific settings on object properties, such as the ability to read a user's certificates or set the user's e-mail address.

When a principal attempts to access a resource, Windows 2000 performs a simple DACL check. It does this by checking the SIDs in the user's token for the type of access requested against the SIDs in each ACE of the resource's ACL. Windows 2000 denies access to the object if none of the ACEs allow the user access, or if an ACE denies the user access; otherwise, access is allowed. Furthermore, when a restricted process or thread tries to access a securable object, the system performs two access checks: one uses the token's enabled SIDs, and another uses the list of restricting SIDs. Access is granted only if both access checks allow for the requested access. [6]

Trusts

Active Directory uses trust relationships to allow Windows 2000 users the use of single sign-on. This means that a user from one domain can access resources from a trusted domain without being prompted to authenticate to the resource domain. Windows 2000 Active Directory allows for a transitive trust relationship throughout the Domain Tree, where if Domain A trusts Domain B and Domain B trusts Domain C, then Domain A trusts Domain C. These trusts are two way implicit trusts between the parent domain and all of the child domains. The child domains trust each other based on the fact that the parent domains trust the other domains. Transitive trusts between trees in the forest can also be established, but they must be established manually.

Delegation of Authority

Because AD is designed with large, segmented organizations in mind, domains within a tree can be administered as a single entity, while still having the ability to delegate control of a container object to a user or group. Administrative control can be delegated to any level of a domain tree by creating organizational units. These OUs include the objects over which you want to delegate control. The administrative control over the OU would be granted to particular users or groups. At the OU level, an administrator can grant permissions for specific operations, such as who can create groups, who can control membership lists for those groups, or who can add computer accounts to the domain.
Further, because of fine-grained access control, administrators can narrowly define the scope of delegated tasks. For example, rather than having to give the support group full access to user account records, an administrator can give the support group the ability to reset a user's password, but not the ability to change his or her address.

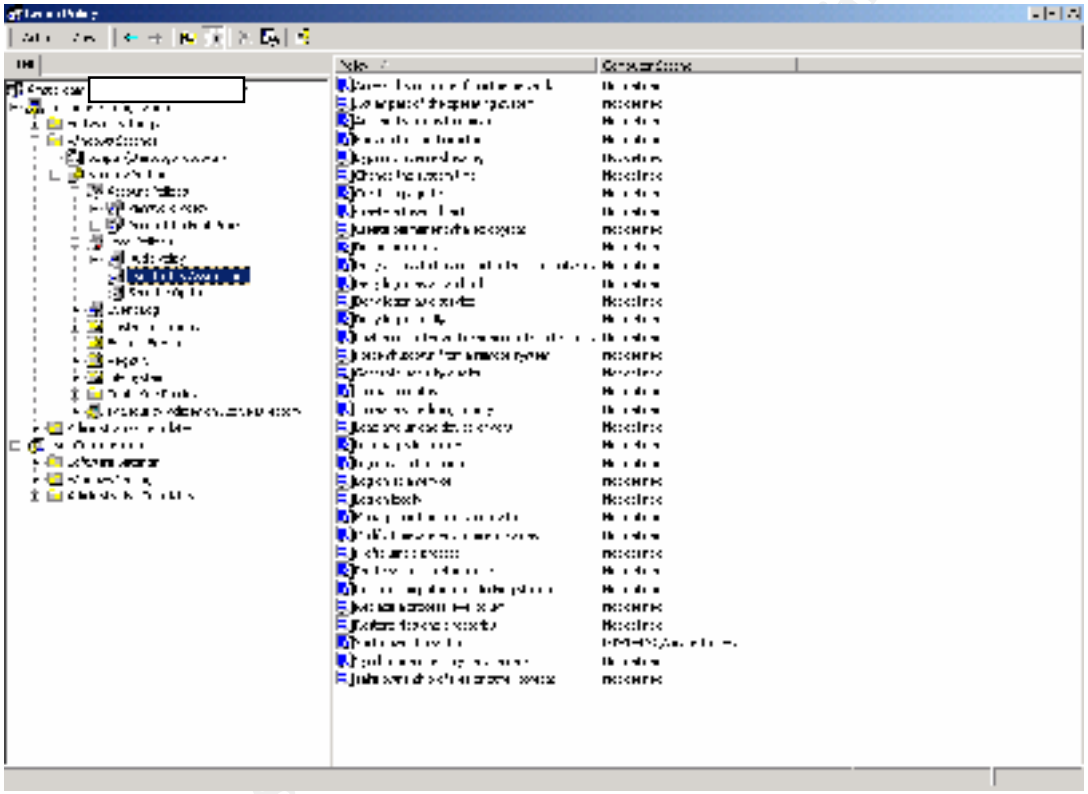
---

[4] Microsoft Systems Architecture: Internet Data Center – Reference Guide Chapter 4 – Security Design – Authorization, p. 60
[5] Microsoft Systems Architecture: Internet Data Center – Reference Guide Chapter 4 – Security Design – Authorization, p. 60
[6] Microsoft Systems Architecture: Internet Data Center – Reference Guide Chapter 4 – Security Design – Authorization, p. 60-61

Security and Group Policies

Security is set in Active Directory using group policies. This allows the administrator to set a uniform security policy across the domain. These policies can be set at the highest level of the organization and pushed down to all users. It is also possible to set a base security policy for the corporation and give domain administrators the right to alter only portions of the policy.

Windows 2000 Group Policies are used to define configurations for users and computers in a Windows 2000 environment. To provide an additional layer of defense, Group Policies allow an organization to configure user and computer security related settings, such as, password, user-rights, and lockout policies. The following diagram illustrates the Group Policy configuration tool where each policy is defined. These policies can then be applied at the Site, Domain, Organization Unit and Local segment of the Windows 2000 Active Directory.



Encryption

Windows 2000 provides encryption for IP packet data via Internet Protocol Security (IPSec). Although it is not a true part of Active Directory, (IPSec) plays an important part of Windows 2000 security. IPSec provides integrity, authentication, confidentiality, and nonrepudiation for IP packets. IPSec is defined within security policies in Active Directory or Windows 2000. IPSec can be used to secure communications throughout the network. An example of this would be if communications across the network from the Human Resources department to the server are required to be encrypted to prevent protocol sniffiing. File resources can also be protected via Windows 2000 Encrypting File System (EFS). This encryption can be used with any application since the O/S is doing the work.

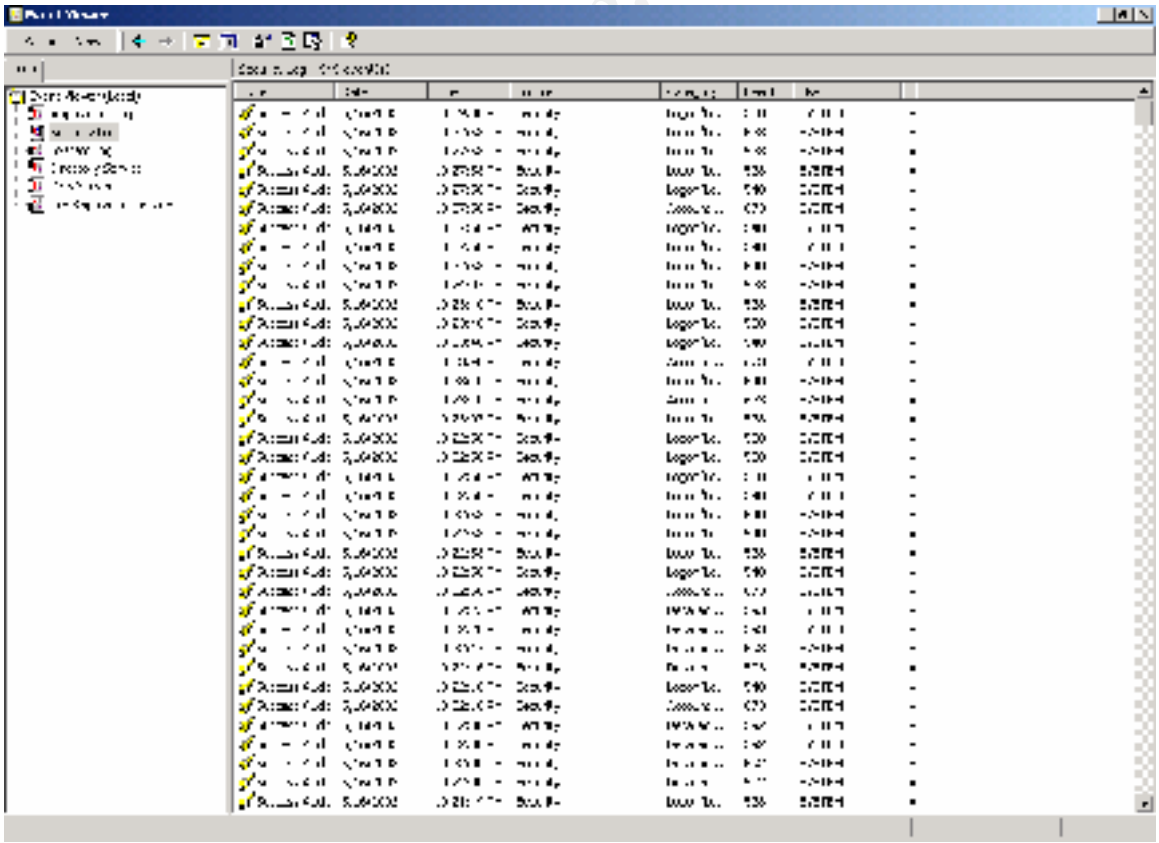
Security Identifiers (SIDs)

All user names and group names are labels that are assigned to the Active Directory objects to allow users and administrators an easy method of identification. Internally, the operating system refers to each Active Directory object by a number that uniquely identifies that object. Each object is issued a unique SID when it is first created. If a user account is deleted, and then another account is created with the same name, the new account will not have the same SID as the original account and therefore, the rights or permissions previously granted to the old account will not apply. [7]

Auditing

Windows 2000 workstations and servers provide the ability to audit all security related events via built-in Event Logging as shown below. To capture these security event logs, an organization must enable security auditing, which can be done throughout the enterprise through Domain wide Group Policies. The audit logs help an organization determine the extent of damage of a security breach. The following identifies what the audit logs can capture.

- Failed logon attempts
- Attempts to access sensitive data
- Changes to security settings
- Process tracking
- User, Group, File, and Policy object access, modifications and deletions



[7] Microsoft Systems Architecture: Internet Data Center – Reference Guide Chapter 4 – Security Design – Authorization, p. 59-60

Solutions to provide Defense in Depth Security for a Windows 2000 Environment

Given all the information provided in the previous sections, it is safe to state that providing a Defense in Depth strategy for a Windows 2000 environment will need to address a multitude of layers.

Implementing Defense in Depth Security for a Windows 2000 environment can be accomplished via knowing your resources, and selection of technology that can be integrated to work closely together.

Technology solutions that work closely together can obtain Defense in Depth for a Windows 2000 environment by providing:

- Network based Intrusion Detection
- Firewall Management
- Virus Detection
- Vulnerability Assessment
- Security Policy Enforcement
- Configuration Management
- Centralized Monitoring
- Event and Data Consolidation
- Host based Intrusion Detection
- Automated Response
- Incident Workflow
- Service Level Compliance and Reliable Reporting

Combining and integrating all of these functionalities/requirements is the key to providing Defense in Depth for a Windows 2000 environment. Once integrated, it would be ideal for the organization to centrally monitor, manage, and report for security activity via a Security Operating Console. (SOC). To accomplish this, the organization running Windows 2000 would want to consider the following technology solutions.

Functionality/Requirements	**Solution**
Network based Intrusion Detection	ISS RealSecure Network Sensor
Firewall Management	CheckPoint Firewall 1
Virus Detection	Norton Anti-Virus Corporate Edition
Vulnerability Assessment	NetIQ Security Analyzer
Security Policy Enforcement	Microsoft Security Configuration Manager
Configuration Management	NetIQ Group Policy Administrator
Centralized Monitoring	NetIQ Security Manager
Event and Data Consolidation	NetIQ Security Manager
Host-based Intrusion Detection	NetIQ Security Manager
Automated Response	NetIQ Security Manager
Incident Workflow	NetIQ Security Manager
Service Level Compliance & Reliable Reporting	NetIQ Security Manager

These solutions are recognized as best of breed solutions for the functionality they provide and will be illustrated below on how they can allow the fictitious organization to provide Defense in Depth for their Windows 2000 environment. The integration among these technology solutions would enable the fictitious organization to maintain confidentiality, integrity and availability via multiple defense layers.

ISS RealSecure Network Sensor

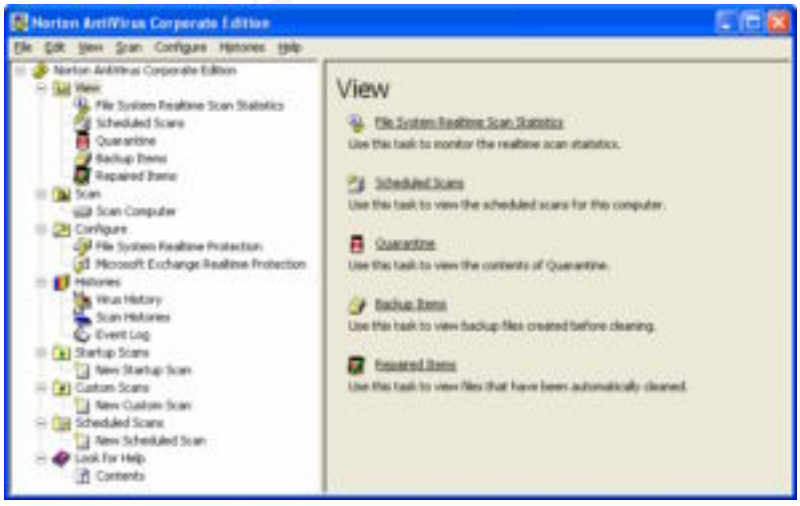
The **RealSecure Network Sensor** provides broad-based detection, prevention and response for attacks and misuse that originate from across a network.
Network sensors monitor network packets and look for events that could indicate an attack against your network. Network sensors monitor all the traffic on their network segments. A network segment is also called a "collision domain" because the network is shared among all of the devices on a single segment and because a station on this segment can see all of the traffic going to other stations. Network sensors provide the earliest possible warning of unauthorized activity and can often terminate the attack before damage is done.
A network sensor is installed on a Windows 2000 computer with a network adapter card that supports promiscuous mode. Promiscuous mode capable cards are required for network sensors only.

CheckPoint FireWall-1

CheckPoint FireWall-1 is an enterprise security suite that integrates access control, authentication, network address translation, content security, data management and auditing. It enables organizations to define and enforce a single, comprehensive security policy that protects all their Windows 2000 network resources enterprise-wide. Its primary responsibility is to keep unwarranted access to the internal Windows 2000 environment from external hackers. It can accomplish this by creating rules for what TCP ports are acceptable on an incoming and outgoing basis. CheckPoint FireWall-1 serves as the initial perimeter layer of defense for an organization's Windows 2000 infrastructure.

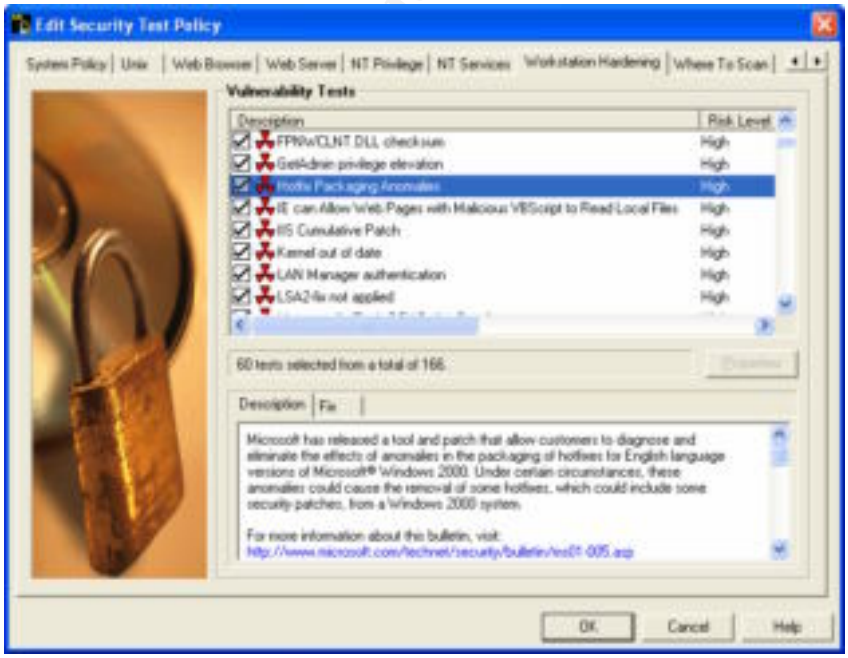
Norton Anti-Virus Corporate Edition

Norton AntiVirus Corporate Edition safeguards Windows 2000 workstations/servers from virus infection. Computers are protected from viruses that spread from hard drives, floppy disks, email attachments, and others that travel across networks. Files within compressed files are scanned and cleaned. No separate programs or options changes are necessary for Internet-borne viruses—File System Realtime Protection scans program and document files automatically as they are downloaded. Norton AntiVirus Corporate Edition responds to infected files with actions and backup actions. When a virus is detected during a scan, Norton AntiVirus by default, attempts to clean the virus from the infected file. If the file is cleaned, the virus is successfully and completely removed from the file. If for some reason Norton AntiVirus Corporate Edition cannot clean the file, Norton AntiVirus Corporate Edition attempts the backup action, moving the infected file to the Quarantine so that the virus cannot spread. The following diagram illustrates the console an organization would use to initiate virus scans of their Windows 2000 resources.



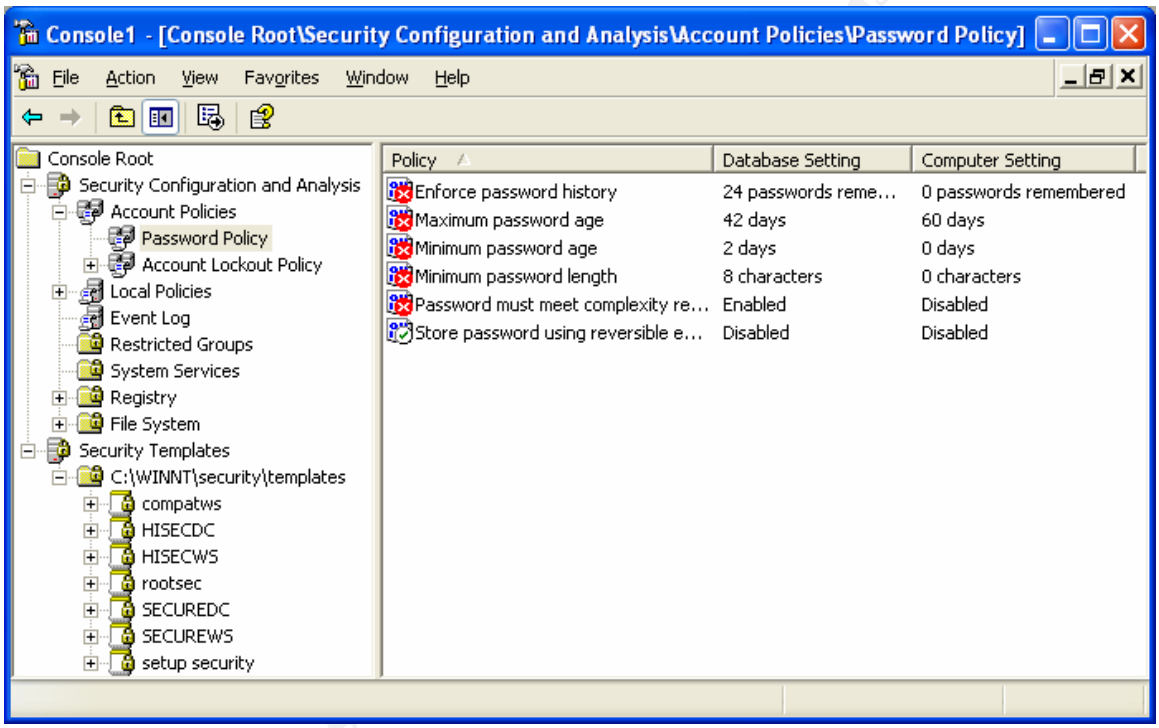
NetIQ Security Analyzer

NetIQ Security Analyzer is a vulnerability scanning and assessment product that discovers and identifies fixes by providing more than 2,300 tests for Microsoft Windows 2000 workstations and servers. Systems are analyzed on demand or at scheduled intervals. The results are used to generate comparative reports, recommend security fixes and prioritize responses. Recognizing the dynamic nature of security threats, the product's AutoSync function allows you to seamlessly update Security Analyzer with the latest security tests from NetIQ. The following diagrams illustrate how a Security Analyzer profile and scan are configured to test for known vulnerabilities. The end result of the scans can then be summarized via a report with recommended fixes for the detected vulnerabilities.



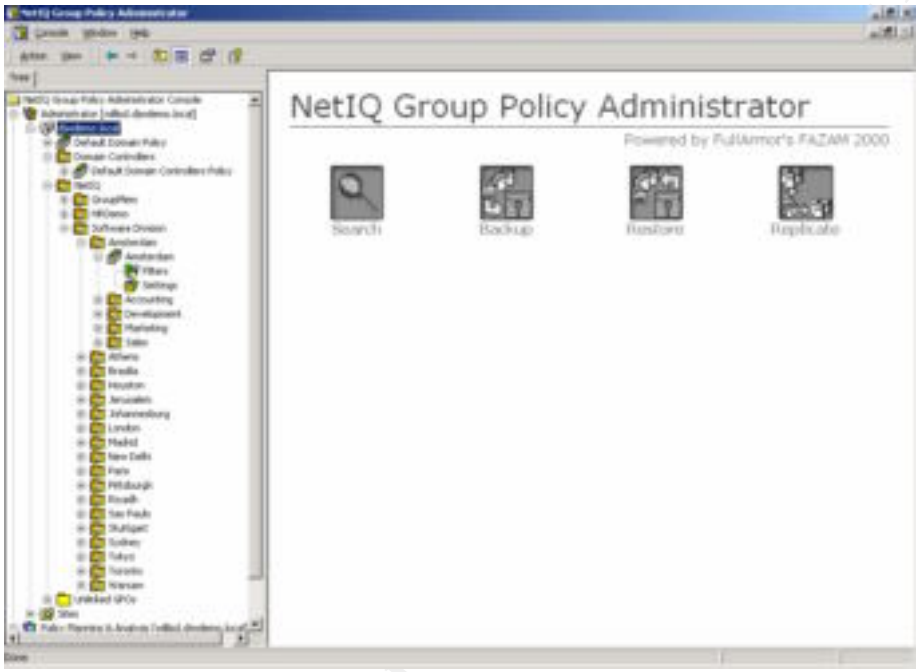
Microsoft Security Configuration Manager

Microsoft provides a Security Configuration and Analysis MMC snap-in to compare a current Windows 2000 system configuration against a pre-defined Security configuration in a database. The security configuration and analysis database, which is also referred to as the local computer policy database, is a computer-specific data store that is generated when one or more configurations are imported to a particular computer. Performing an analysis provides you with information about where a particular system deviates from the stored configuration. This information is useful for troubleshooting problems, tuning the security policy, and, most importantly, detecting any security flaws that might open up in the system over time.
The database is initially created from a Security template policy. The following diagram illustrates the results of a policy scan done by the Security Configuration and Analysis tool.



NetIQ Group Policy Administrator

NetIQ Group Policy Administrator is a Windows 2000 Group Policy solution for planning, managing, troubleshooting and reporting on Group Policy. This solution will allow an organization to effectively implement their change and configuration management of their Windows 2000 resources.
Group Policy Administrator allows an organization running Windows 2000 to manage virtually all aspects of Group Policy. Group Policy Administrator provides a central, easy-to-use console, where an organization can plan and analyze the set of effective policies, perform health/status checks, diagnose problems and delegate GPO (Group Policy Object) management. The following diagram illustrates the interface, which streamlines daily GPO tasks, such as backup/restore, search, managing settings and reporting.



NetIQ Security Manager

The backbone of a Defense in Depth strategy should begin with a centrally managed security framework. This can be accomplished by implementing NetIQ Security Manager.

NetIQ Security Manager assists the organization in reducing exposure time, which is defined by detection time plus response time. E(t) = D(t) + R(t).

NetIQ Security Manager is a Centralized Real-Time Security Risk Management solution. Security Manager's primary functionality provides host-based intrusion detection, data consolidation, incident management, automated response, knowledge management, and reporting. The product is enterprise scalable to thousands of Windows 2000 workstations and servers and allows an organization to integrate and leverage security events from other security solutions operating within the enterprise. It is designed to capture, consolidate, alert, correlate, and manage security events from a single console.

Security Manager is full of knowledge about computer and network security. This knowledge is pro-vided through organizations, such as the SANS (System Administration, Networking, and Security) Institute Center for Internet Security and Microsoft.

Security Manager's knowledge is provided out-of-the box with its pre-defined ActiveKnowledge Modules (AKMs). These AKMs are collections of rules, scripts and knowledge, which identify, detect and describe security activity performed on your Windows 2000 workstations/servers and applications.

The knowledge takes the form of rules and reports. Rules are the evaluation criteria that Security Manager uses to determine whether an event entering the monitored resource should raise an alert or not. Security Manager provides more than 1,200 rules out of the box. The rules include:

- Detect what ports a managed resource is listening on
- Automatic detection when event logs are cleared
- Detect harmful, or unauthorized, processes that are running or attempting to run
- Interactive logons with service accounts
- Individual user logon and logoff
- IIS long URL denial of service attacks
- Suspect e-mail containing possible viruses, Trojan horses, or malicious content
- Unauthorized use of RAS services
- Changes in sensitive group memberships
- Changes to sensitive files and directory's security attributes
- Integration with ISS RealSecure, CheckPoint FireWall-1, and Norton anti-virus solutions.
- Detecting the use of password hacking software, such as L0phtCrack

Security Manager would automatically detect these activities and generate an alert, which identifies who made the change, what they changed, where the change was made, and when this activity occurred. On top of this, an automated response could be generated to: undo the activity if not supported by company policy or send an e-mail to a security group member.

Other examples of automated responses include:

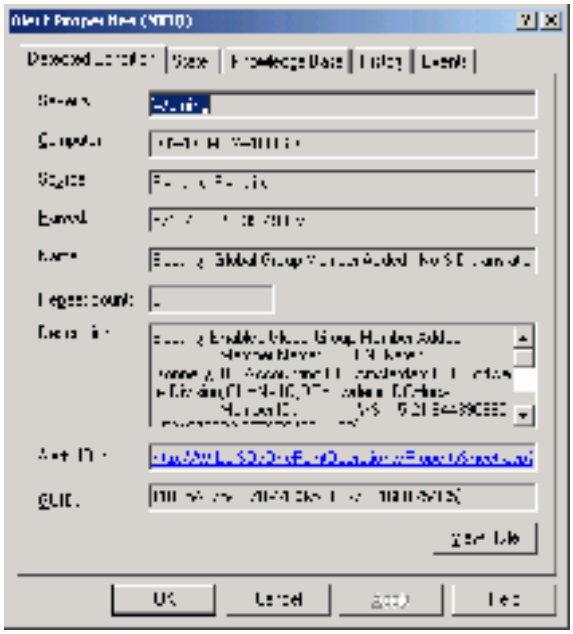
- Disable userid
- Enable userid
- Logoff user
- Shutdown resource
- Reboot resource
- Automatically deny IP addresses to IIS Web servers

These features are of little value if the security or IT teams is unable to effectively report on the state of their environment. Security Manager addresses this by providing 60 reports that focus on security vulnerability and the state of the environment. Some examples include:

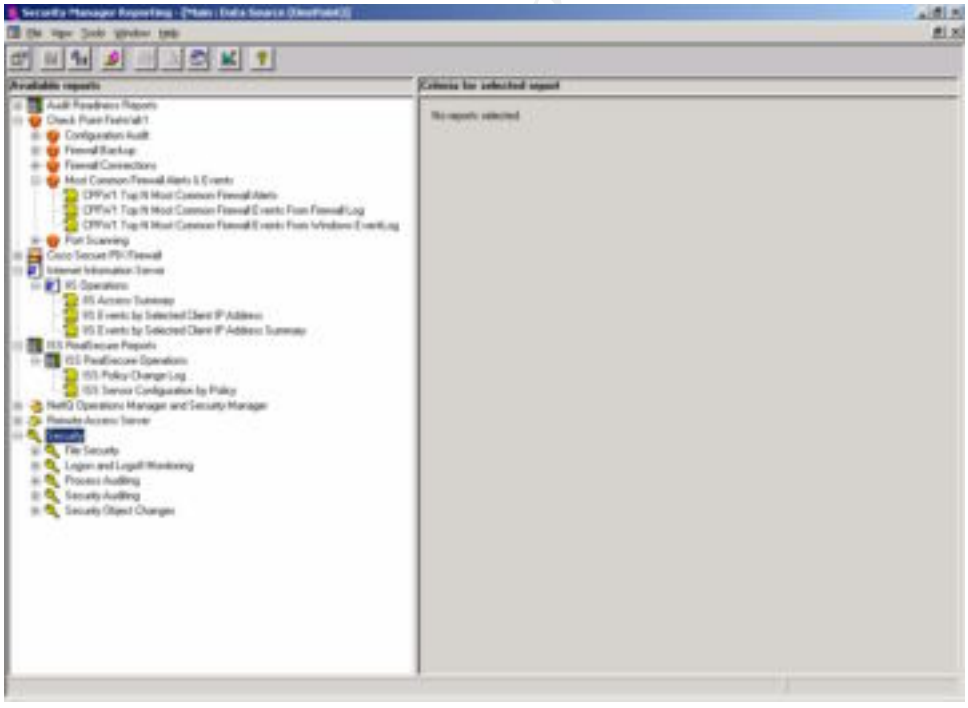
- User Logon and Logoff across the enterprise
- Changes in file security attributes
- Additions and Subtractions of members to groups
- Most common events in the managed environment
- Most common alerts generated by Security Manager
- New computer accounts
- Multiple logon violations within the past 24 hours
- Programs used by user
- Resource auditing by server

The following diagram illustrates the Security Manager management console in which a summary of all security related events and alerts are displayed. The console allows for an organization to drill down into each security related event or alert to determine what caused the incident, manage and document the situation, and add or review information to how, who or what can or was done to correct the incident.

The following diagram is a dialog box provided by Security Manager to identify, manage, and document the security alert.



The following diagram illustrates the categories of reports that can be collected to allow an organization to pro-actively identify, manage, correlate and trend their security incidents.



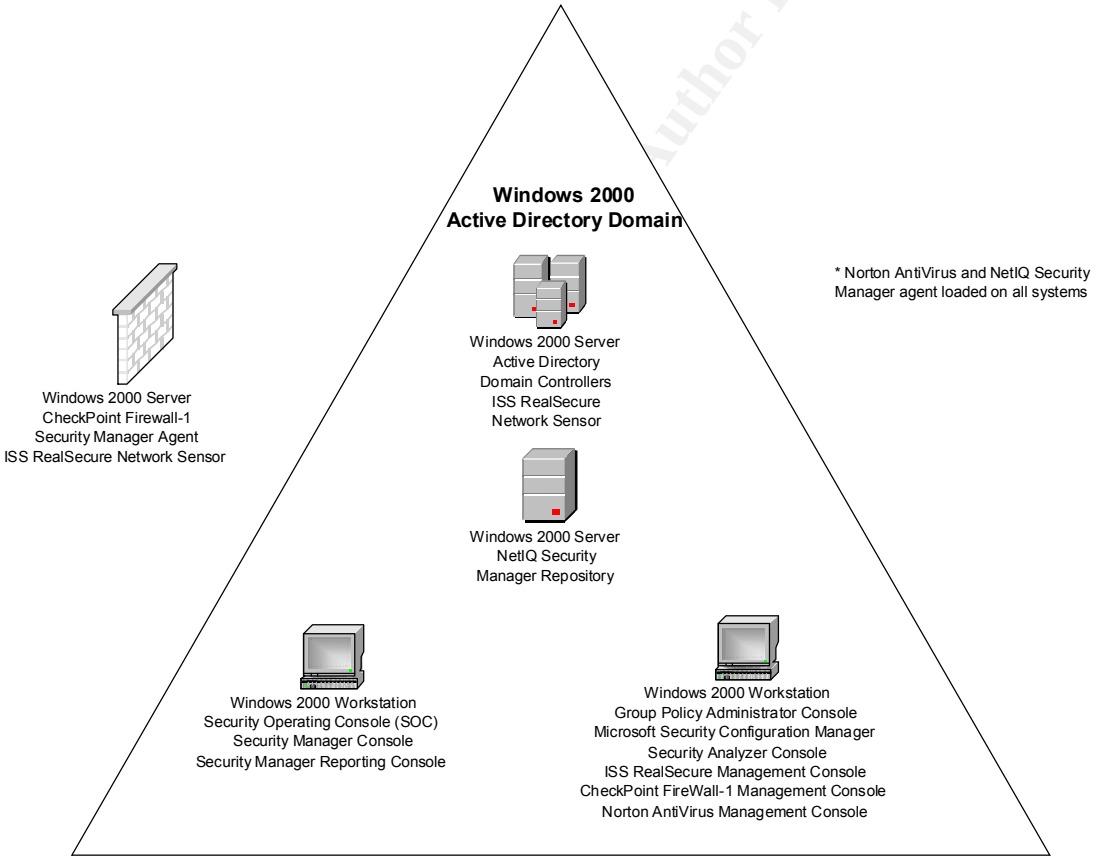
NetIQ Security Manager would be the ideal choice for an organization seeking to centrally monitor and report for all security related incidents, while providing real-time host based intrusion protection. Being able to integrate with other defense layer security solutions gives the organization running Windows 2000 the one single pane of glass view of their security infrastructure, thus providing multi-functional, secure Defense in Depth.

Summary - (Conclusion)

In conclusion, an organization seeking to provide a multi-layered Security Defense in Depth strategy for their Microsoft Windows 2000 environment, must identify known security threats and vulnerabilities, Windows 2000 core security functionalities and implement a combination of best of breed security technology solutions. The organization that can integrate the technologies aforementioned above will go along way in maintaining a secure Windows 2000 environment.

Implementing these technologies with NetIQ Security Manager gives the organization a "single pane of glass" view of all their security related incident, performance, and reporting management. This would enable the organization to provide a centralized Security Operating Console (SOC), thus allowing the organization to stay out in front of all their security management technologies, and to provide Defense in Depth security for their Windows 2000 infrastructure.

The following diagram illustrates how the organization would architect these best of breed technology solutions for their environment. NetIQ Security Manager would be the centralized management solution in which all other technologies would feed its data to.



References:

Windows 2000 Active Directory Security Overview
http://rr.sans.org/win2000/win2000.php

Windows 2000 Security Technical Overview
http://www.microsoft.com/windows2000/docs/SecTech.doc

Security Administration Operations Guide for Windows 2000 Server
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/maintain/opsguide/secadmog.asp

Microsoft Systems Architecture: Internet Data Center – Reference Guide Chapter 4 – Security Design: Authentication
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/idc/rag/ragc04.asp

Cox, Philip; Sheldon, Tom. "**Windows 2000 Security Handbook**", Osborne. February 27,2000

Network and Host Based Vulnerability Assessment
http://documents.iss.net/whitepapers/nva.pdf

Securing the Enterprise with NetIQ Security Manager
http://download-src.netiq.com/Library/white_papers/Securing_the_Enterprise_with_NetIQ_Security_Manager.pdf

Creating and Analyzing a Security Configuration Database
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/reskit/prdd_sec_tzug.asp

Top 10 Tips for Securing Windows
http://download-src.netiq.com/Library/white_papers/NetIQ_Top10Tips.pdf

Lower IT Costs through Anti-Virus Management
http://enterprisesecurity.symantec.com/content/displaypdf.cfm?pdfid=1&PID=na&EID=0

NetIQ Corporation
http://www.netiq.com/solutions/security/default.asp

Symantec Corporation
http://enterprisesecurity.symantec.com/products/products.cfm?productID=23

CheckPoint Software Technologies
http://www.checkpoint.com/products/security/firewall-1.html

Internet Security Systems
http://www.iss.net/products_services/enterprise_protection/rsnetwork/sensor.php

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS