Global Information Assurance Certification Paper

Windows 2000 Security Technologies

GSEC V1.4a

Christopher Cole

Table of Contents

Windows 2000 Security Technologies

Abstract

This paper was written to identify and discuss some of the security technologies that Microsoft has implemented in its Windows 2000 operating system. The information included involves a general discussion on the various techniques a hacker may use to infiltrate a system and the security that Windows 2000 uses to combat those attacks. This paper also includes discussions on how Windows 2000 administrators can secure their systems by use of policies, best practices and security tools created by Microsoft. After reading this document the reader will have a general understanding of Windows security issues, the types of attacks and methods to avoid those attacks on their Windows 2000 based network.

Introduction

With regards to Windows 2000 many security features have been implemented to aid in securing computers and the network with use of policies and tighter security protocols. In the modern environment security is a key technology that will help to move organizations into the future. With proper security methods practiced by an organization a company may more safely move into the future and not have to worry about various outside or inside threats to their infrastructure. Over time proper security methods could help an organization financially by protecting its information technology assets. The past few decades have brought many changes to how we define computing. Information systems have gone from large centralized computers (mainframes) running over proprietary networks and protocols to decentralized, distributed desktop systems and networks running over standard protocols. Information may no longer be kept in a single site, but rather two or many different sites. This distribution is also made possible by protocol standardization in the industry such as a common communication protocol called TCP/IP. This commonality has given industries the ability to interconnect their organizations at a significant cost savings when compared to the proprietary protocols used in the past. This standardization of protocols has increased the potential for error or exploitation as the proprietary protocols offered some protection in their obscurity of operation to the average individual.

Predominately everyone dealing with business networks or information systems today refers to their systems as "interconnected". The concept of connectivity for everyone has become a standard in the work place, and now includes traditional desktops, Personal Digital Assistants (PDAs), phones, pagers and cars. In the end, the result is connectivity that creates effective communication practices, allowing users, networks and applications to receive accurate data quickly that can be translated and understood. Additionally, from a security standpoint, that data transmission is only delivered to the person for whom it is intended.

TCP/IP and Win2k

Over the last decade, networks and computers on the Internet have been exposed to a number of different kinds of attacks utilizing troubleshooting features or modifications of

the TCP/IP protocol stack. TCP/IP is used as the primary communications protocol for almost every Windows 2000 network. It is important to understand how TCP/IP works in order to properly protect a system from network based attacks.

Hackers have used various techniques to initiate attacks on systems including SYNFlood, IP-spoofing, Source-Routing and other types of packet manipulations such as the "Ping of Death". For quite some time the Windows NT platform was not secure and was considered very susceptible to attack. There are many attacks aimed at the TCP/IP protocol. One of the most common attacks goes by the moniker of 'smurf'. A Smurf attack operates by sending a spoofed ICMP echo-request packet where the source field of the IP header has been modified to reflect the IP address of the target of the attack. IP spoofing is when an attacker uses an IP address that a target computer assumes is trusted. The ICMP packet is sent to a broadcast address of a large network, which causes every system on the network to reply to the echo-request. By sending a single spoofed packet to a class B network it would be possible to force over 65000 replies to be sent to the target system. According to Security Administrator magazine, "The Smurf attack is quite simple. It has a list of broadcast addresses which it stores into an array, and sends a spoofed ICMP echo request to each of those addresses in series and starts again. The result is a devastating attack upon the spoofed IP. Depending on the amount of broadcast addresses used, many, many computers may respond to the echo request."**[1]** As a result of a weak TCP/IP stack attacks on NT systems were very common and happened frequently to those who did not secure their server behind a firewall or have good security practices inside the firewall. This prompted Microsoft to re-write their TCP/IP protocol stack and re-write portions of the OS that needed updating, thus came Service Packs and HotFixes. The Windows NT revisions have paid off and now the NT based operating systems are much more stable than they once were.

The New Era – Win2k

Before the Win2k platform was released the protocol stack was once again revised. Microsoft's efforts have greatly improved the protocol stack and created a more secure OS, however, there are still vulnerabilities that a security minded professional must consider.

Since the emergence of Win2k, new methods of attack have come to surface, thus exposing the OS to additional vulnerabilities. The Win2k stack is still vulnerable to hackers by using UDP fragmentation or what is sometimes known as Denial of Service (DoS). When the DoS attack begins the Win2k machine will lock up due to processor utilization reaching 100% from a rogue machine sending packets at a high rate of speed till the machine freezes and can't process them anymore. Once the target machine is disabled a malicious person may spoof its IP address thus making other machines see it as a trusted computer. Once a hacker has access to the network with a spoofed IP they can gather all kinds of information or execute further attacks. It is sometimes difficult to pinpoint where a DoS attack is coming from, because there may be several machines in conjunction serving the attack. As time goes on Microsoft will most likely develop new

[1] Editors, et al. "TCP/IP Flooding with Smurf." Security Administrator. October 1997.

methods to avoid attacks of this nature. Patches and service packs are developed to tighten the security of a computer, thus preventing attacks. Of course, hackers will continue to develop methods of their own to overcome the advancements in security so the Microsoft vs. Hacker will be a long rivalry. A more thorough definition of DoS can be found at the Carnegie Melon Software Engineering Website at http://www.cert.org/tech_tips/denial_of_service.html.

Today's System Threats

Today's hackers are more sophisticated, more motivated, and have better, more easily accessible tools to break into systems. The advent of cellular phones, PDAs and other devices has made access to corporate networks easy. For example a hacker could walk around a business center with a PDA and wireless network card and use a network sniffer till he/she finds an exploitable signal thereby gaining access to the network. **[13]**

Well, who are these hackers and what do they want? Many of them are just curious people bored and looking for a challenge. They really do not have a threat in mind, but they just like the challenge and triumph of accessing a closed network. This hacker could be the kid next door on an America Online dialup with some random hacking tool that a friend gave to him. That means that kid now knows enough to be dangerous to an unsuspecting system. However, there are people out there have much more in store for your system; they are the hard core hackers that are very knowledgeable about computers, security techniques and they have technically advanced methods to infiltrate into systems. It is not uncommon for a competitor to hire a hacker to break into a system in order to help the company identify the security holes. If the hacker's infiltration is done right a company may never know that precious trade secrets or other company information was compromised. In October 2000 Microsoft verified that a hacker gained access to the source code, or blueprints, of Microsoft's Windows-based software, which is estimated to run on about 90% of the world's PCs, which demonstrated that not even the company that develops the Windows 2000 operating system is safe from hackers. This particular hack was done with aid of the QaZ virus which is a worm that opens a hole in the network, which makes an easy access point. This kind of virus is also known as a Trojan horse on a Win2k based system. **[11]** What would hackers take from a company if they gained access? A list of possible targets is below and may give you an idea of what somebody with malicious intent would look for:

- Research Information
- Product Information
- Customer lists
- Employee records
- Server information (i.e. data storage systems, bandwidth information)
- Building access information

Newsgroups offer a great place to share information on virtually anything related to

[11] Weisman, Robyn. "Microsoft Rocked by Hack Attack". NewsFactor Network. October 2000.
[13] Charny, Ben. "Wireless Offices—a hacker boon?". ZDNet News. 25 January 2002.

hacking. A common attack is where a hacker will "deface" a website. This entails gaining access to the web server that is hosting a site and finding a method to access the data store that is holding the website data files. Websites hosted with IIS servers were a particularly easy target because they offered so many vulnerabilities. If those data stores are not secured, the information contained within can be deleted and replaced with something inappropriate, but most the website hackers just leave a calling card and don't actually destroy data. In fact several years ago the CIA, Department of Justice and other government agency websites were hacked. The hackers left messages on the website to support their cause, which was based on the movement for free internet speech. **[12]**

How Attacks are implemented

To really understand hacking you have to understand the behind the scenes methodologies and thought processes. The most common hacking practices today are:

Systematic: This kind of attack usually is more precise and preconceived. There is a method and a step by step approach to this kind of attack. Usually, this attack has many dependencies such as a Denial of Service (DoS) on a machine, next IP spoofing, then followed by data modification.
Quiet: This is a quiet, slow and thought out process. This attack uses many different machines for one common goal and is done over a long period of time. This type of attack is used for gathering information while not being detected.
Unorganized attack: Usually noisy and clumsy. If an organization has system monitoring of any kind, this type of attack can be quickly noticed and avoided. Moreover, the hacker usually is aware he/she will be noticed. Basically, the hacker will throw everything at the system at one time to see what kind of response is issued.

If you have been hacked there are a few things you can do initially to protect the rest of your environment.

1. Start at the OS level and verify that all HotFixes, OS service packs and application service packs are installed according to Microsoft standards.
2. Make sure passwords on your network are complex and secure.
3. Check the logon and log-off scripts that are used on the network.
4. Disable all un-needed services and accounts.
5. Verify the service account passwords have been changed.
6. Check the user rights and permissions. Make sure there are not any unexplainable accounts in any of the administration groups.
7. No default passwords!

By no means is this list complete, but these are a few areas that hackers will target in order to gain access. It's better to be proactive than reactive and by already having the items listed above can help to prevent attack.

---

[12] Drash, Wayne B. and Morris, Jim B. "Hackers Vandalize CIA Homepage". September 1996.

Win2k Security

Windows 2000 offers features that it automatically runs by default and there are things a security minded professional can do to tighten Win2k environment in order to make it more secure. Window 2000 security technologies span a much greater distance than the NT 4.0 platform and any previous versions of Windows. The Win2k platform has introduced: single sign-on, integrated security, secure administration, better authentication methods, interoperability standards and very in depth auditing of your systems and access of those systems.

With the advent of Active Directory Win2k directory services can now use a domain policy which can be distributed over the whole organization. Win2k Policies offer a good way to manage security large enterprise-wide companies. Using domain policies security engineers can harden the Win2k environment on the hardware side as well as the application/software side. These policies can be distributed or set specifically on an organizational unit (OU) and applied to a group(s) and/or certain computers that require specialized security. These policies in effect can "harden" a computer to the point that it would be very difficult to be compromise via outside attack. Only a person with proper rights would have access to a system under such a restrictive policy.

The Under Belly of Win2k

The under belly of Win2k is where the security subsystem lies. The subsystem is the foundation on which Win2k security was designed. The security subsystem governs access to all objects. This includes files, processes and memory, ports, peripherals, and anything else that can be compromised. Below is a list of some of the security related technologies that Win2k uses.

- **Active Directory** – Microsoft's new directory service model based on LDAP.
- **Kerberos** – based on RFC1510 enhanced authentication protocol for Win2k.
- **Local Security Authority (LSA)** – authenticates and logs users into a local system.
- **MSV1_0** – provides NT authentication for clients that do not support Kerberos (i.e. Windows 95, 98, Me).
- **Multiple Authentication Provider (MAP)** – makes the logical decision to which authentication method to use.
- **Netlogon** – communicates with the domain controller and to pass SID information back to the local system for authentication purposes.
- **NTLM** - used for logon services for workgroups and local machines.
- **Security Accounts Manager (SAM)** – a local database that holds account information. This can be used locally or distributed among domain controllers.
- **Security Reference Monitor (SRM)** – monitors processes and limits access to those processes.
- **Secure Sockets Layer (SSL)** – end to end encryption that creates a secure tunnel between two points.

All of these services run in conjunction to make a more secure environment for Win2k. Each of them plays a key role in data security, authentication or encryption.

User Authentication

Within a Win2k domain each user must have an account to access the system. The account information that is entered is checked against the Win2k database (SAM) that holds the account information. When the information is entered it is checked using Kerberos and the Active Directory for verification of the information. Once the authentication process verifies that the information is correct that user is effectively "authenticated".

Based on settings the user will be granted certain privileges or belong to specified groups that can perform certain operations in the Win2k domain. Authentication from the user perspective is handled by the Winlogon and the Graphical Identification and Authentication (GINA) which are important elements in the logon process. The Winlogon and GINA are used to interact and authenticate the user and start the windows shell environment (i.e. Windows). **[14]**

Winlogon manages the logon and logoff of users to the Win2k domain. It handles the loading of a user's profile, protecting the machine; screen saver and handling remote performance monitor requests.

The GINA is probably more familiar to a user than they realize. The GINA is invoked with the CTRL-ALT-DELETE command and is used for sending information from the logon to the LSA which validates the user. The GINA is used for logon interactivity that aids a user in getting access to the Win2k system. More information on the logon process using Winlogon and Gina can be found at:
http://www.windowsitlibrary.com/Content/617/06/1.html.

User Specific IDs

In a large organization there might be several users with the same name and relatively similar information. How is this handled? Behind each user account there is a Security ID (SID) which uniquely identifies a user, group or machine account. This SID is generated upon account creation and will not be duplicated, it will always be unique. For instance if an account is deleted, then re-created the SID will be completely different and never regenerated. All rights and permissions based on the old SID will be removed for the deleted account and it will have to be re-established. This is a good method to prevent unwanted users or masquerade accounts from accessing resources. **[3]**

In the case of migrations, SID information must be migrated from the old domain rather than just recreating the account. Obviously, even if the accounts are named the same, they will be different due to the different SID information. The use of the SID is not a new technology, but with the advent of Win2k the need for strengthening it has increased.

_____

[3] Savill, John. "What is a Security ID?" SavillTech Ltd. 2000.

[14] Balladelli, Micky & De Clerq, Jan. "Windows 2000 Authentication". Digital Press. March 2001.

More information is included on the SID generated for a Win2k based account so that it lessens the chance of repetition between systems.

Assigning Roles and Rights

To truly secure your Win2k enterprise roles must be assigned to each user in the domain. With a larger company administration can be either centrally managed or distributed throughout the locations. Traditionally, in the old environments with NT 4.0 administration was done locally at each site due to the limitations of the operating system and sometimes skill sets of the administrators, however Win2k administration is now easier because each site can now be integrated into the AD and administration roles be assigned to local administrators or remote administrators.

With a large company many times there are many IT administrators with overlapping roles. Many people may have administrative access rights to many of the same workstations or servers, which makes tracking changes difficult. To effectively avoid this problem administrative staff must be assigned specific roles and responsibilities according to the Active Directory structure.

In AD the tree can be broken down and certain organizational units (OU) may be generated that effectively separate different business units or group from one another. For instance if you have two different business units such as research and finance; two OUs maybe generated to separate those business practices. Once the separations and user and computer accounts are moved to that OU a specific administrator can be appointed to manage that OU and the sub-OUs within. Sub-OUs are generally created to contain printers, users and groups, computers, service accounts and anything else that can be categorized separately. **[9]**

Security Policies

Once the OUs are established and the administrators are appointed for his/her OU, a security policy can then create a security policy for each OU and sub OU if needed. According to Michael Reilly of Security Administrator magazine "A system policy is a restriction you place on a user or a user's computer that limits the user's ability to access resources or configure the computer. A system policy might also impose corporate standard configurations."**[5]** A security policy is a good way to manage the OUs and the objects contained within and even distribute software. Once the policy is created to specification it is actually applied to all units downward through the tree unless it is specifically blocked from an OU by denying policy inheritance. The reason a block would be placed on the policy is if the OU contains accounts that the policy would hinder from performing normal tasks.

In the enterprise, policies are not just OU specific. They can be applied locally, at the site level, at the domain level, and/or at the OU level. Within the policy you can configure

---

[5] Reilly, Michael D. "Setting up System Policies." Security Administrator. July 1999.
[9] Rice, David C. and Sanderson, Mark J. "Guide to Securing Microsoft Windows 2000 Active Directory." Network Security Evaluations and Tools Division of the Systems and Network Attack Center (SNAC). Version 1.0. December 2000.

things such as startup and shutdown scripts for computers or have the policy restrict the computer to the point of making it a general workstation such as an internet kiosk at a tradeshow.

Types of Policies

Win2k offers three different kinds of policies for a Win2k network. Those policies are Local group, Active Directory group, and system policies.

Local Group – As the name implies local policies are applied to the local machine. Usually, the machine in mind does not participate in a Win2k domain thus requiring a local policy to strengthen the security of the computer. This type of policy can be applied to a computer that acts as kiosk, but doesn't require Active Directory (AD) to function. This method can be seen at trade shows, sporting events or places where many different people can access the computer.
Active Directory – This policy method is created and applied to all objects in the AD domain or specific OUs. This type of policy is also known as a GPO or Group Policy Object. With this type of policy a security minded administrator can use the full functionality of the policy by using the inheritance, blocking and override functions.
System Policies – This type of policy is created by using the NT system policy editor on the 4.0 platform. The system policy resides in the Netlogon share on a PDC or is moved to the SYSVOL folder on the Win2k platform. A system policy's information is kept in the registry of the machine it governs.

Application of Policies

Policies are applied from the top downward through the AD tree. The application starts at the AD site level, then to the domain level, and finally the OU level. For each object in the policy it has three different settings: Enabled, Disabled or Not Configured. *Enabled* and *Disabled* configures the policy variable to be enforced or not enforced and *Not Configured* simply means no change to the policy.

Within the default domain policy there are several sections of importance. Those sections are:

- **Account Policy / Password Policy** – This section of the policy covers password history, password age, password length, complexity requirements, storing passwords using reversible encryption.
- **Account Policy / Keberos Policy** – This section covers logon restrictions, lifetime for service tickets, lifetime for user tickets, lifetime for ticket renewal, computer clock synchronization.
- **Public Key Policies** – defines parameters for PKI and the encrypted file system (EFS).

Things to consider before applying a Win2k policy are:

- Policy can overwrite what a group policy object has set for logon.
- Can create conflicts with other policies, thus canceling each other out.
- NT policies are set in the registry and are persistent.

When planning for policies there are many variables that need to be considered before applying them to your organization. If proper planning is not done this can cause serious performance issues because each computer must process the policy. Even though policies are a great way to secure your network, a good rule of thumb is to not use policies when they are not needed. This will effectively help overall performance.

Securing Win2k Networks

With whatever OS platform is chosen for an operation, there will need to be some degree of security in place outside of the security on the computer itself. There are several methods in Windows 2000 that may be deployed, but the key notables are the usage of firewalls and proxies to protect your Win2k environment.

Firewalls and Proxies

Firewalls

A firewall is a network component that filters traffic. It has the ability to accept or reject specific types of traffic by referring to a policy. On the policy there is a rule base that explains what is relevant to the network and what isn't. For example, a web server farm would require ports 80 (HTTP), 443 (HTTPS) and possibly port 53 (DNS). A firewall can be thought of as a defense system that protects the interior components of your network. In many ways you can think of a firewall in terms of a private government compound. Usually it is very difficult to get inside and the only points of access are controlled by armed military personnel that require a person coming or leaving to have some type of permission to pass. Usually, the permission is by an ID card such as a smart card or in firewall terms this could be a password and/or a public and private key exchange.

According to Allen Jones of NT Security Administrator "You'll get a lot of requests to provide services and punch holes in your firewall. You can't avoid that. But with diligence, you can avoid making mistakes. Putting up a firewall goes a long way in securing your site. Unfortunately, it's more than just committing a server. You have to commit yourself to staying on top of vulnerabilities and to keeping up with the firewall." **[10]** Basically, all firewalls work on the lower level of the OSI model and secure a network by intense packet filtering, which means every packet's content is examined.

Proxies

A proxy is a component of the firewall that controls how internal users access the internet. Sometimes proxies only allow internal traffic out and no traffic in, but certainly they are not limited to that functionality. Proxies operate on the application layer and are sometimes referred to as Application Layer Gateways.

The Web proxy works with HTTP as an application proxy that works on the application layer level of the OSI Model. It basically works like this: An internet request goes to the proxy and the proxy server makes the request on behalf of the client and then returns the

[10] Jones, Allen. "Your First Firewall". Security Administrator. October 2000.

results to the client. This method of making the proxy the "middle man" allows you to restrict access to certain sites based on defined criteria. Proxies can help performance due to their ability to perform disk caching for frequently requested resources. Once a client is granted access to a resource, the proxy monitors that connection till the client terminates their session. Below is a list of the basic services a proxy can offer a network:

- Better network security
- Faster resource access due to disk caching
- Ability to limit users from accessing certain web content
- Security for IIS based websites

A proxy is an inexpensive, easy to implement solution for your environment. It should not replace a firewall because it does not have as much functionality as a higher level firewall. The goal of any network is to maximize and provide many different levels of security, while not limiting the users from properly performing their jobs.

Remote Access and VPN

Today more and more people are working out of the office and are on the road. This has made the need for remote connectivity greater than ever. There are many ways people can connect to their workplace and gain access to information such as company intranets and email.

First we have to analyze the methods a user might connect to his/her office from home or on the road, then we have to figure out how that information is securely transmitted between each point. A very common method of remote communication is by using a VPN or Virtual Private Network. This method is very popular and embedded in the VPN technology is a feature called tunneling. A private connection is created between a client and the VPN access point that is encapsulated by using a specific kind of protocol. The protocols that are used for Win2k VPN services are:

PPP – Point to Point Protocol is an old protocol that is an industry recognized standard and is mostly used over dial up VPN connection today.
SLIP – Serial Line Interface Protocol – this is the "old school" line protocol that was before PPP. The functionality is limited and can only transmit one protocol at a time so if your company uses both IPX for Novell and TCP/IP for Microsoft, this obviously is not the best choice.
PPTP – Point to Point Tunneling Protocol – this is a very popular protocol because it handles the creation of VPN over TCP/IP. This protocol supports tunneling, authentication and encryption. A more concise definition of PPTP can be found at: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwebtool/html/understanding_pptp.asp.
IPSec – IP Security – this is the highest level security protocol used for remote access. It is the most comprehensive and offers the highest security by controlling access, QoS, data non-repudiation, and confidentiality. It can use 3 main security protocols, but allows the system that it is communicating with to make the call on the protocol to be used. Those protocols are Authentication Header, Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE).

The usage of VPN is very broad and for the purpose of this document is out of scope. Not covered on the subject of VPN is authentication and encryption. It is up to you as an IT professional to determine the methods of authentication and how secure you want your data to be across the internet world. **[8]**

Securing your Workstations

In the past Microsoft has released products that have had many vulnerabilities. As such, workstations are still the main access points for your network. The reason for this is that statistically most attacks come from the inside rather than the outside of your network. To more actively secure a workstation would be to keep it up to date with the latest HotFixes and patches from Microsoft. These can be located at http://windowsupdate.microsoft.com and are broken down into three categories: Critical, Recommended and Drivers.

As previously discussed a proper domain policy should be created in order to protect your workstations and the users that use them. This policy can limit the rights to a user and give them the right amount of permissions on the network. Also, the usage of virus protection software such at McAfee or Norton System Protect should be used to protect against malicious viruses that are mostly received and executed through email attachments. Mail filtering is also done at the server, which is the process of examining each mail message for content and attachments and either quarantining or stripping the attachment.

Below is a list of simple things that can be set up on a workstation to increase its security:

1. Disable File and Printer sharing.
2. Use Encrypting File System so that non authorized users are prevented from viewing those files.
3. Use a personal fire wall such as Zone Alarm or Black Ice Defender on your client machines. In the case of Windows XP a firewall is built into the OS and can be applied to any network interface.
4. Upgrade or remove Windows 95, 98 or Me workstations due to their limited security features.
5. Periodically force password changes and rename accounts that usually have high level permissions such as the Administrator account.

Another great method of securing a workstation is simply making the users aware of the security threats that could potentially harm their data. If collectively everyone participates in good security practices, the better off you will be. Simple things like locking a computer down by hitting the CTRL-ALT-DEL and LOCK COMPUTER command when a user leaves their workstation can save a network from future headaches and downtime.

---

[8] Windows 2000-Based Virtual Private Networking: Supporting VPN Interoperability. Microsoft Corporation. January 2000.

Security over your Whole Operation

If you secure 99 out of 100 computers in your operation, you still have a weak spot that needs to be corrected. A malicious person using a scanner will find that one machine and use it as the entry point and then your efforts to secure your environment were ill-fated. Not securing every device in your operation is a very common problem. Due to the limited IT security staff and sometimes the remote geographic locations makes it virtually impossible to visit each machine. Automation is the key to this type of problem. Methods to perform automatic network/computer security scanning must be in place so that notification can be sent out to an appointed security response team.

The next step is to document what is actually on your network. There are applications out there that can do this such as Microsoft Systems Management Server that takes an inventory of Microsoft based systems and can report a status on a machine. Software can be pushed out through SMS and it can also handle asset tracking. The information collected is very valuable and can help administrators determine proper methods of administration and the total cost of ownership per computer in their enterprise.

An important tool that can be used for determining the security level of a computer is the Internet Security Scanner (ISS) and Microsoft Baseline Security Analyzer. These tools can be run from a workstation with a user that has domain administrator privileges.

System Scanner

System Scanner for Windows is a security-assessment solution for Windows 2000, Microsoft Windows NT 4.0, Microsoft Windows 95 and Microsoft Windows 98. It performs nearly 300 vulnerability checks, which includes scanning for the registry, Java, Microsoft Office projects and other well known vulnerabilities. Another feature is the baseline scanning. Once a computer has a clean build on it, you can run the System scanner to establish a baseline and all subsequent scans will be compared to the baseline. You can use System Scanner to define your own policies, as well as to schedule scans at specified times. It can generate HTML reports that provide detailed descriptions of vulnerabilities detected on your computer and information needed to correct them. The downside of System Scanner is that it was not created specifically for Win2k, but can be modified to scan the additional ports used by a Win2k domain controller by using a policy. For more information on System Scanner visit the Microsoft website at: http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q264178&.

Microsoft Baseline Security Analyzer

With the MBSA you can scan any Microsoft based computer on your network for potential security problems. This utility can run on Windows 2000-based and Windows XP-based computers, and can scan for missing HotFixes and security holes on Windows NT 4.0, Windows 2000, and Windows XP based computers. Once scanning is complete the utility will generate a report based on its findings. The report is broken down into categories based on what is installed on the system. This tool is great for IIS based web servers, and SQL based database servers. Key areas that are scanned are:

- IIS & SQL

- The number and permissions of the administrator accounts
- Status of the guest account
- Password analysis which measures strength of your passwords
- Auditing
- Available published shares
- Performs an Microsoft Office check
- Analyzes Internet Explorer's security features
- OS and application HotFix and service pack levels

If the MBSA is run in conjunction with other security techniques, you as an administrator will have a very firm grasp on your client/server environment. For more information on the MBSA visit the Microsoft website at:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp

Closing Thoughts

IT security is vital to the success of an enterprise. Without security in place from day one the data contained inside the newest, most expensive network is considered vulnerable. This document briefly discussed some of the different technologies that can be used to secure your Windows 2000 network. If the security methods discussed are used properly a hacker would have a very difficult compromising your systems. Fortunately, some of those security features are running by default, giving administrators and engineer's one less thing to worry about. Even though those technologies that are running do not directly impact a user, it is important to be familiar with them as a security minded professional. Familiarity in the environment in which you work with will help you prevent, detect and react to all types of security threats.

References

1. Editors, et al. "TCP/IP Flooding with Smurf." Security Administrator. October 1997. http://www.secadministrator.com/Articles/Index.cfm?ArticleID=9224 (20 August 2002).
2. "IP Security for Windows 2000 Server." Microsoft.com. 19 April 1999. URL: http://www.microsoft.com/WINDOWS2000/techinfo/howitworks/security/ip_security.asp (15 July 1999).
3. Savill, John. "What is a Security ID?" SavillTech Ltd. 2000. URL: http://secinf.net/info/nt/ntfaq/security27.html. (26 August 2002).
4. Optimize GPO Processing Performance URL: http://www.ntsecurity.net/Articles/Index.cfm?TopicID=1029
5. Reilly, Micheal D. "Setting up System Policies." Security Administrator. July 1999. URL: http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=5621 (31 July 2002).
6. Jones, Allen. "Proxy Server Security." Security Administrator. March 2000. URL: http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=8114 (31 July 2002).
7. De Clercq, Jan. "Kerberos in Win2k." Windows & .Net Magazine. Oct. 1999. URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=7193&SearchText=kerberos (5 Aug. 2002).
8. Windows 2000-Based Virtual Private Networking: Supporting VPN Interoperability. Microsoft Corporation. January 2000. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/confeat/vpninter.asp. (26 August 2002).
9. Rice, David C. and Sanderson, Mark J. "Guide to Securing Microsoft Windows 2000 Active Directory." Network Security Evaluations and Tools Division of the Systems and Network Attack Center (SNAC). Version 1.0. December 2000. URL: http://nsa2.www.conxion.com/win2k/guides/w2k-5.pdf (31 July 2002).
10. Jones, Allen. "Your First Firewall". Security Administrator. October 2000. http://www.secadministrator.com/Articles/Index.cfm?ArticleID=15602 (13 August 2002).
11. Weisman, Robyn. "Microsoft Rocked by Hack Attack". NewsFactor Network. October 2000. URL: http://www.newsfactor.com/perl/story/4661.html (20 August 2002).
12. Drash, Wayne B. and Morris, Jim B. "Hackers Vandalize CIA Homepage". September 1996. URL: http://www.cnn.com/TECH/9609/19/cia.hacker/ (20 August 2002).
13. Charny, Ben. "Wireless Offices—a hacker boon?". ZDNet News. 25 January 2002. URL: http://zdnet.com.com/2100-1105-823253.html (20 August 2002).
14. Balladelli, Micky & De Clerq, Jan. "Windows 2000 Authentication". Digital Press. March 2001. URL: http://www.windowsitlibrary.com/Content/617/06/1.html. (27 August 2002).

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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 Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
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
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
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor