Global Information Assurance Certification Paper

You Can't Hack What You Can't Access

Two friends are walking across the African plains. They see a lion heading their way. One friend stops to put on a pair of running shoes. The other says, "You can't outrun a lion!" The first says, "No, but all I need to do is outrun you." [1]

INTRODUCTION:
Security is a big and delicate concern when managing servers (Web or Proxies) connected to the Internet. A system that has high-level security standards with strong authentication methods, access control schemes and enabled auditing or logging, will discourage intruders, "like the lion", to leave your site and pursue the easier prey. Your system's connection to the Internet exposes many threats and vulnerabilities, from data, software, physical and transmission. Remember what we learned in Information Assurance Foundation, "Vulnerabilities are gateways which threats are manifested". The key is not to panic, but be paranoid. My paper is going to focus on high-level security options in Windows NT Servers connected to the Internet, following some keys concepts in protection that deal with Policies, Server Types, Physically Lock Access of the Server, Unnecessary Services, Network Settings, Users and Groups Rights, Account Policy, Registry and Auditing, amongst other things.

POLICY:
Developing a security policy that will deal with your computer security, by protecting your organizations sensitive data before an intruder compromises your system. Establishing a policy will involve many criteria's. The two main areas of concern are:
• To implement guidelines that will protect your assets in a cost-effective manner. Password security, encrypted records, and firewalls are example of cost-effectiveness.
• Improve on all your network-security components each and every time you find a weakness. The controls you select will be your primary focus of defense in protecting your assets. Also, have multiple structures, if one fails, another layer will protect your assets. Lastly, with physical access to your machine, a hacker can alter disks, load Trojans, etc. Allow trusted people near your systems. This process is continuous and tireless, but at least you can go to sleep knowing that some poor souls site is getting cracked, and not ours.
There are other steps that are critically important in making effective decisions on security; such as, what you are trying to protect, whom and what you must protect your assets, and to understand the likelihood of threats. The cost of protecting your system to a threat is more rewarding than the threat succeeding and compromising your network.

SERVER TYPES:
In todays globalized market; businesses must be on the Web to have a competitive market advantage. But part of the cost of reaping these benefits is your corporate network's potential to breaches. So knowing the threats and taking actions to guard data, your business can minimize the risk of Internet related security breaches.

[1] Len D'Alotto, GTE Laboratories. NetSec 1996 Conference. San Francisco.

Windows NT Server supports the following server types:

- **Primary Domain Controller** (PDC) in an NT domain authenticates logons and maintains the directory database for a domain. This is where password changes are made and user accounts created. It tracks changes made to accounts of all the computers in the domain and is the only computer to receive these changes directly.
- **Backup Domain Controller** (BDC) receives copies of the domain's directory database, which contains all account and security policy information for the domain. A copy of the database is synchronized automatically with the master copy on the PDC.
- **Member Server** (Stand-alone) runs Windows NT Server but is not a PDC or BDC of a domain. Member Servers do not receive copies of the directory database; they have their own local accounts.

If your computer will be running on the Internet, make it a **Member Server** on an Island (Workgroup).

PHYSICALLY SECURE SERVER:

In the real world, you know you must lock your car when you park it in the street. Protect your server like you would any valuable piece of equipment.

- Lock the room where the server is located.
- If the server is rack mounted, lock the door of the rack.
- Establish a policy for repairing or moving the server so it cannot be taken under false pretenses.

PROTECT DIRECTORY PERMISSIONS:

When you install Windows NT, it creates default directory permissions for each default group. The one I am talking about is the Everyone group which has full control, and should be replaced by Authenticated Users group or group account you create, everywhere you see the Everyone group. You may want to modify group access to the directories in order to prevent users or intruders from gaining access to important files in your root (%WINNT%). You can use Access-Control Entries that are used to build Access-Control Lists (ACLs). Which contains the following information: A SID, that identifies the trustee, an access mask specifying access rights controlled by the ACE, and containers can inherit the ACE from the primary object to which the ACL is attached to protect directory files.

For high-level protection, ensure that the data is stored on **NTFS** and set the following directory permissions to all subdirectories and existing files, in boot partition and system partition which holds critical operating system files. For example, Security Accounts Manager (**SAM**) is were NT stores user passwords in hash codes, which are backed up by the emergency repair disk and stored in %Winnt%\repair, and the Security hive contains security information for local groups, user rights, and membership of local groups. If both these hives are compromised, start looking for a new job. Microsoft recommends the following ACL, User Rights and Account Policies:

\WINNT and all Subdirectories. Administrator: FC
Creator Owner: FC
Authenticated Users: R

	System: FC
\WINNT\REPAIR.	Administrator: FC
\WINNT\SYSTEM32\CONFIG.	Administrator: FC Creator Owner: FC Authenticated Users: R System: FC
\WINNT\PROFILES.	Administrator: FC Creator Owner: FC Authenticated Users:Dir-R, W, X & File-NONE System: FC
\BOOT.INI, \NTDETECT.COM, \NTLDR.	Administrator: FC System: FC
\AUTOEXEC.BAT, \CONFIG.SYS.	Administrator: FC System: FC Authenticated Users: R
\TEMP.	Administrator: FC Creator Owner: FC Authenticated Users:Dir-R, W, X & File-NONE System: FC

USER RIGHTS:
Be aware of user rights that groups are assigned too. I stress again, prevent ordinary people from gaining access to data and Server

User Right
Open the **Administrative Tools** in Start, Program, and select **User Manager** then select **Policies/User Rights** and configure the following:
Log on Locally-remove Everyone and Guest group from having this right.
Shut down the system-remove Everyone, Guests and Users group from having this right.
Access this computer from the network-remove Everyone group, and add Authenticated users, Also remove the Administrator account. (sounds crazy, but will explain at the end).

ACCOUNT POLICIES:
Since hackers have many methods for attacking NT passwords, it is important to understand that when users pick easy to guess passwords or if you use NT accounts for private access, that policies are set and implemented in order to protect password cracking. Open **Administrator Tools** and select **User Manger** open **Policies/Account**, and set **Minimum Password Length** at least 6,7,or 8 characters (I've checked a lot of resources and each had different figures, so which ever makes you comfortable. I like 7).

Passwords are the golden keys to your network, to discourage password attacks, set **Account Lockout** to 3 or 5 (same as above-different resources have different figures) and the **Lockout Duration**-Forever (until admin unlocks). Some of the other settings are **Maximum Password Age**, **Minimum Password Age** and **Password Uniqueness**. These setting will make passwords hard to guess and limit the number of failed logons that NT allows, which will provide time to spot failed logons in the event viewer. Just remember to enable the audit feature Logon and Logoff events.

SYSTEM POLICIES:
System Editor Policies provide a detailed way to control system policy entries for Computers and Users. To open SPE, and select **Administrative Tools** in **Programs** and then **System Policy Editor** which will show two standard templates: **Default Computer** and **Default User.** As far as security is concerned, configure the following templates:

System Policy Entries for Computers:
- **Windows NT\Network\Sharing\Create hidden drive shares,** and **disable** the automatic creation of administrative hidden shares for an NT computer's drives (C$, D$ etc.)
- **Windows NT\System\Logon\Enable shutdown from Authentication dialog**-Specifies whether a Shutdown button will appear in the NT logon authentication dialog box. (In NT Server it is already grayed out, but just check to make sure).

System Policy Entries for Users:
- **Control Panel\Display\Restrict display** – specifies whether to restrict user's ability to modify display properties (via the Control Panel Display icon) and if so in what ways.
- **Shell\Restrictions\Remove Run from Start Menu** – removes the Run command from Start menu.
- **Shell\Restrictions Remove folders from Setting on Start Menu –** Removes the Control Panel and Printers folders from the Start menu Settings submenu.
- **Shell\Restrictions\Hide Network Neighborhood –** Hides the Network Neighborhood icon.
- **Shell\Restrictions\Disable Shutdown command –** Disables the out the Start menu's Shutdown command.
- **System\Restrictions\Disable Registry editing tools –** Disables the user's ability to run the NT Registry editor tools.
- **System\Restrictions\Run only allowed Windows applications –** Specifies whether users can run only applications on a list of allowed applications.
- **Windows NT\Shell\Restrictions\Remove common Program groups from Start menu –** Specifies whether to remove common (per-machine) program groups from the user's Start menu.

The need to develop a strategically and effective procedures of controlling your network environment, will prevent hackers and malicious users from identifying valid user accounts, network resources, shares, applications and banners, a process called Enumeration.

C2 CONFIGURATION MANAGER:
The National Computer Security Center (NCSC) is a United States government agency responsible for performing software evaluations. The DOD (Dept. of Defense) "Orange Book" bases its rating on a set of criteria that indicate how resistant a Network Operating System is to attack.
In the Windows NT Resource kit, which has a lot of tools for securing and enumerating, is a utility called Configuration Manager. You can use it to modify your system security to comply with DOD C2 criteria by using the following Microsoft recommendations:

- **File Systems** – All system volumes NTFS.
- **OS Configuration** – C2 compliant (cannot boot to MS-DOS).
- **OS/2 Subsystem** – Remove.
- **POSIX Subsystem** – Remove.
- **Security Log –** Set to manually remove, so you can analyze the logs for weird behavior.
- **Display Logon Message** – "This is a private Network. UNAUTHORIZED and MALICIOUS USERS will be punished by the Law".
- **Last User Name Display** - Hide the name of the user to logon.
- **Shutdown** Button – Don't show the shutdown button in the Logon dialog box.
- **Guest Account** – Disabled.
- **Drive Letters and Printers** – Setup so that only Administrators can assign permissions.

DISABLE UNNECESSARY SERVICES:
NT allows any logged on users to connect to a port, bind to the ports used by services such as NetBIOS. The primary vulnerability to compromise Windows NT machines comes from the **services** NT runs which run in the background and lets NT recognize different protocols, manage print servers, storage-devices, etc. You can save memory and system resources by disabling the following services:
To disable services, open the **Start Menu** and select **Setting Option** and **Control Panel** and double click **Services Icon**

- **Alerter and Messenger**. Enables a user to send alert or pop-up messages to specified users in the same or trusted domain. The threat from these two services is a hacker's social engineering attack, which he or she uses to convince users to provide their passwords. Also, the Alerter and Messenger services causes the network to broadcast current user's name in the NetBIOS table, and this might give the hacker or malicious user a valid name to use in a brute force attack.
- **Computer Browers**. Lets you view the shares of other computers on the LAN through the Neighborhood icon. With NULL sessions established, a hacker or malicious user can net view or some NetBIOS scanner to enumerate shares.
- **DHCP Client**. Disabling this service won't prevent you from getting an IP address through DUN.
- **Net Logon**. NT uses this service mainly in validation. If you don't use DUN to log on to your computer, disable Net Logon.
- **Network Dynamic Data Exchange (DDE) DSDM**. Maintains a data-base of all your computer's shared connections.

• **Network Monitor Agent** The Network Monitor service lets any Windows NT machine act as a network sniffer, but requires Administrator level access. NT encrypts the Network Monitor Agent password very weakly into a data-link library. Anyone with read access to that DLL can obtain the password.
• **Simple TCP/IP Services**. Used to test applications that use the Winsock API. A hacker can create a malicious DOS attack with Simple TCP/IP Services enabled, by sending UDP floods to the subnet broadcast address with the destination port of 19 and a spoofed source IP address.
• **TCP/IP NetBIOS Helper**. This service helps IP to NetBIOS name resolution. If not networked, disable it.
• **WINS Client (TCP/IP).** Computer to IP address name resolution.
• **NetBIOS Interface**. Provides access to File server. This layer presents a serious security problem if left enabled.
• **Spooler.** Runs printing service.
• **NWLink NetBIOS**. Disable this support if your configuration does not use the NWLink protocol for NetBIOS.
• **NWLink IPX/SPX Compatible Transport**. (Not required unless you don't have TCP/IP or another transport).
• **Schedule**. Responsible for automatically running batch jobs at specified times, as the system account. A hacker can modify the schedule configuration account to run a Trojan application.

ADMINISTRATOR ACCOUNT and LOCAL GROUPS:
Windows NT bases much of its security model around users and groups and the security permissions, which you grant to those users, and groups. Carefully monitor and secure the access privileges to all local groups and the security their exposure.
• **Server Operators**. Users, who are members of this group, can shut down the server, even remotely, reset the system time, and perform backups and restores.
• **Backup Operators**. Users, who are members of this group, can shut down the server and perform backups and restores.
• **Account Operators**. Users, who are member of this group, can shut down the server.
• **Print Operators**. Users, who are member of this group, can shut down the server.
It is important that you secure and monitor the access privileges of the local groups. If a hacker gains access to a Server Operator account and places a Trojan horse on the server that the hacker will activate after a remote shutdown, the Trojan horse could provide Administrator privileges of the system. The default permission for the local groups is as follows and need to be modified.
• **Winnt, \System32**. Server Operators and Users can R, X files, display permissions, and change some file attributes.
• **\System32\Config**. All Users can list filenames.
• **\System32\Drives, \System\Repl**. Server Operator has full access rights (RWDXC).
• **\System32\Spool**. Server Operator and Print Operators have full access. All users have R.
• **\System32\Repl\Export**. Server Operators can R and X files, display permissions on files, and change some attributes. Replicator has R access.

• **\System32\Repl\Import**. Server Operators and Replicator can R and X files, display permissions on files, and change some file attributes. Users have R access.

The Administrator account is everyone's dream, including our favorite friend, "the hacker". Users in the Administrator group have full access to all resources on a Server. You should restrict Administrative access level to trusted individuals and monitor closely for unauthorized activity. To minimize the potential for hackers to exploit account security, Microsoft recommends configuring the following:

• Rename the Administrator account to something obscure making it difficult for a hacker to locate.
• Create a dummy Administrators account with a complex password and no users rights, so as to give hackers a false target to attack. A hacker can still identity the renamed Administrator account based on its SID, which identifies the trustee. A trustee can be a user account, group account, or a logon account for a program such as a Windows NT service. Monitor security events for failed logons attempts, if hackers are internal users, you will know which workstation they are using.
• IIS creates a user account, IUSR_<MACHINE> account, which is the proxy account for anonymous access to all Internet services configures in Internet Service Manager (ISM). If hackers guess your server's computer name, they will know the name of this NT account. If you allow anonymous access, rename the account to something obscure using a different naming convention. Update the IIS configuration in ISM with this new account information; you must match the account username with the anonymous account name in ISM. If you don't provide public access to your site, disable the anonymous account.

At this point we have securely configured file directories, user rights and permissions and policies. The most common way hackers are able to gain access to the system is through regular system accounts. Once they gain access, whether they have administrative access or not, they are able to use the account to enumerate information. So if a hacker at this junction succeeds in breaking into your system, NTFS and the policies set will limit the damage the hacker can cause. Remember the rule, "discourage intruders, "like the lion", to leave your site and purse the easier prey".

NETWORK SETTINGS:

The NT Server, TCP/IP, and Windows sockets are necessary for Internet access. NetBIOS over TCP/IP are defined port numbers and functions contained in the Requests for Comments (RFC). This allows the mapping of NetBIOS computer names to IP addresses. These ports are:

TCP

• 139- NetBIOS session. Ex. net use \\xxx.xxx.xxx.xxx\ ipc$ "" /user:""
• 42- WINS-Windows Internet Name System.

UDP

• 137-nbname-Name Queries. Ex. nbtstat –A xxx.xxx.xxx.xxx.
• 138-nbdatagram-UDP datagram services. Ex. net send /d:domain-name.

As far as threats are concerned, the majority of attacks on NT machines are focused on TCP port 139 known as nbsession well known port. This shows a serious security hole in the NetBIOS layer if left enabled. Do NULL Sessions ring a bell. You can use the **Bindings** feature in **TCP/IP properties** to unbind or disable **WINS Client (TCP/IP)** over the Server service on **LAN Adapter (XXX 10/100 +Mini PCI)**, same as disabling NetBIOS interface for the Server service over TCP/IP. In the **Control Panel** select **Network** and choose **TCP/IP Properties/Bindings/Server-disable WINS Client (TCP/IP) and LAN Adapter.**
In a securely high environment, lets not discount the other ports, both TCP and UDP. Using the **Advanced TCP/IP Setting** button in **TCP/IP properties**, you can selectively enable **TCP, UDP** ports, and **IP** protocols and disable all others on the network interface card. You should permit only ports over TCP and UDP that the Web requires, (80,8080.443) by **Enabling Security** in **Advanced TCP/IP Settings**. This packet filtering is a simple and usable filtering function that the administrator can configure to just let some IP packets reach the actual applications running on the system.
Since most of us are paranoid security professionals, for added security, changing port assignments for well-known ports in ISM or Registry will do the trick, but make sure you inform your Technical support team which ports to use for service connections and adjust new information in security filtering.

If routing is enabled, consider disabling it when setting up TCP/IP. The threat here is that you run the seriousness of passing information from your internal network (Intranet) to the Internet. In **Control Panel**, open the **Network** icon click **Protocol** tab, select **TCP/IP** and click **Properties**. In the Routing tab, clear the **Enable IP Forwarding** box.

PROTECTING THE REGISTRY:

WARNING: Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk
The Registry is the Heart of Windows NT Operating System, and is the critical location for storing all sensitive information about the machine and users accounts. Before you add or modify a registry value entry, backup the registry.
Use **Regedit.exe** to backup a key or sub keys, select the **target key** and choose **Registry**, **Export Registry File** from the **Menu Bar**. In **Export dialog box**, enter **filename**. To **restore** the original, open **Regedit**, choose **Registry, Import Registry File** and select your **Filename**.
You can also use **Regedt32.exe** to backup the Registry, select the **Target Key** and choose **Registry, Save Key** from the **Menu Bar**. In **Save Key Dialog box**, enter a **Filename**. To **Restore**, open **Regedt32.exe**, choose **Registry, Restore from Menu Bar**, and select the **File content**.

The only users who should have Read-Write access to the registry are Administrators and Super Users. If ordinary people have full access rights and privileges, unauthorized users and hackers can edit the Registry and easily read the access control list for registry keys **HKEY_LOCAL_MACHINE** and **HKEY_CLASSES_ROOT**. And check each entry for write permissions. After changing the file associations, the hacker could install a Trojan, which will forward information to the hacker when the system reboots. As a paranoid security professional, review registry permissions on a regular basis and deny registry access from the network.

In a High-Security environment you want to assign access rights to specific registry keys in controlling user access. According to Microsoft, some keys pose a danger to the system if a user maliciously manipulates them. Setting Special Access Rights will make sure that the Everyone group has only certain permissions for important registry keys. Run **Regedt32**, select the **Key or Subkey,** and then select **Security/Permissions** and choose Read rights.

- **Query Value**. The user can read a value entry.
- **Enumerate Sub keys**. The user can expand and read the sub keys.
- **Notify**. The user can audit notification events for a key.
- **Read Control**. The user can read a key's security information.

Microsoft recommends the above values to have **Access allowed** permissions of Read access for the Everyone group:
The keys that are considered important for securing the registry are:

- **HKEY_LOCAL_MACHINE\Software**. Locks the system that can install software.

- **Microsoft\RPC (sub keys).** Locks the RPC services.

- **\Microsoft\Windows NT\Current Version and the following Sub keys**.
  \Profile List. Prevents users from bypassing mandatory profiles and run bogus files placed in Startup folder.
  \AeDebug. Controls what programs are launched when process crashes**.**
  \Compatibility.
  \Drivers.
  \Embedding.
  \Fonts.
  \Fonts Substitutes.
  \GRE_Intialize.
  \MCI.
  \MCI Extensions.
  PerfLib – This allows remote users to see performance data. Remove Everyone group and give **Interactive** group: **Read** access.
  \Ports (Sub keys).
  \WOW (Sub keys). Supports Window 3.x programs by using COMM.DRV.

SECURING EXECTUABLE KEY:
Here are other places where a hacker can run Trojan programs that can be loaded at startup in NT. Assigning Read access for the Everyone group will prevent attackers from loading bogus applications on your system.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion
\Run
\RunOnce
\RunServices

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\RunServices
\RunServicesOnce
Check regularly for the presence of malicious commands.

- **HKEY_CLASSES_ROOT (Sub keys).** Assign the Special Keys allow access**.**

In addition to assigning rights to specific registry keys, the administrator of a High-Secure network, needs to set protection to the following Registry keys.
- **HKEY_LOCAL_MACHINE\System\CCS\Control\SecurePipeServers\Winreg**. This will restrict network access to the registry. The security permissions should permit only administrator's remote access.

\AllowedPaths. Will prevent an attacker from inserting his or her own allowed paths for anonymous access. The Everyone group to have Read access.

- **HKEY_LOCAL_MACHINE\System\CCS\Services\LanManServer\Parameters**

\NullSessionPipes. DWORD Value Add Winreg. Another protection layer that restricts anonymous (NULL Session) logon to access the network registry through "namedpipes".

- **HKEY_LOCAL_MACHINE\System\CCS\Control\LSA**

\RestrictAnonymous. DWORD Value1. Restricts the ability of anonymous logon users (NULL Session), to list account names and enumerate shares. Also, enable administrator account lockout to secure the Administrator account by running **PASSPROP** and selecting **/ADMIN LOCKOUT**. This will protect LSA passwords and prevent users with administrator access from dumping information, you also have to enable auditing and select **Success** for **User and Group Management** and view failed logon **Event 644**, user account locked out.

\NotificationPackages. MULTI_SZ Value "PASSFILT". Enforce stronger password requirements, which contain Upper, Lower characters, Numeral, Symbols.

\LMCompatibilityLevel. DWORD Value (0,1,2,3,4,5).
- **Value 0** (default). Send both Windows NT and LM password forms.
- **Value 1.** Send NT and LM passwords forms, only if server requests it.
- **Value 2.** Never send LM password form.

LMCompatibilityLevel allows clients to be configured to send only Windows NT authentication (Challenge/Response). Disabling LanManager (LM) password Hash

Support because 1) passwords are not case-sensitive, making them weak 2) no longer than 7 bytes and 3) use DES (Data Encrypted Standard), all of which makes it easier to crack. Window NT (Challenge/Response) prevents users from sniffing clear-text passwords. By using 7 or 14 Enforced Strong user passwords, since 8-13 characters yield a weaker second hashes making it easy for a hacker to guess the first hash and crack it, you can eliminate man in the middle attack with also having SMB enabled. Unfortunately, this is not the ideal world because of the compatibility issue. If a Windows NT client selects level 2 or above, it cannot connect to workstations that only support LM authentication. LSA stands for Local Security Authority. This is an internal subsystem within Windows NT that generates access tokens, manages the local security policy, and provides interactive user authentication services.

\CrashOnAuditFail DWORD Value 1. C2 configuration Manager provides the option to shut down system when security audit log is filled up. With this setting the system will shutdown when full audit is detected. You have to reset value to 1 after clearing log and then rebooting.

\AuditBaseObjects. DWORD Value 1. Enables auditing for base system objects, to start generating audits, enable **Auditing** and select "**Object Access**" in **User Manager**.

- **Enhanced Protection for Security Accounts Manager Database**.

SystemKey adds an extra layer of security to passwords stored in the SAM database by using strong encryption hash passwords using 128-bit system key. Once generated, NT uses it to encrypt and decrypt all password data. Only Administrators can turn on system key protection. Run **SYSKEY.exe** and **Secure the Windows NT Account Database** by enabling **Encryption**. **Specify the SYSKEYS's location**, either stored on **Floppy** or **Locally**.

SECURE FILE SHARING.

Windows NT file sharing service is provided by Secure Message Block (SMB) based server and redirector services. The SMB protocol controls network and remote access to server services. This important protocol allows users to access shared directories, the registry and other system services remotely. SMB sends passwords across the wire in clear text which a hacker can intercept the sessions and perform a man in the middle attack. By incorporating message signing into SMB packet you can protect the users passwords with digitally signed packets, which are verified by the server and workstation services.

- **HKEY_LOCAL_MACHINE\System\CCS\Services\LanManServer\Parameters \EnableSecuritySignature and \RequireSecuritySignature. DWORD Value 1**.

Will have the SMB server respond to the client with message signing only.

- **HKEY_LOCAL_MACHINE\System\CCS\Services\Rdr\Parameters \EnableSecuritySignature and \RequireSecuritySignature. DWORD Value 1.** Will allow clients to communicate with servers that support message signing.

• **HKEY_LOCAL_MACHINE\System\CCS\Services\LanManServer\Parameters \AutoShareServer and \AutoShareWorkstation. DWORD Value 0**. For another layer of protection, you can disable administrative shares and prevent enumeration attacks.

SECURING BASE SYSTEM OBJECTS:

• **HKEY_LOCAL_MACHINE\System\CCS\Control\SessionManager \ProtectionMode. DWORD Value 1**. Enables stronger protection on base objects. Informs session manager that security on base objects should be at C2 level.

AT COMMAND (SCHEDULE)

The Schedule service is used to run batch jobs automatically. To reduce the risk of the Schedule service, reconfigure the schedule service to execute commands as a user with lower access rights or in high security installations disable entirely. Also, access to the key should only permit administrators to submit to run jobs.

• **HKEY_LOCAL_MACHINE\System\CCS\Services\Schedule.** In **Security Permissions** allow only **Administrator**.

SECURING EVENT LOG:

Default configuration allows guest and null sessions to view event logs. Restrict guest access to these logs and assign **ONLY** administrator and system permissions.

• **HKEY_LOCAL_MACHINE\System\CCS\Services\Event Log**
\Application
\Security
\System. \RestrictGuestAccess. DWORD. Value 1.

DISABLE CAHCHED LOGONS:

This is the final location that Windows NT stores password hashes. The default configuration caches the last logon credential for users that have logged on interactively to the system. Even though well protected, in a highly secured environment, you may want to disable this feature.

• **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CV\Winlogon \CachedLogonsCount. SZ Value 0.**

At this point we have improved our system by focusing on the threats and added many layers of security. I wish this was the end of the story, but in actual reality, it is just the beginning. Installing and configuring your network to become bullet proof takes a lot of planning, once it's done, the next process is to monitor and analyze possible breaches. This brings me to the next and most important topics, "Auditing" and "Passwords"

AUDITING:

Audits can inform you of actions that could pose a security risk and identify suspicious activates of users account. Windows NT by default disables auditing during installation. The auditing policy should be include:

1) What the server should log (user behavior, changes to files).
2) How long to keep the audits.

3) Whether you should turn on auditing for all machines.

Increased auditing may generate network traffic and slow down your server, so be careful in what you audit. Also, Windows NT saves the logs locally on a disk, if the machine is compromised, the hacker will also manipulate the logs. Therefore you might want to make copies of the log files onto protected centralized log-servers.

To activate NT security event logging, click the **Start** button. Select **Programs** and choose **Administrative Tools**, select **User Manager** and then select **Policies** menu **Audit option.** The Audit policy lists the following events.

Logon/Logoff. Instructs the Event viewer to maintain local and remote logins.
File and Object Access. Maintains records of all files, directory, and printer access on NTFS partitions. Once enabled, use Explorer to select auditing for individual files. (boot files – Boot.ini, Ntdetect.com, Ntldr. Regedit.exe, Regedt32.exe, Atsvc.exe, Sam hive, Internals).
Use of User Rights. Record successful and unsuccessful uses of user rights.
User and Group Management. Maintains the users accounts the system administrator or authorized users create, change or delete. It also records changes of passwords the user sets.
Security Policy Changes. Maintains information of any changes to users rights.
Restart, Shutdown and System. For shutdowns and restarts for local workstations.
Process Tracking. Information of program activates, duplications, and process exits.

The following is Microsoft's recommendation on settings for Auditing:

	SUCCESS	**FAILURE**
Logon/Logoff.	Disable	Success
File and Object Access.	Success	Success
Use of User Rights.	Success	Success
User and Group Management.	Success	Success
Security Policy Changes.	Success	Success
Restart, Shutdown and System.	Success	Success
Process Tracking.	Disable	Disable

All audited logs are listed in the Event Viewer. Check your events for any suspicious activates, like, failed logon attempts and date and time of logons, can be good indications of intrusion.

PASSWORDS:

The most important topic of this paper. Passwords are the crown jewels for your Network. To get access of the NT password, a hacker to have access to a username and collect clear text and hashes from **Local Security Authority** (LSA). The attacker can then perform brute force attacks, which are character combinations, in order to get the password. However, the hacker must have physical access to the console or require administrator access and trick the administrator to run a rogue program under the administrator account. To keep the hacker away from password files, which are stored in a Seven locations: 1) HKEY_LOCAL_MACHINE\SAM,

2) %Winnt%\System32\Config\Sam.hive, 3) Emergency Repair Disk, 4) %Winnt%\Repair, 5) Backups, 6) Network, 7) Cached Logons, Physically secure your server, so the hacker goes not have access to the file and force your users to regularly change their passwords.

ADMINISTRATOR ACCOUNT:

The Administrator account is the most privilege NT account and is vulnerable to attacks from outside and inside your network. To protect the Administrator's account from undesirables:

- Rename the Administrator account that malicious users might not guess.
- Create a new Administrator account and add it to a group that has no privilege access.

Also, give the account a long password (14 characters), which will be difficult to guess. Enable failed logons in auditing and monitor attempts to login for the Administrator account.

- Remove the Administrator account right to log in from the network, which will force the Administrator to log into the network from the console. Therefore, you also force hackers bruteforce attack to come from the console.

CONCLUSION:

Windows NT was designed to protect against security problems by providing security Upgrades, Service Packs, and Hotfixes, for every timely vulnerability. As we know, an NT system "Out of the Box", has significant security weakness that hackers or malicious users can exploit. Without the Administrator privilege, a hacker has to use different types of methods to acquire an Administrator password, ranging from password guessing, to social engineering. As we have seen, NT passwords have weakness in features that enable compatibility with other Operating Systems. To reduce this vulnerability, NT compensates by using the SYSKEY, disabling LM authentication and selecting quality passwords. The last two options will increase security but reduce the networks compatibility with non-NT clients and servers.

Secondly, Blocking access to TCP and UDP ports 135-139, enabling Security Filtering to allow ONLY those ports and protocols necessary, and RestrictAnonymous access, will prevent remote NT vulnerability by a malicious user.

The Windows NT Operating System has a secure security interface layer. It is the applications and legacy systems, which make NT vulnerable to attacks. In order to create a secure environment, develop strong security policy and security awareness, will prevent damage to your system.

"Vulnerabilities are gateways which threats are manifested", and the most imminent threat come from within.

SOURCES and LINKS:

Stuart McClure & Joel Scambray, George Kurtz. Hacking Exposed – Network Security Secrets & Solutions. Osborne/McGraw-Hill. ISBN 0-07-212127-0.

Microsoft. White Paper. August 11, 1997. Securing Windows NT Installation.

Lars Klander. Hacker Proof-The Ulimate Guide to Network Security. Jamsa Press. ISBN 1-884133-55-X.

The SANS Institute. Windows NT Security Step by Step. Version 3.03, February 2001

Sir Pent. Winnt Hacking.txt. http://www.hackcentral.org/learning/Win%20nt%20hacking.txt. Last Modified 06-Jan-2001.

Robert Malmgren's. NT Security FAQ. Homepage. http://www.it.kth.se/~rom/ntsec.html.

Clayton Johnson. June 1997. Troubleshooting and Configuring NT Registry. http://www.docs.rinet.ru:8080/Registratura/htm/toc.htm. Sams Publishing; ISBN: 067231066X.

Robert Slifka. February 1997. How to Edit NT 4.0 System Policies. http://www.win2000mag.com/Articles/Index.cfm?ArticleID=104.

Sean Daily. April 1997. Further Explorations of the NT System Policy Editor. http://www.win2000mag.com/Articles/Index.cfm?ArticleID=90.

Tom Sheldon. October 1996. Steps for Evaluating the Security of a Windows NT Installation. http://www.tec-ref.com/ntchecks.html. Updated November 1, 1996.

dildog@l0pht.com. February 18, 1999. Any local user can gain administrator privileges and/or take full control over the system. http://www.atstake.com/research/advisories/1999/dll_advisory.txt.

Deep Quest Inc. Homepage. Hacking NT in few minutes by the Web. http://webstore.fr/webabonnes/tahiti/nt.htm.

Deep Quest Inc. Homepage. NetBIOS based NT Hacking. http://webstore.fr/webabonnes/tahiti/netbios.htm.

Lexikon Sevices. <C> 1995. Computer Security and Privacy. Version 6-F. http://www.sevenlocks.com/SWTutorials.htm.

Microsoft Internet Information Server 4.0 Security Checklist. http://www.microsoft.com/technet/security/iischk.asp. Last Updated: 15-Mar-2000.

James Morey. January 5 1999. Getting the most from IIS Security. http://www.microsoft.com/technet/IIS/technote/websec2.asp. Last Updated January 12 2000.

Ethan Wilansky, Geoff Moes. November 1 1998. Accessing and Securing your remote Web Server. http://www.winntmag.com/. DocID: 3942.

Kathy Ivens. February 1998. Securing the Registry. http://www.windowsitlibrary.com/Content/368/09/1.html.

Wayne Maples. NT Registry Index.http://www.is-it-true.org/nt/registry/. Last modified 21-Apr-01.

Wayne Maples. NT Tips for Administrators. http://www.is-it-true.org/nt/atips/index.shtml.
Last modified 20-Apr-01.

Kbase: Windows NT. How to Enable SMB Signing in Windows NT. Last Modified on 12-13-2000. Q161372

Tom Dodds, Eric Miyadi, and Tom Fuchs. 4/13/1999. Designing and Planning Windows NT External Security. Microsoft TechNet, Volume 7, issue 5.

Kbase: Windows NT. How to Enable Strong Password Functionality in Windows NT. Last Modified 0n 12-18-2000. Q161990.

Kbase: Windows NT. Security Privilege Must be Enabled to View Security Event Log. Last Modified on 07-07-1999. Q188855.

Kbase: Windows NT. Windows NT System Key Permits Strong Encryption of the SAM. Last Modified on 01-22-2001. Q143475.

Kbase: Windows NT. Can No Longer Access the Registry with Null Sessions. Last Modified on 02-0901999. Q143138.

Kbase: Windows NT. Restricting Information Available to Anonymous Logon Users. Last Modified 12-13-2000. Q143474.

Kbase: Windows NT. How to Disable LM Authentication on Windows NT. Last Modified on 12-15-2000. Q147706.

Kbase: Window NT Current Release. How to Disable Installation of NWLink NetBIOS. http://support.microsoft.com/support/kb/articles/Q156/2/03.asp. Last Modified on 02-07-2000.

Kbase: Internet Information Server. Practical Recommendations for Securing Internet-Connections. http://support.microsoft.com/support/kb/articles/Q164/8/82.asp. Last Modified on 04-30-1999.

HB3^. Nov. 9, 1999. www.hackerzlair.org. NT_Security.reg. (www.hackerzlair.org/NT_security.reg-HTTP404.) http://209.143.242.119/cgi-bin/search/search.cgi?authkey=%24fields%7B%27authkey%27%7D&uname=%24fields%7B%27uname%27%7D&searchvalue=NT_security.reg&type=archives&search.x=15&search.y=25.

Christopher Klaus. Windows NT Security FAQ. Version 3.0. http://packetstorm.securify.com/docs/infosec/computer-security_Windows_NT_Security_FAQ. Last-modified: 1999/9/11.

Slash. Windows NT Security Check Part 1. http://packetstorm.securify.com/advisories/b0f/nt.security.check.part1.txt.

Slash. Windows NT Security Check Part 11 – For BufferOverflow Security. http://packetstorm.securify.com/advisories/b0f/nt.security.check.part2.txt.

Randy Franklin Smith. October 1998. Protect your Passwords. http://www.win2000mag.com/Articles/Index.cfm?ArticleID=3844.

Tom Sheldon. December 1996. NT Security Tips. http://www.winntmag.com/. Doc ID: 2874.

Microsoft. TechNet April 1999. Internet Information Server Resource Kit.

Wamala Paul Mubanda
SANS Security Essentials
GSEC Practical Assignment
Version 1,2b

Dedicated to my lovely wife, for being patient. Love always.

Last Updated: July 25th, 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 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
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
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
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
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
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
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 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
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event