Global Information Assurance Certification Paper

Daily Processes for Maintaining a Secure Windows Environment

Larry Wayne Arant II
GSEC Practical Assignment 1.4b option 1
October 15, 2003

Introduction

Threats to system security can originate from a variety of sources, can come in many forms, and are constantly advancing in severity and complexity. As a result the process of maintaining a secure Windows environment must account for multiple avenues, with multiple methodologies, and be able to adapt to the changing times. I have seen write ups and books covering the finer points of server hardening, patch management or account management. It is not the intention of this paper to delve into the finer points of things such as that or port scanning, or virus protection. Rather it is an attempt to describe, from a high level, all of the daily task, and the processes surrounding them, for maintaining a secure Windows system, to act as a guide for administrators and managers alike, for how to keep your data safe, and your services available.

The inspiration for this topic stems from my efforts to understand and comply with the guidelines outlined in "Suitable Trust Services Criteria and Illustrations" also referred to as "Trust Services Principles Version 1.0" the successor to "SysTrust v 2.0" especially the Security and Availability sections, as they relate to Windows[1]. While it is not intended to be a comprehensive "How-To" this paper does aim to provide a real world picture of what is necessary to accomplish that goal.

Where to begin

The Trust Services Principles document defines the security principal as "…the protection of the system components from unauthorized access…" Microsoft describes the high level classification of protective measures, designed to achieve that goal, as prevention, detection, and reaction.[2]

Prevention is defined simply as: taking measures that prevent your information from being damaged altered or stolen. This echoes the three primary states of data that must be maintained to say that it is secure.

Availability – First the data must be available to authorized users. If it is not available, because it is stolen or lost, then it is impossible to ascertain its security state, and should be considered compromised. If it is not available due to system outage, then it is of little use.

Integrity – Those users who are authorized to access the data need to know that it is accurate. If it has been compromised in some way, then that could be difficult or impossible to know. The only thing worse than no information, is misinformation.

Confidentiality – The data must remain confidential. A leak in corporate secrets or practices can be devastating.

It is important to note however, that there are always exceptions to these rules. For example, the data placed on a public web page, has no concern for confidentiality. You would not normally be concerned over the integrity of test data in a training facility. And, certain types of archived or historical data can have availability measured in days instead of seconds. What makes the difference is the data's classification. Make sure when you are deciding how best to protect your data, that you understand its value to your organization.

Detection, the second classification of protective measures, refers to the ability to know when data has been damaged, altered, or stolen, how, and by whom. There are many tools and processed designed to assist in that endeavor.

And last but not least, reaction. There must be processes and procedures in place to allow for the recovery or correction of lost or damaged information.

A similar philosophy can be found in SKiP (Security Knowledge in Practice), provided by the Carnegie Mellon, Software Engineering Institute, CERT Coordination Center. Here they define a seven step method. Each step is associated with a set of security practices, designed to meet the need of system security.[3]

First, *Select systems software from a vendor and customize it according to an organization's needs*. Unfortunately in most environments, this is considered a strictly business process, and does not involve administrators until after the fact. This could however also be applied to the selection of infrastructure and support software.

Second, *Harden and secure the system against known vulnerabilities*. Hardening, as the name implies, is the process of establishing and reinforcing the security capabilities

of the system. Practically any system can be hardened, but we will be looking at how this applies to Windows systems specifically. Hardening begins when you decide on and select your hardware. It is important to select standard, dependable hardware from reputable companies. But as important as that is, most of the hardening is accomplished by how you configure the system. It is much easier to configure the system with security in mind, than to retrofit the system after the fact. However, how you configure the system must be a balance of security and functionality. It has been said that the only truly secure system is turned off and locked in a closet. However, that system isn't very useful.

Enter preparing; *prepare the system so that anomalies may be noticed and analyzed for potential problems*. Preparing could be described as the process that ties hardening to detecting (the next step). It supplements the hardening done during the configuration by providing you with a means to detect activities on the system that could lead to a compromise of security. Because preparing is done separately on each server, it can be tailored to compensate for the weaknesses inherent to the specific configuration, but should at a minimum include things like enrollment into a patch management process and baselining the normal activities and behaviors of the system.

Detect; d*etect those anomalies and any other system changes that could indicate evidence of an intrusion.* Securing your servers and making a valiant effort to keep them secured, wont stop people from exploiting any weakness they can. Be it on purpose or by accident, software changes will violate security best practices, users will gain unauthorized access, and hackers will make every effort to damage or steal anything they believe is of value. To reduce the risk of someone or something succeeding in overcoming your security measures, you need to “keep an eye on” the system. Scan it for software and configuration issues, monitor it for unusual activity, and audit it for violations of policy.

Respond; When you see something, you need to *respond to intrusions when they occur.* Respond in an appropriate manner, and in an appropriate time frame. Knowing what to do and when to do it can be a taxing, time consuming process. Creating a structured Incident Response Team can help minimize the stress by providing a central location with definable, structured processes to evaluate the risk and impact of security related events and problems, and to provide guidance for the best course of action. And, defining various “Management” processes can help alleviate the burden of implementing those actions.

Improve; *Improve practices and procedures after updating the system.* Of course, no one ever gets it exactly right on the first try. You can be guaranteed that no matter how much thought you put into the original configuration, there will need to be changes. And, if you have never heard the phrase “...The only constant is change…” commit it to memory now.

Repeat; *Repeat the SKiP process as long as the organization needs to protect the system and its information assets.*

In the sections that follow, I will outline the appropriate industry standard procedures necessary to meet each of these steps.

Hardware/Software Selection

Selecting the right hardware or software for your environment may seem like a trivial task, but to not dismiss it too quickly. If you do not review the product carefully, you could wind up implementing software or hardware that cannot have even the most basic security measures applied without breaking functionality. If you don't then step back and reconsider your processes, it will only happen again and again until there is no way to secure your environment without bringing business to it's knees.

The first step is to look at vendors with a good reputation. Do a little research, and find out how they rate in customer satisfaction, problem resolution, and other related topics.

Next, read the fine print. Compare support contracts and terms. If a vendor is less willing to provide support it could indicate that they would be overwhelmed by the workload if they did.

Stay with tried and true. Don't be swayed by the latest gadget or coolest new feature. It is often better to go with a product that has been around for a while, and had a chance to “work out the bugs” in the real world.

Of course with the complexity and overwhelming quantity of products available today, you can never be too sure that what you choose will work within your existing environments. Make sure that anything you consider is put through the paces in a test environment. If necessary solicit 3rd parties to help assess your environment and make recommendations based off of their experience with others.

Finally, set and publish standards. So others can benefit from your efforts. This will minimize the likelihood of someone introducing an incompatible product or device into the system, and will help to ease the burden of support by narrowing the scope of necessary technologies to learn.

Server Security Configuration

This section gives basic guidelines for configuring security on Windows Server computers. [4] Many of these settings can be applied by use of security policy templates and the Security Analysis and Configuration tool provided with Windows as an MMC plug-in. Policy templates include a fairly exhaustive list of security related settings (See appendix A) and can be customized based on role, or specific function. It is also possible to apply policy templates on top of each other, allowing you to define a default “baseline” template and use specialized templates to increment the changes to the servers during installation before they are ever placed within the environment. Also, if your environment leverages Active Directory, you can use Group Policy Objects to

apply security policies based on their location in the AD tree. However you choose to deploy security settings within your environment, it is important to well document the process of server security configuration; this information should be included or referenced in your organizations server build document.

Secure default account configurations

The Administrator account

The Administrator account is present on all Windows installations by default, and there no way to readily remove it. It is also not normally subject to account lockout policies. This makes it a primary target for brute force attacks. It is very important to mitigate this risk. Microsoft recommends renaming the account to a non-obvious name (e.g., not “admin” or “root” etc.). If you use a standardized naming convention, consider using a name that will blend in. It as also recommended to create a decoy account named “Administrator” that has no privileges. This will come in handy later when we discuss “Event Management”.

Another way to minimize the risk should the real account be discovered, is to ensure the use of a complex password. Microsoft has this to say regarding Windows passwords.

…Windows 2000 allows passwords of up to 127 characters. In general, longer passwords are stronger than shorter ones, and passwords with several character types (letters, numbers, punctuation marks, and non-printing ASCII characters generated by using the ALT key and three-digit key codes on the numeric keypad) are stronger than alphabetic or alphanumeric-only passwords. For maximum protection, make sure the Administrator account password is at least nine characters long and that it includes at least one punctuation mark or non-printing ASCII character in the first seven characters...

For a list of non-print ASCII characters See Appendix B

The Guest account

The guest account is disabled by default. Enabling this account would allow anonymous access to the system. Make sure that the account remains disabled.

Other local accounts

Local system accounts should only be created when absolutely necessary. Distributing accounts across multiple systems introduces a number of security and administrative concerns.

Enforce account configurations

Password policies - Account Lockout Policies

Standard password and Account lockout policies can be enforces to include things like, minimum length, complexity requirements, lockout after X retries. But, be careful that you consider your environment. There are known issues with using account lockout in environments with non-trusted NT4 domains.

Protect files and directories

Limit the use of File Shares

One of the best ways to maintain the security of your data is to not expose it to remote access. Only create file shares when absolutely necessary.

The NTFS file system

Microsoft Windows has supported many disk formats over the years, from FAT and HPFS to FAT32 and NTFS. NTFS partitions offer features that aren't available with other file systems. From ACLs that provide granular security to built in data reliability features to help ensure availability. Make sure that all partitions are formatted using NTFS. If necessary, use the convert utility to non-destructively convert your FAT partitions to NTFS.

Warning: If you use the convert utility, it will set the ACLs for the converted drive to Everyone: Full Control. Use the fixacls.exe utility from the Windows NT Server Resource Kit to reset them to more appropriate values.

Set appropriate ACLs

ACLs (Access Control Lists) are used to assign access rights to users or groups of users. Directories and files both support the use of ACLs when stored on an NTFS volume. File shares also support the use of ACLs. When applying ACLs remember the *principal of least privilege*, only grant access to those persons that need it, in order to do their job.

Configure the system registry

The system registry contains practically every conceivable configuration detain of a windows system. Taking the time to understand and secure the registry can prove invaluable to the overall security of the system. The two topics that follow are both listed in the SANS “Top 10 Vulnerabilities for Windows” (W5).[5]

Protect the LSA from anonymous access

By default Windows allows remote access to account information. This access should be limited to authorized users only wherever possible.

Protect the registry from remote access

By default Windows allows for users to connect to a subset of the registry from across the network. It also allows users to modify data within the remote registry.

Set registry ACLs

The system registry also supports the application of ACLs. There are several known windows vulnerabilities that can be mitigated by the proper application of ACLs.

Set warning message

Technically setting a logon message can not stop someone from logging on. However, just like the "This car protected by…" stickers used to thwart auto theft, it can act as a deterrent. Especially for those that have stumbled into the situation unknowingly. It can also play an important role when it comes time to prosecute an attacker. Before you implement a warning message, be sure you consult with your legal department, and you may want to give anyone that would be affected by the change a heads up, so there won't be any confusion when they are suddenly faced with a strong worded warning about entering their system.

Disable Unnecessary Services

Services are background processes that are usually executed at startup and remain running as long as the session is active, typically running in a security context other than the currently logged on user. They also expose ports and services that can contain vulnerabilities that can be used to compromise the system.
A good rule of thumb is to uninstall or disable any service that is not critical to the functionality of the system. A good source for information about system services and their role on the system can be found at: www.theeldergeek.com/services_guide.htm

Enable Security Event Auditing

Event logs are an excellent source of information about security events on the system. However, it does no good if the proper event logging I not enabled. Review the available logging configuration options to ensure that they fit the needs of your environment. But, be careful, it can be easy to over do it and wind up with far more information than you could ever manage.

Vulnerability Management

Vulnerability management is a complex on-going process that can best be described with just two words… due diligence. This is the process by which you make sure that what you have secured stays that way. And recent software vulnerabilities have taught us that we can no longer be complacent. While we once had months to respond to the latest security bulletins and advisories, and apply the appropriate update, the current "window of opportunity" is consistently measured in weeks or even days and less, complicating this already difficult task.

Often the first step in managing a vulnerability is knowing of its existence. This, the process of staying informed, is sometimes referred to as Technology Watch; there are numerous sources for information regarding vulnerabilities, their impact, and how to manage them.

The World Wide Web is one excellent source of "editorial" type information. Web sites tend to vary from the very generic to the highly technical and is generally best for self education and business ready reasoning for the latest security trends. Look to sites such as www.blackhat.com www.sans.org or www.cert.org for general security related information and education. Or, look to your product vendor's home page for specific information.

List servers represent another useful source of information. They utilize e-mail to alert their "subscribers" of information that is relevant to their topic. They are usually able to provide useful information faster than web pages, and tend to be very specific in nature. www.secunia.com www.securityfocus.com both provide general security list, and www.ntbugtraq.com and the Microsoft Security Notification Service are Windows and related systems specific lists servers.

If all else fails, or if you need help correcting or mitigating the risk of a new vulnerability, newsgroups and are a good source for "on topic" discussions designed to help those with a specific interest or question. And they don't require a subscription; Of course they are not really designed to keep their viewers notified of the latest threats so don't depend on them for up to the minute information.

Vulnerability Scanning

As much as we would all like to believe otherwise, systems that should not change do. And vulnerabilities in both software code and system configurations are discovered on an almost daily basis. But keeping up with which server, needs what update can be an overwhelming task. A vulnerability scanner such as Nessus (www.nessus.org), LanGuard (www.gfi.com/languard/), or Internet Scanner (www.iss.net) can be used to assist you in keeping your system up to date by periodically scanning them for known vulnerabilities. When selecting and using a vulnerability scanner, keep the following important concepts in mind.

Vulnerability scanning is product specific. In other words, it is accomplished with a commercial or 3rd party product, using their techniques, and their definitions of what is and is not a vulnerability. Therefore, it is important that the product(s) be carefully selected and reviewed for fitness on a regular basis.

Nearly all “scanning” solutions depend on some type of “definition” files or plug-ins that describe the known vulnerabilities, and how to detect them. These files should be kept up to date. You want to use a product that supplies regular updates. And be sure that you apply those updates as often as reasonably possible.

Since vulnerabilities are discovered so frequently, the systems should be scanned as often as possible. But, keep in mind the potential impact on the systems you are scanning. Not only will you be generating a considerable amount of network traffic, but if you are not careful in how you configure your scanner, you can actually damage the very systems you are attempting to protect. Make sure you read the documentation carefully and understand the impact before you scan. Also, be sure that you include management in your scheduling plans and that they are aware of the implications of deliberately trying to “hack” your own systems. It is strongly advised that you receive approval in writing, or you may find yourself defending your job, or worse.

Patch Management

A security patch is one way of correcting a vulnerability discovered during scanning or revealed by means of technology watch. In most cases a security patch is relatively benign, and it is acceptable to take time to thoroughly test before applying them to production systems. However, occasionally there is a need to update ALL servers as soon as possible due to the severity of the risk associated with NOT applying the patch.

Patch management revolves around need. The need to apply the patch in order to maintain the integrity of the systems security. If the need is high, then patch management is expedited, if it is low then a methodical approach can be taken. This determination should be made through a formal assessment process. Such a process is often handled by a Security Incident Response Team, but should at a minimum should consider the criticality of the patch and the impact installing (or not installing) could have on the system.

Once you know how important applying the patch is, and you know how it could impact your environment, the task of deployment can begin. Start with letting the technical teams responsible for the systems know what's going on. You will need their help in coordinating and testing. Make sure you convey the urgency of your efforts so they can respond appropriately. When the testing is complete, you will likely need their help again to migrate the changes into your production environment and test the success of that move.

In order to accomplish all of this in a timely manner, you will need a strong deployment plan. Consider a software deployment product such as St. Bernard’s – Update Expert, or Microsoft’s SMS Server to assist you here. Some are even tailored around patches and patch management and can help take the guesswork out of knowing which server needs what patch.

Of course sometimes the patch just will not or cannot be installed. Make sure you have a rollback plan and if possible a disaster recovery option can save hours of time spent troubleshooting a glitch or re-installing your application from the hardware up.

If you do have problems or exceptions, it is important to document and report any issue as a security violation. It is also a good idea to store the current deployment state of patches on all of your mission critical systems.

Configuration management

Sometimes a configuration change is the proper corrective action for an applicable vulnerability. And sometimes configuration changes occur to meet some other business or technical need. Any change to a Windows system represents an opportunity to expose a security weakness. It is imperative that any change to a production system be reviewed for weaknesses in the security model, and well documented. If a change does expose a security weakness, that should be considered a security incident, and handled as such. The process for managing configuration changes is essentially the same as for managing patches.

Virus Protection

A well-planned configuration and regular software updates may not be enough. Viruses, worms and other forms of "Malicious Code" represent one of the greatest threats to the integrity of Windows system security. Often the fastest, and sometimes the only way to mitigate the risk of an exploit associated with a known vulnerability is to use "active" countermeasures, such as virus protection.

One of the most common mistakes in implementing a virus protection solution is in ignoring the concept of *Defense in Depth.* In the same way you would not depend solely on a firewall to stop all attacks, do not rely solely on a virus gateway, or server side solution. Implement a solution that accounts for insertion points, servers and workstations. And, since the effectiveness of any solution is derived largely from the virus definitions in use, and vendors typically use the same set for all of their products, be sure to include products from different vendors for each layer.

Keep your virus definitions up to date. Go so far even as to consider the reaction time of the vendor during the selection process. And try to find products that can both update themselves on a regular basis, as well as be told to update when necessary. Viruses are infecting computers at an alarming rate. PC-World reported that the "Blaster" virus (a recent virus exploiting a known vulnerability in Windows RPC DCOM) "Took off" in the first hour it appeared.[6] You don't want to be hit by the next "Blaster", that you learned about at 10:00 am, at 12:55 in the afternoon just because your virus update schedule occurs at 3:00 in the morning.

Treat every virus infection as if it were an attacker hacking away at your data, because it just might be. It has become common practice for a virus to insert a backdoor or trojan on any machine it infects to give some unknown assailant unfettered access to your system.

Event Management and Auditing

Just one server with event auditing enables and a couple of file shares can generate hundreds or even thousands of entries every day. Multiply that by X number of servers, and it doesn't take long to see how difficult it could be to keep an objective view of the security activities on your network. Not having a clear picture of your security events can seriously impair your ability to detect attacks against your system. Even security firms are not immune, E-week magazine states in one article “In fact, had [the security firm] not assigned someone to comb through the logs, experts predicted, the company may never have detected the intrusion.”[7]

Every event management system begins with a good audit policy. An audit policy is a business language list of security related activities that are relevant to your organization. This list should be reviewed by both technical and legal personnel for any regulatory requirements you may have. Once the requirements are clearly defined you should incorporate the settings necessary into your server build document.

Another important component is a centralized collection and reporting system to provide a one stop view of the security events, to unify the what GFi refers to as “Fragmented audit trail”[8] Ideally it would store the events in a secure, queryable format, that can be easily archived, such as an SQL database.

If you are content to spend countless hours sifting through megabyte after megabyte of redundant cryptic text, or “noise events” you are done. Otherwise you will want to include analysis and alerting into your process. To let you know when something anomalous or unexpected is showing up in the collected logs. But, make sure they are reviewed one way or another, and that any suspicious behavior is reported for the proper analysis and response.

For a list of common security related events, see appendix C.

Account Management

Access control, is defined as; “*Process of limiting access to the resources of an IT product only to authorized users, programs, processes, systems, or other IT products."*[9] All other security considerations will mean very little if you are not maintaining the proper access controls. That process begins with the setting of ACLs on the resources of each system, and is continued with the daily task of account management.

You can use the analogy of a club member (Jack) entering a private club to describe accounts and ACLs. If the **account** (Jack's digital representation) is on the **ACL** (The Members List) and he can provide the proper **credentials** then Jack is given an **access token** (his hand is stamped) and allowed to come in. This process is known as *authentication*. Jack's next stop is the bouncer, who determines that Jack is a stand up kind of guy and leaves him free to roam anywhere in the club he would like, except for the “back room”, because only club owners get to go there, and Jack is not in that

security group (the list of owners). That process is known as *authorization.* Sounds simple, but there is plenty going on in the background to make it all work.

To keep it as simple as possible, it is strongly recommended that you use a centralized account management model. Centralized management simplifies the process of adding, removing and modifying users within the system. It also makes it much easier to find out what access any given person has at any given time.

Always follow a set practice. It is possible to grant access to resources at different levels and in different ways. If you stay consistent, it will be much easier to keep up with it. This includes everything from following the AGLP process to using standard naming conventions for all users and groups.

Audit changes and settings on a regular basis. It is very easy to loose track of stale accounts, and unnecessary rights, especially if you have a large environment, or regular changes and turn-over.

Appendix A – Windows Policy Template settings

Account Policies
Password Policy
Enforce password history
Maximum password age
Minimum password age
Minimum password length
Passwords must meet complexity requirements
Store password using reversible encryption for all users in the domain
Account Lockout Policy
Account lockout duration
Account lockout threshold
Reset account lockout counter after
Kerberos Policy
Enforce user logon restrictions
Maximum lifetime for service ticket
Maximum lifetime for user ticket
Maximum lifetime for user ticket renewal
Maximum tolerance for computer clock synchronization
Local Policies
Audit Policy
Audit account logon events
Audit account management
Audit directory service access
Audit logon events
Audit object access
Audit policy change
Audit privilege use
Audit process tracking
Audit system events
User Rights Assignment
Access this computer from the network
Act as part of the operating system
Add workstations to domain
Back up files and directories
Bypass traverse checking
Change the system time
Create a pagefile
Create a token object
Create permanent shared objects
Debug programs
Deny access to this computer from the network
Deny logon as a batch job
Deny logon as a service
Deny logon locally
Enable computer and user accounts to be trusted for delegation

Force shutdown from a remote system
Generate security audits
Increase quotas
Increase scheduling priority
Load and unload device drivers
Lock pages in memory
Log on as a batch job
Log on as a service
Log on locally
Manage auditing and security log
Modify firmware environment values
Profile single process
Profile system performance
Remove computer from docking station
Replace a process level token
Restore files and directories
Shut down the system
Synchronize directory service data
Take ownership of files or other objects
Security Options
Additional restrictions for anonymous connections
Allow server operators to schedule tasks (domain controllers only)
Allow system to be shut down without having to log on
Allowed to eject removable NTFS media
Amount of idle time required before disconnecting session
Audit the access of global system objects
Audit use of Backup and Restore privilege
Automatically log off users when logon time expires
Automatically log off users when logon time expires (local)
Clear virtual memory pagefile when system shuts down
Digitally sign client communication (always)
Digitally sign client communication (when possible)
Digitally sign server communication (always)
Digitally sign server communication (when possible)
Disable CTRL+ALT+DEL requirement for logon
Do not display last user name in logon screen
LAN Manager Authentication Level
Message text for users attempting to log on
Message title for users attempting to log on
Number of previous logons to cache (in case domain controller is not available)
Prevent system maintenance of computer account password
Prevent users from installing printer drivers
Prompt user to change password before expiration
Recovery Console: Allow automatic administrative logon
Recovery Console: Allow floppy copy and access to all drives and all folders
Rename administrator account
Rename guest account
Restrict CD-ROM access to locally logged-on user only
Restrict floppy access to locally logged-on user only
Secure channel: Digitally encrypt or sign secure channel data (always)
Secure channel: Digitally encrypt secure channel data (when possible)
Secure channel: Digitally sign secure channel data (when possible)
Secure channel: Require strong (Windows 2000 or later) session key
Secure system partition (for RISC platforms only)
Send unencrypted password to connect to third-party SMB servers
Shut down system immediately if unable to log security audits
Smart card removal behavior

Strengthen default permissions of global system objects (e.g. Symbolic Links)
Unsigned driver installation behavior
Unsigned non-driver installation behavior
Event Log
Settings for Event Logs
Maximum application log size
Maximum security log size
Maximum system log size
Restrict guest access to application log
Restrict guest access to security log
Restrict guest access to system log
Retain application log
Retain security log
Retain system log
Retention method for application log
Retention method for security log
Retention method for system log
Shut down the computer when the security audit log is full

Appendix B – Non-Printing ASCII characters

Char	Dec	Oct	Hex
(soh)	1	0001	0x01
(stx)	2	0002	0x02
(etx)	3	0003	0x03
(eot)	4	0004	0x04
(enq)	5	0005	0x05
(ack)	6	0006	0x06
(bel)	7	0007	0x07
(bs)	8	0010	0x08
(ht)	9	0011	0x09
(nl)	10	0012	0x0a
(vt)	11	0013	0x0b
(np)	12	0014	0x0c
(cr)	13	0015	0x0d
(so)	14	0016	0x0e
(si)	15	0017	0x0f
(dle)	16	0020	0x10
(dc1)	17	0021	0x11
(dc2)	18	0022	0x12
(dc3)	19	0023	0x13
(dc4)	20	0024	0x14
(nak)	21	0025	0x15
(syn)	22	0026	0x16
(etb)	23	0027	0x17

(can)	24	0030	0x18
(em)	25	0031	0x19
(sub)	26	0032	0x1a
(esc)	27	0033	0x1b
(fs)	28	0034	0x1c
(gs)	29	0035	0x1d
(rs)	30	0036	0x1e
(us)	31	0037	0x1f
(sp)	32	0040	0x20

Appendix C – Security Related Event Ids

Logon Events	
EventID	**Description**
528	A user successfully logged on to a computer.
529	The logon attempt was made with an unknown user name or a known user name with a bad password.
530	An attempt was made to log on with the user account outside of the allowed time.
531	A logon attempt was made using a disabled account.
532	A logon attempt was made using an expired account.
533	The user is not allowed to log on at this computer.
534	The user attempted to log on with a logon type that is not allowed, such as network, interactive, batch, service, or remote interactive.
535	The password for the specified account has expired.
536	The Net Logon service is not active.
537	The logon attempt failed for other reasons.
538	A user logged off.
539	The account was locked out at the time the logon attempt was made. This event can indicate that a password attack was launched unsuccessfully resulting in the account being locked out.
540	Successful Network Logon. This event indicates that a remote user has successfully connected from the network to a local resource on the server, generating a token for the network user.
682	A user has reconnected to a disconnected Terminal Services session. This event indicates that a previous Terminal Services session was connected to.
683	A user disconnected a Terminal Services session without logging off. This event is generated when a user is connected to a Terminal Services session over the network. It appears on the terminal server.
Account Logon Events	
EventID	**Description**
672	An authentication service (AS) ticket was successfully issued and validated.
673	A ticket granting service (TGS) ticket was granted.
674	A security principal renewed an AS ticket or TGS ticket.
675	Pre-authentication failed.
676	Authentication Ticket Request failed.
677	A TGS ticket was not granted.
678	An account was successfully mapped to a domain account.
680	Identifies the account used for the successful logon attempt. This event also indicates the authentication package used to authenticate the account.
681	A domain account logon was attempted.
682	A user has reconnected to a disconnected Terminal Services session.
683	A user disconnected a Terminal Services session without logging off.

Account Managment Events	
EventID	**Description**
624	User Account Created
625	User Account Type Change
626	User Account Enabled
627	Password Change Attempted
628	User Account Password Set
629	User Account Disabled
630	User Account Deleted
631	Security Enabled Global Group Created
632	Security Enabled Global Group Member Added
633	Security Enabled Global Group Member Removed
634	Security Enabled Global Group Deleted
635	Security Disabled Local Group Created
636	Security Enabled Local Group Member Added
637	Security Enabled Local Group Member Removed
638	Security Enabled Local Group Deleted
639	Security Enabled Local Group Changed
641	Security Enabled Global Group Changed
642	User Account Changed
643	Domain Policy Changed
644	User Account Locked Out

Object Access Events	
EventID	**Description**
560	Access was granted to an already existing object.
562	A handle to an object was closed.
563	An attempt was made to open an object with the intent to delete it. (This is used by file systems when the FILE_DELETE_ON_CLOSE flag is specified.)
564	A protected object was deleted.
565	Access was granted to an already existing object type.

Privilege Use Events	
EventID	**Description**
576	Specified privileges were added to a user's access token. (This event is generated when the user logs on.)
577	A user attempted to perform a privileged system service operation.
578	Privileges were used on an already open handle to a protected object.

Process Tracking Events	
EventID	**Description**
592	A new process was created.
593	A process exited.
594	A handle to an object was duplicated.
595	Indirect access to an object was obtained.

System Events	
EventID	**Description**

512 Windows is starting up.
513 Windows is shutting down.
514 An authentication package was loaded by the Local Security Authority.
515 A trusted logon process has registered with the Local Security Authority.
516 Internal resources allocated for the queuing of security event messages have been exhausted, leading to the loss of some security event messages.
517 The security log was cleared.
518 A notification package was loaded by the Security Accounts Manager.

[1] "Trust Services Principles Version 1.0" can be found at: https://www.cpa2biz.com/ResourceCenters/Information+Technology/SysTrust/None_00_aicpaorg_assurance_systrust_index_systrust_in_09914.htm

[2] Taken from "Best Practices for Enterprise Security – Security Threats" Part 1 or a three part series of white papers published by Microsoft found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Default.asp

[3] Taken from "Securing Networks Systematically — the SKiP Method" and related articles published by the CERT Coordination Center, found at: http://www.cert.org/security-improvement/skip.html

[4] Derived primarily from "Windows 2000 Server Baseline Security Checklist" found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/chklist/w2ksvrcl.asp

[5] Taken from "The Twenty Most Critical Internet Security Vulnerabilities" found at:http://www.sans.org/top20

[6] Taken from "Blaster Worm Continues to Spread" an article published by PCWorld.com found at: http://www.pcworld.com/news/article/0,aid,111973,00.asp

[7] Taken from the Eweek magazine article "Even Security Firms at Risk for Break-ins" February 17, 2003

[8] Guidance for this section taken from "Why event log management?" a KB article for GFi Event Log Monitor 4 found at: http://kbase.gfi.com/showarticle.asp?id=KBID001624

[9]As defined in "The Consolidated Security Glossary of the National Institute of Standards and Technology (NIST)" found at http://www-08.nist.gov/posix/framework_wg/glossary.asc

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event