# Global Information Assurance Certification Paper

# GSEC Practical Assignment Version 1.2d
# Raymond C. Hall III
# Title-Out of the box and into the fire

## Don't go with "Out of the Box" Installs

So you just installed a new workstation and are ready to connect it to your corporate network. There is nothing else to do right? Wrong. A situation of plug and play becomes an issue of plug and pray. There are measures and precautions that need to be addressed for the system to be within an acceptable risk or proper accreditation. An accreditation is a set of guidelines by which a system is to be setup or configured. Every organization should have all their computer systems that come through the door configured with these basic guidelines. The next section goes into a description of what should be included in a computer accreditation.

## Accreditations

Any system that goes online in an organization should meet an acceptable risk assessment or accreditation. This is a set of guidelines that an administrator or end user follows to bring their system up to par as far as being within an acceptable state for processing information, whether online or stand alone, mainly online. This is something that the end user should be aware of in how and what the guidelines accomplish. These guidelines go through such things as gathering information about the system such as make, model, serial number, and IP address and MAC address of the system. Getting information about the user like name, room number, phone number and employee number.

Then you step through the guidelines with the system and check off items such as the following;

- What is the operating system running on the system and are the latest stable patches installed?

  Sometimes you can install a patch or update and have that update cause more problems than it fixes. Test all patches, service packs, or equivalent fixes on non-production systems before implementing in a production environment.

- Is the system running an antiviral program and how is it updated?

- When are scans run?

- Is it a multiple user system? If so, who are the users and how is their online activities tracked as far as audit trials go?

- Who is responsible in the event of an incident?

Some additional items should be;

- Does the system have a modem in it and why?

  Modems can be back doors into corporate networks and circumvent first line defenses such as firewalls. One would only have to war-dial or dial each number within an organization to see if a modem picks up or answers the line. There are many programs available that accomplish this task automatically.

- Are passwords changed frequently and are they complex, i.e. not easily guessed.

- Do they process sensitive information on the system?

- How long till the next evaluation of the system?

- Are there log files and who checks them?

  This information should be filed and maintained for future reference in the case of an incident occurring. A system administrator can go back and see by the accreditation paper work that the system met the minimal set of requirements set fourth by the corporation. They can also check to see if something was missed or possibly changed that caused a vulnerability to occur. Maybe it is something new that was not part of the evaluation that now can be included in the accreditation. Doing these evaluations and reviewing them on a periodic schedule can keep the system, as well as the process, up to date.

The next two sections cover the basic minimal security settings for Windows NT 4.0 Workstation and Linux Mandrake Workstation (to be referred to as just Linux through out the rest of the paper) that will allow them to meet accreditation requirements. In other words, a basic general configuration of each operating system that helps minimize possible security threats. This by no means will go into detail about security form a server point of view, which is more in depth than that for a typical workstation or go into a step-by-step setup. This also doesn't make the operating systems impervious to attacks, just mitigates some of the risk. This is because an "out of the box" install unfortunately comes with minimum-security settings. This is something that operating system venders should address at the level of manufacturing. Systems should go out with security settings set higher with the option for the end user to downgrade the security settings when and if they need to. This approach would be greatly appreciated in the system administration arena. Furthermore, the next sections do not go into the security settings of Windows 2000 Professional. Although there are some similarities between the two as far as concepts and even some practices, Windows 2000 introduces some new features and considerations that should be addressed separately, for example Active Directory. Windows 2000 is just now beginning to

be closely scrutinized as far as security and there should be some good information provided in the not to distant future.

**Windows NT 4.0 (Workstation Only)**

A basic fresh install of NT leaves some security issues to be desired. There are a number of great resources available online and in print that step through the process of securing an NT workstation. This section will not go into great detail about the actual steps required to secure the workstation, for that is a subject in itself. What will be covered here are the fundamental concepts that most of the resources explain. For example, file permissions, password rules, file system properties, and system settings.

Some of the items in question are done during the install process of NT. The issue of whether or not the drives are NTFS for instance. NTFS is a 32bit file system for Windows NT that is more secure than the old FAT file system. This allows you the ability to assign authenticated permissions to files and folders. Another thing is what services should be installed? The best bet is to only use what you need to use. The more services that run, in turn, are all the more things that need to be keep track of and possibly patched.

Once the system is up and running you will want to check and make sure it has the latest stable service pack installed including updated security patches. Configure the auditing of user accounts for such things as failed login attempts, policy changes, and failed access permissions on protected folders. One will also want to set the log files to not overwrite when full as well as increase the size of each log. It is recommended that these logs be checked frequently. Another good measure is to ensure that the SAM database is encrypted with syskey.

With NT you will need to be comfortable and know your way around the registry editor so that some changes can be made (i.e. the clearing of the page sys file on shutdown and enabling the logging of system backups). A few issues include: setting the right permissions on certain registry keys to disallow particular users to access portions of the registry; knowing who has a current recovery disk and where is it kept; and ensuring a strong password policy is enforced. These are just some of the things that should be done at a minimum to bring a system up to an acceptable risk factor. There are certainly many more, however too many to mention in this paper. As mentioned before, this is a description of the concept behind making NT secure, not a detailed step-by-step. The message to take away here is that NT has some problems that one wants to realize and take care of before putting the system online. A helpful tactic is to keep track of the latest vulnerabilities and patches. Subscribing to a good mailing list is one way to accomplish this for both NT and Linux.

**Linux (Workstation Only)**

The best and easiest way to secure or "harden" a Linux workstation is to run a program called Bastille Hardening Script. This script is a menu drive program that will step you through a series of questions about your system. What security measures the script will implement is dependant on the answers you give. This is a very sound way of covering most of the vulnerabilities that exist in an "out of the box" install of Linux. Although these settings can be done manually, it is less time consuming and more convenient to use the script. Therefore, a strong understanding of how Linux works is not necessary to secure the system. It is written in such a way as to describe and explain what each step does to your system and why it should be corrected. Bastille is a proven security-hardening tool and works with Linux distributions that are compatible with RedHat Linux.

Bastille steps through such things as: installation and the use of SSH (Secure Shell) over telnet and FTP (this is important because both are not secure due to the use of clear passwords and unencrypted connections); locking down super user account access for certain services; disabling unused services to cut down on possible backdoors to the system; enabling proper auditing of system usage and user accounts; installing TCP wrappers and modifying the /etc/hosts.allow and /etc/hosts.deny files appropriately; checking for the latest patches or updates; disabling anonymous access; and disabling r* utilities, such as rlogin, rshell, etc. These are just a few of the things that Bastille will do for you allowing the system to work at an acceptable risk level.

**Educating the End User**

In the world of computer support having an informed end user can be both a good thing and a bad thing. Sometimes you want an end user to take care of small things but not try to rebuild their own system or install un-tested updates or service packs. When it comes to information security, as far as "the last line of defense", having an end user with basic knowledge of what to look for or just the understanding of the minimal security precautions taken on their own system, can be of great importance to an organization, but may lead to a "cry wolf" scenario. One needs to weigh the odds of the problems against the benefits of the solutions.

Once you have stepped through the accreditation paper work with the end user and they understand what was done to their system, they now become part of your information assurance program. It is your job to make them security aware. Teach them to understand what it means if they find a failed logon. While this may cause false alarms, at the same time, it may bring to light possible compromises as well as what may have been missed otherwise. An educated end user is a useful end user. This by no means replaces the need for properly trained individuals to carry on daily security activities such as log review and virus tracking. Simply think of the end user as another tool for discovering potential incidents.

Users must be aware of their system and how they are protected. A similarity can be found with home security. Homeowners don't have security systems in their homes without the basic knowledge of how they work. If you open a door or window the alarm will go off. If there are motion sensors and motion is detected, the alarm will go off. The same thing is true with an end user's system. If a virus is detected how does the system respond and who is notified? Inform them that any and all virus activity should be reported to the proper person within their organization. It could be the beginning of a new attack or just an old reoccurring pest, like the "Concept" virus. Either way, a trail needs to be followed to find out where it came form in order to prevent it in the future. The majority of end users disregard such an event potentially causing crucial forensic data to be lost. End-users should be provided with security policy procedures to follow, which have been signed off on by upper management. This is very important, upper management must be involved and aware of the policy in order to back up the procedures you wish to put in place. This ensures that everyone is covered and ignorance is no longer an excuse. A good end user guide, which includes an organization's security policy, becomes an indispensable knowledge tool for the computer user community. The next section will go into some of the basics to include in a good security policy.

**Security Policies**

Every organization that have users with computers, either standalone or networked, must have an effective and clearly stated security policy which is approved and signed by upper management as well as each and every end user. The key point here is that both upper management and the end users understand what this policy is and what it accomplishes. When you start implementing strict security policies you begin to hinder workflow. If you increase the ease of workflow, you cannot have effective security policies. There has to be a balance, one that reflects the stance of the organization. Does the policy reflect the organizations views of importance concerning the protection of information assets? Answering no to this question may be all it takes to make them tempting targets for attack. If your end users find the policies in place hard to understand or difficult to follow on a daily basis, then the users might gravitate to trying to circumvent the policies to meet their needs. Similarly, if upper management fails to realize the importance and protection good policies offer, it might setup the organization to internal as well as external problems.

A security policy should leave no room for assumption. If there is an important point to make, state it clearly in general terms so that the average user can understand it. Points such as notifying the user that use of the computer system subjects them to monitoring and that any information collected can be used against them. What type of access to the network and file servers is allowed (i.e. save,

move or delete capability) needs to be spelled out. A user may have access to resources, but not have a right to use them. An option is to deny all access to resources on your network and then on a case-by-case basis individually allow users access. You could deny all access to resources on your network and individually allow, but this creates more administrative work for you. Just use the policy to educate the user to common sense in a network environment.

You may also want to include possible repercussions that might be taken if a policy is violated. This reinforces the organizations stance on security and the importance of following the security procedures. At the same time you want to point out the advantages the policies provide to the end user. Besides making them security aware, the policies also protect them and safeguard their information. As I said before, the end user can be another useful tool in information assurance.

Time should be taken to re-evaluate the policy throughout the year. Collect feed back from the user community as to how they feel about the procedures. Keep them, as well as upper management, in the loop at all times. Security procedures are not "provide and forget." Policies should be constantly updated and modified to fit the growing needs of the organization. Provide training courses and/or have resources available to help end users understand why and what the policies are for, thus lessening the possibility of end users working against your efforts. Security can be hard enough without your users making it harder.

**Summary**

No system is completely 100% secure. This is true especially if it is connected to the outside world, but even if the system is a standalone there are physical security problems. Is it possible for anyone to get physical access to the system? With physical access there is very little that one cannot do to get into a system. With this in mind, security needs to be addressed with the "speed bump" mentality. You want to slow intruders down in order to see what they are doing and from where. Make an intruder work for whatever they are trying to accomplish. Find the hole they came in through, plug it, and wait for the next attack.

People falsely believe that just because they are behind a firewall, everything is safe. Users often don't realize that attacks can be internal, both purposely and unintentionally. People can bring a Trojan horse virus from the outside on disk or CD and unknowingly infect their own system. These viruses can then establish connections to the outside world. This is why Firewalls should block not only incoming ports but also lock unused outgoing ports. An outside threat can gain access to a network and completely go around the firewall by war-dialing someone that has a modem installed on his or her system. This is where an IDS (Intrusion Detection System) comes into play.

Having an IDS in place, with sensors deployed throughout an organization, one has a better chance of picking up on an attack. An IDS, in its basic design, looks at traffic on the network for certain patterns whether the patterns come from log files or erroneous packets on the network itself. If the IDS program picks up on a pattern match, i.e. multiple failed logins on one account followed by a successful login from the same account, it would likely notify an administrator about this activity. Another way is to deploy a sensor on your DMZ (network space on the outside of your firewall) and have it match its findings with an inside sensor. The outside will certainly pick up on more traffic than the inside one. However, if a match of unusual traffic can be established between the two, then there might be a compromise somewhere. None of this can be guaranteed, but it does allow for possible activity to be brought to an administrator's attention without the administrator having to sort through numerous logs to discover it themselves. A possible incident might be overlooked if a pattern is not otherwise noticed. Although IDS does not replace the need for administrators to review logs or watch traffic on their network, it does add another line of defense to the already complex world of information assurance.

**Conclusion**

Security is an ongoing, developing, adaptive creature. Trained people must manage it, however a well-informed, aware person can be taught to spot possible incidents. An organization must have multiple layers of protection. Firewalls, IDS, virus protection, security policies, and end-user training are just a few of the things that should be in place. With the ever-growing trend of sharing information across the globe, organizations cannot afford to underestimate their security needs. When it comes to addressing needs, the majority is now realizing that security should be their number one concern and priority.

**References**


- **Naval Surface Warfare Center**, Dahlgren VA Accreditation Forms Page http://www.nswc.navy.mil/ISSEC/Form/AccredForms/index.html (May 10, 2001)

- **CERT® Coordination Center (CERT/CC)** UNIX Configuration Guidelines http://www.cert.org/tech_tips/unix_configuration_guidelines.html (May 20, 2001)

- **CERT® Coordination Center (CERT/CC)** Windows NT Configuration Guidelines http://www.cert.org/tech_tips/win_configuration_guidelines.html (May 20, 2001)

- **Control Data Systems, Inc.** Why Security Policies Fail http://www.securityfocus.com/data/library/Why_Security_Policies_Fail.pdf (May 18, 2001)

- **The SANS Institute** How To Build A Successful Security Infrastructure, Section Three

http://www.sans.org/newlook/resources/policies/bssi3/sld001.htm (May 21, 2001)

- **CERT® Coordination Center (CERT/CC)** Security Knowledge in Practice Module http://www.cert.org/security-improvement/skip.html (May 21, 2001)
- **The SANS Institute** Intrusion Detection FAQ Version 1.51 http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm (May 21, 2001)
- **The SANS Institute** Windows NT Security Step By Step Version 3.03 February, 2001
- **The SANS Institute** Securing LINUX Step By Step Version 1.0
- **The Royal Institute of Technology** NT Security – FAQ Version 0.29 http://www.it.kth.se/~rom/ntsec.html (May 21, 2001)
- **Bastille Linux** Linux Hardening Script Version 1.2.0 http://www.bastille-linux.org/ (May 21, 2001)
- **Computers and Academic Freedom Project** Academic Computing Policy Statements Archive updated June 28, 1999 http://www.eff.org/pub/CAF/policies/ (May 22, 2001)

Last Updated: May 28th, 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 |