Global Information Assurance Certification Paper

Securing a Small to Medium Enterprise: An Overview

David Olsen

January 3, 2005

Practical Assignment version 1.4b – Option 1

Securing a Small to Medium Enterprise

Abstract

With the constant threat to today's businesses from viruses, malware and persons with malicious intent inside and outside its doors, it has become an operational imperative to secure the network infrastructure from attack. Unfortunately for the Small-to-Medium Enterprise (SME), this can be a very difficult task. Lack of specific training, small to non-existent security budgets and more projects than personnel make securing a network nearly impossible. Additionally, monitoring and maintaining a network becomes more and more demanding. Daunting as it may seem, there are ways to accomplish the job. The intent of this paper is to aggregate resources to help the technical person or persons responsible for implementing security for their company and present them in a way that will allow the reader to design their own plan for securing their corporate network. I will present a broad outline of the tasks necessary, the reasons for them and some resources to accomplish them. The areas I will be covering here are as follows: Perimeter/Network, Server/Workstation and Policies/Procedures. I am defining an SME as having up to 1000 employees, 10 - 50 servers and up to a handful of sites connected via Wide Area Network. Additionally, it is assumed that all the work is being done by employees, not contractors or other third parties. Also, this is not a "Configure Your Router Securely", "Lock Down Your Firewall" or "Harden Your Server" paper. That has been done many times before and it is not necessary to reiterate here, though there will be references to some of these materials within this discussion.

Designing A Secure Network

There is an oft quoted phrase that, "Security is a process, not a state". This is an important concept to keep in mind. The ideas in this exercise are a starting point, something to build a process around. They are not a finished product. Once you have begun the process of Security, you can never stop and relax. There are always new threats, new situations, and better ways of doing things. It is hoped that after reading this paper, the person or group assigned with securing their company's network will be better equipped to create a *more secure* environment for their company and can be ready for new security issues as they occur.

Design is the first step in making your network secure. If you have the opportunity to design your network from scratch, you have a significant advantage since you don't have the problems of maintaining uptime and availability for the company while locking down the network. If you do not have that luxury, make sure that you have informed the users at each step exactly

how it will affect them and, if possible and budget allows, put a temporary device in place to replace the service, in order to mitigate any possibility of an unavailable resource. The irony of causing downtime because you are trying to increase security and stability in the network is lost on most end users, including management.

In designing a network that is as secure as possible, you need to first understand how your business operates. Some questions a security professional should ask as they begin that process of understanding are: What are the important functions of the company's day-to-day business? How are they implemented in technology? Once that is understood, a plan can be devised to protect the important resources, assets and processes and make them reliable and secure so that your business is not compromised. An added benefit to closing your network to intruders is that you are not making your network a place for others to stage an attack. If you can keep your network from being used as a haven for illegal activity, you are protecting yourself from further potential compromise, as well as possible legal action from other entities attacked by someone from your network due to negligence.

An important principle in any IT practice is K.I.S.S., or Keep It Simple, Sir. You want to keep the design of the network as simple as possible, because overly complex networks are difficult to manage, maintain and secure. One way to do that is to segment your services as much as you can. It's easier to lock down, monitor and troubleshoot when it is with others of its kind than when they are scattered around the network. For instance, you could keep all your web, file, application and database servers separated by Virtual Local Area Networks (VLANs). Using this configuration, it would be possible to allow only traffic from appropriate individuals or groups to that network. In addition, by monitoring activity on that segment, seeing and acting on abnormal network behavior would be greatly facilitated with the appropriate tools. The subject of monitoring activity will be dealt with later in the paper.

"Defense in Depth" is often stressed in security literature, training and discussion and is an idea in which I firmly believe. Its basic premise is that if done right, a layered construction of data protection makes it more costly to compromise the data than the data is worth to an intruder. By layering your defenses, as one gets closer to the data, the more difficult and time consuming it is to get through those defenses. What I will discuss now are the layers in our scenario and their design and implementation.

Securing the perimeter

The first thing someone in charge of securing a network does is purchase a firewall. This is a good idea, but it can turn into a liability. According to the SANS Institute, "Implementing firewalls with rules that don't stop malicious or dangerous traffic-incoming or outgoing" is one of the worst mistakes a technology professional can make[4]. A good place to start looking for help in configuring firewalls is at Lance Spitzner's website (http://www.spitzner.net). His articles explore the entire process of firewall installation, from hardening the

server on which it resides to auditing the firewall once it is installed and configured. It is important to remember that normally configured firewalls are designed to allow some traffic into the network, such as email, web traffic or vpn tunnels. Unfortunately, it is relatively easy for this traffic to be compromised, bypassing your firewall's defenses in the process. In addition, users inside the network can wreak havoc on data without touching a firewall unless proper internal access controls are implemented. Terry Grey, of the University of Washington, has distilled these problems into what he calls the *"Perimeter Protection Paradox"* . In essence, it states that as the number of devices inside the border firewalls increases, the value of the defensive device increases, but the effectiveness decreases. This does not mean that a firewall serves no useful function, but it does mean that you shouldn't rely on them as your sole means of defense. A firewall should provide a basic control of what goes in and out of a network. The CERT® Coordination Center (http://www.cert.org) (who, according to their website, was the first computer security incident response team) provides an excellent series of articles on security, including one on firewall design and deployment that can be a great assistance to the Security professional.

Firewalls are not the only perimeter devices. In most situations, a router is installed in front of the firewall as the first device between the Internet and the Network. Since this is an extremely exposed position, it is vital to lock it down as securely as possible. The SANS™ (SysAdmin, Audit, Network, Security) Institute (http://www/sans.org) has a Checklist document specific to Cisco routers, but its principles are valid for routers by most any manufacturer. Here again, it is a matter of only allowing inbound and outbound traffic necessary to the function of your business. It is much easier to add services as requested than it is to take them away later after they have been put into use.

Once security on the external devices has been tightened, you can move on to the next phase of perimeter security. Separating internal processes from external processes is imperative and is usually implemented with a DMZ, or De-Militarized Zone. A DMZ is, in its simplest implementation, a firewall with 3 interfaces. As with a normal firewall, one interface points to the insecure, external network, often the Internet. The second points to the more secure, internal Local Area Network, or LAN. The third interface connects to another, smaller network. It is not fully trusted by the internal or external network, but it allows traffic of a specific type to enter and exit toward a specific place. As part of the design process, the security professional will have discovered any services that are used by the general population or by business partners outside the network. These services include web servers that provide the external Internet presence of the company, ftp servers to access or post data, smtp servers for routing mail to and from the outside world, plus many other possibilities. In many instances, these services would need to be accessed by employees or contractors inside the network, as well. An example would be an external web server that is maintained by someone on the internal side. A very useful security tool that can assist in securing this configuration is a network-based intrusion detection system or NIDS

(http://www.sans.org/resources/idfaq/network_based.php). A NIDS is either a software program that resides on a hardened computer with a network card configured to be in promiscuous mode (i.e. listening to all traffic on a subnet, not just traffic destined for it) or a single function appliance, whose purpose is to monitor and make note of network traffic that is considered “abnormal”. This device can also be used, as mentioned previously, in VLAN segments. One drawback with these devices is the difficulty in defining “normal”. Establishing a baseline is an important part of the definition process and will be discussed later in the paper. Another challenge is keeping up with changes to what has been established as normal. As each new exploit comes out, a new definition must be added to the device so that the NIDS can mark that traffic as out of the ordinary.

Getting access through the secure perimeter into the internal network is a frequent request to security professionals. In the last several years, as private corporate networks have become more prevalent, sharing data between companies more common and employees working outside the office, there is a need for opening up the network. Ideally, this is done in as secure a fashion as possible by implementing a Virtual Private Network, or VPN. VPNs allow a user or corporate entity access to a LAN through the insecure public Internet via an encrypted tunnel. These tunnels are created with a variety of protocols, including PPTP (Point-to-Point-Tunneling-Protocol), IPSec (IP Security Protocol) and, recently, SSL (Secure Socket Layer, the protocol used in securing most web-based transactions). An important consideration with these tunnels is that, while the tunnels and data are encrypted, the computer user on the other end of the tunnel has complete access to the network, as if they were sitting in your office. It is for this reason that it is vital to make sure the computers connecting to your network via a VPN tunnel are secure. When you have the ability to control what is on the other side of the tunnel, securing the clients is a relatively straightforward process. However, when you are connecting a customer or business partner to your network, there are more complex issues at stake. These issues have little to do with the technical side of IT and much more to do with the political and business side. They often involve policies outside of your control, but if possible, try to get the owner of the other network to agree to an independent audit and implement connection policies to protect both companies. These precautions are as much in their best interests as they are in your company's.

Locking Down Servers and Workstations

Once the external portion of the network is secured, it is time to move on to the servers themselves. There are several steps in the process of securing the computers on your network. There are some interesting anecdotal stories of people who connected a freshly installed computer directly to the Internet without patching it (perhaps they were planning on going to the vendor's website to download the patches). Within a matter of minutes, the computer had been compromised. Of course, most IT professionals would at least have had a

firewall between them and the Internet, however the point is made. It is imperative to download patches and service packs on a known good machine, burn them to a CD and install them on a new machine before ever connecting it to any sort of network, much less directly to the Internet. Another step to take before networking the computer is to remove or at least disable any service or program you don't need. In some cases this can be easier said than done, particularly with Windows-based machines. Microsoft has a 300+ page document that explains in detail what you can do to harden your Windows 2000 server and domain. The paper also explores how the functionality of the server and other computers on the network is affected by locking them down. In the last several months or so, Microsoft has begun a push for better documentation of securing its products. You can find extensive information on securing Windows machines and other Microsoft products on the websites listed in the Resources section at the end of the paper. Compared to Windows, it is relatively easy to install a Linux or Unix-based system with only the exact set of features and functionality you want. The difficulty begins when addressing dependencies, though these concerns are being addressed by many distribution vendors. If you attempt to install a service or feature without installing software it is dependant upon, most major distributions will warn you and offer to install the missing software.

After you have completed patching the system and before you connect to a network, you should install some sort of Host-based Intrusion Detection System, or HIDS. This software service takes a baseline of the system as it is at the time of installation and monitors any changes to software and files that you have told it to watch. This useful tool can enable you to determine whether your machine has been compromised. Unfortunately, in most instances this software is also complex and difficult to maintain. Windows machines have some ways of monitoring and denying the installation of “unsigned” or untrusted software using Group Policy settings. There are also commercial software packages that will do a more comprehensive job of tracking changes and notifying the appropriate people of what has changed. Tripwire is a prominent player in this field. Their website has an excellent section on best practices of Change Management (http://www.tripwire.com/practices/index.cfm). Linux distributions come with an Open Source version of the Tripwire product, though it doesn't seem to be very actively maintained at the moment, with the latest update from 2001[13]. This version can be difficult to install, configure and maintain if you are unfamiliar with the concepts of the software, though if you have the time, it is a good way to learn about them. There is a commercial version also available for Linux, and it is similar to the Windows version in terms of features and configurability. On a side note, Tripwire also has products for routers, which is a something to seriously consider for your network.

Once you have a server installed, configured, patched and baselined for HIDS, it's almost ready to be connected to a trusted network. In many circumstances, a software firewall is a good idea to install on the server itself, even though this is often considered an optional step. There are commercial firewalls that can be installed on servers from companies like ZoneLabs, Tiny, Symantec and McAfee. Linux has an Open Source firewall called netfilter which

uses iptables as its rule definition table. It is also used as the basis of many commercial products for Internet facing firewalls. The netfilter website has many HOWTO documents that can assist you in utilizing this software as well as coming to grips with the concepts of networking, filtering, and Network Address Translation (NAT) among others.

The final piece of the server hardening puzzle is antivirus (AV) software. These products are an important component of any security software package, particularly on Windows servers, as they seem to be the most prominent targets of viruses and other malware. Linux and Unix-based servers can also install AV software. This can be especially useful for email servers and file servers that provide services to Windows-based machines. Many vendors also provide other features, such as spyware scanning and firewalls. Get the latest version of your particular vendors product from its website and also download the latest virus signature. Install the software, reboot (this is usually required of Windows machines) and then install the updated signature. You can now connect to the network with relative security.

Now that you've installed, patched and hardened the server and configured its security software, the hard work begins. Software is never perfect, no matter how hard an individual or company tries to make it so. There are always stability and security patches and functionality enhancements that are required over the course of an applications lifecycle. This has become a growing problem for IT professionals because of the constant release of patches, the fact that some of them are not necessary for a given situation and also that there are occasions when they end up causing problems where none existed. Another problem that is becoming more and more prevalent is the “zero-day” exploit. As vulnerabilities are found in software, most responsible security professionals release their findings to the maintainer of the software through private channels, giving them an opportunity to fix the vulnerability and release a patch to the public. There are also malicious developers who create software templates. This would allow them to, once a vulnerability is released to the public with the accompanying patch, add code on top of the template to take advantage of that security hole and release it to the cracker community or utilize it themselves almost immediately. This becomes a quandary for IT professionals. Patch your server quickly and risk causing a problem or don't patch it and hope that you are able to avoid becoming a victim of malware. Because of this, Patch Management has become a growing industry in the security field, with several companies offering a wide variety of products. When considering a product, try to keep in mind what you need to manage (whether it is multiple Operating Systems or office suite software, for example), where the managed systems are located, how quickly the patches are received from the vendor, and whether you can rollback the patch or not. Some providers of patch management software include Ecora, St. Bernard Software, Shavlik, BigFix and several others. There are even some vendors who provide a limited version of this functionality, Microsoft and Red Hat Linux being two examples. In an interesting article that deals with the process of developing patch management

strategies, the author talks with those in charge of patch management at various companies and questions them on how they deal with the pitfalls and the evolving nature of applying patches for systems from servers and workstations to routers and switches. In addition, you will find a good list of “Do's and Don'ts” at the end of the article that can be useful in implementing your own policies.

Over the course of the last several years, security exploits have been expanding from the perimeter of the network to the servers and have most recently been rapidly growing on the desktop. You have probably noticed an increase in computer viruses and spyware, not to mention spam. Now these different client-side security issues are beginning to merge. How can a network administrator deal with these added security problems? Fortunately, many of the processes we have dealt with earlier in hardening servers can be implemented with some modifications on the desktop. Since the dominant desktop in the world today runs a Windows operating system, we will deal with that exclusively.

Locking down a desktop is similar in many ways to the concept of locking down a server. It is best not to connect it to the network before it is completely patched and the appropriate security software is in place. In many instances, companies have at their disposal software that will create “images” of a desktop computer's configuration and allow you to make copies of it to place on one or more computers in rapid succession or even simultaneously. This is an ideal situation in many respects since the computer can be installed, patched and configured and software can be added (including security software) to a single machine and replicated out to a large group at once, without having to go seat to seat to install and configure it. This scenario can work very well for most of your desktop clients, but there most likely will be situations when other options need to be used. There are methods of locking down a desktop that utilize the built-in functionality of Microsoft's latest desktop client. Windows XP Professional has several tools to allow a desktop computer to function in its business capacity, but not allow an end-user to make unauthorized changes. Group Policy is a feature that can be applied on an individual desktop (via Local Security Policy) or distributed throughout the domain to enforce restrictions. This can allow ongoing maintenance of a computer's security and functionality on the network. You can apply a policy to a person, group or computer and change what they have access to on the network or on their desktop as their job requirements change. Another part of the Group Policy infrastructure is called Software Restriction Policy, which can allow or deny a non-administrator end-user the ability to install any applications not on an approved list or an approved “type” (for example, an executable or .exe, or a software installation script like .msi, .bat or .cmd). There are other parts of Group Policy that apply a particular set of features to the operating system and deny access to all others. An example would be a policy that gives access to Microsoft Word and Excel, but denies access to any program that could be used to change the configuration of the computer and will not allow the user to browse their computer for any documents other than those required by their job description. There is a

comprehensive guide to securing Windows XP Pro on Microsoft's website. The document details various ways to secure the desktop in different situations, such as a Stand-Alone workstation or part of an Active Directory domain, in addition to many sample policies and templates. There are also several books on the subject. One which comes highly recommended from several sources is Osborne/McGraw-Hill's Windows XP Professional Security, by Chris Weber and Gary Bahadur of Foundstone, Inc. It has a comprehensive and concise descriptions and examples of how to use the included features to secure Windows XP.

In addition to locking down the Operating System, you need to install the same type of security software which we looked at for the server. Antivirus software is the most common type of security software you will find installed on the desktop. Just about every product has a set of features that can scan your hard drive on a schedule or manually, scan suspicious activity on your PC as it happens and scan your email as it comes into your Inbox. Once again, it is very important to maintain the virus signature files and the scanning engine. When looking at these packages, be sure that they have a way to track, monitor and report on these configurations from a central location and whether they are updating appropriately.

Once you get past the antivirus software, there is a significant drop off in recognition of what else should be installed. Just like with the server, a firewall is becoming an important part of a client installation. Windows XP comes with one and Service Pack 2 improves on it (it is even turned on by default). There are more robust packages available that can for example, restrict outbound as well as inbound traffic, so keep that in mind when choosing what to use on the desktop.

Another program that is probably not on very many people's list of desktop security software is Host-based Intrusion Detection Software (HIDS). This type of software can be useful on desktops with configurations that are not likely to change frequently to monitor for possible spyware or virus activity. Sometimes firewalls, antivirus and HIDS come in a suite to provide multiple layers of protection.

As has been alluded to previously, spyware and adware together are becoming an increasing security issue on the desktop. Spyware removal programs have emerged to counter the problem. These are programs that check your computer for known applications that can send information about you to third parties and will also check your computer for settings that make it easier for third parties to gain information about you and your activities from your computer. Some examples of spyware removal programs are Lavasoft's Ad-Aware, PepiMK's Spybot Search & Destroy, and Webroot Software's Spy Sweeper. There are even some companies which included this sort of application in their security suites (McAfee, Symantec and Trend Micro are examples). Using spyware detectors on a regular basis provides another layer in the defense of your network. All of these things put together will get you a long way toward securing your desktop environment.

The second phase of securing your network begins with establishing a baseline of normal activity and monitoring and maintaining the products you have installed on a regular basis. Products mentioned previously, like the commercial versions of Tripwire, the various antivirus products and patch management software have reporting and monitoring capabilities. There are also several large software management frameworks like IBM's Tivoli, Unicenter from Computer Associates and Patrol from BMC which can tie a lot of information together and display it in a single interface. These are unfortunately out of the range of most SME's budgets, but they can be an option for some. In addition, the operating systems themselves have monitoring capabilities that many third party software vendors have built upon to allow you to aggregate and monitor log files, send out notifications of abnormal activity and display and print reports or store them in a database for later analysis. With all these elements installed, baselined, and monitored you are another step closer to a stable and secure environment.

Maintaining Security And Stability

There are some other things to consider that are not often thought of when discussing information security. What happens when the unthinkable happens and your systems are compromised and all your data is destroyed? You restore them from a backup, of course. Do you know when your systems were actually compromised? How far back do your backups go? Have you done a test restore recently? What happens if the site where the tapes are located is destroyed? These are all questions that not only point to a policy and process that need to be addressed, but to the implementation of a Business Continuity Plan (BCP). In addition to natural and man-made disasters that can cause loss of data, loss of equipment and worst of all, loss of life, security issues can also cause business to be interrupted to the point of financial disaster. According to Contingency Planning Research, over 50% of companies close after a catastrophic data loss. A good place to get started looking at creating a BCP is the Security Portal at InfoSysSec (http://www.infosyssec.net/infosyssec/buscon1.htm). There you will find many links to resources in BCP to gain an understanding on how they are put together and what should be considered.

Your network, servers and workstations are configured and locked down, you have established baselines and are monitoring them to make sure nothing unusual is taking place and you have a plan to recover when disaster strikes. You've almost attained the goal of: As Secure as is Reasonable. The only thing remaining is to make sure you stay that way. This is done with Policies and Procedures. A policy is, according to the SANS Institute™, "...a document that outlines specific requirements or rules that must be met." Policies generally cover a single topic. Their website contains well over 20 policy templates created by a group of security professionals at a large organization and is a very useful resource. The following referenced series of articles are quite useful in providing information on beginning to write Security Policies, and a directory

with many downloadable templates and resources for their implementation. Creating policies is a very personal project as it involves how things are done at your company and can only be implemented at a level you have control over, unless you can convince your superiors of the need for the policy you've created. It is important, however, to create them, write them down and attempt to gain administrative approval for them. Without a written policy, there is an opportunity for exceptions to creep in that cause the security of your network to become lax and ultimately be compromised. Even with a written policy, there is still a chance that the secure network you've built will be exposed. Procedures need to be in place to carry out the policies that have been created. These are the actual detailed instructions to implement the requirements of the policies. For each policy that affects a department or individual, a written set of procedures should be put in place so that there is a path for people to follow. This does not mean that there is no room for flexibility, but it does mean that casual disregard for the policies are less likely to happen and breaches in security are less likely to occur.

In the preceding pages, we have covered the process of creating a secure and stable network for a small to medium size enterprise. A series of layers from the perimeter to the desktop were described and discussed as well as a path to monitor, maintain and improve that level of security by creating policies and implementing them with appropriate procedures. In following this exercise, an SME's network security team should find areas where they will be able to enhance their level of security. I believe that the more secure each of us is individually, the more secure we are collectively.

REFERENCES:

Otth, Giuliano. “50 years of Crypto AG – ‘Security for ever” 2002. 14 Dec. 2005 <http://www.crypto.ch/pages/htm/crypto/ceo_letter/ceo_letter_detail.asp?id=677>.

Kiefer, Kimberly B. and Randy V. Sabett. “Am I Liable?” 2004. 17 Dec. 2004 <http://www.intek.net/Secure/White/121302404am_i_liable.htm>.

Paul, Brooke. “Building an In-Depth Defense” 9 Jul. 2001. 17 Dec. 2004 <http://www.nwc.com/1214/1214ws1.html>.

[4] The SANS Institute. “Mistakes People Make that Lead to Security Breaches” 23 Oct. 2001. 21 Dec. 2004 <http://www.sans.org/resources/mistakes.php>.

Grey, Terry. “Firewalls: Friend or Foe?” Jan. 2003. 12 Dec. 2004 <http://staff.washington.edu/gray/papers/fff-final.htm>.

CERT Coordination Center. “The CERT® Coordination Center FAQ.” 26 Feb. 2004. 21 Dec. 2004 <http://www.cert.org/faq/cert_faq.html#A2>.

CERT Coordination Center. CERT Security Improvement Module - Deploying Firewalls. 20 Apr. 2001. 21 Dec. 2004 <http://www.cert.org/security-improvement/modules/m08.html>.

Naidu, Krishni. “Cisco Checklist.” The SANS Institute. 2001. 14 Dec. 2004 <http://www.sans.org/SCORE/checklists/CiscoChecklist.doc>.

McKeag, Louise. “Building a security DMZ.” Techworld 04 Feb. 2004. 15 Dec. 2004 <http://www.techworld.com/security/features/index.cfm?fuseaction=displayfeatures&featureid=322&page=1&pagepos=7>

Kelly, Teresa. “Security Policy Harmonization in Extranet Connection Projects.“ 23 Nov. 2002. 12 Dec. 2004 <http://www.giac.org/practical/GSEC/Teresa_Kelly_GSEC.pdf>.

Microsoft Corporation. “Securing Windows 2000.” 2003. 13 Dec. 2004 <http://www.microsoft.com/technet/security/prodtech/win2000/secwin2k/default.mspx>.

Microsoft Corporation. “Microsoft Security Content Overview.” 2003. 20 Dec. 2004 <http://www.microsoft.com/technet/security/bestprac/overview.mspx>.

[13] Tripwire Project. Home page. 21 Dec. 2004 <http://sourceforge.net/projects/tripwire/>.

netfilter Project. FAQ page. 2004. 12.Dec. 2004 <http://www.netfilter.org/documentation/index.html>.

Fontana, John. “How to handle patch management.” NetworkWorldFusion. 01 Dec. 2003. 14 Dec. 2004 <http://www.nwfusion.com/research/2003/1201howtopatch.html>.

Greek, Dinah. “Huge increase in virus-infected spam.” VNU Network. 17 Aug. 2004. 14 Dec. 2004 <http://www.vnunet.com/news/1157397>.

Microsoft Corporation. “Windows XP Security Guide, v2.” 25 Aug. 2004. 18 Dec. 2004 <http://go.microsoft.com/fwlink/?linkid=14840>.

Contingency Planning and Research. “The Cost of Downtime.” 1996. 19 Dec. 2004 < http://www.contingencyplanningresearch.com/codgraph.pdf >.

The SANS Institute. The SANS Security Policy Project. 2004. 10 Dec. 2004 <http://www.sans.org/resources/policies/>.

van der Walt, Charl. “Introduction to Security Policies.” 27 Aug. 2001. 19 Dec. 2004 <http://www.securityfocus.com/infocus/1193>.

Information Security Policy World Home page. 2004. 13 Dec. 2004 <http://www.information-security-policies-and-standards.com/>.

ADDITIONAL RESOURCES:

Linux Server Hardening:
http://www.linux-sec.net/Harden/howto.gwif.html – An excellent extended list of links for hardening various different Linux distributions as well as other operating systems.

http://www.securityfocus.com/infocus/1539 – An article targeted at hardening the Linux kernel

http://www.freefire.org/lib/hardening.en.php3 – Another list of links to articles on Linux/Unix hardening

http://www.linuxsecurity.com/component/option,com_weblinks/catid,155/Itemid,134/ - A large number of HOWTOs and FAQs on securing Linux and services running on Linux

http://www-106.ibm.com/developerworks/linux/library/l-seclnx1.html
http://www-106.ibm.com/developerworks/library/l-seclnx2.html - An excellent pair of articles on security principles and how they apply to securing Linux

http://www.governmentsecurity.org/forum/index.php?s=821b1a4851f0db234699061f5602f15e&showtopic=1695&pid=100904 – Good article on locking down a Redhat 9.0 server

Microsoft Security pages:
http://www.microsoft.com/technet/security/default.aspx
http://www.microsoft.com/security/default.mspx – The first two places to search for the latest information on securing Windows and other Microsoft products from Microsoft's web site

http://www.microsoft.com/technet/Security/topics/issues/w2kccscg/default.mspx - A thorough walk through of the hardening process of Windows 2000

http://searchwindowssecurity.techtarget.com/bestWebLinks/0,289521,sid45_tax297381,00.html – A directory of security related links

Network:
http://www.secinf.net/misc/The_IT_Security_Cookbook/The_IT_Security_Cookbook__Securing_LANWAN_Networks_.html - Excellent “recipe” for securing a

LAN/WAN

Last Updated: May 30th, 2017

Upcoming Training

SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
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 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
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
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 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
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
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 Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event