Global Information Assurance Certification Paper

Topic: Taking over the reins - Replacing another Administrator

Name: Justin Stuart-Young

Version 2.2

August 21st, 2002

Introduction

At some point in our careers as IT professionals, we may be hired into a situation where we are asked to take over the duties of someone else. Incoming administrators face a unique set of challenges, as they are entering into an environment that is not of their making and hence uncharted territory. Put simply, it is impossible for an administrator to be effective in any respect if he does not know the network for which he is responsible. This paper details the challenges faced by me when I accepted the job of systems administrator in a Caribbean branch office of a very large, global firm. It covers the initial processes of learning the setup of the current network, pinpointing weaknesses, and developing / implementing the appropriate resolutions to these weaknesses.

Step1: Evaluating The Current Setup

Shortly after joining the firm, the arduous task of becoming familiar with the system began. I felt the best way to begin was by sitting down with the two other I.T. staff that were in the office. While their role in the firm was more as I.T. Consultants for external client services, they had good working knowledge of the network and were able to answer some of my more technical questions. I soon learned that this branch of forty persons was part of a wide area network (WAN) consisting of hundreds of other offices around the globe – some branches as small as 10 persons, while others were over a thousand. The very nature of the firm's business requires most of the staff to travel to clients. Consequently, the bulk of the computers in use were laptops. Laptops, though convenient and portable, represent a physical security risk – especially where hardware theft is concerned. Further discussions with the Consultants highlighted important points that will be discussed in detail shortly.

A tour of the facility was also on the agenda. This was necessary to become familiar with the physical layout of the network. Physical threats such as theft or unauthorised access can be some of the most devastating types of attacks – often because it is written off as the least likely form of attack. The office was basically split into three sections, the largest of which was the cubicle area that accounted for over half the network connections. The other two sections were for Managers and Partners and the I.T. section. The layout itself was fairly basic, with the cubicle area wiring leading back to a single 24-port 10/100 hub, which was then uplinked to a 12-port hub upstairs for Management, and another 24-port hub that covered the I.T. department and server room. It was clear to me that the original design of the building did not include a room specifically made to house servers. The door to the room was fairly decorative and would seem to put up limited resistance to an attacker – a serious concern for me. The server room itself consisted of 3 servers. Each was a dual processor machine, all running Microsoft Windows NT 4.0. One served as the Primary Domain Controller (PDC), the second as a Backup Domain Controller (BDC), and the third as stand alone server running Lotus Domino (more on this later.) Physical console access to the servers is an easy way to circumvent any protection set up on the network shares themselves. It is a direct means of stealing and / or compromising server data, especially when there are no console restrictions in place (e.g. the administrator account is left logged in on the server

screen.) The server room was also home to the office's connection to the outside world, and the rest of the firm. This link is facilitated by a CSU/DSU connected to a Cisco 2610 router. External network links of any kind are always a potential entry point for those looking to compromise the system, and represent a risk factor that cannot be ignored. Physical access to the router itself poses a serious possible network compromise. With physical console access, it is possible to reset most Cisco routers to the point where new passwords can be set (Cisco).

Before long, the roles of the three servers became more apparent. Besides authentication, the PDC was the file and printer server for the network. Each user had a personal folder off of a 'Users' share in which they stored their word processor files and spreadsheets. Other shares present on the server were ones for general shared files (timesheets, expense reports, etc.) and client accounting information (billing forms, financial statements and cash receipts.) The general shared files, while available to everyone, are not intended to be modified. The client accounting information is a bit more privileged and very few people actually need to access to it. Improperly modifying either sets of files could, at the very least, greatly inconvenience the users. At the worst, private client information could be obtained and used for more sinister purposes. The PDC was also the printserver for the three high volume laserjet printers – each serving one of the three sections of the office. The BDC hosted the application used to handle the office's internal accounting. This had various shares relating to this application. The data in these shares is very privileged, as they contain bank account and billing information for the firm. The abovementioned shares had little, if any, permissions in place – leaving the data potentially open to prying eyes. The third server was dedicated to running Lotus Domino. Now, every large firm must have a way of dealing with internal and external communication, and Lotus Domino / Lotus Notes was the solution of choice. To draw a parallel to a more popular product, Lotus Domino / Notes is similar to Microsoft Exchange / Outlook. Both are used primarily for messaging (email) and calendaring within an organization and are designed upon a server / client architecture – Exchange / Domino being the servers and Outlook / Notes the clients. Email clients are one of the prime avenues of entry for malicious code (viruses, Trojans, worms.) Special care needs to be taken to sure up defences in these areas. Domino, however, played a more integral role in the organization than simply a calendaring and email server. Domino can also serve as an application server, for applications written in its native LoutsScript. There were several custom applications written for our staff to allow them to perform their client work. These applications are in heavy use on a daily basis, making the health and security of the Domino server a priority. Each of the servers was equipped with a DDS-3 24GB tape drive for backup purposes. With all this valuable data stored on the servers, a thorough backup plan is necessary should the worst-case scenario happen – whether this be theft, hardware failure, or data compromise.

As mentioned earlier, this office was part of a global WAN. As such, it is worth speaking a bit about our place in this global network structure. Firstly, it should be noted that matters pertaining to the global connections are planned by the firm's global I.T. group and executed by the local I.T. departments – so the local administrators are reduced to 'following orders' in such cases. Our office in the Caribbean is part of the Americas

theatre of operations. The centre of operations for this is the datacentre in Tampa, Florida. The office had purchased a 128k Internet link from a local ISP, and this was to be used for the virtual private network (VPN) link back to the Tampa office. The VPN tunnel created between our router and the router in Tampa is used for all traffic destined outside the local LAN – this includes all Internet traffic, Lotus Notes traffic, DNS traffic, etc. The majority of this traffic is Lotus Notes related. The local Domino server replicates with a Domino hub server in Tampa – which serves all the Caribbean countries. The information replicating includes such things as the email (both internal and external), the Domino Directory (a name and address book database for staff in other offices) and various shared databases. The content of these databases varies greatly, some are discussion forums where various groups within the firm can share ideas, and others are client information or documentation of firm standards. Among these standards are the Global I.T. standards and policies which we will discuss in more detail in the sections to follow.

The laptops in use by the majority of the staff varied in terms of speed, but all were equipped to meet the minimum system requirements for running Microsoft Windows 2000 Professional. Much as with the WAN connection, the operating system was a global firm standard – with Windows 2000 being the OS of choice since 2001. In fact, a global firm standardisation was in place for the base install of the OS. This base install, dubbed 'ePC' internally, included Windows 2000 Pro SP1, Office 2000 SP1, and miscellaneous other utilities for which the firm had purchased volume licenses (WinZip, Acrobat Reader, McAfee virus scan). It is also my understanding that the base install had been pre-configured to reduce some of the possible vulnerabilities to the 'out-of-box' Windows 2000 install (removing Guest account, administrative shares, etc.) The ePC install was distributed to the offices as a bootable CD with a custom installation script. Then, each office would typically install the base setup and then customise it to their specific region and office environment, and hardware. Once the final install is complete, a system image is made and stored on a server for use in rolling out future installs as required. Applications are often a gateway for attacks, as various vulnerabilities are always being discovered. Internet Explorer 5 and its companion Outlook Express are some of the prime culprits. With its ActiveX and Java vulnerabilities, Internet Explorer is the target of many different forms of attack (PivX). While most undesirable sites are filtered, there is always the chance that an unsuspecting user might download an infected file off the Internet. Thankfully, Outlook Express was in very limited use on the LAN. The amount of viruses written to exploit its attachment and script execution vulnerabilities is frightening (SecurityFocus). It will be a goal of mine to eradicate all usage of this program from the network.

As time went on, I began to feel more and more confident in my understanding the network and connections to it. Then, of course, the more I became acquainted with the network, the more I saw its flaws and dirty little secrets. While the overall configuration seemed sound, the network was the victim of an Administrator that was perhaps lacking knowledge in certain respects, or had become complacent and failed to place system security high enough on the priority list. At any rate, it had all become my job now, and with my reputation on the line I was not about to let things stay in the state I

found them. Now, we take a look at process of further identifying and rectifying the flaws in the firm's I.T. systems.

Step 2: Improving the situation…

Larger firms, especially those with a global presence, must be well organised and efficient in order be successful. One of the benefits of working with a large firm is having access to well-established standards and policies. These policies were readily available in the form of a Lotus Notes database, and shared on the Notes hub servers for all to access. Of course, one can have access to all the policies and recommendations in the world, but unless they are implemented it is quite pointless. Unfortunately, it seems that the previous administrator had not been taking advantage of resources at hand. It is worth noting that some of the policies were designed for much larger offices, with much larger budgets. And indeed, we will see that budget constraints will play a part in the decision making process.

Let us first discuss the issue of physical security with regards to the firm's computer assets. In the tour of the facility, we learned that the servers and Internet connection (router and CSU/DSU) were located in the same room. This room was located in the I.T. section of the building, away from staff, and the regular path of any visitors to the building. The door to this room is locked at all times and there are two keys available. One is in my care at all times, and the other is stored in a key vault in case of emergencies. I had expressed my concern with management over the quality of the door and lock, which seemed less than secure if someone were determined to break in. While my complaint was noted, little could be done at the time to facilitate a more secure door due to cost constraints. Nevertheless, as 'defence in depth' teaches, a more secure door would not have meant the end of the exercise as the equipment inside still needs to be physically secure on their own.(Fraser) The servers themselves were hooked up to KVM switch, and once at the console, I had open access to the OS. There were no screensaver passwords in place to deter or even slow someone with unauthorised physical access. I enabled the screensaver password for 5 minutes, and also set the KVM password to 45 minutes. The logic behind this being that after extended periods of inactivity, say after hours when a break in is more likely, there would be two passwords to contend with. The servers themselves were tower servers and could easily be removed from the office. Other towers and desktops in the office were secured with locking steel cables, but the servers were not. Upon my request, steel loops were bolted to the wall behind the servers and locked steel braided cables were used to hinder the removal of the machines from the room. The keys for the server cases were removed from their resting place (sitting in the locks) and secured with all the other relevant keys. The servers were secured with the help of the SANS recommendations in Phase 1 of the 'Windows NT Security' module – preventing floppy/cdrom boot access by setting a BIOS password and changing the default boot options. This would prevent and attacker from simply booting of a diskette to DOS or some other OS to circumvent the password protection.

We spoke earlier about the risk involved in having physical access to the router. Disabling console access to the router is not an option, and the passwords that do exist are not even given to me. All router passwords are created and held by the Tampa office as the router administration ultimately lies with them. The routers were constantly monitored and maintained from the Tampa office using Ciscoworks management software. The 24-hour staff monitoring the network would notice any configuration changes or network outages. Any suspicious activity would prompt them to notify the office and disconnect the secure VPN tunnel to prevent any compromise of the internal network.

Physically securing access to the firm's laptops was one of the more challenging tasks that needed attention. It became a perfect example of how policies were in place but not enforced. All of the laptops were issued with braided steel, combination laptop locks, but a walkthrough of the office showed that few of them were actually in use. Fortunately, this was taken care of by a simple email reminder, followed by some random spot checks. But theft can happen at any number of places while the laptop is not secured with the lock. The first line of defence in such a case would be the BIOS password. Much like the servers, booting off the floppy or cdrom drive were disabled in the BIOS to prevent circumvention of OS password protection. BIOS passwords were also used to lock the hard drive, in the event that someone attempted to boot one up in another machine. With the first lines of defence in place, we must now look at the security risks once the OS itself is booted up. The Windows 2000 laptops all require the user's password to logon initially. The users are then responsible for 'locking' their computer when they are left unattended (Ctrl-Alt-Del, Lock Computer) but a password-protected screensaver is put in place to help secure the laptop should they forget. This is important because if changes to client data were made as the logged in user, it would be very difficult to track, hence compromising the integrity of the data. As staff members were often assigned to several clients at any given time, there are databases with other client information also present. Due to the confidentiality agreements we use, allowing such information to be stolen is a serious liability. With the advent of CDRW drives in laptops, it had become ridiculously easy to copy large amounts of data off a machine. Fortunately, Lotus Notes provides a means to protect databases from such situations. The firm security policies suggest that the Lotus Notes local database encryption be turned on for all client files – a simple ticking of a checkbox in the database properties. This process encrypts the database with the user's Lotus Notes ID file – after which the database may only be opened if the user's ID file is present and the correct password entered (more on Notes authentication later). Again, this was a policy that was not enforced, and one that few staff even knew existed. The second part of that same policy dealt with the removal of unneeded client data from laptops. Once a client had been 'wrapped up' for that year, all data for that client databases should be deleted locally and all other client data (MS Word / Excel files) should only reside on the server. The Domino server copy of the database is archived at that point in case the client database needs to be revisited. Now, the IT Global Standards also recommend using a 3rd party disk encryption solution to provide a further layer of protection. Their software of choice was Safeguard Easy, but it was not covered under the company's software licensing. After investigating the licensing costs for the office and putting the proposal to management it was decided that cost was too

significant to be justified at this time. With the physical security of the systems looking tighter, it became time to put the network itself under the microscope.

The Internet connection is normally the high point of concern when looking at network threats. Ironically, this would turn out to be one of the areas I had to worry about least because of the configuration of the network. Though we had a direct Internet connection, no traffic could come onto the LAN directly from an outside IP. The router ACLs and configuration were set to allow traffic to cross only over the secure tunnel created between our router and the Tampa office router. This tunnel was 3DES encrypted and our router was equipped with a Cisco AIM encryption module to help offload some of the encryption processing from the router CPU. The tunnel carried all protocol traffic, including Lotus Notes, HTTP, etc. So, in fact, there was no need for a local firewall as all Internet related traffic actually came and went via the Internet connection in Tampa – which was heavily firewalled, logged, and content filtered. This was an efficient way of doing things from both an administrative and cost perspective, as small offices didn't have to install and maintain other servers for firewalls and intrusion detection systems. Nevertheless, there were still areas of concern with regards to Internet related threats. The Partners and some Managers had their dial-up accounts to a local ISP set up on their laptops. They were using this to be able to check their home email accounts while at work. This was potentially dangerous as being connected to the LAN and dial-up simultaneously could allow an attacker to circumvent the firewalled connection in Tampa by using the dial-up connection as the path into the LAN. One way of reducing this risk is by installing some form of personal firewall to protect the dial-up connection. Not only is this a further expense, but personal firewalls are not nearly as safe as their more expensive brothers, and firm policy clearly states that dial-up connections should not be allowed anywhere on the network. Still, we have to strike a balance between security of the site and the needs of Management. The email clients could not be configured to check the POP email servers over WAN connection because Tampa had it blocked for security reasons. Luckily the ISP the staff was using offered web-based access to email accounts. This was my preferred solution because it could be done over the WAN connection, and the web based email system isn't as prone to viruses that exploit Microsoft Outlook Express' address book and code execution vulnerabilities. One other concern for me was the wide use of file sharing applications. While users sign agreements stating that they are not allowed to install any unauthorised software, there are always those who forget or ignore that clause. Global IT decided to deal with the problem by rate limiting the known ports for such applications (because blocking the ports would only cause the applications to choose another random port.) But even with rate limiting, there are so many viruses on these file sharing networks I wanted to be able to regulate the usage on my network (Loney) . Most of these applications attempt to contact their makers AD server to display banners (Kazaa.com, etc.) By using the protocol analyser Observer (http://www.networkinstruments.com/html/products.html) to monitor port 80 traffic, I could periodically sort the list of sites and look to see which machine had contacted a suspicious site. There were several other options for WAN connectivity other than the VPN option. Using a leased line connection back to Tampa would have provided the same functionality, without ever having to expose the office to the Internet (our VPN required the use of a public IP address.) Similarly, another option would have been using

a frame relay network connection – a private ISP network completely separate from the Internet itself. Weighing both of these options against the current solution showed them far too expensive in comparison.

As Lotus Domino / Notes plays such an integral part in the firm's business, it is worth taking a closer look at its security features. Earlier on we discussed that the firm used a custom designed Lotus application for its client work. The firm's work is done on a yearly basis, so each client has a database for each year. The database application exists on the Domino server as well as on the local laptops of staff assigned to that client. The benefit of this is that several staff members can work on different sections of the database application separately on their respective laptops, and then replicate the changes with the server copy when they return to the office. Domino handles this database replication and deals with any replication conflicts that may arise. The application databases, like any other Notes databases, have access control lists (ACLs) to set various levels of access. The applications use the ACL to determine what the user can and can't do within it. For example, if a user is given Manager access he can access, edit and delete any information within the application. Editors can enter, modify, and mark information for deletion – though the actual deletion can only be done by the manager. When I first began inspecting the database ACLs I noticed that they were not done with any kind of consistency. It is recommended practise to avoid placing individual users in ACLs, only groups. Doing so makes it easier to modify permissions if need be. Say, for example, one manager leaves and another takes over his clients, all of the client databases in question would have to have their individual ACLs changed – removing the old manager and adding the new one. If there were group names in the ACL then simply removing the old manager from the group and adding the new one would effect the change on all the databases with the group. Organising and streamlining the Notes ACLs was one of the first major network revisions I made. It was as simple as meeting with the Managers to find out who needed certain levels of access to client files, and I created the groups accordingly. Groups were created according to level of employment within the firm and the client databases were updated accordingly using the principle of least privilege. Notes itself has many security features that I had to learn to use. Notes utilises a public key infrastructure (PKI) for authentication. The key pair is created when the user's Notes ID is created. The public key is placed in the Domino Directory and the private key is within the ID. The ID also contains a certificate for the Notes domain to which it belongs. Unlocking the ID with the user's password sends the private key and certificate information to the server to authenticate the session. The session traffic between the client and the server can may encrypted if it is enabled on the client. It was not enabled on the majority of the clients and I made sure that the remainder of them had this feature turned on. When setting the Notes ID password, the administrator can require a password based on complexity, rather than just password length. I chose to set the minimum complexity to level 8, which is characterised as 'strong'. (Nielsen, et al)

After the Domino server, the next most important network resources were the Windows NT file and print servers. I began my analysis with one of my favourite networking tools, Hyena (http://www.systemtools.com/). This tool allowed me to quickly determine what shares were present and the permissions they were assigned. I

used this to create a logical network diagram showing how the various resources were set up and who was given access. Armed with this diagram I set up another meeting with one of the managers to discuss what the shares were being used for, the sensitivity of the data in the shares, and who needed to access them. As I suspected, far too many people had more permissions than they required. The lack of structure seen in the ACLs of the Domino server was also apparent there. There were no user groups in place, people were added directly into share and file permissions. In fact, I came across several accounts from former employees that were still present on the system and still listed in permissions. I created all the appropriate groups, doing my best to mirror the groups I created on the Domino server. Using the information gathered from my meetings, I simply adjusted the file security and share permissions using the least privilege principle. These shares consisted of a mix of personal files, client related files, human resources files, accounting related files, etc. While the permissions and security was in place, it is always useful to be able to hold users accountable for actions on files. I chose to enable auditing of the access of some of these shares, especially the more sensitive data, such as H.R, accounting, and client data. With auditing enabled it became essential to review logs often for any suspicious activity. Fortunately, the aforementioned networking tool, Hyena, also made it easy to review the various logs without having to be at the server console.

While the Global IT policy for password length and expiration were being enforced (minimum 8 characters, 3month expiry) the quality of the passwords were of more concern to me. I enabled Microsoft's password filter (passfilt.dll) as a step in the right direction – though I would research and choose a more customisable solution for the future. Password strength would have been much less effective had I not also disabled Lanman authentication – which can effectively reduce the complexity of cracking passwords using a divide and conquer principle. Following the SANS recommendation, I also enabled SYSKEY to encrypt the SAM password stores. Given the relatively inexpensive power offered by today's machines, password crackers are now more powerful than ever. Only by enforcing the complexity of the password can we decrease the ease with which the attackers can crack them.

Security is an ongoing task, and keeping up to date is essential. The NT servers were using service pack 4 (SP4) at the time I joined the firm. The latest release from Microsoft at the time was SP6a. This told me that there was a lot to be done to bring the machines up to speed. Of course, patching up NT is often a dangerous task as there have been may instances of patches breaking each other, cause program errors and opening up security holes. I decided to consult with one of the Global IT contacts on this before I proceeded. They use server labs to test patches and service packs before they are rolled out to the productions servers, and are therefore well aware of potential conflicts. They were able to send me instructions on updating the servers to the most current, stable state. They also made use of a program called Patchlink (http://www.patchlink.com/) , which aids in safe deployment of patches and fixes any known holes created by patches.

The antivirus procedures in place were another area in need of review. There was a mix of Norton Antivirus and McAfee antivirus on the computers in the office – for what

reason, I do not know. Once a month the administrator would download the virus definition updates, place them on a shared folder on the server, and go to each machine and manually perform the update. The first thing I did was to consult the firm standard on antivirus software. This happened to be McAfee VirusScan. I made sure that all the Norton AV scanners were replaced with McAfee so we'd have a standard means of dealing with the task. Next, I read up on the AutoUpdate feature of the application and how it operated. Because of our limited bandwidth, it was impractical to have each laptop updated the definitions individually from the Internet. The second option allowed the update file to be placed in a network share and have the clients all use the same file. This was a much more elegant solution, and was the one I opted for. Lastly, updates were automatically scheduled to happen once a week to ensure the latest virus definition file was being used – it was just a simple matter of downloading the update file once a week and putting it in the network share. The corporate licensing also covered McAfee Netshield and Groupshield. Netshield is used to protect the NT servers and Groupshield is NAI's antivirus package for Lotus Domino. It provides the ability to filter out viruses before the user even sees it. This greatly reduces the chances of the user executing the attachment if they are unsure of the contents.

A look back…

Working in an unfamiliar environment is always a challenge in any profession. The key to not getting lost is taking the 'bull by the horns', so to speak. As network administrators it is essential that we take the initiative to learn and take control of the network as quickly and thoroughly as possible. In my situation, the analysis and changes discussed in this paper were executed and completed within the first week of my employment. I believe that the efficiency of my work had much to do with the concepts learned in the SANS security essentials course. Picking out the major risk areas first was key, but could only be done after becoming more familiar with the systems in place. I chose to put the risk areas into three categories: physical security risks, external network risks, and internal network risks.

Before I began enforcing the physical security policies of the firm I believe that there was a significant risk of physical attacks and / or theft. Someone breaking into the office would have been faced with a candy store of goodies. For those wishing to steal equipment for resale, there would have found unlocked laptops, ripe for the picking, not to mention $5000+ servers. For others wishing to steal or compromise confidential information, they would have been pleasantly surprised by unlimited server console access, or hard drives that could be removed and attacked at their leisure. After taking steps to sure up the physical side of things, attackers would be faced with several challenges they would have to overcome before getting their hands on the data itself. Having said that, there still remain areas that can be improved. There is no electronic security system or building guard present after hours. Either of these would provide a good deterrent to would –be thieves.

External network threats, normally the bane of network administrators, actually represented a more controlled situation when compared to the other threats discussed in

this paper. This is primarily thanks to the research and manpower behind the protection of the external network connections by the Global IT team. Still, that is no excuse for doing your homework and understanding the security that is actually in place. As the local administrator, it is my responsibility to look out for the threats of which the Global IT team may not be aware. In this case I found the dial-up connection being used could undo the excellent external network protection in place. Incoming viruses via email or the Web will always be a problem. It is only by keeping the users vigilant and the antivirus up to date that the problem may be curtailed. Part of this is educating the users to make smart decisions. Future plans will include informative emails on how to deal with suspicious emails as well as actively informing them of virus outbreaks. For those users that violate their users agreements, there will be a straightforward procedure whereby I would issue a notice to them of the infraction. If the notice were ignored then a formal notification would be made to the relevant supervisor.

Sometimes the enemy within is the easiest to forget about. Internal network threats are serious business as it only takes one disgruntled employee or an attacker on the inside to destroy or compromise data. The internal controls in place were simplistic at best. By arranging users in groups and assigning their permissions as such, it not only reduces the chances that people are getting more privileges than necessary, but it makes the organisation more logical for those that may have to deal with the network in the future. If an incident were to occur, audit logs can go quite a way towards tracking down its source. Still, analysing logs can be a tedious task or one that slips by the wayside when things get hectic. I decided to try out a demo of a program called Enterprise Event Log Manager (http://www.tntsoftware.com/) to help me manage this. ELM allows the administrator to monitor event logs remotely and configure various alerts for various types of events. For instance, a logon failure could be set to cause a pop up window on my workstation, or an audible alert on the monitoring machine. I found this kind of ability very useful, as I am alerted of the events in real time, not after when I have the chance to check the logs. Unfortunately such functionality comes at a hefty price, and at the time it was not an expense we could afford. Still, I will put in a request which will hopefully make its way into the next I.T. budget.

I considered myself lucky to have access to a wealth of knowledge in the form of the guidance of the Global IT group and the standards and policies they developed. It really is a shame when administrators have such resources at their disposal and fail to use them. They were especially beneficial in helping be to understand the kind of thought and planning that large enterprises must do to be secure and successful and definitely played a part in my ongoing education in the field. It should be noted that all the observations, analyses, suggestions and solutions were documented in one way or another. After having had to learn the network and its workings the hard way, I would be hypocritical if I did not, in some way, make it easier for another administrator to 'take over the reins' if the situation arose.

References

(1)Cisco. "Password Recovery Procedure."
http://www.cisco.com/warp/public/474/pswdrec_2600.shtml#proc

(2)Loney, Matt. "New Worm Eats Into Kazaa." ZDNet UK. 8 July 2002
http://zdnet.com.com/2100-1105-942033.html

(3) Nielsen, Dahm, Lüscher, Yamamoto, Collins, Denholm, Kumar, Softley. Lotus Notes and Domino R5.0 Security Infrastructure Revealed. 6 May 1999.
http://www.redbooks.ibm.com/redbooks/SG245341.html

(4) Brenton, Chris. Mastering Network Security. Alameda: Sybex Inc, 1999.

(5)Northcutt, Stephen. "Defence in Depth." SANS GSEC Training Material. v 1.11. 2 January 2002. page 3.

(6) PivX. "IE security holes". http://www.pivx.com/larholm/unpatched/

(7) SecurityFocus Online. "Vulnerabilities by Vendor: Microsoft ,Title: Outlook Express". http://online.securityfocus.com/cgi-bin/sfonline/vulns.pl

(8) Microsoft. "Windows NT 4.0 Domain Controller Configuration Checklist"
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/dccklst.asp

(9)Fraser, B. "Site Security Handbook". September 1997.
http://www.ietf.org/rfc/rfc2196.txt?number=2196 . Page 29.

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
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 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