GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

CREATING SECURITY IN A SHARED WORK ENVIRONMENT

Nathan Darling
GSEC Practical Assignment - Version 1.4b Case Study
January 22, 2004

Abstract

Our company began 2003 with an appalling lack of physical security in our shared office spaces. We were purchased by what became our parent company and they addressed this lack of security upon their first inspection. The following is an account of the steps taken to lockdown and secure the office spaces in our building, paying special attention to those areas that are shared by one or more organizations. This paper will provide a detailed account of the steps taken to enhance security in three physical locations, as well as steps taken to increase security on the network as a whole. Each section begins with a simple description of the modest security that we had in place to begin with, and ends with the security steps implemented and the flaws that still exist within the system.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Beginning

Let's be honest. In the beginning we did not feel much need for security of any kind. I mean, we understood the need for Disaster Recovery Procedures, but as far as being hacked, or compromised, well, we were a small company and felt like we were beneath the radar. Even if someone did get control of our systems, what could they do with it, other than erase it, or steal it? If they erased it, we could back it up, and if they stole it, most of them would not know what to do with it. Our security model during this time could have best been described as nonexistent. We simply felt that network security was beyond our needs.

> It is easy to claim that one does not need to worry about computer security, if one does not have anything to hide. By this is often meant that if you are not doing anything questionable and/or the data you have on a computer is not sensitive or valuable, you would not need to 'waste your energy' on 'being paranoid'… However, over the years I have come to believe that *all* arguments which are based on the assumption that the innocent and honest do not need any formal or technical protection are plain wrong. (Addams-Moring)

The push for increased security began for us when our new parent company came and audited our security procedures. This was really the point at which we first understood that there was a problem. The research group consisted of the Senior Network Administrator from our parent company; the Senior Network Administrator from our company; and myself, the local Network Administrator. We knew the audit was coming, and we took what we felt were appropriate steps to make sure the network was secure before they arrived.

The senior network administrator for our parent organization purchased Anti-Virus software for us. I implemented this AV Software by installing it on one central server and configuring it to push out its installation to the other workstations. It is configured to automatically download and push out the latest updates, and to run regularly scheduled scans on every server and workstation on the network. I did it this way because I didn't want to have to check each and every workstation periodically to make sure the scans were running, when I can just monitor them all from a single server. Also in the event we did get a virus I wanted one central machine from which I could pinpoint where the virus had been found. The quicker you can isolate a threat, the less damage it can do.

We issued a written company policy that clearly outlined acceptable use of the internet, as well as other procedural items. All employees were required to read and sign it. Having a policy in writing helps employees know what is expected of them, and what they can expect. It also helps management know how to deal with specific issues. In layman's terms, a written policy gets us all on the same page.
One notable passage in the company policy prohibited wireless networking

© SANS Institute 2000 - 2005 Author retains full rights.

devices, until such time as proper security exists to provide protection. "The combination of uncontrolled broadcast areas and use of a weak encryption standard creates an environment in which unauthorized access to systems and information can occur." (www.bankinfosecurity.com)

We hired a software developer who is certified in GIAC Security Essentials, and he set up an Intrusion Detection System (IDS) running a packet sniffing program that allows us to view the traffic moving across our network.

We also hired an individual to document our various policies and procedures, as well as day to day operations. In short, our "project manager" wrote the corporate guidebook. Thus providing accountability; and checklists for certain complicated procedures.

Armed with what we felt were suitable protections for the majority of our network, we faced what we thought would be a pleasant and painless audit. In retrospect it is surprising how much we overlooked. The audit uncovered a number of simple things such as server racks and phone closets that were not locked. The notorious hacker Kevin Mitnick "warned against keeping certain rooms unlocked when not in use, such as conference rooms with data jacks, computer training rooms, and telephone and cable closets." (Cole, pgs 494-495) We had not been heeding his warning. A number of simple network security procedures were implemented on the spot, such as keeping the telephone and cable closet locked. There were three distinct areas that required in-depth attention.

1 Our Shared Server Room – One Server Room shared by all the various companies in the building. As you will see, this sharing allows for a great many potential dangers, from intruders as well as from simple accidents.

2 Our Front Lobby –The only area in our office with a network jack that is easily accessible to the public. Our most insecure space, and a prime target for hackers.

3 Our Conference Room – This room is not shared with the other offices in the building like the previous two rooms are. However we do share this room with a restricted group of individuals. Individuals who we do not necessarily wish to have access to our network.

Shared Server Room

Before Security Enhancement

The building has 3 floors, and currently is home to 4 separate and unique businesses, with room for one more. There is one Server Room, in the basement that all the companies in the building share. It is behind a magnetically locked door, and only representatives trusted by the owners or general managers of each of the individual companies have access to this room. In our organization, there are 7 individuals who have keys that allow

© SANS Institute 2000 - 2005 Author retains full rights.

access: The Network Administrator, the Database Administrator, 3 of our Software Developers, our Facilities Manager, and the organization's local VP. Although it is easy to see why any of the aforementioned individuals would require access., if you assume the other organizations in our building are as liberal in their permissions, we may well have 7 times 4, or up to 28 individuals with access. The servers are mostly contained within cabinets which do not possess locks. In fact many of them do not possess front or side panels, and are simply open. There is one particularly good example of potential disaster in the form of a router that is dangling completely outside the cabinet. The only thing holding it in place is its own network cables connected to a switch that provides this company's access to the internet. It would be far too simple to trip and fall and rip the router right out of its connection, taking the company's external network connectivity down. On a more malicious note it would be exceedingly simple to disconnect all the network cables leading in to the switch, or to connect one of our own laptops directly to the their switch and wreak havoc on their network.

In the event that something did go wrong for our servers, we had one machine that had a DLT tape drive. We were using Windows 2000's built in backup software to create backups of our systems. One limitation of this system was that the DLT drive was built into our primary File Server. The one server that was already handling the heaviest load was the only one we had that could run backups. Certainly a good way around this problem would have been to only do backups in the evenings and weekends, when the workload was less, but there was one more problem. The DLT drive was old. Even though we had Type IV cartridges, capable of storing up to 80 GB of data, the tape drive was incapable of cramming more than 40 GB of data on a tape. Our primary server at that time had 120 GB of useful data, so to do a complete weekly backup, required swapping out the tapes 3 times. It took about 8 hours to fill up 1 tape, so in order to do a complete backup required an individual to come in during the weekend on 2 separate occasions at least 8 hours apart. When our database grew even larger a fourth tape became necessary requiring a third trip.

Steps taken to Secure Server Room

In our Server Room, my biggest fear was accidental tampering. So I wanted to concentrate on prevention. As mentioned above there were a great number of unauthorized access points to the various organizations networks…most of them still exist. I was determined to close all of ours. There are enough individuals with access to this room that trying to track down a responsible party if something were to occur would be time consuming. We had purchased a half size Server Rack to hold some of our newer servers. Our first logical step towards securing these servers was to lock up the rack. I took one key, and the other key was locked up in a company safe. Now that our new servers were physically secure, we turned our attention to the legacy servers on which we continue to maintain crucial data. Since they were the wrong shape to fit inside

© SANS Institute 2000 - 2005 Author retains full rights.

the rack, the senior network administrator for our company suggested purchasing a full size rack, and replacing our legacy servers with new rack mount servers. The senior network administrator for our parent organization promptly suggested that the cost to replace our servers would be greater than the cost to have side panels and locking doors installed. So we did it the less expensive way. I had our building facilities personnel equip the cabinets we were using with side panels and locking doors. I obtained the keys to the cabinet doors and along with the keys to the rack, and other keys to be mentioned later, placed them in a safe in our supply closet. The safe can only be opened by our office Facilities Manager, or our Senior Software Developer. A copy of all the keys is also held by me. Instead of upwards of 28 people who have access to our systems, there are now 3.

In addition to protecting the physical environment I wanted to improve our ability to recover from any disaster. Therefore an improvement was needed in our Tape Backup system. Although in retrospect this appears to have been the wrong way to go, we focused our efforts on the Unix Server first, because it did not have any kind of backup schema in place. We determined that the Unix server, which houses our Oracle Database, has strong enough security built into its design. It consists of about 42 disks, mirrored, and the data is striped in such a way that the only conceivable failure is if 1 disk from each mirror set in the exact same position of each mirror set were to fail. As of now our solution to this problem is the high state of redundancy involved in having 2 mirror sets…and in the technical support package we have purchased with the Server's Manufacturer. The chances of two disks, one from each array, each in the same physical slot position, going bad are so low as to be considered of no real concern by our management. I however, remain concerned, and will keep searching for an alternative other than replacing the entire system. (Our finance department already shot down the replacement idea.)

This brings us right back to the Windows Servers. The need to come in and swap out a tape every 8 hours was beyond the scope of what I considered reasonable. My first choice was to purchase an external autoloader DLT tape drive. However the cost on such a unit was not approved by our financial department. Instead the senior network administrator for our parent organization purchased an external AIT drive, a tape backup software package, and a number of AIT tapes. The new software was complicated and did not seem to function properly. I would install the software and back up our critical servers. It would work for about a week, and then it would fail. I would call technical support and they would shrug their shoulders at me across the phone lines. Then they would take me through a number of settings, making sure the server names were set correctly, and the user account I was using was the correct one. Then they would tell me to call back if there were anymore problems. Well calling them back meant waiting on hold again until one of them was free to talk to me, so if it still didn't work I found that the only way I could get it to work again was to uninstall it, and reinstall it all from scratch. Then it would

© SANS Institute 2000 - 2005 Author retains full rights.

work again for a few weeks. Finally after a couple of times of this uninstall-reinstall process, I got a hold of that rare individual at technical support who really knew about her product. She talked me through a number of steps including granting; Domain Administrator, Local Administrator, and Backup Operator status to the Tape Backup account; inserting specific lines in the Environment Variables on the machine running the backup; and installing the software client on machines on which I wanted to back up the registry, or system state. Now I can back up any data on any Windows Server anywhere in our organization. This software is supposed to be able to back up an Oracle database, so once I unlock the secret to that, I might be able to suitably resolve my concern with our Unix Server.

Current State of our Shared Server Room

For easy access we purchased a KVM switch and connected a monitor, keyboard and mouse through the switch to all the Servers in the Rack. The monitor, mouse and keyboard now sit on top of the Rack and are easily accessible to all who enter the Server Room. The Servers are logged into remotely when we need to login to them at all, and only on rare occasions does one log on to them locally. It is the responsibility of whoever logged in to log back out when they are finished, but just in case they forget a screensaver password, and short auto logout, have been setup on each machine. In order for an intruder to gain access to our Servers they would have to get past the magnetically locked doors. Next they need to successfully crack a password. Then to further secure the windows environment, we followed Microsoft's advice.

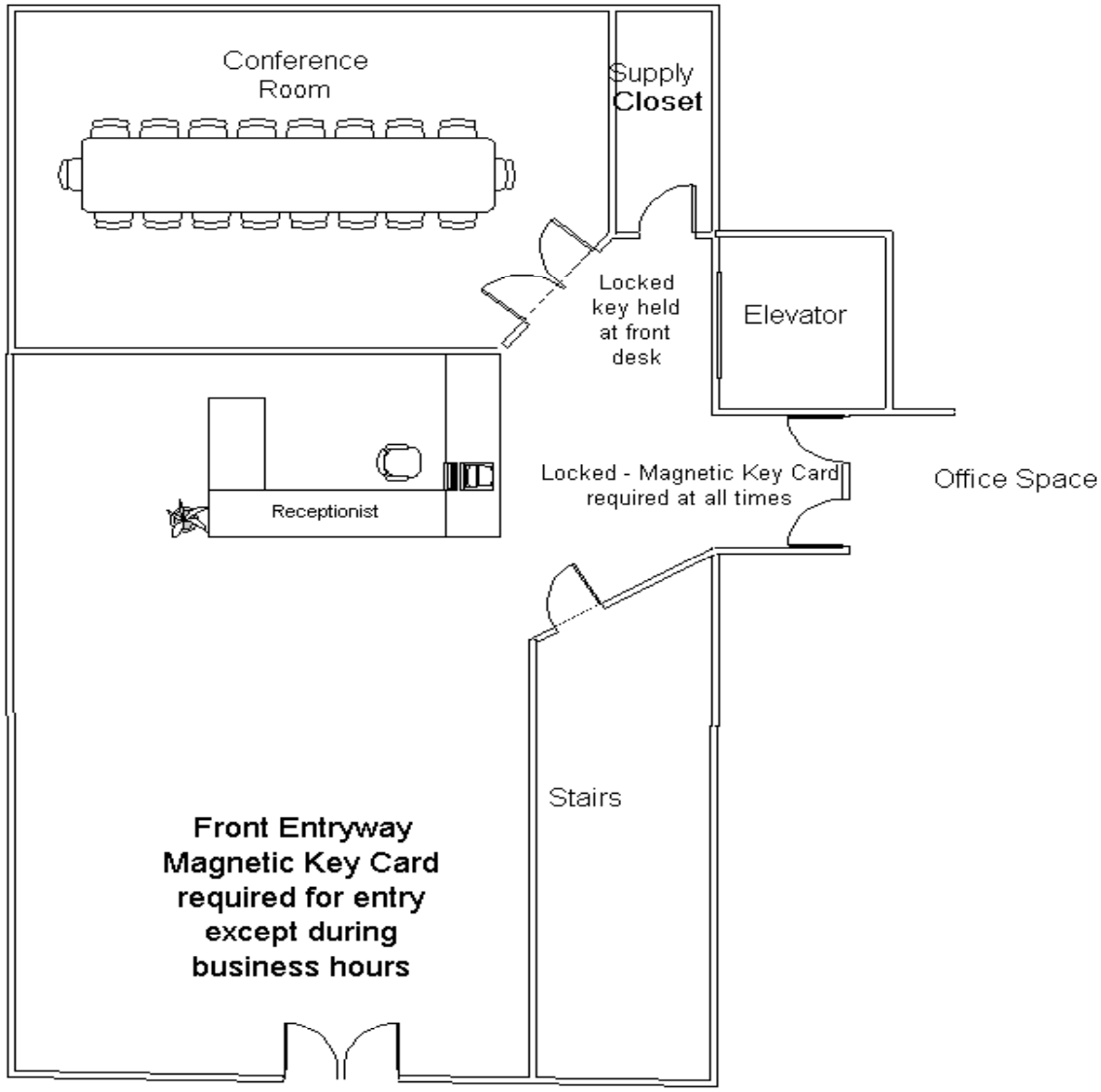
> Rename the built-in Administrator account to provide a greater degree of security. Use a name that does not identify it as the Administrator account. This makes it difficult for unauthorized users to break into the Administrator account because they do not know which user account it is. For additional security, after you rename the built-in Administrator account, create another account named Administrator that has no rights to the system. This will frustrate a hacker's attempt to use the Administrator account to access the system. (Madden, p.321)

All the rest of our Servers are inaccessible without a key to the cabinet they reside in. Our Tape Backup system has been modified so that a full backup fits on one AIT tape (which can hold 100-200 GB).

© SANS Institute 2000 - 2005 Author retains full rights.

The Lobby

This is a representation of our lobby which will be discussed next. It is not to scale, and is by no means comprehensive. In this layout you can also get an estimate of the location, shape and size of our conference room.



© SANS Institute 2000 - 2005 Author retains full rights.

Before Security Enhancement

There is only one entrance to our building. A magnetic key card lock near the door bars access to any who do not possess a key. This is deactivated during business hours, during which we have a receptionist who sits in the lobby and directs traffic for all of the other offices. Even during those times when our receptionist is not there, access to the main offices is blocked by another magnetic key lock. The only parts of the building that can be accessed without a key card are the bathrooms; and the stairwell and elevator. The stairwell and elevator lead to other floors with similar lobbies, receptionists, and magnetic key locks. A supply closet and a conference room are accessible from the lobby but require a key for entrance. The receptionist holds this key. Security cameras are positioned in such a way as to grant a full view of our lobby, and these cameras are monitored by our on-campus security staff. (See lobby layout diagram above.)

Because we do not have a great many visitors, our receptionist is often called upon to engage in other job functions which requires her to have a computer on our network, with all the rights and privileges necessary to do her job. However because her desk is in an area easy for the public to get to, we are concerned about intruders gaining access to our network through our receptionist' computer. Less than a year ago a case was brought against Juju Jiang. "…Mr. Jiang recently plead guilty to five counts of fraud after using a keystroke logger on a public internet terminal to steal passwords and other identifying information from unlucky victims…" (mhamrick) In Mr. Jiang's case the public terminal was at a Kinko's. As the article goes on to demonstrate, locking down a true public access terminal like that would be very difficult. Public access terminals are designed specifically to allow access to the public, so locking them down, and installing appropriate levels of security, would prevent the primary purpose of the machine. Fortunately I only have to lock down a workstation that happens to be in a public location, but is not intended for public use. We want to make sure no intruders gain access to the machine, or even the network port and use it to insinuate themselves into our network.

Steps taken to secure the Lobby

Although the lobby is locked with a magnetic key lock, it is simple enough to gain entry to the building without a card. The lock is disabled during the day,, so entry at this time is as simple as pulling the door open. Of course since the lock is enabled on holidays, the only time someone could waltz right in to the lobby, is during business hours, and at that time our receptionist is there unknowingly providing security. However during non-business hours when the lock is enabled all an intruder would have to do is stand by the door and wait patiently. Eventually someone will either arrive, or will leave. Either way, the intruder has access. Since we have a connection to our network in the lobby we have a potential access point for an intruder to take advantage of. There are, of course,

© SANS Institute 2000 - 2005 Author retains full rights.

security cameras, but prevention is quicker and less expensive than arrest and prosecution.

The most likely thing an intruder might attempt is to simply log on to the receptionist computer. To discourage this, I put in place a BIOS level password, as well as the standard Windows Logon. There is also a screen saver password that kicks in if the receptionist leaves the computer unattended for 5 minutes. (None of these passwords are the same). To prevent any tampering of, replacing of or simple theft of the hard drive, I placed a padlock on the system preventing the case from being opened without a key; a key that is kept in the safe, in the supply closet.

With the physical security in place, the next most likely attack would be for an intruder to pull the network connection out of the back of the receptionist's computer, and place it in the intruder's laptop computer. If the intruder is set up for DHCP, our DHCP Server would issue a proper IP address and subnet mask, and all that would be left would be authenticating to the domain controller as an authorized user. This was our biggest challenge. To deny DHCP to our authorized employees would have required too much training and administrative overhead. The Network Administrator would have had to configure each system individually and trained the employees who travel frequently to configure their computers to use DHCP when away, but the locally assigned IP address when in the local office. Of course it would not have been difficult to set up the receptionist computer off the DHCP network, but if the intruder were using the network cable to connect his or her own workstation, it would not matter how the receptionist computer was configured. Besides even if we did disable DHCP, it would be easy enough for the intruder to just set a static IP address, and gain access anyway.

The senior network administrator for our parent organization had sent us a firewall device that they did not need anymore, so I looked into setting this up to provide our security. The device we obtained had been manufactured by a company that had gone out of business, so there was no technical support, other than the documentation. I tried a number of times to set up the device but invariably I kept hitting the same problem. Either the device was locked down so tightly that the user could not even log in, or the device was open enough to allow full access to any computer connecting through it. Finally we stumbled across the secret to make it work for our situation. We realized that the receptionist would have to be on a different IP address than the rest of the network. The firewall was getting confused because with the same network IP on both sides, it could not differentiate between which was external and which was internal. The problem there seemed to be that if we assigned an IP address to the receptionist, and it was different than the network IP on our network, she would not have access to network resources. This problem was overcome when I discovered that the device itself is configurable to do a One-to-One NAT(network address translation). The firewall is still limited in that it

© SANS Institute 2000 - 2005 Author retains full rights.

cannot block specific ports, but it allows our receptionist access to the resources she needs. When the computer requests a DHCP acknowledgement from the firewall, the firewall queries the computer to determine its MAC address. Since MAC addresses are unique to each network card, the chances of an intruder's laptop having the same MAC address as our receptionist's computer are insignificantly small. If the MAC address response is incorrect, the firewall blocks all access. If the MAC address is correct the firewall assigns the IP address that it associates with that MAC address and access is granted. Now before you readers start getting all upset, I know MAC security is easily evaded. It is simple to get a MAC address, and not too difficult to spoof it. This solution is simply far better than what we had in place before.

Current State of our Shared Lobby

If an intruder were able to guess the BIOS password, and the password to a valid user id, they would have full access to our network…so to limit the intruder even further we programmed the firewall to only allow access to the receptionist computer during business hours. Any other time the firewall will deny access even if the MAC address is correct. In fact it will deny access during these times even if the intruder were able to accurately guess the specific IP address, subnet mask, and default gateway that the firewall assigns to the receptionist computer…although during business hours an intruder could conceivably get through our firewall that way. Fortunately during business hours, the receptionist is in the lobby most of the time, and there is enough traffic through the lobby that we feel an intruder would not have time to gain access without being detected.

Our Conference Room

Before Security Enhancements

As previously mentioned, and displayed, the conference room has only one point of access; through the lobby. To enter one must have a key, which can be provided by our receptionist. In the conference room there are two live network jacks, which provide a point of entry into our network.

Steps taken to secure Conference Room

There are two types of individuals we invite into our conference room. Employees from other offices who are in town visiting with us, and Clients we wish to do business with. We want to grant full access to our employees, but obviously we do not want to grant network access to our clients. My first idea was to simply connect the network port in the conference room to one of the empty ports on the firewall device we used to secure the lobby. The problem we ran into with this solution was that the device we have is not sensitive enough to block particular ports. It can block all usage, or it can allow all usage. We could

© SANS Institute 2000 - 2005 Author retains full rights.

have configured the firewall to recognize the MAC addresses of every employee likely to visit our office, and configured unique IP addresses with One to One NAT for each. For clients we would simply not enable One to One NAT…which means they would keep their IP address they receive on the outside of the firewall. They would be able to see other nodes on their side of the firewall, such as the receptionist's computer, but would not be able to get to nodes within the internal network. This is still not really good enough. We don't want them to access our network, not even our receptionist computer. Correcting this problem turned out to be simple. We got a second firewall device assigned setup to distribute a completely different IP address and subnet mask than the first one. It is set up in such a way that it does not allow any access to our network, only to the internet. Our employees can connect through the first device and get full network access, and our clients can connect through the second and get only the internet.

Current State of our Conference Room

When an employee needs to connect to our network, we get there MAC address and set them up a One to One NAT translation, alongside our receptionist When a client needs to connect to the network, we still advocate, and recommend to them that they use our analog phone line and connect to their office that way. If that does not work for them they can connect to the internet through our second firewall, without being to access any part of our network.

Plans to maintain and improve security in the future

We have our Intrusion Detection System running full time connected between our router, and our switchboard, so any thing going out or coming in is logged. We also have our Antivirus software updating weekly and pushing the updates out to all the workstations. We have scheduled visits from our parent company, and they audit our security and policies as part of their visit. We have a Tape Backup system in place to enable us to recover from any disaster. We are in the process of building a firewall out of a server, that will be able to close out unnecessary ports to further protect us from virus' and other forms of hacking, both internal and external. Finally we have an employee devoted to monitoring these devices as well as our tape backup strategy, and it is his responsibility to create a DRP (Disaster Recovery Plan) for every possible contingency. (That is a job that will not soon be finished.)

Summary

As you can see we have progressed from being an organization that was wide open and practically begging for an intrusion, to being a more security—conscious, better protected organization. Now that we realize many of the ways in which an intruder might compromise the integrity of our data, we have made tremendous advances in establishing a level of security that makes

© SANS Institute 2000 - 2005 Author retains full rights.

us, and our parent company feel safer. We have established a level of protection in two areas in which we have limited control over physical access, by establishing a secondary level of physical security (keys and padlocks) and a level of network security (firewall). Further, we have increased security on the network as a whole by creating an Intrusion Detection System, improving our Disaster Recovery Program, and even documenting a security policy. We have assigned an individual to constantly poke at and test our security to improve upon it until no further improvements can be made.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

LIST OF REFERENCES

1 Cole, Eric; Fossen, Jason; Northcutt, Stephen, Pomernez, Hal. SANS Security Essentials with CISSP CBK Version 2.1. USA: SANS Institute, 2003. 494-495.

2 Madden, Jeff. MCSE Training Kit—Microsoft Windows 2000 Server. Redmond: Microsoft Press, 2000. 321Addams-Moring

3 Addams-Moring, Ronja. "A beginner's guide to data, computer and network security." 4 Nov 1997. URL: http://www.tml.hut.fi/Studies/Tik-110.300/1997/Essays/security_guide.html#Why_care (19 Jan 2004)

4 mhamrick. "Securing Data on Public Terminals." 29 July 2003. URL:http://www.cryptonomicon.net//modules.php?name=News&file=article&sid=417 (20 Jan 2004)

5 anon. "OCC Advisory: Risk Management of Wireless Networks." URL: http://www.bankinfosecurity.com/?q=node/view/334 (20 Jan 2004)

© SANS Institute 2000 - 2005 Author retains full rights.