Global Information Assurance Certification Paper

Information Security 101 :Security for Newbies

Frederick Kim, MCP
Aug.18, 2001
Version 1.2e

Earlier this year, the director of IT who now is my boss had come to me and offered me a position called "Information Security Administrator". This was like a dream come true for me since I had just watched a movie called "Hackers". Yes! The movie where Angelina Jolie still had some innocence left. I was going to be fighting hackers and live a life of suspense. Now, I am going to become this super, computer genius who will protect our company network on one hand where on the other hand get all the hackers to be afraid of me. Since I am given the title of Security authority, all the magical tools that can do anything and everything will come with the territory. Right? Wrong! Hollywood had extorted and exaggerated the life of hacking and information Security to this dramatic, unrealistic, exciting fantasy where things look more dramatic than reality. That is, a technology fairytale. As we journey through the world of information Security, we are going to see things that would have made the movie, boring and difficult to understand. I for one didn't know where to take the first step. When I first began this course, I was a bit lost. I didn't know where to begin. The course itself was excellent and I got to learn many different things from it. But I actually didn't know how it was applicable. I needed someone or something to guide me to the right direction. As I write this paper, my intention is to help guide another poor soul(s) such as the one I used to be. This paper however is not intended as substitution to the course itself(nor other security books that cover the security technology in depth), rather as a guide and a starting point to get a sense of what information security is all about. That is, a good starting point for a newbie security personnel in a small company who does not have anyone to go to for guidance to the right direction. For those of you who are surfing through the SANS Reading room to find a reason for taking the class, I hope this paper can serve as a good reason to take the course since it would be virtually impossible to cover the 600-700 pages of in-depth training materials in a small research paper. (What will be covered in this paper may or may not be relevant to the reader's situation. Covering the entire aspect of security is beyond the scope of the intended purpose.)

WHAT?

First thing I did when I became the security administrator was to learn the infrastructure of our company; The Big picture! That is, our company's entire network and all of its included systems. This is to learn what you must protect (Data) and to learn what you have to work with to accomplish this. This is a very time-consuming procedure. But once you complete it, it will help you a lot during the incident handling process. Best approach would be observing and spending time with the appropriate systems administrators. That is, for network, NT, Unix with Network administrator, NT systems administrator, Unix systems administrator respectively. Since they are the ones who are managing the systems, they should be the best resource to start with. However, you should not stop at the Operating system level. Once you define hardware and systems configuration level, it is important to move on to the software/application level. Again, this is to ensure that you understand the complete BIG-PICTURE of what you have to work with.

WHO?

Once you've figured out what you have to work with, then the next thing to do would be figuring out who you are protecting your information/data from? All malicious hackers are calling from far away location such as China or Russia. Right? Wrong! Studies have shown that great portion of hacking activities do come from inside of the company. It also makes sense since hacking done from inside of the company would be much easier than from outside. This is because 1) They have some knowledge of the systems. 2) They already have some level of access to the systems. 3)The have some level of trust inside of the company 4) They are inside of the company's firewall. I am not insinuating that all you would have to worry about is inside disgruntled employees. Obviously there are outside malicious hackers to worry about as well. Much like a physical war, understanding your enemy is very important. Without that, your battle is halfway over in favor of your enemy. Different methodologies (such as social engineering to IP Spoofing to any one of the Denial of Service attacks(Ping-of-death, SYN Flood, etc…) that hackers use to penetrate into your company's line of defense are often hard to detect(Sometimes too late when detected)simply because there are too many of them. Therefore, best approach would be to stop it from happening in the first place as much as possible. Point of all this is that everyone is a suspect and that you can trust no one. Also, just like the proverb "history will repeat itself", hacking history would be no exception. That is why it is also important to research and learn who the great hackers are and what they are known for.

Covering detailed explanation of who the hackers are and how hacking is done is beyond the scope of this research paper. However, I will be providing some well-known hackers along with brief description to help ease the studying process. (Please note that this is no way near the complete list of well-known hackers.)

- **Brian Martin**, cult_hero also known as Jericho: He is known for web-defacement. While Kevin Mitnik was in jail, he worked at "Free Kevin" association as a technical consultant.
- **Eric Raymond** : Very well-known hacker. Master of C, LISP, Pascal, Fortran, etc… While he contributed in Linux, played big part in improving EMACS Lisp as well. Author of many well known books including Hacker's dictionary.
- **Carolyn Meinel** : White Hat Hacker. Many of underground hackers hacked into well-known web sites such as that of White house, New York Times, etc… and left a message stating "Hacked by Carolyn Meinel". Therefore she once became a main suspect of FBI. Specializing in cryptography, she gave many well-known seminars on Security.
- **Phil Zimmerman** : Inventor of PGP. (Not a hacker)
- **Sir Dystic** : member of Cult of Dead Cow since May of 1997. Major contribution in 1st version of BackOrifice.
- **Jarkko Oikarinen** : He is the person responsible for well-known IRC software(1988).
- **Mudge** : White Hat Hacker. Big contribution in making L0phtcrack, an NT password auditing tool.
- **Dildog** : Member of "Cult of the Dead Cow" since 1998. Major contribution in making Backorifice2000.
- **Kevin Poulson** : Hacker for the darkside. He is very well-known for many famous hacks including hacking KISS-FM for radio contest. Very good case-study material. For more information, www.kevinpoulsen.com

HOW?

Now that we've established "what" and "who", all that's left would be "how?" Unfortunately, this part will be lengthiest of all. However, this is probably going to be the most useful information of all for most readers.

1) First thing's first. Now that we've defined what we have to work with, we now have to figure out how to make everything secure. Best starting point would be checking for vendor's recommended

security patches. By staying up-to-date in all security recommendation, you are protected from most of the known security risks. It is always good idea to take additional steps outside of what is recommended by your vendors. For instance, NT Security involves registry security that is covered only vaguely by Microsoft. SANS offer Step by step procedural documentation to secure NT, Linux, and Solaris operating system

2) Now that we've got everything (servers and PCs, network equipments) secured, we are done right? Wrong. Maintaining the security is just as important as making it secure in the first place. In fact, it actually would be harder task to accomplish. Think of it this way. When you were back in school, depending on how you look at it, everyone started off the semester with an "A" grade. Keeping it at "A" throughout the semester was more difficult since you had to work hard to make sure you are up to date with all the class materials. Same concept applies here. In order for you to maintain hard-core security, you have to make sure that all the patches are up-to-date, daily review of event logs and so on. Since there are too many things to account for, it is not productive for one person(A security administrator) to be handling all of these tasks alone. Having a check-list prepared with appointed responsibility is a good method to approach this problem. Therefore prepare one check-list per system type and make sure that person in charge of each section to handle the process. Weekly report (filled out check-list) should be submitted by each systems group to the security department for review.

3) Once some level of security is in place, it is important to get user-community involved. This can be done via user security awareness program. This is to educate users why security is responsibility for everyone, rather than just Security team of MIS department. Making sure that everyone can relate with the materials would be important since too much legal and technical terms may only inspire boredom. Get users to imagine being part of conspiracy to defeat hackers. Comparing to the success of neighborhood watch and worthy fight against crime should encourage users to play stronger part information security.

"You can have the best technology, firewalls, Intrusion-Detection systems, biometric devices. All it takes is a call to an unsuspecting employee, and that's all she wrote, baby. They got everything."

Above is a quotation from a famed hacker, Kevin Mitnik. Any information security expert will say that there is no such thing as 100% bullet-proof network. This is partly because human beings are

users of computers and it's network. Until human beings begin to act like computers to not be influenced by perception, subjectivity, desire to be helpful to others as a basis for human-nature, they will continue to be the 1st layer target for malicious hackers. As Mr. Mitnik reminds us the importance of educating end-user community, it should be our mission as security professionals to commit to educating and reminding the importance of security as a whole. Good method of presentation would be 1) Annual all-employee security awareness conference 2) Monthly security emails 3) Employee Security awareness contest. 4) Etc… Only when security becomes second nature will it become truly and most effective.

4) Once the importance of Security has been delivered to everyone in your company, it is time to practice what we've preached. How are we going to make sure that everyone will act accordingly to what was taught in Security training? Since all of our employees are nice, we should be able to just trust them and move on to the next topic? After all, some of them were nice enough to give away their corporate user password to a friendly stranger over the phone(Social Engineering)in willingness to help. If we just ask really nicely, they will be as nice to us(security department) as well. Right? This is a BIG NO. Though they may be nice, one element we are forgetting over-rules and it's called "Naïve". There is no doubt in my mind that your employees are nice people and that most of them will try their best to do what was taught in the seminar. But you have to remember one thing. These are the same people who thought their printer was broken when it was out of paper. Chances are ,most of these people will forget about it the moment they get to their cubicle. Best way to approach this would be putting information security Policy in place. Information security policies and procedures are a critical component of corporate MIS infrastructure and are highly effective when made part of normal business. Going over detail on writing policy would again be beyond the scope of this paper. This paper is merely emphasizing the importance of enforcement of policy. Therefore only the basics of some of the most important factors of policy-making and it's enforcement will be covered by this author. SANS course, however covers in depth tutorial of how to write and implement information security policy.

- Though what was taught in the security seminar can be perceived as verbal/implied policy, written-policy that is read and signed by each employee will carry much more weight and therefore easier for enforcement.

- This policy should be created in response to direct and significant threats against the company with in regards to information security.

- One thing to consider when writing a policy is that it should be applicable to everyone. Everyone by definition includes you (security personnel) along with everyone else in your MIS department. Sometimes, people in MIS department feel that they are above the law(in this case, Security policy). If you want to enforce these rules, you must be willing to practice what you've p-reached. Setting an example as an enforcer is an important element. If you are enforcing these rules and regulations to the end-user community, you should do the same to the systems administrators as well. No exceptions. When you start bending rules for people, it will be the starting point of nullifying what was once known as information security policy and may become voided.

- Policy should be realistic thereby enforceable. There is no such thing as 100% Security. When implementation of security cause problems for operation and production of the company, then we are in some sense defeating the purpose of Security. Without the company, there is no data to protect. Defining a fine line between Security and production is very important when writing and implementing Security policy.

- Information security policy should include topics such as 1) user account and password management 2)Remote-Access Policy, 3) Software installation 4) Internet usage, 5) E-mail usage (***I think it is worth mentioning that majority of incoming viruses are via email attachments. Users therefore should be prohibited from using email to send or receive file attachments except for business use. On top of that, users should also never send or open programs via email. This should include but not limited to files that end in suffix EXE, VBS, BAT, REG. Since our job is to become a professional paranoid, if possible, it may be better to block these attachments at the email-server level.***) 6) and so on… Since there are too many different topics to be included specific to your company's profile, many security experts recommend outsourcing this task should your company's budget allows. There are number of professional security consulting firms that can help your company to develop good security policy to fit your company's needs. Normally, after the policy is written, your company's legal department will take charge to make sure that everything is worded correctly in legal aspect before handing it out to all employees.

- Security policy is something you would have to work on in an on going basis. That is, as security status changes, so will the security policy. As you find more different security issues within your company, you should be adding addendum to your company's security policy.

- Since anything and everything could be considered as security risk(s), it is necessary to consider security as an evaluation criteria when choosing any new products. It is important to have employees' research and test all security measures on the product before approving them. Having a documented check-list of minimal requirement in place for approval of the product from the security department would be a good resolution for this problem.

- It is imperative to enforce policy on not allowing any of the following: 1) Napster (or any Gnutella), 2) Any of Instant Messenger services (Like MSN, Yahoo, Aol/ICQ…) 3) Mirc client. Napster is based on turning your workstation into a peer-to-peer network thereby posing as a substantial security risk to your company. It requires a download of the Napster software to your machine(Same applies for Mirc and IMS), which may interfere with other, business-related software on the workstation. More significantly from a security standpoint, it opens your machine to unauthorized access by users outside of the company, who are presumably looking for music but can use Napster to hack into other areas of your machine or your company's network. There are many other, lesser known but similar, file-sharing programs that should not be downloaded from the internet as well, including Gnutella, Scour, FileNavigator, and Napigator. Mirc is a client used to connect to IRC(Internet relay Chatting). By authenticating to IRC chat, you are vulnerable to some IRC specific hacks such as DCC hack thereby posing a great deal of security hazards. If for any reason, they are out in your network, remove them immediately.

- Anti-virus policy is one of the most important part of Information security policy. It should include the product information along with deployment procedure. At minimal, the name(or the position) of the responsible person for anti-virus management along with how often definition files are updated, and what to do when virus is detected should be included in this section.

- There should be a specific section(or a separate addendum) dedicated for functions of MIS group. This should include Privileged account management where stronger password policy is enforced, while renaming all administrator/root accounts. Another example is PCAnywhere policy. Since many NT administrators use Pcanwhere to access and manage different Windows NT servers, it would be imperative that some policy is set in place. Since PCAnywhere passwords are not strongly encrypted, capturing a PCAnywhere session across an un-switched network segment will allow a hacker to obtain the password. The threat is compromise of a single PCAnywhere account means compromise of entire company

domain. My recommendation would be that different account/password be used for each server and that this account not use the Windows NT database but instead "PCAnywhere" account database. Also it is important that PCAnywhere should only be used across 100% switched networks while be not adding the administrator group in the PCAnywhere settings. Termination policy, Systems backup and recovery policy are just some of many things that should be included in this section.

5) Firewall is the first layer of protection against DoS attacks for most companies. There are 2 major types of firewall in the industry. One is called application proxies and the other is called packet filtering. Application proxies are generally known to be more secure yet has limitation of securing outbound traffic in the most part. Packet filtering firewalls on the other hand are high performance with inbound traffic. If a firewall that is well designed are well configured and well maintained, it would be almost impenetrable. Since hackers know how difficult this would be, hackers will start out with different yet easier methodology, such as social engineering on users. They will jump into the targeted company's garbage dump before attempting to penetrate into a well managed firewall. With this in mind, any good network manager(s) will make sure to have a firewall in place while keeping it at it's peak performance. The way you can see if there is a trojan connection into your system (in Windows NT) is to type netstat –a command in command prompt. It will tell you what ports are being used. Since this is really important issue to know, I will include some of more well-known trojans and it's default TCP-port.(Please note that some of these default ports can be manipulated with different port number)

Trojan	TCP-Port number
- NetBus 1.x	12346
- NetBus Pro	20034
- BackOrifice	31337(ELEET)
- SubSeven	1243
- NetSphere	30100
- IcqTrojan	4950
- Attack FTP	666
- GirlFriend	21554
- TheSpy	40412
- WebEx	1001
- Backdoor	1999
- ICQKiller	9989
- AOLTrojan1.1	30029

6) Considering IDS(Intrusion Detection system). IDS is an extremely important component of security solution on a critical information technology systems. While firewalls minimize the threats from external, internet based attacks, an Intrusion Detection system will protect your data from within. Unfortunately, it is very likely that most corporations will experience at least one major security event in a 12 month period, and some of these attack(s) will likely occur from inside by disgruntled employees. Computer security incident may be detected by intrusion detection system on the servers, network, firewall logs, server security logs, modified password files, or the deletion, modification, or attempted deletion of data. Security logs and IDS should be monitored at least on a daily basis. IDS monitoring systems, including hardware/software components, can be categorized into 3 basic product areas. 1) Host-based IDS, 2) Network-based IDS, 3) Hybrid-IDS.

- Host-based IDS are implemented as an "agent" or software module, on each host that is to be monitored. Agents can be configured to monitor native event logs, critical systems file "reads" or modification, registry changes, and other security events on local machine. When suspicious activity is detected, the agent will send alert to the IDS console. It should be configurable to monitor in real time or in scheduled intervals. They are not supported on network switch operating systems like Cisco IOS. An example of host-based IDS is Axent Intruder Alert.
- Network-based IDS operates in promiscuous mode as a sniffer and capture/analyze network traffic on a network segment. It will monitor the machine containing the IDS software and other devices on the same network segment. However, in a switched network, port spanning/mirroring must be enabled on the network segment being monitored. It will capture network traffic and compare it to defined attack signatures. Network-based Ids example is Axent Netprowler.
- Hybrid IDS combines both an agent-based IDS and Network based IDS on one device to identify a greater number of intrusion attempts or security events. However in here, network based IDS does not operate in promiscuous mode and only capture network based destined for the machine with hybrid solution. As with host-based IDS, event logs, critical system files, registry entries can be monitored. When suspicious activity is detected the hybrid IDS will send alert to configure monitoring consoles. Some solutions may attempt real-time responses such as offending IP address disabling the account. Cybersafe Centrax is an example of Hybrid IDS.

When considering IDS system, in this author's point of view, important factors should include 1) Is it easy to use? 2) Capability of detecting numerous detect types? 3) Ability to create custom attack signature? 4) Generating report capability 5) Is price right?

7) Defining the Security department's roles and responsibility could be very helpful when security administration is implemented. Given the nature of security administration, it is only matter of time before you are faced with resistance. However, in order for security administration to be effective, it must rely on everyone's cooperation. Therefore, security team's role should be written/predefined and should be approved by management. This will allow security team to take appropriate action without reprisal. By defining scope and responsibility, it gives authorization to take action. In emergency cases, it may be necessary to take actions beyond average day-to-day given authority. This gives permission in advance to take appropriate action during incident handling process. It is good idea to determine what policy/already implemented security roles(Even though it may not be in written format, there should already be in place unwritten/implied policy. For instance, who adds/removes users and so on…). Review and recommending improvement should follow thereafter in a form of addendum (With outlining the risks involved as well as proposed solution). Written policy is more official and tends to carry more weight than verbal/implied policy since it is documented and signed by appropriate authority. This should also include written permission for password assessment as well.

8) What do you do when one of the disgruntled employee was terminated? What do you do group of people were just laid off from your company? How to handle hoax emails since it can serve as Denial of Service attack? These are just some of questions to be considered before this takes place. How to respond to these situations are called "Incident handling". Though planning everything ahead would be impossible to accomplish, it would be wise to put in place some sort of incident handling/escalation procedure. For example, it may be too late to start thinking about disaster recovery procedure right after your important, time-critical server goes down due to some Denial of Service attack. There will be circumstances/incidents where situations arise off guard. Also, following an incident is one of the most important, and effective time to review policy. Lesson learned from such incidents should be used to evaluate current policy in place to determine where it wasn't effective. These incidents should alert everyone to problems and provide motivation (Also strong reasons) for the change. Therefore, it is very important that these policies can adopt to changes. SANS Computer Security: Incident

handling Step-by-step is an excellent documentation that can guide you in starting this procedure.

9) Many of security related tools are available in the internet for free distribution. Bad news is that you do not know how reliable and trustworthy these tools are. As a Security professional, you will want to familiarize yourself with reputable tools. Many tools like nmap(vulnerability scanner) and tripwire are known in the industry and is talked about in SANS courses. Tools that are talked about in the Security courses, or books like Hacking exposed, tend to carry more weight since it's been tested by many recognized security leaders. This however doesn't mean that you can automatically trust these tools the moment you see them. Unless you purchase commercial security tools from recognized vendor with tech support, you are to take these tools with much caution at your own risk. Obviously, smart thing to do would be to download from reputable web sites such as www.perdue.org (Tripwire along with many other security tools were originally written by students and faculty at Perdue University). Though it would still be wise to take caution, it obviously would be safer than to download from an unknown hacker sites. One other thing to consider would be that many of these tools were written by hackers, just how much can you trust it. It is important to test any tools(even the commercial ones) in a security test lab before attempting to load in a production environment.

10) It is important to have appropriate people to be on the computer security advisory email list. This is to ensure that right people will be informed of new security events,news in their technology realm.

- SANS Newsbites: To subscribe email digest@sans.org with the subject "NewsBites subscription".

- CERT Security Advisories List:
CERT (Computer Emergency Response Team) Advisory mailing list.
To join, send email to cert@cert.org and in the text of the message write "I want to be on your mailing list".

- CIAC Security Advisories List
The CIAC (Computer Incident Advisory Capability) of the U.S. Department of Energy. "CIAC Bulletin" contains important, time-critical computer security information.
To join, send email to majordomo@tholia.llnl.gov and in the body of the message write, "Subscribe cias-bulletin".

- SUN Microsystems Security Advisory List
To join, send email to security-alert@sun.com and write "Subscribe CWS(your email address)"

- Virus Security Advisories List
A high-traffic real-time advisory listing of virus attacks from businesses, government agencies, and educational institutions.
To join, send email to LISTSERV@lehigh.edu and write "Subscribe valert-l your-name"

- Coast Security Advisory List
To join, send email to coast-request@cs.perdue.edu and write "Subscribe coast"

Conclusion :

As I conclude this paper, I would like to think back to when I first stepped into the field of information security. If I can express how I felt at the time in just one word, it would be "frustration". I knew that I needed to learn different techniques and gather much information. However, more I studied, more confusing it got to be. As Mr. Norcutt mentioned in the interview on whether certifications matter and I will quote it "When I moved from network management to take over the information assurance function, I was shocked to learn that a high percentage of the employees in information security lack the basic skills and knowledge to accomplish their jobs. They come to work day after day to produce policies or run tools with no understanding of the fundamental technologies and principles of security. They are often stressed out, secretive, edgy, and defensive, because they know they do not have the understanding or mastery of tools they need. Unskilled security professionals do not reduce risk one bit. In fact, they put the organization in jeopardy", information security professionals (especially ones considered as newbie) need good training tools. This industry lacks good, solid training guide for new security personnel. SANS along with handful of other security training institutes offer excellent security training programs. But as always, non of them are for free. Not everyone has the luxury of being able to pay thousands of dollars for classes. Though this paper will never be able to substitute such excellent class training materials, hopefully this will be good enough to be used as a guide to learn how and where to start. As I walk in the journey of information security, I constantly find myself needing for more training/information. I give so much credit to SANS for having "READING ROOM" in their web site. I think this is probably the most useful security resources gathered in one place. Maybe one day, opportunity will knock on these newbies front door and be able to attend classes. Until then, I hope this

paper(along with other excellent papers in the reading room) can be of some help to them. If I have helped just one person with this paper, all the time spent in preparing this paper was well-spent for. Thank you all for reading this paper.

References:

SANS Resources:

Kistler, Kris. "Paranoid PC Anywhere." 29 May 2000. URL: http://www.sans.org/infosecFAQ/win/paranoid.htm

Levine, Stuart. "Instant Messaging. How dangerous is it?" 19 May 2001. URL: http://www.sans.org/infosecFAQ/threats/IM.htm

Loschiavo, Dave. "Common Errors in OS hardening instructions, security Audit findings and Security Patch Information for Windows NY." 12 Oct 2000. URL: http://www.sans.org/infosecFAQ/win/common_errors.htm

Ludwig, Katherine. "Security Awareness: preventing a Lack in Security Consciousness." 25 May 2001. URL: http://www.sans.org/infosecFAQ/aware/lack.htm

Wilson, Zachary. "Hacking: The Basics." 4 April 2001. URL: http://www.sans.org/infosecFAQ/hackers/hack_basics.htm

Non-SANS resources:

Balgorri, Laura. "Hacking History." May 2001. URL: http://www.interzona.org/transmissor/hackers.htm

Brandt, Andrew. "How Hollywood portrays hackers." 4 May 2001. URL: http://asia.cnn.com/2001/TECH/internet/04/05/hacking.hollywood.idg/

Lucumo. "SITE ABOUT HACKERS." URL: http://www.luckylucumo.f2s.com/info.php3?style=terminal

BOOKS:

Anonymous. MAXIMUM Security Second Edition. Reading: SAMS. 1998

Scambray, Joel. HACKING EXPOSED SECOND EDITION. Reading: Osborne/McGraw-Hill. 2001