Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Option 1 Research Project in Information Security
By Neil Walberg
Submitted 7/2/2003

The Tools of Integrity

A Guide to Evaluating Tools that Evaluate Security

Abstract

The computer age of innocence is long gone. No longer is security just a section in the installation manual that gets skipped over. Today security is an orchestration of many different components that make up the layers of defense. The purpose of this project is to offer a comprehensive guideline to the process of evaluating security tools or products that are being considered for deployment and use within an organization to develop a security strategy. Great consideration should be given to choosing a tool, testing it within a similar environment to that in which it will be used and then providing adequate documentation to an executive level in order that well informed decisions can be made and with it a corresponding assurance level.

The first portion of this document will outline a form to follow with questions and specific criteria that should be thoroughly documented when testing and evaluating a tool. The guideline presented here is not a quick and simple process for an evaluation, [1] but rather a very detailed and elaborate means to provide the reader with enough information to clearly understand the purpose of the tool and what benefits of security it will provide to the organization. Ultimately the resulting report will be used to gage the product's effectiveness in assuring the confidentiality and integrity of intellectual property and related business processes.

Later in the document we will discuss other important issues that should be considered as well as some other interesting perspectives that the industry is facing today.

Vendor and Product Information

Product:_____.
Current Release:_____.
Company Name:_____.
Contact:_____.
Phone Number:_____.
WEB Site URL:_____.
Technical Support:_____.

Some freeware tools may not have an actual company name but it is important to provide as much company or author information as possible for the purpose of how to

acquire the product, a sales contact and technical support. Particularly the version number of the product you're testing.

Describe the product and its position in the marketplace

Is it for intrusion detection, vulnerability scanning, port mapping? How would you categorize the product? A search on the Internet should lead to articles that may offer comparisons and rank to other products with the same scope of functionality and features. Don't go by what the author or vendor thinks about their product. They will always be number one.

Key clients and size of implementation

Try to obtain the names and possible contacts of other organizations that are using the product. Ask the vendor or search the Internet. If you can obtain contacts, inquire if you can get their opinion from their perspective and prejudices. Does the product do what it promised to do? Document and reference other customers with their response.

Price & licensing structure (cost per seat, per CPU, per user, Enterprise Licensing)

Outline the possible purchase scenarios. Freeware is easy here! But if it is a commercial product, list the various ways the product can be acquired relative to the possible deployment plan within your organization. The prices here will most likely be the advertised list price not a negotiated price. Negotiations will come later and are often handled by heavyweights in procurement. Also document if a maintenance contract is required in order to be assured of technical support and access to revised code and materials.

Is a Trial or Evaluation Copy Available?

If so, state the length of time the evaluation copy is valid and if it can be extended. If it can be extended does it require the product to be completely re-installed or can a new license key be used to extend it's operation. Also ask if there is an NDA (Non-Disclosure Agreement) required. Often an author will require an NDA in order to protect his or her own intellectual property. If one is required it should be reviewed and signed by the legal department or legal council, or at least signed by someone in management. Don't take it upon yourself to take on any personal legal obligations.

Is the Software Downloadable from the WEB?

If so, what is the actual web URL address? This could be used to state whether either or both the trial version and production version of the software is available from the web. If not then describe how the software can be acquired and the timeframe.

Backward Compatibility between Versions

This is a major issue. How are patches and upgrades handled? What are the ramifications when there is a new version release? Sometimes functionality will change or be lost when products are revised. Not always will sales or technical support

personnel be forthright with information on future revisions but it should be discussed and researched. Also if there are costs involved in an upgrade.

Technical Support

- 24/7 online, voice and E-mail support
- Deployment Guide
- FAQs online
- News Groups

Technical support is always a clincher. Freeware is often "use as is". Some will offer support via e-mail but there may be a slow turnaround. If you're actually purchasing a product, technical support is a must. The integrity of the product rests on the author or vendor's commitment to customer service and support. Otherwise what are you buying? Describe what the agreements on support will be and if there are different levels based on purchased maintenance contracts. Support on larger enterprise license agreements will almost always include a yearly maintenance contract where many different aspects can be written in. The level of call in support, whether it is just a help desk taking calls or can you call direct to engineering who can provide immediate remediation. Can the vendor provide sufficient fulltime resources to assist with implementation needs? Will on-site support be available and for how many hours per year. Does on-site support include per diem expenses? (Travel, Lodging and Meals). Will on-site installation support and training be included? This all may be quite overkill if you are evaluating a small tool for a mom and pop shop but for a scalable enterprise wide solution these things are imperative. This is your chance to be creative. Be specific. If you have to pay more for premium support make sure you get what you pay for.

Documentation

Are the manuals hard copies or online. Is online help available or is it built into the product? You should simply state where the documentation is readily available.

Training

Is training available on-site, at the vendor location or through a third party training center? Is there a web site that lists where training courses are available and schedules? Is training included in the purchase price or yearly maintenance? Training may sometimes be overlooked in the final summation but could be critical to the success or failure on the use of the product. Consider training costs for employee turnover.

System Requirements (Minimum and Recommended with Full Load)

- Operating System
- Disk Space
- RAM
- CPU
- Network Protocols and Topology

The system requirements you list should be separated into three parts. First the requirements specified as minimum by the author, then the requirements that will be needed in the testing environment. Then you'll need to determine your recommendation based on a full operating load within your production environment. What is the number of systems and also the number operators need to manage the product. Separately it should be noted the scalability of the product considering future expansion of the project. Negotiated purchase contracts and SLAs (Service Level Agreements) may be based on you recommendations.

Additional Software Required for Deployment

List any other software that may be required for the tool to work. Such as the IDS (Intruder Detection System) SNORT™ [2] that must install Winpcap, an additional piece of software used for network password sniffing. One will not work without the other. Be sure and indicate whether the additional software is included in the price or will it have to be acquired separately at an additional cost. Work any additional cost into your pricing structure as previously discussed.

Testing

Now this is where the fun begins. Up until this point the information you have gathered for the most part can be found on the vendor's web site, white papers or from sales support. In order to substantiate the author's claims of functionality and features there must be evidence of functional testing. To be objective it should be tested with consideration to the environment it will be used in your organization, although it is recommended the testing occur on an isolated network not connected to your production network. Some tools used for network exploration, port mapping and vulnerability scanning such as Nessus [3] or ISS [4] (Internet Security Systems) Internet Scanner® or Nmap [5] will interject traffic on the network that may be detected by IDS (Intruder Detection Systems) and set off alarms. The most important point is to "Get Permission". Management should be well advised and you should get written permission before any evaluation testing begins. Many large networks will have some form of IDS monitored by NOCs (Network Operation Centers). False alarms will only create unnecessary concern and may even jeopardize your entire project. Even for a small organization without IDS some testing may create DOS (Denial of Service) and disrupt business continuity.

Push or Pull Technology

Some tools will use the architecture of having an agent running on the client machine that then will be controlled and monitored by a central manager and console. It may be important to understand the method the client and console communicate. A product such as Network Associates ePO [6] (enterprise Policy Orchestrator) which is used for updating desktop and server systems with the latest anti-virus software and virus definition files, operates with an agent running on each client system on the network. The agent itself initiates the communication session with the ePO server and pulls the necessary updates down to the client. Other client server architectures may use connectionless UDP transports and push data to the manager. Either way it is important to fully understand and document how communication occurs and investigate

specifically what vulnerabilities may be associated. There would be nothing worse than deploying a tool that is intended to provide another layer of defense and at the same time introducing the risk of another vulnerability.

Dedicated TCP and UDP Ports

Any communication in or out of a system will require a specific TCP or UDP port, a point of connection to the network. TCP and UDP ports function within the transport layer of the OSI (Open Systems Interconnect) stack. Client agents that communicate to a central server or to the management console will have services running that may open certain port(s) temporarily or dedicate open port(s). They may even use more than one during the communication session. The product documentation should tell you what services are running on which ports, but you can also use other tools such as the Microsoft utility NETSTAT [7]. NETSTAT is a command line utility that will display every open TCP or UDP port and it's state, whether it is connected, listening or waiting for a network connection. NETSTAT will display network connections looking from the inside of a system. Inversely you can use a port scanner such as the Linux utility NMAP [5] to display open ports from the outside looking in. Both methods should be used and the results compiled in your final evaluation. Any open port is an open doorway for an intruder opportunity.

Encrypted Network Traffic and Data Repository

Security tools are effective because they collect and examine vital information about the security of your computer systems and network. Just the type of information a hacker is looking for. How this information is communicated over the network or stored can be just as much a risk as the vulnerability you're trying to mitigate. "Encryption is a form of cryptography that scrambles plain text into unintelligible cipher text." [8] It enables users to ensure the confidentiality of files and transmissions and to authenticate one or both parties engaged in a communication exchange. There are many different methods of encryption and their associated algorithms, the formulas used to mathematically encrypt the data. It is important to determine the type of algorithm being used whether it is proprietary or open standards. Proprietary algorithms are private and often protected by patents. Open standards algorithms are usually considered to be more secure because they are continually being scrutinized by the open public. If it is a weak formula it will usually be discovered and broken rather quickly. Although a proprietary algorithm may sound like it would be safer and may be harder to crack at first, they often prove to be quickly broken such as with DeCSS. [9] CSS (Content Scrambling System) was developed for the movie recording industry in order to encrypt DVDs so they couldn't be copied. Unfortunately they used a proprietary algorithm that hadn't been thoroughly tested by the security world and the formula was broken within a very short time after its release.

The point being is to ensure and document that the security tool you are evaluating incorporates acceptable methods of encrypting data so that it is not transmitted in clear text across the network or storing confidential data on a system where it could easily be hacked and accessed.

Web Based or GUI Based Interfaces / Usability

Many newer software products are incorporating browser based user interfaces for administration. The advantage is that you do not have to physically install a portion of the actual application code on a system in order to use the tool. Anyone with an Internet browser can address the administrative URL provided they have the necessary credentials to sign in. Whatever the interface method may be, verify that the data stream is well protected and encrypted such as with SSL (Secure Sockets Layer).

The results obtained from the use of a security tool are often dictated by the competence of the operator. People of course have different educational levels. Even though they may be experts in certain areas doesn't mean they are security experts. Critical user errors will be made if the interface is too complex. [10] The overall evaluation of the user interface must be relative to the capabilities of who will use the tool. A nice GUI interface is good for the novice to quickly learn whereas a command line interface is for expert level automation.

Authentication and Authorization

How does the system verify the identity of someone accessing the user interface? Even though the data stream may be encrypted, encryption does not provide proof of identity. PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol) and Kerberos are just some of the more common methods. PAP is the least secure because passwords are transmitted in clear text. CHAP is more secure in that the user is presented with a challenge message. The response is calculated with a one-way hash and the value is transmitted. The authentication mechanism compares the response with its own one-hash calculation of the expected value. The password itself is never transmitted. Kerberos is by far more secure through the use of encrypted keys and authentication tokens. The author may use any one of a number of methods. Verify what method is used and then research and document the vulnerabilities associated.

Once a user or operator is through the front door what can they do? DAC (Discretionary Access Control), RBAC (Role or Rule Based Access Control) and MAC (Mandatory Access Control) are all different methods that define the limits of access to devices or resources. One of these methods should provide the framework for how a security tool collects data and how users are authorized to access that data and what functions they are allowed to use. Determine what authorization processes and methods are used.

Auditing

Auditing is a process to record the events or errors that occur while operating the tool. A good security tool should be configurable in order to track the success or failure of specific events. At a minimum there should be text based log files generated detailing the functions the tool is processing.

Authentication, Authorization and Auditing are all components that provide for the confidentiality, integrity and availability of our computing systems as well as the tools we use to ensure security.

Real Time Monitoring

- Local and Remote Monitoring
- Alerts
- Performance Monitoring

Other monitoring and management tools are available that can actively retrieve event logs from other security products and then using methods like audit log reduction will alert on specific predefined events such as a brute force password attack. Placing IDS (Intruder Detection System) sensors at strategic locations on a large enterprise network can collect events effectively but also require a back-end monitoring service that can correlate related events in real time. Forward monitoring products such as HP OpenView, [11] e-Security [12] and Tivoli [13] are just a few in that space. The security tool you are evaluating may not necessarily need to be designed to be compatible with a monitoring system. It is more a matter if the monitoring system will work with the security tool.

Comparable Products

A lot of research can go into finding and determining if there are products that can be realistically compared to the one you are evaluating. Sometimes you are comparing apples and oranges. Generally speaking they fall into well-defined categories such as Anti-Virus, Intrusion Detection, Penetration Testing, etc. A full-scale evaluation such as is outlined here is intended to provide decision makers with the ammunition needed to justify the expenditure. Inevitably the question will come up. What other tools do we have to choose from? It's easy to come up with a list of alternatives but the tough decisions will also require an evaluation of the closest competitors. Then you get to start all over again.

Executive Summary

Use this as a conclusion to summarize and emphasize the key and important points you've discovered during the evaluation. It can be most effective by using a pros and cons approach. List out the individual points that are a positive benefit for using the product and then list the negative aspects. Avoid using terms like 'I feel' or "I think". Be objective. An executive summary should be used to state the objectives coming in to the evaluation and the outgoing results. You can state your overall opinion but be prepared to substantiate your personal views points. Decision makers will be interested in how appropriate the tool is to their environment.

This wraps up the step-by-step form I've outlined to use when documenting the evaluation of a security tool or product. Over the last several years I have used several different methods and there are always other issues and processes that need to be considered, tested and documented. There is no set format. Try to be open with questions that suddenly come to mind and document the findings as you pursue the answers.

From here we'll discuss some additional topics that add to the scope of the big picture.

Open Source Code?

There is debate on whether or not a tool should even be considered based upon the source code being available. Some would say there is no way to audit or thoroughly evaluate a security tool without the source code and to be sure there are no bugs or holes in the code that may leave open back doors.[14] This is all fine and well considering, but do we as security practitioners have the programming expertise let alone the time to examine every line of code and routine in order to determine its integrity. It's a point well taken and certainly there are numerous benefits to open source code. Another viewpoint that often comes up during discussion is if the source code is available to us it is available to the hacker who certainly has more time to dig into the code and determine ways to circumvent the process. Maybe even plant their own back doors then replace the code at the download source or on a production system, the author or administrator being none the wiser. To further emphasize the point some organizations have even gone to the extent of writing policy that prohibits the use of tools or any application if the code is open source. It's a tough call as to what extent we trust the author and supplier.

Off Shore Code

Another area that is creating serious concerns are the increasing number of companies that are considering outsourcing IT services and software development to overseas countries such as China and Russia. [15] Economic conditions are driving companies in this country to assess the risks of using cheap labor overseas. Terrorist are know to exist in Southeast Asia and China where there is known espionage taking place against U.S. technologies. It is reported that "North Korea is training around 100 computer hackers each year to boost its cyber-warfare capabilities, pushing the South (Korea) to fortify it own computer security" [20], as well as everyone else. The risks involved are becoming a national security issue.

False Sense of Security

As quoted by Kevin Mitnick the renowned black hat turned white hat, "Having a false sense of security it worse than having no security at all." [16] How well put. We implement security policy and use an array of tools to incorporate a sense of security. The forethought of the evaluation of any security tool should be centered on what level of security this will provide. What's the point? Is it cost effective to spend all the time and resources to test and evaluate a tool if the perception of its capabilities is misguided or non-effective? Worse yet will the results of the tools functionality give a sense of security to yourself and management jeopardizing the integrity of the company as well as your own integrity? Have others review your findings. Rely on the facts as others my understand them. Don't stick your neck out into a short noose.

Commercial vs. Freeware

How to choose the right tool for the right job? Do you go with freeware or a commercially marketed product? There are an ever-increasing number of truly useful

tools. If you're looking for something for personal home use your criteria may not be as stringent. But for deployment on the internal data network of a large corporation you must be much more objective. Integrity and availability become key factors and ones that should be emphasized in the executive summary. Is technical support available? Is the product being continually scrutinized and revised with updates and patches. These are the kinds of questions that need to addressed and documented in the final evaluation. The answer may revolve around how in-depth the tool will be used. If it is only used for spot checks or specific events then it may not be so critical, but if the tool will be used in 7x24 operations, support and assurance may mean everything.

Keep Things Under Wraps

The role of a security organization is to develop and enforce security policy by integrating processes and tools to ensure the confidentiality, integrity and availability of the network infrastructure and information systems. The methods used to integrate these processes and tools become critical and classified information available only to trusted individuals within the organization and executive management. Allowing administrative and un-monitored access to these systems to anyone outside of the security organization violates the essence of a minimum-security policy and jeopardizes the confidentiality and integrity of the company's intellectual property. All security systems play significant roles in auditing, assessing vulnerabilities, administering private personnel data and user account management to name a few. Open access to these systems outside of the security organization would be considered unethical and unnecessary.

Microsoft versus Not Microsoft

It seems in today's world of data processing and information systems there is division between the followers of Microsoft Windows based products and on the other side are all of the other operating systems such as UNIX and Linux. Notably there are even opposing sides between UNIX and Linux with the same arguments arising between proponents of commercially sold versions of UNIX and the open source community pushing Linux. The common ground may be the differences in the reality of their perception. [17]

Many companies will say that security is their main concern when it comes to deploying Windows yet the majority will continue to deploy windows despite their concern. Up until a year or so ago Microsoft products were not necessarily security-oriented. Window NT and 2000 are feature-oriented with almost all features installed by default to give the user a richer user experience. Since then Microsoft has initiated the Strategic Technology Protection Plan that provides their customers with a "Security Tool Kit" which includes a wide array of security guides, tools and checklists designed to "Get Secure and Stay Secure". [18] The architecture is there and Windows can most definitely be secured. In fact with the release of Windows Server 2003 most add-in components are not installed or activated by default and Microsoft developers have intensely reviewed the new operating system code to identify possible fail points and exploitable weaknesses.

Now, on the other side of the ball court is what I like to refer to as the "Command Line Junkies". All along it has been fairly well accepted that Linux and UNIX are more

secure. In fact numerous tools have been written to run on these O/Ss that are used to evaluate the security of not only their own but also Windows based systems. [19] The largest number of freely available, public domain security tools are UNIX or Linux tools. Here's the deal. I propose that if the "Black Hat" hackers of the world were to concentrate as much of their time on breaking in to Linux or UNIX systems there would be many more vulnerabilities and holes found and exploited, in fact probably more. It's just like the encryption algorithm debacle as previously discussed. The more an operating system is scrutinized and hammered against, the more secure it will become. But then, that's just my opinion.

The Next Generation

Even with all our policies, administration techniques and tools we are still faced with what seems to be a futile attempt to secure systems. Although we've covered all the bases and a system may appear to be secure and operating normally, while in fact it may have been modified and is compromised. If and when will operating systems and applications truly be secure? What is next?

What may be part of the answer and definitely is on the horizon is the 'Trusted Computing Platform Alliance'. [21] TCPA was initiated by Intel to provide a new hardware platform to improve trust with software. Microsoft on the other hand is developing software call Palladium to be built into future versions of Windows. Palladium has recently been renamed the 'Next Generation Secure Computing Base' (NGSCB). The idea being that the combination of hardware and software would provide a secure computing platform where the operating system and applications could be tamper resistant. It would also be harder to run bootleg software.

It would work something like this. Intel's TCPA will incorporate a chip set (called Fritz) mounted on the motherboard. As the system boots up the Fritz chip would check the serial number of the Pentium processor and each piece of hardware to see if it is on the TCPA approved list. On a side note, the Fritz chip is named after Senator Fritz Hollings of South Carolina who lobbied strongly to make TCPA a mandatory part of consumer electronics. [21] After Fritz has checked the hardware it will then turn control over to Palladium in the operating system. Palladium can then communicate with vendors to verify the O/S and applications are actual licensed copies and even signed indicating the software is legitimate. TCPA can tie each licensed copy of the Windows operating system to the motherboard it is running on and Palladium can tie the licensed copy of Office to the operating system, or any other application that is a registered NGSCB application. Using this technique it is feasible that application software could even be rented or the vendor could charge and deliver upgrades on-line. This brings us to another feature inherent to the TCPA / Palladium platform, 'Digital Rights Management'.

Digital Rights Management (DRM) is a technology developed by Microsoft in 1999 that delivers legitimate music, video and other media content online securely. The technology allows the owner to stipulate a set of rules and policies that govern how the content can be used, for how long and by whom. The upcoming Office 2003 suite will allow users to designate who can open and edit a document or read an e-mail message. They can specify the 'Terms of Use', whether or not they can print, copy, edit or forward the data. They can even specify that after a certain period of time the data

will automatically be deleted. These rights management policies will remain within the files during and after they are transmitted and can be enforced even after the data leaves the network. This would effectively help to protect confidential and personal data such as health records and financial information. Microsoft claims that Palladium could even stop spam and viruses. "AMD and Intel plan to release NGSCB enabled hardware in time for the next release of Microsoft Windows codenamed "Longhorn". [22] The next version of Intel's Pentium processor with 'Fritz' incorporated into the processor has been officially named 'La Grande' after a town in eastern Oregon. [21]

Even with all the advantages, NGSCB and TCPA are facing some serious criticism. These trusted platform based systems are being accused of violating user privacy and undermining user rights to digital content. The argument being that once you buy a piece of software it is yours to copy for personal use. As long as you don't distribute or sell it for gain you're not in violation of copyright agreements. The platform would give software vendors the ability to disable or erase pirated copies of software and it attempts to destroy the open-source software community. Whether or not NGSCB and TCPA will succeed and are accepted will depend on how effective they are, how it is incorporated in our applications and at what cost. If in the future the only way you can perform an on-line credit card transaction is with a trusted platform system, then a lot more people will move over to the system.

In recent news

If undermining user rights and violating user privacy isn't bad enough, the battle by the music industry and Washington against pirates that download music illegally has brought about some very drastic ideas. At a recent meeting with technology experts Senator Orrin Hatch, R-Utah, said that he was all for a technology that would destroy the computer of people who continually violate copyright laws and download music illegally. [23] Rather than go after the ones that provide the file sharing services like Kazaa for BearShare, go after the individual breaking the law by breaking his computer. Warn them two times and then the third time, smoke it. You can image the liability issues from damaging someone's computer. Most would agree that Senator Hatch's idea is far too drastic and to remotely attack someone's computer even violates anti-hacking laws. Even so, the problem is very serious and has gotten out of control. "There is no excuse for anyone violating copyright laws," Hatch said. [23]

Worse yet, or better depending on how you look at it or what side of the fence you're on, the Recording Industry Association of America is escalating the battle and threatening to sue individuals who download and share music illegally. [24] They are not saying how many songs you have to have downloaded and are present on your machine before they come after you but with the declining sales the record industry is experiencing, they are obviously getting desperate. If they really plan on going through with this idea they must plan on suing a lot of minors. Are parents totally responsible for every action of their children? There is no doubt that the vast majority of those violating these very copyright laws are kids that have no idea they are breaking the law. Besides, everyone is doing it.

Conclusion

Back to the subject at hand. When evaluating tools that will be used to evaluate the security of you systems and network, be skeptical. Don't become convinced and believe everything a salesman may be telling you. Their job is to sell and make themselves and their company money. They often may tell you just what you want to hear. Your final decision should depend on weighing the results of your research, criteria and testing. Have fun. My experience is that as you get good at writing evaluations, management will look to you for your contributions, opinions and perspective. Management is becoming much more aware and appropriating a much greater budget for information security. The focus is shifting toward acquiring human resources and evaluating security tools and solutions. Installing and testing new products is fun and can offer a magnificent learning experience, one that may benefit the longevity in your current position but may also make you more marketable for your next endeavor. In today's turbulent business atmosphere with sometimes an uncertain future, the more products we know and experience we have will always give us the edge.

References

[1] Boran, Sean. "Tips on evaluating / buying security tools" 5 September, 2001 http://www.boran.com/security/sp/testing_products.html (1 July, 2003)

[2] Caswell, Brian and Roesch, Marty. "Snort™" 15 May, 2003 http://www.snort.org/ (1 July, 2003)

[3] Deraison, Renaud. "Nessus" 5 May, 2003 http://www.nessus.org/ (1 July, 2003)

[4] ISS Internet Security Systems. "Internet Scanner®" http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php (1 July, 2003)

[5] Insecure.org. "Nmap" 3 May, 2003 http://www.insecure.org/nmap/ (1 July, 2003)

[6] Network Associates, Inc. "McAfee ePolicy Orchestrator v. 3.0" http://www.networkassociates.com/us/products/mcafee/antivirus/fileserver/epo.htm (1 July, 2003)

[7] Microsoft Product Support Services, Knowledge Base Article – 137984. "TCP Connection States and Netstat Output" 7 May, 2003 http://support.microsoft.com/default.aspx?scid=kb;en-us;137984 (1 July, 2003)

[8] Cross, Michael. Security + Study Guide. Rockland, MA: Syngress Publishing, Inc. 2002. 12-23, 498-499

[9] Lumeria.org. “CSS (the "encryption") and DeCSS (the decryption tool)” http://www.lemuria.org/DeCSS/decss.html (1 July 2003)

[10] Kaiser, Johannes and Reichenbach, Martin. “Evaluating Security Tools Towards Usable Security” http://www.iig.uni-freiburg.de/telematik/atus/publications/KaRe2002.pdf (1 July, 2003)

[11] Hewlett Packard Company “OpenView” © 1994-2003 http://www.hp.com/products1/softwareproducts/software/openview/ (1 July, 2003)

[12] e-Security Incorporated. “e-Security” © 2003 http://www.esecurityinc.com/ (1 July, 2003)

[13] IBM ®. “Tivoli” http://www-3.ibm.com/software/tivoli/ (1 July, 2003)

[14] Ross, Seth T. “Evaluating Security Tools” Unix System Security Tools © 1999 McGraw-Hill Companies http://www.albion.com/security/intro-6.html (1 July, 2003)

[15] Verton, Dan. “Offshore coding work raises security concerns” © 2003 Computerworld Inc. May 5, 2003 http://computerworld.com/newsletter/0,4902,80935,00.html?nlid=SEC (1 July, 2003)

[16] Mitnick, Kevin “FREE KEVIN” http://www.kevinmitnick.com/home.html (1 July, 2003)

[17] Mullen, Tim. “The Reality of Perception” ©1999-2003 Security Focus. 7 April 2003 http://www.securityfocus.com/columnists/152 (1 July, 2003)

[18] Microsoft TechNet. “Microsoft Security Tools and Checklists” © 2003 Microsoft Corporation http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools.asp (1 July, 2003) http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/default.asp (1 July, 2003)

[19] Red Hat Inc. “Chapter 9. Vulnerability Assessment”. Red Hat Linux 8.0: The Official Red Hat Linux Security Guide. © 2003

[20] Rijswijk, Oskar van , The Command Post, "DPRK training hackers" 17 May, 2003
http://www.command-post.org/nk/archives/007078.html (1 July, 2003)
Originally posted on CNN.com, 17 May, 2003, Article no longer available.
http://www.cnn.com/2003/TECH/internet/05/16/korea.hackers.reut/

[21] Anderson, Ross, "Trusted Computing Frequently Asked Questions
- TCPA / Palladium / NGSCB / TCG" Version 1
http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html (1 July, 2003)

[22] Microsoft, "The NGSCG Community" 13 June, 2003
http://www.microsoft.com/whdc/winhec/eyeonwinhec/NGSCB.mspx (1 July, 2003)

[23] The Associated Press, "The Colorado Springs Gazette", Business Section
18 June, 2003

[24] The Associated Press, "The Colorado Springs Gazette", Business Section
26 June, 2003

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event