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 Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Steve Clancy
GSEC Practical Assignment Version 1.4b

Network Security Blueprint ..... 1
SOCIAL ENGINEERING ..... 3
PHYSICAL ..... 4
HOST SECURITY ..... 5
NETWORK ..... 6
PERIMETER ..... 7
EXTERNAL ..... 8
TOOLS ..... 8
DOCUMENTATION ..... 9
APPLICATION ..... 9
DATA ..... 10
Executive Summary ..... 11

# Network Security Blueprint

The purpose of this paper is twofold. The first part is to serve as a security overview and memory jogger for the security professional to help them ensure they haven't overlooked a critical piece of the security puzzle and the second part is to provide an executive summary for the IT management level so that they can make an educated security decision. The reason for approach is to provide the security professional with a two-pronged tool. 1. A high level checklist to be used to ensure that all the security components have been addressed whether or not they have been chosen to be implemented. 2. A reference for any executive requiring justification for any part of the security puzzle, with the additional credibility of coming from an outside source. Hopefully it will also provide the knowledge that effective network security isn't just a collection of pieces. It must be a planned interwoven series of tools to minimize exposure of the corporate network. Topics I plan to discuss are listed below

1. Social
2. Physical
3. Host
4. Network
5. Perimeter
6. External
7. Tools
8. Documentation
9. Application
10. Data

While there isn't any particular reason for the order above, my focus here is to provide a broad-brush approach and add detail as space allows.
Summary

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

There is no substitute for a good solid security plan. While many try to buy their way to security with single faceted tools, a comprehensive layered approach to security yields the best, most cost effective results. “There is no such thing as a completely secure infrastructure.” (Young)

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

I'd like to start off with an overview of the attack process. It generally consists of:

Information Gathering
Probing
Violating
Covering

How the actual attack occurs will depend on the information gathered in the first two parts. While probing is really part of the Information gathering process I separated it in this case to emphasize the importance of information gathering via social engineering. Significant attention is paid to electronic scans and port probing but the same can't be said of the people side. Any serious attack will start out with the attacker performing reconnaissance to gain information. The methods are to numerous to list all of them here but some of the most common are dumpster diving, Web pages, phone books, new user phone calls, demanding boss phone calls. The purpose of this information gathering is to get pieces of the puzzle to allow further information gathering. The cycle of information gathering continues until proprietary or sensitive data is compromised. Once the attacker has gathered sufficient information about your organization, IT systems, user accounts, physical security, etc the probing begins. Probing generally consists of port scanners to determine what systems there are and what ports/applications are available, which translates into what vulnerabilities will work against your organization. Other probing methodologies may include "War Dialing", the process of dialing a large number of phone numbers to determine which have modems attached to them, thus providing a soft entry point to the network, or "War Driving", which involves driving around with wireless sniffing capabilities to determine unprotected/unauthorized wireless access points. Once the attacker has determined what systems and applications are being used they can search for specific attacks or vulnerabilities they can use. This is what I call the violating phase, it doesn't necessarily mean that data is destroyed or stolen it could also be setting up a launch point for future information gathering and possible attacks. Lastly, the attacker will typically cover their tracks. This may occur as a result of destruction of data or the modification of logs or applications so that they give the appearance that nothing has occurred or is currently occurring. As you read through this paper try to see the attackers side of the picture to help you better understand why each of the areas below depends on the other.

## *SOCIAL ENGINEERING*

What is "Social Engineering"? It is taking advantage of the fact that people are inherently helpful. Specific examples are phone calls asking for seemingly useless information, possibly allowing the attacker to know who is not in the office and thus whose account won't be used in the next couple of days or holding the door open for someone with their hands full of boxes thus allowing them to not badge in and the proverbial dumpster diving. What does that have to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

do with IT Security? Any serious attack on your organization will start with an information-gathering phase; this is primarily where social engineering comes into play. Any information the attacker can obtain reduces the amount of effort that will ultimately be required to break in to your systems. Social Engineering, in my opinion, is one of the most important aspects of security but also the most difficult because it requires an organizational security mindset. Security has to start from the top of the organization. There must be written policies for employees to follow, they must be clear and concise. They must be adhered to from the top down, NO EXCEPTIONS, especially for executives. One of the most basic social engineering attacks is to call in and pretend to be some high level executive and brow beat passwords or sensitive data out of the poor person on the other end of the phone. These policies must define what information leaves the organization and in what form. For example all personal information will be shredded, all contact information will only given out by the public information officer, email addresses will be based on job positions. They must categorize the value of data within the organization and who gets what access to what data. These policies must be well publicized with repercussions when the policies are not followed. Sounds a little draconian but as well known hacker Kevin Mitnick has said "You could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain vulnerable to old-fashioned manipulation." (Mitnick) One of the first things an attacker does is collect information about an intended target, as simple as a few phone calls, friendly conversation in the parking lot or building lobby. These innocent contacts can provide valuable insight into the organizations network and system administration policies. Once that information has been gathered it can be used to defeat other portions of your security model. It allows an attacker to focus on your weaknesses, which reduces the time required to break down your defenses. Which in turn gives less time to other security pieces like network and host based intrusion detection systems to do their job. As you can see, without a sound security policy and proper training of employees, social engineering can easily allow an attacker to circumvent high priced security measures.

Quick List

| | | |
|---|---|---|
| Policies | Procedures | Training Plan |
| Audit Schedule | | |

## *PHYSICAL*

Physical security is just what it sounds, preventing physical access to the IT infrastructure. As basic as that sounds I'm constantly amazed when I see networking devices stuffed in closets and under counters. Physical security can be as simple as a locked door and a key or as elaborate as man trap, where one access point must be secured before the next can be opened, and landscaping designed to prevent building access and reduce effects from an explosion. Physical security requires significant attention to detail. Some examples are monitors should be placed to prevent prying eyes either from in the office or

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

through the window by someone with binoculars, parking lots designed to reduce employees exposure to persons attempting to gather information through social engineering, and package delivering procedures, especially in today's environment where reducing your building to rubble or contaminating it with some chemical is acceptable to some attackers. The level of physical access controls should be guided by your organizations security strategy. Each location should be evaluated to determine the value of the IT systems and data located there. Value should include the cost to recover the data as well as the cost of doing without those resources for the time period required to recover the data. Physical security must also take into account natural acts like earthquakes and tornadoes as well as outages that may occur as collateral damage, power outages, riots, etc. Admittedly there are a large number of things that can be done for physical security many are inexpensive and easily implemented with the right corporate security mindset. Properly preventing physical access to equipment means that any attacks will have to come across the network, which will allow detection to occur with proper network IDS tools. Physical access allows an attacker to run numerous tools that can compromise the OS, copy data or just outright theft. There are no network devices I know of that can resist an attacker with physical access. The layered security approach provides an indication of physical security compromise by proper host and network security procedures. Once again this is a game of inches and by reducing the threat through one axis the overall security is enhanced.

Quick List

| | | |
|---|---|---|
| Power | Building Access | Business Continuity (DR) |
| Shoulder Surfing | Computer Room Access | Janitorial Access |
| Document disposal | | |

## *HOST SECURITY*

Host based security focuses on the host itself. Ideally the security policies detail how each new machine comes into being in the organization, from the business justification for the machine to what security measures that machine requires. Host based measures should be driven by the simple question "What is the data worth?" Even if the answer is nothing the security for that machine should include a recovery plan and a lockdown of any software on the machine to prevent it from being used as an attacking tool. For the machines that do have data that needs to be protected, they need to have backups and disaster recovery plans in place to minimize any outage and those plans need to be tested on a scheduled basis. Some of the minimum requirements are: Backups, host based IDS like Tripwire, Anti Virus software, removing unused services and documentation which should include the following: Who should have what access for what purpose, disaster recovery plan, modifications to the standard application installation, OS modifications, i.e. patch level, any special hardware configuration, what the purpose and business value of the machine is and it's vulnerability profile. Host based security also provides protection against

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

internally originated probes/attacks. Whether a successful penetration of the perimeter defenses or a disgruntled/inquisitive employee, many attacks still originate internally, another reason for the layered security model.

Quick List

| | | |
|---|---|---|
| Host IDS | OS Patches | Application Patches |
| Remove Unneeded Services | System Build Documentation | Redundancy/DR Plan |
| Local logon | Physical Access | Network access |

## *NETWORK*

Most of the network protection should be provided by other pieces of the layered model. The primary network item is Intrusion detection or IDS. While some may say that IDS is dead I totally disagree. You don't not buy and alarm system for your house because it doesn't go off until they've broken in do you? Properly configured and monitored IDS allow multiple opportunities to learn about what is going on in your network. How do you know they have broken through the perimeter if you don't monitor the network? While host based IDS focuses on the most valuable of your systems, network IDS (NIDS) should be configured to monitor the most likely break in points on your network as well as just outside those break in points. Placing your NIDS around your most likely break in points will maximize the return you get on your software/hardware expenditure. Placing NIDS outside allows you to gather information on what attacks are prevalent or where they are coming from so that you can take a proactive approach. Staying ahead of potential problems allows time to do research on the prospective vulnerabilities and to determine the best way to lock down your systems while minimizing any impact on your own customer base. One of the misconceptions about IDS is that you can just set it up and forget it. This is hardly the case, as attacks continuously change the IDS must be monitored and modified to adapt to the threats. One of the more tedious jobs but essential to proper security. Another key component is proper access control. This aspect requires Authentication, Authorization, and Accounting (AAA) capability. Currently there are three preferred methods: Tacacs+, Radius, Kerberos. Which is the best solution will depend on your infrastructure. AAA brings a centralized administration of accounts for a variety of platforms including routers, switches, firewalls and the typical network logons as well as the possibility of multiple NOS logon capabilities. The latter possibly bringing your organization closer to the holy grail of single sign-on. Many devices enable levels of access through AAA instead of the standard all or nothing access that was previously standard. AAA servers are available from a variety of venders so you should be able to find a solution whatever your organizations preferences. Lastly, ensure port security. An open live network port allows unauthorized network access. Turn off all unused ports and setup the port so they will only allow the proper MAC card to connect. While this will result in a little more overhead it will result in a more accurate network diagram as well as reduce troubleshooting time when things go

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

wrong with a specific NIC or system, or when and unauthorized system attempts to connect.

Quick List

| | | |
|---|---|---|
| Network IDS | AAA | Physical Device Access |
| Physical Port Access | Network Audits | Network Diagrams |
| VLANs | MAC to port mapping | Configuration Backups |

## *PERIMETER*

Perimeter is anything that sits between the inside and the outside. Some of these components will be obvious others you may not have thought of, firewalls, phones lines, wireless access points, Email, Web, Name services, floppies, CD ROMs, USB, etc. Typically people only think of the firewall as the way in or out of the network but each of the items mentioned above can provide access to the internal portion of your network. Modem and wireless connectivity to your network needs to be tightly controlled and monitored. Modems allow machines that typically don't warrant protection by host IDS software to be attacked and possibly taken control of with little ability to detect this attack. Once the system has been subverted the attacker can continue to improve their access by subverting other systems, hopefully your NIDS will pick up this activity. While it may take a while to determine attack points presented by the presence of modems, wireless access points provide an even greater challenge to identify and secure. Many capable wireless devices can be purchased cheaply at the local computer store and are fully functional once plugged into the network. Many are not even protected because the default configuration allows maximum access. They are typically rogue network connections created by a power user employee knowledgeable enough to set one up but not knowledgeable enough to secure it or even knowing it should be secured. When designing wireless networks ensure to use VPN and encryption technologies as well as implementing a firewall capability between the network and wireless access point. As far as Email, Web and Name services, any systems that will interface with the outside, either Internet or directly to another companies network should be protected by being placed in a semi-protected network area, a DMZ. A DMZ is a network area that has a firewall presence at each entry to the protected area. This DMZ approach allows a significant reduction in exposure as traffic transits the external firewall and the additional protection, if the traffic should be inbound to the internal network, by passing through the internal firewall. All systems in the DMZ should be locked down to the maximum extent possible and be protected by Host IDS; the network should be running a NIDS as well. Removal or reduced capability for any remote access software, Telnet, Terminal Services, VNC, as well as GUI, Xwindow software for Unix systems, should be seriously considered for systems in the DMZ. As this will be the area of highest exposure for your network it makes sense that the security should be maximized at the DMZ. One other entry point to your organizations network is all those portable drive/disk devices. While inadvertent exposure will occur through virus-infected diskettes or

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Trojan Horses introduced via USB, portable drives and diskettes, these should be minimized by proper installation and configuration and an enterprise wide anti-virus solution. Intentional introduction is another issue altogether and limiting their use has to be balanced with the needs of your organization. Just as these access points are ways into your network they are also ways out. Care must be taken to ensure that corporate policies appropriately cover their use.

Quick List

| | | |
|---|---|---|
| Wireless LAN Security | DMZ/Internet presence | Firewalls |
| NAT | Audit Plan | Configuration Backups |
| PBX Security | Independent, Redundant Internet Connectivity | |

## *EXTERNAL*

Many organizations just block anything they don't want to have access to their network, but if you don't have something watching the outside so that you can be aware of the potential problems you will only be able to react after they have gotten in. Wouldn't it be better to take action before they figure out how to get in? This typically involves Network based intrusion detection, but can also include things like honey pots, systems specifically setup to draw an attackers attention. Properly managed honey pots can provide significant insight to what attacks are prevalent. Since security is such a volatile environment security professionals must continually pursue additional knowledge to protect their systems and using external information gathering tools, like honey pots, can contribute to that requirement.

Quick List

| | | |
|---|---|---|
| Network IDS | Honey Pots | |

## *TOOLS*

Security professionals are judged by what tools they know how to use. While there are many out there, you need to get a handful that focus on your primary responsibilities and become well versed in them. While many organizations are unwilling to use free tools as a standard you may be able to use them for training/familiarization or as a backup to the highly priced commercial tools. In the references section I have included a link to insecure.org's Top 75 Security Tools article. It's an excellent resource for any security administrator, new or seasoned. I highly recommend becoming familiar with as many tools on this site as possible. Many tools are double edged; they start as "Hacking" tools and are picked up by a security administrator to understand more about the weaknesses of their systems. Something to keep in mind as you practice with these tools, either practice on an isolated network or get written permission prior to running them. Then run them on an isolated network until you are proficient. Some of these tools will generate a significant amount of network traffic flow or set off any network/host detection alarms you may have installed. Some of the different

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

methods of these tools use are active, where the tools does something to find out information, and passive, where the tool just collects packets to gather information. Examples of active tools are: SAINT, Nessus, which are vulnerability tools. Examples of passive tools are: Snort and Ethereal, which are both packet sniffers. While Snort fills an IDS role by gathering up the packets and trying to determine if there is any fowl play on the network, Ethereal collects the packets allowing an administrator to view and manipulate the data as necessary. The ability to view packet data is a must when troubleshooting a variety of network problems so these tools come in doubly handy. Also be aware of how your tools communicate like SSH vs. telnet, for example telnet passes information in the clear and SSH doesn't.

Quick List

| | | |
|---|---|---|
| Network Scanners | Sniffers | IDS |
| Secure remote tools (like SSH and SFTP) | Password Checkers (Unix, NT, others) | Service/Support Contracts |
| Pagers/ Cell Phones | | Monitoring Software |

## *DOCUMENTATION*

You've heard it over and over, No job is complete until the paperwork is done! If making your job easier wasn't motivation enough think of documentation as skills documentation. What? Sure, take your documentation to your boss so they can see the great job your doing, or a sanitized version to a prospective employer to show them what a great job you can do for them. Proper documentation will result in reduced troubleshooting and down time in the event of a problem, provides for good pass down to lower skilled or newer employees, serves as an excellent disaster recovery document, and can serve as an excellent tool to ensure that all security aspects have been covered.

Quick List

| | | |
|---|---|---|
| System Build | Disaster Recovery Plan | Network Diagram |

## *APPLICATION*

Much of the security requirements currently required could go away if software developers wrote secure code. Maybe a better title for this section would be software because I include operating systems in this area. The Department of Energy recently placed a security requirement on software developers before they will buy their product. Most of the security for this has already been discussed in the host section, but there are a couple things you can try to do. If your organization writes code try to get involved in the process try to emphasize the value vs. just the cost of better security. If your organization buys software try to influence the purchase toward more secure software. As an administrator all you can do is stay on top of the OS and application patches.

Quick List

| | | |
|---|---|---|
| Security Patches | Secure communications | Data Encryption |

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## *DATA*

Your data should be fairly well protected by proper access policy, host based security, backups, etc., but one thing that might be beneficial is encryption. Encrypting the data can reduce the exposure of data being stolen as well as providing a method of exchanging data over the Internet. Encrypting data is resource intensive so only systems that are evaluated as having sensitive data or proprietary data should be considered for encryption as a matter of course. Data that will be transiting the Internet should routinely be encrypted either directly or via a tunnel established between two endpoints (Virtual Private Networking, VPN.) Creating a VPN allows organizations to reduce costs by utilizing network connectivity already in place via the Internet. As network traffic leaves the network it is encrypted by a VPN end point and sent to another VPN end point to be decrypted and placed on that organizations network. If your organization only has an occasional need to encrypt data you should consider one of the software products that do that, like PGP. Encrypting data also protects against internal prying eyes as well as the possibility of stolen or lost hardware, like laptops. Of course a determined attacker will be able to use any and all tools in their arsenal with time not being a factor if the are able to get physical access to your hardware.

Quick List

| | | |
|---|---|---|
| Drive Encryption | Communication Encryption (VPN) | File Permission |

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

## *Executive Summary*

Information Technology security is a balance between cost, usability and protection level. One of my favorite questions is “What is your data worth?” That is the question that should be answered for every bit of data on every piece of equipment. Is the CEO’s schedule worth something? It certainly can be, anyone who can see the executive assistant’s monitor can capture that information. With that in mind a little bit of paranoia can be a good thing. The best way to achieve the proper level of security for your organization is to have a solid vision of where you want to be and what your willing to spend to get there, also known as your security strategy. Taking the time to define your organizations goals will allow you to take advantage of the synergy offered by a well planned and executed layered approach to IT security. Once the goals have been set, policies need to be defined and the example set from the TOP down. This top down approach cannot be underestimated. “Most employees want to impress the boss, so they will bend over backwards to provide required information to anyone in power.” (Granger) Once the strategy and policies have been documented the how or procedures must be addressed. A layered approach to security based on your organizations strategy and policies allows significant cost savings due to the synergistic effect of complimentary technologies. No “SILVER BULLET”, “over 90 percent of fortune 500 companies have detected breaches even with firewalls deployed.” (Recourse Technologies) You can have the best firewall that money can buy but if the attacker can gain physical access to an important device or come in through an unprotected wireless access point then you end up with a net effect of NO security. "This dispels one of the popular security myths: that a company can focus only on securing its perimeter and remain secure." (Hulme) Each of the areas below should be addressed to ensure your organization is protected to the level that you desire.

1. Social
2. Physical
3. Host
4. Network
5. Perimeter
6. External
7. Tools
8. Documentation
9. Application
10. Data

You will find that significant savings can be realized by properly addressing each area thereby reducing over expenditures in others. For example a proper corporate security mindset, if you don’t have a badge you don’t belong here, may eliminate the need for security guards at the entrance. Another example is managers that expect special treatment, many social engineering techniques that take advantage of executives not following the security policies established as

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the standard, by establishing policies that prevent or reduce this tendency you will reduce exposure to these attempts. The best protection against “Social Engineering”, which is the process of gathering information or access by taking advantage of people’s natural desire to be helpful, is to have well defined security policies that employees are very familiar with through recurrent training so that everyone knows what is expected and what the repercussions are for failure to comply.

Physical
Preventing access to IT equipment through proper physical security is critical to protecting your infrastructure. Physical access to the equipment allow an attacker to outright steal data, running attack tools against the device or physically disable it as well as gather information about your network. Since the physical security manager is not typically and IT person, one the of the IT security personnel needs to be involved in the physical security process.

Host
Host based security focuses on the host itself. Ideally the security policies detail how each new machine comes into being in the organization, from the business justification for the machine and what security measures does that machine require. Even if a machine doesn’t have any data it should be secured to prevent it from being used as an attacking tool.

Network
Most of the network protection should be provided by other pieces of the layered model. The primary network item is Intrusion detection or IDS which will provide an alert mechanism should your perimeter be compromised. Properly configured and monitored IDS allow multiple opportunities to learn what is going on in your network. How do you know they have broken through the firewall if you don’t monitor the network? “Since almost 80 percent of cyber-attacks on companies are perpetrated from an inside source, NIDS is critical. Although it is an “after-the-fact” measure, it keeps damage to a minimum.” (Young) The same goes for host protection.

Perimeter
The perimeter is the area where data crosses from your network to someone else’s, typically across a firewall but it may have other paths like through modems, wireless access points or a variety of portable media. Things to consider: Ensure security policies cover the use of Wireless Technology, portable storage technologies like floppy disks, USB attached devices, PDA’s and modems.

EXTERNAL
You need to have something watching the outside so that you can be aware of the potential problems and take action before they figure out how to get in. While

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the tools to do this should already be implemented at you organization the management direction to implement this philosophy may not.

TOOLS
Provide the proper tools and the training to use them. Training is critical to have a successful security team. Training is one of those items that the earlier you get it the longer you can take advantage of its benefits. Training of the users can substantially reduce exposure to social engineering attacks. The key here is once the corporate security policy is established buy the software and hardware to support that level of security.

DOCUMENTATION
Insist on proper documentation. It will reduce the hours required to maintain as well as restore the equipment. To often the crisis of the day is given priority by management, proper documentation will reduce the crisis of tomorrow.

APPLICATION
Much of the security requirements currently required could go away if software developers wrote secure code.

> The department of energy has done something unusual for a federal agency. It has become an example of excellent cyber-security practice. It has done this by pressuring Oracle to elevate security in its 9i database product—in the process, taking software out of the shadows of "as is" licenses and putting it in the spotlight of a government procurement action. DOE's action could begin a process that improves the security of the technologies available to the public and private sectors alike. (eweek)

Things to consider: If your organization writes code try to get involved in the process try to emphasize the value vs. just the cost of better security. If your organization buys software try to influence the purchase toward more secure software.

DATA
Your data should be fairly well protected by proper access policy, host based security, backups, etc., but one thing that might be beneficial is encryption. Encrypting the data can reduce the exposure of data being stolen as well as providing a method of exchanging data over the Internet.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Security Quick List

| | |
|---|---|
| Corporate Security Policy | Employees Security Training Plan |
| Intrusion Detection (IDS), Host and Network | System Risk Management documentation |
| Disaster Recovery Plan | Firewall |
| Anti-Virus Plan | Audit Requirements |
| Remote Office Connectivity (VPN) | Internet Presence Redundancy |
| Physical Security Requirements | Wireless Policies |
| Modem policies | Portable storage policies |

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

# References


Alberts , Christopher J. Dorofee, Audrey J. Allen Julia H. "OCTAVES Catalog of Practices, Version 2.0" October 2001
http://www.cert.org/archive/pdf/01tr020.pdf 25 October 2003

Bois, Justin "Protect Yourself" 4 April 2002
http://www.sans.org/rr/papers/index.php?id=271 26 November 2003

Cisco Systems, Author Unknown "Action Steps for Improving Information Security" http://www.cisco.com/offer/tdm_home/pdfs/vpn/roi5_wp.pdf 13 October 2003

Coffee, Peter "Broad Security Focus Is Critical" eWeek.com 13 October 2003
http://www.eweek.com/article2/0,4149,1335392,00.asp 15 October 2003

Danchev, Dancho. "Building and Implementing a Successful Information Security Policy" http://www.windowsecurity.com/pages/security-policy.pdf 7 October 2003

Fyodor "Top 75 Security Tools" 1 December 2003
http://www.insecure.org/tools.html

Granger, Sarah "Social Engineering Fundamentals, Part I: Hacker Tactics" 18 December 2001 http://www.securityfocus.com/infocus/1527 25 November 2003

Granger, Sarah "Social Engineering Fundamentals, Part II: Combat Strategies" 9 January 2002 http://www.securityfocus.com/infocus/1533 25 November 2003

Hulme, George V. "How Hackers Break In To Enterprise Networks--A Step-By-Step Demo" InternetWeek.com
http://www.internetweek.com/shared/printableArticle.jhtml?articleID=14700217
13 October 2003

Mitnick, Kevin "My first RSA Conference" 30 April 2001
http://www.securityfocus.com/news/199 25 November 2003

Pescatore, John; Stiennon, Richard; Allan, Ant "Intrusion detection should be a function, not a product" 13 October 2003
http://techrepublic.com.com/5102-6298-5078279.html 15 October 2003

Ranum, Marcus "HOLY TOOL BELT, BATMAN! A smorgasbord of free tools for no-nonsense security administration." August 2003
http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss21_art103,00.html


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Recourse Technologies, Author Unknown “Intrusion Detection: Reducing Network Security Risk” December 24, 2001 http://www.isp-planet.com/perspectives/ids.html November 24, 2003

Rooney, Paula “Microsoft's Muglia Details 'Securing The Perimeter' Initiative” 8 October 2003 http://www.crn.com/sections/BreakingNews/dailyarchives.asp?ArticleID=45000

Unknown Author “Security: A Federal Case” October 6, 2003 www.eweek.com/article2/0,4149,1307596,00.asp

Unknown Author, Cisco “Cisco IOS Security Configuration Guide“ http://www.cisco.com/application/pdf/en/us/guest/products/ps1835/c1069/ccmigration_09186a008011dff4.pdf

Young, Charlie. “Hacking through the Firewall Myth: Think You're Safe? Think Again.” http://www.itinsight.net/idc/pdf/02-1001_Hacking.pdf 14 October 2003

Harris, Shon All in One CISSP Certification. Chicago: McGraw-Hill/Osborne, 2002.

Beach, G. “Beware of the Telephone” CIO 1 October 2003 http://www.cio.com/archive/100103/publisher.html

Ali Pabria, Uday 0. “Enterprise Security Strategy.” Certification Magazine November 2003:48-49

Alexander, Bruce and Snow, Stephen “Preparing for Wireless LANS” Packet Magazine October 2002:36-39

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: April 30th, 2017

# Upcoming Training

Click Here to
{Get CERTIFIED!}

| | | | |
|---|---|---|---|
| SANS Riyadh 2017 | Riyadh, Saudi Arabia | May 06, 2017 - May 11, 2017 | Live Event |
| SANS Security West 2017 | San Diego, CA | May 09, 2017 - May 18, 2017 | Live Event |
| SANS Northern Virginia - Reston 2017 | Reston, VA | May 21, 2017 - May 26, 2017 | Live Event |
| SANS Melbourne 2017 | Melbourne, Australia | May 22, 2017 - May 27, 2017 | Live Event |
| SANS London May 2017 | London, United Kingdom | May 22, 2017 - May 27, 2017 | Live Event |
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| Community SANS Boise SEC401 | Boise, ID | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| Community SANS Philadelphia SEC401 | Philadelphia, PA | Jun 19, 2017 - Jun 24, 2017 | Community SANS |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |