Global Information Assurance Certification Paper

Ronald Wayne McClellan
GSEC v1.4 Practical
ID ronmac0002
Re-Submission
SANS San Antonio

Security In-Depth

The Problem

There are more and more companies connecting small offices together using the Internet without taking the proper precautions to ensure the integrity of their information. So many companies are taking their small private networks and connecting them to the Internet to communicate faster and easier with their customers. This document describes the problems associated with taking those small private networks and connecting them to the Internet without the proper security features.

Introduction

This report details the logic for implementing information security in-depth practices into network architecture. Today, more and more companies are connecting offices together using the Internet; this opens up a new threat to small companies that they are not setup or staffed to handle. This can be a costly and rigorous venture to undertake, due to the necessary changes that must be made both in hardware, software and personnel training.

With the increasing number of Internet and Network vulnerabilities and incidents that are occurring, the likelihood of having an information security problem is growing rapidly. There are no definitive fixes to protect against hackers with the exception of disconnecting from the Internet, but that is not easy to do in this information age. However, there are many steps that can be taken to guard against those attacks. As with all major projects the key to success is planning. One of the main issues with security is knowing the risks as they pertain to your network, so you will know the extent of protection you will need. This process is called Risk Analysis and will determine the steps you take to protect your network and to limit the impact of an attack.

Impacts can range from malicious code that can be disruptive and destructive such as Viruses, worms, Trojans and backdoors. Depending on the results of your Risk Analysis, the fix could be as easy as installing Anti-Virus Software. If some cases your Risk Analysis might dictate stronger measures to protect against these risks. In such cases a combination of routers, firewalls and specialty computer systems can be used to create a barrier between your sensitive networks and the Internet. These types of software and hardware put together can make an excellent defensive line against these types of attacks. The combination of these two preventive measures would be deployed as the first phase of securing the networks.

While some malicious code can be destructive to your network, most are only disruptive, but can be easily protected by Anti-Virus software. The larger risks to networks are hackers with malicious intent. There are several steps that can be taken to protect against hackers. One such defense would include additional systems being deployed on the network to monitor network traffic, these devices are commonly referred to as Intrusion Detection Systems (IDS). These systems detect attack signatures in near real-time and can take action to defend the networks by either alerting the network staff or by sending commands to the firewalls and routers to block the suspicious activity.

Finally there are new viruses and vulnerabilities being found each and every day. As hackers and malicious code writers get more advanced, so must out defensive systems. Security is not a one time quick fix, it requires due diligence to stay one step ahead of the next virus or

vulnerability. CNN correspondent Ann Kellan reported "Computer hackers breaking into government and corporate computers is estimated to be a $10 billion-a-year problem.[1]" The alternative is to wait until an incident occurs, but that could be catastrophic.

Information Systems and Security Planning

The economic analysis was discussed in the executive summary and will be discussed in detailed in the organizational impacts section. The upfront costs of setting up the office with security in mind will be a little higher, but the savings in the long run far exceed those costs. This will also reduce the upgrade costs and lower the costs when adding additional security hardware and software in the future.

As an example, adding simple Anti-Virus software is an excellent return on investment. The chart below shows the statistics of viruses from the past year, Anti-Virus software could have blocked almost all of these, saving countless man-hours and dollars from recovering from an infection. The Chart shows percentage, but a better understanding comes from the simple numbers, according to RAV[2], there were 300542 occurrences of the Klez virus in the last week and 40386 occurrences in the last 24 hours.

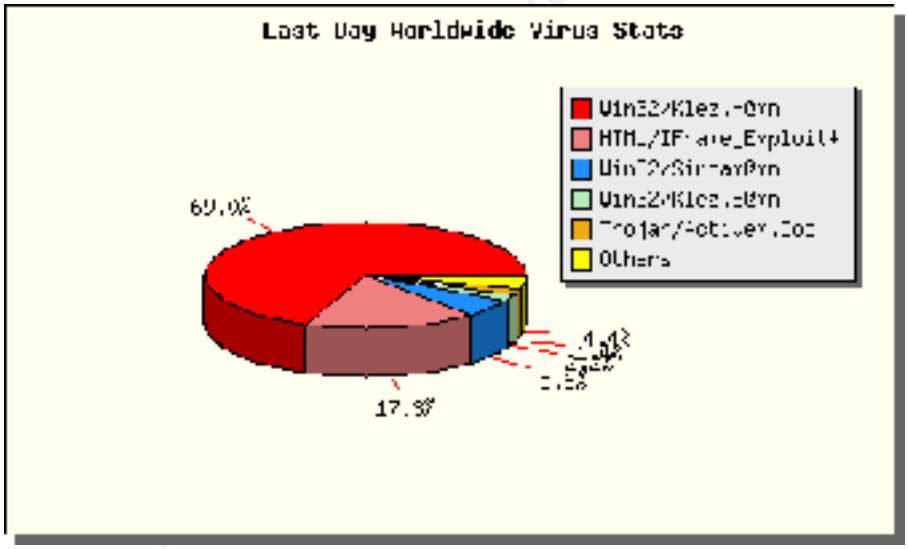


Chart 1: Virus Statistics [3]

It will be necessary to do a resource analysis to ensure that all equipment is ready prior to proceeding with each phase of the operation. This should follow a set timeline and match up with the operational schedule, so that the upgrade will not cause an interruption to ongoing operations.

[1] CERT Coordination Center, Carnegie Mellon University, 6 April 1998
"CEOs hear the unpleasant truth about computer security"
[2] Reliable Anti-Virus (RAV), Copyright date 1999-2002 "VIRUS STATISTICS"
[3] Reliable Anti-Virus (RAV), Copyright date 1999-2002 "VIRUS STATISTICS"

The key to accomplishing this upgrade will be the technical analysis and a good Risk Analysis. There are several major implications in connection a private network to the Internet, least of which is the technical issue of just the physical connection. Each phase of the project should involve managers, administrators and a qualified security engineer. After each phase an operational analysis should be conducted to ensure that there were no impacts from the upgrade and to review the next phase of the upgrade.

Organization Impacts

The major impact to the organization is actually not from taking steps to secure the networks but from not taking these steps. The actual impact of adding security features into the network is minor with the proper planning and preparation. The upgrades can be done during none critical times and can be phased in to avoid causing problems. But the impact can be major if these steps are not taken and the network is hacked. The losses can come from lost Internet sales, lost or corrupted data and losing proprietary business data that could allow your competition to get an unfair advantage.

The following tables will show the costs and trends of not being prepared for an information security attack. Table 1 proves that the costs of adding security features into the current network are both beneficial and cost effective compared to the costs to recover from an incident. As the table shows the cost of a single web site compromise in 1998 was $70,000, with the increased sales that are being conducted on the Internet, this figure today could easily be two or three times that amount if you are not protected.

Time Line	Attack Information	Costs (protection/recovery)
1995	GAO estimates 250,000 unauthorized efforts in 1995	Not Released
1996	Pentagon Reports 25,000 attacks	$10 Billion
1997	50% of companies experienced more than 30 penetrations	Up to $10 million per Case
1998	Single NASA Web Site Hacked	$70,000 $10 Billion for DOD

Table 1: Hacking Costs [4]

Table 2 shows the increasing number of security incidents that have been reported. These numbers are low, due to the fact that banks and other financial institutions do not report incidents, so these numbers could actually be approximately 25-50% higher. If incidents continue on the current pace, the total for 2001 will be surpassed by the end of the second quarter of 2002.

[4] Attrition.org, Not Dated "Errata: Statistics"

Year	1993	1994	1995	1996	1997	1998	1999	2000	2001	2002 (1st Qtr)
Incidents	1,334	2,340	2,412	2,573	2,134	3,734	9,859	21,756	52,658	26,829

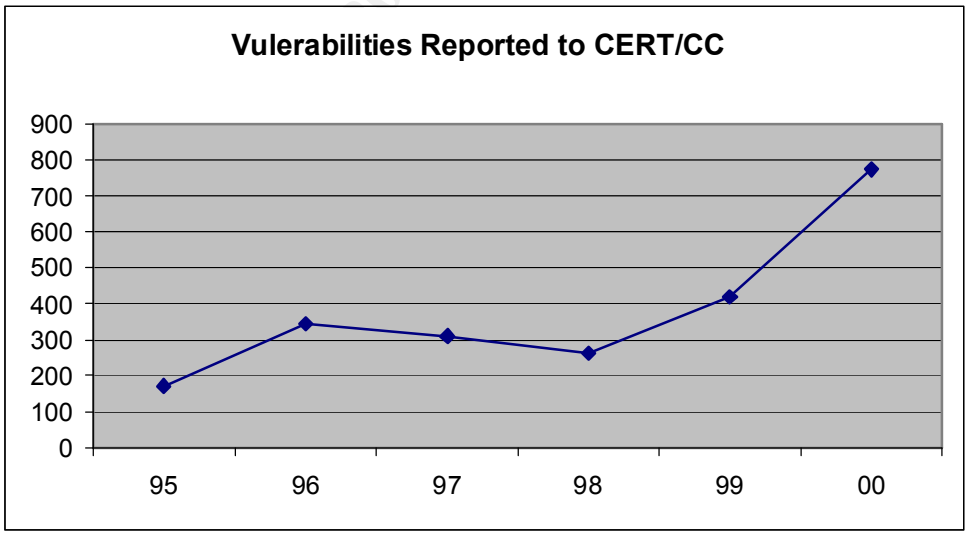
Table 2: Hacking Incidents Timeline*[5]

**Please note that an incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time.*

There were incidents that occurred that directly caused several companies to completely collapse due to the information and consumer trust that was lost. As you can see from the statistics in the tables above, the cost of deploying network security devices can save a great deal of time and money. For a small to medium organization, the simple addition of a firewall can be accomplished for under $5000 and will offer a great deal of protection. Even with the number of incidents climbing higher all the time, it is keeping with the growth of networks connecting to the Internet. From my experience in computer security, there is no total protection from hackers, but by taking small steps to secure your systems; it will lead hackers to look for an easier target.

Future

Computer and Network Security are both ongoing battles that require constant review and updates. The number of vulnerabilities reported is growing every day and that does not account for the ones that hackers have found and not reported. Graph 1 shows why it is important to stay on top of computer security. As the information that I have presented shows, the problems that face businesses on the Internet are not going away, so how does your organization manage the risks.



Graph 1: Vulnerability Growth[6]

[5] CERT Coordination Center, Carnegie Mellon University, 6 April 1998 "CEOs hear the unpleasant truth about computer security"

Methods of Protection

There are many tools available that can aid in securing your networks. Before I discuss these tools, it should be made clear that some of the more advanced tools require a certain level of expertise, if used incorrectly, your business could be left with a false sense of security. For example, installing a firewall may be a good step for your business but if the right rules are not set, the firewall might not be fully protecting your business. With that in mind there are companies that will come into your business, do a threat analysis and make recommendations to secure your networks. Most of the companies also have the expertise to install and configure any security devices that your business may require. Finally, in evaluating your business needs for security software and hardware, especially smaller businesses, you should find out what protections that your Internet Service Provider (ISP) provide.

Before I go into the tools that are available to aid in protecting your systems, I have to cover what I see as a major for the networks that I deal with on a day-to-day basis. A lot of exploits that are being taken advantage of today would not have happened if the security update or patch were applied. I know that a lot of people have looked at Microsoft's Outlook software as being a villain with some recent exploits. They are not completely wrong on some points but I would have to say that half the systems I have scanned during my normal work were missing patches from 6-12 months ago. This tells me that a major problem is with administration of machines; patches, hot fixes, and updates are not being applied in a timely manner. As my grandfather always told me, "An ounce of prevention is worth a pound of cure".

Of late, one of the biggest problems facing companies on the Internet is computer viruses and worms. While this is a large problem, it has a relatively cheap and inexpensive answer. Installing Anti-Virus software can defeat most of these problems with very little knowledge or expertise required for the basic packages. For some of the larger corporate companies, there are additional Anti-Virus packages that can run on your servers and which allow your administrators to ensure that virus definitions are kept up-to-date. One of the biggest short falls of Anti-Virus software is that users do not keep their definition up to date; most Anti-Virus software vendors provides updates on a weekly basis. This allows for the newest virus definitions to be used on your systems, which usually includes variants of some older viruses. It is up to each business to decide the level of Anti-Virus protection that is right for them.

For some companies Anti-Virus software might be enough, but for larger companies or companies that need more security, the next step is adding a firewall. A firewall is a powerful defensive tool for protecting your networks. That said, it could also give businesses a false sense of security as mentioned above. A firewall can lead an administrator to think that he does not have to apply patches when they come out because it is behind a firewall. This really fits into the security in-depth concept, for example if your business is a web based company running web servers on your network, then your firewall is more than likely allowing port 80 (http service, i.e. web traffic) through. If your system is hit with a port 80 attack the firewall will probably not stop the attack.

[6] CERT Coordination Center, Carnegie Mellon University, 6 April 1998
"CEOs hear the unpleasant truth about computer security"

There are several types of firewalls available and it really takes an expert to determine what your needs are. There is no need to spend up to $25,000 for a firewall when you do not need that level of protection. It is more cost effective to pay a professional to come into your business and do a review of your needs and to recommend what will be most effective for your particular circumstances. Firewalls generally fall into two categories, the first being an application-level firewalls (sometimes referred to as proxies) and the second type being network-level firewalls (such as packet filtering). There are subsets of these two categories such as stateful and stateless, but those are beyond the context of this paper. A simple proxy firewall allows a great deal of protection and limits your exposure to the Internet. Hackers use random port scanning tools to find targets and in a normal network your company might have 20 or more machines that the hackers might find with these scanning tools. However, if you were using a proxy-based firewall, you could only have one address that the hackers could possibly find. This is due to the fact that the firewall can mask your machines behind it by using network address translation (NAT) to limit your Internet exposure. This basically works using the firewall as a go between for your Internet activity; from your machine you can request a web site and the firewall will process your request. The firewall takes your request, receives the information from the website and then forwards that information to your machine. Through this process it looks like your network only consists of one machine but in reality could consist of hundreds. This will sometimes be referred to as security through obscurity.

The second type of firewall is the network-level firewall and it can actually examine the packets of information sent at the transport level to determine whether or not a particular packet should be blocked. This is where having a qualified person configure your firewall is crucial, because a bad rule could either allow someone in that should not have access or it could stop some critical information from being transmitted. When used correctly this type of firewall can examine weather information should come into your network, it can do this based on weather the information was requested by someone on your network or by any predefined rule. This type of firewall can be extremely hard to configure and maintain.

In most larger companies there are usually one or more routers; these can usually also be programmed or configured in a way to add to your networks' security. Routers can be set up to determine what protocols and the types of traffic to forward. Remember that security in-depth takes in account several different layers of protection, just because something may be blocked by the firewall does not mean you can't still block it at your routers. Sometimes this can also aid in the work load that is placed on your firewall, if the router is blocking traffic of a certain type that is one less rule or packet that the firewall will have to process.

For some companies there is the need for even further security features. The next step a business might consider after a firewall is an Intrusion Detection System (IDS). As with firewalls there are two major types of IDS systems, the difference is that these two types can be used in conjunction with each other. The first type of IDS is a host-based system, which is a piece of software that is installed on each and every machine that you want to monitor. For the networks that I work with, I usually only use the host-based IDS on critical machines, usually only on my web servers, file servers and any other sensitive machine. The advantages of a host-based system is that it can watch all of the communications that are coming in and out of a single machine and that it can also monitor critical system files for suspicious activity and modifications.

Some security professionals, as well as myself include personal firewalls into this category. Certain types of host-based IDS systems can report back to a centralized management position, this type of IDS is usually referred to as an agent-based IDS package. For smaller networks the personal firewalls are economical and can handle your security needs, but for larger networks the agent-based system is the way to go for the ease of management and incident response.

Network based is the second type of IDS system. Network based IDS systems are usually placed strategically throughout a network to monitor network traffic. A network IDS can watch traffic for signs of network attacks, misuse and suspicious activity. I said earlier that network and host-based IDS could work together; there are some products that allow both network and host sensors to report back to a single management position to track all activity. This combined information can usually give the administrator a broader picture of what is actually going on in a network.

Once the network based IDS picks up an attack signature or suspicious activity, most have the capability to alert the appropriate personnel either through pagers or email messages. Messages are also sent to the management console and a full log of the incident can be logged on the console as well, some IDS allow for raw coping of the data. This means that every packet of the activity is stored so that it could be played back at a later time if necessary; this data can be very helpful for forensic analysis. Also some IDS systems have the capability to take action to stop an event from happening, sometimes this could include offensive type actions. There is nothing wrong with dropping connection from a hostile site, but I would not recommend any of the offensive actions, in most cases the attacks could be coming from an innocent intermediary. As with firewalls the policies (rule sets) can be a burden to build and require constant monitoring and revisions.

IDS systems do not have to expensive at all, I have avoided talking about specific tools so that I do not create a bias one way or the other, but Snort IDS[7] is a freeware IDS systems. Snort is an open source tool that is constantly being revised and updated. I have used Snort in the past and it is a very strong IDS system.

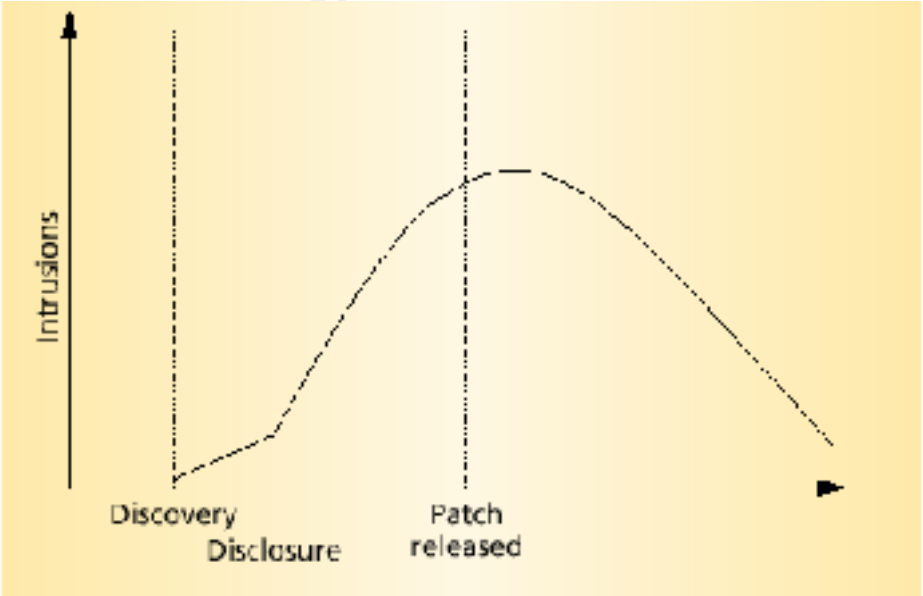
Lastly there is discussion of a third type of IDS system that is being discussed by some professionals in the security field. The one problem that cannot be overcome by a firewall or an IDS system is new vulnerabilities, because a firewall cannot detect something that it does not have a rule for, the same is for true of an IDS. If the IDS does not have a signature for a specific attack, it does not know how to process the data, some might report the data as suspicious but that is usually the extent of what it can do. So the future of network protection is Anomaly Detection Intrusion Detection Systems (AD-IDS)[8], these systems detect attacks by looking for network traffic that is not normal for your network. While AD-IDS systems are still in the early stages of development, they definitely could aid in the detection of new and undocumented vulnerabilities and attacks.

[7] Brian Caswell and Marty Roesch, Copyright © 2002 http://www.snort.org/
[8] By Marcus J. Ranum, CEO, Network Flight Recorder, Incorporated, Copyright date 1998 "Intrusion Detection: Challenges and Myths"

In most companies the types of traffic and network activity are pretty much the same each and every day. This allows an AD-IDS system to learn what types of traffic is normal for your network, when an AD-IDS is installed it starts learning about your companies communications patterns, types of network traffic and even when you network loads rise and fall. This information can be analyzed to form a baseline for your network activities and then the AD-IDS can pickup on anything that is not normal for your network. It then has pretty much the same options available as the other types of IDS systems that we have discussed.

The short falls of AD-IDS are that most large network have a hard time defining what is normal network traffic, as networks get larger and busier the traffic becomes very random. An AD-IDS is also very time consuming with false positives, especially as it is going through its learning process, which can takes several months to complete. That said normal IDS systems have their share of false positives. There is still a great deal of research being done in AD-IDS, but it is not a finished product yet and by no means is it going to be the silver bullet for all of our security needs.

The reason that AD-IDS is becoming a more popular idea is due to the fact that there is a lag time between when a vulnerability is discovered, then announced and then finally fixed. Graph 2 shows that there is usually a period of time between when a vulnerability is discovered and then patched. What usually happens in between the discovery and patch, is Anti-Virus and IDS vendors are working on a signature file to identify the attack that is related to the vulnerability. An AD-IDS system should pick up on the vulnerability in the very early stages of this process and provide your company with some level of protection prior to the release of the update for your IDS or Anti-Virus program.



Graph 2: Vulnerability Cycle[9]

[9] William A. Arbaugh, William L. Fithen, and John McHugh, December 2000.
(footnote continued)

I have discussed some of the most commonly used security tools that are available to protect your organization and which through them at a very basic level to provide the essential information that you need to make informed decisions. I still recommend contacting professionals to aid in picking the right tools for your situation, because this information is changing at a fast pace. Remember a none of these tools are a cure-all for all of your security problems, but the right combination of these tools can place you on the un-appetizing list for hackers.

Conclusion

As the charts and statistics show, it imperative that network security is a key point when planning to connect your networks to the Internet. The information provided above shows that not taking security into account when connecting your network to the Internet could be a fatal mistake. As stated before smaller businesses should make sure to account for all the threats mentioned above before they take steps to connect to the Internet. Otherwise, expanding your business through the Internet could be the end of your business

The diligent management of security is essential to the operation of local-area networks, regardless of the size. It's important to point out that absolute security is an abstract, theoretical concept and does not exist anywhere. The only completely safe computer is one that is not networked to anything. No one wants to risk having his or her data exposed to the casual observer or open to malicious mischief. It should be clear from the discussion above that the costs from being a victim of network attack could be astronomical and could be the end of your business. Steps can and should always be taken to preserve network security and integrity.

I discussed several types of tools that are available to add security to your networks, each one providing a layer of protection. The concept of having multiple layers of security has been around since the legends of Knights; the Castle was strong and built of rock but still had a moat to surround it, that idea still holds true today. If your network is protected as several layers, if one layer fails it does not bring your network down with it. When it comes to security I have always thought that if you take the logical steps to protect your systems, if nothing else you have made the company that didn't look like a much easier target.

As a closing thought, two years ago, the first Distributed Denial of Service (DDoS) attack took place. This attacks took down large major technological businesses such as Yahoo, eBay, Amazon.com, Buy.com, ZDNet, CNN.com, E*Trade and MSN.com. These businesses had all the security features and the personnel in place to keep their systems up and running. Still all these sites were still shutdown for hours at a time, some repeatedly. As a result of these attacks the traffic across the Internet slowed by as much as 26%[10].

All you can do is take the necessary precautions that are necessary to protect your network and your business, but there will always be a threat. But as long as you take the time to find out

Windows of Vulnerability: A Case Study Analysis *IEEE Computer*, volume 33, no. 12

[10] By Robert Lemos, Staff Writer, CNET News.com, February 7, 2001
"A year later, DDoS attacks still a major Web threat"

what threats face your business, weather it is Viruses or hackers, and take the appropriate steps to safeguard your systems, your venture on the Information Highway will be a smooth one.

Bibliography

[1] CERT Coordination Center, Carnegie Mellon University, 6 April 1998
"CEOs hear the unpleasant truth about computer security"
http://www.cnn.com/TECH/computing/9804/06/computer.security.pm/

[2] CNN Correspondent Ann Kellan, 5 April 2002
"CERT/CC Statistics 1988-2002"
http://www.cert.org/stats/cert_stats.html

[3] Attrition.org, Not Dated
"Errata: Statistics"
http://www.attrition.org/errata/stats.html

[4] M. E. Kabay, PhD, CISSP, Associate Professor, Computer Information Systems, Norwich University, Northfield, VT, 2001
"Understanding Studies and Surveys of Computer Crime"
http://www2.norwich.edu/mkabay/methodology/crime_stats_methods.htm

[5] William A. Arbaugh, William L. Fithen, and John McHugh, December 2000.
Windows of Vulnerability: A Case Study Analysis
IEEE Computer, volume 33, no. 12

[6] By Robert Lemos, Staff Writer, CNET News.com, February 7, 2001
"A year later, DDoS attacks still a major Web threat"
http://news.com.com/2009-1001-252187.html?legacy=cnet

[7] Reliable Anti-Virus (RAV), Copyright date 1999-2002
" VIRUS STATISTICS"
http://www.rav.ro/ravmsstats/

[8] By Marcus J. Ranum, CEO, Network Flight Recorder, Incorporated, Copyright date 1998
"Intrusion Detection: Challenges and Myths"
http://secinf.net/info/ids/ids_mythe.html

[9] Brian Caswell and Marty Roesch, Copyright date 2002
http://www.snort.org/

Last Updated: July 24th, 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 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
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
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 Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
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 Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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
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