Global Information Assurance Certification Paper

Network Security

Who's winning this war?

By

Jerry L. Jackson

Practical assignment for the GIAC Security Essential Certification version 1.4

Introduction

Security professionals in today's information technology environment are faced with an alarming and increasing assortment of threats and vulnerabilities. Systems are constantly being attacked by literally thousands of hackers scanning the Internet searching for holes in the systems. The skill of these hackers can range from hard-core code writers to script-kiddies, a term given to inexperience hackers that use pre-made tools for hacking. The destruction capability of hackers has grown tremendously as new hacking tools are developed almost daily. It's becoming a very demanding if not impossible task to stay ahead of these lethal intruders. The purpose of this paper is to serve as a briefing to those that are new to the Information Technology (IT) field and report the current status of security issues that are affecting the networks. Who are these hackers? What are they doing to the networks and how are they doing it? Additionally, this paper will present an analysis of the legal and social trends that are reshaping the perception of network security.

What are the damages and costs?

Digital attacks including viruses caused more than $8 billion in damages worldwide in January (of this year) alone.[1] The Slammer virus cost businesses close to a billion dollars by itself. The cost associated with protecting networks can be astonishing to say the least. Companies attempt to protect their networks by hiring security professionals as well consultants, in addition to purchasing the most up-to-date equipment with the latest technologies. Network security is undoubtedly one of the fastest growing areas of the information technology market. The International Data Corporation reported that the security consulting market could reach a cost of $14.83 billion in 2003,[2]. This does not include the cost of the additional staff and equipment. This could double or maybe triple that figure to $40-45 billion for network security. Some of other costs that are absorbed when a system go down are:

Salaries – overtime for system/network administrator and staff.

Lost customers – if the company's website is down, customers will shop elsewhere. Can you imagine how much Ebay would lose if their web server was unavailable for two days?

Internal – productivity of employee with lost of network connectivity or email, inventory overruns or shortfalls, accounts payables not collected, and business reputation.

---

1 *Datamation magazine*

2 *Information Security*

What is a threat?
A threat is a person, circumstance, or event with the potential to compromise the integrity, availability, or confidentiality of the network or the data on the network. Integrity is the ability to ensure that the information on the network accurate, availability is the ability to ensure that the network is available and reliable to ensure that day-to-day business can continue without interruptions and downtime, and confidentiality is the ability to ensure that proprietary data as well as client data is protected from unauthorized visitors. Threats can be categorized as man-made or natural, deliberate or unintentional acts caused by authorized and unauthorized individuals or groups. Threats can be further divided into two groups: "Insiders" and "Outsiders." Insiders are persons authorized to access some part of the system and are trusted not to use this access privilege to harm the system. Outsiders are persons not authorized to access the system. Threats exist because the Internet is easily accessible and operating systems have over a million lines of code, and some have serious flaws.

The insider threat arises from multiple sources and manifests in various ways. Four of these sources are described below:

1) The threat of the coercion of users with authorized access to the system, technical support personnel, or employees or other contract personnel with physical access to the system components arising from the motivation of financial gain.
2) The threat posed by disgruntled employees, especially those who are terminated for cause.
3) The threat posed by users of the system who negligently or inadvertently fail to follow security requirements for the handling and labeling of system output or media, or the rules against the introduction of unauthorized software or data imported from unauthorized sources.
4) The threat coming from authorized users failing to employ proper procedures for the entry or manipulation of system data, due to negligence or the failure of users to be properly trained in the use and operation of the system.

These insider threats can be manifested in the following ways:

- Unauthorized reading, copying or disclosure of sensitive information
- Execution of denial of services attacks
- Introduction of viruses, worms or other malicious software into the system
- Destruction or corruption of data (intentional or unintentional)
- Exposure of sensitive data to compromise through the improper labeling or handling of printed output
- Improper labeling or handling of magnetic media resulting in the compromise of sensitive information.

The coerced insider would most likely copy to disk and remove from the system any and all types of sensitive information to which such user had authorized access. Such a user might also probe the system in attempt to discover ways to circumvent access

permissions and copy and remove from the system sensitive information to which such a user did not have authorized access. In addition, either a coerced insider or a disgruntled employee might attempt denial of service attacks through the manipulation of system software; or the malicious introduction into the system of viruses, worms, or other destructive software.

The outside threat comes from individuals or groups attempting to hack into the system using various hacking tools. An extremely sophisticated user, hacker, or someone under the direction and control of such a person, might attempt to obtain the user ID and password of a privileged user (e.g. system administrator) in order to circumvent the access permissions. Then masquerading as such a user, bypass access controls and permissions to gain access to the most sensitive information on the system. In most instances of these types of attacks, there could well be attempts to gain unauthorized access to and to modify audit data in order to prevent analysis and detection of the source and nature of the attack.

Who are they? White hat vs. Black hat.

The word hacker has always been associated with a kind of evil connotation ever since it was first introduced into society. The image of a hacker was that of usually a male teenager with limited social skills, spending countless hours in his bedroom surrounded by sophisticated computer equipment. Although his action was technically illegal they were considered harmless and few thought he could really do anything destructive to himself or others. This image was further glamorized by the movie "Wargames," in which a teenager is able to hack into a Pentagon's system and convince the system that the U.S. was under attack. The magnitude of his actions coupled with the hero status he was given afterwards, gave creditability to this type of behavior. Hackers break into systems and/or release malicious code to crash networks for a variety of reasons. Some popular reasons are greed, power, money, politics, prestige, bragging rights, or just the challenge or thrill of successfully penetrating a system. Like most criminals, the bottom line is that they all think that they can succeed without getting caught. Regardless of the intent, when you access or achieve something that wasn't intended for you and the owner made an effort to protect the information from you it is a crime. You can be charged with breach of computer security, which could range from a misdemeanor to a felony charge. Punishments can range from probation to ten years. Over the years the word hacker has taken on an even darker meaning in society with many so called hacker disassociating themselves from the mainstream hackers by renaming their cause as "white hat" hackers. The hacker community has begun to label hackers based on what they do with the information they discover. If they use it to inform the public then they are called white hats, and if they use it to exploit or damage a system they are called black hats.

White hat hacker is a term given to hackers that are considered good and ethical. Some think of this analogy as similar to labeling a criminal an honest thief. Many organizations and the media describe the white hat hacker as someone that conduct

software and penetration testing to find vulnerabilities and release results to the vendors and to the public. Their belief is that the vulnerability is there whether they find it or not, and this way the vendor has to supply a patch before the black hat exploits the vulnerability. The white hat hacker does serve a valuable role in the fight to help protect our networks. Their testing of new and existing software for vulnerabilities serves as a sort of watchdog for inferior products released by vendors. There are some vendors that prefer that they be notified prior to the release of the vulnerability. The new Organization for Internet Security (OIS) group, which contains some of the larger software firms as members, recently announced that their goal is "To propose and institutionalize industry best practices for handling security vulnerabilities."[3] This is a way to prevent the release of vulnerabilities until the vendors has chance to create a patch. This is an ongoing debate on this subject, if the vulnerability is released to the public, you are also notifying the black hats. If you don't release it, the vendors can take their time and some unsuspecting customer can be attacked. The penetration of networks is a different issue entirely. Most security professionals will tell you that the difference between a penetration tester and a hacker could be permission. Without permission from the owner or their representative, regardless of your intentions you are conducting an illegal activity. While the intention of a white hat hacker may be honorable, the result of his action may determine if criminal charges are filed.

The black hat hacker is considered the evil hacker, whose intentions is to deface, bring down, or damage any system that they are able to penetrate. Their philosophy is that vendor shouldn't release defective software with vulnerabilities, therefore they are doing the public a favor by exploiting them and exposing the vendor. While there may be some validity in that, breaking into network system is still a crime. There is also an interesting development in the labeling of hackers when a hacker does something or performs an action that is a reverse of their label. These hackers are identified as "gray hat" hackers. For example, a white hat hacker penetrates a system and destroys data for personal gains. This brings up the subjectivity of the labeling of hackers as white, black, or even gray. As one ex-hacker pointed out, " the line between good hackers and bad hackers was thin."[4]

How do they attack?

When hackers attack a system they want to either gain access or bring the network down. If they do gain access they want the privileges of the system administrator or root services within the network. Naturally these are the privileges that will give the intruder the ability to modify the system and access all files. Hackers hack into systems by scanning for open ports, Internet protocol (IP) spoofing or hijack, or getting a user to download a Trojan horse, which is exactly what the name implies – a Trojan is a

---

[3] *Techweb*

[4] *Wired News*

malicious program inside a legitimate application or program. Examples of these techniques are:

Scanning port – a hacker will scan the network for ports that are listening, if port 80 is listening then they can exploit vulnerabilities with HTTP protocol.

IP spoofing/hijack (fig. 1) – a hacker pretends to be a trusted source or hijack a session enroute to its destination. When a client and server communicates the client sends a packet that says "hey, I want to talk", the server send an acknowledgement that says "okay, you can talk", then the client sends an acknowledgment that says "Thanks, I will begin". The hacker can hijack this conversation and pretend to be the client and once inside the network he can look more vulnerabilities or leave malicious programs.

Trojan horse – a hacker can embed a malicious program into a legitimate program such as a screen saver. The malicious program could execute a script that may open up a back door or send the user userid and password information to the hacker.

To bring down a system, the hacker simply has to crash the server. Some of the most popular destruction tactics used by hackers are denial of services attacks and viruses or worm uploads. Examples of these techniques are as follows:

Denial of service – (fig. 2) the denial of service attack is intended to keep the server busy so that it will not be available for legitimate request from user. The attacker send request to the server, but what he does is increase the bit size. A ping request is 32 bytes, let say he increased it to 3200 bytes and he can set the machine to send it out continually.

Distributed denial of service – (fig. 3) the distributed denial of service is when the hacker uses multiple clients to send the same request with an increase size.

Virus – a program code that destroys or erases files on a machine when the user performs some kind of action. It is usually limited to that machine and it spreads when the user send it to another machine.

Worms – replicate itself on their own, moving throughout the network from computer to computer. It's more dangerous than the virus because it needs no assistance to move through the system.

Buffer Overflows [5]- one of the most popular techniques used by hackers today is the buffer overflow. The hacker infects a system with a piece of code that when any particular program is executed, the code increases the size of the information that's intended for the program. When the program receives the oversize data, the excess overwrites some of the computer memory. When the computer loses the memory

[5] *Software Engineering Institute*

space, all information that is being processed is interrupted and the program can't find its way back to the original state. The code is then able to take control of the program.

These are some of the many attacks that hackers will use against a system. There are more and as technology advances, I can almost guarantee there will be even more, but they will be better and faster.

What can we do?

As security professionals we must address these threats when securing our networks. The insider threat is the most difficult to defend, because in many cases you have trusted the employee and they are more familiar with the system and can do more damage. To help you defend against these attacks you must ensure there are policies and procedure in place and you must enforce these policies and enlist management's support in enforcing these policies. The policies should address of the following topics:

a. Employee usage – set guidelines on when and how employees can access the network.

b. Limit access – compartmentalize departments by function and limit access to a need-to-know basis.

c. Password – ensure they contain at least the minimum character length and are changed on a regular basis. Conduct walk through of areas for signs of employees writing down passwords.

d. Prohibit modems – they act as a backdoor entrance and can circumvent network security.

e. Prohibit personal software – they may contain malicious code or remote program such as PCAnywhere.

f. Install firewalls and appropriate intrusion detection systems (IDS) both host and network based.

g. Monitor, audit, and analyze network activity on the system.

h. Define incident handling procedures – ensure all users and supervisors know what to do if they suspect or know of a violation or unauthorized access to the system.

i. Conduct backup and practice Continuity of Operation Program (COOP) exercises.

j. Install patches and updates – ensure system administrators installs patches as soon as they become available. To prevent disruptions on your network, a test lab should be installed to test the patch first. One of the more intriguing things I found out

while researching for this paper was that most attacks on large systems could have been prevented had the system's patches and service packs been up to date. Most vulnerabilities are identified long before they are exploited and turned into a weapon against the public. Vendors are now reacting faster to release patches as soon as vulnerabilities are discovered, although some feel they could be reacting faster. Some vendors are accused of holding information about the vulnerability until they have a patch, rather than releasing the problem and then face the pressure of getting a good patch out to the public.

Webster defines vulnerability as "capable of being wounded." or "open to attack or damage."[6] Security expert must analyze the vulnerability versus the threat to assess risks. Vulnerabilities are discovered during a variety of ways. Many are found during normal operations when a system administrator realizes that certain applications do not work well together or open doors through system flaws. Most vulnerabilities are actually discovered during some form of penetration testing and scanning. There are a variety of organizations that track vulnerabilities. All security professionals should be on their mailing list to ensure you stay abreast with the most recent changes.

What's our legal system doing about this?

Since the events of September 11, 2001, Internet security has move closer to the top of the priority list within our legal system. The Melissa virus, the Code Red worm, nor any scares in between could ignite our legal system to pass tougher laws. In October 2001, President Bush signed the USA Patriot Act (USAPA).[7] This came about during a time when we all had a feeling of insecurity, and was the turning point for Internet security. The intent of the law was to give law enforcement agencies more freedom to fight all type of crimes. In doing so it sent a message to the hacker community that hacking is serious and will be handled in accordance with national security. Some of the key issues of the USAPA in regards to hacking were:

A. Section 1030(c) - Raising the maximum penalty for hackers that damage protected computers and eliminating mandatory minimums

Previous law: Under previous law, first-time offenders who violate section 1030(a)(5) could be punished by no more than five years' imprisonment, while repeat offenders could receive up to ten years. Certain offenders, however, can cause such severe damage to protected computers that this five-year maximum did not adequately take into account the seriousness of their crimes. For example, David Smith pled guilty to violating section 1030(a)(5) for releasing the "Melissa" virus that damaged thousands of computers across the Internet. Although Smith agreed, as part of his plea, that his conduct caused over $80,000,000 worth of loss (the maximum dollar figure contained in the Sentencing Guidelines), experts estimate that the real loss was as much as ten times

6 *Merriam-Webster*

7 *Computer Crime and Intellectual Property section*

that amount. In addition, previous law set a mandatory sentencing guidelines minimum of six months imprisonment for any violation of section 1030(a)(5), as well as for violations of section 1030(a)(4) (accessing a protected computer with the intent to defraud).

Amendment: Section 814 of the Act raises the maximum penalty for violations for damaging a protected computer to ten years for first offenders, and twenty years for repeat offenders. 18 U.S.C. § 1030(c)(4). Congress chose, however, to eliminate all mandatory minimum guidelines sentencing for section 1030 violations.

B. Subsection 1030(c)(2)(C) and (e)(8) - Hackers need only intend to cause damage, not a particular consequence or degree of damage

Previous law: Under previous law, in order to violate subsections (a)(5)(A), an offender had to "intentionally [cause] damage without authorization." Section 1030 defined "damage" as impairment to the integrity or availability of data, a program, a system, or information that (1) caused loss of at least $5,000; (2) modified or impairs medical treatment; (3) caused physical injury; or (4) threatened public health or safety.

Amendment: Section 814 of the Act restructures the statute to make clear that an individual need only intend to damage the computer or the information on it, and not a specific dollar amount of loss or other special harm. The amendments move these jurisdictional requirements to 1030(a)(5)(B), explicitly making them elements of the offense, and define "damage" to mean "any impairment to the integrity or availability of data, a program, a system or information." 18 U.S.C. § 1030(e)(8) (emphasis supplied). Under this clarified structure, in order for the government to prove a violation of 1030(a)(5), it must show that the actor caused damage to a protected computer (with one of the listed mental states), and that the actor's conduct caused either loss exceeding $5,000, impairment of medical records, harm to a person, or threat to public safety. 18 U.S.C. § 1030(a)(5)(B).

C. Section 1030(c) - Aggregating the damage caused by a hacker's entire course of conduct

Previous law: Previous law was unclear about whether the government could aggregate the loss resulting from damage an individual caused to different protected computers in seeking to meet the jurisdictional threshold of $5,000 in loss. For example, an individual could unlawfully access five computers on a network on ten different dates — as part of a related course of conduct — but cause only $1,000 loss to each computer during each intrusion. If previous law were interpreted not to allow aggregation, then that person would not have committed a federal crime at all since he or she had not caused over $5,000 to any particular computer.

Amendment: Under the amendments in Section 814 of the Act, the government may now aggregate "loss resulting from a related course of conduct affecting one or more

other protected computers" that occurs within a one year period in proving the $5,000 jurisdictional threshold for damaging a protected computer. 18 U.S.C. § 1030(a)(5)(B)(i).

D. 1030(c)(2)(C) - New offense for damaging computers used for national security and criminal justice

Previous law: Section 1030 previously had no special provision that would enhance punishment for hackers who damage computers used in furtherance of the administration of justice, national defense, or national security. Thus, federal investigators and prosecutors did not have jurisdiction over efforts to damage criminal justice and military computers where the attack did not cause over $5,000 loss (or meet one of the other special requirements). Yet these systems serve critical functions and merit felony prosecutions even where the damage is relatively slight. Indeed, attacks on computers used in the national defense that occur during periods of active military engagement are particularly serious — even if they do not cause extensive damage or disrupt the war-fighting capabilities of the military — because they divert time and attention away from the military's proper objectives. Similarly, disruption of court computer systems and data could seriously impair the integrity of the criminal justice system.

Amendment: Amendments in Section 814 of the Act create section 1030(a)(5)(B)(v) to solve this inadequacy. Under this provision, a hacker violates federal law by damaging a computer "used by or for a government entity in furtherance of the administration of justice, national defense, or national security," even if that damage does not result in provable loss over $5,000.

E. Subsection 1030(e)(2) - expanding the definition of "protected computer" to include computers in foreign countries

Previous law: Before the amendments in Section 814 of the Act, section 1030 of title 18 defined "protected computer" as a computer used by the federal government or a financial institution, or one "which is used in interstate or foreign commerce." 18 U.S.C. § 1030(e)(2). The definition did not explicitly include computers outside the United States. Because of the interdependency and availability of global computer networks, hackers from within the United States are increasingly targeting systems located entirely outside of this country. The statute did not explicitly allow for prosecution of such hackers. In addition, individuals in foreign countries frequently route communications through the United States, even as they hack from one foreign country to another. In such cases, their hope may be that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution.

Amendment: Section 814 of the Act amends the definition of "protected computer" to make clear that this term includes computers outside of the United States so long as

they affect "interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). By clarifying the fact that a domestic offense exists, the United States can now use speedier domestic procedures to join in international hacker investigations. As these crimes often involve investigators and victims in more than one country, fostering international law enforcement cooperation is essential. In addition, the amendment creates the option, where appropriate, of prosecuting such criminals in the United States. Since the U.S. is urging other countries to ensure that they can vindicate the interests of U.S. victims for computer crimes that originate in their nations, this provision will allow the U.S. to provide reciprocal coverage.

As you can see this law started a drastic change in the way we look at Internet security and the way the legal system viewed hackers and their capabilities. Now hackers that attempt to damage or access government or commercial systems are viewed as a threat against national security. Following the Patriot Act, congress passed the Cyber Security Enhancement Act (CSEA) of 2002. One author quoted that "The act directs the United States Sentencing Commission to amend Federal sentencing guidelines for crimes that are related to fraud or unauthorized access to federal government computers and restricted data. Hackers will face harsher penalties if they knowingly cause or attempt to cause death or serious bodily injury using the computer as an "instrumentality" for committing their crime. Although there is room for debate about how this provision will be implemented, it seems reasonably limited to distinguish garden variety hackers from hacker-terrorist".[8] Also this act, which was approved as a standalone bill in July, expands the police ability to conduct Internet eavesdropping and grant Internet providers more latitude to discuss information about their users.[9]

In November 2002, the president signed the Homeland Security bill, which created the Department of Homeland Security. Among other duties to protect the homeland, the department, "envision a far greater role for the government when it comes to making sure operating systems, hardware and the Internet are secure."[10] Finally in January of this year the Justice Department drafted a new bill called the Domestic Security Enhancement Act of 2003.[11] This bill would increase the law enforcement abilities that were granted in the Patriot Act in 2001, some groups are calling it Patriot II. The Justice department decision to come onboard with this fight against hackers couldn't have come at a better time, or should I say" better late than never."

Some will say that the new laws are not a deterrent or that the hackers won't be prosecuted, and that may be the case, but this is a start. Now there are more profile hacker cases that are being brought to trial. In a case in Texas the prosecutors are asking for a sentence of ninety-five years for a hacker that hacked into Yale University

8 *Computer Crime and Intellectual Property*
9 *Findlaw's*
10 *CNET News*
11 *SecurityFocus*

system.[12] The arrest of hackers across the country has ignited reactions from across the globe. The Canadian arrest of the infamous "Mafiaboy" prompted their government to get active in the fight against cyber crimes.[13] The European Union recently passed a law to prosecute computer hackers and virus spreaders.[14] Hackers are no longer being seen as just a nuisance.

War of words

Fellow security professional, make no mistake about it, we are at war. The uniqueness about this war is that the enemy is very elusive and can attack from across the globe. There are three basic items an attacker needs to damage a system, knowledge, a computer, and access to the Internet. Knowledge is probably the most important because our systems are becoming more sophisticated every day and tools downloaded for script-kiddies are usually well defended and can't do much damage to a system. On the other hand knowledge coding program language gives the hacker the ability to write his own program to fit his needs. These are the most dangerous of our enemies, because they are smarter and can penetrate with greater accuracy. In this war, the enemy is faceless and you can't see them before the damage is done. They come in all ages, races, genders, social positions, and nationalities. You can't distinguish between Hassem the terrorist from Bora Bora, Ivan the communist from the Georgia Republic, Carlos the czar from Columbia, or Richie Rich from Milwaukee.

Conclusion

The ability to cause grave damage to our networking systems has become a chilling reality. The Justice department and our legal system is starting to get on board, and the tougher laws should make some difference to the average hacker. We can't rely solely on the laws to protect us, even if the hackers are prosecuted. The fact is the law can't return the lost revenues, client confidence, or the reputation in the business community. It was reported that the average corporation gets hit 30 times a week and there are 10 to 15 new viruses or malicious codes released every day.[15] The job of network security is frontline foxhole duty with 24/7 responsibilities. The balance between availability and security is a constant challenge. If security is too tight, there is very little availability and if your system has a greater availability, then security is loosen. The right mix would be to have only the things that are needed available, and everything else either disabled or deleted. Unlike any other war, this will last a long time because anyone can join and there are no geographical or language limitations. All that is need is access and motivation. Who's winning this war? Well, I don't know, but we are looking a lot better and security of our networks is something that people from all walks of life are starting to be concern with.

---

12 *SecurityNewsPortal*

13 *LinuxSecurity*

14 *Reuters*

15 *Technews*

List of References

1. Guadin, Sharon. "Slammer Damage May Top $1 Billion". Datamation, January 31, 2003. URL: http://itmanagement.earthweb.com/secu/article.php/1577611
2. Kleespie, Steven, L. "White Hat" Hackers in Information Security. January 20, 2000 http://www.wbglinks.net/pages/reads/misc/whitehat.html
3. Lange, Larry. "Will OIS Put Bite On White Hats?" TechWeb, October 23, 2002 URL: http://www.techweb.com/tech/security/20021023_security
4. Delio, Michelle. "A White Hat Goes to Jail". Wired News, May 22, 2001. Url: http://www.wired.com/news/politics/0,1283,44007,00.html
5. Rogers, Larry. "Buffer Overflows – What Are They and What Can I Do About Them" Software Engineering Institute, URL: http://www.cert.org/homeusers/buffer_overflow.html
6. Merriam-Webster, Dictionary URL: http://www.webster.com
7. Computer Crime and Intellectual Property Section, "USA Patriot Act 2001" URL: http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm
8. Computer Crime and Intellectual Property Section, "Cyber Security Enhancement Act of 2002". URL: http://www.cybercrime.gov/homeland_CSEA.htm
9. Ramasastry, Anita. The Cyber Security Enhancement Act's "Good Faith Disclosure" Exception., FindLaw's, March 28, 2002 URL: http://writ.news.findlaw.com/commentary/20020328_ramasastry.html
10. McCullah, Declan. "Bush signs Homeland Security bill" , CNET News, November 25, 2002. URL: http://www.news.com.com/2100-1023-975305.html
11. Poulsen, Kevin, "Ashcroft proposes vast new surveillance powers", SecurityFocus., February 7, 2003, URL: http://online.securityfocus.com/news/2296
12. SecurityNewsPortal, "Yale hacker faces 95 years in prison says DA", April 4, 2003 http://www.securitynewsportal.com/cgi-bin/cgi-script/csNews/csNews.cgi?database=JanY%2edb&command=viewone&id=69&op=t
13.., Olson, Jen., "Mafiaboy opened eyes to computer crime" LinuxSecurity, February 24, 2003. http://www.linuxsecurity.com/articles/government_article-6797.html
14. "EU sets jail terms for hackers" Reuters, February 28, 2003. URL: http://news.com.com/2100-1002-990669.html
15. MacMillan, Robert., "Wartime Internet Security Is 'Business as Usual', TechNews, March 27, 2003. http://www.washingtonpost.com/wp-dyn/articles/A37785-2003Mar27.html

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
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
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 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 Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	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 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
SANS London September 2017	London, United Kingdom	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