Global Information Assurance Certification Paper

The Third Element
(The rise of the NEO hacker)

Jayson Street, CISSP, CCSA
September 08, 2003
GSEC Version 1.4b

It's the first Friday of the month at a Houston mall and a crowd has gathered around a table where a seventeen-year-old young man is showing off his latest prize. Is it the newest sneakers, or the hottest new video game? No it is a box of documentation that he took from a communication company's dumpster. The information he gathered is customer's names and private phone numbers, and IP addresses for their internal network. He also pulls out user manuals for a CISCO Cerent device, and several other routers. He has saved the best for last. He proudly displays an old used router that was thrown away. The questions he asks are not "how much can I get paid for it?" or "What damage can I do with this?" No, his questions are "How can I make it work?" "What does it do?" "What is it for?" He asks these questions because he is a NEO Hacker.

In recent history the hacking community has been divided into two main distinctions. There is the white hat hacker - one who uses their skills for security awareness and requested vulnerability assessments and the black hat hacker - one who uses their skills for criminal activity by various vectors of attack. This paper will create a more precise definition by dividing the black hat hacker community into three categories: a cracker, a criminal hacker and a neo hacker. The focus of this paper will be the third group, which in the author's opinion presents a greater threat to the enterprise. Threat in this case is a factor of risk and likelihood of an exploit. For more precise definitions and uses of the terms "risk" and "threat" and how they are used by security practitioners, see "An Overview of Threat and Risk Assessment" by James Bayne in the SANS Reading room.[1]

There will be no discussion of the white hat hacker since they are essentially in the INFOSEC community. The author would like to state that this is only a narrow view given to these categories for the purpose of this paper. The variations are as limitless as there are people on the Internet.

The Cracker

The motivation:

The word vandal goes back to the time of warriors who did nothing but pillage and destroy all within sight. Their disproportional act of destruction is the reason we still use the word today to describe someone who destroys or defaces other's property for the simple enjoyment of doing it. A cracker is of the same mentality but just not the inclination to go out into the real world and spray paint walls or knock over mailboxes and throw rocks through car windows. They prefer to hide in the confines of their own home where they perceive themselves to be safe from detection or direct retaliation from the victim. With a plethora of tools and exploits at their disposal there is no need for the cracker to take time to learn how or why the exploits work. The only skill they need is to navigate through Google and click a mouse. Most professionals will ask themselves "There has to be a deeper reason for their actions." "Why are they lashing out?" The answer is they are mostly juvenile delinquents doing juvenile things and using the computer as their tool of choice to do them. A virus writer fits in this definition because they create code to cause damage oftentimes for no other reason than his or her own enjoyment. Here is one case to highlight this point. Please note that throughout this paper unless otherwise noted all references and news clips comes from the SANS newsletters.

U of Michigan Student Arrested for Alleged Computer Crimes
(1/2/4 August 2003)Authorities have arrested a University of Michigan graduate student who allegedly broke into university computer systems. Ning Ma, a Chinese citizen with a student visa, allegedly used keystroke loggers to obtain others' usernames and passwords; he also allegedly stole a student's credit card and PIN number, and accessed two professors' network storage areas, where they kept exams and answer sheets. If he is convicted, Ma could face five years in prison. [2]

Methods of attack:

There are few avenues available to the cracker since they must rely on the tools leeched from websites and IRC channels. This does not diminish their ability to cause damage to a victim's network. I do not want to help arm anyone so I will not name a tool specifically. Instead, I will only describe generic functions i.e. scanning tools, root kits, etc. The Cracker will normally start off doing an Internet wide IP scan. It is about as subtle as going to every person's door in your neighborhood and asking if they are home. A Cracker does not grasp the concept that there are means of tracking them back to their location. Another reason is that they think they have hidden themselves too well using a tool found

on the Internet to hide their original IP. Once they have a list of IP's to work with they then use a freeware or even a commercial vulnerability scanner (one that has been distributed on the IRC with the serial key if needed). Once the vulnerability is found all that is left is for the hacker to find an exploit tool or code that will allow them to deface or DDOS the victim's machine.

Targets:

Any Company or Government that has a high presence on the Internet is a likely target. The greater the level of public exposure, the greater the threat they face.

Japanese University Server Used to Try to Break into NASA Computers
(25 June 2003)
Kobe (Japan) University officials say someone has broken into a university server and installed a program as part of an attempt to break into NASA computers.[3]

Countermeasures:

Since a good majority of attacks perpetrated by the cracker come right out of the box preconfigured for a known exploit chances are that there is already a patch available to close that vulnerability. The best way to counter these basic attackers is with the basic security practice of always keeping your systems patched.

To take this countermeasure to the next level, a program of active vulnerability management is required. Good vulnerability management is a systematic process of identifying and correcting security weaknesses in systems. In this case, systems refers to both "off the shelf" software and the interrelated solutions built by connecting many vendor products. Often security weaknesses are not in a particular component, but in the way two or more components interact. Both phenomena must be considered for effective vulnerability management.[4]

The Criminal Hacker

The motivation:

To make as much money as they can by any means necessary. Plain and simple the criminal hacker hacks for profit.

Methods of attack:

There are a great variety of techniques used by criminal hackers. Some are truly creative, others are old attacks re-worked to be done with a computer. Examples include, but are not limited to; identity theft, credit card fraud and hacking into a corporate site to steal information for blackmail. (The criminal hacker is not the focus of this paper. For a more thorough discussion of this type of threat, refer to "Secrets and Lies. Digital Security in a Networked World" by Brice Schneier).

Targets:

Their main targets, directly and indirectly, are retail websites (i.e. a direct attack to gain confidential customer information stored on the web site vs. an indirect attack by emailing customers as the company in question and having them divulge their confidential information by various means.) The second most sought after targets are financial or corporate institutions. In these scenarios, the criminal hacker will compromise systems or information resources of the institution to expose a security breach. When this occurs the hacker then contacts the victim and tries to extort money from them. Usually a threat is made demanding a specific amount of money or the criminal hacker will leak information and details of the hack to the public. Because protecting customer data is such a sensitive topic today, this would expose the company to loss of market value and / or market share. Due to this fact, a good number of attacks are not reported to the proper authorities for fear of information being leaked to the public.

Massachusetts State Lottery Commission Web Site Spoofed
(9 July 2003)
A phony web site that mimics the Massachusetts State Lottery Commission site was being used in an attempt to try to steal personal data. Some people received e-mails and text messages telling them they had won $30,000 in a lottery and directing them to the phony site. Once there, they found they were required to enter personal information and pay a $100 processing fee in order to claim their prize. The site has been taken down. The Commission is working with the FBI to find those responsible for the scam.[5]

PayPal Customers Targeted by ID Data Theft Scam
(8/9 July 2003)
Some PayPal customers have received messages telling them that their billing information has been lost and that in order to keep their accounts, they must re-enter the data on a specific site. Though many of the sites' links point to the PayPal web site, the form which requests personal information, such as name, address, credit card information and social security number, is on an server at a different IP address. The phony site uses a valid SSL certificate.[6]

Adult Web Sites Targeted by Extortionist
(10 July 2003)
Someone using the on-line name "Deepsy" has been attempting to extort money from adult web sites, threatening to take them off-line with denial-of-service attacks unless they pay him $1,500. "Deepsy" has apparently made good on his threats; one of the targeted adult web sites has contacted the FBI.[7]

Countermeasures:

Organizations must have a well thought out and implemented security awareness plan. This must encompass both internal and public concerns so customers can protect themselves online. When a company is targeted and a criminal sends out a false email representing the victim, it does not matter that the company was not at fault. It will still be reported that customers from that company were exploited. A company's website must be secure and hard to spoof to minimize counterfeit website scams. Finally, as in the case of the Cracker, a company must have an effective patch maintenance program. These types of attacks are not going to go away. As the timeline below shows, they are only going to increase in number and severity.

February, 2000: A 15-year-old hacker known as Mafiaboy attacks Internet sites operated by Yahoo Inc., Dell Inc., CNN, Amazon.com Inc. and eBay. His denial-of-service bug hits the computers with requests over a six-day period, shutting down the sites for a total of 16 hours.

July, 2001: CodeRed, a computer worm, attacks Microsoft's networking software. The worm finds weaknesses in computer systems and copies itself as it travels. Downtime and computer costs total $2.6-billion (U.S.).

November, 2001: Microsoft releases games console Xbox. The system's powerful processor, sophisticated graphics and audio system make it a favourite of hackers, who are able to convert the Xbox into a powerful PC for less than $200 (U.S.). It's estimated more than 200,000 hackers have downloaded the software necessary to complete the conversion.

January, 2003: The SQL Slammer worm creates havoc on a worldwide scale. Internet service providers in South Korea shut down, plane schedules are disrupted and about 13,000 Bank of America automated teller machines shut down. Damage is estimated at $1.1-billion (U.S.).

March, 2003: The U.S.-led invasion of Iraq inspires a wave of pro- and anti-war hacking. Between 3,000 and 5,000 government and corporate sites around the world are shut down and defaced each day, including Arabic broadcaster Al-Jazeera.

May, 2003: Russian-based hackers search U.S. corporate Web sites for vulnerabilities, stealing data and credit card numbers. Then, via e-mail, the companies are warned that their Web sites are insecure. The hackers promise to return the data and fix the breach for a fee. U.S. government agencies arrest more than 130 people. An estimated 89,000 consumers and businesses are taken for $176-million (U.S.) over the course of five months.[8]

The NEO Hacker

The motivation:

The third element, the "NEO hacker" is not out to damage a corporate network. There is no desire to steal confidential information from the systems that are compromised for profit. The main goal of the NEO hacker is the quest for knowledge, to seek out forbidden areas in cyberspace and to conquer it.

A NEO hacker will try to invade a company's network just for the thrill of the hunt. They do not debate if it is right or wrong. They believe if a victim's system is compromised then they are not responsible for the intrusion. The victim, after all, did not adequately protect their systems.

They do not perceive themselves to be criminals. They are often harder to find because they do not actively steal, alter or blackmail. The real damage is done after the intrusions are detected or publicized. Then most companies will experience adverse financial effects.

This is why the threat of the third element is often overlooked and often more damaging to a business. These are the reasons why this paper was written, and why more attention must be made to this third element of the hacking community.

Targets:

Any machine connected to the Internet and any facility that might house something of interest is a potential target. As an example I recall a conversation in which a Neo Hacker was explaining how he was with his Dad visiting a law office. While he was waiting he booted up his laptop and found that the law office was using a wireless unencrypted network. So he connected to it and started surfing the network for servers and routers. He did scans on the servers to see what OS and service packs they were running. He connected to the routers just to see if they were using the default passwords, which they were. He then left the same note on several servers to the system admin, letting them know all the information he found and steps on how to fix them to tighten up security. I asked him why he did this since it would still be considered a crime no matter if he damaged anything or not. His reply was that he was bored and the system admin should thank him since the systems should be secured and the admin was not doing his job.

He does not believe he did anything wrong because he was exploring in an area that was not secured. Therefore it was acceptable for him to do so. I tried to

explain to him that even though I may be curious what kind of belongings my neighbors have, I am not allowed to go through their house if they leave the front door unlocked. Even if I leave a note on the table reminding them to lock their doors, I'm still breaking the law. It was a wasted effort. He did not see the correlation that he did something wrong since his activities were "not in the real world."

Methods of attack:

1. Foot printing (hacking with Google)

The main goal for a NEO Hacker is to find out the most information about the chosen target without getting caught. Therefore automated scanners will not be the first choice. There is plenty of information to be had on the Internet. You just need to know where to look. If a hacker is interested in going after ACME INC. the first step is finding out what kind of environment is running in that company. This is also known as foot printing your target.

> For example, system Administrators will occasionally post a question to a newsgroup or forum asking for help and information on a problem at hand. Going to Google and doing a search for @acmeinc.com will give you all the forum and Usenet postings from that domain through out the years. It will also give you information on any person who has used their work email for personal reasons. The author has personally done several security audits where this first step of gathering information has resulted in system configurations, IP address ranges and operating systems that were being used in the targets' environment. A few examples of this are as follows.

I found a system admin who was responsible for a NT RAS server and needed help configuring it. He confessed to being more familiar with Unix, and didn't know how to solve a particular problem. For a hacker searching through Google newsgroups or any Usenet search engine this is pay dirt. They now know several things the Company wishes they didn't.

1. They have a predominantly UNIX environment (why else would they need a System Admin who knew so much about UNIX?).
2. They are adding NT into the environment.
3. The person responsible for the network is not familiar with the new operating system.
4. The most likely target for entry into this network is any machine found running a windows based operating system since chances are they are not as secured as the UNIX machines due to the system admin not knowing the best practices for hardening a windows machine. Conversely, the odds are the UNIX machines are hardened and configured properly and may raise an alarm if they are tampered with. As such, they are too risky a target on which to attempt an attack.

Another good example is a person I found who was listed as a volunteer for a non profit organization on the organization's web site. The person used their work email as the primary point of contact. They also listed their home phone number and address. By allowing this, they created at least two scenarios an attacker might exploit:

1. A social engineering attack can be made by calling the person and trying to get them to divulge user IDs and passwords by posing as a help desk technician from their company. With so much personal information on the non-profit's web site, there is plenty to work with.
2. A more creative possibility is to use the address to drive by the home with a laptop and a wireless sniffer. There may be opportunity if an unencrypted access point is in use. This could provide a goldmine of information since a lot of employees will do company business on home computers and even connect their company laptops to their home network even if company policy prohibits this.

Now some will say that is going a little far. Why would someone go through so much trouble to just look through a company's network for no profit or pure mischief? The reason is simple. A NEO Hacker is looking for the challenge. Anyone can port scan and release a Trojan and remotely take over a machine with sub-seven. They seek the thrill of the hunt and the chance to brag of the indirect route they took to own a network. This shows off not only their skills but also their ability to set themselves apart from an ordinary hacker, which is what they desire the most.

Countermeasures:

The best defense will always be a well thought out and implemented security policy. The key here is enforcement and monitoring of this policy. At least once a month a thorough search of Google and Usenet should be conducted by INFOSEC to ensure the only references to the company on the Internet is sanctioned and expected. There is a really good tool for this – www.googlealert.com. You can put in a search on Google, and then it will email you whenever the Google search produces different results. The email you get is only the difference. If this is done after the barn door is already opened (someone has already posted inadvertently sensitive information like mentioned above). Then resources should be used to change the configuration that is mentioned if at all possible or at the very least the email address used should be changed so it cannot be spoofed and used in a future social engineering attack.

2. Social engineering (because there's no patch for security awareness)
People will always be the weakest link in the security chain. However, if they are not properly trained in information security, then the fault lays with INFOSEC and not them. Here are two examples from the best to the worst in social engineering.

> The first comes from when the author was working at an Internet based bank. Every person who went through training received a two-hour class in information security covering topics from proper password creation to how to detect if someone is conducting a war dial on the phone systems. They were so well trained that when the president and owner of the bank was trying to enter a secure area, he was denied entry from an employee who had been there only two weeks because he was not wearing his badge. When the president found the author and notified him of this it was with satisfaction that the policy was being enforced with no exceptions. The president was then given a temporary visitors badge so he could be let in.
>
> This also illustrates another important and integral part of information security. The program must be fully supported by upper management. If employees believe their management does not take Information Security seriously then why should they?
>
> ---
>
> I was once hired to do a penetration test for a financial services company. Their Internet perimeter security was the best I have seen in a corporate environment. I knew there was not much chance of getting in remotely. Instead, I went to their main corporate building. After getting in (which will be used later as another example) I was able to walk into secured areas where employees were working and without being questioned. The employees were wearing business attire and the author was wearing jeans and a t-shirt from SANS that said on the back "I hacked the NET."
>
> At one point a supervisor questioned why I was walking around taking pictures. I explained that Tech Support needed to take pictures of network couplings to help speed up performance. That was enough of an answer to be allowed to continue. One employee was helpful enough to get out of their seat so I could browse the network on their computer and even waited patiently while I took pictures of all the server names on the network neighborhood screen.
>
> I quizzed employees and found some that were willing to divulge their passwords to a complete stranger.

Will a NEO Hacker do something like this - brazenly try to enter a corporate building and risk being caught? The answer is "Of course." That is one of the

easiest and most fun ways for a hacker to own a network. Kevin Mitnick is not a famous hacker because of his exceptional technical knowledge. His skill was letting the trusted employee of the target company do his dirty work.

Countermeasures:

Employees are the first line of defense in a social engineering attack. But they must be taught how to detect and react to an attack. They must also be empowered to challenge anyone or any situation they believe is suspicious. In the first example, the employee was given special recognition in the company newsletter for the actions, which helped reinforce every employee's role in the security matrix. This action also gave other employees seeking positive recognition something to strive for.

3. Accidental discovery (Hacking favors the well prepared.)

How I was able to gain access to the building in the previous Social engineering example is instructive for this point.

> I arrived at the building at 5:30pm - a time when most people are leaving but traffic coming in is not looked at too suspiciously. The doors from the lobby to the main elevators are locked twenty-four hours a day seven days a week. Access is controlled by a card system. So there were only two ways to gain access into the building. One was to try to convince someone who was leaving to hold the door open while they were leaving. That would also potentially lead to questions that could not be readily answered. Things like "Who are you here to visit?" "What's your name?" And the dreaded "Can I see some Identification?"
>
> The second turned out to be the way in this time – be lucky. It turned out the receptionist had already left for the day. For the convenience of visitors who left later there was a basket for them to return their cards. A few visitor cards were there, but none would grant access. However, an employee who needed a temp badge had been thoughtful to not leave it in the general basket but left it in the penholder on the receptionist's desk. Unfortunately this day there was an attempt to breach the building security and I was provided a way into the inner area and also other secure areas that the employee was allowed to access.
>
> If this attempt had been tried any other day, that badge would not have been there and access would not have been possible. The visitor cards left in the basket would not have worked. But the one card left in the penholder did. Accidental discovery can be just as harmful to a target as a forceful attack. Similarly, many exploits that have been created in the past came from hackers who got lucky and found the right combination

needed to cause a buffer overflow, an exploit for remote access, or code execution.

Countermeasures:

To counter this type of attack, INFOSEC must understand that the unlikely and improbable can and will happen. Look at the places where security systems interact. That's where they will fail. And they will fail in unexpected ways. Get in the habit of asking "What if…" questions. If you don't foresee and prepare for it, Murphy's Law dictates that it will likely happen.

4. Dumpster diving (one person's trash is a hackers way in.)

As referenced in the introduction, dumpster diving does happen quite frequently. It is not just a method over dramatized in hacker movies. It is a serious form of information leakage that occurs in most companies today.

> At one firm where I did an assessment, there was a tight policy regarding trash disposal inside the work areas. If it was sensitive in any way it was to be placed into locked shred bins, which would be emptied weekly. Construction was going on as the company was expanding. On top of a big heap of construction debris in the dumpster I found the blue prints for all the floors leased to the company. This provided details showing where all the patch closets were. It also showed phone numbers and names of people involved in the construction from the construction company and the client company. Now all an intruder needed to do was drop a few names to the receptionist and purposely stroll to the nearest patch closet and hide a patch cable going to a laptop sniffer to capture login exchanges to be dumped into a password cracker.
>
> For this scenario to be successful, other processes would have had to fail. And sometimes they do. INFOSEC should make sure the hacker has as little information as possible. There is no need to dump hints into the trash for them to take and use. The reverse occurred at the financial services company that the author was penetration testing. All the outside dumpsters were locked and monitored. They were checked on different days to see if this strict policy was adhered to, and it was.

Countermeasures:

Create a secure document disposal policy and make sure it is adhered to. This means check your dumpsters and shred bins. Ensure they are locked. Make sure that your disposal company is following their procedures as well. Take the extra step to check out the references of the disposal company. Train your employees to place the right trash in the right containers.

And then go one step further – make sure you have an electronic disposal policy. Too many hard drives are thrown away or donated with sensitive information still intact. It is amazing what a NEO hacker will find at a swap meet.

5. Employee snooping (idle hands are the hackers' playground)

It has been stated in several reports that the majority of security breaches have occurred from an internal source. NEO Hackers often have regular jobs. And they may be using those jobs to practice their "skills." Best practices dictate that any INFOSEC department should assume that they have one or more NEO hackers working for them and protect themselves accordingly.

> A NEO Hacker with access to your internal network is not a thought that sits well with someone in INFOSEC but it is a reality that must be faced. I have done an audit where a few technicians decided to use the company's T1 access to host a game server on the network. This decreased the overall bandwidth that the company had available. It also opened a way for crackers to get in and exploit the servers. Additionally, it was then used as an illegal warez site. This is just one example of many illustrating the fact that INFOSEC must closely monitor the activity on both sides of its digital perimeter.
>
> ---
>
> At one engagement, the practice at the company was for the INFOSEC team members to run host based intrusion detection software on their own PC's. On one occasion, an alert sounded when a port scan was run against the subnet assigned to INFOSEC. A quick investigation identified the "intruder" as a network engineer testing a new version of Nmap on the production network without authorization.
>
> This infraction was very significant in several ways:
>
> 1. It tested the preparedness of INFOSEC for a possible foot printing attack.
> 2. It was a good exercise, forcing the team to track down an internal threat that had been detected.
> 3. Most importantly, it raised security awareness throughout the technology areas. By demonstrating a fast response, everyone learned that the company is vigilant in monitoring for improper activity on the network. This serves as a deterrent for "bored" employees who may decide to turn their curiosity into a pattern of behavior – becoming NEO hackers themselves.

Disgruntled Employee Sent Confidential Document to Employees

(23 June 2003)

ThruPoint is investigating an instance of an employee allegedly breaking

into company computers, accessing a confidential document relating to the restructuring of the consultancy's European offices, and e-mailing information contained in the document to other employees. In addition, information from the document appeared on a website for former company employees.[9]

Former Employee Pleads Guilty to Computer Intrusion

(4 August 2003)

A former Telecast Fiber Systems, Inc. employee has pleaded guilty to breaking into the company's computer system and deleting files. John Corrado will pay the Worcester, MA company $10,360, the estimated amount of their losses. Corrado apparently remotely accessed the computer system about a month after he left the company; he will be sentenced in early October and faces up to a year in prison and a fine of $100,000.[10]

Countermeasures:

As stated throughout this paper, a well thought out and implemented security policy is the first and most important countermeasure. Part of this policy must include active internal monitoring. Only watching outside the digital walls of an organization is leaving the job half done. Network and host-based intrusion detection systems must be installed at strategic points with special attention given to sensitive areas.

Conclusion:

INFOSEC professionals should remember – NEO Hackers do this because they find it fun! Take this story about the poster child for the NEO Hacker, Adrian Lamo:

Lamo Hacks Cingular Claims Site:

"Adrian Lamo, a hacker who in the past has broken into The New York Times and Yahoo, found a gaping security hole in a website run by a company that issues the insurance to Cingular customers. By accessing the site, Lamo said he could have pulled up millions of customer records had he wanted to. The Cingular discovery is the latest in a line of exploits from Lamo. In the past few years, Lamo has found his way into the database containing sources for the The New York Times, has altered news stories on Yahoo and has repeatedly compromised AOL. Companies have contemplated suing him, but security experts have lauded his efforts for pointing out flaws.

Lamo, 22, doesn't have a permanent address. He wanders cross-country on foot or by public bus. Spring and summer usually bring him to Northern California. Until recently, he used terminals at Kinko's to perform his hacks. He has since moved on to using a Wi-Fi laptop at Starbucks to do his work." [11]

NEO hackers are not paid for their activities, nor motivated by emotions like greed or anger. INFOSEC professionals must defend their organizations with the same enthusiasm as the NEO hacker uses to break in. It is dangerous to assume that most hackers are bumbling script kiddies who are nothing more than an annoyance to the well prepared. NEO Hackers are analytical and methodical in their approach to compromising a network. They have a fierce determination to find creative ways in just for the sake of being able to brag about their accomplishment.

An INFOSEC professional should not condone or even admire these actions. But failing to respect the tenacity and creativity of this threat is to invite compromise. This threat is real and growing. The attack you don't expect is the one that is most effective.

Sir Arthur Conan Doyle said through his character Sherlock Holmes: "It is an old maxim of mine that when you have excluded the impossible, whatever remains, however improbable, must be the truth." A NEO Hacker uses this as a credo but with a twist. "When you have excluded the impossible, whatever remains, however improbable, must be the **way in**."

References

[1] Bayne, James. "An Overview of Threat and Risk Assessment." SANS Reading Room. http://www.sans.org/rr/paper.php?id=76

[2]Chang, Soojung "Alleged 'U' hacker arrested, arraigned" The Michigan Daily. August 4, 2003. http://www.michigandaily.com/vnews/display.v/ART/2003/08/04/3f2e12e7790b0

[3] "Hacker Targets NASA Via University." June 25, 2003. http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20030625a8.htm

[4] For a more extensive discussion of the topic of Vulnerability Management, see "Are You Vulnerable?" Shipley, Greg. Network Computing. June 26, 2003. http://img.cmpnet.com/nc/1412/graphics/1412f1_file.pdf

[5] Rosencrance, Linda. "Cyberscam strikes Massachusetts state lottery." Computerworld. July 9, 2003. http://www.computerworld.com/printthis/2003/0,4814,82892,00.html

[6] Roberts, Paul. "New site spoofs PayPal to get billing information." Computerworld. July 9, 2003. http://www.computerworld.com/printthis/2003/0,4814,82888,00.html

[7] Shachtam, Noah. "Porn Purveyors Getting Squeezed." Wired. http://www.wired.com/news/print/0,1294,59574,00.html

[8] Damsell, Keith. "'Ethical hackers' test for weakness." The Globe and Mail. August 5, 2003. http://www.globetechnology.com/servlet/ArticleNews/TPStory/LAC/20030805/RHACK/TPTechnology/

[9] "'Disgruntled employee' hacks own company's computer system." Silicon.com. June 23, 2003. http://www.silicon.com/news/500019/14/4804.html

[10] "Former Telecast Fiber worker pleads guilty to hacking" **Boston Business Journal. August 4 2003.** http://boston.bizjournals.com/boston/stories/2003/08/04/daily11.html?t=printable

[11] Null, Christopher. "Lamo Hacks Cingular Claims Site." Wired. May 29, 2003. http://www.wired.com/news/privacy/0,1848,59024,00.html

Last Updated: July 27th, 2017

Upcoming Training

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