|  |
| --- |
| CS 213 Introduction to Network |
| An Introduction to Network Security |
| HHHS\*Admin |
|  |
| **HHHS\*Admin** |
| **10/16/2015** |

|  |
| --- |
|   |

**Table of Contents:**

**Introduction..................................................................................................................................................1**

**Types and Categories of Threats to Network Systems.............................................................................1**

**Mitigation Techniques in Networks...........................................................................................................1**

**Forensic Investigation Methods in Networks............................................................................................2**

**Legal requirement for Reporting of Unauthorized Access......................................................................2**

**Stuxnet..........................................................................................................................................................3**

**Top 3 Attacks Currently in Operation that Work Primarily Over a Network.....................................3**

**SANS and What They Do...........................................................................................................................4**

**CERT............................................................................................................................................................4**

**Firewalls and What They Do......................................................................................................................4**

**Potential Resources in an Organization that are targeted by a network attack....................................4**

**Desirable Qualifications of Personnel to Hire in Security........................................................................5**

**Salaries of Security Personnel.....................................................................................................................5**

**Certification in Security..............................................................................................................................5**

**CCNA Security.............................................................................................................................................6**

**What is a CISSP?.........................................................................................................................................6**

**What is a Network + Certification?...........................................................................................................7**

**CPE’s.............................................................................................................................................................7**

**Conclusion.....................................................................................................................................................8**

**Introduction**

Network security is a field that has exponentially grown in the past years as cyber attacks have become more sophisticated and networks have become vaster. In this paper, different types of network threats are reviewed, as well as mitigation techniques and forensic investigation methods. The legal standards for reporting unauthorized access are mentioned and in-depth look at the virus Stuxnet is included. Next the top three current network attacks are examined and then we see what part SANS institute and CERT organizations have played in preparing resources for cyber security personnel. Firewalls and the resources often targeted by cyber criminals are the last technological aspects that are examined. The qualifications required of network security personnel is addressed next as well as the expected salaries of such. Lastly, three certifications: CCNA, CISSP, and CompTIA Network+ are discussed in detail.

**Types and Categories of Threats to Network Systems**

Interestingly enough, there are many different types of threats to network systems and many different ways of grouping them together. In the experience of this writer, there isn’t really an agreed-upon number or category of threats. According to the CCNA study guide, there are 5 major classes of attacks: passive, active, distributed, insider, and close-in. Passive attacks are when the attacker passively looks for information like passwords and other sensitive information by monitoring unencrypted traffic. Active attacks mean the attacker is trying to break in to a certain secured system through viruses, stealth, or Trojans. A distributed attack is where the attacker introduces a piece of code to a “trusted” software, and as the software is distributed, so is the malicious code. An insider attack entails an “insider,” usually a disgruntled employee, to attack the system from inside. A close-in attack means that the attacker will try to get in close physical proximity to the network to try to attack it. [1] Some of the other kinds of attacks listed by Network Monitoring are logic attacks, which take advantage of software vulnerabilities, resource attacks, which overwhelm computer resources like CPU or RAM, Trojan horse viruses, and worms. [2]

**Mitigation Techniques in Networks**

The mitigation techniques for minimizing threats and attacks in networks are almost as broad as the types of attacks. Triple A or AAA is a group of three services, Authentication, Authorization, and Accounting, that work in conjunction with TACACS and RADIUS to provide secure networking. A CISCO access control list (ACL) is a list of permit or deny permissions that allows a CISCO system to filter the incoming packets. SSH is a data transmission protocol that uses strong encryption to protect the data as it is transferred. SNMP is a management protocol that is always monitoring the network and assessing it’s performance to search for vulnerabilities. A firewall protects the network from outside the network and is generally installed software. An Intrusion Prevention System (IPS) listens to all incoming traffic, and if it detects a threat, the system can block it. The IPS is often assisted by the Intrusion Detection System (IDS). [3] Another suggestion for mitigation includes user training and awareness, which is often considered the most effective and least expensive of the mitigation techniques. Patch management requires keeping all software up-to-date on all the patches that are released to fix vulnerabilities. Policies and procedures should be clearly defined in writing for an organization and incident response should be thoroughly thought out before executed. [4]

**Forensic Investigation Methods in Networks**

Network forensics appears to be a relatively new field of study in the cyber security world. As such , the author of this paper found relatively little information on the subject and it appears that the tools and methods for examination are quite new and undeveloped. One academic paper from Jackson State University mentions some of the available tools, including: “eMailTrackerPro – to identify the physical location of an email sender; Web Historian – to find the duration of each visit and the files uploaded and downloaded from the visited website; packet sniffers like Ethereal – to capture and analyze the data exchanged among the different computers in the network.” [5] It goes on to present different IP tracing techniques like packet marking and Honeypots and Honeynets. [5]

**Legal requirement for Reporting of Unauthorized Access**

This greatly varies depending on the company someone may be working for and the individual situation, but it is interesting to note that several policies have been put in place to prevent unauthorized access. Paragraph C9.1.4.2 of DoD 5200.2-R states that individuals who have access to classified information must report promptly to their security office:

 “1. Any form of contact, intentional or otherwise, with individuals of any nationality, whether within or outside the scope of the employee’s official activities, in which:

 1.1. Illegal or unauthorized access is sought to classified or otherwise sensitive information.

 1.2. The employee is concerned that he or she may be the target of exploitation by a foreign entity.” [6]

The Gramm-Leach-Bliley Act Data Protection Act of 1999 (GLBA) – Section 501 requires financial services companies to protect the confidentiality and integrity of the National Provider Identifier (NPI), and to make sure it is secure from unauthorized access as well. [7]

**Stuxnet**

Stuxnet was a highly sophisticated worm that targeted Iranian centrifuges, specifically, a uranium-enrichment plant. The 500-kilobyte computer virus is thought to be one of the first cyber weapons, and certainly the first that left the digital world to wreck physical property. According to Wikipedia.org, Stuxnet is believed to have been a joint American and Isreali cyber weapon designed during the George W. Bush administration to target Iran’s nuclear program.[8] It first targeted Windows machines, and then sought out Siemans (a German software firm) Step7 software, which is used to control centrifuges. [9] It is also believed that there was an original version of the software, that manipulated the valves on the centrifuges that allowed for increased pressure inside the tubes and damages not only the enrichment process, but also the containers themselves. The second version could spread through USB drives and Stuxnet started slowly working its way from computers outside the uranium enrichment plants to its actual targets. Within months, the number of working centrifuges had dropped drastically, and the new ones that were being installed weren’t being fed any gas. The technicians couldn’t figure out what had gone wrong, but Stuxnet had carried out exactly what it had been designed to do. [10]

**Top 3 Attacks Currently in Operation that Work Primarily Over a Network**

According to PC world, there are several attacks that black hat hackers could potentially explore for some disastrous results. The first has to do with the Internet of Things (IoT) which they have decided to nickname the Insecurity of Things. The IoT refers to the idea that everyone’s tablet, cell phone, computer, and etc is connected to the internet. This brings a lot of sensitive information into the reach of malicious attackers. “In previous years the Internet of Things was not a big deal," warns Robert Hansen, VP of WhiteHat Labs for WhiteHat Security, "but we’re seeing an increasing number of vulnerabilities in internet capable devices, like TVs, home security systems, automation.” [11]

Sophisticated DDoS attacks are the second attack to worry about in upcoming years. They don’t do any real damage, but they can cause a lot of trouble for companies whose main way to interact with there customers is through the internet. Also, it is thought that most of the traffic on the internet now is due to botnets, which can be controlled remotely by a single user to render larger, more effective DDoS attacks.

Social Media Attacks are the third large attack that Mark Bermingham, director of global B2B marketing at Kaspersky Lab, believes will be the next large attack. Kevin Epstein, VP of advanced security and governance at Proofpoint notes, “In 2015, Proofpoint expects inappropriate or malicious social media content to grow 400 percent as attackers target enterprise social media accounts to perpetrate confidence schemes, distribute malware, and steal customer data.” [11]

**SANS and What They Do**

SANS is an American company that specializes in information security training. It grew out of the belief that instead of rigid rules and regulations, cyber defenses needed a resource that would evolve along with the threats. The consortium of U.S. and world agencies grew into Critical Security Controls. SANS Institute coordinated the recommendations for the Controls center that later became the Council on Cybersecurity, a non-profit, global, and independent entity that is committed to providing a secure internet. SANS is actively collecting and documenting what works in case studies about cybersecurity. [12]

**CERT**

Computer emergency response teams (CERT) are groups of computer experts that respond to computer security incidents. The first one was started in 1988 as a division of the Software Engineering Institute (SEI) in response to the Morris Worm. Now, it has more than 150 cyber experts working proactively to resolve security issues. The CERT division is also considered a national asset for cybersecurity and is recognized as a trusted and authoritative organization. It often partners with academia, law enforcement, government, and industry to create highly developed software to counter cyber attacks. [13]

**Firewalls and What They Do**

Firewalls can be either programs or devices that protect a network or a single computer from from destructive elements. You can think of them as a kind of traffic cop. They can be software, hardware, or both, and they are configured to prevent unauthorized access to a network. In a large corporation, they can protect up to thousands of computers by blocking packets of information that are seen as dangerous. In order to be fully effective, they should be put at every connection to the internet. Surprisingly, they can also control outbound traffic in a large company. There are several different strategies that Firewalls use to keep a system safe by traffic control. “Packet filtering is when small chunks of data (called packets) are run through a filter and analyzed. Stateful inspection is where the contents of each packet are not examined, but instead key parts of the packet are compared to a database of trusted information, letting through the packets that pass this test. Firewalls can be configured to filter by several variables: IP address, domain name, protocol, port or even specific words or phrases.” [14]

**Potential Resources in an Organization that are targeted by a network attack**

One of the main things black hat hackers are interested is personal information. Robert J. McCullen, Chairman, Chief executive officer and President of Trustwave said that “Cybercriminals will never stop trying to compromise systems to obtain valuable information such as customer and private user data, corporate trade secrets and payment card information.” [15] The healthcare industry is another field that is getting hit hard by hackers. In 2014, 600+ breaches were made and the community that received the most cyber attacks, was healthcare. Using extremely sophisticated phishing emails, the cyber criminals took personally identifiable information from 4.5 million people out of Community Health Systems (CHS) alone. [16] Another interesting resource hackers may be after isn’t actually something they can directly get, but more like something they can prevent. DDoS attacks, as previously mentioned, are often seen as passive attacks, but according to incapsula.org, they can often cost the company being harassed up to $40,000 per hour. [17] Who need sabotage when you can just launch a DDoS attack?

**Desirable Qualifications of Personnel to Hire in Security**

A person looking for a job in network security can expect to “detect, prevent and resolve security threats to computer networks.”[18] They are also responsible for maintaining the integrity and confidentiality of a system’s data and information systems. A bachelor’s degree in a computer-related field is generally required, as well as experience in information technology, networks, and network security. Other areas of knowledge should include “network access control (NAC) systems, firewalls, routers, incident response techniques, intrusion prevention systems, information security methodologies, authentication protocols and different attack types.” [18 ] Certifications such as Certified Information Systems Security Professional (CISSP), CompTIA, and the Cisco Certified Network Associate (CCNA) are other desirable traits in a candidate.

**Salaries of Security Personnel**

Security personnel salaries differ within organizations and across different disciplines. A Network Security Engineer earns an average salary of $84,000 according to Indeed.com. Different from a Network Security Engineer, a Network Security Administrator earns an average salary of $71,000, and a Network Specialist only makes an average of $55,000 a year. [19]

**Certifications in Security**

Certifications in security are generally tests taken by security personnel that, once passed, will provide that individual with accreditation. They are highly valuable as many employers require individuals to have them, and if the person does not have the certification they require them to get it within a certain amount of time working for their company. It’s a way of proving your skills to your employer. Depending upon the individual test, they are usually offered at specific testing centers within each state. The cost is usually between $100 and $600 according to individual research of this author. Table 1: Job Board Search Results shows what the most popular certifications are. From this, it appears that the Certified Information Security Manager (CISM) test is the most sought after by employers, although it would depend upon the individual employer. [20]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **SimplyHired** | **Indeed** | **Dice** | **LinkedIn** | **TechCareers** | **JustTechJobs** | **Total** |
| **CEH** | 3,789 | 2,364 | 288 | 1,197 | 2,354 | 234 | 10,226 |
| **CISM** | 69,997 | 3,965 | 645 | 1,447 | 8,689 | 366 | 85,109 |
| **CISSP** | 66,939 | 13,271 | 2,014 | 6,013 | 12,755 | 1,401 | 10,2393 |
| **GSEC** | 2,101 | 1,581 | 218 | 651 | 266 | 177 | 4,994 |
| **Security+** | 3,497 | 2,772 | 226 | 999 | 468 | 328 | 8,290 |

**Table 1: Job Board Search Results**

**Source: TomsITPro.com**

**CCNA Security**

The Cisco Certified Network Associate Security (CCNA Security) is a validation process that proves an individual has the knowledge to secure Cisco networks. This certification demonstrates that the professional has the skills required to “develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. The CCNA Security curriculum emphasizes core security technologies, the installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that Cisco uses in its security structure.” [21] The best way to prepare for the test is a five-day instructor-led course offered by Cisco Training Partners. The price of the course is about $3,500 and the price of the test is between $150 and $250. It is interesting to note that you must be recertified every three years. The test is 90 minutes and the passing rate is 85%. [22]

**What is a CISSP?**

CISSP is a vendor-neutral certification, ideal for “those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their overall information security program to protect organizations from growing sophisticated attacks. Backed by (ISC)², the globally recognized, not-for-profit organization dedicated to advancing the information security field, the CISSP was the first credential in the field of information security to meet the stringent requirements of ISO/IEC Standard 17024. Not only is the CISSP an objective measure of excellence, but also a globally recognized standard of achievement.” [23] CISSP is a 6 hour test with 250 questions and requires at least a 700 out of 1000 to pass. These tests are offered at Pearson Vue Testing Centers and the standard cost for an American is $599. The standard pass rate for the CISSP exam is 70%. [23] You must have five years of work-related experience to become CISSP certified and recertification is required every 3 years. According to simply hired, Trustwave, Boeing, Dart Container, Dignity Health, Northrup Grumman, Cybercoders, Kaztronix, Healthit Jobs, Home Depot, and Verizon Wireline are just a few of the companies that require CISSP certification for information security positions. [24] The average salary range for a CISSP certified professional is between $73,000 and $120,000. Figure 2 shows the median salary of individuals with a CISSP by job. Job titles include such things as Information Security Analyst, Information Technology Director, Security Architect, Security Engineer, and a host more. [25]

**What is a Network + Certification?**

Figure 2: CISSP Median Salary by Job

Source: PayScal.com

CompTIA Network + certification is another vendor neutral network certification that is highly sought after by worldwide employers. It proves that a technology specialist has the skills needed to aptly design, configure and implement any wired or wireless devices. The test is 90 minutes long with no more than 90 questions on the test. You must score at least 720 out of 1000 points to pass the test and the cost is around $250. There are many online resources available including one named CertMaster which will help you prepare for the Network + Certification test. It is also recommended that you have at least 9 months of job-related experience before attempting the test. [26] There was no available information from a reputable source concerning the pass/fail rate of this test.

**CPE’s**

CPE stand for Continued Professional Education. Basically, after someone is professionally certified, they are required to get a certain number of CPE units each year to continue their learning. The general understanding is you can get 1 CPE for every hour of learning. The CPE’s have to be reported each year and kept track of. Depending on which certification you have, you may have to earn anywhere from 40 to 120 CPE’s before recertification, which, as we discovered above, is about once every 3 years. There are lots of different ways to earn CPE’s – some are free and some are not. Conferences are a good way, but often cost money. Reading books and magazines are one way, but there is generally a limit, so writing your own book is another option. Podcasts, webcasts, and even being a supervisor are all other ways to earn CPE’s. [27] The CISSP certificate requires 40 CPE’s to be recorded every year, so 120 CPE’s before recertification. Neither the Network+ certification nor the CCNA require CPE units, but CompTIA does have a CPE program that you are automatically enrolled in if you take the Network+ Exam.

**Conclusion**

As network security continues to be an evolving career of interesting and exciting opportunities, it is important to understand the particular details related to the job. There are five main categories of threats: passive, active, distributed, insider, and close-in. Mitigation techniques are broad, but it is thought that awareness and training of employees is one of the most effective methods, while being the least costly. Network forensic tools are just starting to develop, with some of the first tools recognized being eMailTrackerPro and WebHistorian, as well as Honeypots and Honeynets. Unauthorized access is often required by law to be reported if seen by other individuals, although it does depend on the specific employer and company policies. Stuxnet was a highly sophisticate worm that attacked Iranian centrifuges and crippled their Uranium Enrichment plants. Although Stuxnet is no longer a problem, hackers are continuing to find ways to cause problems. The top three network attacks that experts think will happen in the future will involve the Internet of Things, more sophisticated DDoS attacks, and social media. SANS institute is an educational organization committed to providing training for information technology and security. CERT is a group of organizations also committed to providing necessary resources for cybersecurity personnel. Firewalls are like the traffic cop of a network, reviewing and monitoring incoming and outgoing packet traffic for a given network or computer. Most resources that are targeted by cyber attackers are personal information found in a company’s data. The qualifications for network security personnel usually include a bachelor’s degree in a field related to computer science. Certifications such as the CISSP, CCNA, and CompTIA Network+ will also help ensure a career in information security. CPE’s are Continued Professional Education often required to maintain one of the previously mentioned certifications. A career in network security can be an exciting one; however, as examined in this paper, there are many things to learn and many requirements in order to be successful.

**Resources:**

[1] Computernetworkingnotes.com, 2015. Retrieved October 15, 2015 from [http://computer‌networkingnotes‌‌.com/network-security-access-lists-standards-and-extended/types-of-attack.html](http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html)

[2] Networkmonitoring.com, 2015, Network Security Threats, Retrieved October 15, 2015 from <http://www.networkmonitoring.org/network-security-threats/>

[3] Minutella, David., Cioara, Jeremy., Stevenson, Heather., 2008. CCENT Exam Prep: General Network Security, Mitigating Network Threats, Retrieved October 15, 2015 from [http://www.pearson‌itcer‌tifi‌cation.com/articles/article.aspx?p=1151753&seqNum=3](http://www.pearsonitcertification.com/articles/article.aspx?p=1151753&seqNum=3)

[4] ExamCollection.com, 2015, Network Security: Common threats, vulnerabilities, and mitigation techniques. Retrieved October 15, 2015 from <http://www.examcollection.com/certification-training/network-plus-network-security-common-threats-vulnerabilities-mitigation-techniques.html>

[5] Meghanathan, Natarajan; Allam, Sumanth; Moore, Loretta, A., April, 2009. International Journal of Network Security & Its Applications (IJNSA), Vol .1, No.1,14. Tools and techniques for Network Forensics.

[6] Henderson, William. Nov 7, 2011. Self-Reporting Potential Security Clearance Issues. Retrieved October 15, 2015 from <https://news.clearancejobs.com/2011/11/07/self-reporting-potential-security-clearance-issues/>

[7] Intrusion.com, 2015. Regulations for NPI & PII. Retrieved October 15, 2015 from [http://www.intr‌us‌ion.com/index.php?option=com\_content&view=article&id=30&Itemid=60](http://www.intrusion.com/index.php?option=com_content&view=article&id=30&Itemid=60)

[8] Wikipedia.org, 2015. Stuxnet. Retrieved October 15, 2015 from <https://en.wikipedia.org/wiki/Stuxnet>

[9] Kushner, David. February 26, 2013. The Real Story of Stuxnet. Retrieved October 15, 2015 from <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>

[10] Zetter, Kim. November 3, 2014. An Unprecedented Look at Stuxnet, the World’s First Digital Weapon. Retrieved October 15, 2015 from <http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>

[11] Bradley, Tony. January 14, 2015. Experts pick the top 5 security threats for 2015. Retrieved October 15, 2015 from <http://www.pcworld.com/article/2867566/experts-pick-the-top-5-security-threats-for-2015.html>

[12] SANS.org. 2015. Critical Security Controls for Effective Cyber Defense. Retrieved October 15, 2015 from <https://www.sans.org/critical-security-controls>

[13] Cert.org. 2015. Carnegie Mellon University. Retrieved October 15, 2015 from [http://www.cert‌.org‌/about/](http://www.cert.org/about/)

[14] PCtools.com. 2015. What does a firewall do?. Symantec. Retrieved October 15, 2015 from <http://w‌ww‌.pct‌ools.com/security-news/what-does-a-firewall-do/>

[15] Trustwave.com. 2013. Trustwave Reveals Increase in Cyber Attacks Targeting Retailers, Mobile Devices and E-Commerce. Retrieved October 15, 2015 from [https://www.trustwave.com/‌Company/‌Newsroom/News/Trustwave-Reveals-Increase-in-Cyber-Attacks-Targeting-Retailers,-Mobile-Devices-and-E-Commerce/](https://www.trustwave.com/Company/Newsroom/News/Trustwave-Reveals-Increase-in-Cyber-Attacks-Targeting-Retailers%2C-Mobile-Devices-and-E-Commerce/)

[16] Sherry, J.D. December 19, 2014. Healthcare Industry: The Top Target of Cyber Attacks. Pharmacuetical Compliance Monitor. Retrieved October 15, 2015 from [http://www.pharma‌compl‌iancemonitor.com/healthcare-industry-top-target-cyber-attacks/8175/](http://www.pharmacompliancemonitor.com/healthcare-industry-top-target-cyber-attacks/8175/)

[17] Incapsula.com. 2015. Denial of Service Attacks. Retrieved October 15, 2015 from [https://www.‌inca‌psula.com/ddos/ddos-attacks/denial-of-service.html](https://www.incapsula.com/ddos/ddos-attacks/denial-of-service.html)

[18] Study.com, 2015. Network Security Specialist: Job Description and Requirements. Retrieved October 15, 2015 from [http://study.com/articles/Network\_Security\_Specialist\_‌‌‌Job\_Description‌\_and\_Requirements.html](http://study.com/articles/Network_Security_Specialist_Job_Description_and_Requirements.html)

[19] Indeed.com. 2015. Network Security Engineer Salary. Retrieved October 15, 2015 from [http://www‌.indeed.com/salary/Network-Specialist.html](http://www.indeed.com/salary/Network-Specialist.html)

[20] Tittel, Ed. September 3, 2015. Best Information Security Certifications for 2015. Retreieved October 16, 2015 from http://www.tomsitpro.com/articles/information-security-certifications,2-205.html

[21] Cisco.com. 2015. CCNA Security. Retrieved October 15, 2015 from [http://www.cisco.com‌/web/‌learning/certifications/associate/ccna\_security/index.html](http://www.cisco.com/web/learning/certifications/associate/ccna_security/index.html)

[22] Abbas, Naveed. June 23, 2014. How to pass CCNA certification in first attempt. Retrieved October 16, 2105 from <http://www.holidayeducationist.com/pass-ccna-certification-first-attempt/>

[23] ISC2. 2015 CISSP® - Certified Information Systems Security Professional. Retrieved September 24, 2015 from https://www.isc2.org/cissp/default.aspx

[24] SimplyHired.com. 2015. Retrieved October 16, 2015 from [http://www.simplyhired.com/‌search?q‌=cissp&pn=3](http://www.simplyhired.com/search?q=cissp&pn=3)

[25] InfoSec Institute. 2015. Average CISSP Salary 2015. Retrieved October 16, 2015 from http://res‌ources.‌‌infosecinstitute.com/average-cissp-salary-2013/

[26] CompTIA.com. 2015. CompTIA Network+. Retrieved October 16, 2015 from [https://certification.‌comptia.org/certifications/network](https://certification.comptia.org/certifications/network).

[27] Parker, Jeff. April 20, 2011. CISSP Continuing Education Requirements. Pearson IT certifications. Retrieved October 16, 2015 from [http://www.pearsonitcertification.com/articles/article.‌aspx?p=‌1701053](http://www.pearsonitcertification.com/articles/article.aspx?p=1701053)