Fall 11-30-2016

# Who's In and Who's Out?: What's Important in the Cyber World?

Tony M. Kelly
kellya12@student.lasalle.edu

Tony Kelly

Dr. Narendorf

Professor McCoey

HON 499

29 November 2016

# **Who's In and Who's Out: What's Important in the Cyber World?**

## I. Introduction

Since the dawn of the 21st century, the word "cybersecurity" and its prefix "cyber" have grown exponentially in usage and in importance. In the last ten years, the realm of cybersecurity has exploded with public, professional, and academic interests. In his revolutionary work, *Blown to Bits*, Hal Abelson touches on the rapid growth of the digital world as a whole, remarking that "The world changed very suddenly…the digital explosion is changing the world as much as printing once did – and some of the changes are catching us unaware, blowing to bits our assumptions about the way the world works…" (2-3). Abelson is not alone in his recognition of how quickly the world is changing due to technology. In their book "The New Digital Age: Reshaping the Future of People, Nations, and Business", co-authors Eric Schmidt and Jared Cohen write that "We believe that modern technology platforms…are even more powerful than most people realize, and our future world will be profoundly altered by their adoption and successfulness in societies everywhere" (9).

Amid this technological revolution, the importance of secure computing, data storage, and communication is at an unparalleled high, and it is not likely to see a decrease in priority. As the general public's usage and dependency on technology increases, so do the efforts to maintain a safe and stable infrastructure for those new technologies. Those efforts to tighten security are often hastened by the antagonistic countermovement of developments that are designed to threaten and destroy the same integrity that this new technology both necessitates and creates. World famous security expert Bruce Schneier's book, *Beyond Fear*, describes this direct relationship of the proliferation of these attacks and the defense thereof, writing "…and so changed the defensive front, just as quickly as the attacks did…" (Schneier, 5). It is not difficult to see how quickly one side will react to its opposition.

The aim of this paper is to attempt to uncover the major and most important concepts of cybersecurity. Meaning, what are the important topics, practices, skills, and systems for an individual looking to gain practical knowledge and experience within the cyber arena. This paper will provide readers with an erudite knowledge of cybersecurity themes and language, a comprehensive background about common practices, vulnerabilities, and prevention methods, and a working understanding of the critical importance of cybersecurity and its effects on the world.

To properly ascertain the most important themes of cybersecurity, the question of "importance" is addressed under two lights: one, which attempts to determine the most important cybersecurity topics in the realm of academia, and the other, which aims to understand the most important cybersecurity matters within the professional worlds. This information is blended with a bevy of personal research and experience to properly unmask the key concepts within the rapidly advancing field of cybersecurity.

## II. Information Procurement

This information will be collected from a variety of sources. Much of it is derived from scholarly works (generally consisting of journals or papers) from the Institute of Electrical and Electronic Engineers (IEEE), the National Institute of Standards and Technology (NIST), and the

Association of Computing Machinery (ACM). Media sources from various public and technical news outlets are incorporated, as well various books about computing, cybersecurity, cyber warfare, and technical education. Lastly, the paper includes research from personal experience in cyber competitions and personal penetration testing during two internships at Northrop Grumman Corporation and during undergraduate studies at La Salle University. Additionally, graphs, charts, and some slides might be referenced to provide a visualization of data.

## III. Penetration Testing

The term “penetration testing” is common in the security field, especially when dealing with cybersecurity. Kevin Henry, a security expert and well-known public speaker, defines penetration testing as “…the simulation of an unethical attack of a computer system or other facility in order to prove the vulnerability of that system in the event of a real attack” (xii). Penetration testing is the most common method of evaluating the strength of a security system, and is employed both in academic and professional environments with great frequency. Penetration testing is primarily composed of two components, the hacker and the hacking operating system, and the victim and the victim’s system. In figure one, the info graph shows the systematic flow of penetration testing.

http://www.slideshare.net/anishcheriyan/

*Figure 1: Cheriyan, Anish, Dr. "Penetration Testing Dont Just Leave It to Chance." Slideshare. N.p., 39 Nov. 2015. Web. 23 Nov. 2016.*

The term “hacker” is rather encompassing, and is rightfully categorized by three major distinctions. Colloquially referred to as “hats”, there are three colors which represent the intentions of the hacker. A white hat is a hacker who performs penetration testing for academic, educational, or ethical purposes. Normally found in the security industry, a white hat may be a contractor from a security firm who is recruited to test the integrity of a network. The antagonist of the white hat is the black hat, whose intentions are generally malicious and whose attacks are for personal or commercial gain. These hackers are individuals who seek to crack the hardened security practices established by the white hats, and are normally represented by cyber criminals and opposing governments. A median of each extreme is the grey hat, whose intentions are blurred somewhere in between the white and black hats. Grey hats may, at times, violate certain laws or ethical procedures that white hats uphold but do not harbor the same intent as those in the black hat family.

Script-kiddies are a splinter group that don’t necessarily fit into the other three categories. This group consists solely of those users who are only capable of downloading and using a tool, often incorrectly, without making any modification or customizations of their own. Script-kiddies are universally dismissed by the cyber community, regardless of hat color. Though, they can cause havoc on systems or stop others from causing damage, even with their relatively low skill level.

Penetration testing, in most cases, is performed within a virtual network instead of a live network. A virtual network, simply, is a network of virtual machines. More technically defined by TechTarget, “A virtual machine is an operating system or application environment that is installed on software, which imitates dedicated hardware. The user has the same experience on a virtual machine as they would have on dedicated hardware” (Rouse, Kirsch). Since these machines are not live systems responsible for hosting services for the end user, they are often safer to test on rather than potentially disengaging an entire network. Further, these virtual machines can be customized into any state desired, and allow for creative situational testing.

## IV. Technical Terminology

Some of the more complicated technical terminology and concepts used need to be understood to provide the appropriate background. The following terms have been defined for the purposes of this essay:

- **Hardening** means that the computer or the network has had many of its possible vulnerabilities removed and resolved.

- **Open-Ports / Port Scanning** means checking a system, network, computer, or server for an open connection to the computer that is ready to receive communication or data inputs from an outside source. This may leads to malicious entry from afar.

- **Elevation Control / User Permissions** means the user is granted additional abilities to execute commands, create and move files, install and edit programs and software, within the network.

- **Vulnerable Software** is software that can be edited so it may be used maliciously against its creator.

- **SQL Injection** is a type of computer attack where a hacker enters code into a data entry field, which is then executed on the victim's database and allows access to the system.

- **LAMP** is an operating environment that stands for "Linux, Apache, MySQL, and PHP". It is also to as a "web stack", that allows the items to work together create a web application platform.

## V. User Systems and Software

Offensive maneuvers, which are called, "preemptive defensive tactics", are normally sent from a Linux-based operating system. The term "Linux" is encapsulating; as there exist more than 800 different Linux-based operating systems, with twelve of those being extremely common ("Search Distributions"). This is a glaring difference to Windows and Apple based operating systems, which support at most three popular operating systems at most. Although it is not uncommon to find a live (non-virtual) Windows or Apple operating system between the crosshairs of a black hat, it is common that the black hat is running some version of a Linux operating system. This is not to say that Linux systems are not targeted as victims, since Linux is frequently used to host LAMP environments on servers that fall victim to cyberattacks.

The common user will likely have a Microsoft or Apple based operating system, such as Windows 7 or OSX El Capitan, which combine for over two billion users (Thurott). It is common for those who are engaging in offensive security penetration testing to use a Linux distribution, since it is much more malleable than an orthodox operating system (Thurott). It can be installed and run on both a [normally Windows configured] personal computer, or a computer manufactured by Apple. These Linux systems can also be installed on devices such as gaming systems, small circuitry (such as the Raspberry Pi), and even mobile phones.

The most common Linux distribution used for offensive security is Kali Linux, which was designed specifically for penetration testing, and comes prebuilt with more than one hundred tools and functions ported specifically for penetration testing and cyber security.

Because of its availability, flexibility and potential for customization, it is frequent to find an attacker using some branch of a Linux operating system for an attack. Microsoft Windows is the most commonly targeted system, as more than half of all personal computers (1.5 billion daily users) and slightly under half of all servers are running some variant of a Windows operating system (Thurrott). Other Linux distros, such as Ubuntu Server and Ubuntu Desktop, CentOS, and Apache are all common operating systems to fall prey to black hat attacks as well, since they are also popular end user and server systems. It is less common to find an Apple based system as a victim of a cyber-attack. This is largely due to the intentions of the famous Apple operating system, which exists to provide an easy user experience and to provide a computing experience for the creative end user. The operating systems are not very customizable, often rigid, and Apple systems are rarely used to host public servers, as it is a general rule of thumb that an Apple server can only host other Apple devices.

The oft-quoted flexibility of the Linux operating system and its numerous derivations exist Linux is a version of open-source, allowing for both individual and communal editing and customization. The open-source feature makes it clearly invaluable to any user within the cyber spectrum; because the unmatched customization is vitally important.

## VI. The Importance of Open-Source in the Cyber World

Open-source code, or open-source programs, "…refers to something people can modify and share because its design is publicly accessible" (Redhat). This way, the source code is published freely to the public, and is highly customizable, allowing for users to edit or modify the program (or in this case, operating system) as they see fit. The open-source initiative (OSI) is a massive movement, with household names such as Google Chrome and Mozilla Firefox being created because of multiple individuals and groups sharing code and collaborating on these extensive projects. One example of the sheer power of open source software would be the Apache HTTP Web Server, which hosts at least 51% of all websites (W3). The OSI affects all areas of technology, with the cyber arena falling under that umbrella. Many of the tools used in penetration testing and cyberattacks,  (one tool, the Low Orbit Ion Cannon (LOIC) was responsible for destroying and closing many websites from the Church of Scientology during Anonymous' famous Project Chanology), are open source tools and projects. Since the code is available publicly, users and communities can manipulate these tools as they see fit. (Norton). The LOIC is freely available in the Kali distribution of Linux.

Kali is also equipped with many other tools useful for both penetration testing and cyber education. Some of these include: nmap (short for Network Mapper), which is an open source tool capable of detecting a myriad of information about the victim such as open ports, what services are running, what operating system is running, and what types of defenses are currently in use. An equally powerful penetration testing tool is hping3, which can send a large amount of data packets and can simulate common attacks such as a Denial of Service (DoS), Distributed Denial of Service (DDoS), and a SYN flood attack. Kali does include several tools designed for educational purposes as well, such as Metasploit, which is the most downloaded free penetration tool (Rapid7 Penetration Testing). Metasploit allows for the creation of common types of infections such as rogues, keyloggers, and personal password crackers. Metasploit’s functionality can be graphically augmented by another piece of software, called Armitage, which provides visual displays and explanations for many of Metasploit’s functions. These are often used in cyber education.

This small handful of tools is a minute representation of the vast number of open-source options that exist in the cyber world. Though software like nmap, metasploit, hping3, and the Low Orbit Ion Cannon are capable of immense damage and have been used in some of the more famous breaches in recent history, there are thousands of other utensils used for penetration testing. Another utility, Cain and Abel (often abbreviated CAIN), is a password cracking tool developed for ethical purposes. Having the capability to recover various types of passwords, such as the passwords to wireless networks and user accounts on those networks, CAIN is often used for educational purposes and for penetration testing. Akin to CAIN, Aircrack-ng monitors or “sniffs” wireless networks to capture information about the data, or “packets”, being transmitted across the network. It also offers similar cracking services as CAIN, allowing users to crack the passwords for protected wireless networks. Other tools such as Maltego and Nikto serve as “vulnerability scanners”, or quick scanning tools that check for common vulnerabilities and weaknesses in a network, such as open ports, missing passwords, or absences in normal defense protocols (such as a firewall). Another type of tool, headlined by John the Ripper, is an advanced type of hacking utility intended to quickly break and reassemble hashes and hashed passwords. Hashes, often used in the storage of passwords in Windows and Linux operating systems, are generally very difficult to crack due to the complexity of the algorithms that are used to generate them. However, tools like John the Ripper convert any average computer user into a script-kiddie capable of significant damage. Figure two illustrates other types of open source tools and software.

http://www.slideshare.net/anishcheriyan/

*Figure 2: Cheriyan, Anish, Dr. "Penetration Testing Dont Just Leave It to Chance." Slideshare. N.p., 26 Nov. 2015. Web. 23 Nov. 2016.*

This array of attack methods is a supple example of the raw power of the OSI and its affiliated programs, dually serving as a testament to the ease for an average computer user to transform into a potent hacker.

## VII. Social Engineering

Even though Linux systems are often hosts to a various types and degrees of cyber-attack methods, they are not the only option for a cyber-attack, especially on a large scale. The more common method, attempted millions of times each day, is done through cleverly deceptive social engineering. Social engineering is the concept of breaking the user, not the security system in place. Social engineering is deployed when an attacker, usually in a team, attempts to trick the user of the targeted system into releasing confidential information, such as log in credentials, instead of directly attacking the system itself.

The concept of social engineering is not new to the modern era, as it has been used for thousands of years. The Trojan Horse tale (the namesake for a Trojan Horse virus) tale from

Hellenic Greece writes that during the Trojan War, the Greeks constructed a massive wooden horse with the intention of fooling the Trojans into believing that this horse was simply a delivery of good will and faith. However, the Greeks had actually hallowed out the horse and filled it with their bravest and strongest soldiers, who would (after admittance to Troy), escape the horse and wreak havoc on the city. After some convincing from a deserted Greek soldier, the horse was accepted and brought through the impregnable walls of Troy. That night, the Greek soldiers escaped, and Troy fell.

The Greeks recognized the strength of the defense (walls and army) of the Trojans (victim system), and knew that it would be impossible or, in an optimistic scenario, very difficult to “crack” the system. Therefore, the Greeks employed a social engineering tactic to trick the users (Trojans) of the system to grant them access. This is a perfect microcosm of the devastating destruction that social engineering can cause (“Trojan Horse”).

Social engineering attacks have affected a large number of today’s internet users, with most not even recognizing that they have been targets of such an attack. One of the most well-known and widespread attacks, coined as the “Nigerian Prince Scam”, comes in the form of an email (often in the Spam, Junk, or Clutter folders) from a purported Nigerian Prince, who has a vast amount of wealth that they need to transfer. The email then asks for the user’s banking information in order to transfer the money, but when the user supplies their banking information, the black hat behind the Nigerian Prince hack takes the information and instead funnels money out of the account. Eric Schmidt and Jared Cohen note that this type of attack is a “world leader in online scams” (154). These types of illusory social engineering faints are responsible for up to $12.7 billion dollars in damages worldwide (Peters, 7).

Social engineering has been used in tandem with other hacking methods to achieve greater access and additional mayhem. In 2013, retail giant Target fell victim to a cyber-attack which resulted in the disclosure of more than forty million credit card numbers, as well as other sensitive information, being released. In order to do this, the hacking group (who remains unknown) employed social engineering to discern that Fazio Mechanical Services was the organization responsible for installing and repairing Target's Heating, Ventilation, and Air Conditioning (HVAC) systems, and was thus a contractor of Target. Fazio had much weaker defenses in place and employees who were not as versed in cyber-defense and aware of cyber-threats. The hackers used a phishing email to retrieve log-in information from Fazio employees. Once the hackers gained access to Fazio's systems, they then used other hacking methods to recover log-in information to Target's systems, which they used to then steal the credit card information.

Despite their simplicity and effectiveness, social engineering attacks do not exclusively target technologically unaware individuals. In 2011, RSA, a very well-known networking and computing security company, was hacked via a social engineering breach which resulted in a $66 million-dollar recovery effort. Per official documentation from RSA, "…The attacker in this case sent two different phishing emails over a two-day period…to two small groups of employees…The email subject line read '2011 Recruitment Plan" (Peters). The wording of the email message was convincing enough for one employee to open the spreadsheet, which unleashed a malicious virus created by the black hat team. Again combining the techniques of social engineering with the craftsmanship of hacking, the spreadsheet contained a zero-day exploit through Adobe Flash Player which allowed the black hat team to breach the RSA's networks completely unscathed ("Common Vulnerabilities and Exposures"). A zero-day exploit is a vulnerability that the software vendor is unaware of, and is thus taken advantage of for malicious purposes by non-ethical hackers. RSA's security breach sent a vicious shockwave throughout the security community; even security companies were no longer safe from social engineering attacks.

## VIII. An Introduction to Cybersecurity in the Business World

As stressed early in this document, the importance of security in a world that is ever-growing in its dependency on technology cannot be over emphasized. Daily, there are billions of people who use the internet and computer based systems, and the majority of those users are protected by some type of security (Davidson).

Naturally, the need for protected communication is only intensified in certain areas of business. Though different types of business may require more emphasis on certain areas of security than others, there is a harmony that regardless of which business type is examined, that there is an unfaltering need for secure operations. The large-scale role and paramount importance of security is not overlooked by modern-day computer scientists. In *Beyond Fear,* security-guru Bruce Schneier devotes a number of pages in his book to the discussion of security in modern business, and how much different – and how important – it is to have a robust and resolute security system. "At a basic level", he writes, "security systems are different from any other type of system. Most systems…are useful for what they do. Security systems are useful precisely for what they don't allow to be done" (50). Bruce continues later, citing an example. He describes a scenario that a general home defense system, such as defending a house in Brussels, might include a number of tactics that would be rendered useless for a home in Buenos Aires, where those types of defenses would be futile because the attackers in Buenos Aires would attack using completely different methods. In cybersecurity, however, the concept of defending yourself against a small number of attacks is trivial. Schneier masterfully describes this notion by expanding his analogy to a computer network, detailing that "…if you run a computer network in Brussels, Argentine attackers can target your computer just as easily as they can target any other computer in the world. Suddenly, the list of potential attackers has grown enormously" (97). Schneier, as are many others, are cognizant of the sheer necessity of cybersecurity in the business realm.

For the purposes of this paper, business has been classified into three primary groups: public, private, and personal. This paper defines public business as encompassing retailers, including giants like Sony and Target. Additionally, any government offices, such as the Department of the Treasury, the Department of Homeland Security, or government-affiliated groups such as the Democratic or Republican National Committees dually fall under the public domain. This "government" title also extends to foreign governmental-like systems and bodies. This paper then assigns security contractors, such as RSA, Northrop Grumman Corporation, Lockheed Martin, and Booz Allen Hamilton (to name a few) to the private realm. Lastly, the personal category is generally full of smaller, more personalized businesses, whose operations differ greatly than those of many public or private giants. For that reason, personal business was not examined in this essay. Figure three provides a visual representation of the "size" of some of the largest data breaches, represented by bubbles.

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

*Figure 3: McCandless, David, Tom Evans, Miriam Quick, Ella Hollowood, Christian Miles, and Dan Hampson. "World's Biggest Data Breaches & Hacks — Information Is Beautiful." Information Is Beautiful Visualizations. Information Is Beautiful, 24 Sept. 2016. Web. 06 Oct. 2016.*

## IX. Famous Attacks in the Public Business Sector

Figure three lists come of the companies and organizations that have been breached. Cybersecurity's role in public business sector has been of large-scale importance as early as the 1980's. Just as quickly as public business became dependent on the internet, terms like virus, worm, and infection became applicable to computing; an alien field for words with biological connotations. In early 1988, MIT graduate student Robert Morris created what would become the first documented "worm" on the internet. Though he claims he created it with a white-hat intention of indexing the size of the internet by exploiting vulnerabilities in the Unix sendmail and rsh/rexec protocols and applications, his worm self-replicated to an unforeseen degree and ended up causing an incredible amount of damage by overloading various systems. Robert was later found guilty of violations against the Computer Fraud and Abuse Act, despite his benevolent intentions (Goodchild).

A computer worm shares similarities to the well-known computer virus because both types of infections replicate themselves before unleashing their malicious payloads (and in some cases, the malicious payload is the replication). However, a worm is different and much more dangerous. Unlike a computer virus, a computer worm does not latch onto existing files to replicate. Instead, it is self-replicating and does not have the need for a host. The rapid file replication often clogs bandwidth, taking some networks completely offline. Worms are also well-known to open many "backdoors", exposing other parts of the computer network or system that were previously thought to be protected, leaving the administrators [and users] completely unaware of their vulnerability.

Thus, when Robert Morris' creation wreaked such havoc without malintent, it wasn't long before the public industry realized the possible extent of the damage a powerful worm could cause. Two of the expensive attacks on public industries are results of exploits by computer worms.

The first and most notorious was the “ILOVEYOU” or “LoveLetter” worm, which was responsible for over $15 billion in damages in 2000. Estimated at its worst to have affected one in every ten emails sent, the LoveLetter infection attacked tens of millions of Windows computers which dominated the business world, and caused massive shutdowns and freezes for numerous companies and corporations, and even some governmental offices (Wildammo).

The second, and the most expensive attack was called “MyDoom”, and was responsible for over $38 billion in damages (Wildammo). First sighted in January of 2004, it became the fastest spreading email worm of all time, and even ended up burrowing its way into companies such as Microsoft and Intel. Because of the time in which it ran rampant – when computing powers were a mere fraction of what they are today – it was very difficult to remove from a network once it begun multiplying on an infected network. Much of the fiscal damage came from the downtime these companies needed in order to remove the infection from their communication networks (Wildammo).

Though worms are capable of inflicting massive amounts of damage, they are not the only type of attack that is found in the public sector. One of the most notorious attacks of all time was the infamous Sony hack in 2014.

In 2014, it was suspected that foreign hackers (likely from North Korea) targeted Sony pictures, likely in retaliation for the recent release of “The Interview”, which had a comical plot featured around assassinating North Korean leader Kim Jong Un. The attackers, known as “Guardians of Peace”, were apparently let into the Sony Pictures building by Sony employees. The Guardians of Peace, who were surprisingly available for comment, remarked that “Sony left their doors unlocked, and it bit them" (Kastrenakes). However, once physically inside the building, the hackers then stole a physical key from someone in the IT department which granted them access as a systems administrator, and as such, unwarranted capabilities in a Role Based Access Control security infrastructure. In a Role Based Access Control security model, users are granted additional access depending on which jobs they are assigned – hence the "role based" namesake. The role of a systems administrator granted them almost universal access. Once there, the attackers planted malware which quickly spread itself throughout Sony Films' networks. The malware found and stole other passwords from within Oracle and SQL databases. Here is where Sony's true errors existed; their open access which opted not to include layered protection methods, led them to be extremely vulnerable. A layered protection that included forms of encryption, hashing passwords, password salts, and requiring different roles to access different levels of information would have helped with additional protection (Bort). Bruce Schneier commented that Sony's security "…clearly failed here" and that their tactics "…turned out to be subpar" (Schneier). Once the Guardians of Peace had infiltrated Sony Films computer network, they stole data, wiped data, and continually suppressed Sony's attempts to rehabilitate their computer systems until Sony agreed to pull the film, "The Interview", from theatres. Despite pleas from United States President Barack Obama, Sony agreed to pull the film (Bort).

Despite the devastating effects of the Sony breach, it still was not the largest hack of all time. In terms of sheer data release, The Yahoo hack of 2014 reigns supreme. Hacking group Peace_of_mind, or often called "Peace", was tied to the attack of Yahoo's database servers which resulted in more than 500,000,000 accounts being stolen. Yahoo discovered that their defenses had been breached when they noticed that Yahoo accounts were being sold on TheRealDeal, a dark web black market site. Their accounts, along with accounts from LinkedIn, MySpace, Tumblr, and Twitter, culminated to nearly 800 million all from the same “store” (or seller) – “Peace” (Greenberg).

Though it is still unknown, or unreleased, how exactly hackers obtained access to Yahoo’s account servers and databases, it was apparent that once they gained entry to Yahoo’s systems, it was not difficult to steal the information, which was likely unprotected (meaning not hashed, hashed and salted, or protected with additional layers of security). The company admitted that some of the information that was stolen was completely unencrypted (Leswing). This bad practice was shared too by LinkedIn, the business-type social media titan. When LinkedIn’s information was compromised, it was found that much was stored as a message text value, but if the information was encrypted, they were doing so with an SHA-1 encryption. The SHA-1 encryption method is a type of encryption algorithm which is static; meaning the math in the algorithm does not change. This type of encryption algorithm is simple and minimally effective; it takes a plaintext password like “1234” and converts it to a hashed, or encrypted password string, 7110eda4d09e062aa5e4390b0a572ac0d2-c0220 (Wood).

The SHA-1 may seem like an effective method to protecting and encrypting information, the SHA-1 method is relatively unsecure. Because of its longtime existence and widespread use, massive libraries and databases exist containing the correct hashed values for millions of potential passwords, allowing for hackers to compare stolen hashed values against these libraries and crack the passwords with very little effort. Further, because of the static design of the algorithm, if two users both have “1234” as their passwords, their hashed values are exactly the same.

A security method to prevent the hashes from providing the same result is called password salting.  The salt entails the company who is storing the passwords to include extra text to enable a much longer and more difficult to crack password (Wood). Salting is incredibly common and is used in almost every instance of password storage [that still relies on SHA-1 Encryption]. However, LinkedIn was guilty of not using any variations of salting to harden the protection on their passwords, and as a result, found that some 73% of their memberships were compromised (Hughes).

This small number of attacks on public business is just a droplet in an ocean of daily cyber threats aimed at disrupting public business. However, the realm of public business also includes governmental bodies and agencies, and they are far from immune to cyberattacks and often find themselves perfectly situated between the crosshairs of many black hats.

## X. Famous Attacks on Governmental Bodies

The public sector of business is dually comprised of governmental agencies as well, who often find themselves as targets for various cyberattacks, ranging from small individual efforts to calculated orchestrations from other foreign governments. Focusing primarily on the United States government, there are numerous agencies devoted to protecting the cyber integrity of the homeland, and this effort is spearheaded by the Department of Homeland Security (DHS).

Devoting a portion of their website to an overview of the stance of the United States government on the cyber world, the DHS writes that “Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy and threaten the delivery of essential services” ("Cybersecurity Overview").

Since 2007, over a dozen federal agencies have been found susceptible to cyberattacks, including a nuclear research laboratory, the Postal Service, and, in one instance, even the White

House (Hernandez). One such government agency is the Department of Veterans Affairs, which has been responsible for denying over 1 billion cyber threats (Bhattacharyya). As illustrated in figure four, those attempts have amounted to a 1300% increase in cyberattacks on government offices in the past 10 years.

http://www.thefiscaltimes.com/2016/06/22/Cyberattacks-Against-US-Government-1300-2006

*Figure 4: Bhattacharyya, Suman. "Cyberattacks Against the US Government Up 1,300% Since 2006." The Fiscal Times. N.p., 22 June 2016. Web. 23 Nov. 2016.*

The United States Pentagon was cognizant of the damage from a cyberattack, and recruited a number of penetration testers to evaluate the strengths and vulnerabilities of their security system. Over 138 security flaws were found on five Pentagon websites (Bhattacharyya).

The U.S. Office of Personnel Management, or OPM, is one of the most damaging cases of a government breach. In April of 2015, it was discovered that the OPM had been breached by foreign hackers (likely from China) (Koerner).

During a routine systems check, security engineer Brendan Saulsbury was decrypting some traffic from the Secure Sockets Layer across OPM's network interfaces. Noticing a weird bit of outbound data, Brendan looked further into the issue before ultimately discovering that this data was being sent from mcutil.dll, a file which is normally contained in a McAfee Virus Scan (Enterprise Edition) package. But, OPM did not use any McAfee products. It was at this moment Brendan identified that OPM's networks were breached (Koerner). Soon afterwards, Brendan and his team noticed that the infection traced back to the name “Steve Rogers”; a trademark signature of a hacker group which was responsible for the damaging Anthem hack that exposed some 80 million Americans' insurance information (Koerner).

OPM's situation is not unlike the disasters experienced by Yahoo, LinkedIn and Sony. After an incredibly thorough and detailed investigation from the United States Computer Emergency Readiness Team (US-CERT), a group from the DHS, it was found that OPM as well suffered from a lack of layered security. During their interviews, US-CERT received testimony that OPM had "…a long history of systemic failures to properly manage its IT infrastructure", which, according to the investigators, could have been easily remediated (Koerner). Using multifactor authentication, according to the US-CERT team, "…is a straightforward way to foil this approach" (Koerner). OPM is not the only US governmental body to be targeted. Recently, the rise of grey hat "hacktivist" groups like the (in?)famous Anonymous have begun to target government agencies and affiliates; including the United States President-elect, Mr. Donald Trump.

## XI. Anonymous

In early March of 2016, Anonymous, the vigilante hacking group responsible for targeting organizations such as the Westboro Baptist Church, The Church of Scientology, Russia, and even the United States Government sent a message to then Republican Presidential Candidate Donald Trump, declaring "total war" on him and promising devastation on April 1 (Klein). Leading to that date, Anonymous published Donald Trump's social security number, cell phone information, and other personal details. Trump's team, aided by the FBI and the Secret Service, was unable to locate a single member of the Anonymous community and could not explain where Anonymous retrieved that information (Klein). As promised, on April 1st Anonymous launched a massive Distributed Denial of Service (DDoS) attack, on Trump Tower's servers after recruiting volunteers on the dark-web portal website 4chan.org.

The DDoS attack is one of the most common, yet most devastating, cyberattacks in the world. In most cases, the attacker will employ the use of a botnet.  A botnet is a large network full of user computers which the attacker has been able to manipulate and gain control.  The botnets are told to perform a certain operation. The attacker will then use this botnet to target a specific victim by setting up the IP address, where the botnet will simultaneously (from each individual node on the network) push forth an incredibly large amount of data, effectively overwhelming the victim recipient and taking it completely offline. Although Anonymous did succeed in taking down Trump's website with their coordinated DDoS attack, it is worthwhile to note that Donald Trump though he did have backup services with old caches pre-prepared, and was able to restore services to his websites relatively quickly. He again demanded the capture and trial of these attackers, but was never able to catch them (Klein).

The Republican Party wasn't the only American political party to fall victim to attacks, however. In July of 2016, in the middle of a historic election period, the Democratic National Committee was also breached, releasing the personal emails of over one hundred party officials. Attributed to non-governmental Russian hackers, "…the personal email accounts of Hillary Clinton's campaign officials and other party operatives" were exposed, and revealing a large amount of information regarding the Democratic National Committee's influence in the primaries (Lichtblau, Schmitt). Some of the information that was released disclosed private conversations between high ranking party members that discussed items relating to Democratic Presidential candidate Hillary Clinton and her Democratic opponent, Bernie Sanders. In the released messages, members of the Democratic National Committee had already committed to naming Clinton their nominee, and were looking at ways to discredit Bernie Sanders in his campaign against Hillary (Hanson).

The effects of these attacks were widespread. The Democratic National Committee hack has, on some cases, been said to have influenced the 2016 United States Presidential election, possibly resulting in Hillary Clinton's loss (Vespa).

Though the United States government has found itself a victim of numerous cyberattacks, they are not the only governmental body that has experienced such a bombardment of persistent threats. Anonymous has also targeted foreign government agencies, both friend and foe to the United States government. In the last year, Anonymous has targeted United States ally Germany, who has since referred to Anonymous as a "terrorist organization" (Philipp).

During an active summer of 2016, Anonymous also targeted the terrorist organization known as ISIS shortly after the Orlando mass shooting. The Orlando shooting, which was the biggest in United States history, was apparently done in the name of ISIS (CBSNews). As a response, Anonymous hacked into dozens of ISIS-controlled Twitter accounts, and posted numerous pictures, quotes, and tweets inspired by pro-LGBTQA+ messages, enraging ISIS sympathizers and leaders. Eventually, the company Twitter condemned the act, stating "We condemn the use of Twitter to promote terrorism and the Twitter Rules make it clear that this type of behavior, or any violent threat is not permitted on our service" (CBSNews). Though unclear exactly how Anonymous managed to gain access to these accounts, it appears that they were able to access secure account information from Twitter's servers, including the IP addresses associated with each account, encouraging other members of the online community to help them (Lee).

The public domain has always been and will continue to be a frequent victim of cyber criminals due to the large amount of financial gain, and the potential for public disruption. Those companies and governmental bodies that find themselves victim of these breaches often have severe security exposure, most normally in their access control protocols. Without implementing a layered level of security, many of these organizations allow for users (with the proper credentials and technical knowledge) to easily promote themselves, thus allowing them to proliferate their attacks throughout an entire network or in some cases [like Sony Films'] an entire company. The graph in figure five illustrates incidents affecting government systems, as reported by the eleven agencies in Bhattacharyya's article.

http://www.thefiscaltimes.com/2016/06/22/Cyberattacks-Against-US-Government-1300-2006

*Figure 5: Bhattacharyya, Suman. "Cyberattacks Against the US Government Up 1,300% Since 2006." The Fiscal Times. N.p., 22 June 2016. Web. 23 Nov. 2016.*

## XII. Cyber Attacks on Business – Private

Public businesses and organizations are not the only victims of cyberattacks. A persistent target of cyberattacks is the banking industry. In the fall of 2014, J.P. Morgan Chase released an official report detailing a severe breach they had discovered in July of the same year.

Though discovered in July 2014, J.P. Morgan Chase recognized that they had been penetrated as early as June, and that this hack released more than seventy-six million personal accounts and over seven million small business accounts, effectively placing this breach as one of the most severe in cyber history (Silver-Greenberg, Goldstein, Perlroth). The attacking group had penetrated the bank's defenses for as long as two weeks before they noticed, but within hours of discovering the breach, J.P. Morgan Chase was able to boot out the hackers and restore order to their systems.

As stated by the New York Times, the breach happened when public trust in the cyber operations of America was already very low, as this attack occurred around the same time as the aforementioned Target attack, as well as attacks on other large retailers, such as Home Depot (Silver-Greenberg, Goldstein, Perlroth). According to a New York Times report, hackers were able to gain access to J.P. Morgan Chase's accounts via another mix of social engineering and clever hacking. The black hat group obtained a list of programs that J.P. Morgan Chase employees use, including applications like Adobe Flash, Microsoft Excel, and SPSS Software. The hackers then cross-referenced this list of applications with all known-vulnerabilities to see if J.P. Morgan Chase's installed systems had been updated to fix the known-vulnerabilities. Due to a laxness in the security team for J.P. Morgan Chase, the hackers found a number of backdoors, or un-remediated security issues, and were able to gain access to the bank's computer networks; siphoning large amounts of private, unencrypted data.

As mentioned by the parameters of this paper, the private sector also includes government security contractors. The two largest organizations, Northrop Grumman and Lockheed Martin, are well versed in cyber defense, as they are frequent targets for attacks both foreign and abroad.

In 2014, Lockheed Martin was hit by at least fifty orchestrated cyberattacks, meaning that these attacks were developed to specifically target Lockheed Martin systems and employees. Though fifty might not seem like an overwhelming number, it was more than the company had ever experienced up to that point (McHale). Lockheed Martin Vice President of Commercial Markets Chandra McMahon said that "Lockheed Martin expects that number to only increase as there are more players, nation states, and other groups, with the capability to deliver cyberattacks…this company is typically targeted due to its work in the defense industry, other arms of the U.S. government, oil and gas industry, and other critical infrastructure (McHale). Out of the fifty attacks, almost all of them included some attempt at social engineering, normally via the spear-fishing tactic. Spear-fishing is considered a type of phishing, where the attackers send out an email message appearing to be from a trusted source in hopes that a user will provide access credentials or expose an unknown vulnerability. Luckily and unlike other attacks mentioned thus far, Lockheed Martin was successful in stopping the majority of attacks in 2014, and did not have a single employee divulge their or any proprietary information (McHale). This is a remarkable achievement in an age where these types of attacks have crippled dozens of organizations.

Lockheed Martin's business competitor and partner, Northrop Grumman Corporation, is also familiar with the cyber industry and finds itself targeted more frequently than Lockheed Martin. At a conference held by cyber victim RSA, with Lockheed Martin in attendance, Northrop Grumman made a shocking revelation to the United States Government and security communities: they are being targeted by numerous distinct hacking groups so much – sometimes as frequently as an attack every eleven minute – that they have actually been able to designate "about a dozen separate legions of organized hackers", who have been "diligently attempting for years to break into…Northrop Grumman to steal sensitive information" (Messmer). Northrop Grumman's cyber-intelligence team has not reacted kindly to these malicious attempts, and the company has devoted a large amount of resources, both in dollars and manpower, to not only stop these attacks from coming in, but to disarm the attackers. As noted by the Chief Information Security Officer (CISO), Timothy McKnight, the most common attack method is to "…compromise user machines through zero-day vulnerabilities. While about 300 zero-day attack attempts were recorded last year, the pace has ramped up enormously where it's not uncommon to see zero-day exploits coming in at eleven-minute intervals" (Messmer). He later added that "Attackers will do as much background investigation on a company as they can to be able to pinpoint the intellectual property they want, and what employees are closest to it" (Messmer).

Northrop Grumman's strong defense against cyberattacks and their low number of vulnerabilities may be due to their efforts for cyber education, mainly through their revolutionary

Cyber Academy program. Cyber Academy is a group of cybersecurity experts, employed by Northrop Grumman, who are trained to provide classes, coursework, and documentation available to any Northrop Grumman employee (“CyberAcademy_overview"). This information is provided on three levels: the first level is intended for any employee regardless of what sector or division they work in, the second is intended for those in management or those with particular roles or responsibilities pertaining to data, information, network, or system security, and the third level is generally reserved with a vetted interest or those who are much more technically adept. These courses are free to all Northrop Grumman employees and are held in a classroom in Virginia, complete with classrooms, labs, assignments, and tests, with Northrop Grumman certifications being issued to those that complete them (“CyberAcademy_overview" ).

The private sector of business is not unacquainted with the cyber world, as they are targeted every day by cyber criminals looking to seize confidential information pertaining to banking, government, and defense operations. However, due to the high-scale business that these organizations conduct, it is clear to see that although they are vulnerable, their level of security is much tighter and more hardened than that of public organizations, especially in retail. Akin to the types of attacks seen in the public sector, it is common for black hats to launch a social engineering attempt in order to gain some degree of access to a private bank or business, and at that point, they can use that opening to exploit other vulnerabilities. Though this is not as affective in the private sector as it is in the public, it is still a testimony to the matchless importance of cybersecurity in the business world.

## XIII. Business – Common Vulnerabilities and Recommendations

Businesses are the most commonly targeted victims of cyber hackers and black hats, much more than an individual users. Composed of industries such as retail, government, and small individual organizations, businesses are responsible for the movement of fiscal traffic all across the globe, thus making them much more enticing targets for malicious computer scientists.

In the public sector, the biggest vulnerability to industries involved in retail is a lack of dedication to maintain a secure environment. A number of technical vulnerabilities including weak access control, employees who divulged classified information, and no password salts resulted in extraordinary damages. But the underlying commonality amongst all of these problems is a severe deprivation of resources into cyber management. Many of the technical issues such as worm proliferation, access control and password salts, can all be resolved with the implementation of newer security methods. Other exploitations, such as zero-day vulnerabilities, are easily remediated with a dedicated IT team who ensure that software is updated as early and often as possible.

In the private business sector, cyberattacks are just as prevalent, but they are much less damaging, and this is likely due to the extraordinary amount of resources, both time and money, that private industries allocate towards their cyber-defense systems. Exemplified by the efforts of security giants Northrop Grumman and Lockheed Martin, it is rare for an employee to fall victim to a social engineering attempt, and it is even less likely that the [seemingly] impregnable defenses of these types of corporations will be brought down by the efforts of an outside party. Even in the event of a breach, such as the one at J.P. Morgan Chase, the response and recovery time is much quicker, thus containing the damage that has already been done.

Even in the private sector, the same types of threats remain, but they are thwarted much more easily due to a tightened focus on employee training and proper security protocols, as compared to the public sector.

Cumulatively, the analysis of public business is applicable to more than that sector, it is overarching for the entire business arena. Companies and organizations that leave themselves vulnerable to improperly managed access protocols, to the lack of dedication maintaining the newest software updates, and to poorly configured password management including an aversion to using default passwords and to applying salts for storage, are likely to be breached by the ever-evolving and growing black hat community. Organizations need to require proper training for all employees to combat cyberattacks and especially, to deter social engineering threats. They also need dedicated resources available for threat containment and removal, and a consistent and driven IT and security force to constantly monitor and thwart penetration attempts. In a world where security is paramount, these issues cannot be overlooked.

## XIV. Cybersecurity in Academia

Cybersecurity education has been growing in the academic realm just as quickly as it has in business areas. Because of this, the United States' Department of Homeland Security (DHS) has created a subgroup, The National Initiative for Cybersecurity Careers and Studies (NICCS) which contains a number of National Centers of Academic Excellence. The website describes, "Our nation is experiencing increasingly complex and challenging cyber-attacks. Nearly one in five Americans has been the victim of cybercrime…" (CAE)**.** Because of this, the NICCS was formed as a joint venture between the National Security Agency (NSA) and academic programs with the intent of finding the best cybersecurity programs in the United States, and designating them as a Center for Academic Excellence (CAE) program. More than two-hundred academic programs in forty-four states, Washington D.C., and the Commonwealth of Puerto Rico have been named CAEs (Gupta).

Designation of CAE requires exploration beyond the formal definition provided by the NICCS. Examination of four different CAE certified schools and the components of their curriculum demonstrated the important concepts and/or courses taught in each of the undergraduate (B.S.) programs.

The first school examined, Towson University, is a public school located in Baltimore, Maryland, and has over 22,000 students. The school offers a very comprehensive undergraduate computer science program with a security track. Some of the pertinent courses that Towson offers include OS Security, Software Quality Assurance, Application Software Security, Selected Security topic, Network Security, and a course on Ethics. ("Major in Computer Science").

The second school examined was Drexel University, which is a private institution located in the heart of Philadelphia, Pennsylvania, and has over 26,000 students. Well known for its engineering programs, Drexel University also boasts a computer science program which offers a number of undergraduate security courses that have resulted in its CAE accreditation. These courses include network security, software security, and a joint computer and network security course ("Computer Science.").

The third and most comprehensive school was the prestigious Carnegie Mellon University, famous for its global recognition for having one of the best computer science programs in the world. Carnegie Mellon is a private university located just south of Pittsburgh, Pennsylvania and has a student population of more than 13,000. It has an incredible array of security programs, and is the only security lab recognized by CERT. Some of the courses in the curriculum include Network Security and Applied Cryptography, Cryptocurrency, and Ethical Hacking.  The Cylab is used specifically for cyber training and coursework. ("Security and Privacy.").

Finally and perhaps the most thorough of the reviewed universities, is the University of Maryland Baltimore County (UMBC) situated in Baltimore County, Maryland. UMBC is a public extension of the University of Maryland education system, with this campus hosting more than 13,000 students. UMBC is home to a cyber-defense lab where numerous undergraduate [and graduate] courses are taught. With an emphasis on malware and viral analysis, courses include systems and security, ethics, computer viruses, and malicious code ("UMBC Center for Information Security and Assurance.").

The aforementioned schools are very different in their composition: geographic location, size, and public vs private. However, they share a commonality in their recognition for outstanding cybersecurity programs. All of the examined institutions offer courses on network security (and theory), ethics (some with an emphasis on ethical hacking), and most offering some version of application or software security.

The shared courses, despite the aforementioned differences, imply that a proper cybersecurity curriculum should contain a number of things. Firstly, there should be an effort to teach secure networking, dictating a need for safe communication, regardless of the content. Curricula should also contain a course on ethics, helping to spread awareness of and increase the importance of penetration testing and the value of using these tests in establishing a hardened system. Additionally, ethics programs also distinguish the efforts of these professionals from hackers who are intent on causing damage. Further, there should be significant attention paid to secure software development, which is important when developing code or new applications. If a program is developed appropriately, the chance of a backdoor vulnerability is low, thus eliminating the threat of a zero-day exposure.

Even those in the business and professional worlds are aware of the need for cyber education. The IEEE library contains a number of papers and journals published by those within the realms of academia and business. One article from the IEEE examines a case study of founding a cybersecurity club in a higher education institution, both for the students and for the institution. In the article, Matt Piazza and Aspen Olmsted describe how a cybersecurity club actually helped to locate malicious traffic moving along the school's network, and provided an opportunity for more introverted students to engage in a large amount of social activity (Piazza, Olmsted). Another article from Purdue University professor Melissa Dark and University of Southern California research professor Jelena Mirkovic identified why "it's common practice to postpone planning an assessment or evaluation until the conclusion of an awareness, training, or education program…", and how that approach "…is a mistake that contributes to less efficient and effective educational programs"  (Dark, Mirkovic). Their research was applied to cybersecurity education to increase the amount of testing in high stress environments, intended to emulate the cyber workplace.

An article from the ACM called for a "Joint Task Force on Cyber Education", and was composed of an international team of computer scientists from Towson University, Intel Corporation, and Nelson Mandela Metropolitan University in South Africa. The article described an effective undergraduate curriculum for cybersecurity, which includes where to teach practical application in the theoretical field of computer science (Burley, et. al) By teaching the theoretical concepts first and then explicating them through real world examples pertaining to cybersecurity, the professors and professionals have found a solution to this complex educational problem.

## XV. Academics – Common Practices and Recommendations

The academic community is teeming with students' interest from a swath of backgrounds, and it is rapidly growing in its importance within the computer science discipline. Cybersecurity is recognized both internally in academia and externally, serving as a demonstration on how the cyber realm has become one of the most targeted concepts for new students' interests. Cyber security is one of the fastest growing and most important fields of study in the twenty-first century. The IEEE is aware of the importance of cybersecurity and recently published a paper titled "The Future of Cybersecurity Education". The paper strongly proselytizes the notion of creating merged ventures between "…government, federal agencies, industry, and academia to work more closely together to defend cyberspace" (Mcduffie, Piotrowski). The article calls for a united effort to spread awareness and training for cybersecurity. This type of coalition-based projects is manifested in the reviewed institutions and their applied academics, such as Carnegie Mellon's Cylab and UMBC's cyber defense lab. Even industry leaders have begun to undertake educational reconstruction, exemplified by Northrop Grumman's Cyber Academy (which also hosts Cyber Patriot – a cyber-tournament intended for high school students) and Lockheed Martin's Cyber Analyst Challenge.

Based on changes in undergraduate curricula, the research of academic professors and the concerns of external organizations, a number of best practices have been proposed and should be considered for adoption. Cyber academics should be taught in conjunction with influence from an outside variable; whether it be a government, federal, private, or industry lead. Strictly, theoretical computer science concepts are not adequate for teaching students proper defense methods and the importance of correct implementation and routine maintenance, which are vital to a secure system. Working in an environment like the Cylab at Carnegie Mellon provides students with a controlled environment to apply these concepts to real world applications. These lab experiences provide valuable foundations that all students to find and fill internships and full-time positions that require the theoretical and practical knowledge in growing cyber industry. Curriculum and course would should include network security, operating system security, and secure software development, while providing controlled lab situations to test and explore the concepts.  Providing a sandbox environment where students can see the results of both good and bad practices can reinforce the importance of the concepts and validate the results helps to reinforce their learning.

## XVI. Results of Research – Personal Experience

Inspirations for this paper include academic coursework, an internship with security contractor Northrop Grumman Corporation, and a cyber-warfare competition.

A brief synopsis of relevant cyber experience includes completion of the Information Security Course at La Salle University. In this class, the professor presented the theoretical concepts of cybersecurity and held a small “hacking competition”, where students were asked to breach the professor’s sandboxed website. While working as an intern at Northrop Grumman, one duty included testing on a classified network, while the internship additionally included participation in a cyber-warfare competition.  The competition was open to all members of the organization. Additional research for this paper included performance of extensive penetration testing on a variety of systems ranging from Linux operating systems to Windows servers in order to find common vulnerabilities in these respective operating systems.

The Information Security Course included the importance of ethical hacking and penetration testing. One activity, a live hacking challenge, intended to bring together the theoretical concepts taught in class with a real world application of them, all while doing so in a sandboxed environment; thus further teaching a lesson on ethical hacking. The professor presented a login screen and asked the class to penetrate the website using whatever tools were needed within a time frame of fifteen minutes. In about thirteen and a half minutes, the system was breached system using a modified SQL-injection. Only two attempts had ever been successful in accessing the virtual system. At this point, it became apparent that even older techniques could still prove useful against a seemingly impregnable system; no defenses are perfect. There was also no alarm system intact to alert the owner or administrator of the site once it had been breached, allowing for a potential hacker to steal or delete an entire database of information before the rightful owner would become aware.

Experience as an intern in Northrop Grumman's Quality Assurance group allowed for some degree of penetration testing, which demonstrated very few vulnerabilities. The system ran on a Linux operating system and easy vulnerabilities including open ports, outdated software, SQL-injections, and access control were not problems on this system. The only vulnerability detected was that the operating system allowed for the creation of other user accounts including administrator accounts. Additionally, testers could run numerous commands using the elevated access status, allowing for data to leave a node on that system unchecked and unflagged, signaling other hackers to target this specific network.

The cyber warfare competition held by Northrop Grumman's Cyber Academy was open to any Northrop Grumman employee. All participants used the same unsecure network and points were based on the following two objectives.

1. Contestants were required to harden the security for the system by removing all existing vulnerabilities.
2. The "hardening" needed to be completed without stopping the system. The system needs to remain operational or "online." It is not difficult to take an entire system

> offline to repair it before restoring its services to the users but this can cost an organization millions (if not billions) of dollars.  Thus, cybersecurity experts must be acutely aware of the damage that can be caused by turning a system off.

As a participant in the contest, I was able to close a number of open and vulnerable ports, discover a large amount of exploitable software including LibreOffice and Mozilla Firefox, reconfigure numerous passwords which were often set to their default values (normally "password"), along with other vulnerabilities without shutting the system down.  This competition spearheaded investigation into common vulnerabilities in many operating systems.

After acquiring premade virtual machines online, the systems were installed and routine penetration testing began.  The testing included the use of numerous open-source tools and techniques to discover vulnerabilities. The research investigated two Linux operating systems: CentOS, Ubuntu Server, as well as one Windows operating systems: Windows Server 2012.

Non-surprisingly, the Linux operating systems yielded a wide variety of weaknesses with relatively no similarities. The CentOS's vulnerabilities included a blank password for the root user account and leaving different files and folders unsecure. Items like the "/etc" and "/bin" folders, which contain vitally important configuration and executable files, are normally unavailable or require special permissions to open. The "root" or administrator account was also normally protected with a password to prevent an average user from gaining access to them, however in this system, these accounts were completely unprotected. Therefore, the testing allowed logging into the super user account and manipulating files in the "/etc" and "/bin" folders, thus granting me unlimited access to the system.

Ubuntu Server was the most unsecure out of the entire bundle. It included a pre-installed LAMP package, riddled with vulnerabilities. The poor security could have led this system to crippling very easily, and in a real-world environment, could have proved detrimental.

Targeting specifically the “MySQL” portion of the LAMP environment, there was no password for the admin entry and no verification of the DROP SQL statement, allowing for any user to sign themselves in as “admin”. Once logged in as an administrator, they could delete the entire database. Moreover, the Apache Web server portion of the LAMP environment was also outdated and contained a known zero-day exploit, meaning that a professional black hat could [and with relative ease] take the entire server offline.

Additional weaknesses in the Ubuntu server include the system’s firewall not recording any logs, meaning that there was absolutely no notation of what type of traffic was going through or leaving the system. Additionally, there were no use of cookies, enabling the system to be hit by a DoS or DDoS attack.

Windows Server 2012 is a complex system which only reveals vulnerabilities with the use of supplemental resources. By default, Microsoft is careful to eliminate common threats such as open-ports, vulnerable software, and user privilege abuse, Integral system files are well protected. However, with the use of resource Nikto, two major weaknesses were identified. The first identified vulnerability used the Microsoft Active Directory Lightweight Directory Service (AD LDS), which allowed for a remote attacker who connected to the server using an SSH connection to query the Active Directory service maliciously.  This caused an internal outage which would quickly take the server offline. The second vulnerability was an issue involving the HTTP.sys file, a crucial file which is normally well protected. Hackers found a way to recode the file and used an infinite loop in the HTTP packet header to overload the server and take it offline. These types of intricate vulnerabilities were only discovered with the help of the Nikto vulnerability scanner.

Extensive testing on these three systems revealed a number of conclusions could be drawn about each variant of operating system. First , it is obvious that different operating system architectures (Unix vs Windows NT-based) will be susceptible to different weaknesses.

Often times the more flexible Unix systems, specifically open source based Linux systems, will find access controls weak and the software prone to zero-day vulnerabilities because of the rapid changes in the development. Being open-source means that (generally) an entire community is continually updating and modifying a program or operating system. This implies that an equal sized, if not larger community, is seeking ways to attack those defenses. Additionally, with so many people working on such a complex system, defenses are sometimes lowered to allow for the rapid and numerous modifications, providing attackers a brief period of weakness. This often happens during an update when a specific service is be turned off.

Windows NT-based operating systems have a much different architecture, and generally provide much less flexibility. The software and updates are managed by a dedicated team from one company (Microsoft). Because of the complexity of the architecture, a breach is more difficult to mediate it has occurred. Dually, the response time to repair an exposure is also generally slower, because Microsoft is the company responsible for receiving the reports of a breach, confirming it, assembling an appropriate response team, devising a solution, and delivering that solution to its millions of customers. For Unix (Linux), there is a worldwide community constantly enhancing and updating the open source software, so the means of repair and delivery of newer and more secure software is much easier.

## XVII. Conclusive Remarks and Recommendations

Undoubtedly, cybersecurity finds itself at the helm of the world's most important industries. Touching areas of commerce, all three fields of business, academics, and social media, along with everyday life for citizens across the globe, cybersecurity has and will continue to grow in importance as mankind becomes more and more dependent on technology and digital communication. Interest in cybersecurity is increasing and individuals are looking to enhance their knowledge of the cyber arena should be keenly aware of a number of topics, especially under the lenses of business and academics.

In business, the importance of security cannot be overstressed. As exhibited, there is no ceiling for how destructive a cyberattack can be, crippling global giants like Target and Sony, and even striking global superpower governments such as the United States of America. Often times, these devastating attacks are a result of three things: lack of proper cyber and security training for all employees, not enough resources (normally fiscal and department size) allocated to cyber defense, and poorly designed security architectures.

Though not all employees are cyber analysts or cyber warfare specialists, it is important to ensure that all employees are aware of the dangers that exist in the cyber world and the constant threat, especially when dealing with classified or fiscal information. Properly training employees to identify and report social engineering attempts and not to succumb to them immediately spoils the plans of many black hats. Further, it is of vital importance that organizations in business also apportion proper resources to their IT and security teams to help mitigate and respond to penetrations. By checking for software updates, monitoring network traffic, identifying potential attacks, and maintaining a secure system, companies are much less likely to be a victim of a cybercrime. Lastly, organizations must remain cognizant of their systems architecture. By properly assigning responsibilities and granting users access only on a need-by-need basis, the companies are securing themselves by limiting any damage that can be done. This task should be performed jointly by the IT and the data owners.

Academia, too, should continue to emphasize cybersecurity in the education field, and with a heightened degree. Cybersecurity curricula, though new, should adapt to the rising importance of the industry. By looking at the success of top-tier programs, new curricula should emulate the nation's top cybersecurity programs, as determined by CAE accreditations. These curricula should include courses in network, operating system and application security along with ethics. The courses should include with a lab-based component that allows students to marry the theoretical concepts with real-world applications. To augment this learning, cybersecurity educational programs should also seek partnerships with workplace institutions including governmental agencies, private contractors, or even other companies who wish to sponsor lab-based learning examples such as those at Carnegie Mellon University and UMBC. These joint-ventures will provide cybersecurity students with a rich canvas to practice their newly taught skills.

Cybersecurity is the art of securing money, people, information, and history. Without cybersecurity, it is possible that mankind could lose all of its stored data, which is growing at a rate that will reach more than 503,059,775,290 terabytes of data per day before the end of 2020 (Marr). Cybersecurity should continue to receive recognition as being one of the most important fields, and be treated with appropriate discipline as more people flock to become experts in the area.

# Works Cited

"10 Most Destructive Computer Worms and Viruses Ever." *WildAmmo*. WildAmmo, 12 Oct. 2010. Web. 07 Nov. 2016.

Abelson, Harold, Ken Ledeen, and Harry R. Lewis. *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion*. Upper Saddle River, NJ: Addison-Wesley, 2008. Print.

"Anonymous Hacks Pro-ISIS Twitter Accounts, Fills Them with Gay Pride." *CBSNews*. CBS Interactive, 15 Jan. 2016. Web. 23 Nov. 2016.

Bort, Julie. "How The Hackers Broke Into Sony And Why It Could Happen To Any Company." Business Insider. Business Insider, Inc, 19 Dec. 2014. Web. 06 Nov. 2016.

"Common Vulnerabilities and Exposures." Center for Vulnerabilities and Exposures. The Department of Homeland Security, 20 Jan. 2011. Web. 15 Oct. 2016.

"Computer Science." *Computer Science 2016-17 Catalog*. Drexel University, n.d. Web. 25 Nov. 2016.

"CyberAcademy_overview." *http://www.northropgrumman.com/*. Northrop Grumman Corporation, 2013. Web. 19 Sept. 2016. Approved for Public Release: 13-0623 IS7840113

"Cybersecurity Overview." *Homeland Security | Cybersecurity Overview*. The Department of Homeland Security, 27 Sept. 2016. Web. 06 Oct. 2016.

Davidson, Jacob. "Here's How Many Internet Users There Are." *Time*. Time, 26 Mar. 2015. Web. 6 Nov. 2016.

Dark, Melissa, and Jelena Mirkovic. "Evaluation Theory and Practice Applied to Cybersecurity Education." IEEE Security & Privacy 13.2 (2015): 75-80. Web.

Burley, Diana, Matt Bishop, Elizabeth Hawthorne, Siddharth Kaza, Scott Buck, and Lynn Futcher. "Special Session." ACM Joint Task Force on Cyber Education (2016): 234-36. ACM Digital Library. Web. 26 Nov. 2016.

Goodchild, Joan. "10 Hacks That Made Headlines." *CSO Online*. CSO, 14 May 2012. Web. 20 Sept. 2016.

Greenberg, Andy. "An Interview With the Hacker Probably Selling Your Password Right Now." *Wired.com*. Conde Nast Digital, 06 June 2016. Web. 07 Nov. 2016.

Gupta, Upasana. "Latest List of NSA-Approved CAE Schools." BankInfo - Security. BankInfo, 4 Dec. 2009. Web. 26 Nov. 2016.

Hanson, Hilary. "Leaked Emails Suggest DNC Was Conspiring Against Bernie Sanders." *The Huffington Post*. The Huffington Post, 23 July 2016. Web. 23 Nov. 2016.

Hernandez, Sergio. "All the Cyberattacks on the U.S. Government (that We Know Of)." *Mashable*. Mashable Articles, 18 Aug. 2015. Web. 10 Nov. 2016.

Henry, Kevin M. *Penetration Testing: Protecting Networks and Systems*. N.p.: IT Governance, 2012. Print.

Hillis, W. Daniel. *The Pattern on the Stone: The Simple Ideas That Make Computers Work*. New York: Basic, 1999. Print.

Hughes, Matthew. "What You Need To Know About the Massive LinkedIn Accounts Leak." *MUO Security, Social Media*. MakeUseOf, 20 May 2016. Web. 07 Nov. 2016.

"Kali Linux Documentation." *Kali Linux*. Offensive Security, 15 Oct. 2016. Web. 15 Oct. 2016.

Koerner, Brendan I. "Inside the Cyberattack That Shocked the US Government." *Wired.com*. Conde Nast Digital, 23 Oct. 2016. Web. 10 Nov. 2016.

Klein, Adam G. "How Anonymous Hacked Donald Trump." *New Republic*. The Conversation, 31 Mar. 2016. Web. 23 Nov. 2016.

Lee, Riordan. "Anonymous Hacks ISIS's Twitter, Makes It as Fabulously Gay as Humanly Possible - Techly." *Techly*. TechlyNews, 21 July 2016. Web. 23 Nov. 2016.

Lichtblau, Eric, and Eric Schmitt. "Hack of Democrats' Accounts Was Wider Than Believed, Officials Say." *The New York Times*. The New York Times, 11 Aug. 2016. Web. 23 Nov. 2016.

Leswing, Kif. "Yahoo Confirms Major Breach - and It Could Be the Largest Hack of All Time." *Business Insider*. Business Insider, Inc, 22 Sept. 2016. Web. 06 Nov. 2016.

"Major in Computer Science." *Major in Computer Science*. Towson University, n.d. Web. 25 Nov. 2016.

Marr, Bernard. "Big Data: 20 Mind-Boggling Facts Everyone Must Read." Forbes. Forbes Magazine, 30 Sept. 2015. Web. 27 Nov. 2016.

McCandless, David, Tom Evans, Miriam Quick, Ella Hollowood, Christian Miles, and Dan Hampson. "World's Biggest Data Breaches & Hacks — Information Is Beautiful." *Information Is Beautiful Visualizations*. Information Is Beautiful, 24 Sept. 2016. Web. 06 Oct. 2016.

Mcduffie, Ernest L., and Victor P. Piotrowski. "The Future of Cybersecurity Education." IEEE Xplore 47.8 (2014): 67-69. IEEE Xplore Digital Library. Web. 26 Nov. 2016.

McHale, John. "Record Number of Cyber Attacks Hit Lockheed Martin in 2014." *Military Embedded Systems*. Avionics Design, 18 Feb. 2015. Web. 23 Nov. 2016.

Messmer, Ellen. "Northrop Grumman Constantly under Attack by Cyber-gangs." *Network World*. Network World, 21 June 2011. Web. 23 Nov. 2016.

"National Centers of Academic Excellence (CAE)." *National Centers of Academic Excellence (CAE) | NICCS*. Department of Homeland Security, 14 Nov. 2016. Web. 25 Nov. 2016.

"NewEraCracker/LOIC." *GitHub*. Open Source Community, 16 May 2016. Web. 06 Oct. 2016. The Low-Orbit Ion Cannon (LOIC) was a tool designed to provide easy access to very heavy and thorough cyber (specifically DDoS) attacks.

Newman, Lily Hay. "Security News This Week: The DNC Hack Was Worse Than We Thought." *Wired.com*. Conde Nast Digital, 13 Aug. 2016. Web. 10 Nov. 2016.

Norton, Quinn. "Anonymous 101 Part Deux: Morals Triumph Over Lulz." *Wired.com*. Wired Security, 12 Dec. 2011. Web. 15 Oct. 2016.

Peters, Sara. "The 7 Best Social Engineering Attacks Ever." *Dark Reading*. InformationWeek, 17 Mar. 2015. Web. 15 Oct. 2016.

Philipp, Joshua. "ISIS Wants to Enable Serial Killers by Hacking Surveillance Cameras." *The Epoch Times*. The Epoch Times, 03 Nov. 2016. Web. 23 Nov. 2016.

Piazza, Matt, and Aspen Olmsted. "Founding a Cybersecurity Club in a Higher Education Environment: A Case Study - IEEE Xplore Document." IEEE Xplore Digital Library. IEEE, 18 Feb. 2016. Web. 26 Nov. 2016.

Publications on Computer Security and Cryptography (as related to Cyber). 20 Sept. 2016. Raw Data. Google Scholar, N.p. These are raw numbers produced by a Google Scholar metric about the number of top visited publications pertaining to Computer / Cyber security.

Rapid7 Penetration Testing. "Penetration Testing Software, Top Rated | Rapid7." *Rapid7.com/products/metasploit*. Rapid7, 1 Sept. 2016. Web. 15 Oct. 2016.

Redhat. "What Is Open Source?" *Opensource.com*. Red Hat Inc, 12 Sept. 2016. Web. 15 Oct. 2016.

Rouse, Margaret, and Brian Kirsch. "What Is Virtual Machine (VM)? - Definition from WhatIs.com." *SearchServerVirtualization*. Tech Target, 1 July 2016. Web. 15 Oct. 2016.

Schmidt, Eric, and Jared Cohen. *The New Digital Age: Reshaping the Future of People, Nations, and Business*. New York: Alfred A. Knopf, 2013. Print.

Schneier, Bruce. Beyond Fear: Thinking Sensibly about Security in an Uncertain World. New York: Copernicus, 2003. Print.

Schneier, Bruce. "Lessons from the Sony Hack." Web log post. *Schneier.com*. Schneier on Security, 21 Dec. 2014. Web. 07 Nov. 2016.

"Security and Privacy." *Carnegie Mellon Computer Science Department Catalog*. Carnegie Mellon University, n.d. Web. 25 Nov. 2016.

"Search Distributions." *Distrowatch.com/Linux*. DistroWatch, 16 Oct. 2016. Web. 16 Oct. 2016.

Silver-Greenberg, Jessica, Matthew Goldstein, and Nicole Perlroth. "JPMorgan Chase Hacking Affects 76 Million Households." *The New York Times*. The New York Times, 02 Oct. 2014. Web. 23 Nov. 2016.

Thurrott, Paul. "Apple's Active Installed Base Is Now Over 1 Billion Strong - Thurrott.com." *Thurrot Mobile*. Thurrott, 27 Jan. 2016. Web. 15 Oct. 2016.

"Trojan Horse." Encyclopedia Britannica Online. Encyclopedia Britannica, 27 Apr. 2015. Web. 15 Oct. 2016.

"UMBC Center for Information Security and Assurance." *Center for Information Security and Assurance*. University of Maryland Baltimore County, n.d. Web. 25 Nov. 2016.

Vespa, Matt. "NSA: The DNC Email Hacks Didn't Cost Clinton The Election." *Townhall*. Politico, 21 Nov. 2016. Web. 23 Nov. 2016.

W3. "Usage Statistics and Market Share of Apache for Websites." *Web Technology Surveys*. W3Techs, 15 Oct. 2016. Web. 15 Oct. 2016.

Wood, Tyler Cohen. "The LinkedIn Hack: Understanding Why It Was So Easy to Crack the Passwords." Weblog post. *Inspiredlearning.com*. InspiredLearning, 21 May 2016. Web. 07 Nov. 2016.