# Hacking as part of the new job market

Hacking: A Way to the Job Market

*Hacking* has essentially been around for more than a century. Before the internet, hackers were tampering with census machines and radio signals. The steady uprising of hacks and the problems that they can cause has led to an influx of cyber security jobs over the past decade. Companies are needing the brightest minds in security to keep information safe guarded from the likes of hackers, and sometimes that even means offering hackers themselves jobs to protect the system they were able to penetrate. In today's world many cyber security jobs have gone unfilled, mostly in part due to the high demand of cyber security professionals needed in the work force, but also due to the high rate at which attacks happen.

In order for cyber security professionals to stop attacks, they must also understand the intricate details of how these attacks actually work, and what are the most common forms of defense against them. There are multiple different ways for hackers to access a system, or attack it, but a few of the most common ones are *Phishing* which " implies the replication of the website with the aim of stealing money or personal information. And once a user enters his credit card details, for example,  a hacker will have access to that data and will be able to use the received information for his own benefit" [1]. Distributed Denial of Service (DDOS) is an attack that is able to compile multiple systems across the internet to form botnets of networks. These systems are remotely controlled either by the attacker themselves or by self-controlled *Trojans* that are able to flood a network with fake traffic in order to slow down a system or even make it crash and shut down completely. Hackers may also use *SQL Injection* where " hackers can get

access to your confidential information by deceiving the system. So, there is no surprise that SQL injections can also be a simple tool. But this simple tool can allow a hacker to access vital information of your website”[1]. Similarly, *Keylogger Injection* uses malware to record users’ key strokes it is able to “ capture all of the user’s actions on the keyboard, and to send all that has been recorded to the hacker ; it also installs a malicious script that produces an in-browser cryptocurrency miner”[1]. With so many various ways hackers can attack a system, companies have resorted to hiring *Ethical Hackers* or also known as *White Hat Hackers* to try and penetrate their system looking for vulnerabilities, and ways to improve security.

What is a White Hat and what other kinds of hackers exist? A White Hat hacker is “ a computer network security professional and has non-malicious intent whenever he breaks into security systems. A White Hat hacker has deep knowledge in Computer Networking, Network Protocols and System Administration (at least three or four Operating Systems and very good skills in Scripting and Programming). White Hat hacker has also good knowledge in hacking tools and know how to program hacking tools”[2]. A White Hat has a multitude of skills to breach networks, however he does so with the permission of companies and organizations in order to find vulnerabilities and assist in repairing security issues. Ethical hacking is becoming a must need for corporations and organizations to keep their information safeguarded, and in doing so must enlist the help of hackers who actually have the intent of helping them. On the other side of the spectrum you run into *Black Hat* hackers or also known as *crackers.* Black Hats always have malicious intent when attacking targets. They possess profound knowledge

in Computer Networking, Network Protocols, and System Administration. These are hackers you commonly hear about on news networks and other media sources that have breached data networks and stolen credit card and personal information. In the middle lies the *Grey Hat* hacker “ Grey Hat normally do the hacking without the permissions from the administrators of the network he is hacking. But he will expose the network vulnerabilities to the network admins and offer a fix for the vulnerability for money”[2]. Grey Hats will at times sell information and vulnerabilities to government or law-enforcement agencies. While these acts may be questionable, they are also viewed as illegal. These three different kinds of hackers are viewed as the most common types.

Cyber attacks remain one of the worlds top threats every year. Cyber attacks are on the rise and have intensified in recent years. Attacks are increasing, both in frequency and unsettling potential. Business’s have reported that cyber breaches have almost doubled in five years [3], and with the *Internet of Things* devices reaching a higher number than the global population there are now more devices on earth than users. Symantec has reported that in 2017 there were more than one billion web requests to analyze threats, which are up 5% from 2016. 1 in 13 of these web requests lead to malware, pair this with a 600% increase on attacks to the Internet of things and a 13% increase in overall reported vulnerabilities and you can see that cyber security jobs are safe for many years to come [4].

By looking at some of the biggest data breach cases in recent years you can see just why users are requesting more security when it comes to their information being safe guarded.

1. In 2014 Yahoo announced that attacks were able to compromise the real names, email addresses, dates of birth and telephone numbers of over 500 million users, but the majority of passwords involved were not compromised to due to their hacking algorithm.” A couple of months later, in December, it buried that earlier record with the disclosure that a breach in 2013, by a different group of hackers had compromised 1 billion accounts. Besides names, dates of birth, email addresses and passwords that were not as well protected as those involved in 2014, security questions and answers were also compromised” [5]. These breaches were estimated to have knocked off more than $350 million dollars from Yahoo’s sale price. Yahoo has since been sold to Verizon, but still remains an internet giant with over $5 billion dollars in revenue each year and over 1 billion active users monthly.
2. eBay also came under attacks in 2014, where impacts lead to over 145 million user accounts being compromised. eBay reported that user names, addresses, dates of birth, and passwords of all of its users had been breached. Hackers were able to access the company network using the credentials of three employees and were able to access that information for nearly 230 days.” It asked its customers to change their passwords, but said financial information, such as credit card numbers, was stored separately and was not compromised. The company was criticized at the time for a lack of communication informing its users and poor implementation of the password-renewal process”[5].
3. More recently in 2017 Equifax had a major impact of Social Security Numbers, birth dates, addresses, and in some cases drivers’ license numbers breached. This affected over 143 million users, and in some

cases, consumers also had their credit card information stolen. Equifax is one of the big three credit bureaus in the United States. Criminals were able to use a website application to find vulnerability and gain access. The occurrence resulted for nearly two months before it was finally caught in July of 2017.

4. JP Morgan Chase, one of the nations largest banks were not immune to data breaches either in 2014. Over 76 million users and 7 million small businesses were also affected. The data breached was contact information such as names, addresses, phone number, and email addresses. JP Morgan Chase is estimated to spend over $250 million a year on security. Armerding states that " the hackers were reportedly able to gain " root" privileges on more than 90 of the bank's servers, which meant they could take actions including transferring funds and closing accounts" (Armerding, 2018).
5. The worst gaming community breach happened in 2011, where Sony's PlayStation Network was hacked. Over 77 million user accounts were hacked, and an estimated loss of over $171 million was reported while the service was down for over month. Hackers were able to gain access to full names, passwords, emails, addresses, purchase history, purchase history, and log-in information. Nextgov. com reported that the Homeland Security Department had to step in to mitigate damage caused by hackers. Much of the public was outraged when it took Sony more than week to announce the intrusion of their network. By then hackers had already used account information for illegal purchases. Author Aliya Sternstein a Senior correspondent for nextgov. com reported that " While gaming and music networks may not be

> considered “ critical infrastructure,” the data that perpetrators accessed could be used to infiltrate other systems that are critical to people’s financial security, according to some computer experts. Stolen passwords or profile information, especially codes that customers have used to register on other websites, can provide hackers with the tools needed to crack into corporate servers or open bank accounts”(Sternstein, 2011).

With cases such as data breaches and other attacks why does it seem as if security is always a step behind? Companies and organizations remain trying to fill the void of cyber security specialists. The recent influx in crime has sent cyber security jobs through the roof with requested positions, however there just not enough bodies to fill the positions.

Cybersecurityventures. com has predicted that there will be 3. 5 million job openings in the cybersecurity field by the year 2021. Cyber threats continue to create a seemingly unrealistic number for individuals with skills and talent in cybersecurity to try to keep up.

## Works Cited

[1] “ 8 Most Common Website Hacking Techniques You Should Know.” Cobweb Security – WebDefender Website Security, cobweb-security. com/security_lessons/8-common-website-hacking-techniques-know/.”

[2] “ Types of Hackers.” Asymmetric Encryption Algorithms, Diffie-Hellman, RSA, ECC, ElGamal, DSA, www. omnisecu. com/ccna-security/types-of-hackers. php.

[3] Accenture. 2017. *Cost of Cyber Crime Study* . https://www. accenture. com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy. pdf

[4] Symantec. 2018 *. Internet Security Threat Report* , volume 23. March 2018https://www. symantec. com/content/dam/symantec/docs/reports/istr-23-2018-en. pdf

[5] Armerding, Taylor. “ The 17 Biggest Data Breaches of the 21st Century.” CSO Online, CSO, 26 Jan. 2018, www. csoonline. com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century. html.

Sternstein, Aliya. “ DHS Probing Sony PlayStation Network Attack.” Nextgov. com, Nextgov, 22 Dec. 2016, www. nextgov. com/cybersecurity/2011/04/dhs-probing-sony-playstation-network-attack/48982/.