Cyber Ethics and the Efficacy of Ethical Hacking

Abdullah Al Rifat

Department of Computer Science and Engineering, East West University

Apr. 16, 2021

Abstract

Cyber ethics is the application of ethical principles for the online environment. In general, it is quite difficult to define something as ethically right or ethically wrong as it varies from place to place. A code of conduct for using the Internet is known as cyber ethics. Generally acceptable behavior on the internet is very similar to acceptable behavior in real life, which is a simple way to learn about cyber ethics. It also assesses the social rules, policies and laws enacted for the arising issues from the growth and application of technology related to the cyber world. Nowadays "Hacker" is a quite popular term but as of today the first known event of hacking took place at Massachusetts Institute of Technology (MIT). And from there the term "Hacker" originated. The hacker is nothing but a computer specialist, whose main goal is to use his expertise to overcome any obstacles, finding loopholes of the existing system and ensure maximum security for both the clients and users without doing any damage.

Keywords: Ethical Hacking, Cyber Attacks, Hacker, Banking, Social Media

Introduction

In the era of modern science, hacking is a quite common phenomenon but still, there are many misconceptions about it. In the beginning, hacking was not promoted as an immoral thing. On the other hand, hackers were quite encouraged to do their work. They used to operate closely with many governments, private corporations, and many more. Often, they were assigned as security specialists. Their task was to provide support for existing systems and implement security credentials in entry points, and overall ensure a safe environment for both the clients and users. It was even a highly paid and demanding job in many first-world countries.

However, many hackers went rogue and got driven by evil deeds and personal gains. In the 1990s, there was an increase in cybercrimes by malicious hackers and followed by a lot of high-profile arrests. Instead of finding loopholes in the system and informing the administration, they started gaining access in an unethical way and took control of many major systems. In many cases, they demanded money and threatened the users. Due to the bad deed of a few, now the term "Hacker and Hacking" is in a place of displeasure. People are in a dilemma to tag someone as a good hacker or someone as a bad hacker. First of all, there are a lot of notable incidents relating to hacking that may influence people's perceptions towards both the hacker and hacking. Bangladesh Bank Incident, Recent Facebook Users' Data Hack, Celebrity Social Media Platforms Hack, Phishing Attack and Ransom, Denial-of-service (DDoS) Attack, Edward Snowden Case, Russian Hacking, Pirated Music and Books, Whistleblowing, Hacking and Election Interference and many more incidents like these made their marks in public.

The purpose of this research is to provide a clear insight into different types of hacking terminologies with proper reasoning and example from the recent headline-worthy incidents and how can we prevent the damage by utilizing ethical hacking without creating any conflict with cyber ethics.

Banking

Bangladesh is a country in South Asia. Like every other country, Bangladesh has its central bank. In February 2016, there was a massive cyber heist relating to Bangladesh Bank. There were thirty-five fake instructions sent by the hackers through the SWIFT network to transfer approximately one billion dollars from the Federal Reserve Bank of New York. Bangladesh Bank kept the money as a reserve in the Federal Reserve Bank of New York. Out of those thirty-five fake instructions, only five succeeded which resulted in transferring hundred and one million dollars. Eighty-one million dollars was traced back to the Philippines and twenty million dollars was traced back to Sri Lanka. Later on, twenty million dollars were recovered from Sri Lanka. Till 2018 only eighteen million dollars were recovered from the Philippines. Most of the money in the Philippines went to four personal accounts [1].

The hackers injected malicious codes into Bangladesh Bank's server and then initiated the attack. In the Bangladesh Bank heist, there was a similarity with two quite common vulnerabilities; Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) were found. Open Web Application Security Project (OWASP) is a nonprofit foundation that always works on improving software security [2]. From time to time they rank the topmost security threats and publish standards so that the companies, organizations, and developers can ensure the utmost safety of their web applications.

Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) both secured their place in the "Top 10 Web Application Security Risks" of Open Web Application Security Project (OWASP). However, security specialists and developers were always concerned about these security risks. They were also very vocal on creating awareness but the Bangladesh government didn't fully acknowledge these risks and never took actions accordingly till this severe mess took place [3].

Social Media

If we list the top most popular and visited social media platforms, Facebook will be there. People share a lot of personal information and their day-to-day lifestyle on Facebook. Whenever there is an incident relating to the data hack, people lose their trust in these platforms. Recently, there's news that became the headline in several international newspapers. 533 million Facebook users' data such as name, phone numbers, and emails were posted in a hacking forum. After this incident, the government, security forces, and mass people all were waiting for an official response from Facebook.

In their defense, Facebook said the data wasn't obtained by getting illegal access into their system. It happened before September 2019 by web scraping which is a very common method of collecting public information from the internet. The Product-management director of Facebook, Mike Clark wrote in his blog post that there was a vulnerability in the Facebook contact importer tool. This tool allowed users to find other Facebook profiles on the platform by using phone numbers. However, Facebook said in August 2019, they fixed that vulnerability [4].

Many experts and mass people are still not convinced by this explanation. Many people got random phone calls, emails, online advertisements, and much more trouble as their personal information was compromised. In the future, hackers may trace back these people's actual identities by unethically using those leaked data.

The security breaches in these social media platforms are not a new thing. In the past, there were many well-known incidents relating to this. Many celebrities, corporate giants and influential people were always a victim of these type of uncomfortable situations. Hackers took control of their profiles and pages to boost the propaganda campaigns. The followers of these pages fell for the trap and many lost their money by thinking that they are giving it for a greater cause but the reality is often disappointing. Many political and non-political organizations are also exploiting social media platforms to gain benefits from it in an unethical way. Paid reviews and creating a new trend by boosting the algorithms are a core part of the fashion industry now.

Cyber Attacks

There are many common forms of cyber attacks such as phishing attacks, ransomware, malware, denial-of-service (DoS), distributed denial-of-service (DDoS) attacks that can sabotage our regular online activities.

The purpose of denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is to disrupt the regular user flow of a website or a service or network by creating artificial traffic [6]. The main difference between DoS and DDoS is in the denial-of-service attack a computer is used to flood a server with TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). On the other hand, in a denial-of-service (DDoS) attack multiple systems from different sources are utilized to attack a single system [5].

In terms of DDoS attacks, it's quite impossible to identify the source and block it from the system which makes it tougher for the system security experts to provide us with an effective solution. According to Cisco Systems, Inc. which is an American multinational technology company, in total, the number of worldwide DDoS attacks will be 15.4 million by 2023 [7]. On the other hand, malware and ransomware are too common. Email is a highly popular way of communication now. Official work to legal dealing everything is somewhat dependent on the email communication. But it's a matter of grave danger that according to CSO, another technology company that works on security measures and risk measurements, 94% of malware is sent by email [8].

Phishing is a very common tactic online by impersonating any reputable source and try to gain sensitive information from users. Stealing credit card information, gaining access to social media accounts or any login credentials are very common practices in phishing. If we talk about phishing, according to Symantec, 1 in 13 web requests lead to malware [9]. According to CSO Online, $17,700 is lost every minute due to a phishing attack [8].

Ethical Hacking

It’s not logical to assume that all the hackers are immoral. Unfortunately, the term "Hacker" is commonly used to send a bad signal towards the mass people. But the reality is quite diverse. We can generally categorize the hackers into three categories, "Black Hat Hackers", "White Hat Hackers" and "Grey Hat Hackers". This categorization is inspired by the Western film genre where the bad fellow wears a black hat and the good fellow wears a white hat.

Black Hat Hackers are highly driven by personal and financial gains by violating rules and regulations. On the other hand, White Hat Hackers are competent in doing the same that a Black Hat Hacker would do but they use their expertise on doing righteous works. Many corporations hire them to check for vulnerabilities and loopholes in the system. This type of hacking is perceived as Ethical Hacking. Grey Hat Hackers will also check for vulnerabilities of the system but without having the proper authorizations. However, we are not sure whether their intentions are malicious or not. So these types of hacking by Grey Hat Hackers are illegal same as the Black Hat Hackers.

There are numerous advantages of Ethical Hacking. A concise list is given below:

- Create a safe and secured system that is protected from malicious threats
- Be aware of the potential security breaches and take precautions
- Recover important sensitive information which is already lost
- Ensure safety to customer’s data i.e. credit information, transaction details, login credentials, etc
- Arrange community awareness and educational programs

Concluding Remarks

Hacking includes stealing confidential information, passwords, and login credentials to gain access to a server or a website without any prior permission. As technology revolutionized our world, it is a must that unethical hackers face criminal charges. They can create viruses that can bring critical websites or computer systems down. As a result, we must create awareness of the importance of ethical hacking. Ethical hacking is quite expensive but still, the effectiveness of ethical hacking is immense. If these high-profile corporate companies were concerned about the security of their users, then they would take strong measures in the very first place. Governments should step in to ensure public safety and security in online platforms without meddling with the freedom of expression. Nowadays, many governments are employing ethical hackers but still, there are many security concerns. What if the government uses their specialist to spy on the mass people or their political opponents to downplay? What if these ethical hackers write malicious codes to create massive security breaches during the period of working with the government closely as they are exposed to a lot of confidential information?

Technology has changed how we interact with people, how we purchase the new thing online, how we watch TV or read books, how we order food online, how we share the ride, how we transfer money online, how we are getting into the ecosystem of Internet-of-Things (IoT) and many more. This is because, in today's fast-paced world, life would be trivial without technology. Nowadays, most things are getting online. People are spending more time on these social media platforms than actually living a social life. Cyberlife is not even fully secured from vulnerability but still with the help of ethical hacking we can minimize the security breaches and make the internet much safer. However, it is still a substantial question to ask that if we are heading in the right direction of the future or not.

References

[1] *Bangladesh bank robbery*. (2016, March 11). Wikipedia, the free encyclopedia. Retrieved April 15, 2021, from https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery

[2] ***OWASP top ten***. (2021). https://owasp.org/www-project-top-ten/

[3] T. Farah, M. Shojol, M. Hassan and D. Alam, "Assessment of vulnerabilities of web applications of Bangladesh: A case study of XSS & CSRF," 2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP), Konya, Turkey, 2016, pp. 74-78, doi: 10.1109/DICTAP.2016.7544004.

[4] Hamilton, I. A. (2021, April 7). ***Facebook says the leak of 533 million users' data online wasn't a hack — but its explanation of what happened doesn't quite add up***. Business Insider. https://www.businessinsider.com/facebook-data-breach-2021-user-data-not-hack-company-says-2021-4

[5] ***Denial-of-service attack***. (2002, February 25). Wikipedia, the free encyclopedia. Retrieved April 15, 2021, from https://en.wikipedia.org/wiki/Denial-of-service_attack

[6] Cloudflare - The Web Performance & Security Company | Cloudflare. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

[7] ***Cisco annual internet report (2018–2023) white paper***. (n.d.). Cisco. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[8] Fruhlinger, J. (n.d.). ***Top cybersecurity facts, figures and statistics for 2020***. CSO Online. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

[9] http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_