EasyChair Preprint

№ 3954

Ethical Hacking: An Arsenal against Black Hat Hacking

Shariq Shoaib, Maeeda Khalid, Talha Amjad and Hassan Shahid

July 27, 2020

Ethical Hacking: An arsenal against Black Hat Hacking

Shariq Shoaib[1], Dept. of Software Engineering, UOG Sialkot Campus, 1724198-082@uogsialkot.edu.pk

Maeeda Khalid[2], Dept. of Software Engineering, UOG Sialkot Campus, maeeda.khalid@uskt.edu.pk

Talha Amjad[3], Dept. of Software Engineering, UOG Sialkot Campus, 17241598-224@uogsialkot.edu.pk

Hassan Shahid[4], Dept. of Software Engineering, UOG Sialkot Campus, 17241598-172@uogsialkot.edu.pk

---

Abstract: Cyber security is becoming a big concern with the development of technology. Black Hat Hackers are increasing rapidly. Ethical Hacking is considered one of the best approaches, but the challenge which is concerned with ethical hacking is to make sure it is done ethically. If we properly monitor and implement code of ethics to these students; with the expertise of Black Hat Hackers. They can help us securing our cyber world. Many bigger organization are making cyber teams and investing a lot of amount for their security. Most of the business owners are getting aware about the risk associated with cyber world. Current crises of COVID- 19 shows our dependability on cyber world. Black Hat Hackers are growing in numbers and brutality. If we failed to secure our cyber world within time, it may collapse due to its insecurities. With or without ethical hackers we are at the stake of risk, but they can be very effective against Black Hat Hackers.

Keywords- Ethical hacking, Black hat hacking, effective approach, Penetration testing.

I. Introduction:

Hackers were known to be skilled individuals who had good practices with the computer languages of that time. They were referred to as “Nerds” and “Geeks” because they would spend most of their time programming non-stop to combat their curiosity. With the development of technology, these hackers started using their expertise for illegal activities for the sake of fun, eventually starting to exploit sensitive information which was stored even on the most protected systems of that time; NASA and CIA. Hackers who use their expertise for illegal purposes are known as “Black Hat Hackers”. The purpose of this research is to review prior researches to understand why we still cannot get the best outcomes of Ethical Hacking? Further we discussed challenges associated with Ethical Hacking, and to demonstrate how Ethical Hackers can be effective against Black Hat Hacker, in short making technology more secure.

“Ethical hacking” is basically a terminology which was first introduced by IBM president John Patrick in 1995[], which is used for the hackers who tries to compromise a system using tools and techniques like Black Hat Hackers whilst abiding by the laws and ethics of hacking. These hackers are also known as Red Teaming or White Hat Hackers. The term “Grey Hat Hacker” refers to those hacker performing hacking illegally but for legal purpose. What makes them different from Black Hat Hackers are their intentions for compromising a system. Ethical Hackers would not compromise the system for their personal gains; they would work on the vulnerabilities of the system and fix them so that they cannot be exploited by the Black Hat Hackers. Different security measures are taken to make the security better. The pace we are improving our security is not enough, the number of Black Hat Hackers are growing coming up with new and better approaches to penetrate security. As the history tells these Black Hat hackers caused a lot of damages to different organizations with the misuse of technology and still they are growing theat. To combat them we need a better and effective strategy.

In the current era of computer, with the development of the computer, its security is a major concern. If we are not able to secure our cyber world due to its insecurities no one would even feel safe to get the best out of it. As we know these hackers were mostly teenager who got exposure to computer in early times. They were just curious about the possibilities of computer. Exploring these possibilities these hackers discovered many security flaws which they can use to penetrate different security measures of a system. In simple words we can say that they are expert analytical individuals who can stress the security of a system to find its flaw. With the passage of time when cyber world got a lot of attentions and become the major source of communication these Black Hat Hackers found it as an opportunity to misuse these flaws for their personal gains illegally. Due to the emerging threat of Black Hat Hacker a dire need of something Ethical Hacking was felt. These Ethical Hackers who possess the skills of hackers but they would use it for ethical purpose. They are doing bad guys job for good purpose. What makes them ethical, is they would not misuse these security flaws, instead they will report it to the organization or help them fixing it for preventing Black Hat Hackers to misuse it. It is noticeable that same type of security flaws are discovered again and again in different organizations. The bigger organizations are handling these security flaws and working on their security to be more secure. On the other hands small and medium businesses fails to cover these common flaws, which makes them an easy target of the Black Hat Hackers. These businesses are major component of cyber world. To make our cyber world secure it is really important to secure these businesses. If we start teaching students Ethical Hacking with the skills of attackers; Black Hat Hackers. They can work side by side with the software developers to come up with better security measures. The demand of cyber security professionals who can face the current and future persistent challenges of Black Hat Hackers is still high, due to which they are paid a lot of money, which might not be affordable by these small and medium businesses. Ethical Hacker are helping different organization to cover their vulnerabilities. If we can teach students ethical hacking with the implementation of code of ethics they can effectively help us making our cyber world secure. Teaching students ethical hacking would grab attention of Grey Hat Hackers for learning and utilizing their skills for legal purposes instead of them becoming future Black Hat Hackers.

II. Literature Review:

In this article [1] Discusses about the emerging need of ethical hackers, after the mid-1960s, when military started using the terms like “Red Teams” or “Penetration Testers”. The need for Ethical hackers initiated a long back. The challenges faced for training these professionals require proper approaches to make sure they do their work ethically. The Information System Security Certification Consortium (ISC) organization proposed their first Certified Information System Security Professional (CISSP) exam, which was first launched in 1997. CISSPs took an oath to follow the code of ethics. After that, the Certified Ethical Hacker (CEH) emerged; the first organization who offered training for this certification was Intense School, established in 1997. Some of the hackers had contradictions, Marc Maiffret, a hacker who co-founded eEye Digital Security in 1998, stated: “Typically hackers are people who didn’t finish college because they were so into finishing [their hacking] project. I didn’t finish high school and there are people here who have PhDs in computer science who learned hacking on the side” [1]. These Certification courses taught about Microsoft hacking tools and buffer overflows but not the real world problems; which are not sufficient enough to make a person a hacker and give strong grasp on the security. Hackers quickly recommended to be more practical instead of being certified. Certification became a means for the job seekers to fulfil their demand from the market, but it was not fulfilling the criteria for what was required from them.

In another article articulated by [2] he supports his claim to clearly have ethical hacking removed from

criminal activities as by law; it is legal. He further explained the whole concept of hacking and defined it as getting a unique way of solving a problem that will benefit the functionality and effectiveness of the software. He stated that these are the people who understand the background working of a software and understand how it works so that they can improve it and make it better. He further said that almost all the technological advancements are due to these hackers who work under the hat of ethics. Hackers who implement hacking for their own personal motives and use their skills with the intent to harm others are to be considered illegal. He explained the different classifications of hackers, and supported ethical hacking as better for the future. He also stated that we need to focus on this concept. He backed his argument by giving us the proper definition of cyber-attacks and threats as by the definition of USA department of justice, it is the violation of criminal law that involves knowledge of computer technology for their preparation, investigation or persecution. As conclusion, ethical hacking is not illegal; it should be given the proper attention and we should contribute as it is required for better technological advancements.

The emphasis of [3] is to answer the question "Should we teach hacking for ethical purposes; is it a right thing to do or not?" In this article, the full spectrum of hacking is examined to answer this question. Many universities and colleges recognized this gap and are offering cyber security programs to educate students to have expertise like Black Hat hackers in order to mitigate the adverse security concerns. Grey Hat hackers are hackers doing illegal activities but for legal purposes. One of the practical approaches we can adopt is by educating these grey hat hackers with the abilities like black hat hackers. These professional cyber security experts are referred to as "Ethical Hackers". Having a poor software quality can leave software with a lot of security loops; these loops can be used to breach the system. Software quality professionals identified the gap for the security of software; therefore, security should be considered in the design and development phase of the software. These ethical hackers can help identifying and fixing different security loops during the development and design phases. Therefore, we need to devise proper code of ethics to make sure Ethical Hackers use their expertise for Ethical purposes.

In the article [4] the author tried to explain what ethical hackers do and how can you master the art of ethical hacking. First, you need to get all the required knowledge and tools that can help you do the penetration testing and apply those procedures on your own machine so you can understand every step as to master it. In short, being an ethical hacker is not just all about coding; it is more about step by step breaking down a concept and understanding its weakness and fixing it. The author has mentioned the different types of attacks that can be used for ethical hacking. Attacks or if one describes it more precisely by calling them "methods" may include: Web Application Penetration testing, Network penetration testing, Gaining access and post exploitation. For performing such methods/Attacks, one needs to have the specific knowledge about the basic tools that may include the basics of Linux, hands on kali Linux, Tor, Proxy Chains, N-map and SQL injections. Furthermore, he included where one can go to practice his/her skills as there are programs that help get a person's skills sharper.

According to [5] the need of cyber security professionals is increasing constantly, but we do not have much cyber security professionals to fulfil the required criteria. It is also suggested in his book's chapter to educate the students to develop expertise in the field of cyber security. They will be forefront to face these challenges which are emerging with the development of technology. We need to have proper ethics of cyber security which will guide the main focus of the content to be taught for better outcomes. As we know there are different illegal markets on the internet that can pay an individual millions of dollar for the expertise these cyber security professionals have, one of the challenge we face is that we need proper cyber ethics to combat this. Different case studies are provided in this chapter to come up with

better solutions which can be implemented to face the challenges concerning cyber security ethics. It also discusses and analyses the challenges faced for cyber security ethics. Some of the organizations are taking different steps to implement the cyber security ethics, but are making very slow progress while the weightage over them is heavy. IEEE and ACM have code of ethics for their engineers, but it is not properly verified as to how many are actually following these codes of ethics. Also, there is no proper role to implement them. Due to this confusion, different approaches are coming in sight to mitigate these problems which can lead to cyber wars like issues; some are also aiding the cyber security. Cyber security is a national security threat. Microsoft president Brad Smith presented the global rules in the form of "Digitalization Geneva Convention" for cyber-attacks at the RSA 2017 conference. However, the need to develop practical and better approaches to tackle these problems efficiently is still dire.

In [6] the authors have described and explained about the pros and cons of new technology in their article. "It has made our jobs and life easier, but it has also opened a never ending trail of cyber-attacks, and so we have to defend ourselves by teaching the concepts of ethical hacking to our students as it can be used as an offensive approach, and at the same time, can be used as a defensive approach against these cyber-attacks" [6]. The authors briefly explained the concept of ethical hacking along with the terminology of computer crime that has been fired up by the internet. The authors also laid stress on the points of why we need to spread the education related to ethical hacking as, (Pashel,2006) purposes that the ability to determine the weakness in a computer system can assist the future security professionals in preventing attacks and getting better at what they do. Other than that, a valid point may be that the computer operators should have the same knowledge as the attackers do. However, the institutes that are offering such knowledge are limited in their own way - they don't offer hands on approach as they the students might go far in discovering the unethical ways with such knowledge. The observation is based on surveys, which showed most of the students under their sheer curiosity attempted to try hack unethically, but many accepted that their intentions were not wrong. The best methodologies for the ethical hacking include hands on approach; if the students are not taught hacking, they may not be ready to defend the real world attacks. So as per [6] conclusion, students should be equipped with the skill set of an attacker so they can stop intruders and prepare for the persistent challenges by these intruders of security in the future. It is also important to encourage them to work ethically and discourage them about the illegal activities. Soft skills may be effective to some extent for boarding this vision.

[7] In detail talks about the different ethical hacking and its importance for enhancing security. On the other side of coin teaching ethical hacking could also result, future threat or Black Hat Hackers. There are different types of ethical hackers which can leave good impact on the society, but if these ethical hackers would cross the region of ethics, they will fall in the category of illegal hackers. It is really important to teaching students how important it is to be ethically right when using their skills. On the other hand, a hacker can be ethically right, for example, Hacktivist and grey Hat hackers would be performing hacks for legal purpose but how they conducted their hack is not legal. No matter how much risk is associated ethical hackers, but their requirement and need is still growing. We need to enhance our security and keep it up to date and ethical hacker can play important role doing that.

The article named [8] first briefly explained what ethical hacking is and what ethical hackers do. As per the author, an ethical hacker is a person who gets hired by a client to find the security flaws that a black hat hacker can potentially use for his personal gains and so as per ethics it's his job to determine what are those security flaws and to fix them, but often times, the concept of law and ethics that are two different things are mixed, and as a result the law gets ignored. It's not the job of ethical hacker to

determine whether the client is working for a terrorist organization, his job is to find bugs and provide patch for them so they can't be exploited by the black hat hackers. The ethical hackers have to think on the grounds of black hat hackers to outsmart them in their own game, and use appropriate defence against their attacks, so for this reason, the number of times for which the lines get blurry and they abandon the ground of ethics, they may be not breaking the law but it will be wrong ethically. The author further described the steps ethical hackers may take to secure a system; the first step involves the planning and reconnaissance, which helps to understand the system. The second step is Scanning, here we scan the weaknesses in a system, and lastly is the step where we finally gain access. After it, we maintain access for as long as we can, and in the end, we prepare the analysis and apply patches and fixes.

In [9], the authors tried pointing towards the challenges faced due to the growing pace of technology development. The authors emphasised on the problems which are related to technologies. The cyber world is the internet world which is doing a very good job in connecting people worldwide, but some people are using their skills for committing different criminal activities like data theft, fraud, blackmailing, and exploiting system weaknesses for unattended or unauthorized access, etc. These people who are skilled with their expertise with growing pace of technology, using such skills to do illegal activities are called "Black hat hackers". Initially, there were little groups of black hat hackers, but now, these groups have grown drastically. Their goals are personal gains; for that they can leave an individual in miserable state. These illegal activities are a part of "cybercrime", which is committed through technology. Cybercrime is becoming a huge threat to the cyber world; these activities formulate an easy way for the criminals to earn good profit. India is one of the most impacted countries by the hand of cybercrime. 41 nations, including Europe, are making universal conventions against these cybercriminals so they can get identified and punished for their illegal activities. North Korea, USA and China are contributing a lot to cyber security. It is not the technology which needs to be improved because it is said that humans are easier to exploit by revealing their sensitive information. According to the analysis of 32 billion people worldwide, masses have compromised accounts and have weak passwords. Hackers can use a list of passwords to brute force such weak accounts. However, we can use the capabilities of humans and computers to find a good solution against these cyber activities. We need to keep our security up-to-date so that we are making it stronger every day; therefore, making it tough for the cybercriminals to penetrate through weak systems or have enough time to find loopholes.

[10] Is about the top 5 famous hackers of the history. It explains the expertise of the hackers which they used for the illegal purposes. It also described their current statuses. 2 of the biggest hackers of the history; Julian Assange and Albert Gonzalez, are still sentenced in prison, while the other top 3 hackers of the history are using their expertise for the betterment of security. Kevin Mitnick is running Mitnick Security Consulting, LLC. Kevin Poulsen used his expertise for law enforcement to catch the sex offenders on Myspace in 2006. Robert Tappan Morris who was the first person to violate the "Computer Fraud Act" with his "Morris" worm; virus, is now, a professor at the Institution of Massachusetts - Institute of Technology (MIT), and is also the founder of the Y Combinator.

In [11], the authors report different statistical analysis of cyber security is done, which are collected from different sources. "According to the Cyber Security mid-year snapshot'19 report", Cyber security budgets have increased by almost 60%" [11]. Due to these cyber security issues rising, people are getting aware about what are the risks and havoc condition of being hacked can cost, so they are investing more in the security and it will grow in future. "43% of breach victims were small and medium businesses" [11]. Bigger organizations are taking their security seriously, and they are investing more in their security measures, which helps to

create a strong defence system which is not easy to penetrate. Small and medium businesses are easy target for the attackers and they can use Water Holing like techniques to compromise the victors of such sites. After being compromising the victim, they can be used as a medium to spread attacker's malicious content for compromising sensitive information without being revealed to their owners. "68% business leaders feel that their security risk is rising" [11]. With the passage of time, the Black hat hackers are developing and enhancing their skills to use the advancement of technology for illegal purpose. "71% of breaches were financially motivated and 25% were motivated by espionage" [11]. The studies elaborate the main motive behind illegal hacking is personal gains; they will misuse this opportunity of the business expanding through technology. "The average time to identify a breach in 2019 was 7 months" [11]. We still need to find a better or make more effective approaches to detect the intrusion attacks - the process of identifying them is slow and during this time a hacker might be able to put their victims in miserable state.

III. Research Methodology:

This research is being conducted on the crucial need of ethical hacking in the future and what should be done to follow up with the pace created by Black hat hackers. The methodology adopted for this research is qualitative in nature, in which, we will be using secondary data in forms of articles available on the internet. This research is based on the content analysis of the prior research to identify the misconceptions around ethical hacking, and to identify its importance in the near future. We included different studies to demonstrate the awareness, importance and challenges of ethical hacking in the contemporary world. The methodology will help to conduct this research in a way which develops the understanding of the gap surrounding the importance of promoting and using ethical hacking efficiently.

IV. Findings:

The above study help us understanding about the importance and the challenges of ethical hackers. 68% business leaders understand the requirement of proper security [11]. Numbers of investments have increased for the security drastically, and it is predicted in the future it will increase more. Bigger scale businesses are investing for their security - bug bounty programs are finding solutions for different security flaws which helped them making their security stronger. Some of the Black Hat hackers after getting punished are contributing towards the society, finding it as an opportunity to ethically hack and improving security to get their personal gains. Most of the small and medium businesses are compromised and spreading malicious content unwittingly. USA is one of the countries advanced with developed technologies, yet it is the most effected by the damages caused by the Black Hat hackers. As we can see demand for these Ethical Hackers is still high, we do not have required security professionals, pace is really low, and many still feel limited with their ability according to them they may cause more harm so the knowledge they have should be limited. If we can teach students with the knowledge of the expertise of the Black hat hackers, it will lead to the prioritization of the code of ethics for these students with the hacking skill. Ethical hackers would be able to think out of the box like the Black Hat hackers to be proactive against the future persistent challenges by attackers.

V. Discussion:

Since everyone's usage and dependency on technology has massively increased more than ever through aspects like online classes, online financial transactions, online healthcare, online e-shopping, and online business meetings during the current ongoing Corona Virus, it is of vital significance that the online world is devoid of any cybercrimes and any other illegal activities taking place in order for everyone to feel safe and secure online during this unprecedented times which require operations to function online rather than in-person.

The demand of cyber security is increasing but with the pace black hat hackers are growing is alarming. Keeping the risk associated with ethical hacker in point of view students should be trained in such a way that they can catch up with the pace of Black hat hackers in the future. This field should be encouraged for ethically performing hacking or the risk of Grey Hat hacker being the future Black Hat will increase.

Ethical hackers working side by side with software developers can create great influence. Ethical Hackers have great potential to identify the security issues during software development phase which will result in more secure software architectures.

Teaching students with the practical knowledge of hacking, besides the fact that it is really important, is to plan and monitor the code of ethics of these students is significant. Their intensions should be evaluated. Some of the above studies show that hackers feel secure doing illegal activities as long as he/she is anonymous with his/her intention of hacking. After getting convicted, these black hat hackers are contributing to the society with their expertise by doing it legally.

Prioritizing security over development is important for the existence of a secure Cyber world. With the pace we are improving our security, is less than the pace of brutality of hackers. They are the threat for human beings existence, as it has the potential to instigate a Cyber war.

VI. Conclusion:

Technology is advancing day by day and it is doing a really good job connecting people. With the advancement of technology, there is a greater risk associated with the security of the cyber world. This technology can be used by people to perform different illegal activities, these people with illegal motives are known as “Black Hat Hackers”, and they are the experts for finding flaws in the technology and exploiting them. They impose great threats for the existence of cyber world. If we failed to stop them within the required time, the cyber world can collapse due to the insecurities which are associated with it. One of the good and proactive approach to fight against them is to hire Ethical Hackers who will hack system for the sake of identifying vulnerabilities and fixing them before they can be exploited by the Black Hat Hackers; such as the IT professional who hack systems to find the security gaps to fix them before they can be exploited by Black Hat hackers are known as “Ethical Hackers”. Ethical hackers have great importance for improving the cyber security, but there are risks associated with them as well. For example, what if they use their hacking skills for their personal gain neglecting their code of ethics? There is a very thin line between Ethical and Black Hat hacking, which can be evaluated by their intension to hack a system. With or without them, we are still facing risks, but they can be very effective to secure the cyber world. Bug bounty programs are utilizing and providing a legal platform for conducting Ethical hacking. Ethical hackers are paid good amount of money for their work which is a legal way of getting their personal gains, as the above study shows that 75% hacker’s motive for hacking was proven to be financial. These ethical hackers’ expertise can be used to secure technologies during the development phase. We need to encourage this field for students so we are able

VII. Acknowledgment:

First of all we would like to thank our teacher Maeeda Khalid for guiding us about conducting a proper research. We would like to express our deep gratitude to Researchers Community for providing us data for writing this research paper. Finally, we wish to thank our friends and family for helping us throughout the study.

References:

[1] S. Rebecca, “The paradoxical authority of the certified ethical hacker,” Limn, vol. 8, 2017.

[2] Olushola, Omoyiola B., “The Legality of Ethical Hacking,” IOSR Journal of Computer Engineering (IOSR-JCE), vol. 20, no. 1, pp. 61-63, 2018.

[3] Radziwill, Nicole and Romano, Jessica and Shorter, Diane and Benton, Morgan, “The Ethics of Hacking: Should It Be Taught?” arXiv preprint arXiv:1512.02707, 2015.

[4] “The Best Ethical Hacking Online Tutorials for Everyone,” 9 March 2018. [Online]. Available: Click Here

[5] John T. F. Burgess, Emily J. M. Knox, Foundations of Information Ethics, American Library Association, 2019.

[6] Hartley, Regina and Medlin, Dawn and Houlik, Zach, “Ethical Hacking: Educating Future

Cybersecurity Professionals,” in 2017 Proceedings of the EDSIG Conference, Austin, Texas USA, 2017.

[7] Munjal, Meenaakshi N, “ETHICAL HACKING: AN IMPACT ON SOCIETY,” Cyber Times International Journal of Technology & Management, vol. 7, no. 1, pp. 922--933, 2013.

[8] “Ethical Hacking,” 2020. [Online]. Available: Click Here.

[9] Sharma, Mirdul and Kaur, Satvinder, “Cyber Crimes Becoming Threat to Cyber Security,”

Academic Journal of Forensic Sciences ISSN, vol. 2581, p. 4273, 2019.

[10] “5 of the world’s greatest hackers and what happened to,” 16 October 2017. [Online].

Available: Click Here

[11] “29 Must-know Cybersecurity Statistics,” 2020. [Online]. Available: Click Here, (Gartner).