TERM PAPER

on

ETHICAL HACKING

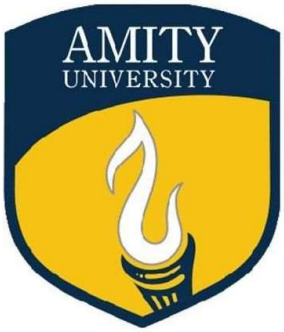
Submitted to

Amity University Noida, Uttar Pradesh

Guided By: Dr Subhash Chand Gupta

Submitted By: Yuvraj Dewan

Enrollment Number: A2305223097



AMITY UNIVERSITY UTTAR PRADESH

GAUTAM BUDDHA NAGAR

DECLARATION

I Yuvraj Dewan, student of BTech (CSE-2 (X)) hereby declare that the project titled “ETHICAL HACKING” which is submitted by me to theDepartment of Computer Science, Amity School of Engineering Technology, Amity University, Uttar Pradesh, Noida, in partial fulfillment of requirement for the award of the degree of Bachelor ofTechnology in Computer Science and Engineering, has not been previously formed the basis for the award of any degree, diploma or other similar title or recognition.

The Author attests that permission has been obtained for the use of anycopy righted material appearing in the dissertation/ project report other than brief excerpts requiring only proper acknowledgement in scholarly writing and all such use acknowledged.

YUVRAJ DEWAN

A2305223097

CSE-2 (X) {2023-27}

ACKNOWLEDGEMENT

The satisfaction that accompanies that the successful completion of any task would be incomplete without the mention of people whose ceaseless cooperation made it possible, whose constant guidance and encouragement crown all efforts with success. I would like to thank PROF. (DR.) SANJEEV THAKUR, Head of Department (CSE), and Amity University for giving me the opportunity to undertake this project. I would like to thank my faculty guide PROF. (DR.) SUBHASH CHANDGUPTA, Dy. HOD (CSE) who is the biggest driving force behind my successful completion of the project. He has been always there to solve any query of mine and guide me in the right direction regarding the project. Without his help and inspiration, I would not have been able to complete the project. I would like to thank my batchmates who guided me, helped and gave ideas to me and motivation at each step.

YUVRAJ DEWAN

A2305223097

CSE-2 (X) {2023-27}

CERTIFICATE

On the basis of report submitted by Yuvraj Dewan, student of B-Tech Cse-2 (X), I hereby certify that the report "Ethical Hacking" which is submitted to Department of Computer Science Amity School of Engineering and Technology, Amity University Uttar Pradesh in partial fulfillment of requirement for the award of the degree of Bachelor of Technology in computer science and engineering is an original contribution with existing knowledge and faithful record of work carried out by him/her under my guidance and supervision. To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

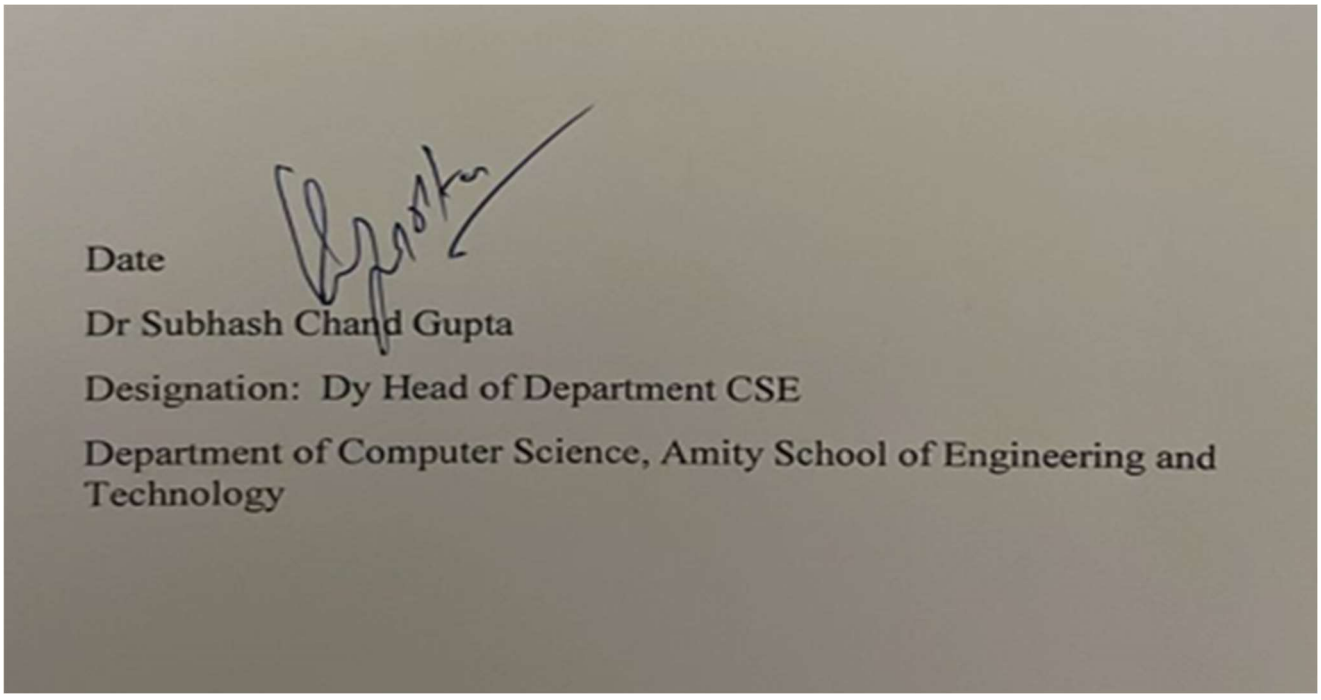


TABLE OF CONTENTS

S. No.	HEADING
1.	ABSTRACT
2.	INTRODUCTION
3.	TYPES OF HACKERS
4.	REVIEW OF LITERATURE
5.	CASE STUDY
6.	RESULTS AND DISCUSSION
7.	CONCLUSION
8.	REFERENCES

ABSTRACT:

Ethical hacking is something intertwined with the use of technology. It is a necessary safeguard which aims to prevent the inevitable misuse of the trust we have placed in our devices. The concept of ethical hacking simply means the penetration and breakdown of your device security and all its protections, but with the compliment of the owner to identify the lapses in security which would be attended to by them. This paper aims to explore the region of cybersecurity, it has a multidirectional purpose and that is to understand and simplify every corner of ethical hacking which might be of cause to the reader. It will put to test the different methodologies used by leading tech-hubs of the world and correlate every aspect of its rewards with the potential risks it all might pose. This paper will also shed light on the challenges this field would face itself and the challenges other technological fields would have through direct or indirect involvement of cybersecurity in human lives. Lastly it would show the stepping stones for future protectors of the electrical world how they could possibly join the much progressive field of cybersecurity

INTRODUCTION:

1878, the year that hacking began. It did not begin with mass disruption of public services nor did it begin with theft of confidential data. In fact, the beginning of 'hacking' was not even a term used for malpractices, it began with a few students of the Tech and Railroad club at MIT who altered the function of train sets to satisfy their wants. This set a path for them to slowly and gradually move on to computers. They used the highly advanced (for that time) IBM 704 computers at MIT to explore the limits of different operating systems. In some cases, the programs they wrote surpassed the capabilities of previous operating systems – like in the case of Dennis Ritchie's and Keith Thompson's UNIX operating system.

The first case of hacking – as we understand it now – happened just a couple years after the creation of alexander graham bell's telephone company. The beginning of the company marked the beginning of electric telephone systems where there would not be any requirement of an operator. John Draper used the toy whistle which came with a cereal box of Cap'n Crunch to produce a high-pitched sound of 2600 hertz, which confused the system and allowed him to make unlimited long-distance calls.

We know humanity does not stop at boundaries nor are they a finite limit of human capabilities. We push boundaries even if sometimes it would be better not to. This curios mindset of ours planted the idea in our head that if we can write code to help a software then we can do the exact opposite with as much ease. This kicked off hacking in the more dishonorable way we know about now.

But when we think about a hacker, the image that gets developed in our mind is that of a teenager in his basement writing codes all day long and trying to steal all our data. But the entire process doesn't always involve writing programs to somehow infest your device with. It can be as simple as faking a phone call as your network provider to get your email address details and then simply logging in as you.

So how do we counter this? How do we learn from our mistakes and protect future devices? The answer lies in the problem itself; we use hacking – but to our advantage. We play pretend as the hacker, test the flaws of our computers and whatever ones we find, we seal them. That is the entirety of cybersecurity, and that process is what we call "Ethical Hacking".

To assume ethical hacking is completely safe would be an understatement at the least. The person who we ask to find our faults can just always give that information to the people who we are trying to protect ourselves from. That person could themselves steal our data and hold us ransom. But let's say that the person is not dishonest, then still the methods used by him could prove to be ineffective against the capabilities of the attackers. Even if we manage to seal the faults in our system, the new approach we tried could always open the door to new possible points of vulnerabilities.

There are lots of different possibilities on what could happen and what might happen. So, it's a lot like a game of chess – one person creates something, and the other person tries to destroy it, again the first person protects himself in ways he might be vulnerable, and the other person finds new ways to defeat him.

1.1 TYPES OF HACKERS:

The quite sharp division between the 'light' and 'dark' side of hacking does not only persist at the process itself, rather it extends even to the professionals who would be actively taking part in the act. This is the fold which created the 2 distinct categories of hackers – a) **white hat** and b) **black hat.**

1.1.1 BLACK HAT HACKERS: these are the anti-hero of the cyber world. They are the authors of acts of corporate espionage, identity theft, financial theft or just simple viruses to infect other computers. In fact, any person who commits a crime using computers is known as a black hat hacker. some of the popular hackers are D3FAULT, Gary McKinnon and the founder of WikiLeaks – Julian Assange.

1.1.2 WHITE HAT HACKERS: the people who contain the technical prowess and the knowledge to break the firewall of computers but use their knowledge to help, instead of hurt different companies are known as ethical hackers or White hat hacker. some of the big names in this field are Jeff Moss and Khalil Shreatah.

2. REVIEW OF LITERATURE

2.1 WHAT IS ETHICAL HACKING?

Hacking, also denoted as "Penetration Hacking", "Intrusion Testing", or "Red Teaming", is a part of the multifaceted world of hacking. This kind of hacking is what we call as 'Ethical Hacking'. These are distinct from the nefarious hackers in ways that they employ various tools at their disposal to protect the computers from any kind of malware that it may be vulnerable to. Their objective is to evaluate the security of the target systems, pinpoint vulnerabilities, and furnish owners with recommendations for remediation.

They furnish reports which contain their findings like the various points of entry for malware, the possible backdoors which could be opened, the data which might be at risk the most. These reports are then compiled by the employers to retain the information provided and then use that information to future-proof themselves.

There are multiple ways in which black hat hackers can contribute to the demise of your computer security, they use the flaws present in your system to brute force their way into your device. Some of those methods include:

- **Exploiting Software Vulnerabilities:**
  hackers search for various flaws and bugs in the system software which could be targeted to exploit the computer. This could include buffer overflow attacks, code injection attacks, or privilege escalation exploits.

- **Malware Creation:**
  malware is a general term for programs that could harm the files or data on your computer, or it could even steal the information on your device. The hackers use these malwares like viruses, worms or trojans to infect devices worldwide

- **Social Engineering:**
  Hackers know that humans themselves are the weakest links when compared to computers. they use this tactic and employ methods like phishing emails and spam calls/messages to gain your confidential information which they use to access any services with those credentials.

- **Brute Force Attacks:**
  There are cases or instances where the passwords employed by us are just too weak or we can say are too easy to guess. Hackers then use various tools to try out every possible

combination for a password until they successfully log in and simply bypass the security mechanism in place

- **Exploiting Misconfigurations:**

System misconfigurations happen when administrators do not properly implement security protocols on the servers or security components. Hackers search for these misconfigurations which could possibly allow them into the software through bugs in them.

Keeping these provisions in mind a generic procedure has been established for white hat hackers. These don't serve as a law but rather as more of a guide to the hacker and guides them on the various strategies that they might explore. All these provisions are further enhanced by the involvement of various tools by the cybersecurity expert. These procedures are as follows

2.1.1 RECONNAISSANCE:

this is the information gathering phase. Before launching any attack, information about the victim is needed, hence the hackers use 'active' or 'passive' reconnaissance methodologies. **ACTIVE** recon involves using software tools such as NMAP to find vulnerabilities in the operating system and whether connections could be established and much more. **PASSIVE** recon deals with information gathering through external banks such as social media, job resumes or even public websites.

there are various steps in this phase itself. After gathering information, the destination IP address is decided and then open ports are searched in the range of the network. OS fingerprinting is used to map out the software being used by the victim. This is done by sending crafted packets to the device and noting down the responses to those packets.

2.1.2 SCANNING:

the second step involves scanning, where the hacker tries to find various pathways to gain access through IP addresses or credentials, etc. there are 3 types of scans mainly-

2.1.2.1 **Port scan** involves using port scanners to identify the open TCP or UDP ports and live running systems to easily find doorways of access.

2.1.2.2 **Vulnerability scanning** includes the use of automated tools such as Nmap, Netsparker, OpenVAS to identify and exploit the shortcomings of the computer.

2.1.2.3 **Network scanning** detects active devices on a network and finds ways to exploit the network itself

2.1.3 GAINING ACCESS:

This is the step where the hacker uses all the means and the tools at his disposal to gain access into the computer. The hacker can then install malware into the computer, steal confidential information, ask for ransom, etc. Tools like Metasploit are useful in gaining illegal access. Ethical hackers and penetration testers can secure potential entry points, ensure all systems and applications are password-protected, and secure the network infrastructure using a firewall. They can send fake social engineering emails to the employees and identify which employee is likely to fall victim to cyberattacks.

2.1.4 MAINTAINING ACCESS:

Simply gaining access is only one side of the coin, the other side is the part where the hackers maintain access to computer by creating and using backdoors. The hacker can completely exploit the system by launching Distributed Denial of services (DDoS) attacks or even stealing an entire database. Ethical hackers or penetration testers can utilize this phase by scanning the entire organization's infrastructure to get hold of malicious activities and find their root cause to avoid the systems from being exploited.

2.1.5 CLEARING STAGE:

This last stage involves the clearing of tracks by the hackers such that nothing can be traced back to them. This is of utmost important to ethical hackers as there must not be any proof of their involvement in the device. It includes editing, corrupting, or deleting logs or registry values. The attacker also deletes or uninstalls folders, applications, and software or ensures that the changed files are traced back to their original value.

3. CASE STUDY

3.1 WANNACRY ATTACK:

The risks of cybersecurity cannot be overstated enough. The potential damage that could be caused due to mis-handling of ethical hacking reports is vast, and it has been demonstrated by the WannaCry malware attack in 2017.

In around January 2017, a group of people known as 'Shadow Brokers' hacked into the National Security Agency (NSA) and leaked a windows exploit which the NSA had created called EternalBlue. The WannaCry attack used EternalBlue as its medium of propagation and the basis of the attack.

EternalBlue found vulnerabilities in the way that windows implemented the server message block (SMB) protocol and duped different windows machines into allowing illegitimate data packets inside the legitimate network and this allowed for a relatively easy method of transfer of malware such as viruses or trojans.

The exploit had been created by the NSA for 5 years but it had not been brought to the attention of Microsoft until the actual leak took place. Microsoft released a patch for the vulnerability but most users did not download the new patch update as it was very new, thus the attack became one of the most disrupting attacks in history.

The hackers easily gained control of your files and initiated a crypto hack – which means that they encrypted all the files inside the computer and demanded a ransom of 300$ worth of bitcoin in exchange for the data.

The WannaCry ransomware attack hit around 230,000 computers globally. The Spanish telephone company Telefónica was one of the first victims of the hack. By May, it spread to hundreds of NHS hospitals across the UK, leading to a cancellation of around 20,000 appointments and leading to a loss of approximately 100 million pounds.

The attack spread across 150 different countries in a short span of time and caused a global loss of 4 billion dollars

3.2 XZ MALWARE:

In the first week of April 2024, a Microsoft developer named Andres Freund revealed that a backdoor had been planted into Xz Utils – which is basically a data compressing utility that is installed on practically every Linux or Unix based computer. This backdoor, he discovered was very close to being merged into Debian and Red Hat, the 2 biggest distributions of Linux.

Xz utils is ubiquitous with Linux. It provides lossless data compression and data decompression across most of the Unix operating system devices, which makes it a crucial component of the software.

Andres discovered that SSH (a protocol for logging into devices) was consuming too many CPU cycles and generating errors while monitoring memory. Through careful digging he found that the root cause of the issues was an update made to the XZ utils.

This update manipulated the SSH executable file for remote SSH connections, allowing anyone in possession of an encryption key to remotely plant any kind of code into the device. This code could have been used for any kind of malpractice including stealing encryption keys or installing any kind of malware.

One important thing to note is how the backdoor was installed into the software. Since Linux is an open-source software, everyone has access to its code and can write code for it themselves which could be implemented by the creator into the actual software. In 2021, a person with the username JiaT75 made the first known commit to the open-source project. Slowly and through multiple commits, JiaT75 became part of the team of XZ Utils. Another person implemented a software that scanned vulnerabilities which was easily exploitable and they also made a block that would prevent the malicious changes from being discovered. These changes were implemented in the 5.6.0 and 5.6.1 updates of the XZ Utils and thereafter the backdoor became a part of the utility of Ubuntu.

This backdoor exploit if hadn’t been discovered could have been hugely detrimental to the computers using Unix based systems. Still the revelation of a hack so vast has raised concerns over the general safety of open source softwares, where once they had been considered much more secure, now reel from the effects of such a massive hack.

4. RESULTS AND DISCUSSION

4.1 MARKET ASSESMENT:

The theme for cybersecurity is an ever-evolving yoke. However, there are certain data sets which might be useful in giving us a broad idea about the rise and fall of different categories in this market. If someone were to try to understand the variabilities of this niche, it would not be a simple task as the number of drivers for any kind of change would be immense and even more so the effects of different drivers could again have compounded effects on the market itself causing further differences.

However, there are certain statistics which might help in easing some of the difficulties of trying to understand this market and simplify the process of it.

REVENUE might be one of the key factors of this industry. Just alone in the cybersecurity industry, the total revenue for 2024 is estimated to be at around US $183.10 billion, and if were to predict a forecast for the year 2030 then the estimated market size of cybersecurity would reach a whopping US $585 billion.

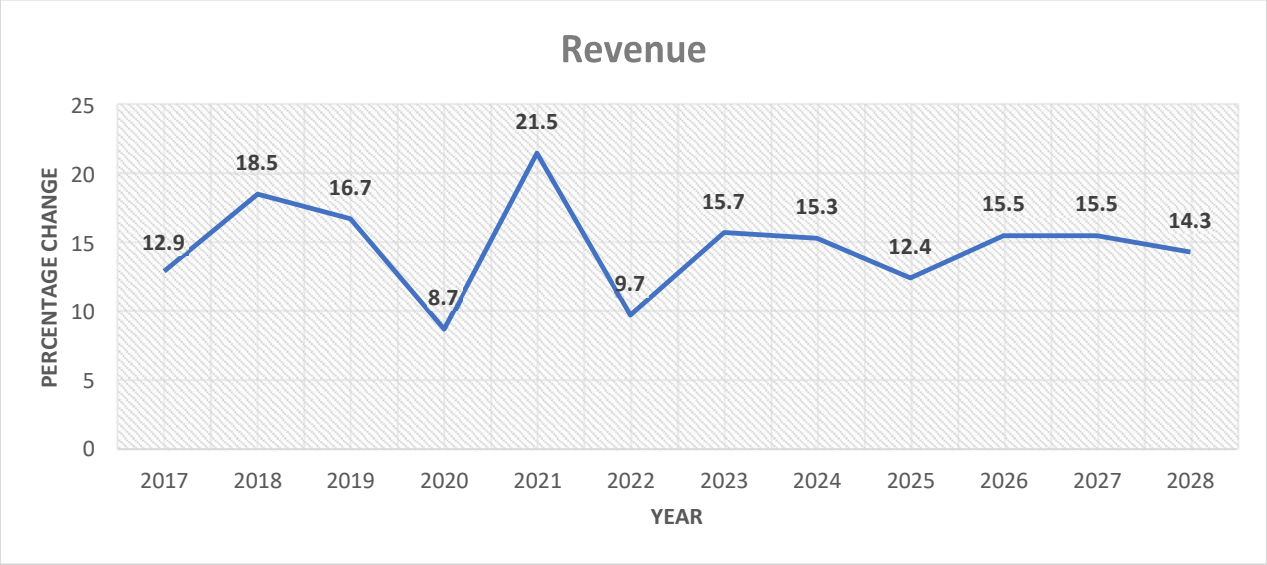


Figure 3.1

This field has seen a steady pace of growth throughout its years of existence with the only exception being the years of 2021 and 2022 which witnessed sharp increase and decrease respectively, the sole cause of which were the effects of the covid-19 pandemic.

Another aspect is COST. Cost is different than revenue in the sense that cost means the money that was affected by Hacking. Healthcare was the leading field for the 12th time in a row in data breaches amounting to a whopping US $10 million in 2022. The United States was the most targeted and hacked country in the world with damages averaging at around US $10 million per data breach. Causing an average loss of US $70,000 per person, investment fraud was the most expensive type of cybercrime.

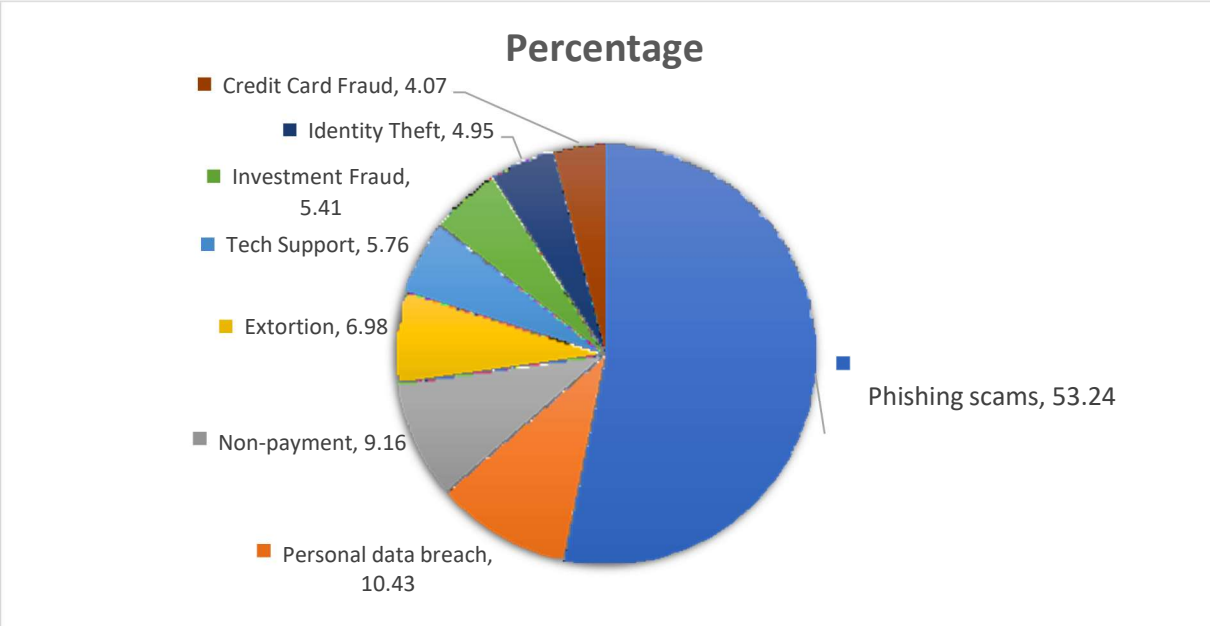


Figure 3.2

4.2 FUTURE APPLICATIONS:

Limiting the usage of a field like this can be subject to the cruelty of scrutiny, as with the rise of a new era of technology, the need for its security is growing at a rapid pace and shows no sign of slowing down. Artificial Intelligence (AI) is a word on everyone's mind, it's a goldmine for the investors and a pet for the users. Thus, the question arises, is it safe? Can we trust it? Should it be implemented in highly confidential situations?

For us to make decisions based on scientific findings we first need to understand – in a basic sense – how AI works. All algorithms like LLM's (large language models) which are termed as generative AI work on a simple concept, they have a huge dataset in their backbones and whenever the model is asked a question or posed with a task, it simply searches the aforementioned dataset

for clues on how to solve the task or simply put, it looks for the answer to the question posed. But the difference between humans and machine is that when we are asked a question we will search for the solution and whenever we find it, we will answer. However, a machine will look for the answer, and once found it again searches in another directory and continues to do so until it gets a similar answer from multiple places and then produces the output.

This ability of models is hugely beneficial when it is combined with the speed of computers. These models can be trained with datasets such that they can recognize patterns, identify changes in trends and detect anomalies allowing swift and definitive action to be taken at speeds much surpassing human capabilities, and by limiting human interference, systems can be made more secure and obliquely, more economical.

However, these models are flawed and their threat detection capabilities can be faulted. A simple method is that a person can use 'Data Poisoning' which essentially means putting false information into the model's dataset which totally corrupts its output and its abilities in analyzing faults. These algorithms are not perfect either (at this stage in time) the AI can 'hallucinate' and on its own present false information which could lead to improper and detrimental actions to be executed. This leads to another opportunity to hack generative AI models, which is essentially coaxing/leading the model into thinking in a certain way in which the user wants and producing immobile outputs. Machines are gullible to all kinds of misleading actions as they have no thoughts of their own, no matter how much you train them, they will never be able to 'think' like humans.

Generative AI (and LLMs in particular) is undoubtedly impressive in its ability to generate a huge range of convincing content in different situations. However, the content produced by these tools is only as good as the data they are trained on, and the technology contains some serious flaws. Thus, despite the integration of AI in cybersecurity, human expertise remains vital in combating cyber threats. While AI can automate specific processes, cybersecurity professionals possess critical thinking and decision-making skills essential in identifying advanced cyberattacks and developing effective strategies to safeguard against them.

CONCLUSION

Understanding the frills of cybersecurity simply by knowing about its concepts is a task best appreciated with the huge research it requires. To simply summarize the whole of cybersecurity as ethical hacking would also be an understatement to say the least. Sure, hacking holds its place as the leader of this field but it is not the entirety.

Through the past few years, we have seen the rise of technology's involvement with our lives, we have seen the machine intertwine itself with our heartbeats and so the with all its glory, its repercussions must be understood as to the effects that it might have on our bodies and minds.

Through meticulous observations, ethical hackers stand at the frontlines protecting us from the omnipresent black hats. The looming threat of the advancement of technology with machines has made the need for ethical hackers much more crucial. They act as shepherds with us as their flock – spending all their working time to protect us from the wolves lurking at the door.

Time has been a spectator to all the advancements we have made, and it will continue to be so. It saw the greatness of machines when we were making them as gods and it also saw the darkness lurking behind them which would attack us at our lowest. The need for ethical hackers was there in the past, that need is much more important now and it will be crucial in the coming years.

REFERENCES

1. Prasad, C., & Kumar, D. B. (2024). Ethical Hacking: Vulnerabilities & Dangers. In *International Journal of Science and Research (IJSR)*. https://www.ijsr.net
2. Haq, H. B. U., Hassan, M. Z., Hussain, M. Z., Khan, R. A., Nawaz, S., Khokhar, H. R., & Arshad, M. (2022). The Impacts of Ethical Hacking and its Security Mechanisms. *Pakistan Journal of Engineering & Technology*, *5*(4), 29–35. https://doi.org/10.51846/vol5iss4pp29-35
3. Bari, M. A., & Ahamad, S. (2016). *Study of Ethical Hacking and Management of Associated Risks*. *01*(01), 07–11. https://doi.org/10.24032/ijeacs/0101/02
4. *What Is Hacking? Types of Hacking & More | Fortinet*. (n.d.). Fortinet. https://www.fortinet.com/resources/cyberglossary/what-is-hacking
5. Simplilearn. (2020, April 1). *What Is Ethical Hacking? | Ethical Hacking In 8 Minutes | Ethical Hacking Explanation | Simplilearn* [Video]. YouTube. https://www.youtube.com/watch?v=XLvPpirlmEs
6. Fern. (2024, March 17). *The Kids Who Hacked The CIA* [Video]. YouTube. https://www.youtube.com/watch?v=PmtFtWVrxFE
7. *D3f4ult – Darknet Diaries*. (n.d.). https://darknetdiaries.com/transcript/139/
8. *What is WannaCry ransomware?* (2024, March 21). www.kaspersky.com. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
9. Online, B. (2021, December 16). Yahoo Data Breach: What Actually Happened? - BPB Online - Medium. *Medium*. https://bpbonline.medium.com/yahoo-data-breach-what-actually-happened-54cf8f3f7c93
10. Johansen, R. (2023, October 13). *Ethical Hacking Code of Ethics: Security, Risk & Issues*. Panmore Institute. https://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues
11. *CSF 1.1 Quick Start Guide | NIST*. (2024, February 26). NIST. https://www.nist.gov/cyberframework/csf-11-quick-start-guide
12. *OWASP Top Ten | OWASP Foundation*. (n.d.). https://owasp.org/www-project-top-ten/
13. *BeCyberSafe.com | How Do Hackers Hack?* (n.d.). BeCyberSafe.com. https://www.becybersafe.com/whowhyhow/how-do-hackers-work.html
14. *Vulnerable By Design ~ VulnHub*. (n.d.). https://www.vulnhub.com/
15. Showers, T. (2023, December 18). *How to Hack: 14 Steps (With Pictures)*. wikiHow. https://www.wikihow.com/Hack

16. Amblard-Ladurantie, C. (2024, July 2). *Will AI Replace Cybersecurity Experts? The Human Vs. AI Debate*. MEGA. https://www.mega.com/blog/will-ai-replace-cybersecurity-experts-human-vs-ai-debate#:~:text=While%20there%20is%20concern%20that,those%20insights%20require%20human%20oversight.
17. *Cybersecurity - Worldwide | Statista Market Forecast*. (n.d.). Statista. https://www.statista.com/outlook/tmo/cybersecurity/worldwide#revenue
18. *The Evolution of Hacking*. (n.d.). Tripwire. https://www.tripwire.com/state-of-security/the-evolution-of-hacking
19. *Cybersecurity Facts and Statistics Report - 2023 | Prey*. (2023, January 27). https://preyproject.com/blog/cybersecurity-statistics
20. Ec-Council. (2024, April 24). *What is Ethical Hacking*. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-ethical-hacking/
21. *What is EternalBlue? | Security Encyclopedia*. (n.d.). https://www.hypr.com/security-encyclopedia/eternalblue
22. Technica, D. G. A. (2024, April 2). The XZ Backdoor: Everything You Need to Know. *WIRED*. https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/
23. Karcherm. (n.d.). *GitHub - karcherm/xz-malware: Stuff discovered while analyzing the malware hidden in xz-utils 5.6.0 and 5.6.1*. GitHub. https://github.com/karcherm/xz-malware