Borneo International Journal eISSN 2636-9826; Vol. 6 (1); 2023; 53-60
Published by *Majmuah Enterprise*
www.majmuah.com

Critical and Creative Thinking in A Hacker's Work

ABDUL KADIR BIN MAHAMOOD and MOHAMAD FADLI BIN ZOLKIPLI
School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: kadirjpn@gmail.com , m.fadli.zolkipli@uum.edu.my | Tel: +60134368080, +60177247779 |

Received: February 23, 2023
Accepted: February 26, 2023
Online Published: March 01, 2023

Abstract

Ethical and unethical hackers possess similar skill levels, intelligence levels, and competency though their manner of practice differentiates them. Ethical hackers practice their skills to identify loopholes and weaknesses within the systems and rectify them. Unethical hackers manipulate the systems to breach organizational data. Consequently, cybersecurity was developed to limit and eliminate the threats of cyber-attacks. Several techniques for limiting cyber threats have been developed, including educating employees on better ways of avoiding cyber threats. As technology advances, unethical hackers are developing newer methods of bypassing all systems to access customers' critical information. This study examines the role of critical and creative thinking in hacking, an area where these two modes of thinking are essential for success. It provides a definition of critical and creative thinking and explores how it can be applied to the practise of hacking. Critical thinking is shown to be essential for identifying vulnerabilities and creating effective exploits, while creative thinking is needed to find new approaches to hacking challenges. The study also discusses ethical considerations in hacking and argues that critical and creative thinking can be used to promote positive change in the field. Overall, this study emphasises the importance of developing critical and creative thinking skills to succeed in the world of hacking and highlights the potential for innovative solutions to cybersecurity challenges through the application of these modes of thinking.

Keywords: Critical Thinking; Creative Thinking; Hackers; Cybersecurity; Ethical Hacking; Technical skills.

1. Introduction

Critical thinking involves evaluating information and arguments, making decisions based on logic and evidence, and questioning assumptions. In the context of hacking, critical thinking is used to analyze security vulnerabilities in systems and applications, evaluate the potential risks and consequences of different types of attacks, and determine the most effective methods for exploiting vulnerabilities. Creative thinking involves coming up with new ideas and innovative solutions. In the context of hacking, this might involve finding new ways to bypass security systems, developing novel methods of attack, or inventing new tools and techniques to automate tasks. Both critical and creative thinking are essential skills for a hacker, as they allow them to identify weaknesses in systems, develop effective strategies for exploiting those weaknesses, and continually adapt to new challenges and changing circumstances. However, it is important to note that the use of these skills for malicious purposes is illegal and unethical, and hackers should use their abilities for defensive purposes only, to improve security and protect against attacks.

Data breaches and hacking of organizational accounts have become common phenomena. Companies like Yahoo, Alibaba, LinkedIn, Facebook, Myspace, and Adobe have all been victims of data breaches (Etuh & Bakpo, 2022). Customers become victims of cyber threats where their personal data is stolen, manipulated, or altered against their will. Undoubtedly, there have always been ways to solve cyber security threats using creative methods such as Anti-virus software, virtual locks, firewalls, Virtual Private Networks (VPN) and Two-factor Authentication, unique solid passwords, disaster plans, and sensitive data training, among other techniques (Hartley et al., 2017; Lessambo, 2023). However, hackers are also creating advanced ways of bypassing all the security and safety guidelines to achieve their goals. Some hackers even share their ideas or work as partners to bypass all the security and perfect their methods of doing that as a career. Today, DDoS issues and malware attacks have increased, and cybersecurity companies can only play catch-up.

2. Overview

Background

The internet and technological advancement have contributed to positive and negative impacts within organizations. Some adverse effects of technology and the internet include cyber-attacks and other security breaches that jeopardize organizations' systems and customers' crucial information. Consequently, cyber security is seen as an antidote to cyber-attacks. The present paper will review the history of cybersecurity and the new mechanisms that are being initiated to prevent cyberattacks in the future.

The topic of "Critical and Creative Thinking in A Hacker's Work" is of growing interest in fields related to cybersecurity and computer science. The increasing prevalence of cyberattacks and data breaches has highlighted the need for skilled professionals who can think critically and creatively to identify and solve security problems. Hacking, in the context of this topic, refers to the use of computer programming skills to identify and exploit vulnerabilities in computer systems. While the term "hacker" can have negative connotations, not all hacking is malicious, and many professionals work as ethical hackers or "white hat" hackers to help organizations identify and fix vulnerabilities in their systems.

To be effective in this work, hackers need to be able to think critically and creatively to identify potential attack vectors and develop strategies for securing systems. They must be able to analyze complex information, evaluate risk, and make decisions quickly. Additionally, hackers must be adaptable and resourceful, as they are often working with limited information and under time constraints. As a result, there is a growing interest in developing educational programs and training opportunities that focus on developing critical and creative thinking skills in the context of cybersecurity and hacking. This includes courses and certifications that cover topics such as risk assessment, ethical hacking, and cyber defense.

History of Cybersecurity

Cybersecurity may have started with the first computers and the beginnings of the internet. Security precautions to guard against unwanted access and assaults grew more and more necessary as computer systems proliferated and became more networked. Several significant occasions and turning points in cybersecurity history are listed below:

- Early computer security: Throughout the 1960s and 1970s, physical security measures like server rooms with secured doors and access restrictions were the main emphasis of computer security. At this time, password-based authentication methods also began to develop.
- Early computer viruses: The first computer viruses were created in the 1980s and propagated over floppy discs and other physical media. As a result, antivirus software was created, and the need for software-based security measures was realized.
- As the internet became more popular in the 1990s, hackers and attackers took advantage of holes in networks and online applications to cause new security problems.
- Cybersecurity standards and regulations were established in the early 2000s to give advice on best practises for protecting computer systems and networks. Examples of these standards and regulations are ISO 27001 and HIPAA.
- Increase in cyberattacks and data breaches: Because of the recent rise in cyberattacks and data breaches, new security technologies have been created, and businesses and governments are putting more emphasis on cybersecurity.

Nowadays, cybersecurity is a major issue for all people, organizations, and governments around the globe. Since threats are always changing, it's more important than ever to have strong security measures and cybersecurity staff who know what they're doing.

Cybersecurity is not a recent invention but dates back to the first-time data was stored on the computer and needed protection using passwords. In contrast, (Greenlaw & Raj, 2022) argues that the need for cyber security was non-existent since the first computers to be manufactured were only operated by a small group of people; thus, no external actors would interfere with the system. However, hacking did not start with computers but phones through a phenomenon referred to as phone phreaking in the 1950s (Hatfield, 2018). According to (Pogrebna et al., 2019), phone users would tamper with the protocols, thus allowing them to avoid paying long-distance charges and enjoy free calls. Even though the idea was absolute in the 1970s, similar ideas would later be used in digital technology (Hatfield, 2018; Lessambo, 2023). As more businesses ventured into buying more computers, the need for cyber security was heightened. The 1970s saw the need for and evolution of cybersecurity, starting with The Advanced Research Projects Agency Network (ARPANET) (DuPont & Fidler, 2016; Fidler, 2017). The Advanced Research Projects Agency Network (ARPANET) was effective in getting rid of unlawful programs. However, one of the ARPANET researchers, Ray Tomlinson, designed a Reaper program that effectively eliminated the Creeper worm (Kamra & Scott, 2019; Shukla et al., 2022). The Creeper did not eliminate all the cyber-attacks that could have occurred; hence there was a need to develop other antidotes to cyber-attacks. High-profile attacks had increased in the 1980s and 1990s, including Los Alamos National Laboratory, AT&T, and National CSS (Lessambo, 2023; Nelson & Endicott-Popovsky, 2016). The "Trojan Horse" and "computer virus" were developed then. Multiple anti-viruses were created to eradicate the program viruses (Zhenfang, 2015). Since then, diverse approaches to cyber security have been developed, with the most significant moments being between 2010 and to date.

Issues/Threats

Unethical hacking is a serious threat to cybersecurity, as it involves the use of hacking techniques for malicious or illegal purposes. Here are some of the key issues and threats associated with unethical hacking:

- Unauthorized access: Unethical hackers may attempt to gain unauthorized access to computer systems or networks, often for the purpose of stealing sensitive information or causing damage.
- Malware and viruses: Unethical hackers may create and distribute malware and viruses that can infect computer systems and cause harm to users.
- Denial of service attacks: Unethical hackers may launch denial of service (DoS) attacks that overload computer systems and networks, causing them to become unavailable to users.
- Ransomware attacks: Unethical hackers may use ransomware to encrypt data on computer systems, demanding payment in exchange for the decryption key.
- Cyber espionage: Unethical hackers may attempt to steal sensitive information from government agencies, businesses, or individuals, often for the purpose of espionage or financial gain.
- Cyberterrorism: Unethical hackers may attempt to disrupt critical infrastructure or cause harm to individuals or society as a whole, often for ideological or political reasons.

These threats pose significant risks to the security and privacy of individuals and organizations, as well as the stability and safety of society as a whole. To combat these threats, it is essential to have effective cybersecurity measures in place, including strong passwords, firewalls, encryption, and regular software updates. Additionally, it is important to have skilled cybersecurity professionals who can identify and respond to threats in a timely and effective manner. One of the main issues with cyber security involves unethical hacking. (Aljebry et al., 2022; Lessambo, 2023; Svabensky et al., 2020; Nelson & Endicott-Popovsky, 2016) argue that unethical hacking has compromised the security systems of organizations and therefore jeopardized customers' information. Unethical hackers' main agenda is to access restricted networks and steal free software, money, and other valuable information (Abahussain & Hammad, 2019; Sen & Heim, 2020). Hackers use different techniques to access organizations' databases, as discussed below. Each threat may require a different cyber security approach to neutralize it.

3. Existing Hacking Techniques

Attackers may use a variety of hacking methods to obtain unauthorised access to computer systems and networks. These are a few typical instances:

- **Phishing**: Phishing is a sort of social engineering in which an attacker sends a phoney email or message in an effort to persuade the receiver to divulge sensitive data, such as login passwords or credit card details.
- **Password cracking**: To access a user's account or computer system, a password must be cracked or tried to be guessed.
- **SQL Injection**: With this attack method, hackers may access sensitive information by bypassing authentication and injecting malicious code into a web application's database.
- **Attacks by a "man in the middle"**: Man-in-the-middle attacks include intercepting and changing communications between two parties in order to get data or credentials.
- **Attacks that deny service**: Denial of service (DoS) attacks include saturating a computer system or network with requests or traffic to the point that they are inaccessible to authorised users.
- Any harmful programme that is intended to infiltrate a computer system or network and cause harm or data theft is referred to as malware.
- **Physical attack**: Physical attack refers to acquiring physical access to a device in order to gain access to a computer system or network. This is often done by stealing the equipment or gaining illegal access to it.

These are but a few instances of the hacking methods that attackers could use to obtain unauthorised access to computer systems and networks. Keep up with the most recent methods and recommended procedures to reduce cybersecurity dangers as they develop. Hackers have numerous ways of hacking a system, and they should take several steps to avoid them. The most common hacking techniques that have been used in the past to date include Phishing, Bait and switch attacks, key logger, Denial of Service Attacks (Dos/DDoS) Attacks, Clickjacking Attacks, Fake W.A.P., Cookie Theft, Viruses, and Trojans, Enumeration, AQL injection, and sniffing (Pogrebna et al., 2019; Yaacoub et al., 2021; Zhenfang, 2015). In Phishing, the attacker sends a fake message pretending to be trustworthy to entice the receiver to respond to that message (Nurse, 2018). Any receiver which performs that action may end up installing a malicious file that makes it easy for the hacker to steal data maliciously. Bait and switch attack is a method where the attacker tricks the user into visiting a malicious site using a link (Mosteanu, 2020). The link can compromise the

system, lock the browser, or download malware. A key logger is a software that can be downloaded into one's computer to record a keystroke (Pogrebna et al., 2019). The software captures the most sensitive personal data, including the credit card numbers and every username of the user. The Denial of Service (DoS\DDoS) Attack is a system used by hackers to crash a website (Yaacoub et al., 2021). Hackers use a myriad of requests to flood and overload the web server. In some instances, the hackers rely on zombie computers and botnets (Yaacoub et al., 2021; Zhenfang, 2015). A clickjacking attack is a method that tricks the user into clicking something else rather than the intended button. Consequently, the fake button, when clicked, performs a different function, thus allowing the hacker to bypass all the securities and control every other aspect of that computer (Yaacoub et al., 2021; Zhenfang, 2015). In most cases, the host website must be made aware of the existence of the clickjacking element.

On the other hand, Fake wireless access point (W.A.P.) has been one of the easiest ways for hackers to bypass all the security and gain access to personal computers. Hackers use softwares to impersonate a Wireless Access Point (W.A.P.) which can connect to the 'official' public place. Everyone who connects to the public wireless access point is prone to the cyber-attack, and their data can be breached (Toh et al., 2017). Hackers use genuine names to entice individuals to join the wireless access point. Cookie theft is also a creative way that hackers are using to breach data. Cookies in web browsers like Safari and Chrome store personal data such as passwords, usernames, and history of browsing for the different sites that users access (Yaacoub et al., 2021). Conversely, a hacker will use I.P. (data) packets and gain access to a user's data whenever the website the user is browsing does not have an SSL (Secure Socket Layer) certificate (Toh et al., 2017). Viruses and trojans are created as malicious programs that a user can download from the internet.

Once the user installs the program, it becomes easy for the hacker to receive all the data and sometimes lock the files and gain access to all other computers connected to the user's computer and breach all the data (Zhenfang, 2015). Enumeration is a process where the hacker gathers all the information needed, like passwords, usernames, I.P. addresses, and other personal data from the victim (Sheikh, 2021). The hacker must establish an active connection with the target host to get all that information and exploit the system. Hackers have also identified other loopholes and use SQL injections by sending a SQL query to the system database (Sheikh, 2021). This method of attack first targets the website before targeting customers' information.

4. Future Hacking Trend

New cybersecurity dangers and trends are expected to emerge as technology continues to advance. These are a few probable hacking tendencies to watch out for in the future:

- AI-powered attacks: As machine learning and artificial intelligence (AI) evolve, it's feasible that attackers may start exploiting these technologies to create more complex attack techniques.
- Ransomware as a service: Although ransomware assaults are currently a widespread danger, it's feasible that attackers may start providing ransomware as a service in the future, enabling others to launch attacks in return for a charge.
- Attacks on the supply chain: Attacks on the supply chain are directed against the companies who provide hardware and software to businesses, often with the intention of infecting the goods with malware or other harmful code.
- Exploiting new technologies: As developing technologies like the Internet of Things (IoT), 5G, and cloud computing continue to gain traction, it is expected that attackers will start focusing on these platforms for new kinds of assaults.
- Quantum computing: As this technology develops, it's feasible that hackers may use it to bypass present encryption protocols and access sensitive data.

These are only a few possible future hacking trends, therefore it's critical to keep up with the most recent dangers and effective mitigation techniques. It is critical to have strong security measures in place and knowledgeable cybersecurity personnel who can recognise attacks and act quickly and effectively. This is because cybersecurity threats are always evolving. Hackers are not liming themselves to the current hacking techniques even though they are still utilizing them because of system vulnerabilities and betrayal from insiders (people working for the companies that are at risk of cyber threats). Since most companies have already created mitigative measures and are investing in security, hackers take more time and have introduced other techniques, such as brute force. Brute force is a hacking technique whereby the hacker repeatedly tries several passwords and username combinations until they succeed (Mohamed Mizan et al., 2019; Stiawan et al., 2019). Others include waterhole attacks, DNS Spoofing, UI Redress, Eavesdropping, Cross-site Scripting (XSS), AI (Artificial Intelligence), Network analyzers, Spidering, Geo-Targeted phishing threats, and other users of other devices connected to personal data (Chiew et al., 2018; Leal et al., 2017). A waterhole attack is a method that requires the hacker to survey the victim and follow them to their favourite

public places like a shopping mall, cafeteria, and coffee shop because it is easy to inject and spread a virus to many victims because there is a public Wi-Fi available (Dakov & Malinova, 2021). On the flip side, DNS spoofing is a hacking technique that occurs when the Domain Name Server is used as the traffic warden of the internet. UI redress is also a technique that hackers will utilize in the future by targeting unsuspecting victims (Dakov & Malinova, 2021). This technique requires the victims' users to click elsewhere because the user's interface is always covered, leaving them without a choice. By clicking another place, the victim is taken to another unknown page. Eavesdropping is a unique attack technique because it requires one to be passive when the others are active (Dakov & Malinova, 2021). The hacker harms other networks by compromising the accessed system and harming the data.

In most cases, passive attacks occur when the attacker wants to monitor the networks for them to obtain sensitive data without any detection. Cross-site scripting is used by the hacker to target the visitors of a website by using malicious code injected into the website (Tariq et al., 2021). Unknowingly, the script runs automatically on that site, and all website visitors will be affected. Artificial Intelligence is being exploited by hackers in several ways. AI may be used to track and identify patterns in computer systems to reveal all the weaknesses in the security programs and software (Tariq et al., 2021). Network analyzers are similar to AI intelligence because they exploit weaknesses in the system and programs using multiple tools (Sheikh, 2021). The network analyzers allow hackers to monitor and intercept data packets sent to other networks. This method enables hackers to obtain plain text passwords that are contained within (Sheikh, 2021). One of the unique things about this attack is that it needs the hacker to either to have physical or malware access to a network switch instead of exploiting an existing network bug or system vulnerability. In the future, network analyzers will use this tool as the first phase of an attack and proceed to use a brute force attack.

Hacking will be challenging in the future because of the new developments in cyber security; thus, a technique like spidering will also be one of the popular options among hackers. Spidering will require the hackers to develop intimate relationships with the targets so that they can easily acquire credentials based on their activity (Tariq et al., 2021). Even though this method takes more time, it is more effective. Nonetheless, the success associated with this method will depend on the targets. In cases where the target is a large corporation, hackers will try to use internal documentation to obtain some of the securities the target uses. On the other hand, phishing is being advanced to suit the hackers' objectives. A new method of hacking is named Geo-targeted phishing threats, whereby hackers only target victims who live within specific locations (Nirmal et al., 2021). With only one innocent clickbait, the victim may reveal some personal information, including employee IDs. The attacker can later use that information to gain access to all the internal networks and launch several attacks or ransomware. Lastly, hackers have become more creative and better understand the Internet of Things. The internet of things describes the connectivity between physical objects embedded with multiple technologies, software and sensors to connect and exchange data with the systems and devices over the internet (Arif et al., 2022). Conversely, the hackers take control of some of these devices, such as the cameras, microphones, and connectivity with phones, to obtain personal data such as passwords and later use them to breach the data.

5. Discussion

Ethical Hacking

The practise of employing hacking methods to find security flaws and vulnerabilities in computer systems and networks is known as ethical hacking, commonly referred to as "white hat" hacking. In order to find possible security flaws and fix them before they can be used by bad actors, corporations often engage ethical hackers to do security assessments or penetration tests. The security of computer systems is tested by ethical hackers using a range of methods and technologies, such as port scanning, vulnerability scanning, and social engineering. They could also try to access sensitive data or systems by trying to exploit security flaws. The objective of ethical hacking is to find and fix possible security flaws before attackers can utilise them. It is not to injure or destroy computer systems. Strict moral and legal rules must be followed by ethical hackers, and any vulnerabilities found must be immediately disclosed to the company and fixed.

Ethical hacking is crucial for companies because it allows them to identify loopholes and possibly develop mitigative measures to protect the system. Ethical hackers are critical and creative thinkers who understand the system better and have to re-think all possible ways that unethical hackers could use to hack into a system (Saha et al., 2020). Some of the skills needed by ethical hackers include cryptography, cloud computing, operational technology (OT) hacking, Internet of Things (IoT), wireless network hacking, web application hacking, Network, and perimeter hacking, system hacking phases and attack techniques, reconnaissance techniques and information security (Sheikh, 2021). Some of the courses available for teaching ethical hackers include hacking mobile applications, hacking wireless networks, hacking web servers, evading intrusion detection systems, firewalls, and honeypots, session hijacking, social engineering, malware threats, system hacking, vulnerability analysis, scanning networks, foot printing, and reconnaissance (Yaacoub et al., 2021). Lastly, ethical hackers can work with multiple organizations, such as information security

managers, architects, engineers, consultants, analysts, vulnerability assessors, and penetration testers (Sheikh, 2021). Ethical hacking is crucial because it provides a solution for the current security threats and issues.

Latest Solution for Current Security Threats/Issues

Organizations and individuals may employ a variety of best practices and solutions to address the current security risks and issues. These are some of the most recent techniques and solutions:

- Use of multifactor authentication (MFA) is an excellent approach to guard against illegal access. MFA mandates that users log in to a system or app using two or more kinds of authentication, such as a password and a biometric scan.
- Zero trust security: Zero trust security is a security paradigm that continuously verifies identity, access, and other characteristics before giving access to resources. It operates on the premise that all people, devices, and applications are unreliable.
- Endpoint detection and response (EDR) solutions can locate and neutralise sophisticated threats that conventional antivirus software is unable to identify. To identify potential risks and react to them in real time, EDR systems leverage machine learning and behavioural analytics.
- Security information and event management (SIEM) systems gather and analyse data from many sources in order to identify possible security risks and issues in real time.
- Software should be updated often in order to address known problems and prevent attackers from exploiting them.
- Employee education on cybersecurity best practises and dangers is crucial to preventing human error and lowering the risk of security breaches.

These techniques and solutions may lessen cybersecurity dangers and problems. Being aware of the most recent dangers and solutions is essential for maintaining effective security measures since cybersecurity threats are continuously changing. Cyberattacks are diverse; thus, there is a need to have multiple strategies needed to protect the organization and all customer's data from any of the attacks. Again, each organization must realize that there is never a 100% vulnerability-free or "hacker-proof" system because a threat actor is sometimes equipped with enough manpower, resources, and time to launch an attack. Therefore, a combination of solutions is needed (Abahussain & Hammad, 2019; Lessambo, 2023; Sen & Heim, 2020). Some current and future solutions for such attacks include keeping the software's and system updated, ensuring endpoint protection, using a firewall, backing up data systems, controlling access to other systems, and using passwords. Attackers always look for weaknesses and loopholes to utilize. Therefore, all the systems should be updated regularly using tools such as patch management that ensures that all the software and systems have been updated to keep the system resilient. Endpoint protection helps to protect all the networks remotely bridged to devices like laptops, tablets, and devices connected to the main Network (Lessambo, 2023). Installing a firewall is one of the guaranteed ways to protect the system against cyber threats. Ideally, a firewall system functions by blocking all the brute force attacks made on the systems or Network before they can result in any damage (Lessambo, 2023).

There are instances where the threat actor may find their way into the system and breach some data. To avoid such scenarios, it is recommendable for an organization to have a backup plan within the system to which the attacker cannot gain access. A backup system ensures that all customer's data is protected from any breach and that anything that has been altered would be restored to avoid severe financial losses, data loss, and severe downtime (Lessambo, 2023). The other preventive measure involves controlling access to the systems. There are instances where the attacks are physical. A perimeter security system is one of the efficient ways of protecting the system from break-in attacks (Lessambo, 2023). Nevertheless, it is crucial to conduct regular employee training to know how to detect phishing emails or any form of a cybersecurity attack and how to prevent them (Abahussain & Hammad, 2019). Weak passwords have also been an easy way for attackers to bypass the systems and breach data. Password cracking technology has also significantly advanced in recent times; thus, there is a need to deploy multi-factor authentication strategies and complex passwords that discourage cybercrimes. The employees should also be prevented from sharing the passwords to ensure that the system remains secure in case the other desktops are hacked. Lastly, some companies prefer to rely on third-party vendors for cyber security. Assessing and monitoring the vendors is one grantee way to ensure that all threats have been eliminated. The organization's security manager should focus on particular issues like strategic, operational, legal, regulatory, compliance, and cybersecurity risks.

6. Conclusion

This article talks about how important it is to be able to think critically and creatively in the fields of cybersecurity and hacking. The article says that for hackers to be successful in this field, they need to be able to think creatively in order to find potential attack vectors and come up with ways to secure systems. They also need to be able to analyse complex information, evaluate risk, and make quick decisions. The article explores various aspects of the work of a hacker, including the technical skills, problem-solving abilities, and motivations required to be successful in this field. It also discusses the various roles that hackers can play, from malicious attackers to ethical hackers and security experts. The article concludes that developing critical and creative thinking skills is essential for anyone working in the field of cybersecurity and hacking. With the increasing prevalence of cyberattacks and data breaches, the need for skilled professionals who can think critically and creatively to identify and solve security problems has never been greater. As a result, there is a growing interest in developing educational programs and training opportunities that focus on developing critical and creative thinking skills in the context of cybersecurity and hacking.

Ethical hacking is a guarantee that will help eradicate most of the cyberattacks experienced by individuals and global organizations. Hackers rely on various techniques to steal personal information and bypass systems, thus breaching all private information within multiple systems. Ethical hacking aims to identify all the loopholes and create mitigative measures to help limit the damage. Employees should also be taught about possible threats to ensure that they do not disclose private information, allowing hackers to manipulate the system.

7. Acknowledgment

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project.. This work was supported by Ministry of Higher Education Malaysia and Universiti Utara Malaysia.

References

Aljebry, A. F., Alqahtani, Y. M., & Sulaiman, N. (2022). Analyzing Security Testing Tools for Web Applications. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2021, Volume 1* (pp. 411-419). Springer Singapore.

Abahussain, O., & Hammad, M. (2019, September). Validating Software Security using Regular Expressions. In *2019 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)* (pp. 1-5). IEEE.

Arif, S. M., Bacha, B. A., Ullah, S. S., Hussain, S., & Haneef, M. (2022). Tunable control of internet of things information hacking by application of the induced chiral atomic medium. *Soft Computing*, *26*(20), 10643-10650.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, 1-20.

DuPont, Q., & Fidler, B. (2016). Edge cryptography and the codevelopment of computer networks and cybersecurity. *IEEE Annals of the History of Computing*, *38*(4), 55-73.

Dakov, S., & Malinova, A. (2021). A SURVEY OF E-COMMERCE SECURITY THREATS AND SOLUTIONS. *Proceedings of CBU in Natural Sciences and ICT*, *2*, 1-9.

Fidler, B. (2017). Cybersecurity governance: A prehistory and its implications. *Digital Policy, Regulation and Governance*.

Greenlaw, R., & Raj, R. K. (2022). ABET's cybersecurity accreditation: history, accreditation criteria, and status. *ACM Inroads*, *13*(4), 14-21.

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102-113.

Hartley, R., Medlin, D., & Houlik, Z. (2017). Ethical hacking: Educating future cybersecurity professionals. In *Proceedings of the EDSIG Conference ISSN* (Vol. 2473, p. 3857).

Kamra, S., & Scott, J. (2019). Impact of data breaches to organizations and individuals. *Available at SSRN 3510590*.

Lessambo, F. I. (2023). The Cybersecurity Counteroffensive. In *Anti-Money Laundering, Counter Financing Terrorism and Cybersecurity in the Banking Industry: A Comparative Study within the G-20* (pp. 11-32). Cham: Springer Nature Switzerland.

Leal, C., Meirinhos, G., Loureiro, M., & Marques, C. S. (2017, March). Cybersecurity management, intellectual capital and trust: a new management dilemma. In *ECIC 2017-9th European Conference on Intellectual Capital* (pp. 171-183).

Nelson, S., & Endicott-Popovsky, B. (2016, February). Cyber Public Private Partnership ICS/SCADA and Critical Infrastructure Protection Strategic Vision. In *Journal of The Colloquium for Information Systems Security Education* (Vol. 3, No. 2, pp. 47-47).

Nurse, J. R. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. *arXiv preprint arXiv:1811.06624*.

Mosteanu, N. R. (2020). Artificial Intelligence and Cyber Security–A Shield against Cyberattack as a Risk Business Management Tool–Case of European Countries. *Quality-Access to Success*, *21*(175).

Mohamed Mizan, N. S., Ma'arif, M. Y., Mohd Satar, N. S., & Shahar, S. M. (2019). CNDS-cybersecurity: issues and challenges in ASEAN countries. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(1.4).

Nirmal, K., Janet, B., & Kumar, R. (2021). Analyzing and eliminating phishing threats in IoT, network and other Web applications using iterative intersection. *Peer-to-Peer Networking and Applications*, *14*, 2327-2339.

Pogrebna, G., Skilton, M., Pogrebna, G., & Skilton, M. (2019). Cybersecurity threats: Past and present. *Navigating New Cyber Risks: How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age*, 13-29.

Saha, S., Das, A., Kumar, A., Biswas, D., & Saha, S. (2020). Ethical hacking: redefining security in information system. In *Proceedings of International Ethical Hacking Conference 2019: eHaCON 2019, Kolkata, India* (pp. 203-218). Springer Singapore.

Sen, R., Verma, A., & Heim, G. R. (2020). Impact of cyberattacks by malicious hackers on the competition in software markets. *Journal of Management Information Systems*, *37*(1), 191-216.

Shukla, V., Deshmukh, A., & Tyagi, A. K. (2022). Role of Artificial Intelligence in Cyber Security: A Useful Overview. In *Information Security Practices for the Internet of Things, 5G, and Next-Generation Wireless Networks* (pp. 92-104). IGI Global.

Stiawan, D., Idris, M., Malik, R. F., Nurmaini, S., Alsharif, N., & Budiarto, R. (2019). Investigating brute force attack patterns in IoT network. *Journal of Electrical and Computer Engineering*, *2019*.

Sheikh, A. (2021). Enumeration. In *Certified Ethical Hacker (CEH) Preparation Guide: Lesson-Based Review of Ethical Hacking and Penetration Testing* (pp. 27-34). Berkeley, CA: Apress.

Švábenský, V., Vykopal, J., & Čeleda, P. (2020, February). What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences. In *Proceedings of the 51st ACM technical symposium on computer science education* (pp. 2-8).

Toh, J., Hatib, M., Porzecanski, O., & Elovici, Y. (2017, April). Cyber security patrol: detecting fake and vulnerable wifi-enabled printers. In *Proceedings of the Symposium on Applied Computing* (pp. 535-542).

Tariq, I., Sindhu, M. A., Abbasi, R. A., Khattak, A. S., Maqbool, O., & Siddiqui, G. F. (2021). Resolving cross-site scripting attacks through genetic algorithm and reinforcement learning. *Expert Systems with Applications*, *168*, 114386.

Etuh, E., & Bakpo, F. S. (2022). Social Media Networks Attacks and their Preventive Mechanisms: A Review. *arXiv preprint arXiv:2201.03330*.

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). A survey on ethical hacking: issues and challenges. *arXiv preprint arXiv:2103.15072*.

Zhenfang, Z. H. U. (2015). Study on computer trojan horse virus and its prevention. *International Journal of Engineering and Applied Sciences*, *2*(8), 257840