ETHICAL HACKING INNOVATIONS FOR MITIGATING CYBERSECURITY THREATS

[1]Joy Ebere Ezeife & [2]Victoria Okoma Nwabiarani

[1]ezeifejoy@gmail.com, Federal Polytechnic Oko, +2348061126745

[2]divinevictory77@yahoo.co.uk, Federal Polytechnic Oko, +2348064789269

Abstract

In this generation where there is a high degree of cybercrime and many fraudulent activities, the importance of cybersecurity cannot be overemphasized. As days go by, these cybercriminals continue to device highly sophisticated tools with which they invade the infrastructure of organizations causing much havoc. As a proactive measure, organizations are adopting the expertise of ethical hackers to protect their sensitive digital assets. Ethical hacking, also known as penetration testing, is a very crucial tool in the cybersecurity domain, allowing experts in the hacking field to identify and address potential threats and possible vulnerabilities in order to prevent the exploitation of cybercriminals.

Keywords: Cybersecurity, ethical hacking, security, penetration testing and cyber-crime.

Introduction

Ethical hacking, also called penetration test, pen test is a cybersecurity technique that is employed by organizations in identifying, testing and highlighting vulnerabilities in the security of their systems. These penetration tests are often done by professionals in the cybersecurity world known as ethical hackers.

One feature of ethical hacking is that it involves the controlled and authorized simulation of cyber-attacks on networks, systems, or applications to uncover vulnerabilities or weaknesses. Ethical hackers operate within legal and ethical boundaries, aiming to enhance the overall security posture of an organization, unlike malicious hackers. This proactive approach enables companies to stay one step ahead of potential threats, mitigating risks and minimizing the impact of cyber-attacks

(Naveen, 2024). Hacking is also seen as infiltration since it is a typical method for breaching confidential and personal information. Ethical hackers are people and members of an organization who carries out ethical hacking and are paid in several ways from the organization or employers for going into a system or network to test and expose the possible vulnerabilities in the network, find out and repair other loop holes. Hence, the type of intrusions arising from ethical hacking are not seen as cyber theft because their aim is to improve the security status of the organization, thereby improving their efficiency.

Since most of the things about our lives are done digitally, there is a great need to shield our private data from the risk of cyber-attack from malicious hackers. Such hackers called 'black hat' hackers use various methodologies, approaches and tools to test networks and systems since they do not have any knowledge of the system. This paper discusses the work of ethical hackers in helping to protect organizations from the incessant menace posed by cybercriminals. It discussed the effects of malicious attacks on organizational or individual systems, the phases of ethical hacking, its components and the tools used in carrying out ethical hacking. It also examines and highlights the benefits or importance of ethical hacking in organizations and the challenges associated with it.

The proactive work done by ethical hackers helps to improve an organization's security posture. They often obtain approvals beforehand from the organization making their goal quite an opposite of that of the general malicious hackers. Ethical hackers can also carry out assessments of the security state of the system in form of 'white hats', where they are given much knowledge of the nature of the system.

Kamal *et al.*, (2023) note that a cyberattack disrupts the continuity of a business by damaging the reputation or obtaining their intellectual property, thus it can destroy the physical infrastructure, services and logical connectivity of a victim as also noted by UVM (2022). According to Dimitar

(2015), physical assets and secret information can be stolen by hackers. These kinds of information can be utilized for political agenda or religious propagation as observed by Alzoubi (2021). Hacking can also be as a result of individual interests: desire for ransom money, ability to show hacking skills (especially in young people), or receiving earnings by exposing sensitive information to a third party (Kamal *et al*., 2023).

The main goal of ethical hacking is to assess the target system's security, system infrastructure, or network and identify the weaknesses. The aim of this process is to discover and exploit the network vulnerability and determine whether unauthorized persons can have access to it or whether there are other malicious activities going on. Phishing is the most common of all hacking technique and due to the fact that there is a great increase in the number of attack, it is necessary for people to understand the concepts of ethical hacking to keep themselves secured (Sonali *et al.,* 2017).

The Goal of Ethical Hacking

Hafiz *et al.,* (2022) notes the ethical hackers and 'black hat' hackers use the same methods except that network administrator privileges are obtained by ethical hackers. The 'black hat' hackers however, do not obtain any permissions and they do not make the methods they use open neither do they report the vulnerabilities found. They aren't concerned with improving the organizations security posture. Knowing that the world is fully digitized, including our biometrics, we should be vigilant since hackers can steal these sensitive information and cause several kinds of damage. Great amount of money are paid by several companies to ethical hackers while they also lose great amount of money yearly even after the payments to different forms of hacking attacks (Nagadeepa *et al.,* 2019).

The explosive growth of the Internet has brought many good things such as electronic commerce, collaborative computing, ease of access to a large amount of reference material, new avenues for

information distribution, advertising and e-mail. There exists a dark side of criminal hacking also just like majority of technological advances. This is where the services of ethical hackers are highly needed. Palmer (2001) states that around the world, private citizens, companies and governments are highly interested in taking part in this technological revolution. However, they are afraid having these miscreants invade their servers in the network, having access to their mails, invading their online e-commerce sites and stealing their credit card number, replacing their logos with all kinds of pornography. These criminals can even implant software which can be programmed to make the organization's secret information open or accessible to the general internet.

One of the major goals of an ethical hacker is to report discovered vulnerabilities to an organization. They additionally provide the organization advice on how to correct the anomalies. Severally, they can also carry-out a re-test procedure in order to ensure that the issues have been fully resolved. The ethical hacker does all these with the consent of the organization having a good intention while the malicious hacker intends to gain unauthorized access to the resources of an organization, especially the more sensitive ones. They do these for several reasons such as personal achievement or financial gain. Certain 'black hat' hackers can manipulate websites, use ransomware and crash backend servers. They may do these with the intention of damaging the company's reputation, causing financial loss or just for the fun of it.

In the process of examining the security of an organization's digital assets, the aim of an ethical hacker is to act like an attacker, gathering the attack vectors to be launched against the victim. Their goal is to understand the system fully, obtain information as much as they can and prepare a comprehensive report after the testing period.

The enormous information gathered by the ethical hacker is used for finding the weaknesses existing in the system or asset. These assessments are performed while combining manual and

automated testing. Ethical hacking is needed in all kinds of systems no matter how sophisticated they are since the success of a critical cyber-attack can reduce it to nothing.

Kamal *et al.*, (2023) pointed out that ethical hackers do not stop at revealing vulnerabilities. They use the informative report obtained to prove how a malicious hacker could exploit the system. This knowledge exhibited by ethical hackers help to improve and secure the technology of an organization.

Effects of malicious attack

Cyber-attack is high. Hence, in order to avoid endangering the organization's infrastructure. An attack causes economic losses by deducting the number of customers (Schwartz, 2011; Lee, 2015). An attack compromises reputations and adds extra fixing expenditures (The Huffington, 2024). Post disturbing general growth and increasing stakeholders' frustration or anxiety (Ashley, 2022; McDaid, 2022). Ethical hackers are employed to discover vulnerabilities such as: misconfigured security, the use of components with known vulnerabilities, injection attacks, sensitive data exposure and broken authentication.

Phases of ethical hacking/penetration testing

a. Reconnaissance: This is where hackers gather as much information as possible from private and public sources to outline the target's attack surface and possible loopholes.
b. Scanning. Examine the target system or platform for weaknesses in various aspects such as application security issues, open services and open other vulnerabilities.
c. Gain access. Select the best tools and methods to gain access to the system. This may be through a weakness, such as SQL injection, malware, social engineering or any other means.

d. Maintain access. Stay connected long enough to demonstrate the potential impact of a breach, such as exfiltration or modifying data.

Components of Ethical Hacking

Authorization and Legal Compliance: Ethical hacking starts with obtaining official permission from the organization or system owner. This is to ensure that the testing is carried out within legal and ethical frameworks, in order to prevent any unintended legal consequences. It is necessary to adhere to relevant laws, regulations, and industry standards is paramount throughout the process.

Scoping and Planning: It is crucial to define the scope of the ethical hacking engagement. Establishing clear boundaries helps to avoid disrupting critical systems unintentionally. Identifying the assets to be tested, the testing methods to be employed, and the overall goals of the assessment are all involved in planning.

Methodology: A range of tools and techniques are used to simulate potential cyber threats. These are: vulnerability assessment, network scanning, social engineering and penetration testing. These methods are aimed at mimicking real-world attack scenarios and identifying vulnerabilities which could be exploited by cyber attackers.

Documentation and Reporting: Ethical hackers carefully document their findings throughout the testing process. They generate a comprehensive report that details the weaknesses discovered, the methods used, and documents their recommendations The documentation provides a very important resource for organizations to prioritize and address security issues.

Types of Pen Testing

There are three main pen testing strategies, each offering pen testers a certain level of information they need to carry out their attack.

White box testing: This provides the testers with all the details about an organization's system or target network and checks the code and internal structure of the product being tested. White box testing is also known as open glass, clear box, transparent or code-based testing.

Black box testing: This is a type of behavioral and functional testing where testers are not given any knowledge of the system. Normally, organizations hire ethical hackers for black box testing where a real-world attack is carried out to get an idea of the system's vulnerabilities.

Gray box testing: This is a combination of white box and black box testing techniques. It provides testers with partial knowledge of the system. Such knowledge can be low-level credentials, logical flow charts and network maps. Gray box testing is basically used to find potential code and functionality issues.

Ethical Hacking (Penetration Testing) Tools

Hacking tools are software, computer programs or a complex type of script designed by the developers that are used by hackers to know the weaknesses in computer operating system, various web applications as well as servers and networks. Several employers, especially in the financial institutions use ethical hacking tools to secure their data from attackers. Hacking tools are available either in commercial solutions or in open source form such as freeware v. sor shareware.

These tools are used by security professionals especially to get access to computer systems in order to access the vulnerabilities in computer systems so that their security will improve. Professionals in the security field use hacking tools such as packet sniffers to intercept the network traffic, password crackers to discover the passwords and port scanners to identify open ports on computers.

Some of the most famous hacking tools in the market are Nmap (Network Mapper), Nessus, Nikto, Kismet, NetStumbler, Acunetix, Netsparker, and Intruder, Kismet, Fortify WebInspect, Cain & Abel, Nmap, Nessus, Invicti, Metasploit and Aircrack-Ng.

Benefits of Ethical Hacking

Kinza (2023) notes that during the test-run of a cyber-attack, a penetration test or ethical hacking process provides insights into the most vulnerable aspects of a system. It also serves as a mitigation technique, enabling organizations to close the identified loopholes before threat actors get to them.

The following are four reasons organizations should conduct pen testing (Kinza, 2023).

Risk assessment: The rate at which distributed Denial of Service, phishing and ransomware attacks is rapidly increasing is alarming. It puts most companies at risk. The effects of a successful cyber-attack continues to increase and calls for concern. A ransomware attack, for instance, could block a company from accessing the data, devices, networks and servers it relies on to carryout business. Such an attack could result in millions of dollars of lost revenue. Pen testing uses the hacker perspective to identify and mitigate cybersecurity risks before they're exploited. This helps IT leaders perform informed security upgrades that minimize the possibility of successful attacks.

Security Awareness: As technology continues to evolve, so do the methods cybercriminals use. For companies to successfully protect themselves and their assets from these attacks, they need to

be able to update their security measures at the same rate. The caveat, however, is that it's often difficult to know which methods cybercriminals are using and how they might be used in an attack. But by using skilled ethical hackers, organizations can quickly and effectively identify, update and replace the parts of their systems that are particularly susceptible to modern hacking techniques.

Reputation: A data breach can put a company's reputation at stake, especially if it goes public. Clients or customers can lose confidence in the business and stop purchasing their, while investors might be hesitant to invest in a business that doesn't take its cyber defense seriously. Penetration testing protects the reputation of a business by offering proactive mitigation approaches.

Compliance: Industries, including healthcare, banking and service providers, take compliance and regulation seriously and include ethical hacking as part of their compliance efforts. Common regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), require pen tests to be compliant. Therefore, by performing regularly scheduled pen testing, organizations can stay on top of their compliance needs and be more efficient.

Proactive Risk Management: Ethical hacking allows organizations to identify and address vulnerabilities before they can be exploited by malicious actors. This proactive approach enhances overall risk management strategies and helps prevent potential data breaches or cyber-attacks.[9]

Cost-Effective Security Measures: It is better to invest in ethical hacking since it is more cost-effective than handling the effects of a cyber-attack. It helps to identify and mitigate weaknesses in advance. This helps organizations to save their reputation and the financial expenses associated with successful data attacks.

Continuous Improvement: Ethical hacking is not an activity done once. There should be regular assessments and testing to ensure that an organization's cybersecurity measures continues to

improve as emerging threats increases. The continuous improvement routine is very important in the field of cybersecurity.

Challenges of Ethical Hacking

Jean-Paul *et al.*, (2021) note the following limitations of ethical hacking (pen testing).

a. **Time**: Here, each test requires a specific amount of time to be performed, especially with no fixed time to finish conducting a given test when dealing with large organizations. In fact, such a process can range from days, and sometimes it can take up to weeks, months, and even years.
b. **Scope**: This is based on the limitation of scope. The scope is limited to the resource, budget and security constraints. This prevents ethical hackers from performing all the intended and required testing.
c. **Method**: The methods in use for pen testing can lead the system to crash. This may cause damage and harm to the system, which is not the aim and intent of conducting ethical hacking.
d. **Skills**: Professional pen testers are limited in terms of certified/licensed members, available skills and manpower, despite that skilled pen testers rely on using a specific technology in their expertise, field and domain.
e. **Restricted Access:** In addition, ethical hackers have a restricted access right to a given targeted environment, due to a given organization's policy wanting to conduct external remote network pen testing. This problem also falls into the domain of experienced ethical hackers to cover all possible aspects in pen testing domain.
f. **Mostly focus on known attacks:** The major drawback of pen testing is based on the pen testers' ability and capability to conduct their pen testing against only already known

attacks and threats. Thus, rendering them unable and useless when it comes to dealing with unknown threats and attacks.

g. **Uniform Thinking:** Another challenge is having a uniform thinking over conducting a given pen testing without thinking outside the box. This prevents them from finding new methods and mechanisms to use. As a result, their tasks are limited, unlike attackers who rely on creating new methods to evade detection and perform their cyber-attacks.

Conclusion

Ethical hacking is a vital component of modern cybersecurity strategies, empowering organizations to stay ahead of cyber threats. By embracing responsible and authorized hacking practices, companies can build resilient defenses, protect sensitive information, and foster a secure digital environment. As technology continues to advance, ethical hacking will remain a stronghold in the ongoing battle against cyber threats, reinforcing the foundations of a robust and secure digital future. Ethical hackers provide an essential service to these organizations by looking for vulnerabilities that can lead to a security breach. Ethical hacking is very crucial because cyber attackers are always active. Nigerian organizations and those in other nations should therefore ensure that they employ their services to ensure the protection of their digital assets.

Recommendations

The following are the recommendations:

1. It is recommended that organizations should employ the services of ethical hackers in order to be proactive and prevent damages to their digital assets.

2. Also, ethical hackers should constantly improve their knowledge of the field of hacking since the tricks of cybercriminals are dynamic.

3. The government should encourage research in the area of cybersecurity to always be ahead of these miscreants.

References

Alzoubi, Y.I.; Al-Ahmad, A.; Jaradat, A. (2021) Fog computing security and privacy issues, open challenges, and block chain solution: An overview. *Int. J. Electr. Comput. Eng.* 11, 5081–5088. [Google Scholar] [CrossRef]

Ashley, M. (2022) Aftermath: Confessions, Suicide Reports and Hot on the Hacker's Trail. National Post. Available online: http://news.nationalpost.com/news/canada/ashley-madison-aftermath-confessions-suicide-reports-and-hot-on-the-hackers-trail Accessed on 11th May, 2024.

Dimitar. K. (2015) Ashley Madison Revisited: Legal, Business and Security Repercussions. Available online: http://resources.infosecinstitute.com/ashley-madison-revisited-legal-business-and-security-repercussions. Accessed on 11th May, 2024.

Hafiz, B., Muhammad, Z. H., & Muhammad, Z., H. (2022) The Impacts of Ethical Hacking and its Security Mechanisms, *Pakistan Journal of Engineering and Technology*, PakJET ISSN 2664-2042, ISSN (e): 2664-2050 5(*4*) : 29- 35.

Jean-Paul A. Yaacoub, H. N., Noura, O. S., & Ali, C. (2021) A Survey on Ethical Hacking: Issues And Challenges 23-24 arXiv:2103.15072v1 https://www.researchgate.net

Kamal, U. S., Farizah, Y. & Aziz, D. (2023) Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods Sustainability 2023, 15(*13*), 10471; https://doi.org/10.3390/su151310471

Kinza, Y. (2023) Pen Testing. Retrieved on 5th May 2023 from https://www.techtarget.com/searchsecurity

Lee, T. (2015) Forget the Ashley Madison or Sony Hacks—A Crippling Cyberattack Is Imminent in the US. The Guardian. Available online: http://www.theguardian.com/technology/2015/jul/26/cybercrime-hacking-internet-of-things-target Accessed on 11th May, 2024.

McDaid, L. (2022) Talktalk Cyber-Attack: County Londonderry Man Targeted. BBC News. Available online: http://www.bbc.co.uk/news/uk-34613921 Accessed on 11th May, 2024.

Nagadeepa, C., Mohan, R. and Singh, A. (2019) "Ethical Hacking: Cyber-Crime Survival in the Digital World," *International Journal of Recent Technology and Engineering (IJRTE)*, 8(*4*) Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP, 10332–10334, doi:10.35940/ijrte.d4612.118419

Naveen Kumar. P. Exploring the World of Ethical Hacking: Enhancing Cybersecurity through Responsible Practices, Retrieved on Feb 16, 2024 from https://www.linkedin.com

Palmer. C.C. (2001) Ethical Hacking. *IBM Systems. Journal* 40(*3*).

Schwartz, M. J. (2011) Dark Reading. Sony Data Breach Cleanup to Cost $171 Million. Available online: http://www.darkreading.com/attacks-and-breaches/sony-data-breach-cleanupto-cost-\$171-million/d/d-id/1097898 Accessed on 11th May, 2024.

Simplilearn (2024) 35 Ethical Hacking Tools and Software for IT Professionals retrieved on 19th May, 2024 from https://www.simplilearn.com/top-5-ethical-hacking-tools-rar313-article

Sonali Patil; Ankur Jangra; Mandar Bhale; Akshay Raina; Pratik Kulkarni (2017) Ethical hacking: The need for cyber security, *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)* 21-22 September

The Huffington Post (2024). A Look Back at the Target Breach. Available online: http://www.huffingtonpost.com/eric-dezenhall/a-look-back-at-the-target_b_7000816.html

University of Vermont (UVM) (2022). Enterprise Risk Management Program: Guide to Risk Assessment & Response. Available online: https://www.uvm.edu/sites/default/files/Enterprise-Risk-Management/POSTED_Prog_Primer_Trustee_Orientation.pdf Accessed on 11th May, 2024.