International Journal of Core Engineering & Management

Volume-6, Issue-7, 2020 ISSN No: 2348-9510

ETHICAL HACKING AND PENETRATION TESTING: ANALYZING THE ROLE OF ETHICAL HACKING AND PENETRATION TESTING IN IDENTIFYING VULNERABILITIES AND IMPROVING OVERALL CYBERSECURITY DEFENSES

Sri kanth Mandru
Mandrusrikanth9@gmail.com

Abstract

This paper explores ethical hacking and penetration testing, two practices effective in minimizing vulnerabilities and keeping the network safe from threats in the era of modern cybersecurity. Penetration testing includes assessing the security features by simulating hacker attacks, whereas ethical hacking allows the hacker to try to penetrate the system. This paper focuses on their beginning, functioning, and influence on the strategy for cyberspace protection. The research discusses the relevance of identifying key results in furthering risk management and compliance and developing the security mindset. To intensify, these factors should be underlined as focal to counter emergent threats and sustain the right degree of organizational cybersecurity readiness by outlining their importance and goals for future studies.

Keywords: Ethical hacking, Penetration testing Cybersecurity, Vulnerability assessment, Network security

I. INTRODUCTION

Organizations face increased concern in cyberspace, with distinct forms of ethical hacking being preventative measures or offenses that protect sensitive data and infrastructure. Ethical hacking is when individuals can penetrate a system or a network to search for weaknesses. The rationale for penetration testing is to assess the current security frameworks because the environment emulates actual attacks. Both are important when used to detect security weaknesses in a system before naughty people exploit them [1]. Ethical hacking and penetration testing gradually appeared as a practice despite computers being available much earlier, and security breaches were due to relatively simple and mundane methods. These processes eventually led to systematic processes of evaluating and fortifying security postures because of new and emerging cyber threats.

International Journal of Core Engineering & Management

Volume-6, Issue-7, 2020 ISSN No: 2348-9510

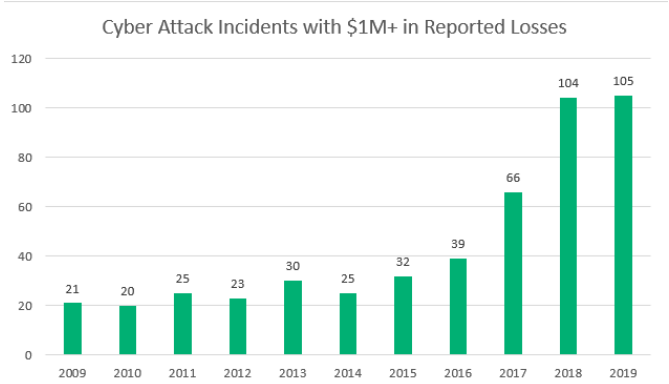

Figure 1: Increase in cyberattacks between 2009-2019

Ethical hacking and penetration testing are crucial in this generation due to the emergence of waves and complex attacks. Thus, this research aims to find out how these factors could improve strategies related to incident response tactics, security policy, and vulnerability identification [2]. This research seeks to expose them to their present and relevant status in the sphere of cybersecurity by investigating their background, working process, and possible applications.

II. PROBLEM STATEMENT

As the world becomes more connected through technology, one can agree that cyber-attack risks are constantly rising, and attacks are continually evolving.

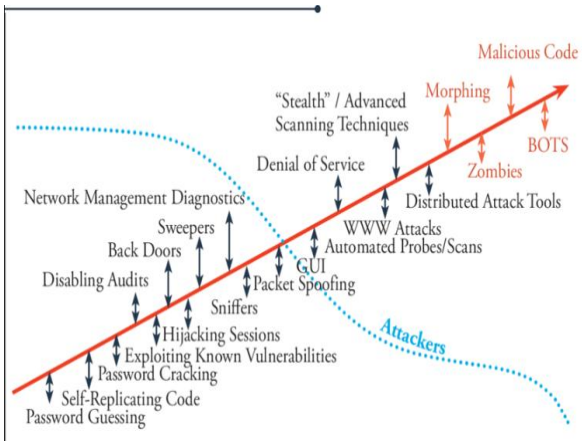

Figure 2: Sophistication of cyber threats

From the basic and mundane, like malware and phishing, to significantly more advanced threats, like zero-day threats and ransomware, organizations have to dive headfirst into every day. Improved threats and attacks have led to the advanced development of new

International Journal of Core Engineering & Management

Volume-6, Issue-7, 2020 ISSN No: 2348-9510

threats and attacks, and traditional security solutions such as firewalls, viruses, and intrusion detection systems have become ineffective [2]. Unfortunately, most of these static defences are generally reasonably defensive. They can only come into play once attackers have gained entry to a network, which is financially damaging and leads to data leakages. It becomes an issue when we have to come to realize that there are adverse effects associated with the classical security approaches, as conventional cybersecurity is indicating. Comparing ethical hacking and penetration testing, it can be said that both are techniques employed systematically to find the gaps in security and sort them out before the wrong individuals utilize them. These procedures involve realistic attack simulations; thus, they facilitate the uncovering and identifying weaknesses that actual attacks might not reveal and, in the process, enhance the formulation of effective protective mechanisms.

However, it is worthwhile to point out that Penetration testing and Ethical hacking are two different terms, meaning two different things pertain to two distinct classes. Ethical hacking, as yet another effective tool, also consists of other processes, including vulnerability assessment, security audit, and compliance audit, all to improve security measures [3]. However, in its broad definition, penetration testing is a kind of ethical hacking, and the principal purpose of this type of work is to find weaker spots in an organization's system using an imitation of an attack.

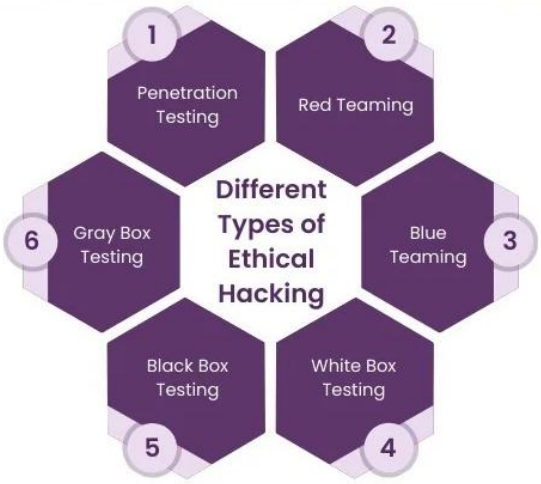

Figure 3: Types of Ethical Hacking

There are distinct types of ethical hackers. For example, a classification of people in computer security is a white hat, grey hat, and black hat. While the 'black-hat hackers' have the intention of achieving a specific aim or benefit within the process of hacking, the 'white hat hackers' are formally trained hackers whose primary purpose is to show a particular company or organization a loophole in the security of that company or organization, to make it better. The grey hat hackers are unlike the black hat hackers because they do not want to harm anyone with their hacking but find a weakness in the system and misuse it unlawfully. However, some evil hackers commit crimes that violate other people or

individuals [4]. Ethical hacking and penetration testing employ procedures and processes that do not look like they were chosen haphazardly but rather sequential or consecutive. Such basic security measures are still less arbitrary and more effective to some extent due to OWASP, NIST, and the system, which includes checklists for the identification of risks and risk evaluation and control.

III. SOLUTION: ETHICAL HACKING AND PENETRATION TESTING

A. Audit and Compliance Issues

Manually entered journals may lack detailed documentation or audit trails, making it difficult to track changes and ensure compliance. Errors or omissions in journal entries can lead to non-compliance with regulatory requirements and financial reporting standards.

B. Delayed Financial Insights

Delays in entering and reconciling journal entries result in slower availability of financial data for analysis and decision-making. The timeliness and accuracy of financial reports are compromised, affecting stakeholders who rely on these reports for strategic decisions. The timeliness and accuracy of financial reports are compromised, affecting stakeholders who rely on these reports for strategic decisions.

IV. ANALYSIS ON THE MANUAL JOURNAL DATA AND THE APPROACH

Penetration testing and ethical hacking form a coherent set of strategies for analyzing the efficiency of the cybersecurity system. Proactive preparation, Reconnaissance, Assault, and Reporting are the four special categories that form the standard Penetration testing model [5].

A. Planning

During this stage, the objectives of penetration testing and the limits of such tests are identified. To address the issue, several actions must be taken to make the test legal and ethical: gathering information on the target system, identifying potential entry points, and outlining rules for penetration [6].

B. Discovery

At this stage, ethical hackers identify background information as close as possible to the targeted subject through reconnaissance. Understanding the system's structure and deeply analyzing its flaws includes activities such as fingerprinting, identifying services (for instance, by using the Nmap), and mapping the network.

International Journal of Core Engineering & Management

Volume-6, Issue-7, 2020 ISSN No: 2348-9510

C. Attack

The attacker utilizes different tools and techniques in the attack phase to exploit the identified weaknesses. For instance, the Metasploit framework enables this process to be very effective in planning attacks, while other tools, such as the burp suite, make it easier and faster to find problems like SQL insertions and cross-site scripting (XSS).

D. Reporting

This comprehensive report is prepared after the assault phase has been completed. It also includes assessments of the discovered weaknesses and implications for attacking them, along with recommendations on improving security measures [7]. Another benefit of the report is that it facilitates the identification of critical measures that should be taken to eliminate various risks.

E. Tools and Techniques

Ethical hackers use varied tools and methods during penetration tests for particular tasks. Tools that may investigate some breached possibilities include forensic analysis tools like EnCase, password cracking tools like John the Ripper, and network scanners like Nessus.

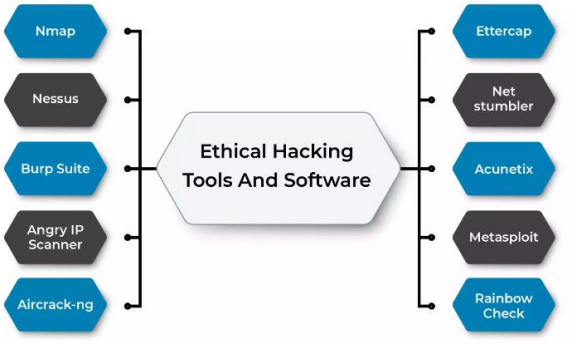

Figure 4: Ethical hacking tools and software

F. Legal and Ethical Considerations

Although entities concerned provide their consent to ethical hackers to operate their data, such hackers must strictly conform to the laws and obligations set in the Computer Fraud and Abuse Act in the United States and those given by Offensive Security and EC-Council. As such, day-to-day operations may not be affected, and privacy laws can be complied with while ensuring no system is compromised by testing [7]. Ethical hacking and penetration testing are thus of immense importance when preventing actual hackers from exploiting

International Journal of Core Engineering & Management

Volume-6, Issue-7, 2020 ISSN No: 2348-9510

known vulnerabilities. They offer organizations unique insights into improving the security state of their systems in this hostile environment.

Other level continuous testing procedures have also been initiated, which are also revolutionizing cybersecurity protection approaches. Continuous testing differs from a normal schedule of occasional testing of security measures since it offers a chance to trace their implementation in real-life situations. Unlike the conventional procedure, this approach also improves the rate of identifying flaws and guarantees that adequate security measures exist to address current emerging risks. With the help of automated solutions and feeds, organizations can ensure that the mentioned misconceptions do not evolve into major threats. Third, knowledge in reacting to incidents and the improvement of catastrophe recovery plans contribute to corporate security; ethical hacking, penetration testing, and employing white hackers are highly advantageous. Some of the advantages might include the amplification of the response to incantations and lessening the consequences of any attacks that these techniques do other than revealing susceptibilities. This is a proactive strategy that gives managing organizations a chance to be better prepared in dealing with cyber threats and to have them have fewer chances for downtimes.

Another relatively recent proactive technique is red teaming operations, whereby a firm hires hackers who practice ethics in hacking and pretend to attack the organization so that the firm knows how secure it is. The most valuable aspect that distinguishes the red teaming approach from other testing frameworks is that social engineering and organizational reaction are inherent parts of the testing models.

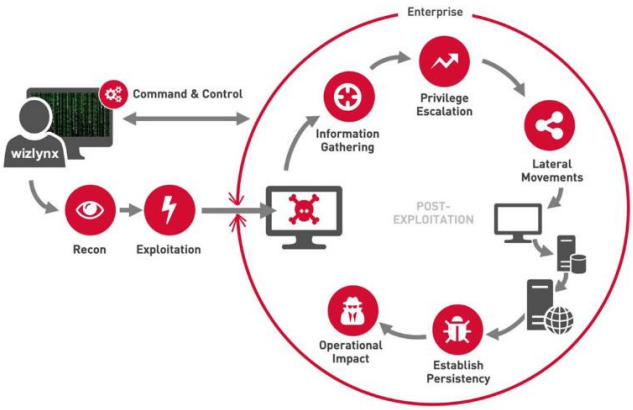

Figure 5: Red teaming operations

A plethora of other simpler forms of checklists, assessments, or methodologies could easily overlook hidden issues or weak points with an organization's incident response strategy; this one will not. In addition, in industries where the issues of personal data protection are especially relevant, ethical hackers and pen testers are the main drivers in enhancing their own compliance programs. A number of useful benefits of performing compliance assessments consist of the following: being able to ascertain that an

International Journal of Core Engineering & Management

Volume-6, Issue-7, 2020 ISSN No: 2348-9510

organization adheres to legal and industry standards like GDPR, HIPAA, or PCI-DSS and proving that security measures are sufficiently in place. Not only that, but these standards contribute to minimizing the risks of violation of the law or getting into problems with it. They also strengthen the believability of consumers to the organization and its capacity to store and protect sensitive information securely.

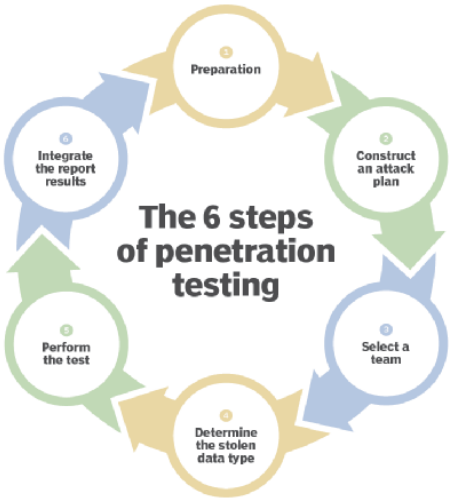

Figure 6: Steps of Penetration Testing

V. USES OF ETHICAL HACKING AND PENETRATION TESTING

As mentioned above, penetration testing and ethical hacking are two related services, and each serves a crucial purpose in improving IT security. These methods can help reveal the lack of security systems, applications, and network support structures. In this way, the honest hacker might come across some glitches that some bad fellas might use with the intention of, in essence, attacking the system [8]. It is thus helpful in managing the risks posed by cyber criminals insofar as businesses apply patches to their systems' flaws before exploiting them. Moreover, the current security policies and programs implemented in the enterprise can also be evaluated by penetration testing and ethical hacking. Security specialists may determine that the applied safeguarding measures are adequate for repelling most generic cyber threats and sufficiently cover all the applicable rules and regulations for the specific context and the fields of business activity indicated [9]. This assessment supports security measures and reveals portions that likely require fine-tuning the set measures.

However, these approaches make disaster recovery and incident response solutions better and in ways that are pretty amazing. Mitigation organizations can conduct rehearsals to test their preparedness to detect and manage a cyber attack and perform reparation exercises such as ethical hacking and penetration testing [10]. With such consideration, companies can blunt the effect of whoever is fomenting the breaches and keep with the operation. Ethical hacking and penetration testing are not merely conceptual tools since these have vast advantages in real-life situations, as evident in the case scenarios and implementation

International Journal of Core Engineering & Management

Volume-6, Issue-7, 2020 ISSN No: 2348-9510

throughout 2016- 2019 [11]. This is evident from police and other emergencies, financial institutions, health facilities, and government institutions, especially after the routine testing began to be implemented. The above examples should demonstrate how ethical hacking may contribute towards preventing future threats in cyberspace and thereby reduce the amount of adverse effects that can be coped with from invasions of data privacy.

VI. IMPACT OF ETHICAL HACKING AND PENETRATION TESTING

Altogether, ethical hacking and penetration testing benefit companies in terms of quality and amount. Therefore, they supplement and strengthen the risk assessment and reduction methods regarding the amount [12]. It would enable corporations to avoid costly security and risk assessment exercises by identifying the insecure areas within an organization and guaranteeing they are secure.

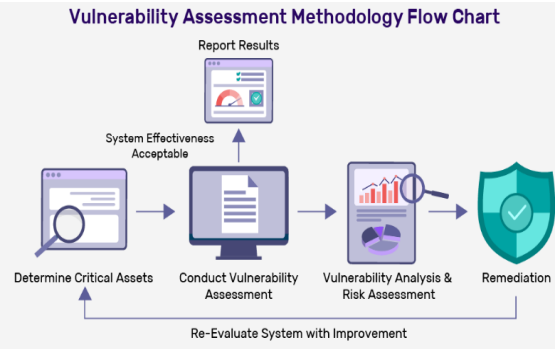

Figure 7: Vulnerability assessment types

It enhances the operations process and convinces the customers without yielding their details. Ethical hacking and penetration testing offer excellent value in building compliance with challenging rules and regulation systems like GDPR, HIPAA, and PCI-DSS by organizations. They ensure that systems and procedures are legal, thus eliminating penalties and loss of reputation that may result from being legal [12]. Moreover, it supplements the legislation and guidelines on data protection and ethical business actions for organizations.
While legal requirements cover ethical hacking and penetration testing, the culture is positively impacted as most stakeholders and company employees become more aware of vulnerabilities and risks. These help to actively engage the protective security process since they mimic attacks and assess potential risks. This increases security awareness and safety procedures among the employees while enhancing the cohesive defence.

International Journal of Core Engineering & Management

Volume-6, Issue-7, 2020 ISSN No: 2348-9510

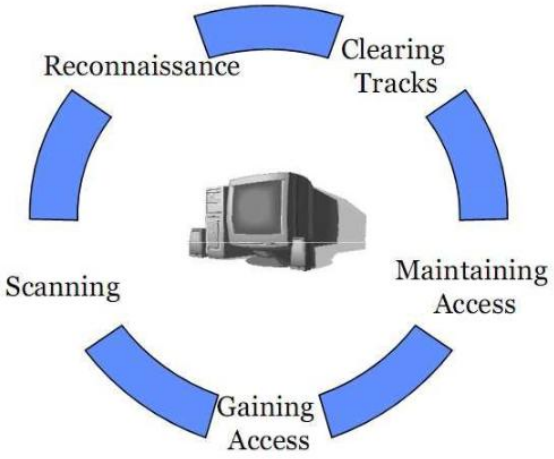

Figure 8: Ethical Hacking and Cybersecurity

Therefore, ethical hacking and penetration testing affect resource deployment and strategic decisions in firms, apart from having an influence on risk management and compliance regulation. Such approaches help stakeholders put in place enough financial capacity to address cybersecurity necessities since they encompass specific threat data and vulnerability sweeps. With this kind of strategic thinking a few years down the road, maybe businesses could begin to think about where they might get the most bang for their buck, perhaps investing in the best-defended infrastructure, fortifying their networks and defences, or getting training for their people more efficiently.

VII. SCOPE AND FUTURE DIRECTIONS

In the cybersecurity industry, penetration testing and ethical hacking are continuous apprenticeships because they are shift workers to respond to new threats and facets of technology. In the given list, these are tendencies and directions, opportunities for further research and development of these professions, and threats. AI-Driven Testing: Adapting methodologies with machine learning and artificial intelligence tools can revolutionize penetration testing and ethical hacking [14]. AI may also augment testing capacity by automating vulnerabilities, a heuristic search of large data sets for signs of an attack, or AI mimicking a hostile, highly advanced cyber threat. While in the past, testing frameworks were offered in periodic forms only; they are provided free and continuous in the present. By such a method, although proactively endeavouring to scrutinize and assess security positions, it might be relatively more straightforward for a business to address threats as much as they are [13]. In this way, they help address new threats as they occur should safety checks be integrated conventionally.

International Journal of Core Engineering & Management

Volume-6, Issue-7, 2020 ISSN No: 2348-9510

A. Integration with Other Cybersecurity Practices

In the past few years, there has been a rising trend of integrating threat intelligence analysis and the SIEM function with ethical hacking and pen-testing. Threat intelligence simulation of ethical hacking illustrates the general improvement of threat identification, response, and management by integrating threat intelligence feeds and SIEM.

B. Challenges and Limitations

When done correctly, ethical hacking and penetration tests is time-consuming, expensive, and requires costly equipment. One of the classic problems many companies face is providing adequate funds to support comprehensive testing programs. Ethical hackers and penetration testers are constantly faced with emerging cyber threats [14]. Therefore, it can be stated that testing approaches and methods must be continually adapted due to ever-evolving threats such as new attack vectors, zero-day exploitation, and advanced malware.

C. Future Research Opportunities

Due to the fact that new technologies are being developed now and then and there are always new threats in the cyber world, there is still great potential for future work in ethical hacking and penetration testing to improve and develop better methods in cybersecurity. Looking at the various ethical hacking and penetration frameworks, it is interesting to point out that AI and ML actually appear to be the subjects that need more research than all the others. There is likely to be a DTP that could be achieved with the use of the technologies developed with the application of artificial intelligence, which might help predict threats and act on them without reporting back to humans. Pursuit of a more intelligent algorithm that can find relatively minor infringements and estimate that routes should improve the reliability and speed of subsequent vulnerability assessment. Therefore, perhaps one should invest some measure of effort and timing in reading up on how behavioural analytics is used in ethical hacking further to get more information on what might be considered to be interesting or qualitative about insider threats and enormous use behaviours [15]. It asked whether threat intelligence platforms may be used to improve ethical hacking techniques, and its answer was that there may be other threats that one could detect in the initial phase, not to mention countermeasures that could be planned.

D. Cloud Computing and IoT Security

In the modern world, the usage of technology such as cloud computing and IoT devices is common & thus, an existing need for specific and specialized ethical hacking/penetration testing frameworks for these technologies. For further research, it may be useful to analyse possible criteria for assessing the security of cloud environments, server less architectures, and IoT networks.

International Journal of Core Engineering & Management

Volume-6, Issue-7, 2020 ISSN No: 2348-9510

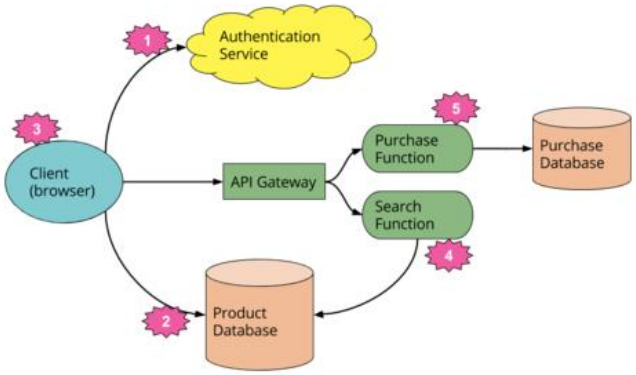

Figure 9: Serverless Architecture

One of the mentioned fields of coverage is the presence of new and unidentified attack vectors, such as APIs or containerization. This is an indication of the need to have better strategies that would assist in reducing such risks.

E. Red Teaming and Organizational Resilience

Further studies on the techniques used in red teaming exercises can offer increased richness into how organizations may enhance their preparedness for current and future cyber threats. Subsequent qualitative investigations can expand on the notions of red teaming, including additional systematic evaluations of specifically technical elements and other subsequent human factors and organizational results. Another use case can be the assessment of the positive or negative influence that red team activities will bring to the general readiness of the organization in terms of managing a particular event or a crisis and making strategic decisions. Hence, a need to conduct more research work, as this eventually brings out the legal and ethical issues surrounding ethical hacking and penetration testing [17]. Future research can be devoted to the determination of universally recognized ethical norms that may be adopted in any state, to the analysis of outcomes of legal measures for new cyber threats, and also to comparisons of visions of members of the international community on principles of Cs legislation and regulation. The inclusion of these future research opportunities will go a long way in helping cybersecurity improve ethical hacking and penetration testing. It will be useful for augmenting the protection of an organization and for sustaining a strong cybersecurity environment in a global environment that remains aggressively challenging.

VIII. CONCLUSION

Building impenetrable cybersecurity structures with threats are constantly emerging is impossible.

- Ethical hacking and penetration testing are inevitable and its use has been described in this article in terms of; application in the first response to an incident, evaluation of security rules, and proactivity in identifying weaknesses.

- These procedures ensure compliance with the regulations and minimize possible risks.
- There is an era to come where a world that is becoming more digital daily offers the best and future protective measures through AI incorporating the testing and enhancing process.
- Ethical hacking and penetration testing will still be relevant in combating data loss, business continuity, and improving organizational security policies when organizations experience more of these for future business prospects.

REFERENCE

1. G. Thomas, O. K. Burmeister, and G. Low, "The Importance of Ethical Conduct by Penetration Testers in the Age of Breach Disclosure Laws.," AJIS. Australasian Journal of Information Systems/AJIS. Australian Journal of Information Systems/Australian Journal of Information Systems, vol. 23, May 2019, doi: 10.3127/ajis.v23i0.1867. Available: https://doi.org/10.3127/ajis.v23i0.1867
2. A. Y. Ding, D. J. G. Limon, and M. Janssen, "Ethical hacking for boosting IoT vulnerability management," Sep. 2019, doi: 10.1145/3357767.3357774. Available: https://doi.org/10.1145/3357767.3357774
3. B. Rafferty, "Dangerous skills gap leaves organisations vulnerable," Network Security, vol. 2016, no. 8, pp. 11–13, Aug. 2016, doi: 10.1016/s1353-4858(16)30077-0. Available: https://doi.org/10.1016/s1353-4858(16)30077-0
4. J. G. Ronquillo, J. E. Winterholler, K. Cwikla, R. Szymanski, and C. Levy, "Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information," JAMIA Open, vol. 1, no. 1, pp. 15–19, Jun. 2018, doi: 10.1093/jamiaopen/ooy019. Available: https://doi.org/10.1093/jamiaopen/ooy019
5. J. M. Hatfield, "Virtuous human hacking: The ethics of social engineering in penetration-testing," Computers & Security, vol. 83, pp. 354–366, Jun. 2019, doi: 10.1016/j.cose.2019.02.012. Available: https://doi.org/10.1016/j.cose.2019.02.012
6. N. T. Cyriac and L. Sadath, "Is Cyber Security Enough- A study on Big Data Security Breaches in Financial Institutions," Nov. 2019, doi: 10.1109/iscon47742.2019.9036294. Available: https://doi.org/10.1109/iscon47742.2019.9036294
7. N. Munaiah, A. Rahman, J. Pelletier, L. Williams, and A. Meneely, "Characterizing Attacker Behavior in a Cybersecurity Penetration Testing Competition," Sep. 2019, doi: 10.1109/esem.2019.8870147. Available: https://doi.org/10.1109/esem.2019.8870147
8. M. C. Ghanem and T. M. Chen, "Reinforcement Learning for Efficient Network Penetration Testing," Information, vol. 11, no. 1, p. 6, Dec. 2019, doi: 10.3390/info11010006. Available: https://doi.org/10.3390/info11010006

9. J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," Computers & Security, vol. 73, pp. 102–113, Mar. 2018, doi: 10.1016/j.cose.2017.10.008. Available: https://doi.org/10.1016/j.cose.2017.10.008
10. Y. Khera, D. Kumar, N. Sujay, and N. Garg, "Analysis and Impact of Vulnerability Assessment and Penetration Testing," Feb. 2019, doi: 10.1109/comitcon.2019.8862224. Available: https://doi.org/10.1109/comitcon.2019.8862224
11. V. Visoottiviseth, P. Akarasiriwong, S. Chaiyasart, and S. Chotivatunyu, "PENTOS: Penetration testing tool for Internet of Thing devices," Nov. 2017, doi: 10.1109/tencon.2017.8228241. Available: https://doi.org/10.1109/tencon.2017.8228241
12. S. Pournouri, S. Zargari, and B. Akhgar, "Predicting the Cyber Attackers; A Comparison of Different Classification Techniques," in Advanced Sciences and Technologies for Security Applications, 2018, pp. 169–181. doi: 10.1007/978-3-319-97181-0_8. Available: https://doi.org/10.1007/978-3-319-97181-0_8
13. R. Upadhyaya and A. Jain, "Cyber ethics and cyber crime: A deep dwelved study into legality, ransomware, underground web and bitcoin wallet," Apr. 2016, doi: 10.1109/ccaa.2016.7813706. Available: https://doi.org/10.1109/ccaa.2016.7813706
14. H. M. Z. A. Shebli and B. D. Beheshti, "A study on penetration testing process and tools," May 2018, doi: 10.1109/lisat.2018.8378035. Available: https://doi.org/10.1109/lisat.2018.8378035
15. S. F. Aboelfotoh and N. A. Hikal, "A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises," JOIV : International Journal on Informatics Visualization, vol. 3, no. 2, pp. 157–176, May 2019, doi: 10.30630/joiv.3.2.239. Available: https://doi.org/10.30630/joiv.3.2.239
16. M. C. Ghanem and T. M. Chen, "Reinforcement Learning for Intelligent Penetration Testing," Oct. 2018, doi: 10.1109/worlds4.2018.8611595. Available: https://doi.org/10.1109/worlds4.2018.8611595
17. M. Brundage et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," arXiv (Cornell University), Jan. 2018, doi: 10.48550/arxiv.1802.07228. Available: https://arxiv.org/abs/1802.07228