DJ

Smith

One question I always had as a cyber security student is what is Ethical Hacking and Penetration Testing. Yeah, I know that I could look it up and see the dictionary version of it, but there is nothing in-depth. As a cybersecurity major those two always come up, if it retains jobs, problems, solutions, etc.

My question wants to dive a little bit deeper and discover what they are. I mean have a description that isn't just a textbook and more of a day in the life as one. I want to have an explanation of the two jobs so that they can explain exactly what they do for people who are not familiar with them. Secondly, have a better understanding of what they do. Thirdly, a better description for less techy people. Lastly, what to expect if you might want to go into these fields of cyber security.

During my research on my first question "How do ethical hacking and penetration testing contribute to strengthening cybersecurity defenses?". I found out that ethical hacking and penetration testing have crucial roles in strengthening cybersecurity defenses by always scanning the system and identifying the vulnerabilities and weaknesses in systems and networks. The practice involves simulating cyber attacks to assess the security posture of an organization's IT infrastructure.

Therefore making sure that it is up to date and working properly, a quick example would be a bouncer checking everyone's ID to get into the establishment with the right

credentials. By adopting the mindset of malicious hackers, ethical hackers can uncover potential entry points and exploit them to assess the system's resilience. Penetration testing goes beyond vulnerability assessment, by trying to attempt to penetrate the network's defenses and gain unauthorized access, providing a more realistic evaluation of security measures.

Through this process of ethical hacking and penetration testing, organizations can identify the problem with their network, prioritize vulnerabilities based on their potential impact, and limit their likelihood of getting exploited. This allows them to address the most critical security flaws that were found and patch them up. The findings from these assessments, allow organizations to implement remediation measures and strengthen their cybersecurity defenses.

Ethical hacking and penetration testing also contribute to improving incident response capabilities by uncovering weaknesses before they are exploited by malicious actors. Organizations will use the insights gained from these assessments to refine their incident response plans and procedures, ensuring a more effective response to security incidents. Making their system harder to get into and preventing hackers from even trying at it, since it would take more time to get into it; therefore lowering the reward and raising the risk of it.

The reason for ethical hacking is to create a culture of continuous improvement and vigilance within organizations, encouraging proactive efforts to identify and minimize security risks. It also promotes a mindset of “security by design,” where security considerations are integrated into every stage of its development. However,

ethical hacking and penetration testing are not just sunshine and rainbows. Organizations must make sure that testing activities do not get in the way of their normal business operations, or accidentally cause harm to systems and data.

Ethical consideration plays a huge role in guiding ethical hacking and penetration testing so it ensures that these activities are conducted responsibly and with integrity. This involves communicating the scope, objectives, and potential risks associated with the testing process. While still respecting the privacy rights and accessing sensitive data, when conducting tests on live systems. Ethical hackers and penetration testers must follow the legal and regulatory frameworks governing data protection and privacy.

Plus being able to minimize harm is a fundamental ethical principle, requiring testers to avoid causing disruptions or damage to systems and networks during testing. Transparency and accountability are also critical in this field because of clear documentation of testing procedures, findings, and recommendations. Testers need to prioritize the interests of the organization and its stakeholders while maintaining professional integrity.

Nevertheless, maintaining confidentiality is crucial to safeguarding sensitive information obtained during testing, ensuring that it is not disclosed or exploited for unauthorized purposes. Therefore, ongoing education and ethical training are essential for ethical hackers and penetration testers to keep evolving their talents while establishing ethical standards in the field.

My last question was, what are the challenges and best practices associated with conducting penetration tests in complex and dynamic environments? What I learned is that conducting penetration tests in complex and dynamic environments presents several challenges and requires the best practices to ensure effectiveness. One challenge that was talked about is the dynamic nature of modern IT infrastructures, which include cloud-based services and interconnected networks, making it challenging to assess the full attack surface accurately.

Another challenge that was addressed is the potential impact of penetration testing on business continuity, especially in environments where systems are interconnected and critical to daily operations, such as train, airport, and metro systems. This is so that they can ensure that the tests are conducted without causing disruptions or downtime requires careful planning and coordination.

Furthermore, maintaining up-to-date criteria amongst the penetration testers is essential, given the rapid pace of technological advancements and emerging threats in today's digital world. Continuous training and professional development are necessary to address these challenges effectively and keep them at bay. Some of the best practices for conducting penetration tests in complex and dynamic environments include doing reconnaissance and scanning to understand the environment and identify potential points of entry for attackers might use to get into the system. Testers should prioritize realistic scenarios and attack vectors that mimic real-world threats, taking into account the specific context and objectives of the organization.

Collaboration and communication between the testing team and stakeholders should take place so they can elaborate on what they have found during the test, this is crucial for ensuring that tests are aligned with business goals and conducted with minimal

disruption. They also need to communicate their testing procedures, findings, and recommendations are essential for facilitating remediation efforts and improving overall security posture. If the tester follows these practices and addresses the associated challenges, the organizations can conduct penetration tests effectively in complex and dynamic environments, while also enhancing their cybersecurity posture and resilience against cyber threats for maximum protection.

Finally I can wrap up my research and give an overview to my question.Overall the information i went over in this research paper i can say that, i have learned what exactly a ethical hacker and penetration tester is. Not only that but what they go through such as challenges they face and have a better understanding of what their job is and what it might entail if I ever go that route in cyber security. Say if I do , I would have to look forward to looking at a system to assess it and look for an entry point. After I find a way in, I would have to clearly report to the organization to whom I found the crack in their system and explain how I did it so their IT team could fix the hole and reinforce said weak spot. Therefore I am glad that I went into more detail about what is an ethical hacker and penetration tester, and the challenges they face in their specific field.

References

Armando, Aobakwe Peddiah. ***Ethical Hacking and Network Security to Prevent Network Cyber Attacks*****. Diss. Botho University, 2019.**

Chow, Emily. "Ethical hacking & penetration testing." ***University of Waterloo, Waterloo, Canada, No. AC*** **626 (2011).**

Al Shebli, Hessa Mohammed Zaher, and Babak D. Beheshti. "A study on penetration testing process and tools." ***2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*****. IEEE, 2018.**

Golightly, Lewis, Victor Chang, and Qianwen Ariel Xu. "Towards Ethical Hacking—The Performance of Hacking a Router." ***Information Security Technologies for Controlling Pandemics*** **(2021): 435-461.**

“61 Stories to Learn about Ethical Hacking.” ***HackerNoon*****, hackernoon.com/61-stories-to-learn-about-ethical-hacking. Accessed 22 Apr. 2024.**

Li, Yang, et al. "An Intelligent Penetration Test Simulation Environment Construction Method Incorporating Social Engineering Factors." Applied Sciences 12.12 (2022): 6186.

Yao, Qian, et al. "Intelligent Penetration Testing in Dynamic Defense Environment." ***Proceedings of the 2022 International Conference on Cyber Security*****. 2022.**