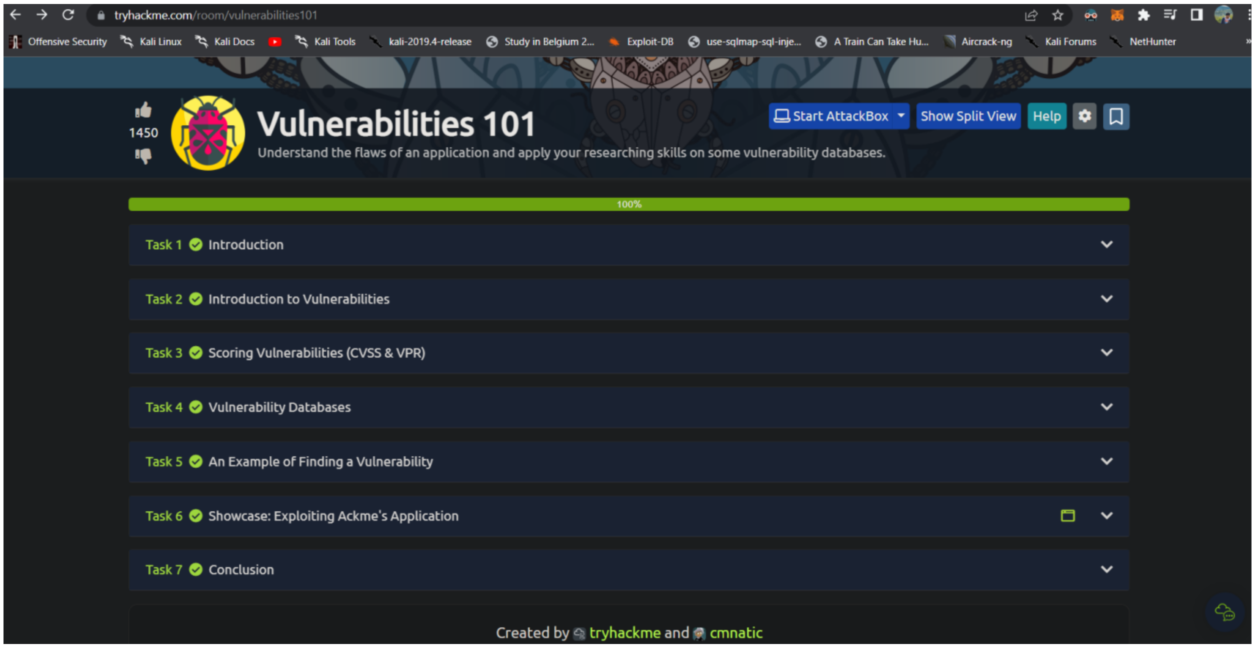

Vulnerabilities 101

Understand the flaws of an application and apply your researching skills on some vulnerability databases.

Task 1 ✓ Introduction

Task 2 ✓ Introduction to Vulnerabilities

Task 3 ✓ Scoring Vulnerabilities (CVSS & VPR)

Task 4 ✓ Vulnerability Databases

Task 5 ✓ An Example of Finding a Vulnerability

Task 6 ✓ Showcase: Exploiting Ackme's Application

Task 7 ✓ Conclusion

Created by tryhackme and cmnatic

1. What is the importance of understanding risk, vulnerability, and threat?

The comprehension and appreciation of the intricacies of risk, vulnerability, and threat are paramount in the development of efficacious cybersecurity tactics, which can provide adequate protection to organizations against the malevolent menace of prospective cyber attacks. The term risk alludes to the probability and impact of a potential security breach materializing. The identification and analysis of risks are imperative for organizations to proactively take measures to assuage their impact and avert potential harm. Vulnerability, on the other hand, pertains to a flaw in the security system, which can be exploited by a nefarious actor. The identification of vulnerabilities can facilitate the adoption of a panoply of steps to patch or mitigate them, thus preventing an attacker from taking advantage of them. Finally, the term threat refers to the likelihood of an attacker exploiting a vulnerability to cause damage to an organization's data or assets. By understanding the specific threats that an organization confronts, such as malware, phishing attacks, or insider threats, they can take adequate measures to safeguard against them. An in-depth comprehension of the correlation between risk, vulnerability, and threat enables organizations to formulate effective cybersecurity strategies, prioritize resources, and focus their efforts towards the most critical vulnerabilities and threats.

2. What are the limitations of CVEs?

The Common Vulnerabilities and Exposures (CVEs), an extensively employed method of recognizing and monitoring security vulnerabilities present in software and hardware systems, albeit their apparent usefulness, are plagued with limitations that can hinder their efficacy in practice. These limitations include incomplete coverage, arising from the fact that CVEs rely heavily on voluntary contributions from security researchers, vendors, and other stakeholders to report vulnerabilities, which in turn, may lead to some vulnerabilities remaining unnoticed or unreported, leading to coverage that is far from comprehensive. Additionally, the process of CVE publication is time-consuming, and typically, a significant lag exists between the identification and reporting of vulnerabilities and their publication as CVEs, allowing attackers to exploit such vulnerabilities during the interim period. Furthermore, CVEs only provide a brief summary of the vulnerability and its impact, which can be insufficient to give security researchers and vendors a full understanding of the vulnerability to address it comprehensively. Another limitation of CVEs is the absence of severity or priority ratings, necessitating the need for alternative sources of information, such as vulnerability scanners and threat intelligence feeds, to prioritize patching efforts effectively. Finally, CVEs can be misused by attackers to uncover vulnerabilities in software or hardware and subsequently exploit them before patches or mitigations become available, which has led to the phenomenon known as "CVE harvesting." Overall, while CVEs remain a valuable tool in the recognition and monitoring of security vulnerabilities, their limitations should be considered and mitigated when managing cybersecurity risks.

3. What is your opinion about this week's activities? Which is your favorite? Why?

Discovering the secrets of vulnerability 101 from the illustrious TryHackMe.com is an absolutely splendid and magnificent method to bolster your cybersecurity knowledge and honing your skill set. In today's world, vulnerability assessment and management are the crux of the matter when it comes to sustaining the security and integrity of systems and networks. By mastering the intricacies of vulnerabilities and their varied types, as well as the ways they can be exploited, one can craft an unbreachable defense against potential cyber threats. To sum up, I implore one and all to relentlessly strive to learn and enhance their cybersecurity knowledge and skills, with TryHackMe.com being an exemplary resource to accomplish that feat.