Rocket software

Bringing Vulnerability Scanning into Penetration Testing

Challenge

A large multi-national bank faced a critical turning point. Following a rigorous PCI audit, the operations director of the mainframe team realized that the responsibility of mainframe vulnerability scanning could no longer rest solely on their shoulders. With this realization, the director called upon the corporate penetration testing team to step up and take charge. However, a significant hurdle emerged—the penetration testing team lacked experience and understanding of mainframe vulnerabilities, risk rankings, and the importance of analytics-driven reporting. The challenge at hand was to equip and educate the penetration testing team on mainframe language and scoring methodologies, enabling them to seamlessly integrate into the vulnerability assessment process.

Solution

In a determined effort to bridge the gap between enterprise operations and penetration testing operations, the bank embarked on an innovative approach to integrate mainframe vulnerability scanning with penetration testing processes. To break down siloes and create a seamless workflow, the bank decided to implement an integrated and automated system that consolidates vulnerability scanning results across all operational and technology layers, generating consistent and automated reports. However, before this transformative shift could take place, the penetration testing team needed to acquire a deep understanding of mainframe systems and the intricacies of vulnerability scanning. Through collaboration with the organization's CISO, they devised a comprehensive mainframe education program that equipped the penetration testers with critical knowledge and operational understanding of mainframe activities. This program covered both mainframe operating system fundamentals and specific vulnerability scanning methodologies, ensuring the team was fully prepared to take on this new frontier of cybersecurity.

The Challenge

After a comprehensive PCI audit, the bank realized its mainframe team had reached a point where they couldn't manage vulnerability scanning. The penetration testing team was only experienced in network and PC testing methodologies.

> We never even thought we could have vulnerabilities on the mainframe, but once we began automated scanning, we found the volume and the severity to be much greater than anticipated."
>
> Chief Information Security Officer

As the bank looked for the right way to integrate mainframe vulnerability scanning with penetration testing processes, a dedicated task force was formed to navigate this transformation shift. Recognizing the need to dismantle existing siloes between enterprise operations and penetration testing operations, the bank made a resolute decision to adopt an integrated and automated process. This solution involved aggregating vulnerability scanning results from all the operational and technology layers, ultimately generating consistent and automated reports that would empower decision-making and collaboration.

Before this system could be fully implemented, it was crucial for the bank to bring the penetration testing team up to speed on the intricacies of the mainframe and the specific requirements of vulnerability scanning. To address this imperative, the organization's CISO was engaged in strategic discussions. Together, they orchestrated a comprehensive mainframe education program specifically designed to equip the penetration testers with the critical knowledge and operational acumen needed to navigate the unique challenges of mainframe activities. The mainframe education program was crafted to encompass both the fundamental principles of mainframe operating system, as well as the intricate realm of vulnerability testing procedures and mitigation processes. Working with KRI (now a part of Rocket Software, Inc.), the team was able to augment its training program with critical support and guidance that made it easier to learn the new systems, tools, and processes.

The Solution

A transformation shift was made to integrate mainframe vulnerability scanning into the bank's penetration testing team, empowering decision-making, collaboration and improved security.

Results

What started as a seemingly monumental task ended up being a seamless transition. With the support of Rocket Software, the bank's mainframe vulnerability scanning responsibilities were successfully centralized within the penetration testing team. The team learned how to utilize the analytics-driven data and CVSS scoring that was being generated by the mainframe scanning software and reported in a Vulnerability Analysis Report.

The accelerated onboarding of the penetration testing team yielded immediate dividends, unlocking the full potential of automated processes and testing methodologies that had a profound impact on reporting. By consolidating the role of vulnerability scanning under the penetration testing team, test and scan results delivered enhanced contextual information during reporting, elevating the organizations ability to identify and mitigate vulnerabilities effectively. The benefits of the shift extended beyond the confines of scanning operations. The organization was able to free up resources from its mainframe team, gaining valuable capacity to address higher-priority tasks and assume greater responsibilities in managing operations.

Impact

Optimized Security

The penetration testing team automated mainframe vulnerability checks, making it easier to identify risks and vulnerabilities.

Seamless Integration

The penetration testing team was brought up to speed quickly, making transitioning a major security responsibility a seamless process.

Improved Reporting

Consolidating vulnerability scanning allowed the penetration testing team to generate more complete consolidated risk reporting.

MAR-8133_CaseStudy_Pentest_V4