Final Paper

SDE 2

Senior Design 2

Prepared By: Faith Olajide

Professor Jason White

Capitol Technology University

April 10, 2024

**Introduction:**

This paper discusses my experiences working on my senior design project, which was based on the use of virtual machines (VMs) for workplace phishing simulation and training, during the course of the semester. It discusses the things I discovered, the difficulties I encountered, and the lessons I acquired while working on the project.

**Lessons Learned:**

One of the key lessons learned from this project was the importance of thorough planning and preparation. Initially, I underestimated the complexities involved in configuring VMs and designing realistic phishing scenarios. As a result, I encountered delays and setbacks during the implementation phase.

Additionally, I learned the significance of continuous monitoring and evaluation. While the initial phishing simulations provided valuable insights, ongoing assessments were necessary to adapt to evolving threats and behaviors effectively.

**Things I Wish I Knew:**

Looking back, there are several aspects of the project that I wish I had been better prepared for. Firstly, I underestimated the technical intricacies of VM setup and configuration. A deeper understanding of networking protocols and cybersecurity principles would have been beneficial in overcoming these challenges.

Furthermore, I wish I had anticipated the resistance and skepticism from some participants regarding the phishing training. Addressing misconceptions and emphasizing the importance of cybersecurity awareness early on could have fostered greater engagement and collaboration.

**Overall Budget and Schedule:**

In terms of budget and schedule, I initially allocated resources conservatively, anticipating minimal expenses. However, unforeseen technical challenges and the need for additional software licenses resulted in a slight overrun. Despite this, I was able to reallocate resources and adjust the timeline to stay within reasonable limits.

Surprisingly, the project was completed slightly ahead of schedule, thanks to proactive planning and effective time management. Regular progress updates and communication with stakeholders helped streamline the workflow and mitigate potential delays.

**What I Learned and What I Appreciated:**

Through this project, I gained a deeper appreciation for the complexities of cybersecurity training and the role of VMs in creating realistic simulation environments. Beyond technical skills, I developed a greater understanding of human behavior and the psychology behind phishing attacks.

Moreover, I appreciated the opportunity to collaborate with classmates and industry professionals, whose diverse perspectives enriched the project experience. Their insights and feedback proved invaluable in refining the training approach and enhancing its effectiveness.

**Conclusion:**

Overall, exploring VMs for Workplace Phishing Simulation/Training was truly both difficult and exciting . At the beginning, some obstacles occurred , hindering the implementation of the project from the very start. Even though most of them were effectively resolved through trial and error, they still posed a challenge to gain prerequisite knowledge and skills.

Upon completion of this project, I have benefited lots from this experience . First of all, I was exposed to the knowledge of cybersecurity. Although it was just an illustrative instance in a training session , setting up Windows , installing as well as practicing phishing with some other tools all proved to be vital in helping me be more adept at such operations. Besides , effectively taming these tools will surely propagate through other workplaces , enhancing the cybersecurity awareness of coworkers.

In view of the complexities and constant innovative stage of cybersecurity , future trainings will pose even greater challenges and demand years to catch up with . Thus , lessons learned from this project may serve as benchmarks for training in the future , and potentially turn into a habit of practicing at workplaces , contributing to promote companies’ security and combat cybercrime .