Jonathan Roeseler

Reflection Paper 4

Date: 9/23/205 - 10/1/2025

ODU Fall 2025

Professor Teresa Duvall

Internship Reflection Paper

200 Hours

Working as a Helpdesk Technician for 200 hours has given me a lot of experience in email, especially email security. I discovered some more advanced phishing practices against my organization, and I reached out to our support contact for our email security gateway to help address them. One attack I found by correlating the logs between Microsoft's Defender for Email and our email security gateway (Mimecast). By comparing the logs, I found that certain messages would appear in Defender's quarantine, and because I wanted to understand why Mimecast did not block them, I found that they were not even in there. At first, I was confused because all legitimate mail comes through Mimecast. We had put Mimecast servers as our MX records. Furthermore, via Defender's investigative features, I found that these messages would include links that reached out to malicious sites, as well as come from IPs that were on abuse lists (I use abuseipdb.com). Once I determined they were indeed malicious, I took action and reached out to Mimecast. I specifically gave them the logs and how they did not even touch Mimecast and hit our Exchange servers

directly. I eventually got a response back, and they sent me a guide on how to lock down our Exchange connector to only take messages from certain IPs (in this case, Mimecast IPs), so that only legitimate messages could hit our Exchange directly, not malicious ones that attempted to route around our MX records. After implementation, I then confirmed that mail flow remained as expected for our environment and the threat was mitigated. I proved it was mitigated by attempting to send mail to our exchange server directly (bypassing MX records like the attacker) and confirming it was blocked. Days later, I found that the attack was being picked up globally and abusing a Microsoft feature. I again retested the mitigation and determined it was still preventing as expected. Here is the article for reference: varonis.com/blog/direct-send-exploit. This experience taught me a lot about incident response and how to implement security measures effectively. Furthermore, following this, I was tasked with implementing Domain-based Message Authentication, Reporting, and Conformance [DMARC] for our organization. DMARC is vital to improving a domain's sending reputation, and it effectively prevents attackers from spoofing your domain if implemented correctly. I am currently in the early stages of this project; however, I have already learned a lot about DMARC, its importance, and how to go about implementing it, while ensuring the current mail flow is not affected.

The value of effective collaboration is the most important thing I've learned during the first 200 hours. In the incident I found between our two email gateways, I would not have been able to respond as promptly or effectively, had I not been able to reach out

for assistance. I found that during these 200 hours of work, communication and teamwork are very necessary in this fast-paced environment.

Overall, the first 200 hours have been a great introduction to learning the ins and outs of email. I now know a lot about why mail may not be delivered, how to respond to more sophisticated threats, and manage a new project. Moving forward, I am much more confident in this role and my ability to combat new threats and challenges to our environment.