Lewis Joseph Feik
Security Awarness
Reflection
Malware & Infiltration

# ***Reflection 3 – Malware & Infiltration***

*This week's material on malware and infiltration deepened my understanding of the variety of threats that can compromise computers and networks. Before this lab, I thought of malware mostly in terms of viruses or the occasional phishing scam. I now realize that malware is an umbrella term for a wide range of malicious software, including worms, Trojans, ransomware, file infectors, and spyware. Each form of malware has its own infiltration methods and system impacts. For example, worms spread automatically across networks, Trojans disguise themselves as legitimate software, and ransomware encrypts valuable files until a payment is made. What stood out to me most was how many of these threats exploit human error rather than technical flaws. A single click on an unsafe link or a careless download can allow attackers to bypass multiple layers of defense.*

*During the Chapter 3 projects, I worked through simulations that demonstrated how malware spreads and how to recognize evidence of infection. One project showed how a Trojan horse can be disguised as a useful tool, tricking users into installing it and silently creating a backdoor for attackers. Another simulation involved a file infector virus, where I observed how executable files became corrupted and how quickly the infection multiplied across the system. The biggest insight I gained was that malware often operates quietly at first. By checking task manager processes, event logs, registry changes, and unusual network traffic, I learned how investigators identify infections even before users notice symptoms. These projects made the connection between theory and practice very clear.*

*Personally and professionally, one important defense habit I will adopt is to be far more cautious about the sources of my software. I plan to install applications only from trusted vendors, verify digital signatures when possible, and avoid free tools from questionable websites. I also intend to keep my operating system and antivirus tools updated and to run regular scans. By consistently applying these habits, I will lower my risk of infection and contribute to stronger overall security in any organization where I work. This reflection reinforced that security is not only about technology but also about building disciplined habits that protect systems and data.*