Week 1 Write up

This week, we covered the introduction to Defense Against the Dark arts. Right away we jumped into some of the basics of what blue team investigators do in order to reverse engineer and create defenses against malicious attacks. These attacks could be one of these popular methods: Parasitic, polymorphic, and worm virus – backdoor, downloader, password stealer, keylogger, bot trojan – adware, spyware, or tools to help with network penetration. He mentioned that often times the most popular attacks are against the user rather than the network security, by using phishing or social engineering vectors. USB sticks, mobile app stores, drive by downloads, PDFs, and office files are all infection avenues for an attacker. He gave some basic definitions as well; White means clean while black means dirty, a goat is a “sacrifice” used to investigate malware such as a VM, and a honeypot is a trap. He went on to give more definitions of attacks and the basics of how they work, such as for ransomware and Blackhole Exploit Kit attacks. He mentioned how malware naming works however it is not standardized across the board. Last of all in lecture one, he showed the basics of how to setup the VM and use some of the tools included.

For lecture 2, he described different aspects of attackers: Advanced, Persistent, and Threat. These represent the attacker profile, intent, and structure which is key to understanding if the attack is an isolated event from a single party or a government backed, widespread attack. Attacks are not always political either, as sometimes corporations can use attacks to steal corporate secrets from competitors or disrupt their supply chain. Perhaps the most important aspect of the lecture was in regards to the “APT Kill Chain”, which describes the process of how an attacker penetrates and exploits a system. It begins with reconnaissance, which involves learning about the people, systems, defenses, and more about the target. Next is weaponization, where the attacker creates their payload which will be delivered to the target based on what they learned from the previous step. Next is delivery, where they infiltrate the system either wirelessly, in person, or through social engineering. Exploitation follows, where they create a discreet and low profile beachhead from which they can escalate their infiltration into the system or device. Up next is installation, where the heavy hitting malware is installed from the beachhead and any defenses already existing are manually destroyed. Command and Control is the second to last step and is about the attacker escalating privileges as far as possible and asserting complete control over the device or network. Finally, we have “Actions on Objectives”, where their ultimate goal is realized. This can be anything from finalizing the encryption process of the ransomware to stealing secrets from High profile accounts. He ended the lecture with different ways to investigate certain files and break past XOR encryption, commonly used to hide malicious code from AV.