**WEEK 2 ASSIGNMENT**

1. What is Cyber defense framework and what are the processes in protecting organizational assets.
2. What is OSINT?
3. What is Email Harvesting?
4. What are some of the tool’s attacker can user for Reconnaissance?
5. Define attack surface and Attack Vector
6. What is the difference between Threat, Risk and Vulnerability?
7. Define a Malware and give 3 examples of malware and how would you mitigate a malware?
8. What is Cyber Kill chain and define the stages of Cyber Kill Chain?
9. What is Diamond Kill chain and what are the component included in each stage?
10. Define MITRE Attack and state all the stages involve with MITRE Attack
11. Define Unified Kill Chain and what are the benefits over other kill chains?
12. What is the name of the attack phase where an attacker employs techniques to evade detection?
13. Explain the Pyramid of Pain and how does that affect your network.
14. What Cyber attack have you defend before?
15. This term is referred to as a group of commands that perform a specific task. You can think of them as subroutines or functions that contain the code that most users use to automate routine tasks. But malicious actors tend to use them for malicious purposes and include them in Microsoft Office documents. Can you provide the term for it?
16. A malicious code that the attacker runs on the system is called what?
17. Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. What is the technique called?
18. What is the C2 communication where the victim makes regular DNS requests to a DNS server and domain which belong to an attacker?