Course: COMPSFI 212 – Scripting for Cybersecurity
Python for Cybersecurity: Chapter 1
Due Date: 09/02/2025 @ 11:59pm

Short Answer

1. Explain the difference between Active Reconnaissance and Passive Reconnaissance. Provide one example of each.

2. Why did MITRE retire “Pre-ATT&CK” as a separate matrix and merge it into Reconnaissance and Resource Development?

3. Describe how DNS can be used by attackers during reconnaissance. Provide at least two insights attackers might gain?

4. From a defender’s perspective, why is reconnaissance difficult to prevent completely?

Applied Scenarios

1. You are a network administrator. During log review, you notice repeated connections to ports that your organization does not normally use, along with unusual DNS lookups for your company’s subdomain.

- Which stage of the cyberattack life cycle does this activity represent?
- How could you determine whether this activity is a harmless misconfiguration or a potential attacker?

2. You organization wants to make reconnaissance more difficult for attackers. Describe two defensive techniques you could recommend. For each, explain how it complicates the attacker’s reconnaissance efforts.

Reflection

Write a short essay (200-250 words) on the following:

Reconnaissance is often said to be the most critical stage of a cyberattack. If you were leading a cybersecurity team, how would you balance the fact that reconnaissance can’t be stopped with the need to protect your organization’s infrastructure? Give specific examples of strategies or technologies you would prioritize.