Course: COMPSFI 212 – Scripting for Cybersecurity
Python for Cybersecurity: Chapter 2
Due Date: 09/04/2025 @ 11:59pm

Short Answer

1. Explain what is meant by the “Initial Access” phase in the MITRE ATT&CK framework. Why is this stage critical for attackers?

2. Describe two different ways attackers can acquire valid accounts and use them to gain access.

3. Why are removable media such as USB drives still considered a threat vector even though modern systems disable AutoRun by default?

Applied Scenarios

1. You are a security analyst. In the Windows Event Log you see multiple 4625 failed login events for the same user account from a single workstation.

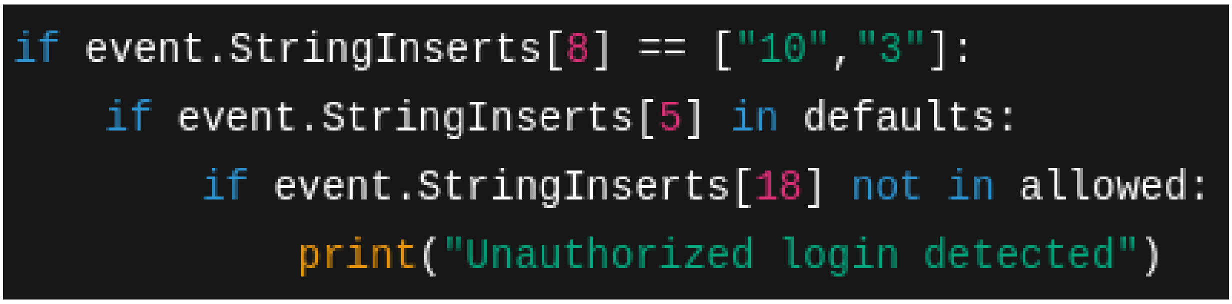
- What does this indicate?
- How would you confirm whether this is a brute-force attack or simply a user typing the wrong password?

2. A suspicious USB device was found in your office.

- Describe the steps you would take to safely analyze the device.
- What Python-based detection methods could you use to monitor for suspicious USB behavior on endpoints?

Script Review

Look at the following snippet from a defensive Python script:



```
if event.StringInserts[8] == ["10","3"]:
    if event.StringInserts[5] in defaults:
        if event.StringInserts[18] not in allowed:
            print("Unauthorized login detected")
```

1. What is the script trying to check for?

2. Can you identify a problem in the condition `event.StringInserts[8] == ["10","3"]`? How might you fix it?

3. Why is it important for defenders to validate logon types in this way?

Reflection (~150 words)

1. Compare the risks of valid account abuse versus replication through removable media. Which do you think poses a greater threat today, and why?