🕐 Hour 1: Orientation + “Hello, Hacker”

🎯 Objectives

- Understand what Python is and how to run it
- Write and run a basic script
- Personalize output and explore terminal behavior
- Begin thinking about visibility and control in computing

🧱 Topics Covered

- What is Python? Why it matters in cyberdefense
- REPL vs. script files
- `print()` statements
- Comments (`#`)
- Basic string literals and escape sequences

🧪 Activities

1. "Hello, Hacker" Script

```
print("Hello, Hacker. Your terminal is now under your control.")
```

✅ *Checkpoint:* What does “control” mean in computing? What can you do now that you couldn’t before?

2. Alias Input

```
name = input("Enter your hacker alias: ")
print(f"Welcome, {name}. Initializing recon protocols...")
```

✅ *Checkpoint:* What does `input()` do? What happens if you enter a number instead of a name?

3. Printing Colored Text

There are better ways to do this, but for our purposes today, we are going to control the color of the text in the ugliest way possible - by using ANSI escape sequences.

```
print("\033[30;40mThe password is swordfish\033[0m")
```

✅ *Checkpoint:* Can you copy and paste the hidden text? Why or why not?

If you want to see nicer ways to control text color, let me know.

4. Bonus: Caesar Cipher Greeting

```
encrypted = "Khoor, Kdfnhu"
print("Encrypted message:", encrypted)
```

✅ *Checkpoint:* What kind of cipher is this? Can you decode it manually?

5. Bonus Bonus: Decoding the Caesar Cipher Greeting using Python

(see file `hour 02 bonus - solving caesar cipher.md`)