Samantha Jones

Security+ Certification 2025SP-CYBR-1200

Module 01 Lab Manual Word Files

1/18/25

**Playbook Entry 1**

1. **Title:**

Playbook Entry 1: Introduction to Security Concepts

1. **Summary of key concepts:**

Foundation of cyber security: Confidentiality, Integrity and Availability (CIA)

Threats to cyber security: Threat actors and attack surfaces. Threat actors in social engineering. Physical controls cyber security use to combat threat actors.

1. **Key takeaways:**

-Cybercriminals use social engineering solely for profit

-Red hat hackers go after black hat hackers with the intent to squander their resources and/or cause harm

-Whaling is a form of phishing where threat actors attack executives or CEOS

**4. Tools and techniques used:**

-Virtual machines

-Data masking

-Restrictions

-CIA and other organizations set standards to help cyber security to combat threats

**5. Lab Summary:**

**-**The objective: Enable Microsoft sandbox to run new software on so it cannot affect your computer.

**-**Steps performed: We were given instructions on how to enable sandbox. Installed a program on sandbox.

**-**Results: We learned that by using sandbox we can run programs on the virtual machine, and it will not affect our personal/office computers

**-**Reflection: We learned that a virtual machine is essential to learning new software or legacy software

**6. Real world applications:**

I work in an office as a cybersecurity analyst. I can use a virtual machine on my computer to run linux. I can use that virtual machine to understand how hackers might use certain malware to gain access to confidential data.