* **Certified Information Systems Security Professional (CISSP) Security Domains:**
  + Security & Risk Management focuses on defining security goals and objectives, risk mitigation, compliance, business community, and law.
  + Asset Security focuses on securing digital and physical assets. It also related to the storage, maintenance, retention, and destruction of data.
  + Security Architecture & Engineering focuses on optimizing data security by ensuring effective tools, systems, and processes are in place.
  + Communication & Network Security focuses on managing and securing physical networks and wireless communications.
  + Identity & Access Management focuses on keeping data secure, by ensuring users follow established policies to control and manage physical assets
  + Security Assessment and Testing focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities.
  + Security Operations focuses on conducting investigations and implementing preventative measures
  + Software Development Security This domain focuses on using secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services.
* Attack Types:
  + Password attack an attempt to access password-secured devices, systems, networks, or data. Some forms of the attack:
    - Brute Force
    - Rainbow Table
    - Fall under the communication and network security domain.
  + Social engineering attack
    - Related to the security and risk management domain.
  + Physical attack a security incident that affects not only digital but also physical environments where the incident is deployed.
    - Malicious USB cable
* Malicious USB cable