This Capstone project focuses on executing a full-scope **Purple Team Exercise** built around the concepts of **Adaptive Deception** and **Active Defense**. Students will first design and implement a complex, realistic **enterprise-grade virtual network architecture** that includes modern services and robust security monitoring. The core deliverable is the execution guide for the Purple Exercise, detailing the **Red Team's Advanced Persistent Threat (APT) simulation** targeting the environment and the **Blue Team's defensive strategy** which must incorporate **dynamic deception layers** (e.g., honeynets, fake credentials) and **automated, active countermeasures**. The project culminates in a final report and briefing that documents the end-to-end exercise, maps the findings to the **MITRE ATT&CK framework**, and provides data-driven recommendations for enhancing the organization's security posture through the principles of deception and automation.

Adaptive Deception involves deploying decoys and fake artifacts designed to lure attackers, gather intelligence on their methods (TTPs), and subtly degrade their effectiveness. The **"Adaptive"** component means the decoys change or multiply once the attacker interacts with them.

Active Defense refers to coordinated, automated responses that aim to disrupt, deter, or gain intelligence on the adversary *after* detection, without taking direct offensive actions.

Capstone Project Deliverables

This project requires five main submissions to fulfill the requirements of the Purple Exercise:

Enterprise Architecture & Automated Deployment Guide

- A **professional-grade network diagram** illustrating the complete enterprise architecture (e.g., firewall, DMZ, internal LAN, Active Directory server, web servers, jump hosts, and logging/SIEM infrastructure).
- A **detailed, step-by-step technical guide** or script (e.g., using Ansible, Terraform, or Vagrant) that allows the instructor/TA to fully and accurately deploy the entire environment (Red, Blue, and Purple components) with minimal manual intervention.
- **Deliverable Format:** Document (PDF) and Deployment Script/Code Repository.

Adaptive Deception & Active Defense Plan

- A strategic document that details the **Deception Architecture**, including the placement and purpose of all honeypots, honeynets, credential canaries, and decoy files.

- A detailed plan for **Active Defense**, outlining the **SOAR playbooks** or logic used for automated responses (e.g., containment, throttling, dynamic logging) triggered by interaction with the deception layers.
- **Deliverable Format:** Detailed Report/Documentation (PDF).

Purple Team Exercise Execution Report

- **Red Team Narrative:** A step-by-step account of the attack path, including tools, commands, and TTPs used, and the *intended* interaction with the deception layers.
- **Blue Team Analysis & Feedback:** Detailed log analysis showing when the Red Team was detected, which deception layers were triggered, and the specific **adaptive changes** made to the defense (e.g., a firewall rule dynamically added).
- **MITRE ATT&CK Mapping:** A table or matrix mapping the Red Team's executed techniques to the MITRE ATT&CK framework and documenting which defense/deception layers were successful (or failed) against each technique.
- **Deliverable Format:** Comprehensive Technical Report (PDF).

In-Class Briefing Deck

- A professional, concise presentation deck (e.g., 8-10 slides) designed for the **In-Class Briefing**. **PLAN MAXIMUM TEN MINUTES FOR YOUR PRESENTATION**
- The briefing must summarize the initial architecture, the key deception/active defense strategy, the most critical findings from the Purple Exercise, and the **top three actionable recommendations** for improving the organization's security posture.
- **Deliverable Format:** Presentation Slides (PPT/PDF).

Executive Summary

- A single-page, high-level summary written for a non-technical executive audience (e.g., the CEO or CFO).
- It must briefly state the exercise goal, the key risk identified, and the business value of implementing the recommended adaptive deception strategies.
- **Deliverable Format:** Single-Page Document (PDF).