**CYBR 7910 Capstone in Practicum Project Plan**

**[Group 4]**

**Date: June 17, 2025**

## Overview

Web Application Honeypot - Present as "SecureLogon Pro" authentication portal to other teams. Intentional vulnerabilities (command injection, directory traversal) serve dual purpose - satisfying exploit requirements while demonstrating attacker techniques in a controlled environment. Reveal honeypot nature during presentation with complete attack timeline analysis. Shows understanding of both offensive and defensive security methodologies.

## Project Team

| **Roles** | **Name** | **Major responsibilities** | **Contact (Email and/or Phone)** |
| --- | --- | --- | --- |
| Team lead | Daley Mackey | Fake login portal logic, attack logging system, data analysis scripts | C: 864-420-5365 / dmackey9@students.kennesaw.edu |
| Team member #2 | Brandon Ejike | VM deployment, web server setup, log rotation, network configuration | C: 770-658-9018 / bejike@students.kennesaw.edu |
| Team member #3 | Carley Hume | research report  basic database/OS assistance/backup  final report | C: 352-871-2611 / chume2@students.kennesaw.edu |

## Major Deliverables

#1 - Configure VM

#2 - Analyze Technology Options

#3 - Create Database

#4 - Development Baseline

#5 - Deployment

#6 - Testing and Demo

Test for GIT

**Strategies for Team Collaboration**

* Team members have constant communication via a text message group and weekly meetings via TEAMS.
* All documentation will be housed on Github including master