

# • IT 4983 Capstone in Cybersecurity Project Plan

[W02-12777 Project 11 Cybersecurity Group 2]

[Brandon Turner, Kowou Agbavon, Andres Morales, Aleksandar Punos, Felton Strickland]

**Date** January 30, 2022

## Overview

Our team will act as security consultants hired to design, develop, and implement a security solution for a small business. The project is divided into 3 phases: project initiation, project progression, and project conclusion. Our goal is to design a security program which will protect our client's system. In phase one, we will develop and implement security programs. In phase two, we will create a plan of attack to exploit other teams' systems. In phase three, we will attack other systems and respond to attacks made on our system by the other teams. We will then deliver a final report and a presentation to conclude the project.

## Project Team

| Roles                | Name              | Major responsibilities  | Contact (Email and/or Phone)   |
|----------------------|-------------------|---|--------------------------------|
| Team lead            | Brandon Turner    | Provides project details and maintains communication with the team.     | Bturne41@students.kennesaw.edu |
| Technical Specialist | Kowou Agbavon     | Technical Specialist: analyze, design, and develop technical solutions. | kagbavon@students.kennesaw.edu |
| Technical Specialist | Andres Morales    | Technical Specialist: analyze, design, and develop technical solutions. | Rmoral10@students.kennesaw.edu |
| Technical Writer     | Aleksandar Punos  | Prepare all documentation including presentation and poster materials.  | apunos@students.kennesaw.edu   |
| Technical Specialist | Felton Strickland | Technical Specialist: analyze, design, and develop technical solutions. | fstrick2@students.kennesaw.edu |

## Major Deliverables

Final Deliverables:

- Written report comprised of an executive summary, description of assessment methodology, vulnerability findings, risk assessment, and recommendations for security solutions.
- Security policy that aligns the security controls with the strategy, goals, and objectives of the organization and effectively addresses all elements of the CIA triad.
- Secure network that has been actively tested for vulnerabilities via penetration testing.
- Website that displays the progress of the team's security effort with project documentation and schedule.
- Formal presentation summarizing project to project sponsor.

#### Milestone #1 – By 02/20/2022:

- Conduct risk assessment to identify the areas of vulnerabilities of business that are susceptible to the security risk.
- Understand the impact of the threat on the business's survival and classify the risk from insignificant risk to the high threat to the business operation.
- To maintain compliance, all shareholders must follow regulatory requirements when using the business IT assets.
- Response recommendations to incident and the remediation restore application and data essential for the business continuity.

#### Milestone #2 - By 03/20/2022:

- Implement the security program on the VM that the team decided to use in phase 1.
- Develop a strategy and research tools that could be used during vulnerability analysis/penetration testing to access the opposing team's server.
- Create a report on the implementation of a security program, and strategies/tools we plan to use to exploit the other group's server.

#### Milestone #3 - By 04/10/2022:

- Project phase 3 report –Protection (group 2) and Security breach (group 1).
- In this phase we will protect our server and at the same time we will test the other team server, we will attempt to break in their server.
- Create vulnerability analysis/penetration testing on the other team (cybersecurity –group 2) web server-create a report about these tests and their results.
- Create a forensic report of the security procedures implemented into defending of assigned server.

### **Project Schedule and Tasks Planning**

See the Gantt chart file in the module for keeping track of the tasks and hours worked for the project.

### **Strategies for Team Collaboration**

- Technologies and strategies for team communication. Each member should provide at least 2 ways that they can be reached (e.g., email or cell phone)
  - The team decided that it would be best to communicate small things that we can message about throughout the week in GroupMe. For our second form of communication, we have created a Group on Microsoft Teams.
- Technologies and strategies for team collaboration. Will there be a fixed meeting time each week? How can members keep track of the status of the project? How the files be shared among team. Who oversees what tasks?

- There will be three fixed meeting times per week, all at 6pm on Mondays, Thursdays, and Saturdays. We will use communication through teams. Files and documents will also be shared on teams so each member has control, edits, and can see the progress that is being made as well as contribute. Kowou, Andres, and Felton will oversee the analysis, design, and development of our technical solutions. Aleksandar will oversee documentation and presentations. Brandon will oversee project management, communication, and be the liaison between the team and the sponsor.
- How to ensure that everyone is contributing to the team? 20% of course grade come from peer evaluation.
  - As we come to the different phases of the project, we will equally divide work based on team members' strengths as well as their designated roles. We will ensure everyone is contributing by having clear objectives for everyone in our meetings that need to be accomplished and maintaining communication.
- MS Teams is recommended for team collaboration. But feel free to use other technologies.