CS 3113: Principles of Cybersecurity
Course Project, 300 points
***Due Dates*: See Individual Assignments**
This is a group project – no exceptions

Conducting Cybersecurity Assessments

Purpose

The purpose of the course project is to gain experience with conducting a cybersecurity assessment. In this case, the target organization is a fictional, non-profit, small business called NARO, Inc. (Not A Real Organization)

This will be a paper-based exercise, meaning there will not be any active assessment activities such as penetration testing. However, this is not unusual in the cybersecurity industry for many reasons, including:

- Some systems – such as those involving critical infrastructure – are not suited for active assessment activities. For example, some industrial control systems can be damaged by a simple network scan.
- The only systems an organization has may be their "production" systems, and disruption of those could impact business operations.
- The organization is still in the design and implementation stage of the system, and a working system does not yet exist.
- The organization does not have the resources to support an active assessment. For example, they may not have an IT person that can quickly restore systems to their original state after it has been compromised (Ex. Small businesses or a remote office)

Overall Project - Background

For this assignment, your group will be taking on the role of cybersecurity assessors working for Death Star Consulting (DSC) that has been hired by NARO, Inc. to conduct an assessment.

Unfortunately, the senior assessors at DSC have been given high-priority tasking by a casino (something about investigating a fish tank that was used in a cyberattack) so your team of junior assessors have been assigned the NARO assessment. You have access to some DSC templates and previous reports that will help guide your work.

Also, before assigning your group this tasking, an initial request for information was made, and you should have received the (short) summary. It isn't complete by any means but should provide enough information to get started. This project is not a "deep dive" and, since NARO, Inc. only has production systems – some of which involve hazmat – no active testing will be performed.

This project is a full assessment, and you will have to:

- Develop a brief project plan for your group, which will include:
    - Planned meeting times
    - Milestone dates for outline, drafts, and final products
    - Assigned tasks (if any)
- Create an introduction/in-brief presentation for NARO, Inc.
    - This will be done as if you are a consulting company briefing a customer on what is going to happen (i.e. – As if you were going to brief William Donaldson III on the upcoming activities)
    - See the provided template and additional guidance for more details
- Create a cybersecurity audit checklist for NARO, Inc.
    - This may be based off the checklist from **Assignment #1 – Pt. II**
- Conduct the assessment activities:
    - Provide NARO, Inc. with your Assessment Checklist
    - Review the materials provided by NARO, Inc.
    - Attend (or watch the recording) of the interview with William Donaldson III
    - Ask follow-on questions to receive missing information, or clarify provided information
- Write an assessment report containing their findings from the assessment. This will include:
    - Evaluation of policies and procedures related to identify and access management (users, passwords, permissions, etc.)
    - Assessment of communication and network security, including remote access, work from home, use of personal devices for work
    - Evaluation of cybersecurity training
    - Analysis of data collection, storage location, retention, and destruction policies and procedures
    - Physical security of systems and information
    - Plans for Continuity of Operations, Disaster Recovery, and Data Backups
    - Identification of any technical vulnerabilities
    - The report will also include potential mitigations for the various findings
- Create an out-brief with William Donaldson III, that would be used to brief the assessment report
    - It should include the key factors from your report, including findings, potential mitigations, overall conclusions and recommendations.

The end product will be a professional assessment report that will be delivered to NARO, Inc. and a presentation of that report. However, to help keep your team focused, and following the process, it has been broken down into smaller assignments that will be due throughout the semester. Although, it is also expected that work on the final report will be done in parallel with the milestones.

Deliverables

The deliverables for this project, which are broken into individual assignments are:

1) **(20 points) Project Plan.** This will include:
    a. Planned meeting times
    b. Milestone dates for outline, drafts, and final products
    c. Any sub-teams you create. (Ex: William and Ben will work together on…; Brad and Tammy will work together on…)
2) **(25 points) In-brief Presentation**. There are two parts to this deliverable:
    a. The slides that your group uses to present to NARO, Inc
    b. Notes that you are using for the various slides. This can be a separate outline, or done using the "Notes" feature in PowerPoint. The notes should provide enough details that I can refer to them to what you plan to cover in the presentation.
    c. You will not actually be giving the in-brief presentation
3) **(25 points) Audit Checklist**. The audit checklist you develop for NARO, Inc.
    a. It can be based off the checklist you develop in **Assignment 1: Part II**
    b. Make sure you follow the guidance given in the assignment for how to develop a good audit checklist.
4) **(10 Points) Checkpoint 1 Survey.** This will be a survey covering:
    a. Whether you have read the provided materials
    b. Group communication
    c. Group dynamics
    d. Overall progress
    e. You will automatically receive full points for completing this survey
5) **(50 points) Project Report – Rough Draft**. This is meant to be a draft of the report you are working on. While you are not expected to have a completed report, it should show significant progress in your work. Some things that can be completed:
    a. Introduction – including background and scope
    b. System Description – you will have information about NARO, Inc. You can complete this section
    c. Assessment Activities – what you have done up to this point
    d. Etc.
6) **(10 Points) Checkpoint 2 Survey.** This will be another survey to ensure groups are working well together, and all group members are contributing
    a. You will automatically receive full points for completing this survey
7) **(100 points) Final Report**. This is the final assessment report that will be delivered to NARO, Inc.
    a. This should address all sections in the provided template
    b. Sample reports – from real assessments – have been provided to use as a guide for what this report should look like
8) **(50 points) Out-brief Presentation**. There are two parts to this deliverable:
    a. The slides that your group uses to present to NARO, Inc.
    b. Notes that you are using for the various slides. This can be a separate outline, or done using the "Notes" feature in PowerPoint. The notes should provide enough details that I can reference it for what was said/covered in the presentation.

However, this should not be an overwhelming amount of text. i.e. – Don't just cut and paste your report into the notes field.

c. This presentation will be given to Professor A. in his role as William Donaldson III

9) **(10 Points) Checkpoint 3 Survey.** This will be another survey to ensure groups are working well together, and all group members are contributing
   a. You will automatically receive full points for completing this survey

Final Report – Additional Details

The final deliverable for this project will be an assessment report that is of a ***professional quality, and could be handed to a customer***.

The final report is expected to include the following information/sections:

- Executive Summary
- Introduction
- System Overview/Description (Critical Views are included here)
- Assessment Methodology (You can modify the IDART™ Methodology)
- Assessment Activities (Critical Attack Graphs are included here)
- Assessment Results and Recommendations (Weaknesses, Strengths, and Observations)
- Conclusions
- Appendices (Includes all additional information, data collection references/results, other views and attack graphs, etc.)

The report does not have a specific length requirement, but will be evaluated on completeness, professionalism (ex. do not insult the organization), impression (i.e. – no obvious errors, formatting problems, etc.), and overall ability to inform NARO, Inc. of identified issues and help them address those issues.

Strong reports are usually over 30 pages.

However, as Douglas Adams says: "Don't Panic!" By the time you have the title page, executive summary, Table of Contents, and allow for proper page breaks (i.e. – Each major section should start a new page, or even a new "odd page") you may find 30 pages is relatively short. For example, the EV Charging Infrastructure report is 66 pages and even the New Jersey Transit report is 44 pages.

Some technical and non-technical areas to consider for the report:

- Evaluation of policies and procedures related to identify and access management (users, passwords, permissions, etc.)
- Communication and network security, including remote access, work from home, use of personal devices for work
- Cybersecurity training
- Data collection, location, retention, and destruction
- Physical security of systems and information

- Plans for Continuity of Operations, Disaster Recovery, and Data Backups

In the event NARO, Inc. does not have appropriate security-related policies, training, etc. you can provide recommendations for what those areas should include. However, keep in mind that you are the red team – your role is not to fix things, it is to figure out how to break them. That's it.

Guidance

- ***A cybersecurity assessment is a lot of work***. If you put things off, you will fall behind and won't be able to complete the assessment. There will be guidelines provided throughout the semester on where your group should be.
- ***Communicate often***. Make sure you are communicating with all of your team members on a regular basis. If you have any communication problems (i.e. – more than 2-3 days without hearing from someone) let me know immediately.
- ***Set regular meetings and milestones***. Don't leave everything to ad hoc emails, or sporadic communication. Make sure there are set meetings and milestones for your work.
- ***Don't try to reinvent cybersecurity assessments***. You may find the template, the sample report, in-brief, or guidance "boring" or not "cool." Resist the urge to improve on things until you have a few assessments completed. Also, a "simple" update can often lead to hours correcting minor formatting issues. (Yes, I have had this happen when a "minor" change was requested for our report format.)
- ***Make sure you are following the instructions and requirements***. For example, make sure you have all the deliverables completed, have covered all the topics requested, and have everything (and the right version of everything) turned in.
- ***Engage with your team***. Make sure you are contributing to your group and the project. I have given 10%, 25%, 50%, and 100% penalties for group members that didn't participate. While a group will only turn in one set of artifacts, that doesn't mean everyone will receive the same grade. Your grade will be individually impacted by your contributions.
- ***Work as a team***. Support each other, help each other with tasks, and read over each other's work to ensure there aren't any errors or inconsistencies. Teamwork will only make for a better end product.
- ***Make sure everything is accurate and true***. There is going to be missing information, contradictory information, and things that aren't known when you get information from NARO, Inc. This is on purpose since this is likely to happen on an assessment. If something is unclear, make sure you state it as such – or ask the organization to clarify things.
- ***Make sure any recommendations are reasonable***. Your recommendations need to take into account the resources available to a small business, and what they would consider appropriate. For example, a small non-profit does not need to maintain a hot site for disaster recovery if there is a fire in their primary office. However, they might need to maintain off-site backups.
- ***Have fun***! This is supposed to be a fun way to learn and gain experience.