CSCI 3403: Project 1

Modern Cybersecurity Fundamentals

Due: 2/6/20 at 11:59 PM

Background

For this project, we want to deeply solidify the groundwork that we're laying for the course. No previous background is necessary, except for some basic concepts in computing. Please read the whole description before starting.

Goal

The goal of this project is to explore and get hands-on experience analyzing modern events through the lens of some cybersecurity concepts. In reality, these are skills that you will continue to refine as you learn more about security and the related concepts, but we're going to practice here so that we have some experiencing focusing on these skills. To demonstrate this, you should make your answers ***as unambiguous as possible***. If you're assessing Identify, don't give a response to Detect, or both Identify and Detect. Convince the reader you know what you're talking about!

While writing your project you should also think about and carefully use terms like "vulnerability, threat, asset, risk, attack, etc." Incorrect usage/lack of critical technical terms discussed in class will result in a loss of points. This will help us to build and become fluent with this type of vocabulary.

Find a Cybersecurity Event

First, go to one of the many news outlets for cybersecurity events. Some may be listed under class resources; a few you're free to use are: Krebs on Security, WIRED, anything from here. Don't stress over choosing the right media site, but choose an article you feel you can offer some insight into. You should find an article that contains significant cybersecurity content. This could be a recent breach, a newly discovered vulnerability, a planned upgrade to security technology, or something else. Some examples for each of these could be the City of Atlanta ransomware attack, the Windows 10 2020 patch, or the coming of DoH (feel free to use those!)

Explain Your Event

Before analyzing your event, you should first gain a solid technical and conceptual understanding of your chosen event. This could involve some in-depth technical research on the technologies behind the event, as well as some of the less-intuitive impacts. Please let your research show in the following questions.

1. **(5 points) In 2-3 sentences, explain what your event was about at a <u>conceptual</u> level. In this, explain how it relates to cybersecurity**
2. **(5 points) In 2-3 sentences, explain some of the <u>technical</u> details of your event.**
3. **(5 points) What is the most interesting thing you took away from reading about your article?**

The CIA Triad

Answer the following questions in a *<u>brief, logical</u>* manner. Your response for each question should be no more than 1-2 succinct sentences. The emphasis is not getting every possible angle out of your response as much as being unambiguous.
For example, if you're analyzing the confidentiality of a ransomware attack, a **good answer** would be, "The confidentiality of the files could be breached if the attacker not only encrypted, but also uploaded the victim's files and threatened to post them if they don't pay the ransom." A **less ideal answer** would be, "The attacker may tamper with the files on the user's computer, allowing them to see or even corrupt the data." This answer discusses both confidentiality and integrity. You may also lose points if your answers are too wordy or excessively long.

4. **(5 points) Analyze some impacts from your event on each of the CIA triad in 1-2 sentences each.**
   a. **Confidentiality:**
   b. **Integrity:**
   c. **Availability:**

Common Design Principles

Now we want to look at our event through the lens of some common design principles. At some point related to your chosen event, somebody violated some design principles. Or, perhaps you think that somebody did an outstanding job of implementing some design principle. Whatever it is, choose a few design principles that you think are most closely related to your event and expand upon them.

5. **(5 points) Pick 3 common design principles and explain the impact on your event in 1-2 sentences each.**

Extra Credit: Attack Trees!

We want to analyze some of the attack surfaces and vulnerabilities, both existing and potential, of the event you're analyzing. To help get you started, perhaps if you're discussing DoH, an attack tree could cover some of the existing vulnerabilities to DNS, and how DoH would fix those. You could also make a tree covering some of the vulnerabilities that won't be addressed. Or, in a breach, you can think about some of the ways that the attackers could have broken into the system and discuss the feasibility of each one. See if you can follow their thought process and think like the attacker! Like usual, the tree should not be excessively large, but it should reflect some thought.

6. **(3 points) Create an attack tree of your current event (15-20 leaf nodes is fine). You may create it digitally or write it neatly and scan it in – whichever is easier for you.**

Submission

Upload a new document with your answers. It should contain the following:

1. Your team members' names and emails.
2. The bold questions and your answers.
3. Any sources that you used to research your article. With no sources, your project will be considered plagiarism. Feel free to gather information about an event from more than one source (hint: you probably should!)
4. A description of what each team member contributed. One person in the group should turn in a single document, but each member should contribute, though naturally, you will contribute to different things