





















**Team Members (Required)**

**Reminder:** Make sure to provide **edit access** for this Milestone document to **everyone on your team!**

 Student Name:  Student Pronouns:  Student Email:  Favorite Animal:		 Student Name: Susanne Santos Erenst  Student Pronouns: She/Her  Student Email: <a href="mailto:serenst2014@fau.edu">serenst2014@fau.edu</a>  Favorite Flavor: Strawberry
 Student Name:  Student Pronouns:  Student Email:  Favorite Park:	Sienna Gaita-Monjaraz She/Her <a href="mailto:sgaitamonjar2019@fau.edu">sgaitamonjar2019@fau.edu</a> Red Reef Park	 Student Name: Maximo Mejia  Student Pronouns: He/Him  Student Email: <a href="mailto:mejiam2017@fau.edu">mejiam2017@fau.edu</a>  Favorite Game: Cuphead
 Student Name:  Student Pronouns:  Student Email:  Favorite Drink:	Tania Alam She/Her <a href="mailto:talam2021@fau.edu">talam2021@fau.edu</a> Coca cola	

[What are pronouns /](#)  
[Why are they included here?](#)

**Select one (or more) open-source Datasets to analyze (Required)**

**Data Set Chosen:** The data set we have chosen to analyze for The Data Dig is...

**Name:** The Malware Traffic Analysis Dataset (MTAD)  
**Primary Link:** <https://www.malware-traffic-analysis.net/2014/11/05/index.html>  
 Other Resource: <https://www.virustotal.com>  
 Other Resource: <https://malwr.com/analysis>

**Data Set Description:** Where does the data come from? Who generated it? What kind of devices / technologies does it target? What format is the data in?

The data comes from malware-traffic-analysis.net It was generated by a phishing email. It targets the victim's host system. The format of the data is PCAP.

**Hypothesis:** What are 3 things you expect to find when you analyze the data?

*Tip: You won't lose points if these hypotheses turn out to be wrong! Make educated guesses!*

**Finding #1:** DNS query for the host's IP

**Finding #2:** Attempted TCP requests

**Finding #3:** Attempted HTTP/HTTPS requests

## Select an incident-response playbook to follow (Required)

**Playbook Chosen:** The playbook we have decided to follow for The Data Dig is...

**Name:** Playbook - Phishing (Incident Response Consortium)

**Primary Link:** <https://www.incidentresponse.org/playbooks/phishing>

Other Resource:

Other Resource:

**Playbook Description:** Who wrote this playbook? Who is the target audience? Does it make any specific assumptions about the data set? If so, do those match your data, or will you have to adapt the playbook?

This playbook was written by Joseph Loomis and Ryan Corey. They created this playbook for the cybersecurity community including professionals, enthusiasts, and students. Specifically, teams looking for easy assistance. Incident Response was intended to provide accessible open source resources on different vulnerabilities to lower incident response times.

**Tools we Plan to Use:** Based on your dataset and playbook, what blue-team tools from this course will you use to analyze the incident? (MINIMUM of 2)

**Tool #1:** Wireshark  
**Tool #2:** File Explorer  
**Tool #3:** Event Viewer  
**Tool #4:**  
**Tool #5:**

## Project Plan (Required)

**Project Plan:** Draft a plan for completing your project on time. Who is doing what? When is the next step due? How will you get from here to your goal?

Milestone 1 will be completed by 11/21  
Milestone 2 will be completed by 11/28  
Milestone 3 will be completed by 11/28

We will all be meeting up in person and parsing out the steps in each milestone until the document and project has been completed. Susanne will be picking the tools we use, Max will be leading the analysis and Tania & Sienna will be doing the initial research and helping with analysis.

## Stretch Feature: Custom Playbook (Optional)

If you have chosen to write or modify a playbook, document it here.

Tip: To link your drafts, we recommend using Google Drive files. **Be sure any linked files are set to “Anyone with the link can View”!** If the grading team cannot open your file, you **will not get credit** for this stretch feature.

**Original Playbook:** The original playbook we started with / used as inspiration:

**Our Playbook:** Our modified playbook for The Data Dig: (Can be a WIP, but clear differences should be visible from the Original Playbook)

**Description of Changes:**

## Milestone Workbook (Optional)

Please use this space to brainstorm, draft, share resources, and otherwise plan out your project!

---

## Submission Checklist

👉 Check off each of the features you have completed. **You will only be graded on the features you check off.**

### Required Features

- ☒ Select one (or more) open-source Datasets to analyze
  - ☒ Data Set Chosen (Name & Link)
  - ☒ Data Set Description
  - ☒ 3 Hypotheses Made
- ☒ Select an incident response playbook to follow
  - ☒ Playbook Chosen (Name & Link)
  - ☒ Playbook Description
  - ☒ 2+ Tools Identified
- ☒ Draft a Project Plan to track your progress

### Stretch Feature

- ☐ Customize a playbook to fit your dataset / scenario

- ☐ Original/Inspiration Playbook Link
- ☐ Custom Playbook Link
- ☐ Description of Changes

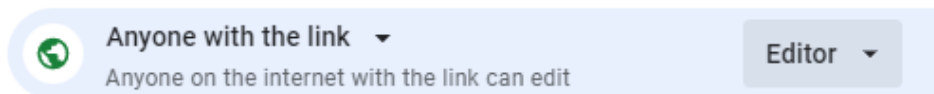
## Submit your work!

Step 0: **Decide** which group member will submit! **Only one person should submit the milestone** each unit – So make sure everyone's names/emails are on this document!

Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit. (This allows our grading team to input your grade below!)



General access



Step 2: **Copy** the link to this document.



Step 3: **Submit** the link on the portal.

## Grader Comments

*Once your project has been assessed, our graders will leave feedback for you in this space. Please do not delete.*

## Grading Rubric

Required Features	Total Received	Total Possible
-------------------	-------------------	-------------------

Select one (or more) open-source Datasets to analyze		6
Select an incident-response playbook to follow		6
Draft a Project Plan to track your progress		4
<b>TOTAL</b>		<b>16</b>
Stretch Features	Total Received	Total Possible
Customize a playbook to fit your dataset / scenario		+3
<b>Total Possible Points</b>		<b>16 (+3)</b>

### Grader Feedback

### References

Garg, P. (2023, June 30). *LR Parsing*. Coding Ninjas. Retrieved February 13, 2024, from

<https://www.codingninjas.com/studio/library/lr-parsing>

Jain, S. (2021, March 31). *LR Parser*. GeeksforGeeks. Retrieved February 13, 2024, from

<https://www.geeksforgeeks.org/lr-parser/>

### References

*Disjoint of Sets using Venn Diagram | Disjoint of Sets | Non-overlapping Sets*. (n.d.). Math Only

Math. Retrieved February 13, 2024, from

<https://www.math-only-math.com/disjoint-of-sets-using-Venn-diagram.html>

Garg, P. (2023, June 30). *LR Parsing*. Coding Ninjas. Retrieved February 13, 2024, from <https://www.codingninjas.com/studio/library/lr-parsing>

Jain, S. (2021, March 31). *LR Parser*. GeeksforGeeks. Retrieved February 13, 2024, from <https://www.geeksforgeeks.org/lr-parser/>