Lab 3- How to use MITRE ATT&CK Navigator

Elaborated by:
Leandro Delgado
114416241

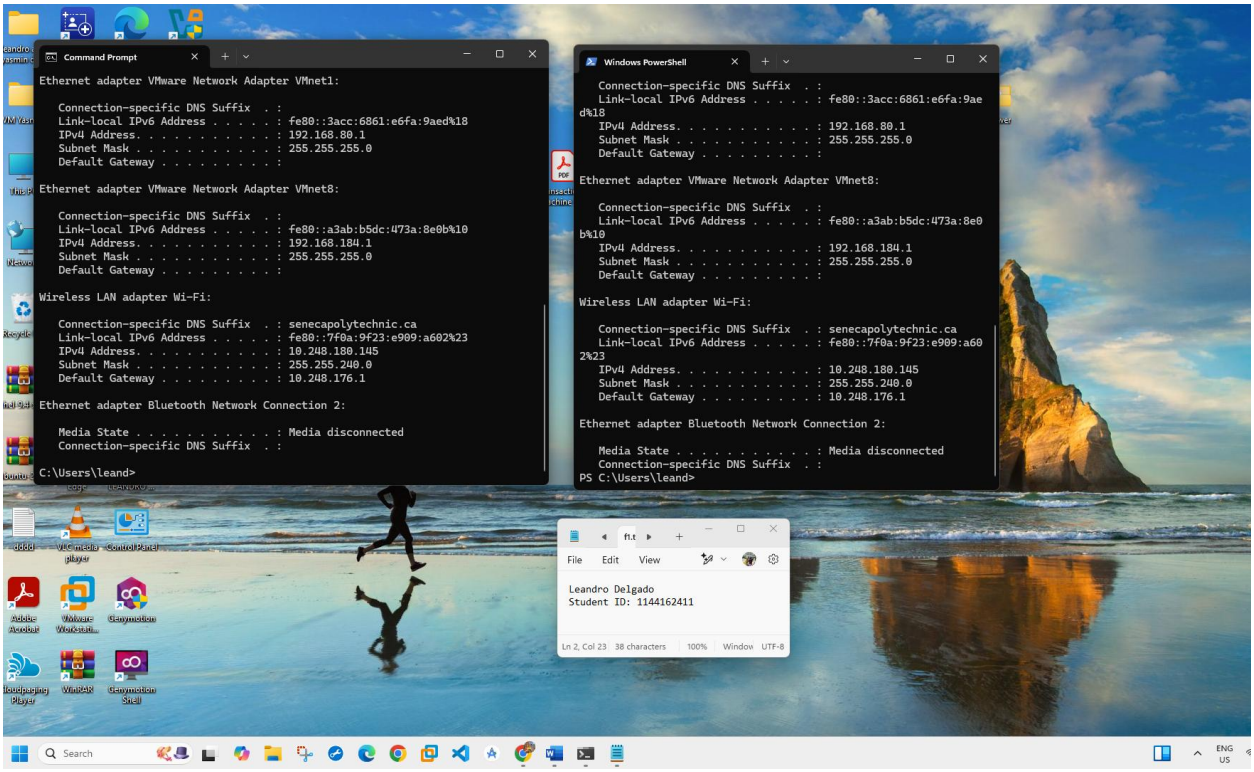
Tatiana Outkina
CYT-250/Threat Investigation

I hereby confirm that this submission is my original work and complies with Seneca College's Academic Integrity Policies.

CYT250 Lab3 Winter 2025 – 4%

Individual work

Preparation - Step 0. At the start, make screenshot of the starting screen. The screenshot must contain indication of the laptop ownership (like user name).



Note from the Article “How to use MITRE ATT&CK Navigator: A step-by-step guide”, by Kurt Ellzey

Sorting through information can be a difficult task at the best of times. When you are dealing with a literal mountain of actionable data like the MITRE ATT&CK Knowledge Base, just picking a starting point can be a tough job. Fortunately, MITRE has created the MITRE ATT&CK Navigator— a tool for searching across the entire KB and bringing together particular attack types and custom notations for organizations. ©

Objectives:

- **Familiarize yourself with the content of the MITRE ATT&CK Navigator tools**

Sources of information:

Links to locate the Navigator on github:

https://github.com/mitre-attack/attack-navigator

Link to see what is "layer" in attack navigator and "sample layer"

attack-navigator/layers at master · mitre-attack/attack-navigator · GitHub

Link to Web-based version of Navigator

https://mitre-attack.github.io/attack-navigator/

Link to the video and learning tools for this Lab 3.

Introduction to ATT&CK Navigator - YouTube

Additional information

How to use the MITRE ATT&CK Navigator - YouTube

https://resources.infosecinstitute.com/topic/how-to-use-mitre-attck-navigator-a-step-by-step-guide/

Local installation (optional)

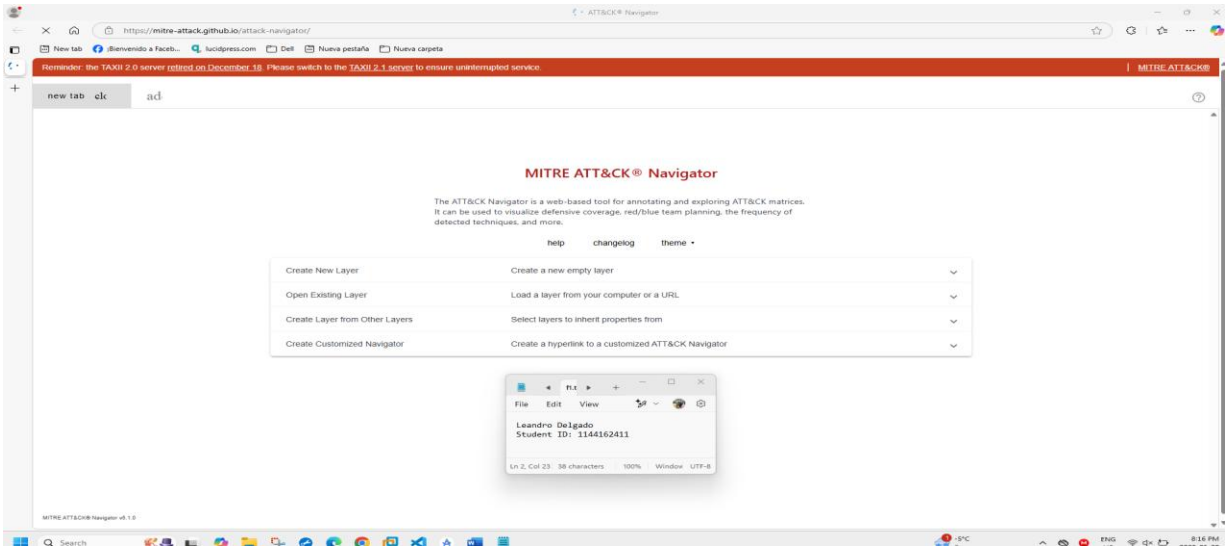
MITRE ATT&CK Series: ATT&CK Navigator Local Installation - YouTube

Latest release

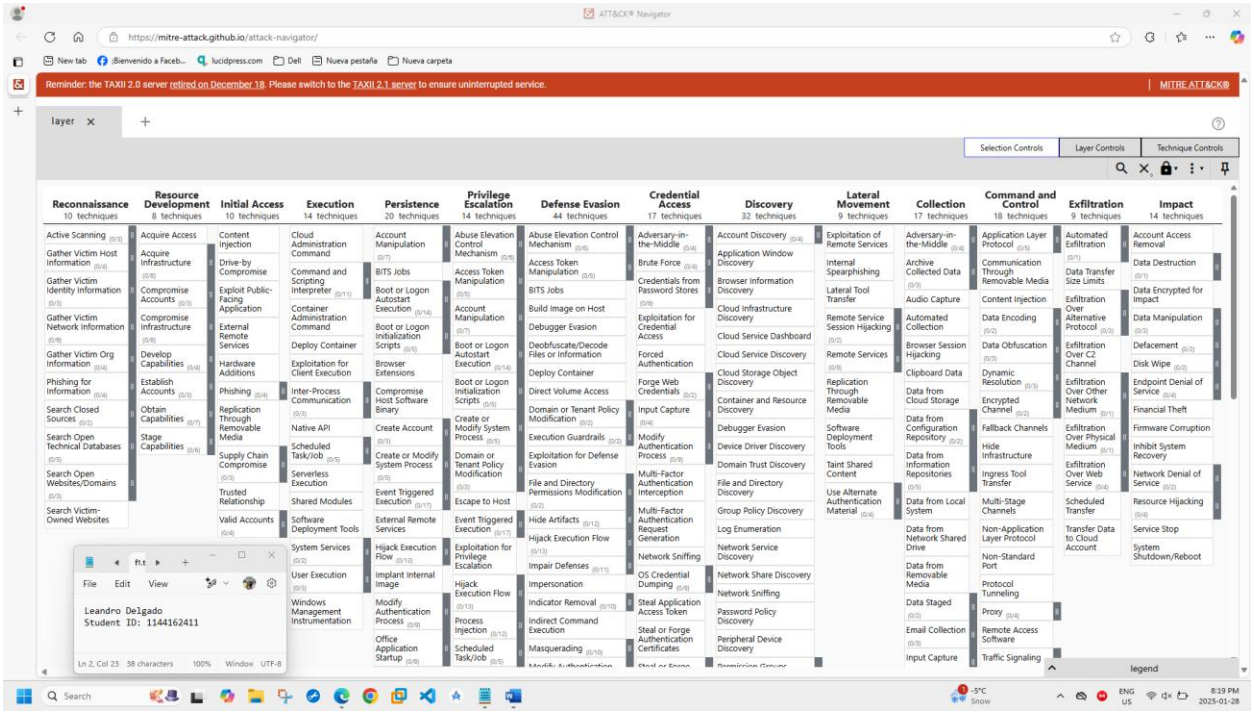
Release attack-navigator v5.1.0 · mitre-attack/attack-navigator · GitHub

Task description:

1. **Read the text from GitHub. When you connect to the GitHub site you see the following screen. Text is located under "help".**

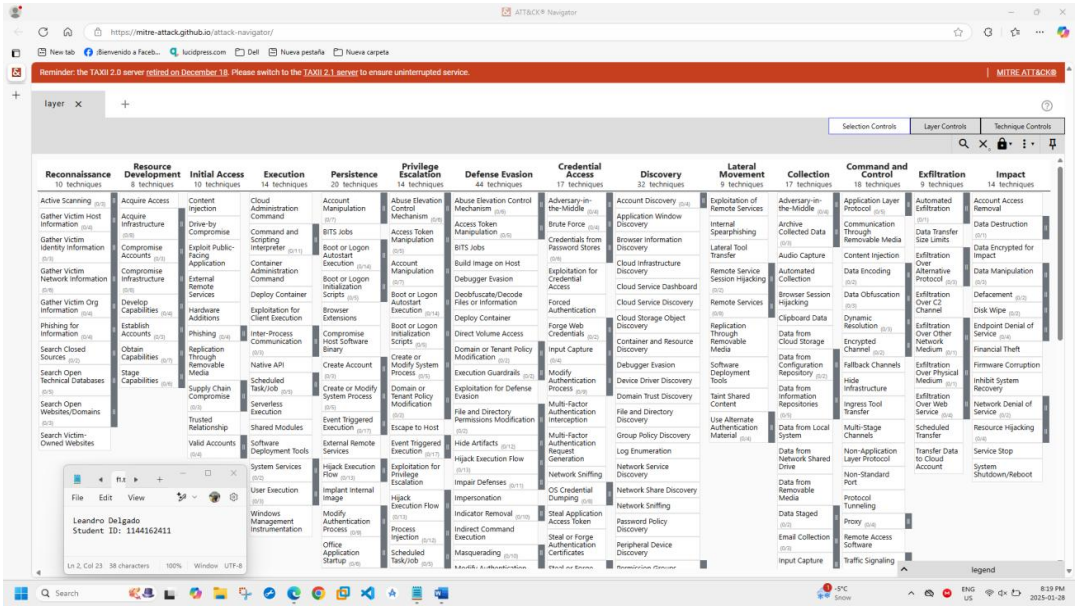


2. **Watch the video, where the Navigator functions are explained.**
3. **Start Navigator on your computer or use Web Interface. Play with the functions to capture the Navigator capabilities.**
4. **Implement the following Use Cases on your computer**
   - **Create new lay**



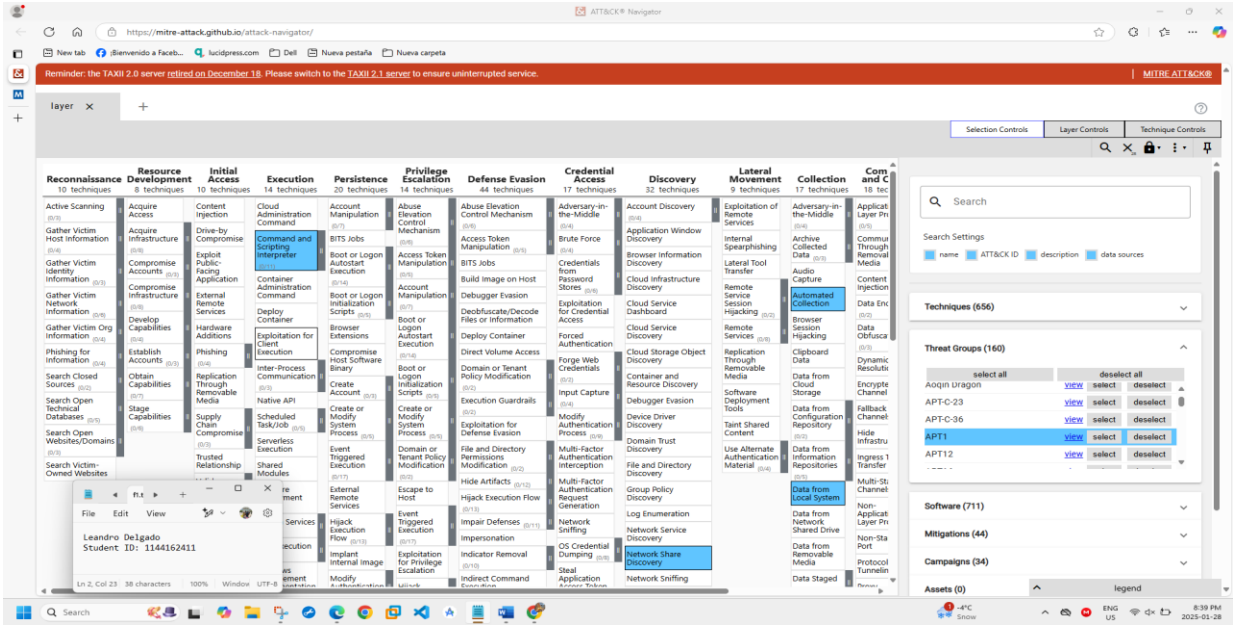
I created a new layer by clicking “New Layer” and selecting the appropriate matrix. The tool automatically displayed the standard techniques, and then I added specific tactics, focusing on initial access. I was surprised at how easy it was to visualize and organize everything.

- **Open existing layer**



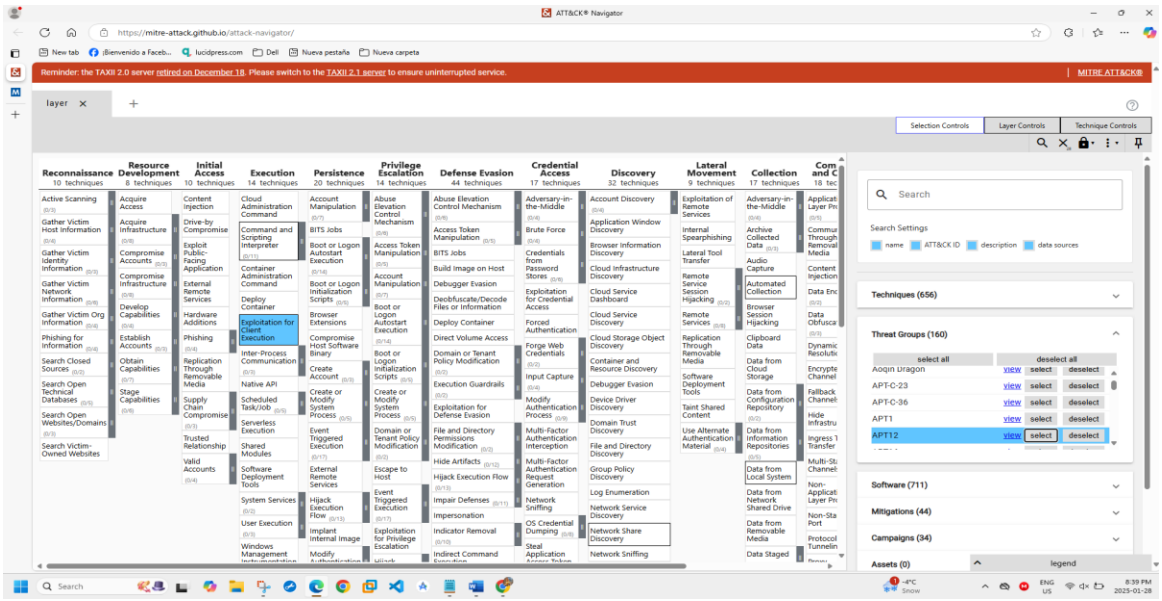
I opened an existing layer using the "Open Layer" function and selected a saved one I had worked on before. This made it easy to pick up where I left off, adjust the matrix, and continue my analysis without starting from scratch.

- **Create layer from other layers**

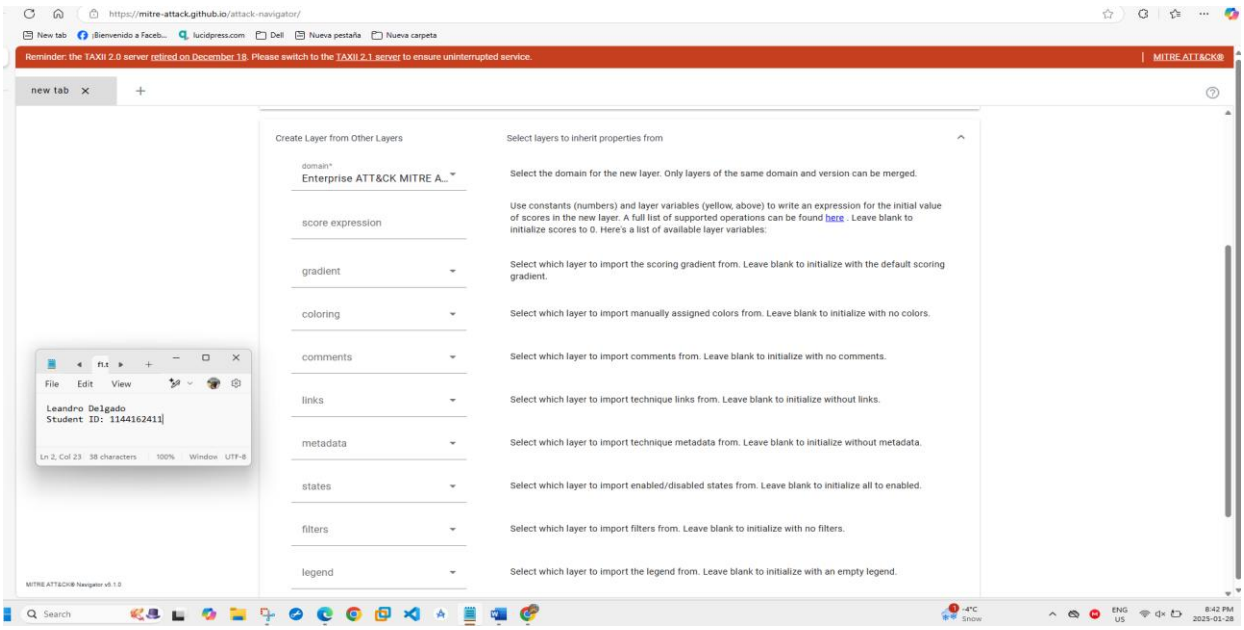


The video guided me to merge two existing layers using the "Create from layers" option. It was a great way to compare attack techniques between different threat groups and spot common tactics briefly.

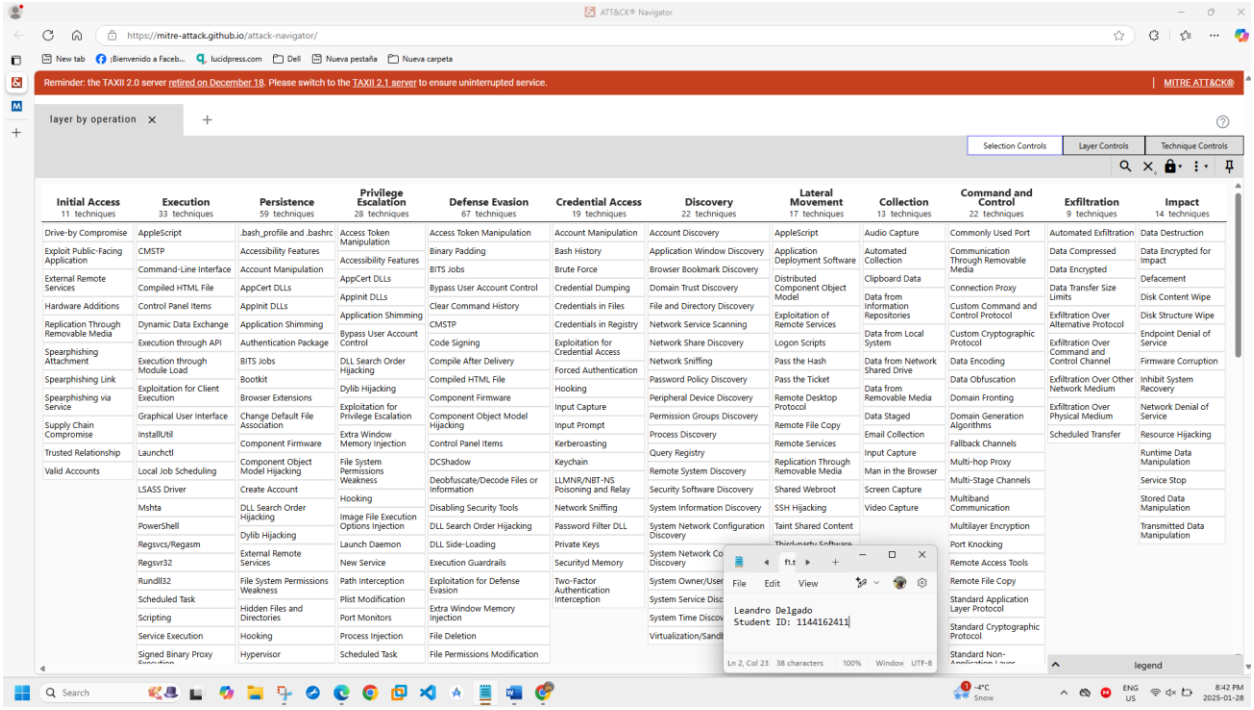
Do that, assuming that you are in need to compare technics which are utilized in 2 groups, for example APT19 and APT33. Actually, you can take any 2 groups, but not the same as used in the video.



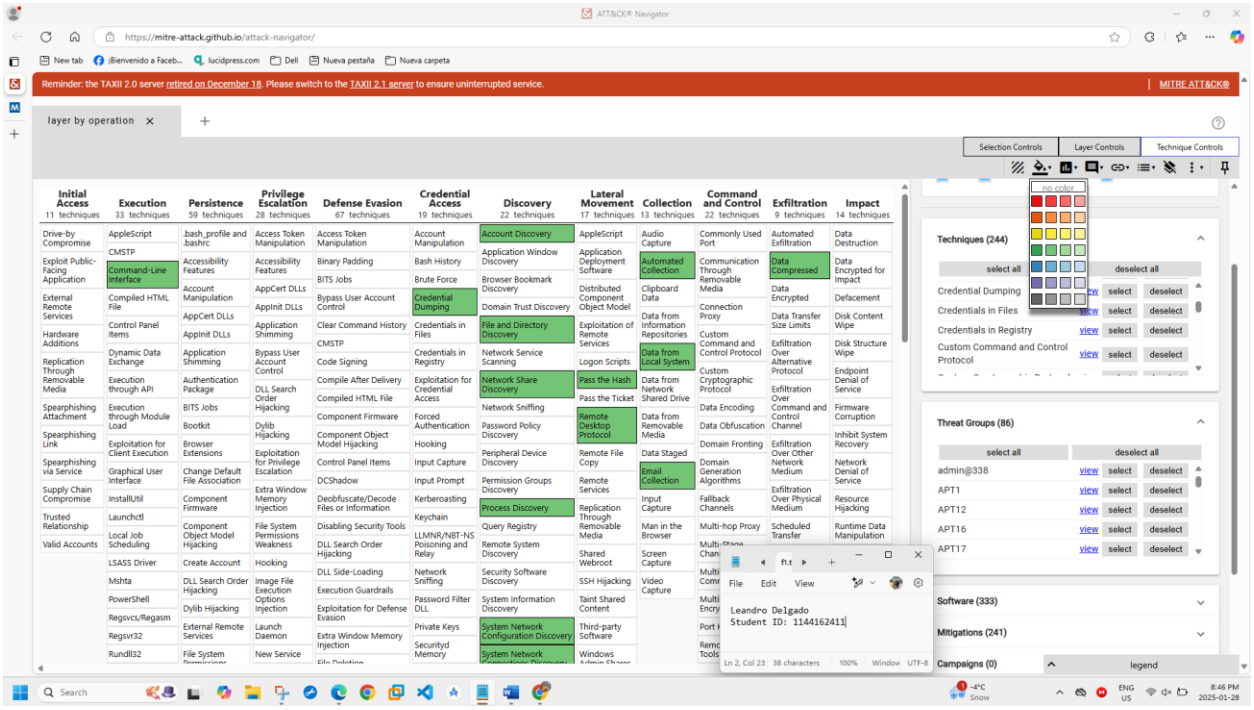
This MITRE ATT&CK Navigator view compares APT1 and APT12, making it easy to spot similarities in their attack methods. It’s a great way to understand how different threat groups operate.



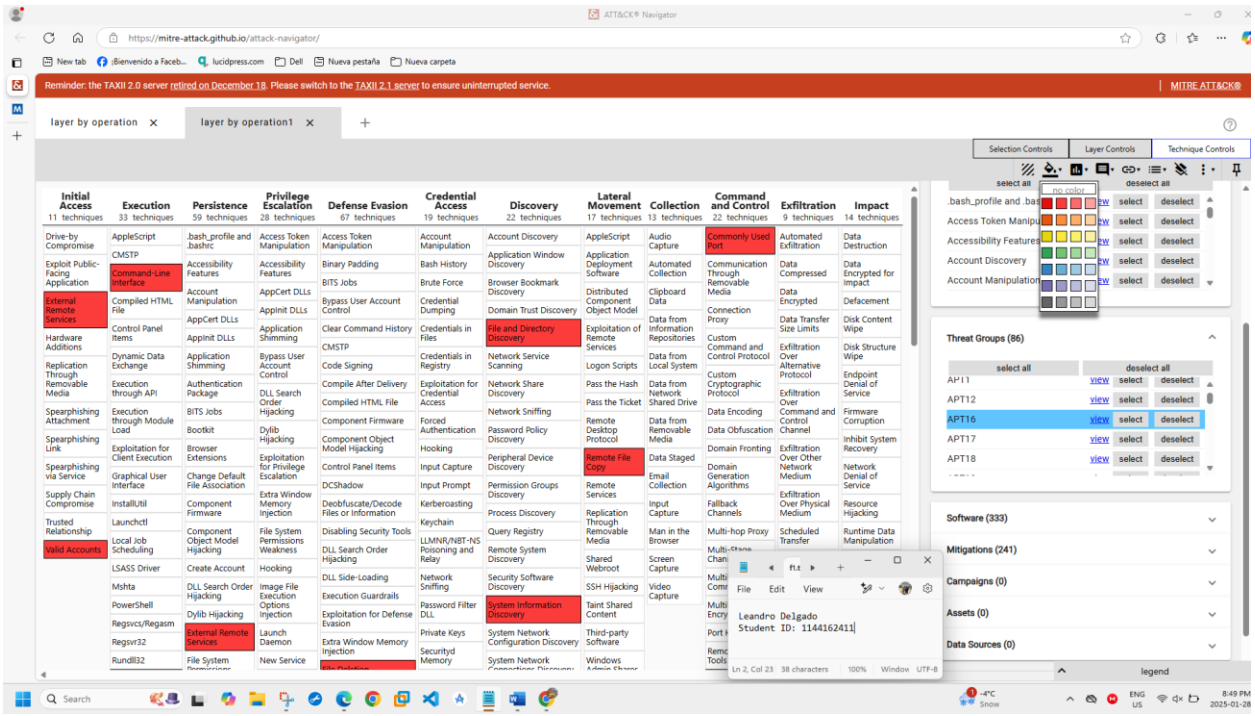
This screenshot shows the "Create Layer from Other Layers" feature in MITRE ATT&CK Navigator, letting you merge data while keeping key details like scoring, colors, and comments. It’s a handy way to compare attack techniques across different groups.

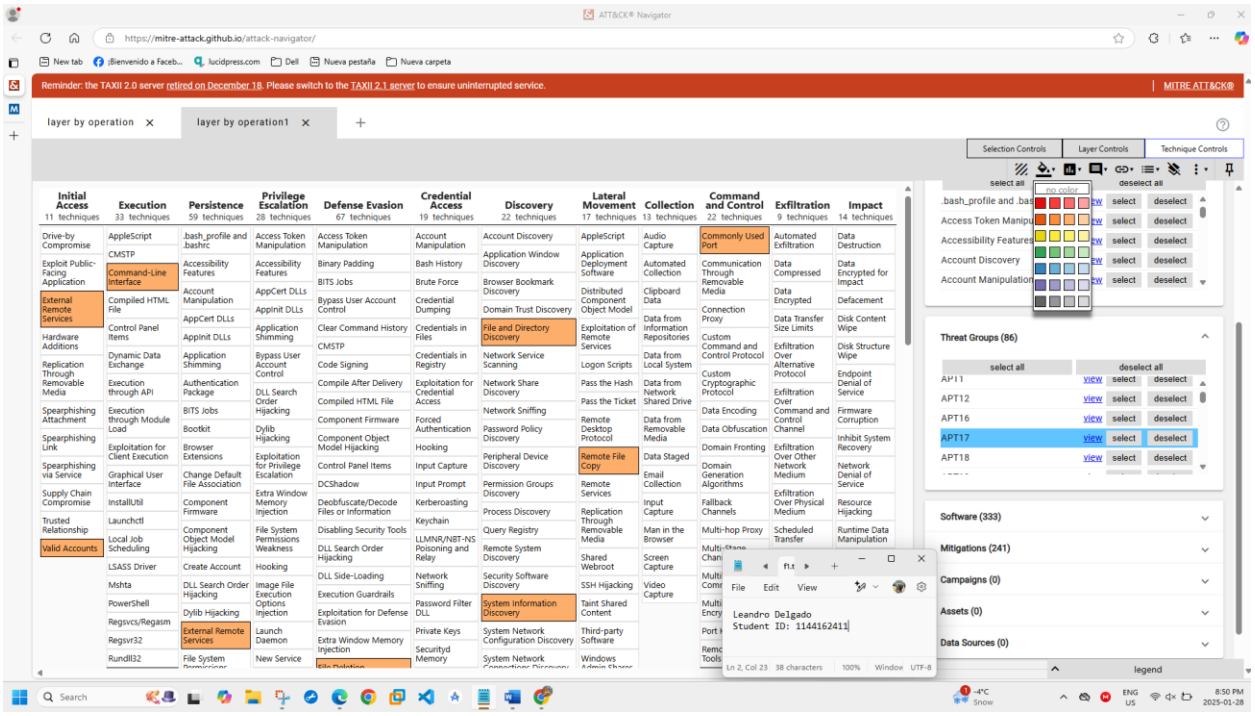


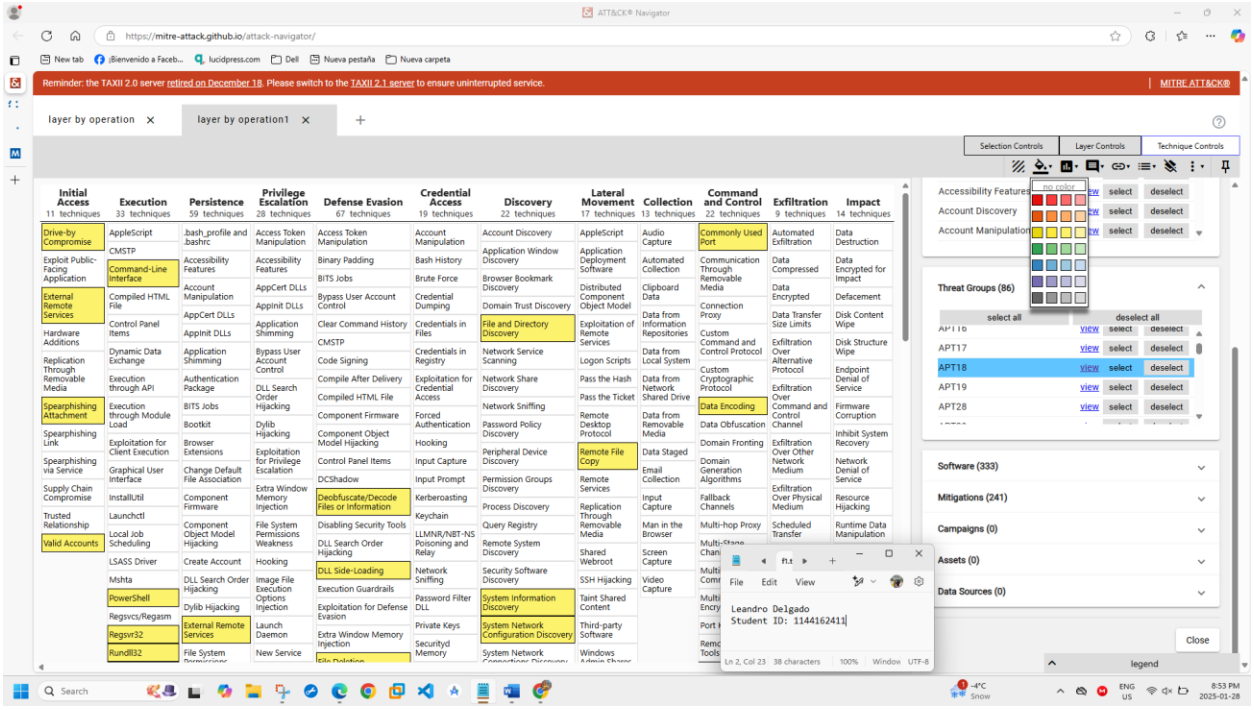
This MITRE ATT&CK Navigator view shows a full matrix of attack techniques, helping to map and analyze adversary tactics. The Selection, Layer, and Technique Controls make it easy to filter and customize the view

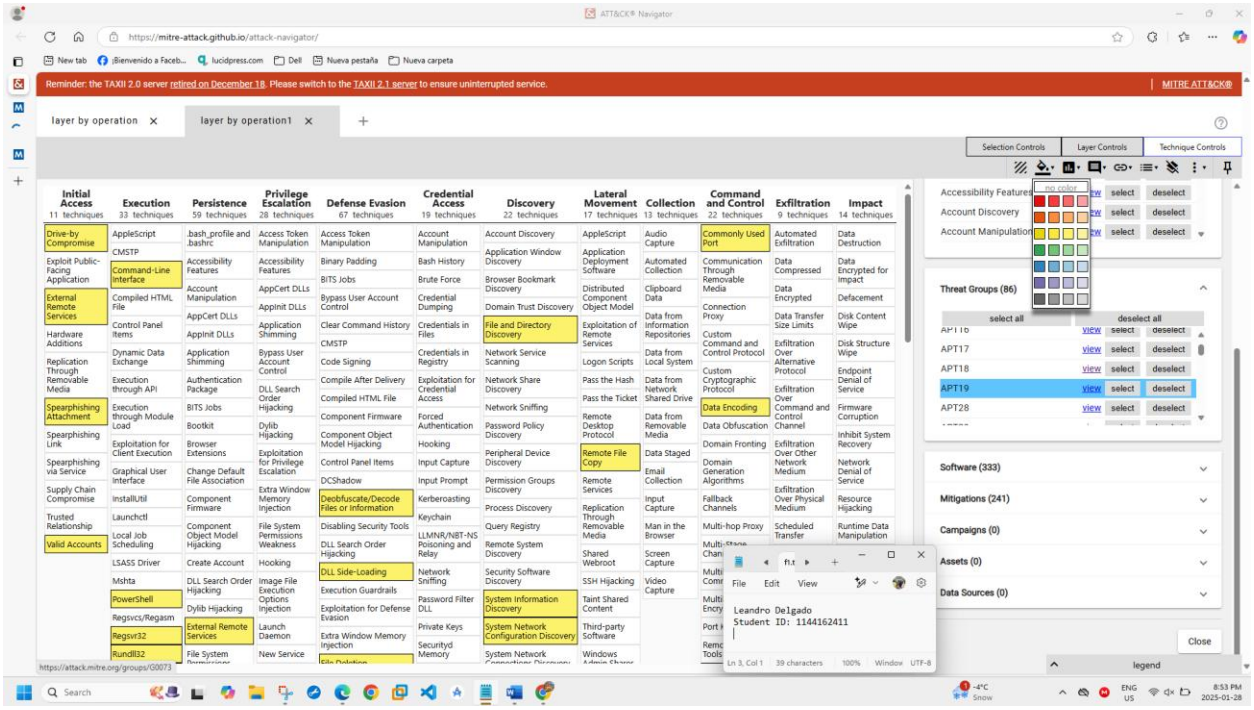


I selected **APT16, APT17, APT18, and APT19** and modified their colors to distinguish them from previous selections. This made it easier to compare their techniques and identify similarities and differences in their attack strategies.









Summary: Using ATT&CK Navigator was a great experience—it made it easy to see how different threat groups operate and spot patterns in their tactics. Exploring its features gave me a better understanding of cyber threats and how to strengthen defenses. I'm excited to keep learning and improving my skills as the course progresses.