MOBIA

MOBIA is a business technology integrator with over thirty years of experience and 500+ employees across Canada and USA. Our talented bench of technical engineers and trusted advisors deliver process improvements and business transformations within our core pillars of Cloud, Infrastructure, Software Development, Cybersecurity and Broadband & Wireless Services.

Our inside-out approach allows us to understand business challenges from deep within the organization, mapping the impact as it ripples outward. This insight enables us to create future-proof solutions that maximize results and repeatedly exceed our client's expectations.

Adversary Simulation Workshop

Lab Guide:
Mitre ATT&CK and Atomic Red Team

Objective:

Use the Mitre ATT&CK Navigator to create a layer that shows how well Atomic Red Team tests cover the techniques in the Mitre ATT&CK Matrix.

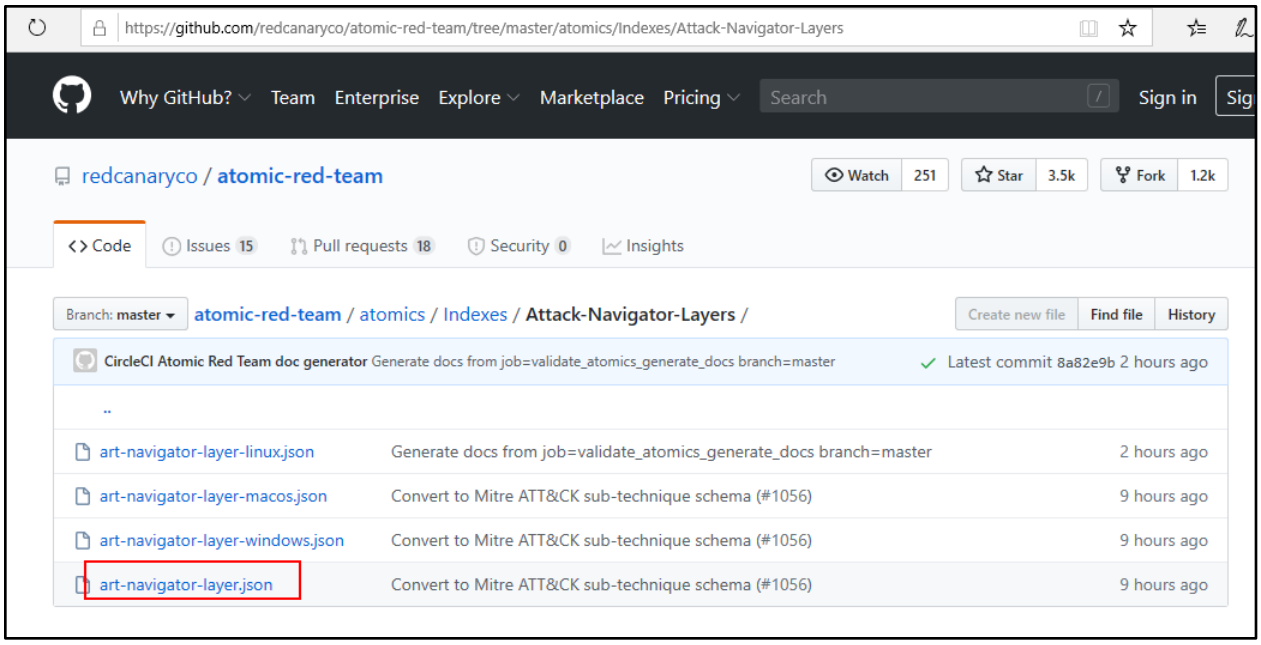
Instructions:

We are going to create a layer that will show the techniques and sub-techniques that have associated atomic tests in the Atomic Red Team project. The Atomic Red Team project publishes Mitre ATT&CK Navigator layers that describe their atomic test coverage across all techniques and operating systems.

We need to get a link to a JSON file containing the layer information. The Atomic Red Team project provides an automatically generated version of the JSON data which always matches the current release. Open another tab on your browser and navigate to the Atomic Red Team Github page, click on the "atomics" folder link, and then "Indexes", and then "Attack-Navigator-Layers".

Bookmarks→ ART→ Main GitHub

Bookmarks→ ART→ Atomics Folder



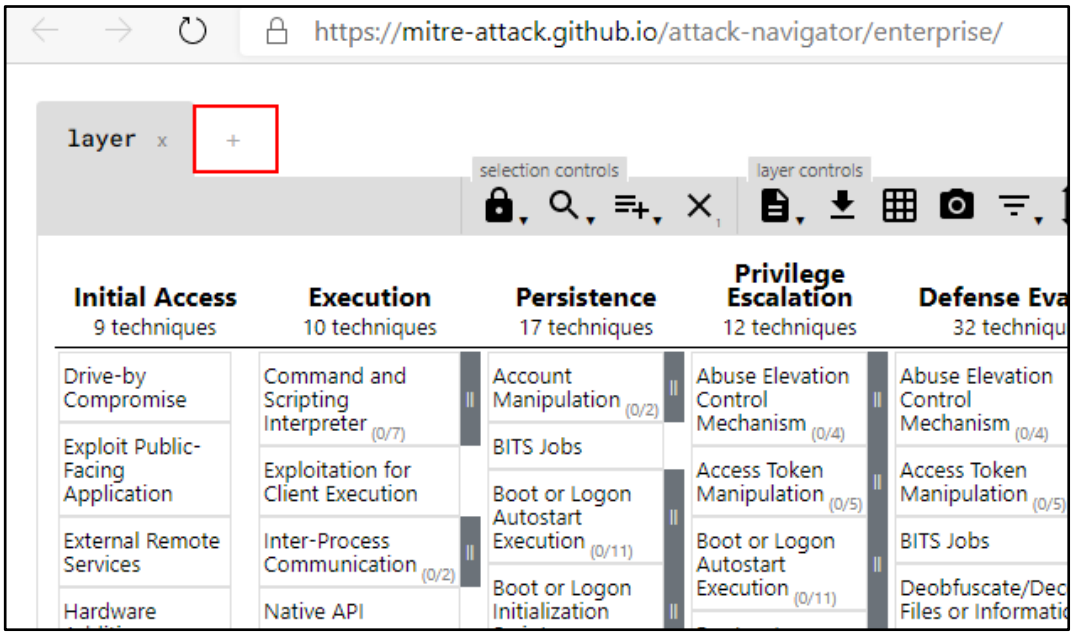
There are four JSON files in this folder that represent the atomic tests that exist within each T# for Linux, macOS, Windows, and finally for all combined. We are going to create a layer for each of these JSON files. First, click on the "art-navigator-layer.json" link, highlighted above.

To use the layer information in this JSON file, we will need to get a direct link to the raw data for each file, so click on "Raw" and save a copy of each URL to the raw data for later use when creating our Navigator layers.

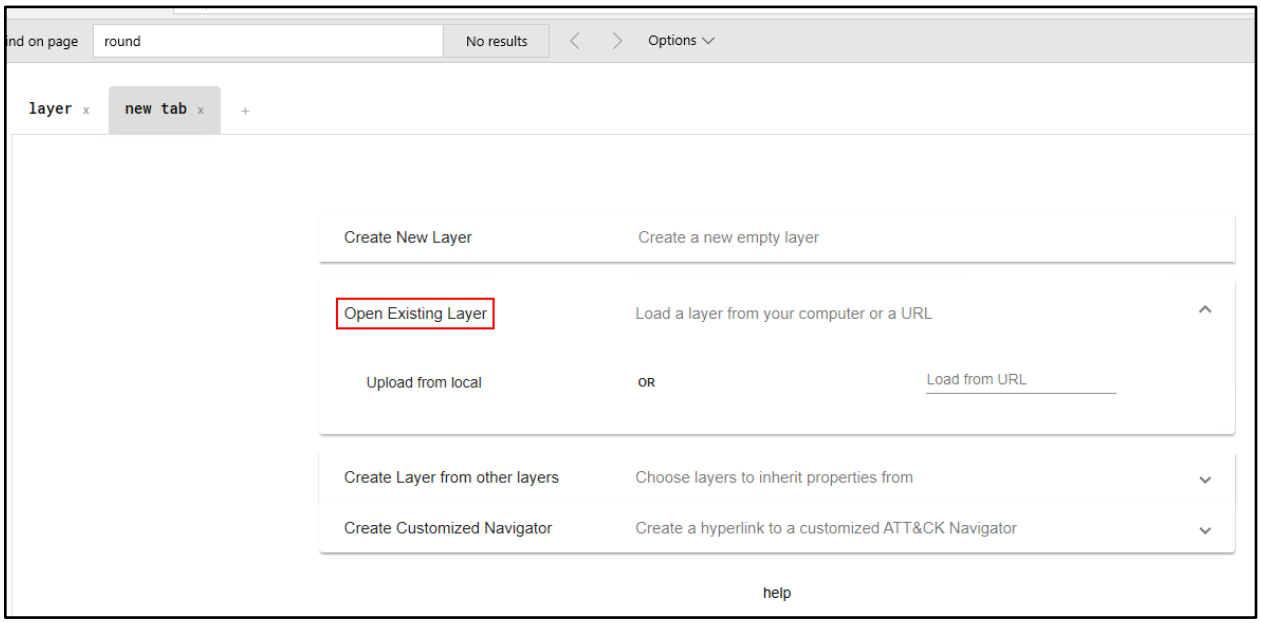
The links you should have discovered for each layer are listed in the table below.

All Operating Systems	https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/Indexes/Attack-Navigator-Layers/art-navigator-layer.json
Windows	https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/Indexes/Attack-Navigator-Layers/art-navigator-layer-windows.json
Linux	https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/Indexes/Attack-Navigator-Layers/art-navigator-layer-linux.json
macOS	https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/Indexes/Attack-Navigator-Layers/art-navigator-layer-macos.json

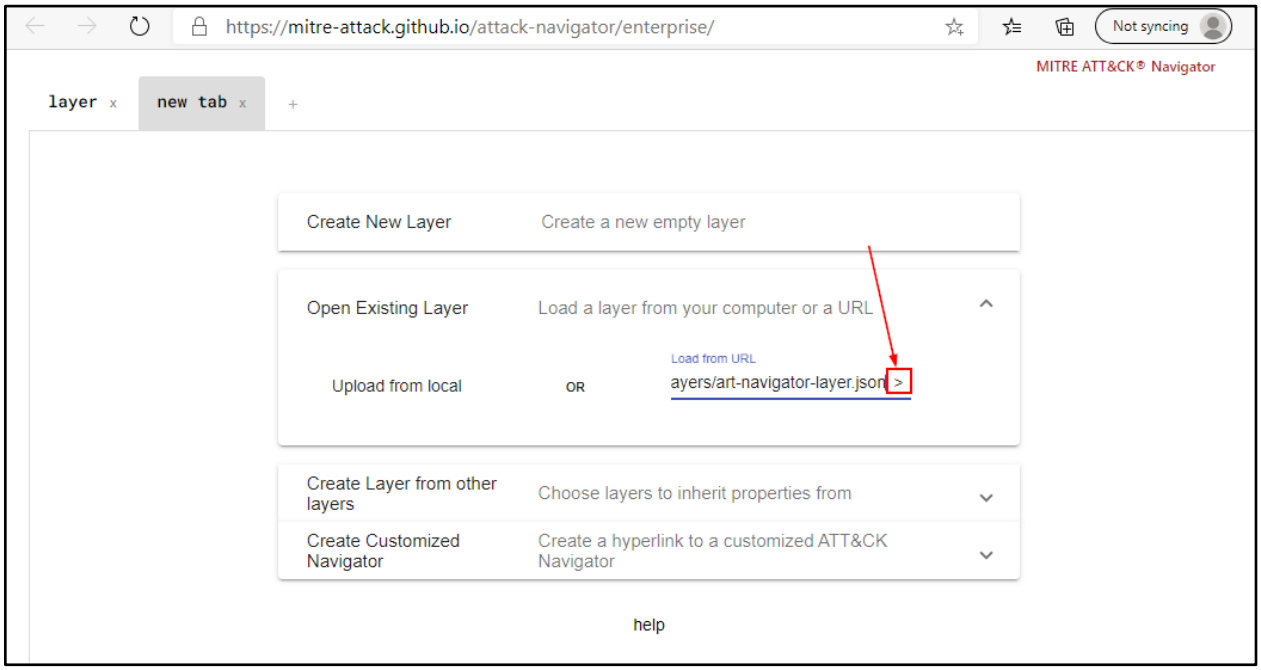
Open the Mitre ATT&CK Navigator and Click on the "+" sign to add a new layer.



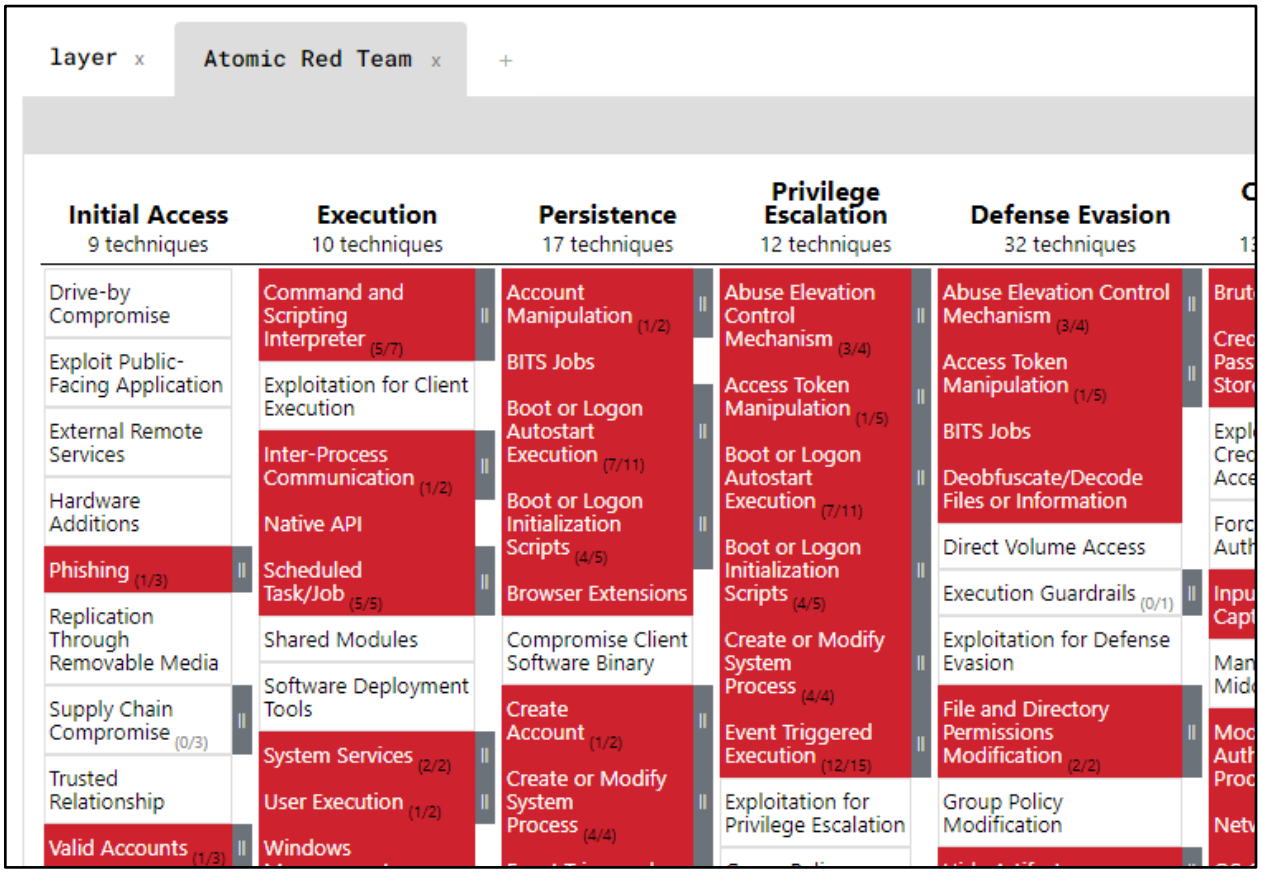
Click on "Open Existing Layer"



Paste [the link] we copied in to the “Load from URL” line. In order to load this layer, you need to click on the “>” symbol at the end of the line after you paste the URL.



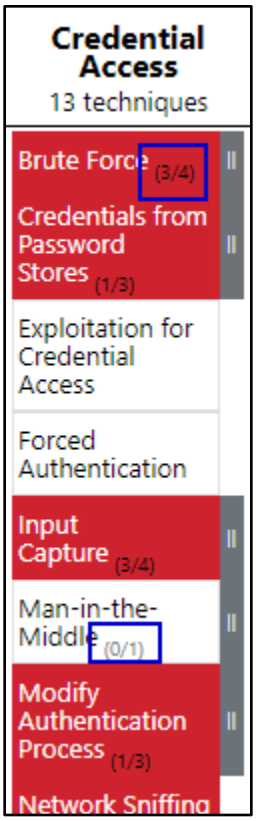
Your new “Atomic Red Team” layer will load with the techniques that have at least 1 atomic written for them shown in red.



This layer is named “Atomic Red Team”. This layer highlights all of the techniques that have at least one atomic test written for it.

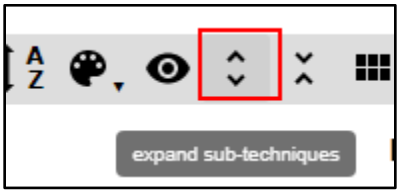
Remember in previous labs we found out how to find if a technique has sub-techniques? The techniques with sub-techniques have the gray bar on the side. On these techniques there are also numbers in parenthesis. The numbers give an indication of how many of the sub-techniques have atomics.

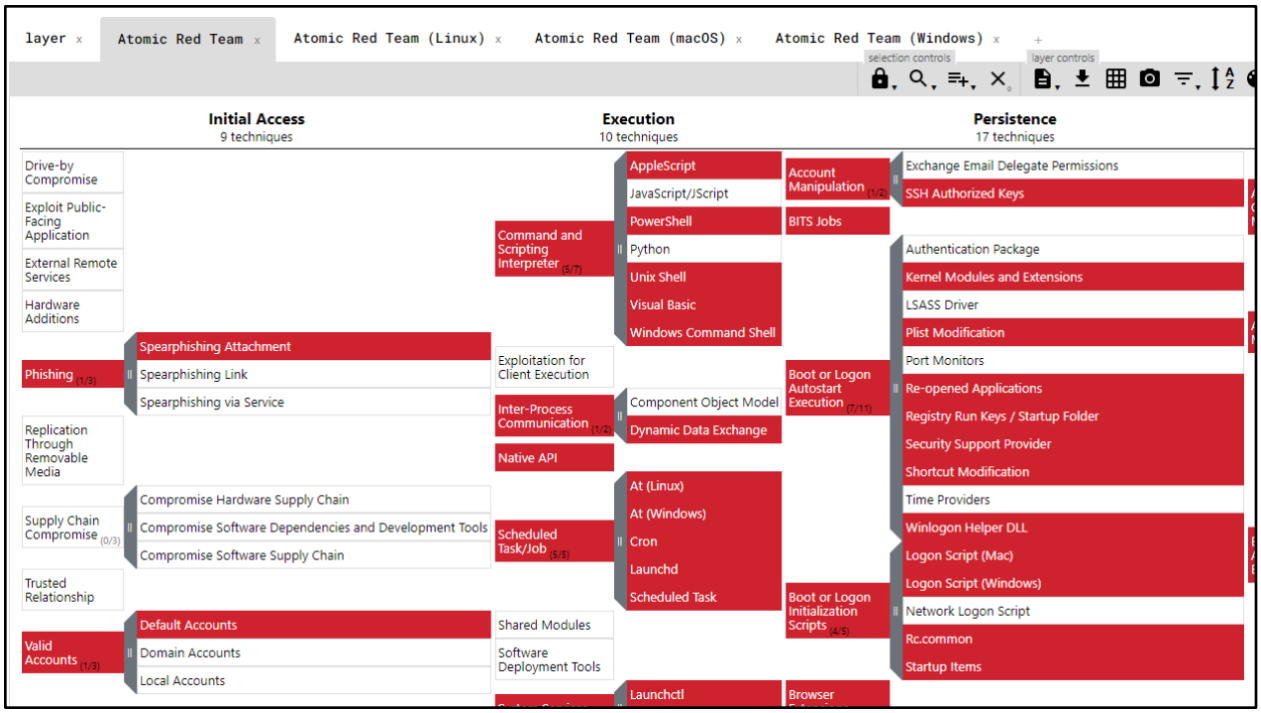
Look at the techniques under the tactic “Credential Access”.



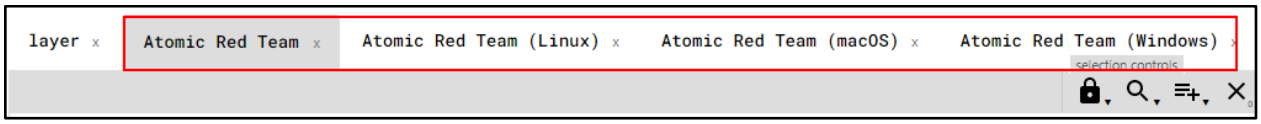
The technique “Brute Force” has three out of four sub-techniques with associated atomic tests. The technique “Man-in-the-Middle” has zero out of one.

In addition to looking at these numbers, you can expand the sub-techniques by clicking on the “expand sub-techniques” button.





Repeat the above steps to create a layer for the remaining three JSON files. When you are done, you should have four layers representing Atomic Red Team coverage as shown below.



The names of the layers will indicate which group of atomics you are looking at. Take some time to compare the different layers to each other. As you can see, Windows has the most atomics written for it but the coverage for Linux and macOS isn't bad.

The nice thing about creating a layer from a URL is that you can share the link to the layer with others and every time it loads, it will grab the latest layer information published by Atomic Red Team. This means that you are always looking at the most up to date information. The links to each layer are included below for your convenience.

- All Operating Systems
- Windows

- Linux
- macOS

Bookmarks→ Mitre ATT&CK→ ATT&CK Navigator ART Coverage

This lab showed you how you can add overlays to the Navigator to visualize coverage of the Mitre ATT&CK space. The coverage could be used to show your testing and/or detection coverage or it could show techniques used by specific APT groups. You can create your own layers or combine layers as well.

End of Lab