Tevora's Execution Engine Streamlines Atomic Red Team Tests

Atomic Red Team is an excellent collection of commands, activities, and other Indicators of Compromise (IoCs), developed and maintained by Red Canary, that your blue team can benchmark against to hone their craft. We've loved using the Atomic tests as a reference and have developed a GUI-based execution engine to run through them automatically on Windows. This blog covers installation and execution of our Atomic Red Team execution engine. You can find more details on Atomic Red Team and the Atomic tests at https://atomicredteam.io/.

To skip the blog and get the execution engine right away, go to https://github.com/tevora-threat/atomic_red_team_gui.

Atomic Red Team Overview

The Atomic Red Team project is an open-source collection of behavior definitions mapping to the MITRE ATT&CK framework maintained by Red Canary. Red Canary describes the Red Team tests as "small, highly portable detection tests mapped to the MITRE ATT&CK Framework. Each test is designed to map back to a particular tactic. This gives defenders a highly actionable way to immediately start testing their defenses against a broad spectrum of attacks."

You can use the Atomic tests to generate IoCs and test your team's ability to detect and respond to them.

Tevora Execution Engine

Tevora developed a GUI-based execution engine for attack definitions in the Atomic Red Team project. It allows you to define Atomic tests and automatically execute them in a Windows environment. The execution engine generates a test plan and report based on the defined tests and creates basic logging of the activity performed.

Installation

The Tevora Atomic Red Team execution engine needs two components:

1. The folder of Atomic definitions
2. The Tevora Execution Engine Executable

To run the red team simulation, follow the Installation Steps below to open the Execution Engine exe and configure it to point at the directory in which the Atomic definitions are stored.

Installation Steps:

1. Open the .sln file in visual studio and compile the exe.
2. Download the Atomic tests (atomics) you wish to run from https://github.com/redcanaryco/atomic-red-team/tree/master/atomics.
3. Select a system to run the tests on.
    a. Tevora recommends running the tests on a standard newly-provisioned employee workstation with normal EDR/AV software installed in detect only mode.
        i. If AV is deployed in block mode, it may interfere with being able to run the execution engine. Tevora recommends running in detect mode to see what would have been blocked without causing issues running the test.
    b. If possible, Tevora recommends running in a VM, taking a snapshot before running the execution engine for easy reversion.

c. Some atomics are destructive in that they add things such as registry autoruns without cleaning up. We recommend reverting from a snapshot, which is an easy way to ensure tests are run on a clean platform each time.

d. For this same reason, Tevora recommends not running this tool on production systems unless: (1) careful tuning and removal of destructive atomics is done, or (2) only a few atomics that are known not to modify the system are run.

4. Extract the zip folder to a location of your choosing.
5. The atomic red team execution engine is now ready to be run.

Execution

1. Open the compiled redsim .exe file.
2. Select "Load Atomics" from the bottom right context menu.
3. Navigate to the unzipped directory and open the atomics folder, or select a customized folder of atomics.
   a. At this point the Atomic Red Team Execution Engine GUI should populate with the loaded atomics.
4. The red team execution engine will output results of its runs. To designate where these will be saved, select the "Output Directory" output and select a folder.
5. (optional) If you want to export a plan of what commands are going to be run, select "Export Test Plan" from the bottom right menu. This will be saved to the "Output Directory" location.
6. After reviewing the loaded atomics, and confirming the test plan, click "Execute Atomics".

a. The tests are now executing, and the progress bar at the bottom will record which tests are currently running and how many remain to be run.

b. As each test is run, the execution engine will log the results to a csv file timestamped to indicate when each IOC occurred.

7. Once testing has completed, review the csv of the test log in the output folder.

Review

After running the automated simulation, many IoCs should have been generated. Review the results from your SOC, EDR solution, SIEM, and other security monitoring tools to understand what was caught and what was not. The CSV output file should contain sufficient detail, including the date and time each command was performed, to cross reference with security alerts or logs.

A key element of this process is to identify areas that were NOT caught by the automated simulation, and to drill down to understand why. Ultimately, the goal of running this simulation is to identify areas of weakness in your security monitoring program and improve them. Once you've identified areas that were NOT detected, remediation should be performed to ensure they will be detected, and tests should be re-run to confirm that they are detected.

Although the automated red team sim is a great tool to assess the state of current detection capabilities and to improve them, it is important to not limit your security detection and response program to one that only uses the defined Atomic Red Team simulations. You should perform periodic manual red teaming and IOC generation to assess new risks and to address a changing threat

posture. Additionally, Tevora recommends periodically reviewing and updating IoCs to reflect current threat actors.