GitHub - dstepanic/attck_empire: Generate ATT&CK Navigator layer file from PowerShell Empire agent logs

By Daniel Stepanic

Archived: 2026-04-06 01:10:06 UTC

Overview

Generate ATT&CK Navigator layer files (JSON) based on PowerShell Empire modules used during red team/pentesting engagements. The modules are pulled from each host's agent.log file and mapped to one or more ATT&CK techniques. This can be used as a learning tool for handoffs between red/blue teams as well as part of a final pentest report.

Please note the layer generation portion (gen_layer.py) was developed by the MITRE ATT&CK team and slightly modified in order to output JSON file. A spreadsheet (Empire_modules.xlsx) is included that contains the technique/module mapping for any custom modifications.

Using the script

1. Perform red team engagement using PowerShell Empire, generate agent.log files by compromising hosts and using different modules.
2. Run main Python script (attck_empire.py) in Powershell Empire downloads folder or point to specific agent.log file:

   python attck_empire.py (Searches within sub-directories for agent.log files)
   python attck_empire.py -a C:/tmp/agent.log
3.

Please note, the Navigator hosted instance by MITRE stores and utilizes layer files on the client-side, not server-side. For any internal/sensitive data, it's recommended to use your own instance.

4. Click on the plus sign on top left corner of ATT&CK Navigator page, select "Open Existing Layer" and choose your generated layer file (JSON).
