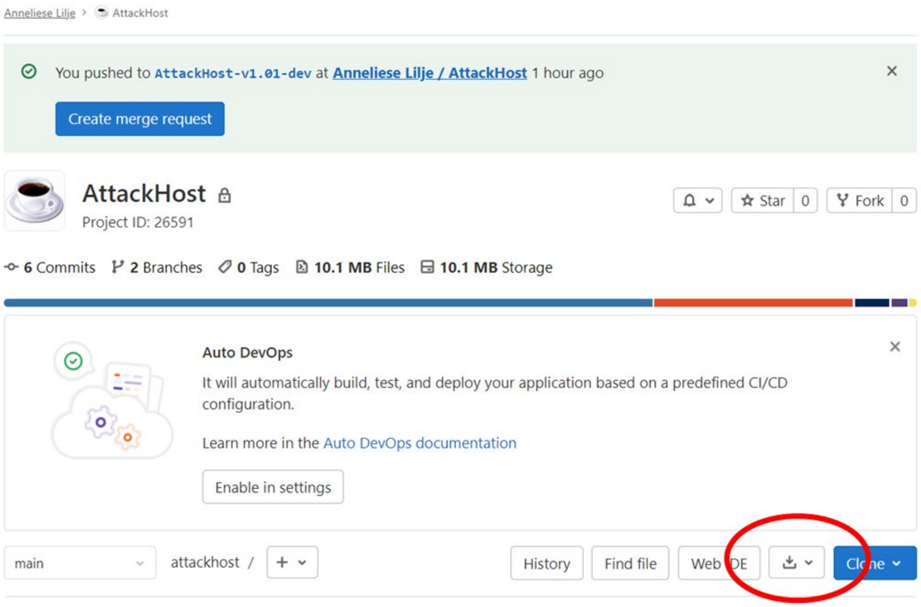
Introduction

Atomic AttackHost is a web-based application that allows users to perform host-based attacks on Windows computers. The current version is 1.01 and this version can be downloaded from the AttackHost-v1.01-dev branch at

https://cee-gitlab.sandia.gov/alilje/attackhost

Installation

To install AttackHost, go to the link above. You should see the following page:



Anneliese Lilje > AttackHost

You pushed to AttackHost-v1.01-dev at Anneliese Lilje / AttackHost 1 hour ago

AttackHost

Project ID: 26591

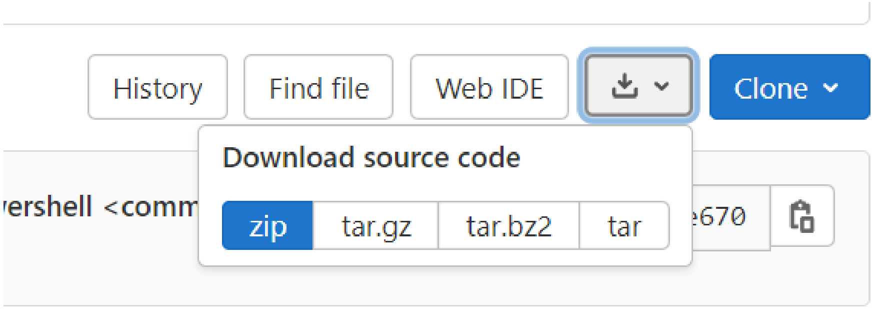
6 Commits 2 Branches 0 Tags 10.1 MB Files 10.1 MB Storage

Auto DevOps

It will automatically build, test, and deploy your application based on a predefined CI/CD configuration.

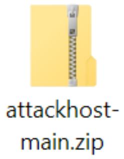
Learn more in the Auto DevOps documentation

You can download the application directly (see button within red circle above.). You will have a choice of several types of files:

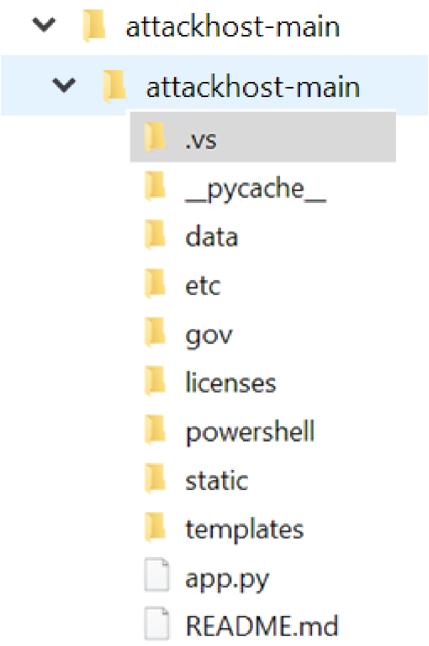


Download source code

If you select to download a .zip file after the download you should have a file named attackhost-main.zip in your directory:



Unzipping this file, you will then see the following directory tree:



```
attackhost-main
  attackhost-main
    .vs
    __pycache__
    data
    etc
    gov
    licenses
    powershell
    static
    templates
    app.py
    README.md
```

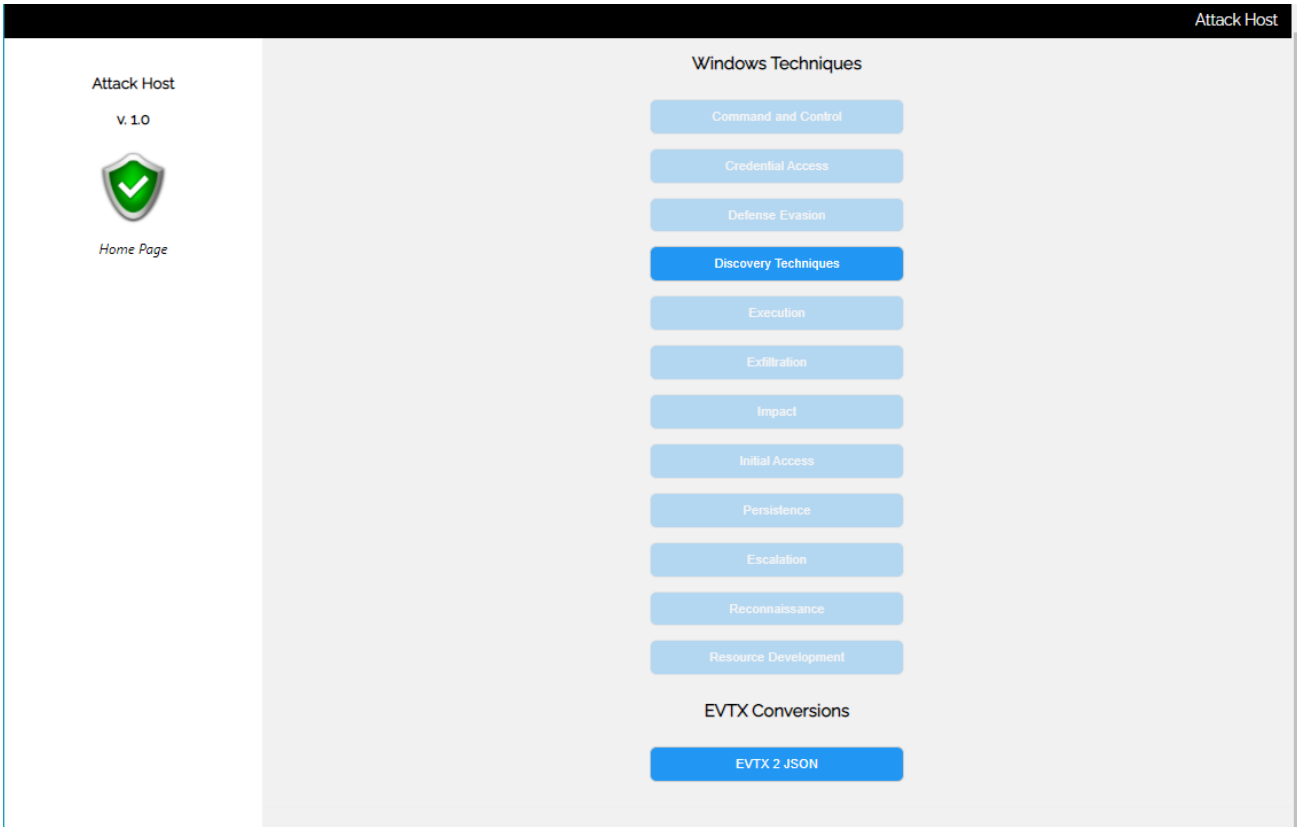
The file "app.py" is the main python program that starts AttackHost. To run attack host simply run it as a python command line program:

```
C:\> python3 app.py
```

When AtomicHost starts it first starts the Flask microserver. To view the application gui open a web browser and navigate to:

http://localhost:5000

You should see the following web page:



There are two sets of buttons on this page. One for running windows Red Canary's Atomic attack "techniques" that are coordinated with the Mitre Attack Framework. Each of the buttons represents a set of specific techniques. The lower button is to launch the conversion of EVTX files to JSON.

Concept of Operations

To use AttackHost you must have syslog installed. After installing syslog, open the Microsoft Event Viewer to record the session. Next, clear the current log from the Event Viewer. You are now ready to start your AtomicHost app and perform an attack.

Start the Event Viewer so new events will be the only events displayed. After collecting the appropriate amount of events, save you evtx file to the data/input/evtx directory. If the directory doesn't exist, make it. Finally go to the AttackHost Home page and in the EVTX Conversions sector, press the button marked "EVTX2JSON". This will create .json files that can then be used in a number of applications.