Web Cyber-attack Tool Installation Guide

Prepared by

Undergraduate Research Group CSSE Department 2024

Collin Bergmann

March 8, 2024

Contents

Introduction: What is it?

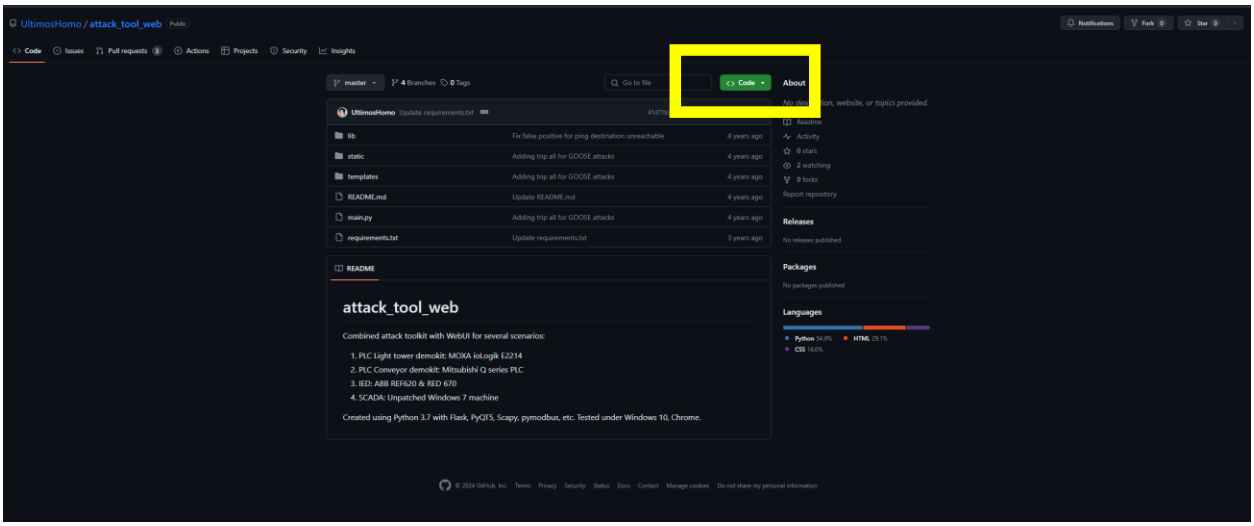
The web attack tool used in this project is a prebuilt collection of python files that can be utilized to run simple attacks on networks. When working with this tool there will be fields you will need to manually configure such as the packet information, the source and destination ports, and addresses as well as configuring the file for what attacks you want to implement. The tool does have a built-in GUI that will be accessible in a web browser.

Device Requirements for Installation

The required python version for this tool is 3.7. Other versions of python will not work properly with older installations of the libraries we need. This tool needs to be used on Windows in its current configuration because it utilizes PyWin32 and windows utilities to create the GUI.

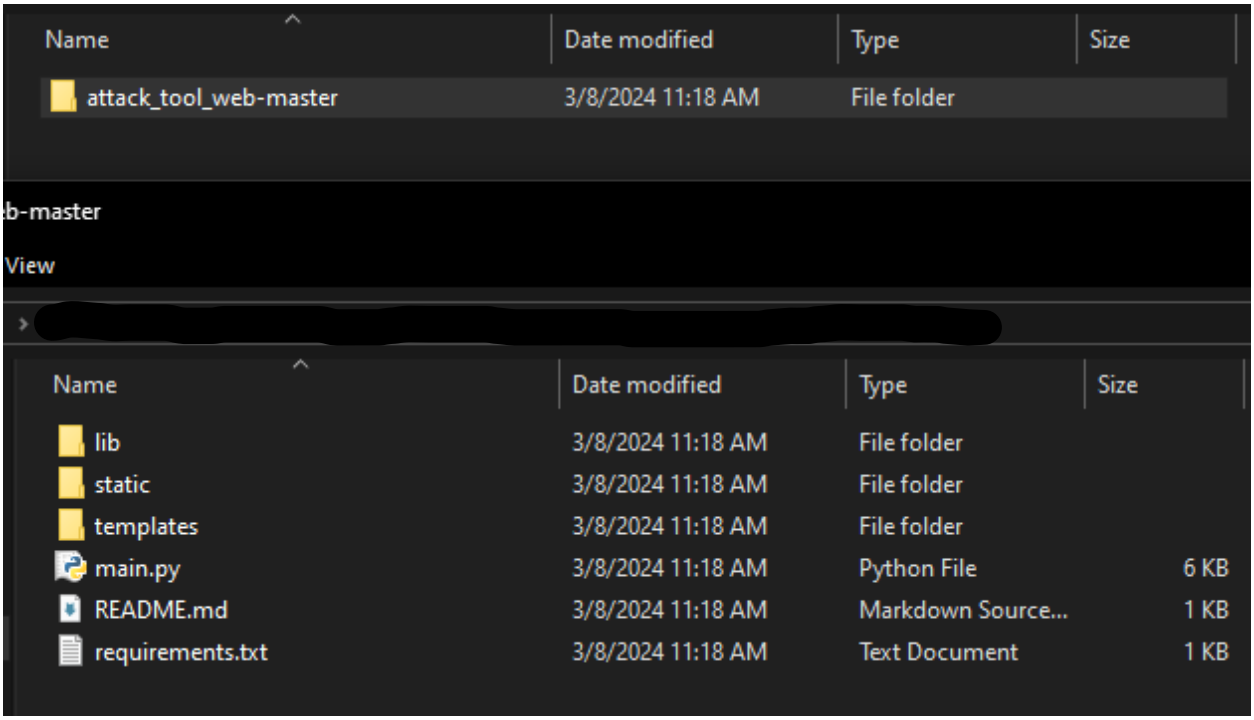
Installing the Code from GitHub

1) To begin the installation of the Python code needed to run this tool you will need to go to this, https://github.com/UltimosHomo/attack_tool_web, GitHub repository and download the .zip file containing all the code for the prebuilt tool.



2) Once you are at this page, click the green ‘Code’ button on the top right to download to code, you can choose between downloading the zip, opening the GitHub application, or copying the GitHub address for downloading through terminal.

3) After downloading the zip file, extract the file into an empty folder on your device.

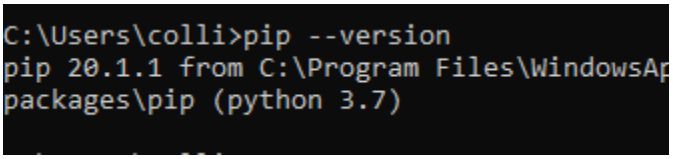


This above screenshot shows the file extracted, and its contents so you can be sure you have the correct file downloaded.

Pip installation for Package Installation

Pip is a tool that can be used from Python to install packages and libraries for use in projects. You can create a virtual environment (venv) if you would like to, but these packages are okay to be installed directly on to your computer.

1) First you want to check if pip is installed on your device, you can do this by going into the command prompt of your windows device and enter the command, “pip –version,” it will display your pip version or that pip is not installed.



2) If you do not have pip installed you can follow this video tutorial, https://www.youtube.com/watch?v=fJKdIf11GcI , showing how to download pip using the ‘curl’ command and then move the file to the environment so it can be executed from anywhere

Installing Required Packages and Libraries

Inside of the attack_tool_web-master folder there is a .txt file named ‘requirements.txt’ this file holds the list of all the packages and libraries you will need to install for the tool to run properly.

1) Begin by setting python to python version 3.7 which is necessary for smooth library instillation

2) Begin by opening the requirements.txt file and looking at the packages needed.

```
cffi==1.14.0
click==7.1.2
concurrent-log-handler==0.9.16
cryptography==2.9.2
dnspython==1.16.0
Flask==1.1.2
future==0.18.2
impacket
itsdangerous==1.1.0
Jinja2==2.11.2
ldap3==2.7
ldapdomaindump==0.9.3
MarkupSafe==1.1.1
portalocker==1.7.0
```

```
portalocker==1.7.0
pyasn1==0.4.8
pycparser==2.20
pycryptodomex==3.9.8
pymodbus==2.3.0
pyOpenSSL==19.1.0
pyserial==3.4
pywin32==228
scapy==2.4.3
six==1.15.0
Werkzeug==1.0.1
```

3) My advice for this next step is to manually install all the packages individually with their specified version to ensure compatibility of all files. To install packages, you will go into your command prompt on windows and navigate to the attack_tool_web-master file and one by one of us the command, “pip install ‘name==version#’”, and example being, “pip install cffi==1.14.0” than hit enter. Do this for every package until you have installed all of them. There is also a way to do pip installations through PyCharm by clicking on the python version in the bottom right and opening the interpreter settings. From there, you can search for specific libraries and specify versions. IMPACKET WILL NOT INSTALL WITH WINDOWS DEFENDER ACTIVE, EXPLAINATION IN NEXT SECTION.

4) There is one installation that installs a newer version of cryptography automatically (most likely pyOpenSSL), so cryptography needs to be manually downgraded after installing all the other libraries. To do this, delete the newer version of cryptography and install the needed version(2.9.2).

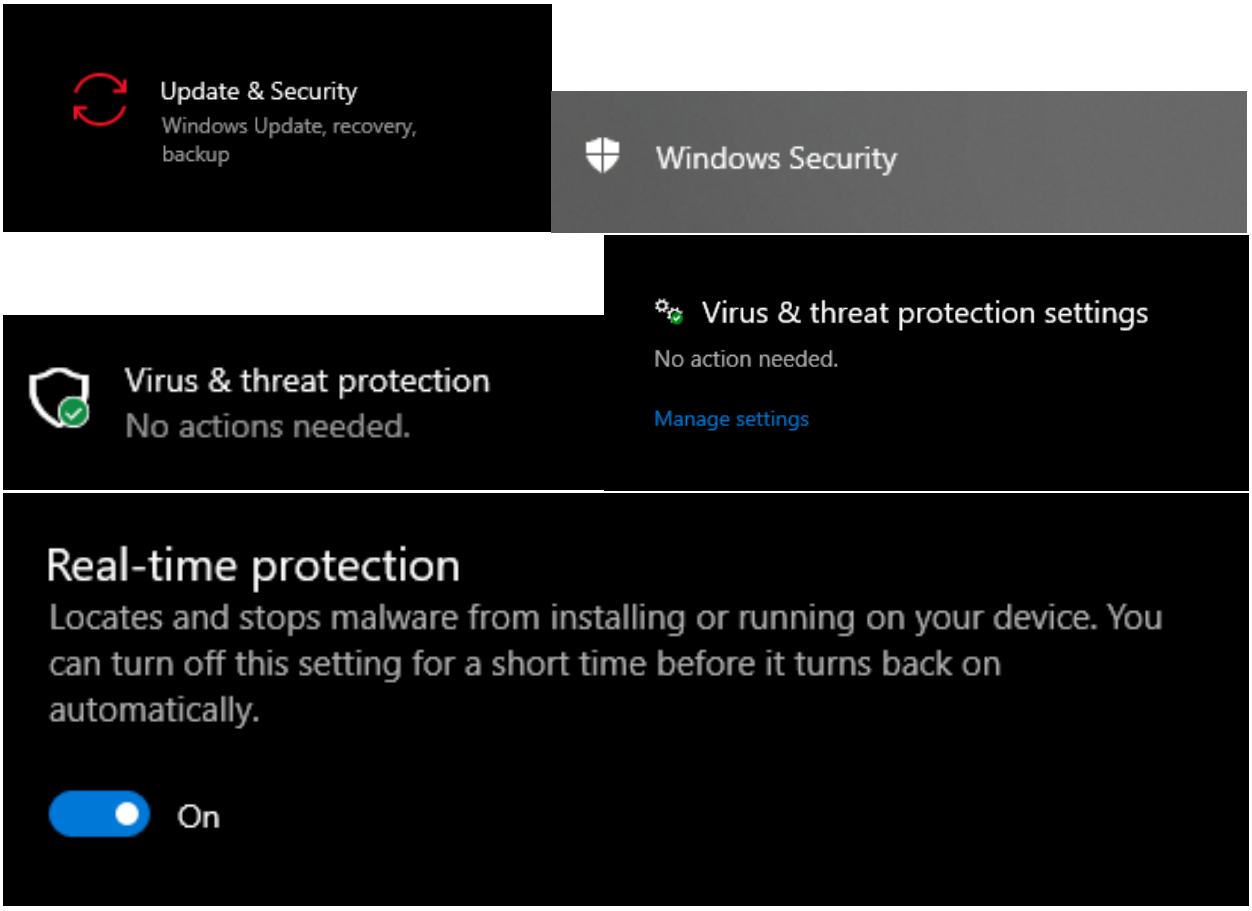
4) You can utilize the ‘pip list’ command to check versions of each package you have installed on your device already to see if you need to install all.

Other Requirements

Dealing with the Impacket installation

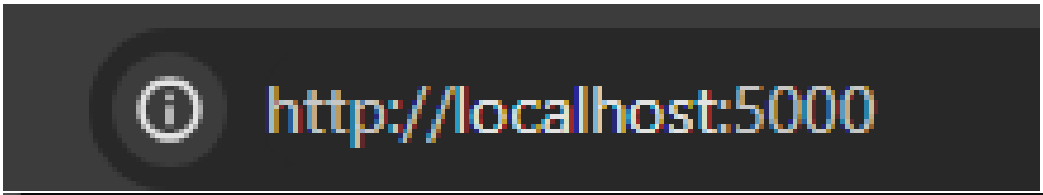
When installing the Impacket package you will run into issues with it not being found or errors with metadata, this is due to windows defender Realtime defense being active. If you are the administrator of the device, you should be okay to go ahead and deal with this issue.

1) First you want to navigate to settings>Update and Security>Windows Security>Virus and Threat Protection Settings>Manage Settings>Real-time protection set to (OFF), install impacket once it is installed you can turn this setting back on. [This path though settings are done on windows 10, may differ for windows 11].



Running the Web Attack Tool

In the second screenshot bellow is the command python main.py to run the tool after all packages are installed, once it is running go to a browser and type “localhost:5000”, this will bring up the attack tool web UI that is running from your device.

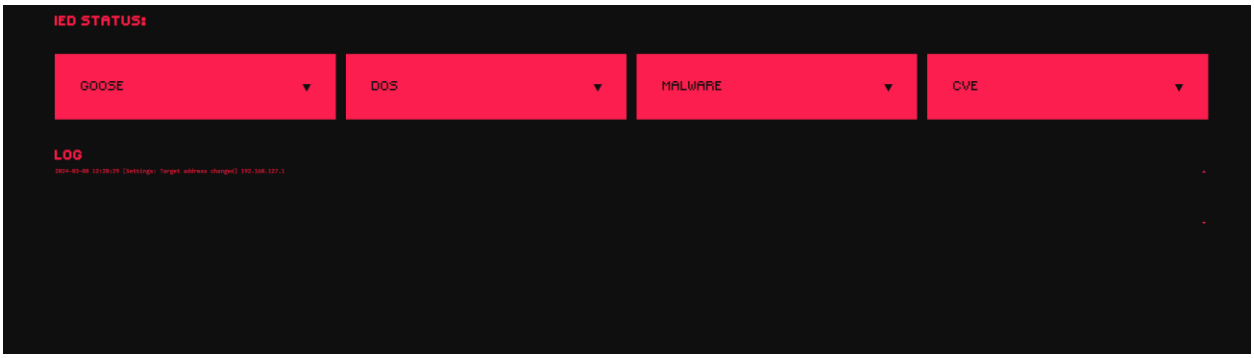



```
(attackEnv3) C:\Users\colli\OneDrive\Desktop\Research\Undergraduate Research\Tool\attack_tool_web-master>python main.py
WARNING: Wireshark is installed, but cannot read manuf !
 * Serving Flask app 'main'
 * Debug mode: off
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5000
 * Running on http://192.168.1.142:5000
Press CTRL+C to quit
```

Below here is the UI for the web application when the tool is active. This first screenshot is the initial screen when you load up the webpage.

To implement the GOOSE Attack, click the top left menu icon and go to IED, once there you will get a new UI of pull-down objects.

The first option under here, “GOOSE”, is where you can trip the ref620 devices. You will simply click on the goose box and click trip.



Final Notes

As a conclusion for this installation guide, the UI we are currently using will not look like this one, as this is the original UI that comes with the web application software. We have modified ours to have capabilities to reset the trip of the REF620-615 devices, so we do not have to manually untrip them. We also have made a few changes to make this UI simpler.

If the user here would like, we do have a .exe file that will run our version of the software that Peter Hahm has made. You can simply run the .exe file and it will execute and run in terminal as if you ran the main.py file yourself but with our updated UI. This .exe is standalone and does not require python or any of the above dependencies to be installed on your system. It can found in the by navigating to Current Attack Tool Versions > LATEST_simplified_with_interface_option > main.exe in the Teams S24 Undergraduate Research Group “Files” section.