CSN 190 – Assignment 6.3 Tutorial

Project Name: OWASP Nettacker

Project Type: Automated Penetration Testing / Security Testing Tool

Introduction

This tutorial demonstrates the setup and use of OWASP Nettacker, an open-source automated penetration testing framework developed by OWASP. The objective of this exercise is to successfully initialize the tool on a Windows system, verify correct installation, and safely test it using a localhost target while observing platform limitations.

Prerequisites

- Windows 10 or 11

- Python 3.x installed and added to PATH

- Git for Windows

- Visual Studio Code

- Internet connection

Step-by-Step Instructions

1. Open Visual Studio Code and navigate to the Nettacker project folder.

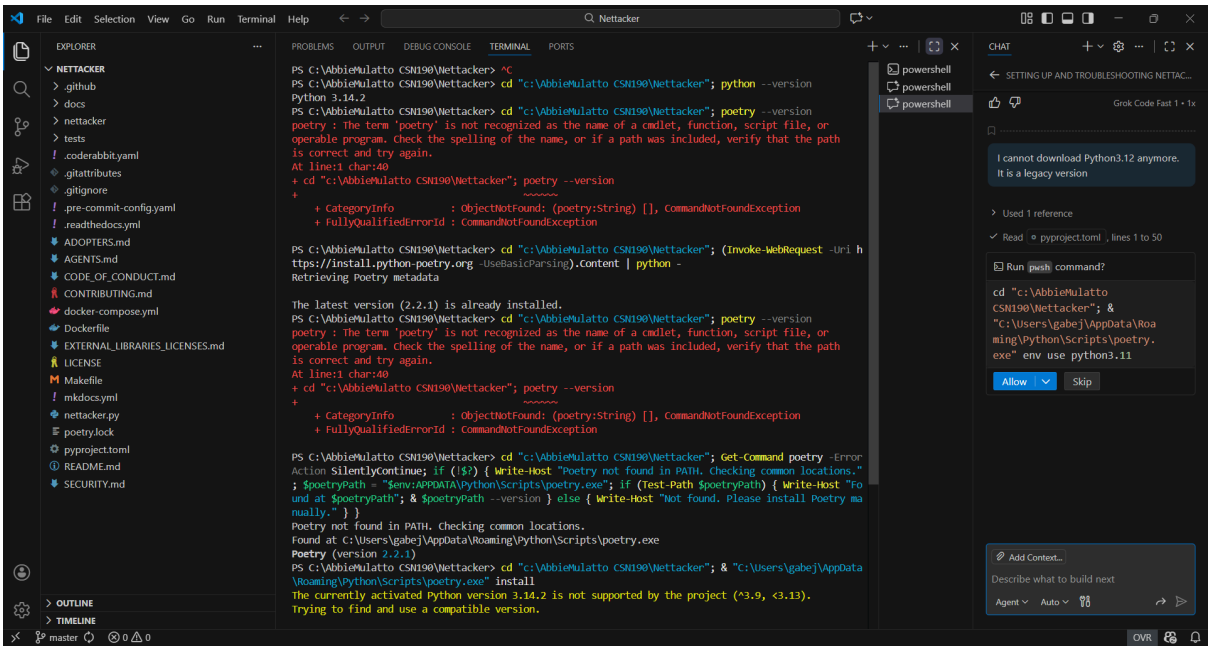
Command:

```
cd C:\AbbieMulatto CSN190\Nettacker
```

2. Verify Python installation.

Command:

```
python --version
```



(Python was downloaded - Copilot wanted use of a legacy version *Problem #1*)

3. Install missing dependencies as errors appear.

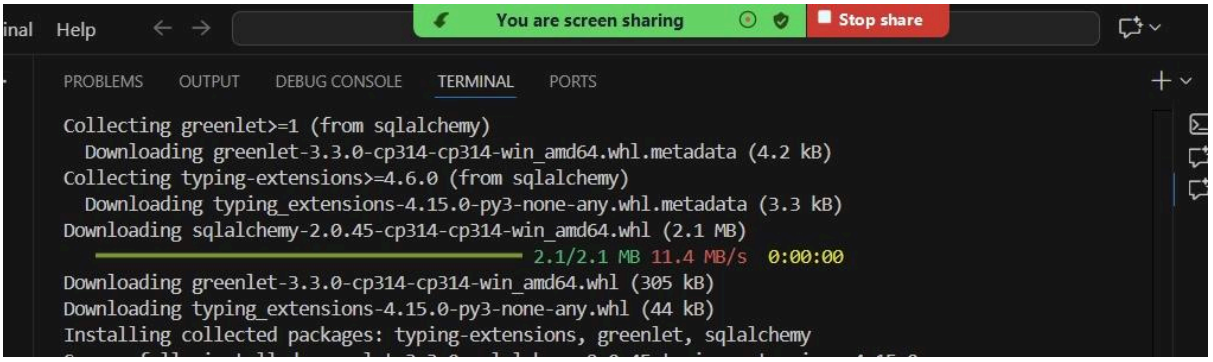
Commands used included:

```
pip install multiprocess
```

```
pip install pyyaml
```

```
pip install netaddr
```

```
pip install sqlalchemy
```



(Installation of missing dependencies - *Problem #2*)

4. Run Nettacker help command.

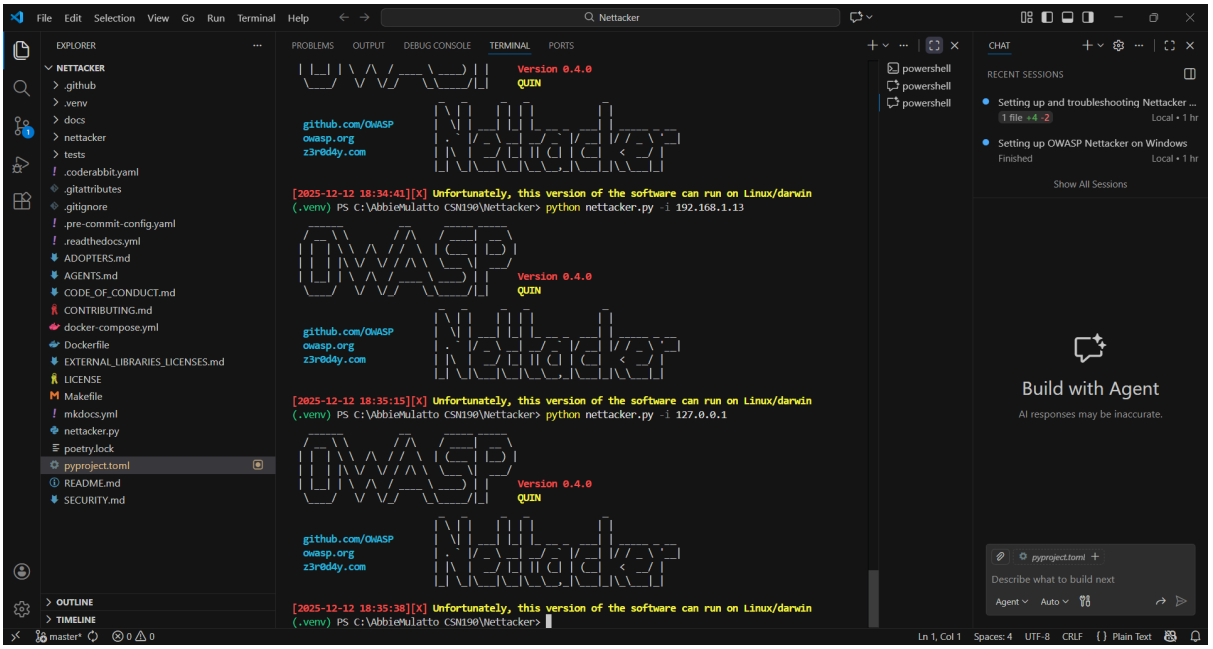
Command:

```
python nettacker.py --help
```

5. Attempt a safe localhost scan.

Command:

```
python nettacker.py -i 127.0.0.1
```



(Attempt at scanning local host - Attempt failed due to environment limitations - Expected Result)

Expected Results

OWASP Nettacker successfully launches, displays its ASCII banner and version number, and reports that active scanning is supported only on Linux and macOS systems. This confirms that the tool is installed correctly and functioning as designed on Windows.

Troubleshooting

During setup, several missing Python modules caused errors. These were resolved by carefully reading error messages and installing the required dependencies using pip. The platform limitation message is expected behavior and does not indicate failure.

Conclusion

This exercise provided hands-on experience working with a real-world cybersecurity tool. I learned how to troubleshoot dependency issues, understand platform limitations, and ethically initialize penetration testing software. Future work could involve running OWASP Nettacker on a Linux-based environment for full functionality