mymitmproxy

Cryptography and Cryptanalysis Project: EPITA Cyber 2

April 2023

Introduction

mitmproxy is a free and open source interactive HTTPS proxy. Useful for many applications such as debugging or pentesting or even malware signature analysis, it's a must know in cyber security. mitmproxy supports SSL and TLS protocols and provides a powerful web interface and Python bindings. The goal of this project is to implement a subset of mitmproxy's capabilities, using the openssl library for secure communication. This will also allow you to manipulate custom certificates and certificates authorities.

Objectives

mandatory

- You must implement the CONNECT header and forward HTTP traffic.
- You must support HTTPS traffic (on port 8443) and HTTP traffic (on port 8080)
- The certificate authority key path must be configurable using the PROXY_CA_KEY environment variable.

Bonuses

- On the fly certificate generation based on the destination
- Expose a front-end socket for the data inspector
- Configurable malware analysis
  - Easy: regular expression matching
  - Hard: YARA rules
- Basic authentication
- man page (can be generated)
- Export a library and python bindings
- Any bonus you want as long as it is documented, you can earn points if the work is therefore.

Handout

The mandatory part gives the grade of 12/20. Each bonus, if completed, adds a number of points to the final grade.

Your repository must contain a README (in plain text, markdown or org format) containing explanation on how to build your project, its dependencies and the bonuses that you have implemented. Since there are no guidelines on how to implement certain bonuses, you must document each feature that you have added.

You binary must provide a --help command explaining the options of the binary.

You must implement said proxy in C99 or C++20.

The project will be in groups of 3, and you will be entirely free on how to implement the server. No code will be given and it will not be tested automatically.

You can ask on the Discord server or via email permission to use an open-source library, by justifying it's utility. If the library is accepted, everyone can freely use it in their project.

Useful documentation

The following documents can help you in your task:

- RFC 2616, RFC 5280
- Tunneling TCP based protocols through Web proxy servers by A. Luotonen
- Wikipedia pages and online documentation
- Beej's Guide to Network Programming