Mitmproxy Setup & Troubleshooting — Step-by-step Walkthrough

Summary

This document walks through a real troubleshooting session while starting and using mitmproxy / mitmweb on a Kali Linux VM and configuring Firefox to use it as an HTTP/HTTPS proxy. It illustrates what to look for in the terminal output, how to configure the browser, how to confirm interception is working, and how to interpret common log messages and a specific traceback observed during the run. Screenshots from the session are included inline and explained.

Table of Contents

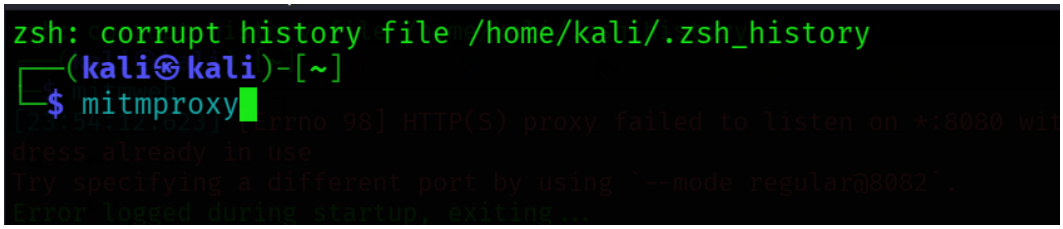
1. Environment and goal

Environment: Kali Linux (VM), Firefox browser running inside the VM. The aim is to run mitmproxy/mitmweb locally to inspect and (optionally) modify HTTP/HTTPS traffic from the browser.

High-level steps:
- Launch mitmproxy or mitmweb on a listening port (default 8080)
- Configure Firefox to use 127.0.0.1:8080 as HTTP and HTTPS proxy
- Install mitmproxy's CA certificate into the browser so HTTPS traffic can be intercepted
- Use the mitmweb UI to view captured flows and examine requests/responses

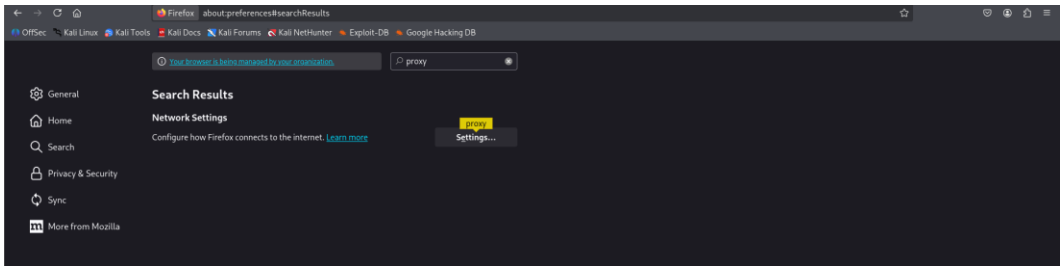
2. Starting mitmproxy and reading the terminal

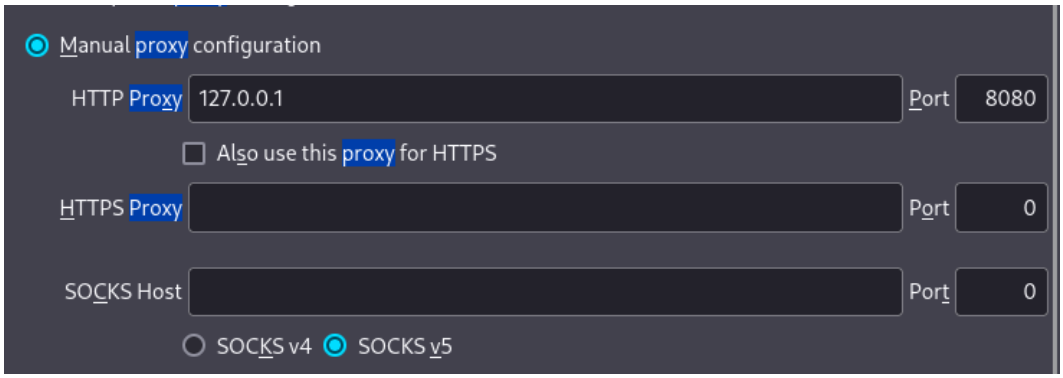
When you start mitmproxy (mitmproxy or mitmweb), watch the terminal carefully for errors or info messages. Errors include 'address already in use' if port 8080 is taken. Info includes proxy/web listen addresses.



3. Configuring Firefox to use the proxy

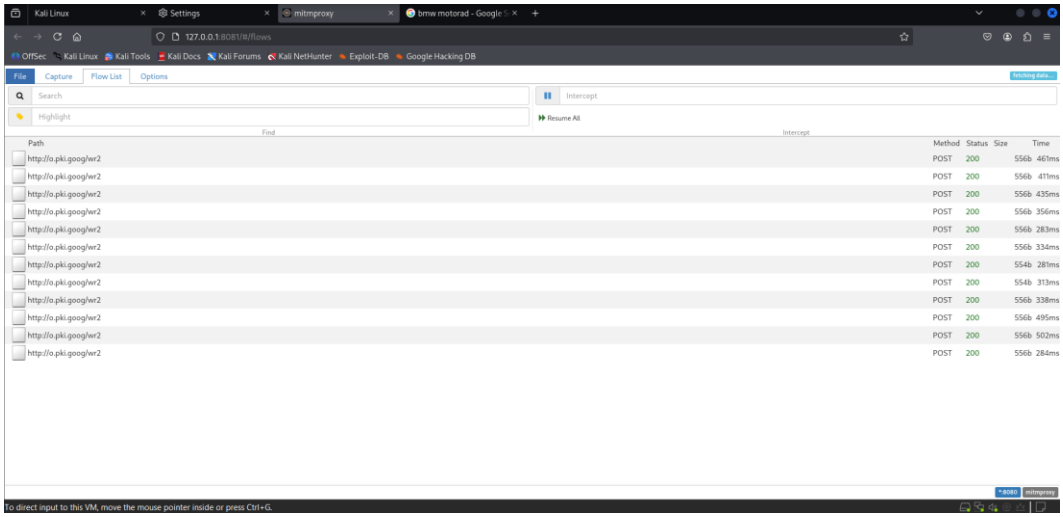
Open Firefox network settings and set manual proxy configuration. In this case, Firefox was set to HTTP Proxy 127.0.0.1, Port 8080.

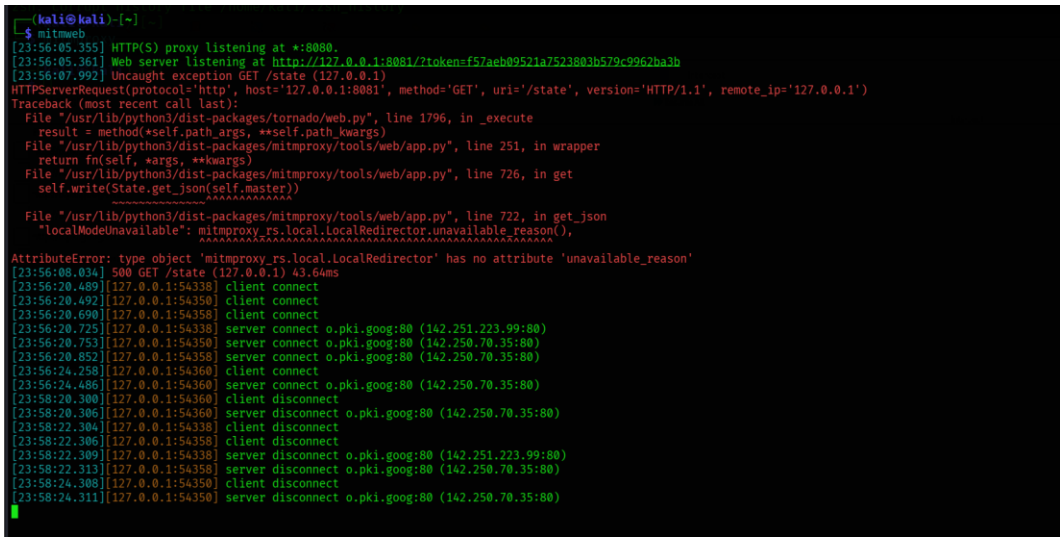




4. Observing mitmweb and captured flows

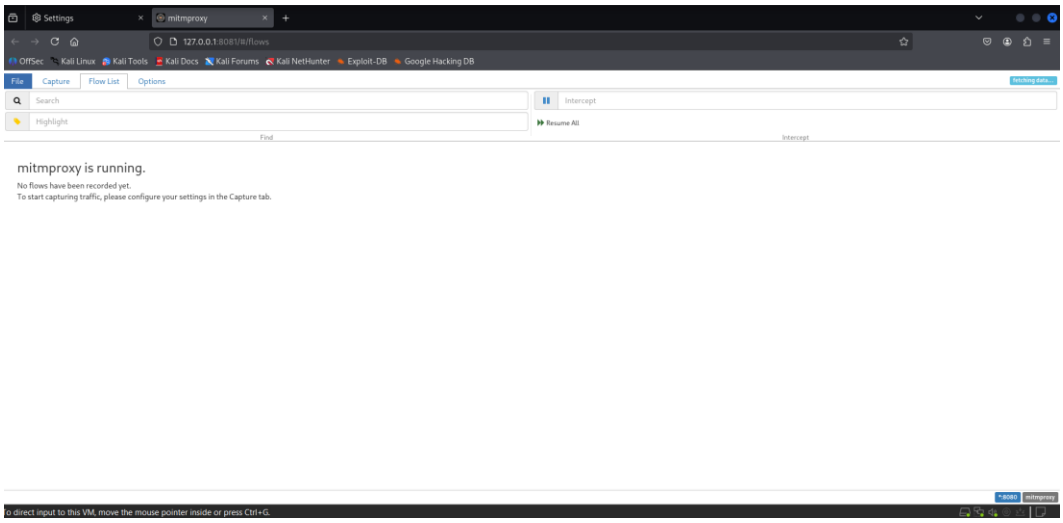
Once proxying is configured, open mitmweb at the address printed by mitmproxy (for example http://127.0.0.1:8081). Initially, flows may be empty. After browsing, recorded flows appear, showing methods, status codes, and paths.





5. Interpreting logs and a Python traceback

Terminal logs include normal lifecycle events like client/server connect and disconnect. But a traceback showed an AttributeError: 'LocalRedirector has no attribute unavailable_reason'. This bug affects /state endpoint in mitmweb UI but not core proxy functionality.



6. Practical fixes & troubleshooting checklist

Checklist:
- Check bind port with ss or lsof
- Ensure browser proxy settings are correct
- Install mitmproxy CA cert from http://mitm.it
- Upgrade mitmproxy if tracebacks persist
- Fix zsh history file corruption separately

7. Security & legal reminders

Intercepting traffic you do not own or have authorization for is illegal. Only use mitmproxy on authorized systems. Remove mitmproxy CA cert after testing.