



mitmproxy

SCRIPTS

- MITMproxy has a scripting API.
- Python code can be used to interact with MITMproxy.
- Python is a very powerful programming language.

→ Python + MITMproxy = very powerful MITM scripts.

TROJANS



- A trojan is a file that looks and functions as a normal file (image, pdf, song ..etc).
- When executed :
 1. Opens the normal file that the user expects.
 2. Executes evil code in the background (run a backdoor/keylogger ...etc).

-> Therefore it is great to social engineer the target into running our evil code

CREATING A TROJAN



- Combine evil file with normal file (image, book, song ...etc).
- Configure evil file to run silently in the background.
- Change file icon.
- Change file extension.



mitmproxy

OWNING DOWNLOADS

- TrojanFactory comes with script (**mitmproxy_script.py**)
- Based on the script created previously.

Extra features:

1. Proper implementation of Trojan Factory.
2. Supports multiple file types.
3. Spoof file extension on the fly.
4. Add appropriate icon on the fly.



mitmproxy

BYPASSING HTTPS

- Everything we did so far will **not** work against HTTPS pages.
- HTTPS data is **encrypted** using SSL.
- Data can **not** be read → can **not** be modified.
- SSLstrip can **not** be used because mitmproxy can not work with another transparent proxy.

Solution: use a mitmproxy script to bypass https.



mitmproxy

GENERATING TROJANS ON THE FLY

- Intercept and replace downloads.
- Combine any file with an evil file.
- Write MITMproxy scripts.
- Lets combine all of this:

→ Replace files the user downloads with a trojan that will run the file they expect + our evil file.