Design Review 1

Akiel Aries - Release Manager
Cody Beck - Team Architect
David Knight - Team Lead
Nathan Chan - Front-End Engineer

Team Mentor: Daniel Kramer
Instructor: Michael Leverington

What is Zeek?

- Network traffic analyzer
- Network security monitor
- Open Source

Meet Tim!

Zeek Package Manager

- Create and publish packages
- Allows users unrestricted access
- Tools that enhance network analysis

Current package website logo

In 2017, researchers from the Berkeley Lab using Zeek noticed strange AFP traffic on their computers

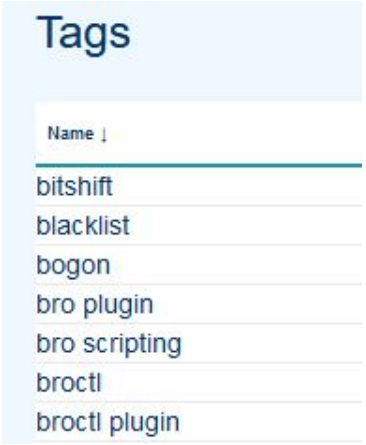
Easily searched through 2 years of logs using Zeek

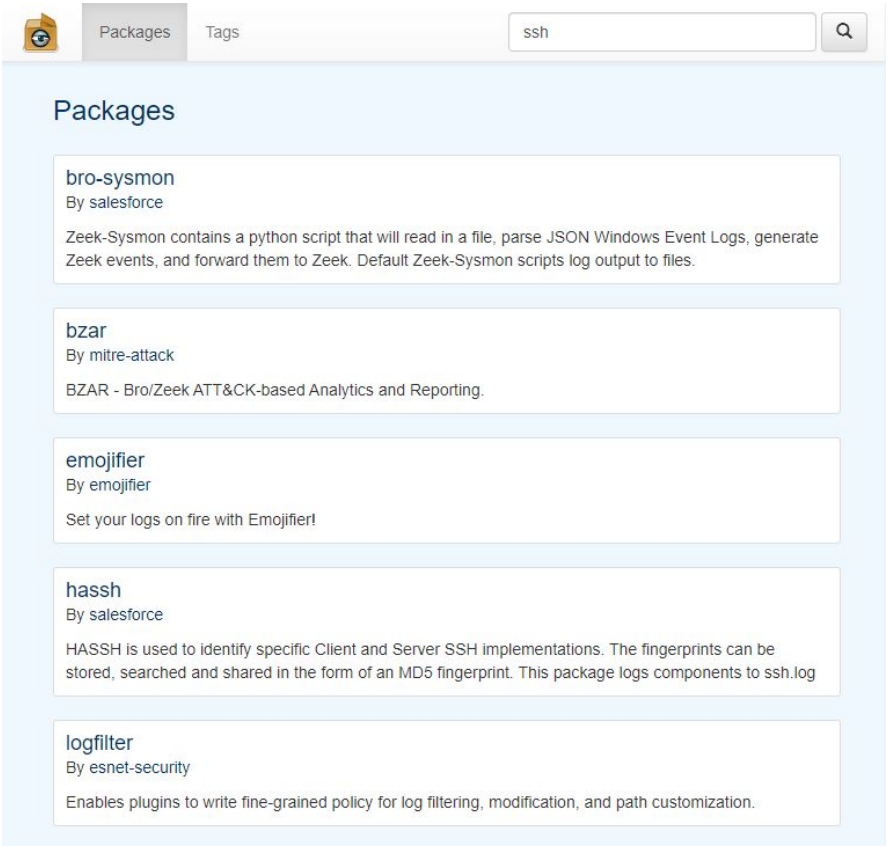
Found strange IoC's connected to a university in Ohio

Emailed said university and called the FBI which lead to the discovery of the Fruitfly malware

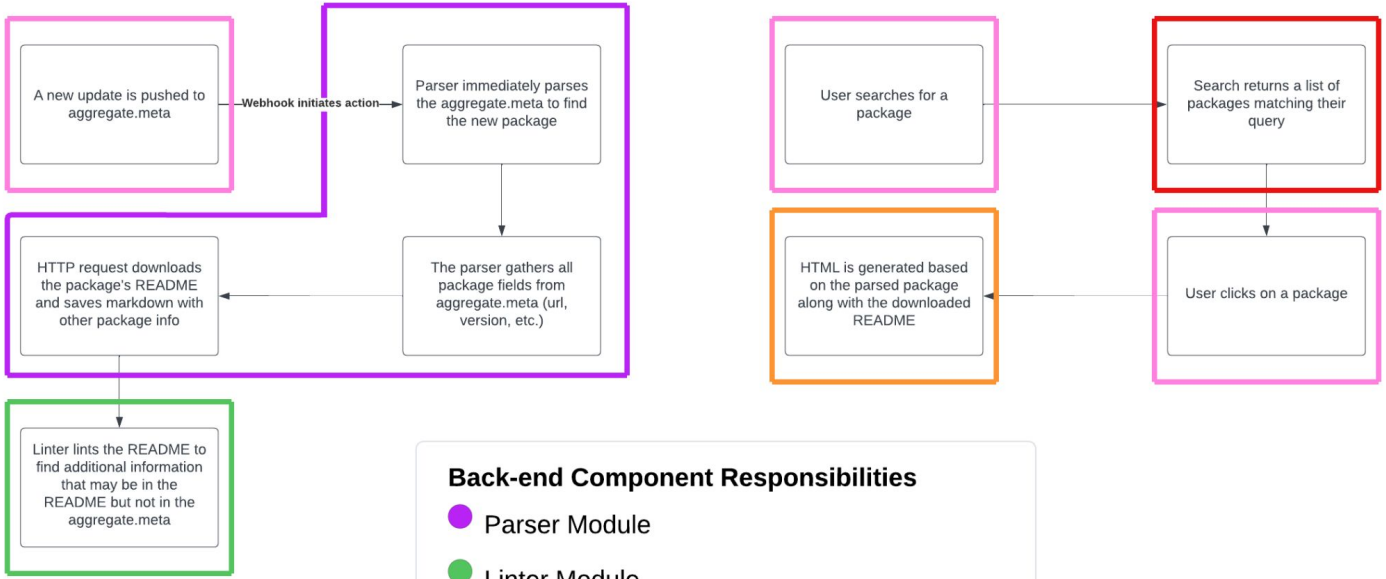
Problem Statement

- Current search feature is substandard
- Irrelevant/Incomplete results
- Inconsistent tagging practices
- Outdated design





Solution Overview



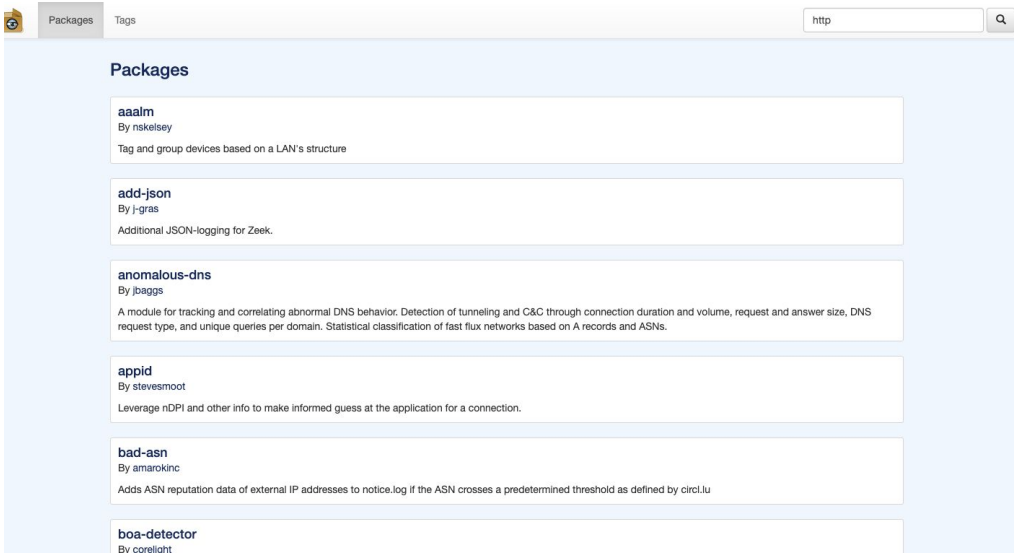
Key Requirements

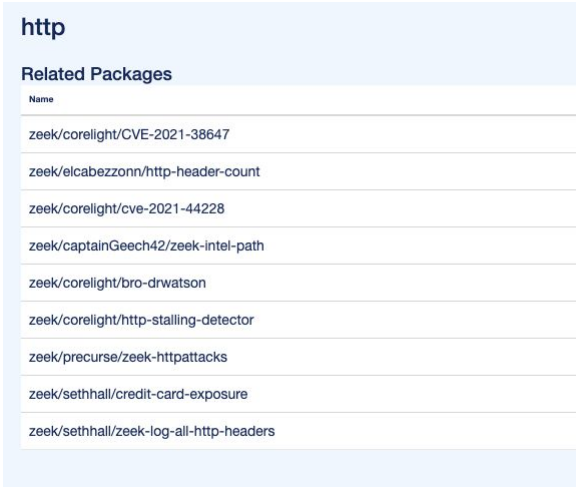
- Parser that can get information from a central metadata file containing information about every Zeek package
- Pull additional package information, such as README files, from each package's GitHub repository
- Improved search functionality to make packages more discoverable
- A modern front-end preserving the look and feel of the zeek.org site
- Linting of packages at parse-time to highlight important information about each one

Functional Requirements - Search

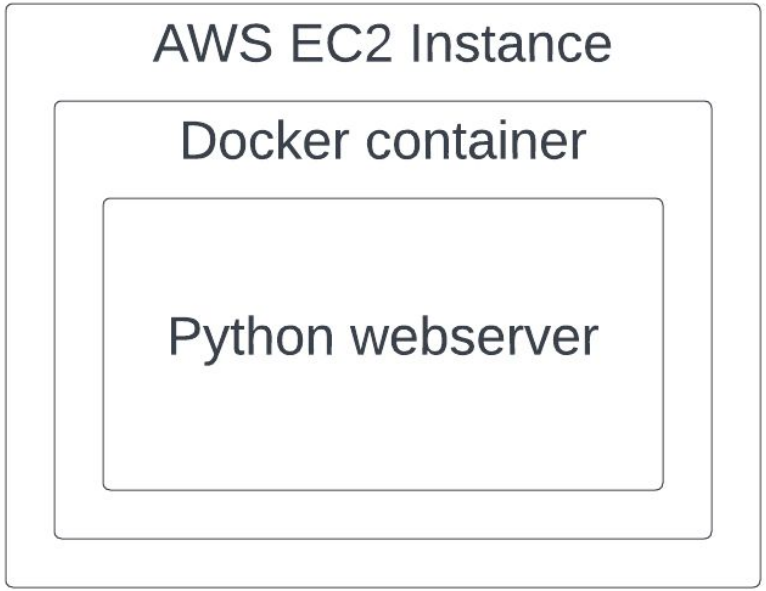
- To implement the our ranking algorithm, we will need to implement it in the following parts:
  - TF-IDF algorithm: term frequency, inverse document frequency
  - Calculate the average document length
- Apply appropriate biases to scores
- Provide a list a packages sorted from most to least relevant

Performance Requirements - Search





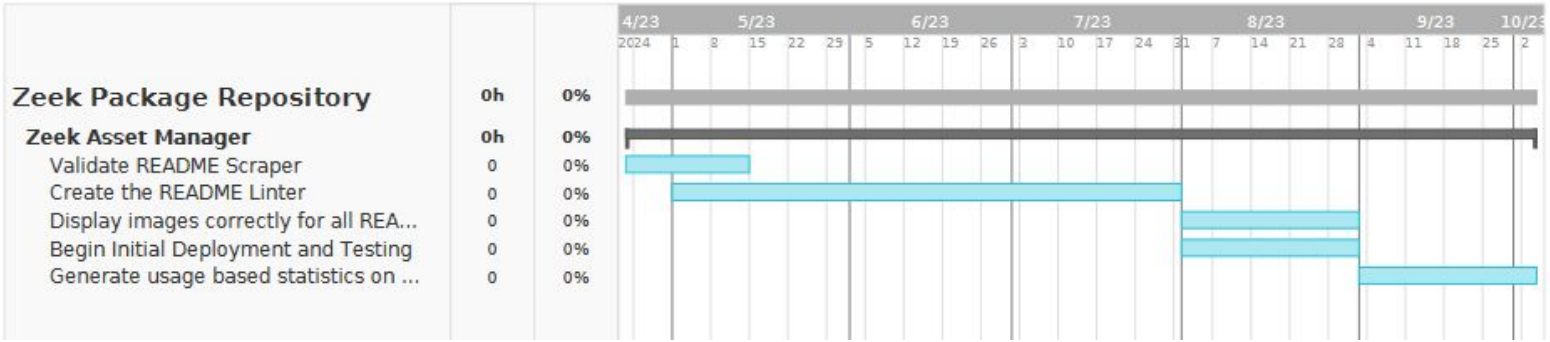
Environmental Requirements - Search



Risks & Feasibility

- Integrity of data sources
- Parsing and scraping of package data could return faulty results also causing the front end injection to be inaccurate
- Search engine could produce inaccurate results to users if original sources are also inaccurate
- Extensive and meaningful testing ensuring package data is injected properly and within an ideal time window will mitigate the potential risks associated with this project

Upcoming Schedule



Wrapping Things Up