



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- Outdated design

Tags

Name ↓

bitshift
blacklist
bogon
bro plugin
bro scripting
broctl
broctl plugin



Packages

Tags



Packages

bro-sysmon

By salesforce

Zeek-Sysmon contains a python script that will read in a file, parse JSON Windows Event Logs, generate Zeek events, and forward them to Zeek. Default Zeek-Sysmon scripts log output to files.

bzar

By mitre-attack

BZAR - Bro/Zeek ATT&CK-based Analytics and Reporting.

emojifier

By emojifier

Set your logs on fire with Emojifier!

hassh

By salesforce

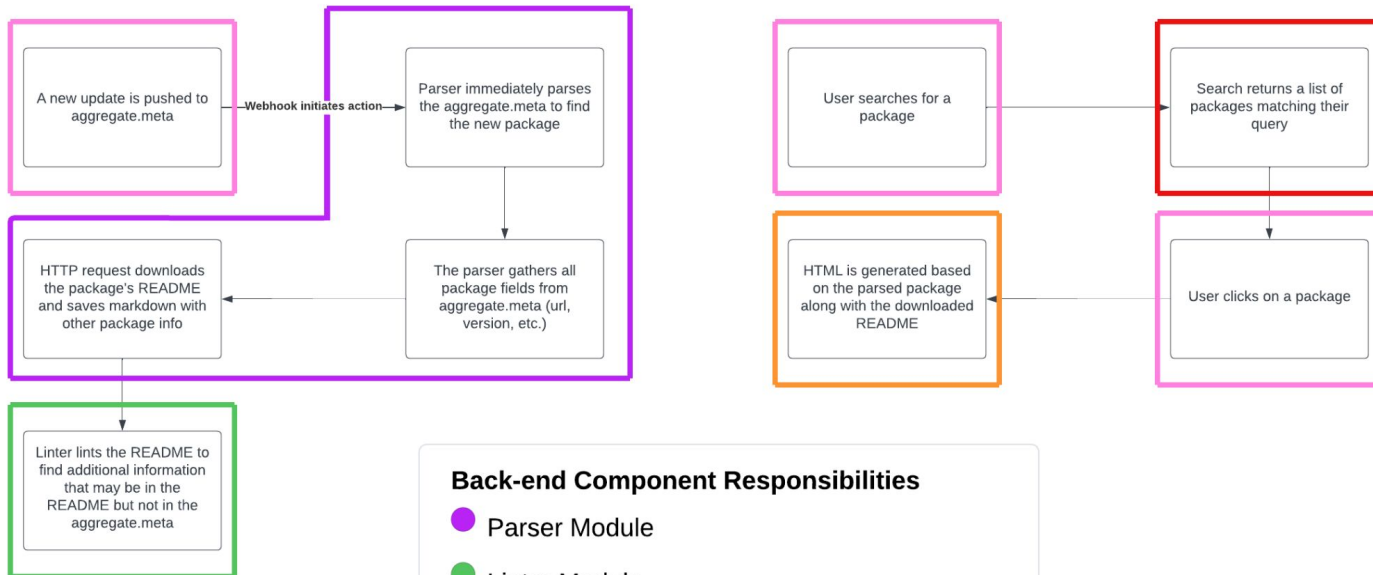
HASSH is used to identify specific Client and Server SSH implementations. The fingerprints can be stored, searched and shared in the form of an MD5 fingerprint. This package logs components to ssh.log

logfilter

By esnet-security

Enables plugins to write fine-grained policy for log filtering, modification, and path customization.

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

Packages Tags

Packages

aaalm
By nskelsey
Tag and group devices based on a LAN's structure

add-json
By j-gras
Additional JSON-logging for Zeek.

anomalous-dns
By jbaggs
A module for tracking and correlating abnormal DNS behavior. Detection of tunneling and C&C through connection duration and volume, request and answer size, DNS request type, and unique queries per domain. Statistical classification of fast flux networks based on A records and ASNs.

appid
By stevesmoot
Leverage nDPI and other info to make informed guess at the application for a connection.

bad-asn
By amarakinc
Adds ASN reputation data of external IP addresses to notice.log if the ASN crosses a predetermined threshold as defined by circl.lu

boa-detector
By corelight

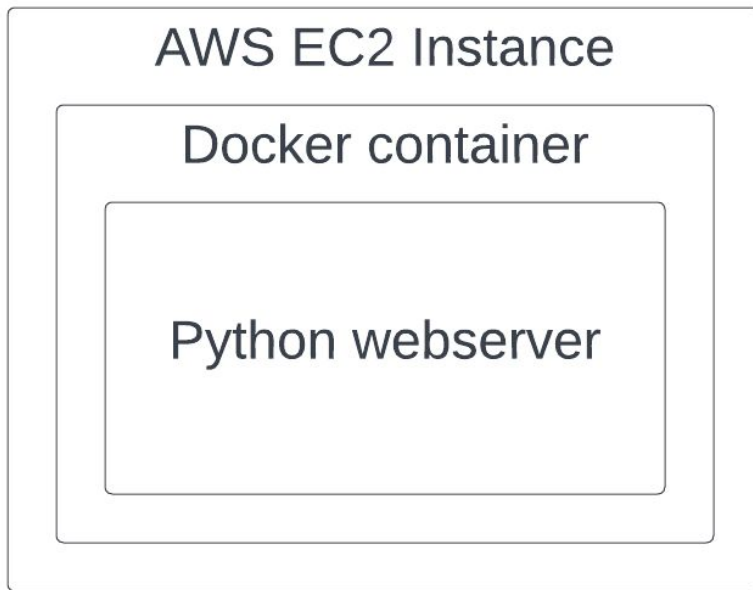
http

Related Packages

Name
zeek/corelight/CVE-2021-38647
zeek/elcabezonn/http-header-count
zeek/corelight/cve-2021-44228
zeek/captainGeech42/zeek-intel-path
zeek/corelight/bro-drwatson
zeek/corelight/http-stalling-detector
zeek/precurse/zeek-httpattacks
zeek/sethhall/credit-card-exposure
zeek/sethhall/zeek-log-all-http-headers



Environmental Requirements - Search



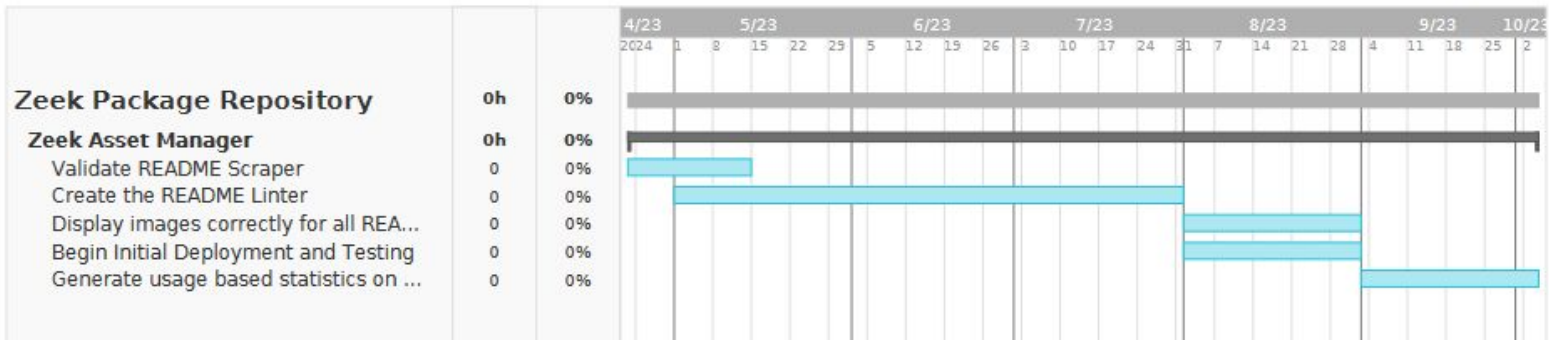


Risks & Feasibility

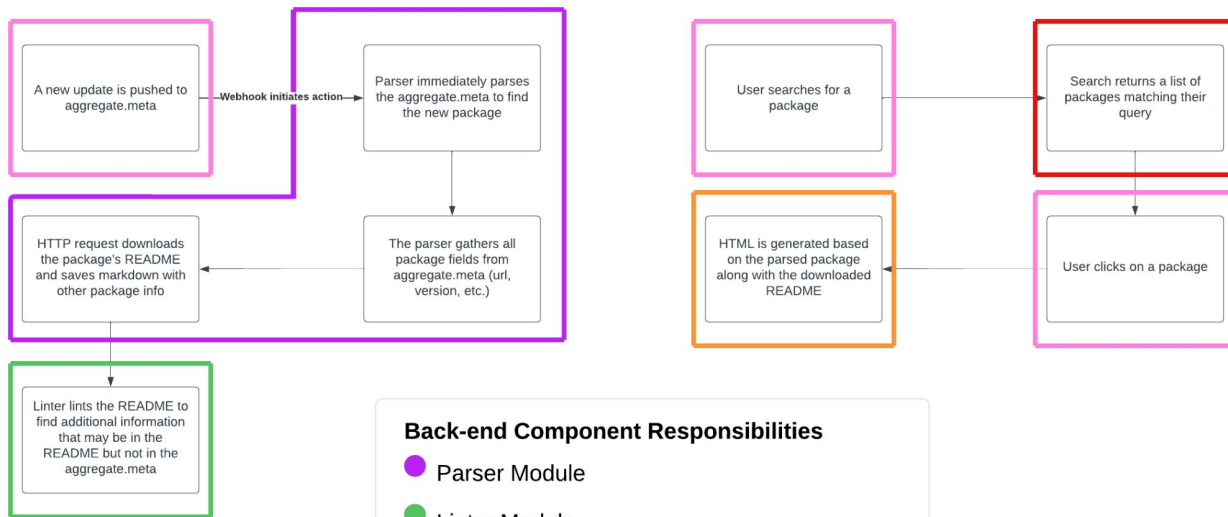
- Integrity of data sources
- Parsing and scraping of package data could return faulty results also causing the front end injection to be inaccurate
- Search engine could produce inaccurate results to users if original sources are also inaccurate
- Extensive and meaningful testing ensuring package data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



Upcoming Schedule



Wrapping Things Up



Back-end Component Responsibilities

- Parser Module
- Linter Module
- Search Module
- Jinja
- External Actions