Vulnerability Watch extension / improvements

Moonen Frederik, Dams Tim (AP promotor),
Vandenbroeck Dieter (EY promotor)

Building a better working world

Abstract

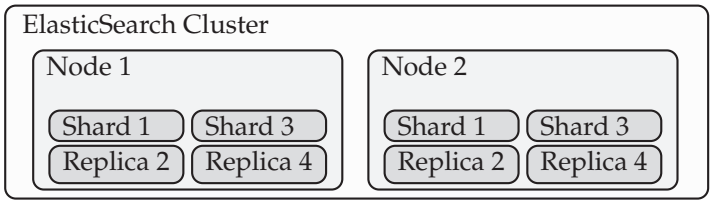
ITRA biedt een service aan die vulnerabilities en zero-day threats opspoort die relevant zijn voor een client. De scriptie bouwt verder door verbeteringen en uitbreidingen aan de Vulnerability Watch service toe te voegen. Zoals de analyse van de gespecificeerde issues van zaken zoals het verwerken van records in MySQL en ElasticSearch, server - side scripting met behulp van dataTables, optimalisatie van de Dockerfiles met docker-compose, automatisch opzetten van een demoplatform met behulp van fabric, live completion in ElasticSearch en ten slotte de optimalisatie ervan.

Technologie

Vat samen met welke applicaties gewerkt wordt om de informatie omtrent de kwetsbaarheden te verwerken. Op gebied van de webclient draait dit rond de manier waarbij de gegevens worden opgevraagd, verwerkt en getoond.

ElasticSearch

Deze software wordt gebruikt om search oriented applicaties te ontwikkelen. Het is een realtime - distributed - search analytics engine. Verder beschikt deze over functies zoals QueryDSL - Query Domain Specific Language, term query, bool query, prefix guery en filters.



Cronjobs

Informatie in ElasticSearch wordt ingeladen met informatie in bepaalde webpagina's, threats, fora, Tweets en CVE - Common Vulnerabilities and Exposure database. Deze informatie wordt gelinkt met de CPE - Common Platform Enumeration database en CVSS - Common Vulnerability Scoring System database.

```
cronjob.sh
cronjob.py (parent)
    cpe_retriever - py
    nvd_nist_retriever.py
    rss_feed_retriever.py
    security_focuspy
    twitter_post.py
```

Flask

Micro web framework dat Python functies globaal beschikbaar stelt.

Jinja2

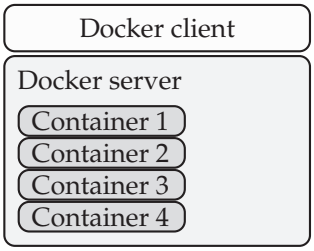
Templating engine die zich baseert op JSON data.

Tools

Ondersteunen de infrastructuur en helpen bij het automatisch opbouwen van het platform.

Docker

Docker stelt de gebruiker in staat om applicaties in containers op te zetten met behulp van docker images.



Docker-compose

Ondersteuning bij het ontwerpen van multi - purpose docker applicaties.

Fabric

Fabric is een Python bibliotheek en command - line tool die het gebruik van SSH voor application deployement automatiseerd.

Resultaten

Analyse hiërarchie, verwerken van Git issues, automatisering installatie demo platform, records verwerken in MySQL, ElasticSearch configuratie / optimalisatie, server-side dataTables, weergeven van tweets, aanpassen templates, en opstellen demo platform.