Žilinská univerzita v Žiline
Grantový systém UNIZA

Manažment dát pre kybernetickú bezpečnosť

Bc. Branislav Kramár, Fakulta riadenia a informatiky

Popis projektu

Na trénovanie úspešnosti sieťových bezpečnostných nástrojov sa nevyužíva reálna prevádzka, ale prevádzka zachytená v súbore vo formáte pcap, tzv. datasete. Datasety zohrávajú dôležitú úlohu pri testovaní a validácii metód alebo systémov detekcie sieťových anomálií. Riešeným problémom bola tvorba vlastných datasetov tak, aby spĺňali kritériá komplexných a hodnoverných datasetov. Riešilo sa tiež nasadenie nástrojov Arkime (v minulosti Moloch) a Suricata v reálnej prevádzke pre efektívnu archiváciu sieťovej prevádzky s možnosťou forenznej analýzy a detekcie útokov v sieťovom toku.

Použité nástroje

Suricata
Systém na detekciu prienikov
Vyhľadáva hrozby
v sieťovej prevádzke

Kibana
Zobrazuje dáta uložené
v Elasticsearch databáze
pomocou rôznych typov grafov

Arkime
Odchytáva a ukladá sieťovú prevádzku
Umožňuje nahliadať na uložené dáta

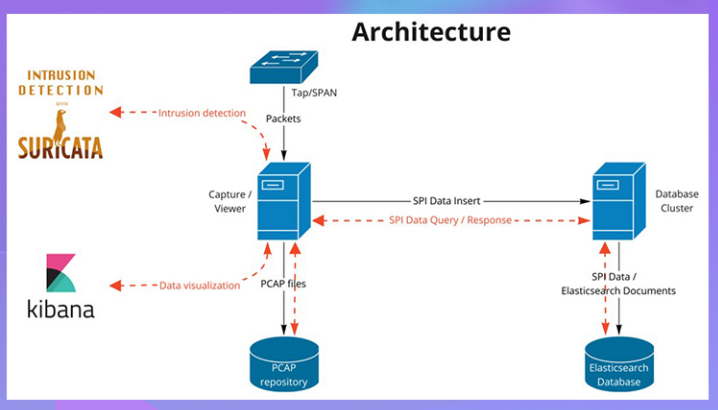
Elasticsearch
NoSQL databáza

Archivácia sieťovej prevádzky

Implementovaný systém pozostáva z dvoch serverov, pričom jeden obsahuje Elasticsearch databázu, druhý nasledovné nástroje:

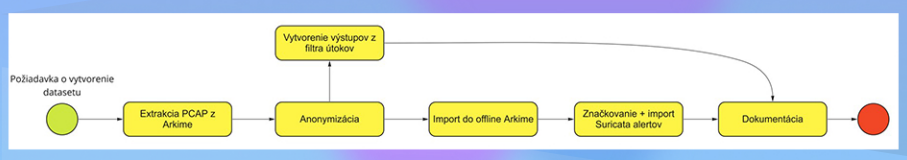
- Arkime Capture
- Arkime Viewer
- Suricata
- Kibana

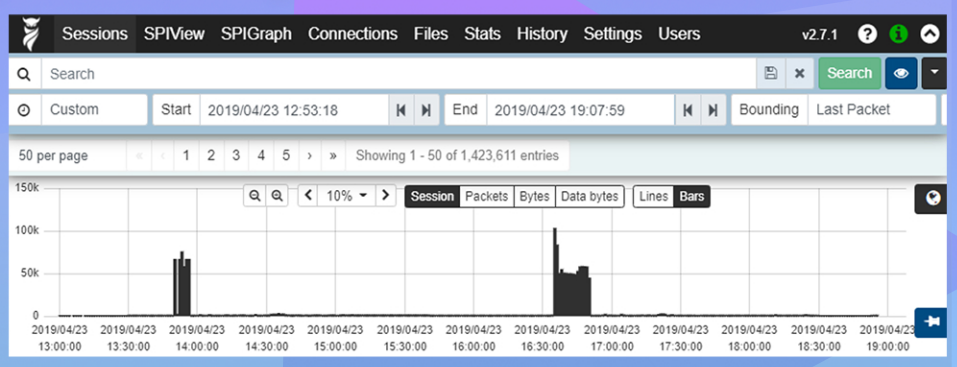
Systém odchytáva kompletnú sieťovú prevádzku z fakultného uplinku a kapacita diskov v súčasnosti umožňuje uloženie prevádzky za posledných 25 dní.



Archivácia anomálnej sieťovej prevádzky

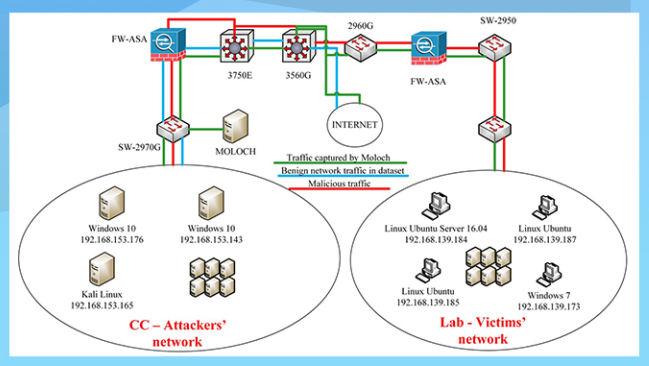
V prípade, že sa v odchytenej prevádzke vyskytne anomálny jav, ktorý môže byť vhodným materiálom pre neskoršie skúmanie, napríklad odhaľovanie DDoS útokov pomocou PCA metódy alebo detekcia anomálií v sieti pomocou strojového učenia, vytvorili sme metodiku ako takúto prevádzku uložiť do datasetu, označkovať a archivovať.





Dataset KIS 2019

Na prípravu vlastného datasetu sme použili topológiu na obrázku vpravo, kde kľúčovú úlohu zohral nástroj Arkime (Moloch). Dataset KIS 2019 pozostáva z jedného súboru formátu PCAP s veľkosťou 12 GB. Sieťová prevádzka v datasete pozostáva z útočnej a benignej, ktoré sú v súbore príslušne označené. V datasete je využitých 5 verzií rôznych operačných systémov s viacerými typmi útokov pri útočných scenároch. Dataset taktiež obsahuje kompletnú sieťovú prevádzku útočníkov a obetí. Informácie k datasetu sú dostupné na stránke nil.uniza.sk (QR kód), prístup k datasetu poskytujeme na požiadanie



Žilina, 2021