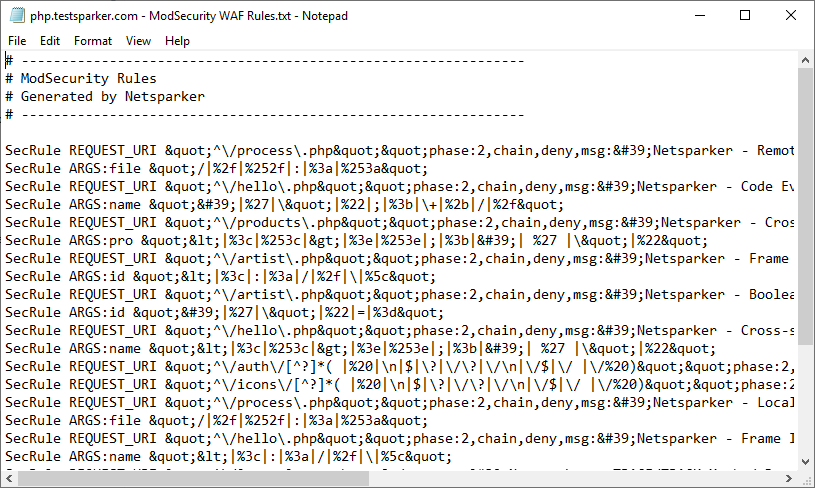
1. **ModSecurity dodatak za zaštitu veb servera**

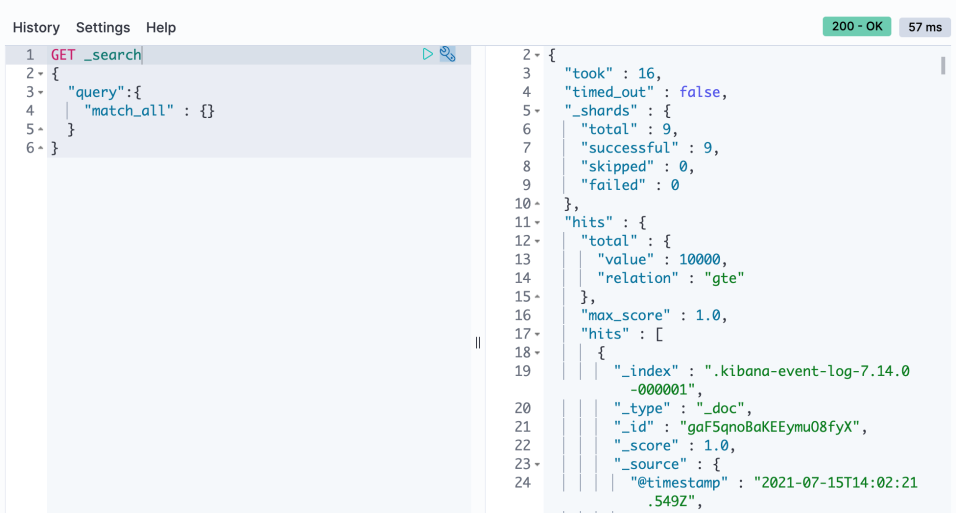
Proučiti ModSecurity dodatak za zaštitu veb servera (*web application firewall - WAF*). Detaljno se upoznati sa sintaksom i semantikom za pisanje bezbednosnih pravila. Implementirati WAF na veb serveru laboratorije L3 i omogućiti logovanje važnih događaja. Deo tipičnih pravila preuzeti, a deo pravila samostalno implementirati. Testirati pravila i logovanje događaja.

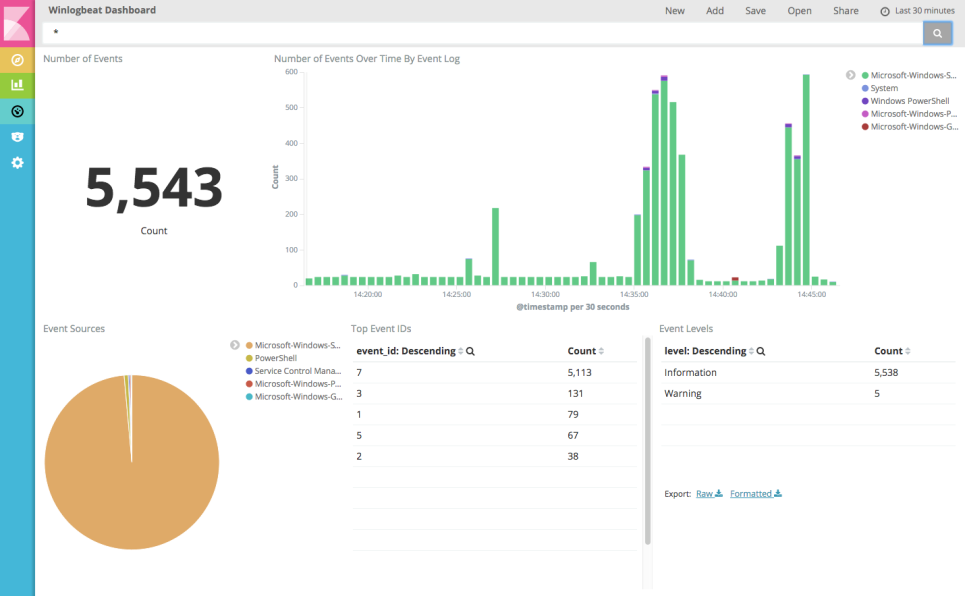
Litetarura: Mischel, Magnus. *ModSecurity 2.5*. Packt Publishing Ltd, 2009.



1. **Kibana templejti dash bordova**

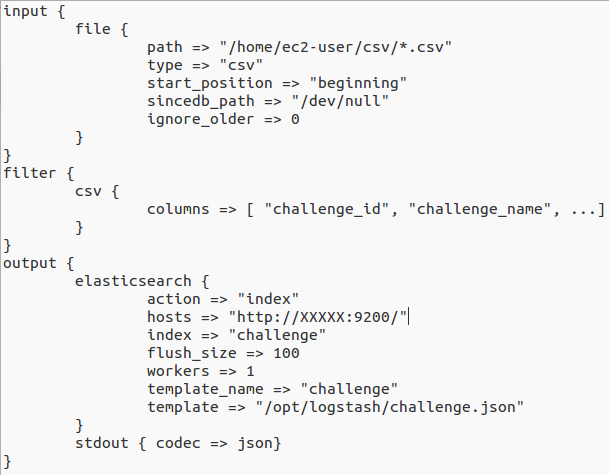
Upoznati se sa načinom na koji Kibana alat za vizuelizaciju čuva vizuelne elemente na ElasticSearch sistemu. Implementirati aplikaciju koja postojeći dahsboard-a pretvara u templejt iz kog može generisati nove dashboard-ove. Prilikom instanciranja novog dashboard-a iz templejta treba omogućiti da se određena polja kao što je indeks iz koga se povlače podaci mogu kastimizovati. Poželjno je aplikaciju razviti kao kozolnu aplikaciju u pajtonu, koja ispoljava REST API interfejs.





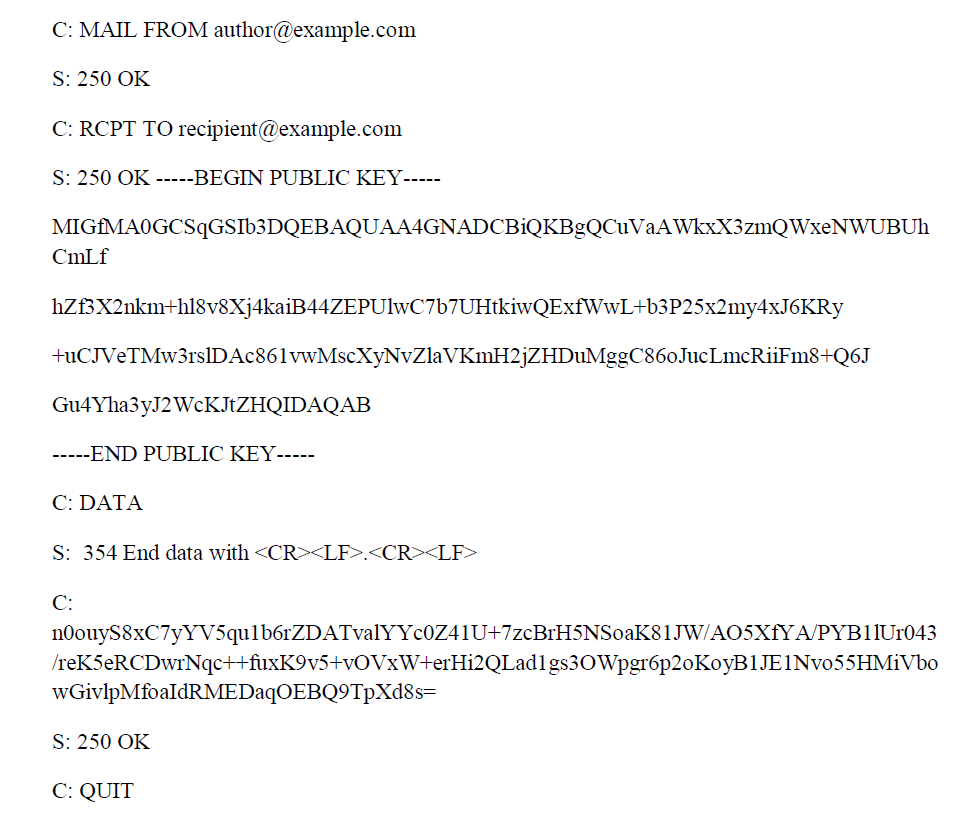
1. **REST API interfejs ka LogStash-u**

Upoznati se sa načinom na koji LogStash vrši transformaciju dobijenih logova u željeni izlaz. Implementirati aplikaciju koja u logstash konfiguraciju dodaje tipične templejte za prihvatanje podataka, odnosno preciznije omogućava CRUD aplikacije nad templejtima. Predvideti mogućnost izveštavanja o trenutno aktivnim paketima, i sl. Takođe omogućiti restartovanje logstash servisa nakon dodavanja templejta. Poželjno je aplikaciju razviti kao kozolnu aplikaciju u pajtonu, koja sve akcije ispoljava kroz REST API interfejs.



1. **Proširenje SMTP-a za šifriranje, ali po S-MIME standardu**

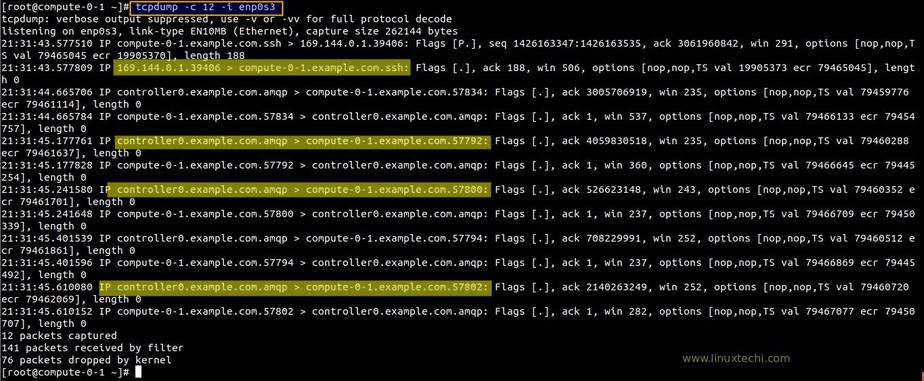
Proučiti aplikaciju za automatsko šifriranje imejlova koja se bazira na dopuni SMTP protokola. Upoznati se sa S/MIME standardom. Omogućiti razmenu poruka, ali po S/MIME standardu.





1. **Statistička obrada i logovanje mrežnog saobraćaja dumpcap/tcpdump alatom**

Upoznati se sa dumpcap/tcpdump alatom (alatima). Proučiti mogućnosti „*full-packet capture“*ovih alata. Implementirati aplikaciju koja prikuplja i loguje statističke podatke na osnovu izlaza ovih alata. Poželjno implementaciju izvršiti u pajtonu.



1. **Klasterizacija mrežnih alerta**

Upoznati se sa načinom za klasterizaciju podataka predstavljenom u [1]. Implementirati program/servis, koji za skup log zapisa koji se nalaze na ElasticSearch-u kreira dissimilarity matricu (Hemingova, Ekuklidska, Menhetn, ili Minkovski metrika), klasterizuje metodom aglomerativnog hierarhijskog klasterovanja i informaciju o pripadnosti klasteru dodaje (update-uje) uz odgovarajući zapis na ElastcSearch-u.

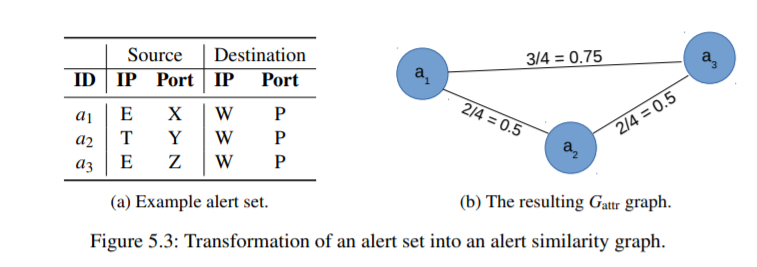
https://online.stat.psu.edu/stat555/node/86/

https://machinelearningmastery.com/distance-measures-for-machine-learning/

[1] Works Cited Hao, Lihua, Christopher G. Healey, en Steve E. Hutchinson. “Ensemble visualization for cyber situation awareness of network security data”. 2015 IEEE Symposium on Visualization for Cyber Security (VizSec). N.p., 2015. 1–8. Web.

1. **Vizuelizacija upozorenja o otkrivanju mrežnih napada u formi grafa**

Proučiti proces klasterizacije mrežnih alerta korišćenjem grafova u [1], u poglavlju 5.2.1. Implementirati konzolnu aplikaciju koja mrežne alerte i korelacije među njima predstavlja u formi grafa. Poželjno je aplikaciju implementirati u pajtonu.

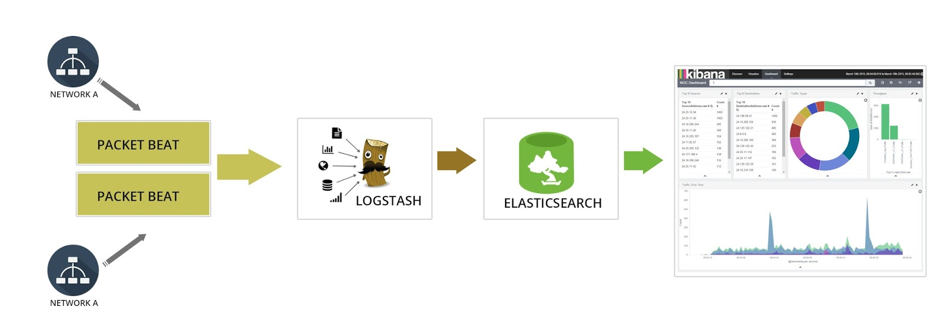


https://www.geeksforgeeks.org/visualize-graphs-in-python/

[1] Haas, Steffen. Security Monitoring and Alert Correlation for Network Intrusion Detection. Diss. Staats-und Universitätsbibliothek Hamburg Carl von Ossietzky, 2020.

1. **Analiza mrežnog saobraćaja upotrebom *Packetbeat* alata i ELK Stack-a**

Proučiti Packetbeat alat za monitoring mrežnog saobraćaja koji sakuplja mrežne pakete, preprocesira ih i šalje ka ELK stack-u. Implementirati Packetbeat alat na veb serveru laboratorije L3 i omogućiti obradu i slanje mrežnog saobraćaja ka Logstash-u.

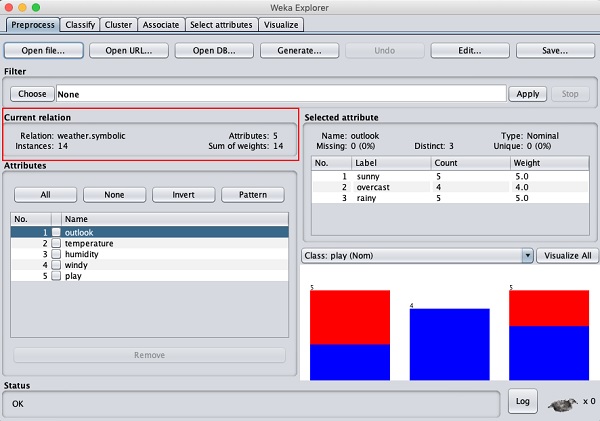


<https://www.elastic.co/beats/packetbeat>

<https://logz.io/blog/network-log-analysis-packetbeat-elk-stack/>

1. **Klasterizacija mrežnih napada DARPA2000 seta podataka upotrebom *Weka* alata**

Upoznati se sa DARPA2000 setom IDS podataka (načinom zapisa podataka i značajnim atributima). Proučiti Weka alat koji poseduje kolekciju algoritama mašinskog učenja i koji se primenjuje u različitim *data mining* problemima. Izabrati najpogodnije algoritme za klasterizaciju mrežnih podataka, primeniti ih nad DARPA setom i uporediti dobijene rezultate.



<https://www.ll.mit.edu/r-d/datasets/2000-darpa-intrusion-detection-scenario-specific-datasets>

<https://sourceforge.net/projects/weka/>

1. **Agregacija heterogenih alarma različitih IDS Sistema upotrebom IDMEF formata**

Proučiti IDMEF (*Intrusion Detection Message Exchange Format*) format za predstavljanje alerta IDS sistema. Upoznati se sa načinom integracije IDMEF formata i postojećih IDS sistema (Snort, Suricata i sl.). Izvršiti instalaciju bar dva različita IDS sistema i implementirati sistem za agregaciju njihovih alarma, upotrebom uniformnog IDMEF formata.

<https://www.ietf.org/rfc/rfc4765.txt> The Intrusion Detection Message Exchange Format (IDMEF)

Plugin za snort: <https://sourceforge.net/projects/snort-idmef/> (ili ručna transformacija upozorenja)