

Meeting

Axel Faes - 1334986

Feb 19, 2016

aanwezig: Bram Bonne, Pieter Robyns, Axel Faes

Professor Quax is aan het bekijken ofdat ik (gelabelde) netflow data kan verkrijgen van Cegeka. Dit zou heel handig zijn om mijn implementatie te testen op real world data.

Voorlopig moet ik enkel focussen op een passive intrusion detection systeem, geen preventie en niet direct inline in het netwerkverkeer. Ook de visualisatie moet later bekeken worden, de gebruiker is een netwerkadministrator. Er is tevens besproken dat python zelf mogelijk te traag is om packet sniffing op een goede snelheid uit te voeren. Hiervoor zou ik wireshark kunnen gebruiken (of de command line versie). Er is besproken om eventueel zelf datasets te genereren door malware te runnen op een VM of aparte machine.

De datastructuur voor de machine learning algoritmes is bekeken. Ik moet eens bekijken hoe de timestamps van de flowdata gebruikt kunnen worden. Om de effectiviteit (van de machine learning algoritmes) mogelijk te verhogen ga ik eens bekijken of ip-adressen ingedeeld kunnen worden in country-of-origin of iets dergelijks. Dit zou de machine learning algoritmes de mogelijkheid bieden om ook op deze parameter te bekijken of data malicious is of niet.

De actiepunten die gedaan zijn:

- Er is al een basis implementatie uitgewerkt voor het IDS
- De netflow structuur is bekeken en er is een datastructuur opgesteld die gefeerd kan worden aan verschillende machine learning algoritmes.
- Progressie in de machine learning cursus: chapter 3 van de 18.

Volgende actiepunten zijn besproken:

- Beginnen aan de thesis: het schrijven van een hoofdstuk over machine learning en over hoe deze algoritmes toegepast kunnen worden op een intrusion detection systeem.
- Verder werken in de machine learning cursus.
- Ik moet eens bekijken ofdat ik een programma vind om pcap files om te zetten naar netflow. Anders moet ik dit zelf schrijven.

Ik heb ook een korte planning gemaakt van hoe de thesis eruit zou zien:

- Inleiding:
 - wat is een IDS
 - Waarom is er gekozen voor dit type IDS (host vs netwerk)
 - Waarom voor data centers

- Waarom netflow
 - Waarom machine learning
- Wat is machine learning
- Hoe passen we machine learning toe op IDE en wat zijn de voor/nadelen
- Welke machine learning algoritmes zijn wel/niet gebruikt
- Wat zijn de voor/nadelen van netflow
- Hoe met combinatie netflow/packets (Als dit gedaan zou worden)
- Welke data sets zijn gebruikt
- Wat zijn de bevindingen
- Hoe kan visualisatie/feedback gebeuren (richting admin en richting automatische preventie)
- Conclusie