1. tjedan (13.07.2016. - 22.07.2016.)

Dosadašnji rad

Upoznao sam se s načinom rada IDS / IPS sustava

Proučavao sam literaturu vezanu za AIDE (Advanced intrusion detection enviroment) sustave

Upoznao sam se sa “Snort-om”, programom za detekciju neovlaštenih upada

Daljnji koraci

Detaljnija analiza načina rada “Anomaly based” i “Signature based” IDS sustava

Daljnje upoznavanje sa software-om za detekciju neovlaštenih upada

Dosadašnji rad

Proučena literatura kako mjeriti sposobnosti IDS sustava. Odabrana metoda temelji se ne teoriji informacije. Kako bi se mogla mjeriti sposobnost IDS sustava potrebno je imati evaluacijski set podataka. U tu svrhu kontaktirao sam Kanadski Institut za računalnu sigurnost koji je osigurao 100GB snimljenog prometa (u pcap formatu - ISCXIDS2012). Promet je sniman svaki dan kroz 24h ukupno 7 dana i sadrži različite vrste napada kao i promet klasificiran kao normalan. Uz svaki snimljeni dan prometa u pcap formatu nalazi se i xml datoteka u kojoj se nalazi detaljni opis svakog paketa, između ostalog i njegova klasifikacija kao normalan promet ili kao neka vrsta napada. Zbog velike količine podataka koju je potrebno analizirati, odlučio sam prvotnu analizu napraviti na drugom evaluacijskom dataset-u. Korišteni dataset je KDD CUP 1999 Data set (DARPA). Prvotnu analizu radim na 10% od ukupnog broja paketa. U KDD CUP99 data set-u svaki paket je klasificiran kao normalan promet ili kao određena vrsta napada. 4 osnovne podjele napada su: dos, probe, r2l i u2r; s 24 različita podtipa u “training” set-u i dodatnih 14 podtipova u “test” setu. Napisao sam program koji klasificira svaki od paketa, izračunava udio svakog tipa i podtipa prometa te izračunava baznu stopu detekcije koja je potrebna za izračun sposobnosti IDS sustava. S obzirom da je promet u pcap formatu, testiranje je moguće napraviti na jednom računalu, odnoso Snort IDS ima mogućnost analiziranja već snimljenog prometa. Problem s kojim sam se susreo jest da Snort pri rekonstrukciji nekih paketa generira veći broj paketa nego što to stvarno je s čime se naručava mjerenje sposobnosti.

Daljnji rad

Dobiti prve testne rezultate i provjeriti njihovu ispravnost.

Napraviti mjerenja nad ISCXIDS2012 datasetom