UNIVERSITATEA TEHNICĂ „Gheorghe Asachi” din IAȘI
FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE
DOMENIUL: Calculatoare și tehnologia informației
SPECIALIZAREA:Tehnologia informației

# Sistem de detecție a intruziunilor

LUCRARE DE LICENŢĂ

Coordonator științific
şef lucr.dr.ing Cristian Aflori

Absolvent
Cătălin Cristian Pomîrleanu

Iași, 2016

# Sistem de detecție a intruziunilor

Cătălin Cristian Pomîrleanu

# Rezumat

Lucrarea curentă își propune construirea unei aplicații care să permită captarea traficului la nivel de rețea și procesarea acestuia în scopul extragerii unor reguli de asociere care vor fi folosite în procesul de analiză a traficului. Totodată, prin intermediul unei structuri arborescente, se va realiza comprimarea traficului și se va rula procesul de detecție a semnăturilor atacurilor externe.

Aplicația deține o bază de date NoSQL care este populată cu logurile traficului de pe rețea. Utilizatorul are posibilitatea de a adăuga noi înregistrări și de a selecta eșantioane de date în vederea analizării acestora de modulul de detectare a intruziunilor.

În momentul accesării aplicației utilizatorul poate alege rularea procesului de detectare a intruziunilor folosind datele stocate în baza de date MongoDB. Totodată, aplicația afișează utilizatorului lista cu adaptoarele de rețea prezente pe mașina acestuia. Selectarea unui adaptor va permite scanarea traficului realizat la nivelul lui. Traficul monitorizat va fi afișat într-o tabelă din aplicație, tabelă ce va fi populată în timp real. Logurile noi ce momentan vor fi stocate în memorie vor putea, de asemenea, să fie trimise în baza de date. Este permisă o analiză imediată a acestora fără a mai fi implicată baza de date ca intermediar.

Modulul de detectare a intruziunilor va realiza o preprocesare a logurilor păstrând doar parametrii care au potențialul de a indica posibile atacuri. Algoritmul folosit în procesul de extragere a regulilor de asociere este Frequent-Pattern Growth (FP-Growth). Acesta va lansa procesul de extragere a pattern-urilor folosind o structura de date de tip arbore numita Frequent-Pattern Tree (FP-Tree). Rezultatul returnat de acest algoritm va fi folosit în analiza traficului de pe rețea. Pentru detecția atacurilor se vor folosi semnături ale unor atacuri cunoscute, semnături ce vor fi aplicate peste versiunea comprimată a traficului de la nivelul rețelei.

Rezultatul oferit de modulul de detectare a intruziunilor va conține lista cu tipurile de atacuri depistate și numărul acestora. Astfel, este posibilă crearea unui grafic bidimensional care va aloca una din axe pentru fixarea tipurilor de atacuri descoperite, iar cealaltă pentru afișarea numărului de atacuri de fiecare tip.