Studiul unor metode avansate de analiză a log-urilor pentru detectarea intruziunilor

Anca Puiu

Rezumat

Sistemele informatice bazate pe rețea au devenit o parte importantă a societății de azi. Pe măsură ce acestea au evoluat, au devenit în același timp potențiale ținte pentru o gamă din ce în ce mai variată de atacuri informatice.

Securitatea unui sistem informatic este compromisă în momentul în care are loc un access neautorizat care încearcă să compromită integritatea, accesibilitatea sau confidențialitatea unei resurse prin metode de întrerupere, modificare, interceptare sau replicare neautorizată a sistemului informatic. Infomațiile legate de astfel de evenimente precum și modul în care au fost tratate se regăsesc în mesajele de tip log generate de componenta de tip server web a unei aplicații software.

Analiza și interpretarea mesajelor de tip log este dificilă datorită volumului mare de date, precum și a modului de formatare al mesajelor: date de dimensiuni diferite, neomogene și în unele cazuri inconsistente.

Prezenta lucrare urmărește să studieze metode de analiză a acestor mesaje pentru a descoperi eventuale tipare de atac care nu au fost interceptate de soluțiile de securizare implementate la nivelul unui server. Analiza mesajelor de tip log se realizează cu ajutorul principiilor de extragere a informațiilor din date (tehnici de *data mining*), prin aplicarea unui algoritm de clusterizare asupra datelor de intrare.

Tehnicile de tip *data mining* sunt folosite pentru a identifica și extrage informații utile din colecțiile cu volum mare de date. Clusterizarea reprezintă una dintre tehnicile de tip *data mining* prin care se realizează gruparea datelor în funcție de gradul de similaritate al acestora.

Pe baza setului de rezultate obținute, se pot observa grupări care delimitează tiparele de acces general către o aplicație web. Atacurile infiltrate în aplicația web pot fi delimitate fie în grupări rezultate în urma aplicării acestor metode de analiză, fie se pot constitui sub formă de zgomote. În urma analizei acestor grupări, se poate consolida securitatea sistemului de calcul.