Aplicație de configurare și monitorizare pentru un sistem de detecție a intruziunilor

George-Sabin Mehedin

Rezumat

Sistemele informatice și de comunicații sunt într-o continuă dezvoltare și din această cauză securitatea lor a devenit o adevărată problemă, destul de importantă pentru producătorii de echipamente, aplicații software, cât și pentru administratorii de rețea.

Din acest motiv apare nevoia dezvoltării unei aplicații software pentru un sistem de detecție a intruziunilor, cum ar fi OSSEC. Practic, această aplicație permite atât configurarea sistemului, dar și monitorizarea activității rău intenționate.

De multe ori mi-am pus întrebarea: Ce se întâmplă în rețeaua mea în orice moment? Așa am ales să dezvolt o aplicație prin care să configurez un server ce detectează intruziunile și totodată să monitorizez activitatea utilizatorilor.

Detectarea intruziunilor este acțiunea prin care se pot vedea evenimentele inadecvate de pe un sistem de calcul. Un exemplu ar fi trimiterea de e-mail-uri secrete ale unei companii către concurență sau monitorizarea conținutului web accesat de pe anumite stații de lucru.

Configurarea serverului care detectează intruziunile, în cazul ales de mine, OSSEC, se face printr-o aplicație web care comunică cu serverul printr-un API sau modul dezvoltat utilizând limbajul Python. Serverul OSSEC se află instalat pe o mașină virtuală cu sistem de operare Ubuntu. Pe această mașină rulează și serverul de Python, care comunică cu aplicația web prin protocolul TCP. Aplicația web a fost creată folosind limbajul de programare PHP și se rulează pe același sistem.

În lucrare m-am axat pe implementarea unor facilități pentru administrarea unui server OSSEC cum ar fi: vizualizarea log-urilor în timp real, pornirea/oprirea/restartarea serverului, editarea fișierului de configurare, adăugarea de agenți noi și comunicarea acestora cu serverul.