REFERAT ASUPRA PROIECTULUI DE DIPLOMĂ

**,,** ***Analiza și valorificarea log-urilor colectate din echipamente și aplicații folosind tehnologia Elasticsearch”***

elaborat de ***stud*. *sg. maj. Lică Alexandru***

din Facultatea de Sisteme Electronice şi Informatice Militare

din Academia Tehnică Militară „Ferdinand I”

Proiectul elaborat de stud. sg. maj. Lică Alexandru abordează un domeniu de actualitate şi importanţă pentru organizaţii, companii şi instituţii publice civile dar şi pentru domeniile de apărare, ordine publică și siguranţă naţională. Astfel, implementarea și integrarea unui sistem centralizat de gestiune a log-urilor este deosebit de importantă deoarece acesta oferă o viziune de ansamblu asupra întregii rețele din care face parte.

Proiectul își propune implementarea unei rețele de dimensiuni mici și integrarea în cadrul acesteia a motorului Graylog-Elasticsearch, respectiv implementarea expresiilor regulate pentru parsarea log-urilor de text colectate, analiza și valorificarea lor pentru a evidenția tendințe, statistici sau anomalii în exploatarea normală a sistemelor.

Prezenta lucrare de licență este structurată pe 5 capitole prezentate într-o succesiune logică, toate referindu-se la tematica acesteia, astfel:

Capitolul 1 prezintă importanța temei alese împreună cu conceptele ce urmează a fi prezentate.

Capitolul 2 prezintă elementele de bază în ceea ce privește fișierele jurnal, modurile de gestionare, analiză și stocare a acestora precum și avantajele analizei log-urilor în investigarea unei intruziuni.

Capitolul 3 prezintă diferite soluții tehnologice folosite pentru indexare distribuită și management al log-urilor.

Capitolul 4 este destinat prezentării aplicației demonstrative. Acest capitol descrie modul în care este configurată topologia aleasă precum și pașii care trebuie urmați pentru a configura sistemul Graylog-Elasticsearch.

Concluziile și direcțiile ulterioare de cercetare sunt prezenate în capitolul 5.

Lucrarea dezvoltată conţine un şir de concluzii bine definite, un glosar de termeni tehnici şi o listă bibliografică.

Pentru realizarea aplicației practice studentul a avut în vedere utilizarea celor mai noi tehnologii iar implementarea rețelei și integrarea sistemului de gestiune a log-urilor s-a realizat conform scenariului definit prin intermediul mașinilor virtuale.

În încheiere doresc să pun în evidenţă câteva din calităţile lucrării realizate de stud. sg. maj. Lică Alexandru:

* caracterul științific și documentat al proiectului, rezultat al mai multor căutări în lucrări de specialitate, pe Internet, dar mai ales în standardele actuale ale acestor tehnologii;
* analiza modului de operare în diferite situaţii şi creearea unor scenarii bine definite;
* folosirea în cadrul proiectului a unei terminologii specializate pentru descrierea tehnologiilor utilizate;
* utilizarea unei game largi de tehnologii în cadrul proiectului.

În concluzie, apreciez că lucrarea elaborată de stud. sg. maj. Lică Alexandru scoate în evidenţă calitățile profesionale ale autorului în abordarea unor probleme complexe și de actualitate. Consider că, absolventul a rezolvat în condiţii foarte bune cerinţele impuse şi sunt de acord cu susţinerea proiectului de diplomă în faţa comisiei.

Bucureşti, 03 Iulie 2019 Col. conf. dr. ing.

Ion BĂDOI