Ασφάλεια Συστημάτων και Υπηρεσιών - ΗΡΥ 413

Αστερινός Καράλης – Ζωγραφούλα Ιωάννα Νεαμονιτάκη

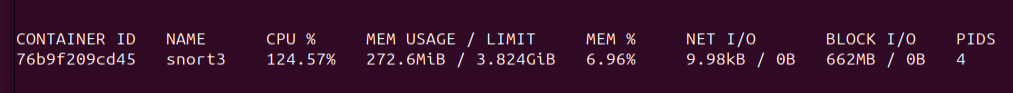
Part 5

Το μεγάλο αρχείο output.pcap που χρησιμοποιήθηκε στο part 5 δεν κατέβηκε έτοιμο από κάποιο link, αλλά είναι ένωση διάφορων pcap files των 150 MB το καθένα όπου βρέθηκαν στο link: [Publicly available PCAP files](https://share.netresec.com/s/nF5zNcaXLgwdQFZ)  
Παρατίθεται και το link για το αρχείο που φτιάχτηκε από την ένωση pcap files, το οποίο είναι ανεβασμένο στο OneDrive: [output](https://tucgr-my.sharepoint.com/:u:/g/personal/zneamonitaki_tuc_gr/ETrOb30_XQBBqz4MOFGEX5UBJ1raOpL2gbYNsTpUD7HoHw?e=0KqLuI).pcap

Τα στατιστικά φαίνονται παρακάτω:



Ο συνολικός χρόνος που κάνει το snort να επεξεργαστεί τα πακέτα είναι 14.5976 seconds και τα συνολικά πακέτα που εξετάστηκαν ήταν 1500812.  
Παρακάτω φαίνεται το CPU και memory usage τρέχοντας σε διαφορετικό terminal και με παράλληλη την επεξεργασία του output.pcap, την εντολή docker stats snort3:



To CPU είναι στα 124% κατά την διάρκεια της επεξεργασίας διότι το τρέχουμε σε VM και οφείλεται στο μεγάλο pcap file, το οποίο σημαίνει ότι το snort χρησιμοποιεί παραπάνω από έναν πυρήνα. Το memory usage είναι στο 6.96% το οποίο είναι φυσιολογικό και μέσα στα επιτρεπτά όρια.

Τα προτεινόμενα actions που θα μπορούσαμε να κάνουμε είναι να τρέξουμε ένα ruleset το οποίο να είναι μικρότερο για να μην γίνονται πολλές συγκρίσεις.

Άλλη μια βελτιστοποίηση που βρέθηκε στο διαδίκτυο είναι να αντικατασταθεί το Libcap library που χρησιμοποιείται από το snort με το framework DPDK.

Πηγή: [Performance optimization of Snort based on DPDK and Hyperscan - ScienceDirect](https://www.sciencedirect.com/science/article/pii/S1877050921006141)