Basic Packet Capture with Snort

לאחר התקנת snort על מחשב linux (השתמשתי בC9 ) התחלתי להקליט את התקשורת ע"י הרצת הפקודה:

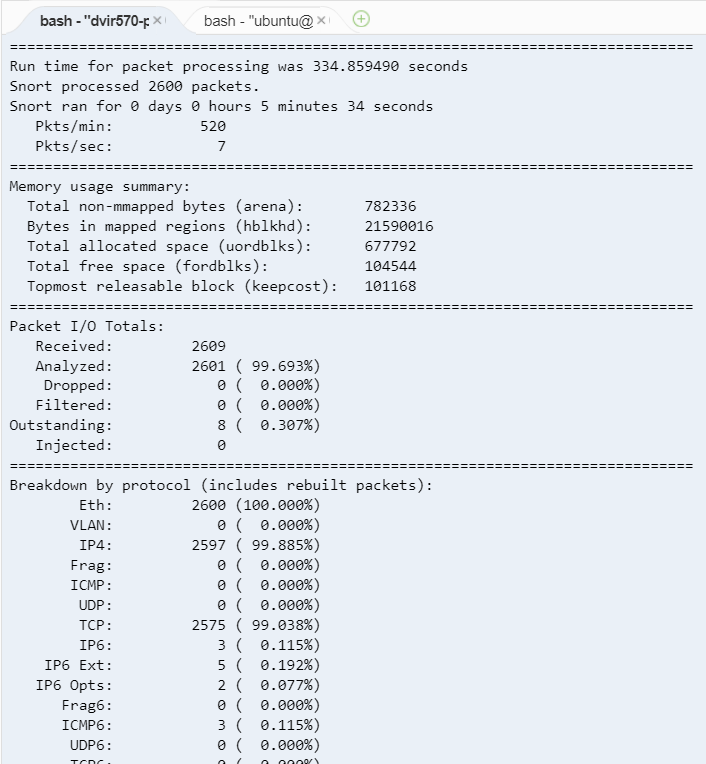
snort –i eth0 –v

כאשר –i eth0 מגדיר את הממשק שבו אני מעוניין להסניף (פעולה זו נחוצה מפני שזו הפעם הראשונה שאני מסניף, מכאן ואילך אין צורך להשתמש שוב בדגל הזה, אלא אם ארצה להקליט מממשק אחר).



בסיום ההקלטה ע"י לחיצה על ctrl+C נקבל סיכום על ההקלטה.

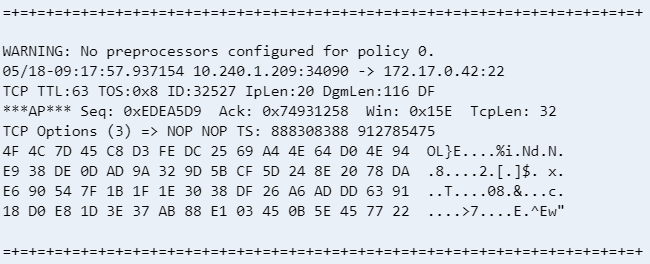
בסיכום זה מופיעים פרטים כמו משך זמן ההקלטה, קצב ממוצע של פקטות שהוסנפו, משקל ההסנפה (כמה זכרון היה בשימוש),סך כל הפקטות שנקלטו וסייוג של הפקטות לפי פורטוקולים כך שנוכל לדעת כמה פקטות הוסנפו מכל פרוטוקול.



בהרצת הפקודה

snort –dv

הודפס לטרמינל גם התוכן של הפקטות עצמן משכבת האפליקציה:



ע"י הרצת הפקודה

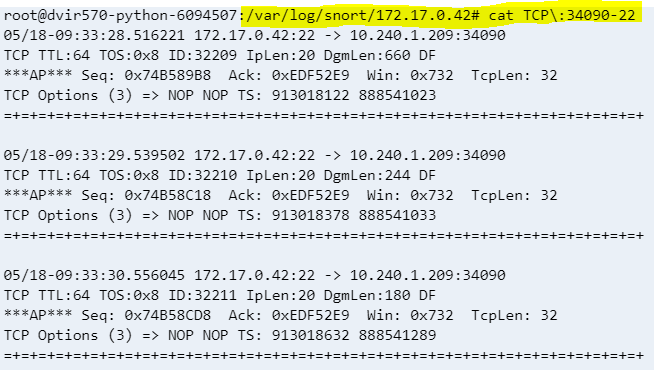
snort –h נוכל לראות את כל הדגלים שאנו יכולים להוסיף:



בהרצת הפקודה

snort –K ascii

ההקלטה נכתבה לתוך קבצי לוגים בתקייה var/log/snort מסווגת לפי כתובת הipaddress שמעורבות ב-session, הפורטים והפרוטוקול שהיה בשימוש:



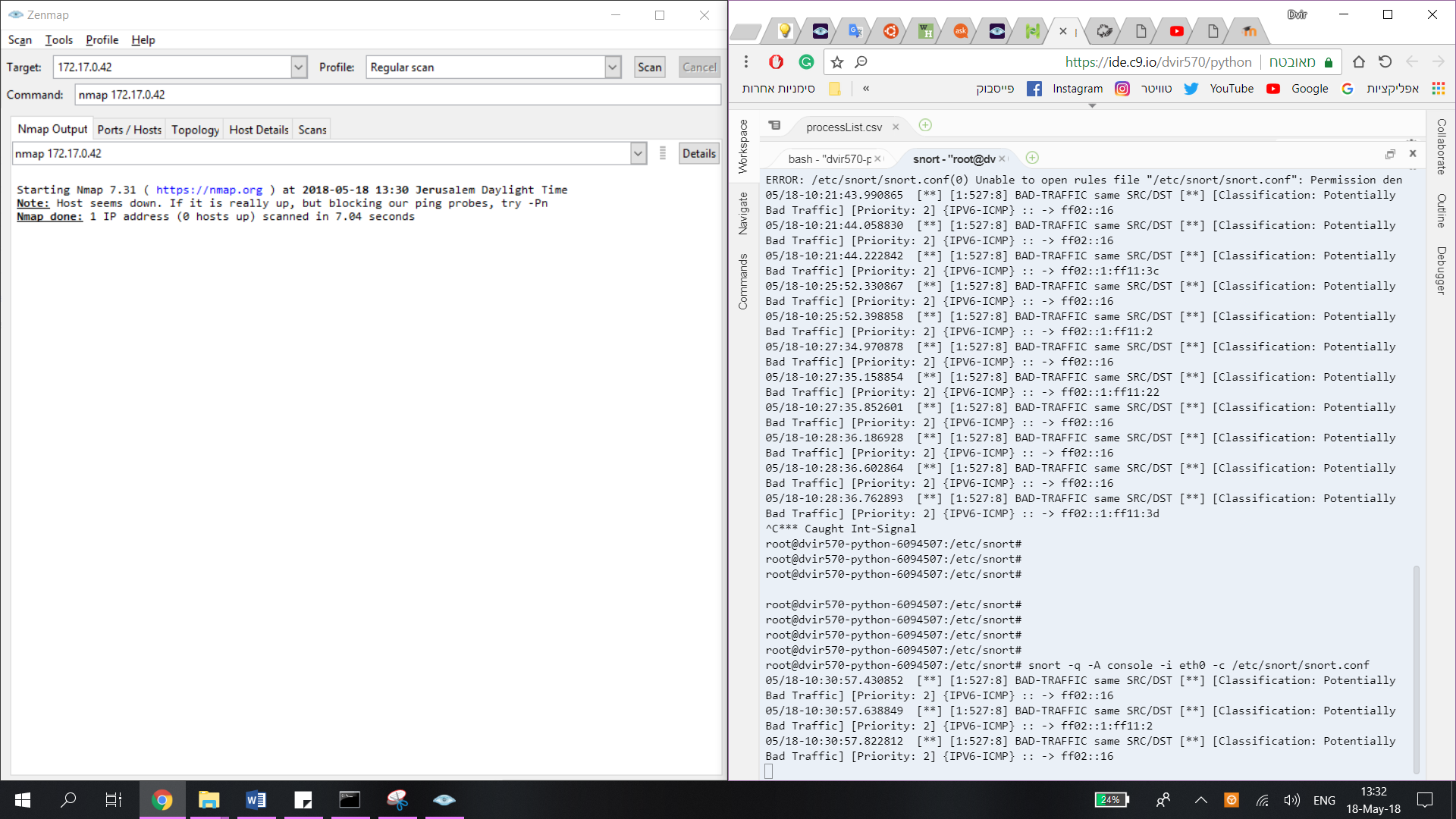
הדגל A- מקבל מצב התראה (fast, full, none, and unsock), וישנה בקובץ הקונפיגורציה בהתאם למצב שנבחר את מצב ההתראה עבור הדגימה. לפי המצב שיבחר יווצרו התראות מתאימות.

IDS Alerts

בהרצת הפקודה

snort -q -A console -i eth0 -c /etc/snort/snort.conf

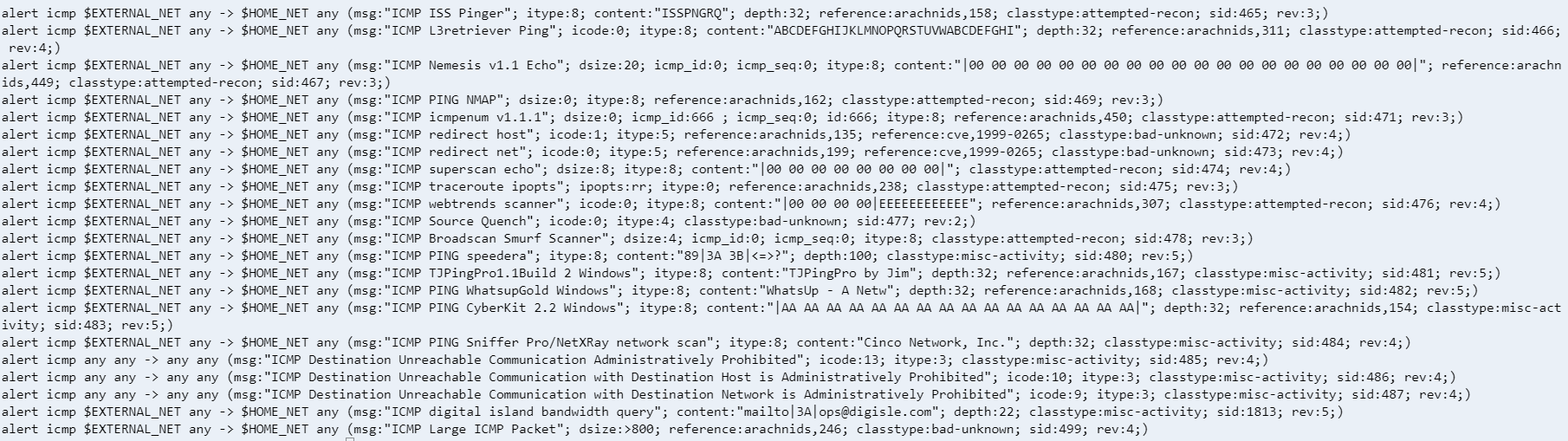
וביצוע של סריקת פורטים ממכונה אחרת על המחשב ע"י הכלי nmap הביא לתוצאה הבאה:



בתמונה זו ניתן לראות שהודפס למסך ה-console התראות על אירועים חריגים בגלל שעשיתי סריקת פורטים על המחשב.

**תמונות של כמה מהחוקים שסופקו:**

icmp.rules



dns.rules



ועוד חוקים נוספים..