מטלה 2 – מעבדת התקפה:

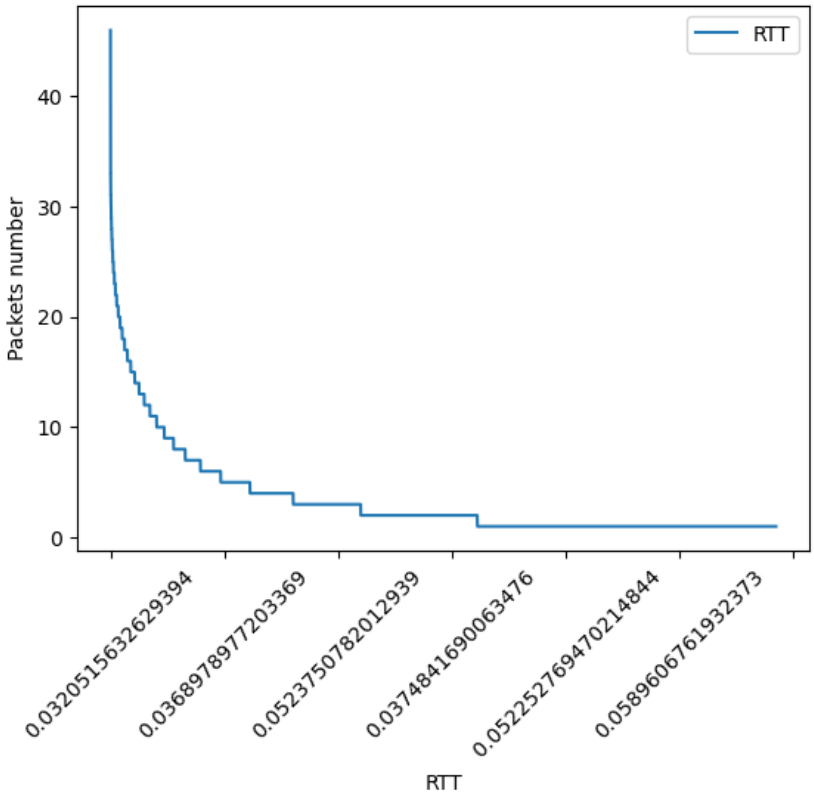
יובל בר מעוז, בן כהן

במטלה הנ"ל בנינו מתקפת DDOS בשתי שפות תכנות שונות C וpython, על מנת להשוות את המהירות של התוכניות מדדנו גם את מהירות שליחת הפאקטות בכל אחת מהתוכניות, וגם שלחנו ממחשב נפרד בקשות ping אל המחשב המותקף ומדדנו את מהירות הבקשה על ידי השרת המותקף.

*** עשינו את הגרפים על פי הבקשה שהייתה בעבודה וכאשר יצרנו אותם על פי ציר הY והX המבוקשים הגרפים לעיתים נראו מוזר. כאשר הפכנו את הצירים הגרפים נראו לנו יותר הגיוניים. ולכן הוספנו גם אותם קובץ הPDF.

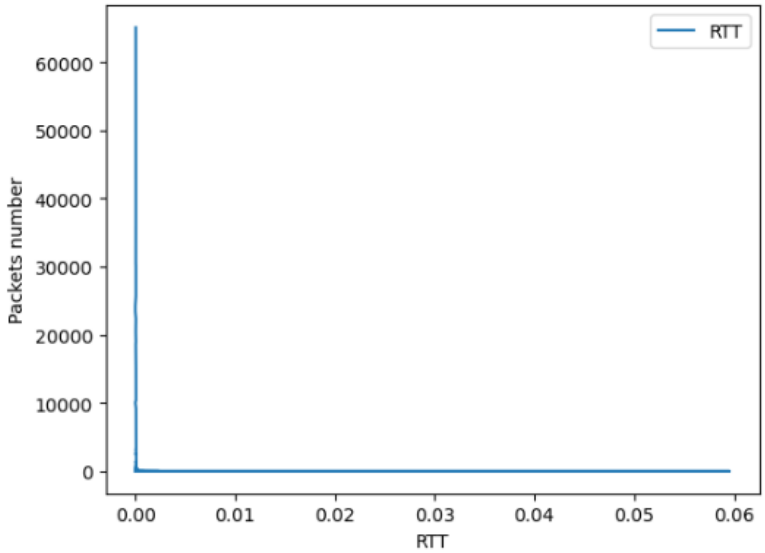
ממצאי המעבדה:

Syn_packet_p



RTT ממוצע לפאקטה – 0.046585630378723146 שניות.
זמן שליחה כולל – 46619.4866502285 שניות. (בערך 12 שעות)
STD - 0.026509590870472034 שניות
התמונה לעיל מציגה את מתקפת הSYN, ניתן לראות שנשלחו יותר מ40 פאקטות בRTT של 0.320515,

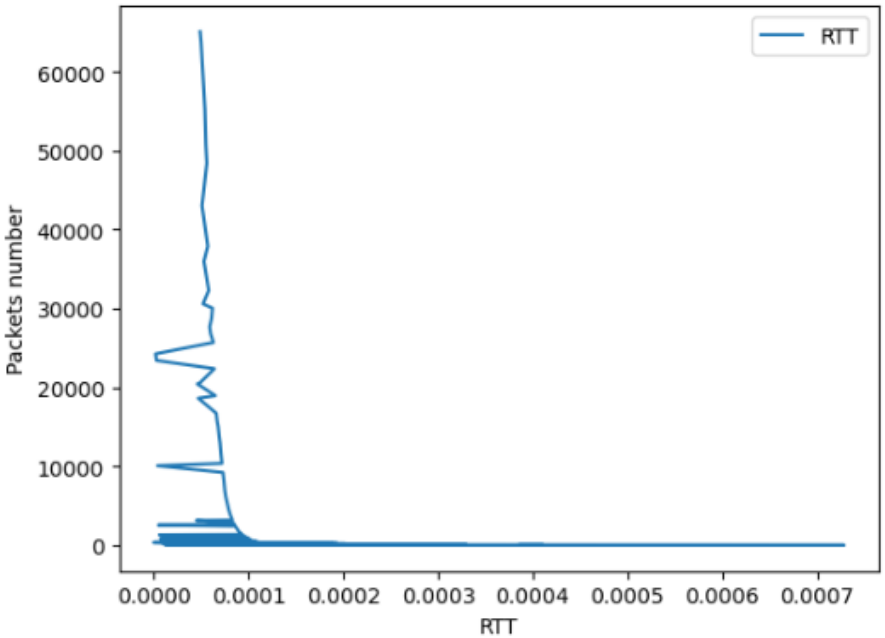
Syn_packet_c



RTT ממוצע לפאקטה – 0.00006264535477385 שנייה
זמן שליחה כולל - 67.566686 שניות
STD - 0.000105 שניות

בתמונה לעיל, ניתן לראות כי הרוב המוחלט של הפאקטות נשלחה בטווח הזמן שקטן מ0.01 שניות, על מנת להפוך את הגרף לקריא יותר, הוספנו גרף נוסף אשר כולל בתוכו את 500 נקודות הRTT הראשונות מתוך כלל הנקודות (1570), כך שהורדנו את הנקודות הזניחות, שבהם יש רק פאקטה אחת שנשלחה בRTT מסוים.

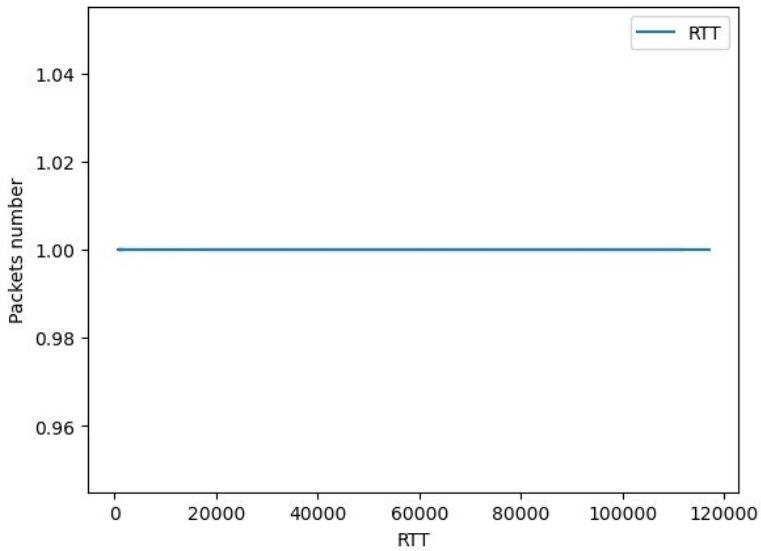
RTT 500/1570



ניתן לראות שכאשר לקחנו רק 500 נקודות מתוך סך הנקודות והורדנו את הנקודות הזניחות, שרמת הדיוק של הRRT הגיע לעשרת אלפית השנייה.

<u>סיכום syn:</u>
ניתן לראות שכאשר המתקפה ממומשת בשפת C, ממוצע הRTT של הפאקטות קטן פי 743 מממוצע הRTT של התוכנית בpython. כלומר כל פאקטה שנשלחה בשפת C נשלחה פי 743 יותר מהר מאשר פאקטות שנשלחו בpython, המהירות של השליחה משפיעה על מתקפת הDDOS והופכת אותה לעוצמתית יותר. מכך אנו מסיקים שגם הפינגים של תוכנית הC יהיו איטיים יותר, כלומר המתקפה עובדת ויש עומס על השרת המותקף.

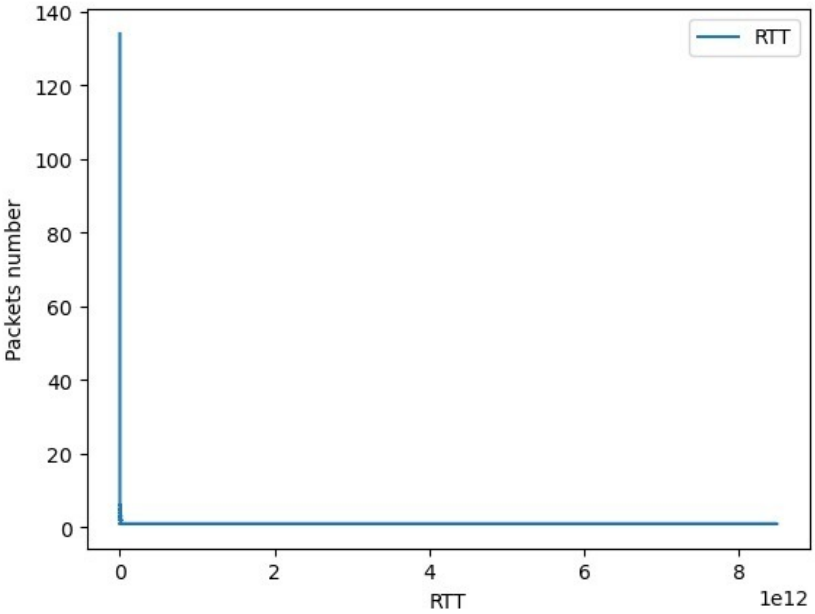
Pings_results_c



RTT ממוצע לפינג – 17.338142857142856 מילי-שניות
SDT - 39.6787196975499 מילי-שניות

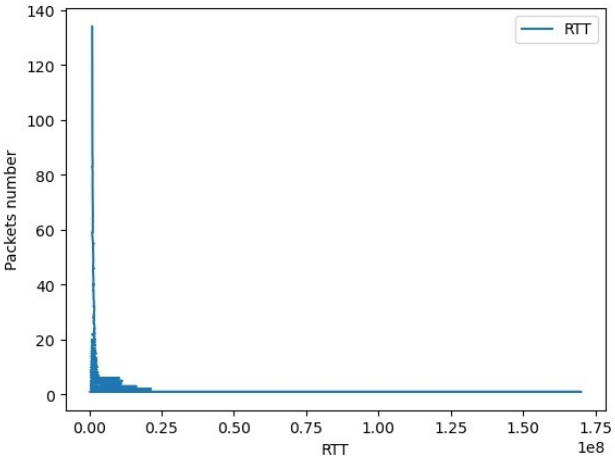
כיוון שתוכנית הC עבדה מהר יחסית היא סיימה לרוץ בתוך קצת יותר מדקה, אנחנו שלחנו פינג ממחשב הmonitor בכל 5 שניות, כך שבסופו של דבר נשלחו רק 14 פינגים שונים, שלכל אחד מהם היה RTT אחר, וזו הסיבה שהגרף שלנו הוא קו ישר.

Pings_results_p

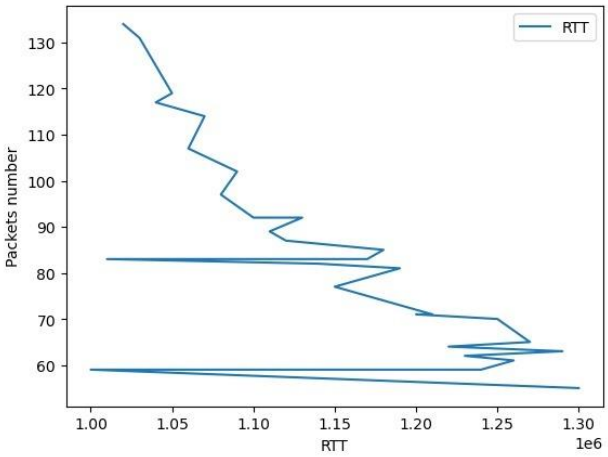


RTT ממוצע לפינג – 3.6950768733850055 מילי-שניות
STD – 119.5658982426305 מילי-שניות
מהגרף הנ"ל ניתן לראות שרוב הפינגים ששלחנו מהmonitor למחשב המותקף חזרו בפרק זמן קצר מאוד, כלומר מתקפת הDDOS שהפעלנו לא פעלה באופן עוצמתי מספיק. על מנת לראות את הגרף בצורה מיטבית, העלנו עוד שני גרפים אשר מורידים תוצאות זניחות (תוצאות של RTT שבהם היו לא הרבה פאקטות).

גרף א' – 900/1020 פינגים



גרף ב' – 30/1020 פינגים



משני הגרפים הנ"ל ניתן לראות שרוב הפינגים חזרו בפרק זמן שקצר מ 0.000025 מילי-שניות כלומר בערך זמן נורמטיבי של פינג, המתקפה בקושי מורגשת.

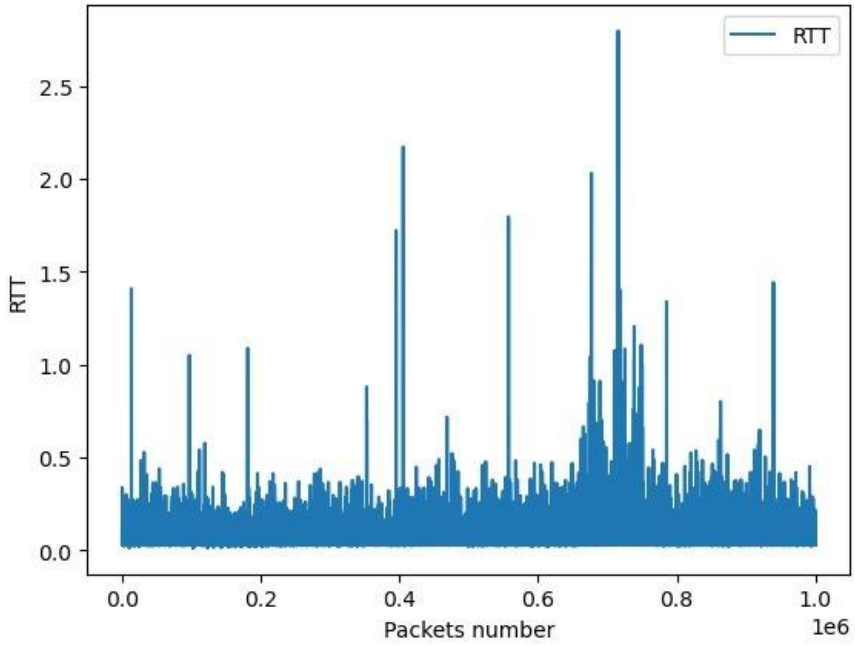
<u>סיכום ping–</u>
בנוסף, ניתן לראות שכאשר המתקפה בוצעה בC זמן הRTT של שליחת פינג הגיעה ms117 בשיא, בניגוד לפייתון שלא נראה חריגות כמעט בכלל למרות אורך המתקפה.
הRRT הממוצע לפינג בתוכנית C היה גדול פי 5.5 מהRTT הממוצע לתוכנית python.

<u>סיכום כללי</u> –
מהגרפים מעלה ומהמסקנות שהסקנו ולמדנו מהם קיבלנו עוד חיזוק להנחה המקורית שהייתה לנו שאמרה שתוכנית הDDOS בשפת C אפקטיבית יותר, הן מבחינת מהירות ההרצה שלה והן מבחינת ההשפעה שלה על המחשב המותקף.

כבר בזמן ההרצה שמנו לב להתרחשות, כאשר ההרצה של תוכנית הפייתון לקחה סביבות ה12 שעות, בעוד שההרצה של תוכנית הC לקחה בערך 3 דקות. כלומר השליחה הייתה של הפאקטות בC הייתה מהירה יותר, ולכן הגיוני גם שהיא יוצרת עומס על השרת.
ניתן לשער מהנתונים שאם היינו מריצים את התוכנה של הC ליותר איטרציות (יותר ממיליון) המתקפה הייתה ארוכה יותר והייתה משפיעה ומעמיסה על השרת הרבה יותר.

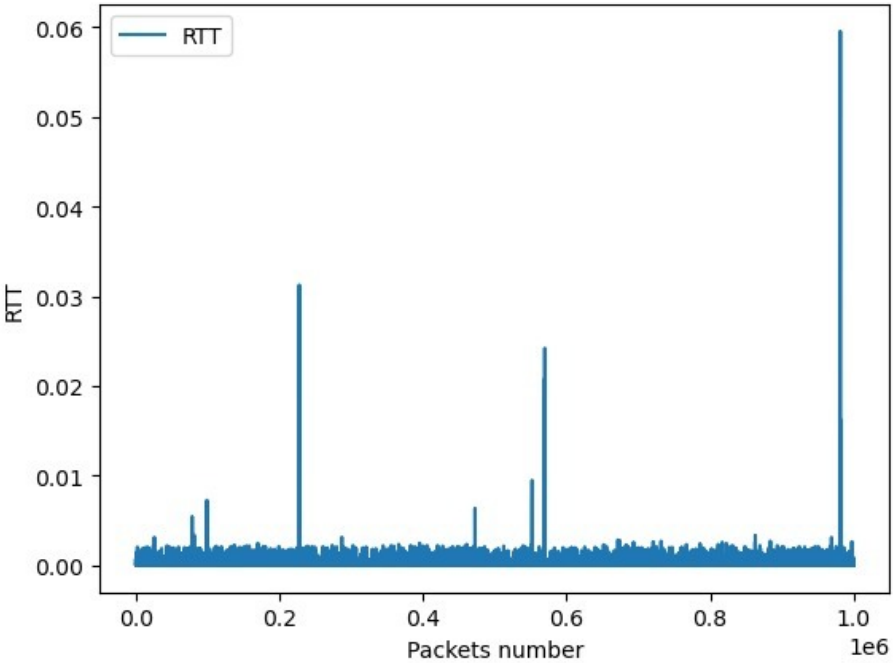
*** גרפים בהם ציר הX והY הפוכים –

Syns_packet_p



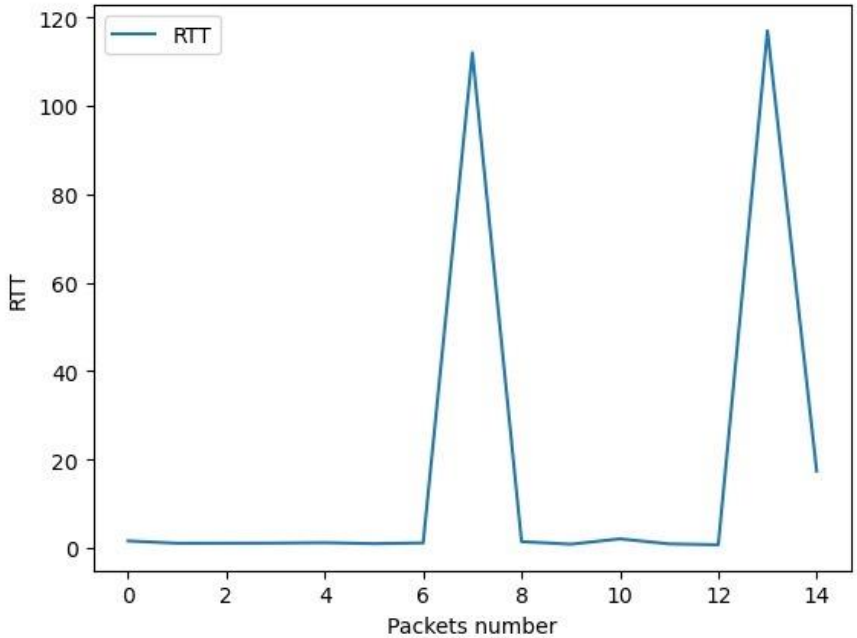
בגרף הנ"ל ניתן לראות את הRTT של כל פאקטת SYN שנשלחה לשרת המותקף.

Sync_packet_c



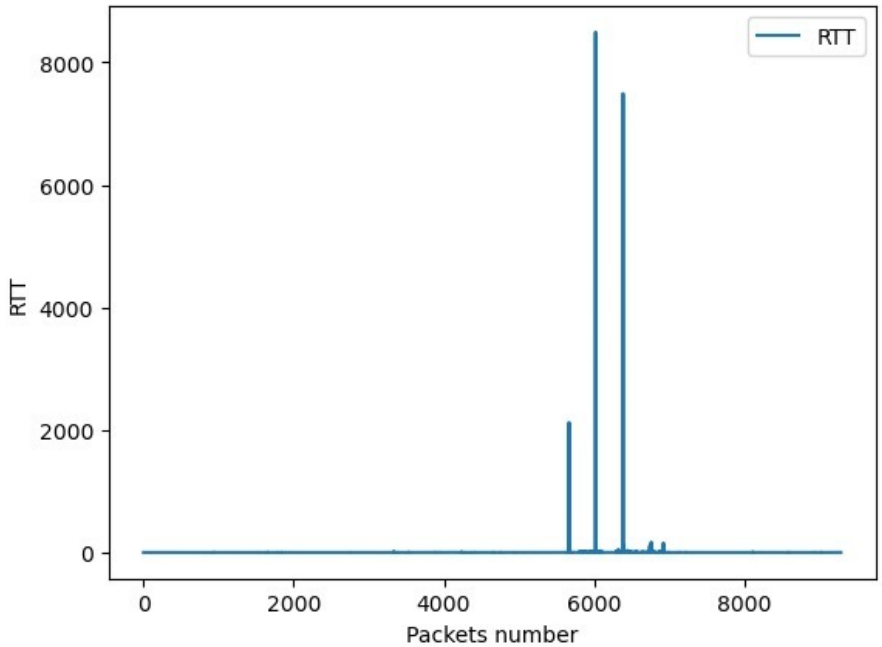
בגרף הנ"ל ניתן לראות את הRTT של כל פאקטת SYN שנשלחה לשרת המותקף.
ביחס לגרף של הפייתון ניתן לראות שהחסם העליון של גרף הC הוא RTT 0.6 וכאשר משווים אותו לגרף של הפייתון רואים שהיו הרבה חבילות SYN שנשלחו בפייתון בזמן קרוב ל0.6, ובתוכנת הפייתון זה נחשב זמן סביר. כלומר שליחת הפאקטות בפייתון ארכה זמן רב יותר.

Pings_results_c



בגרף הנ"ל ניתן לראות את הRTT של כל פינג שנשלח לשרת המותקף.
ביחס לכמות הפינגים שנשלחו (14) היו 2 פינגים שלהם RTT גבוה מאוד, דבר שהשפיע גם כל הממוצע וניתן לראות זאת בבירור מהגרף.

Pings_result_p



בגרף הנ"ל ניתן לראות את הRTT של כל פינג שנשלח לשרת המותקף. ביחס לגרף של תוכנת הC ניתן לראות שלא היו הרבה פינגים באופן יחסי (מתוך 9288) שהחזירו תוצאה גבוהה, גם שגם הממוצע היה 3.69 ms שזה RTT נורמטיבי לping. כלומר המתקפה בקושי השפיעה.