DDOS Attack lab

מגישות:

זוהר שמחון 211871868

אנה פינצ'וק 206431082

הקדמה:

במטלה זו היינו צריכים לבנות התקפת DDoS ששולחת חבילות SYN לשרת Apache מכתובות IP שונות לפורט 80. כתבנו את התוכנית בשתי שפות C ופייתון. הרצנו שרת Apache על קונטיינר תוכנית מוניטור בקונטיינר אחר והרצנו את התקפה מקונטיינר שליש. בכל התקפה, מדדנו את הזמן שנדרש לשלוח כל חבילת SYN, הזמן שנדרש להרצת התקפה כולה, הזמן הממוצע לשליחת חבילות SYN, וכן מדדנו את כל הפרמטרים הללו עבור תוכנית המוניטור. שמרנו את כל הנתונים בקבצים שונים, במהלך התקפה, ואז הרצנו תוכנית נוספת שתרגמה את התוצאות מטקסט פשוט לגרף לוגריתמי. מטרת המוניטור הוא לשלוח בדיקת פינג לשרת Apache כל 5 שניות, כדי לראות כמה השרת נמצא בעומס בכל אחת מההתקפות.

DDOS ATTACK IN C:

במקום לבנות פקטת SYN מההתחלה השתמשנו בפקודת nping ובעזרת הטרמינל הרצנו את הפקודה הנ"ל מיליון פעמים:

nping --tcp -c 1 -H -N --quiet --source-ip %s --seq %ld 10.0.0.8

ע"פ https://man7.org/linux/man-pages/man1/nping.1.html

נוצרת בקשת SYN אחת שנשלחת לכתובת 10.0.0.8 שהיא הסרבר אפאצ'י שלנו כאשר מספר הפקטה משתנה בקוד שלנו באופן עולה וה ip הוא משתנה רנדומלי.

כל שאר הפרמטרים נועד לקצר את זמני השליחה:

```
-H, --hide-sent      : Do not display sent packets.
-N, --no-capture     : Do not try to capture replies.
--quiet              : Set verbosity and debug level to
                       minimum.
```

DDOS ATTACK IN PYTHON:

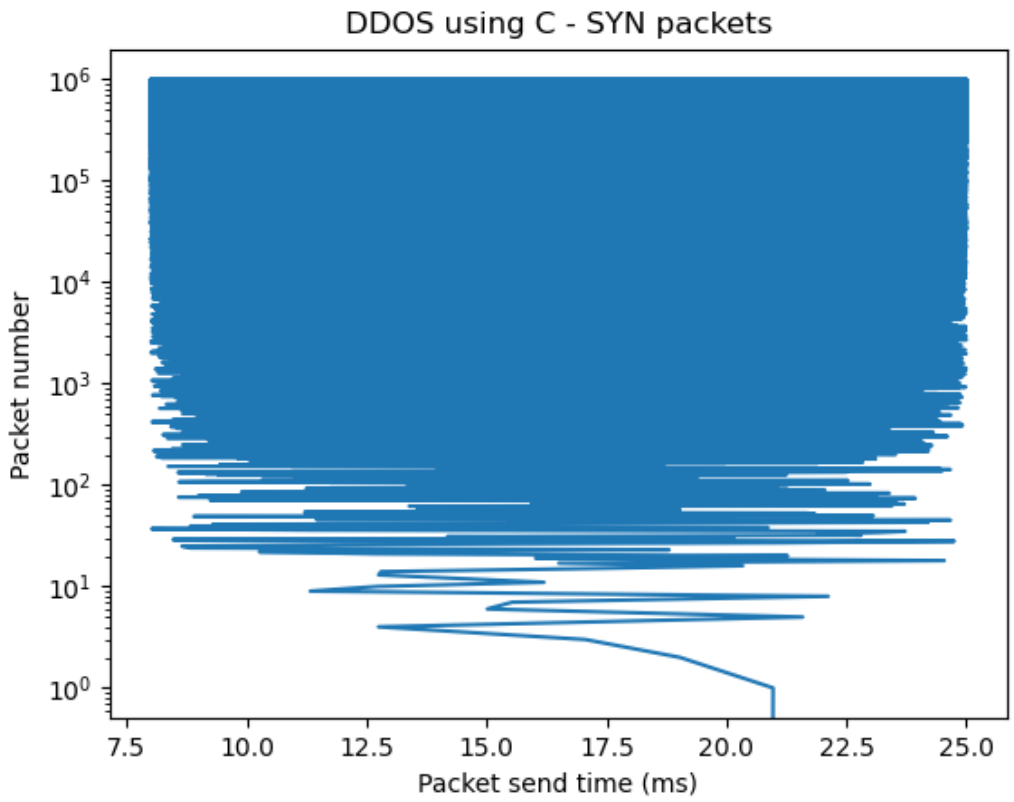
בנינו פקטת SYN בעזרת ספריית SCAPY שבה זה מתאפשר בפקודה create_syn_packet()

בכל אחת מההתקפות פתחנו ורשמנו לקובץ שמכיל את המידע על מספר הפקטה והזמן שלקח לה להישלח.

ממצאים:

DDOS ATTACK IN C:

גרף שמתאר את זמני שליחת פקטות SYN באמצעות שפת C.



<u>הזמן הממוצע לפקטה:</u>

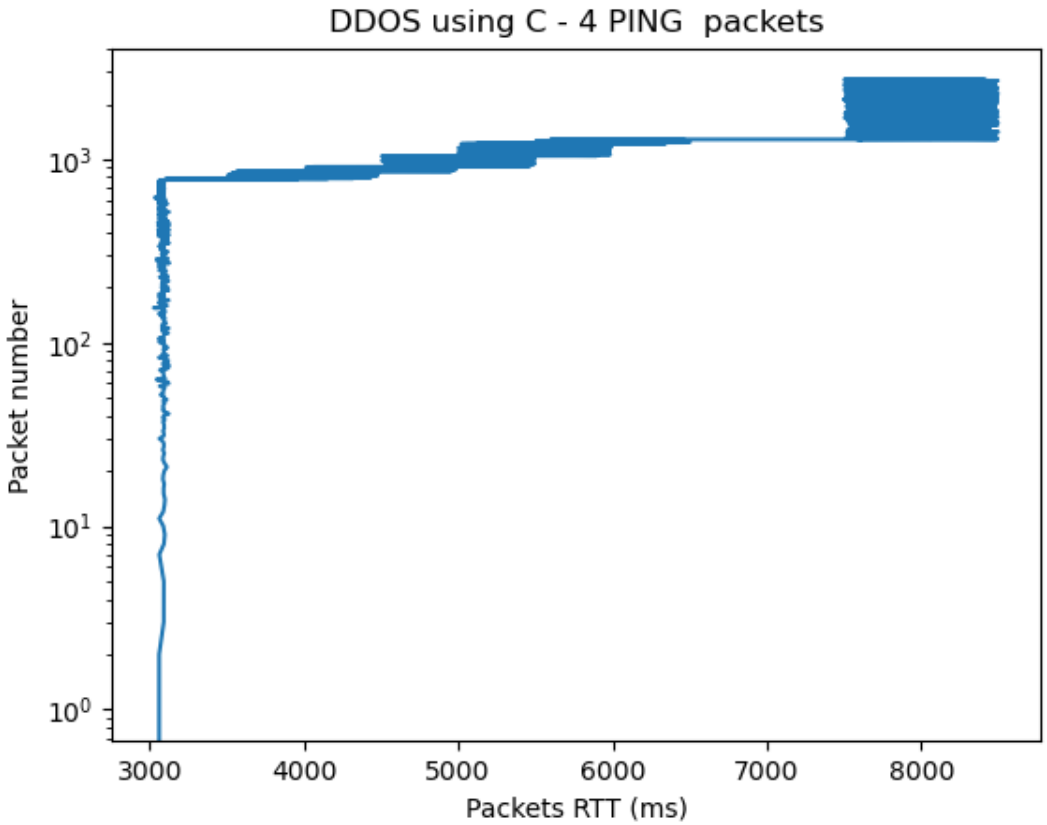
15.500052Ms

<u>זמן כולל של מתקפה:</u>

4.58347778 שעות

מוניטור:

גרף שמתאר את זמני ה RTT של 4 פקטות PING במהלך מתקפת DDOS הנעשית בשפת C.

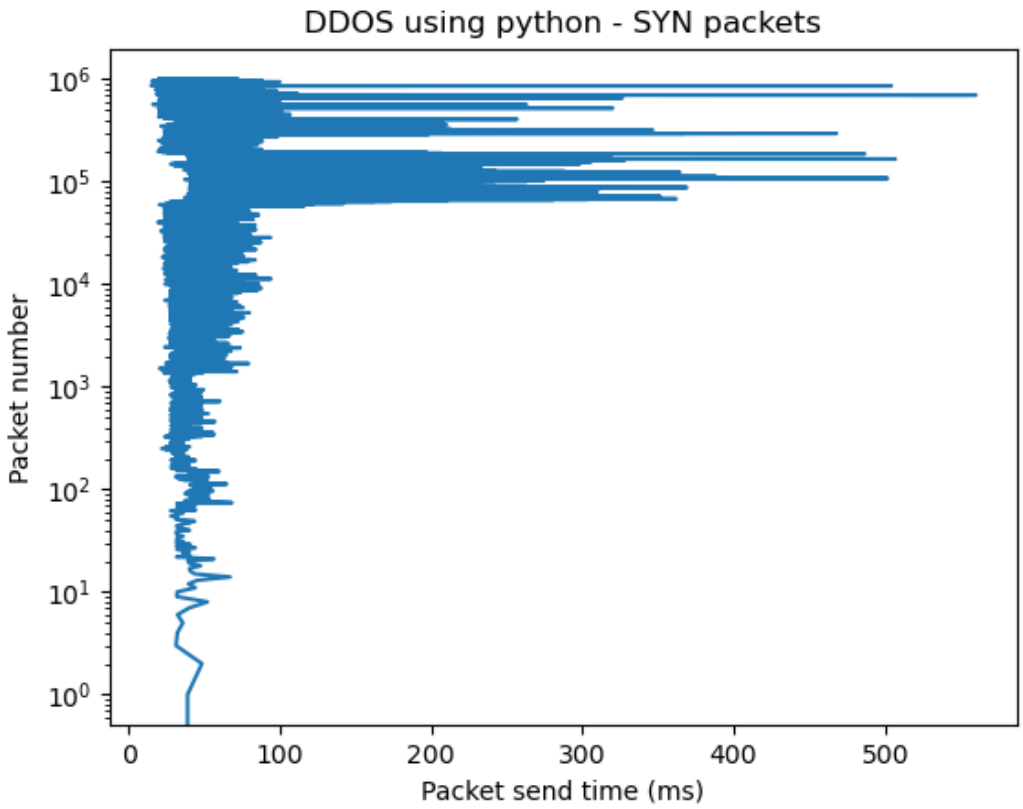


זמן ממוצע לשליחת 4 פקטות PING:

6057.487 ms

:DDOS ATTACK IN PYTHON

גרף שמתאר את זמני שליחת פקטות SYN באמצעות שפת Python



<u>הזמן הממוצע לפקטה:</u>

81.11924ms

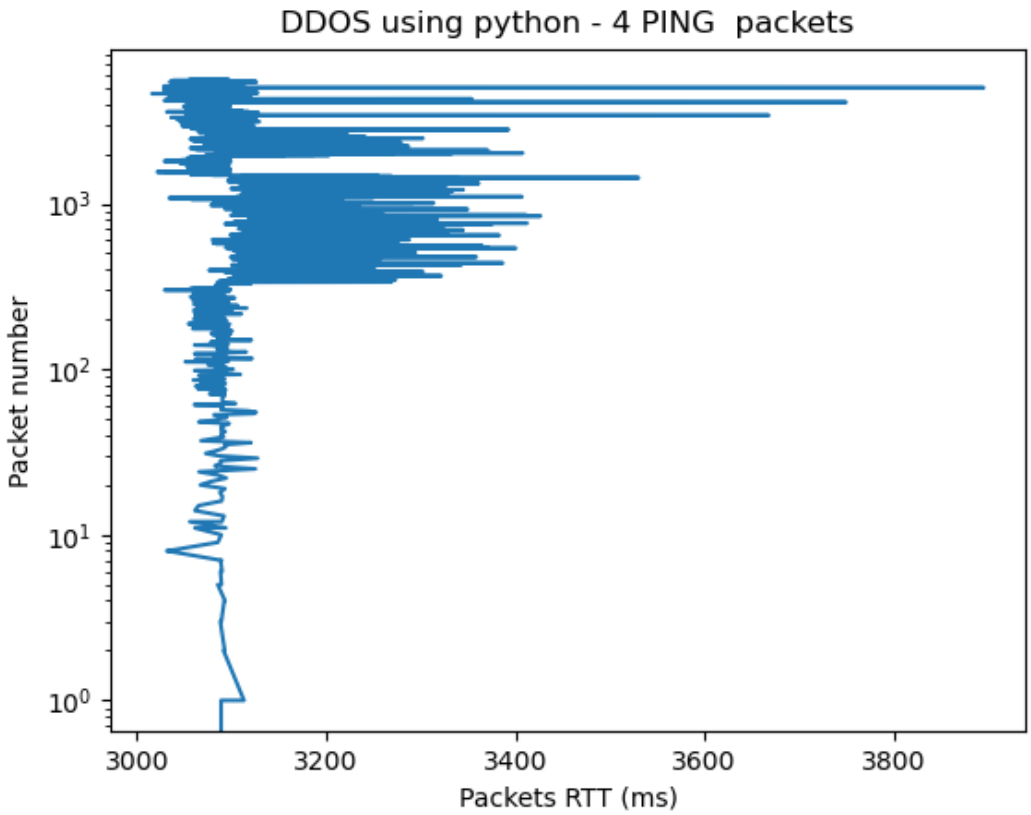
<u>זמן כולל של מתקפה:</u>

22.5331233 שעות

DDOS Attack lab

מוניטור:

גרף שמתאר את זמני ה RTT של 4 פקטות PING במהלך מתקפת DDOS הנעשית בשפת Python.



זמן ממוצע לשליחת 4 פקטות PING:

8579.983ms

מסקנות:

לפי הממצאים שלנו ניתן לראות יעילות התקפה גבוהה בשפת C מאשר התקפה בשפת פייתון משתי סיבות:

1. הזמן הכולל של המתקפה בפייתון קטנה משמעותית, מהזמן הכולל של המתקפה בסי. כך התוקף מבזבז פחות משאבים עבור המתקפה.

2. ניתן לראות שככל שהמתקפה נעשית בזמן מהיר יותר, כך זמן שליחת ה ping איטית יותר. וכאשר מדובר על מתקפה, אנו רוצים להאט את זמן התגובה של השרת הנתקף, ובכך לפגוע בשירותיו.

ולכן אם כותבים התקפה שדורשת יצירה ושליחה של הרבה תעבורה ברשת נעדיף לעבוד בשפת C.