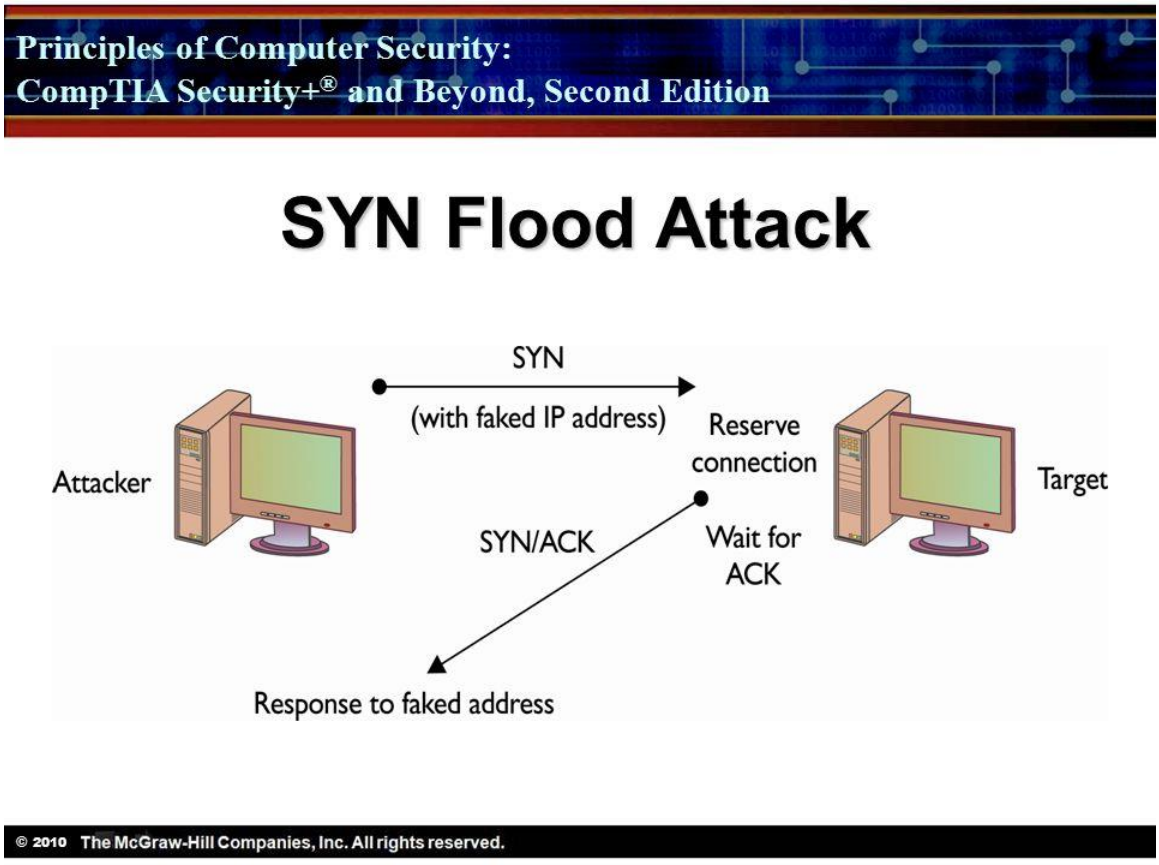
# דו״ח מעבדה- תרחיש מס׳ _אחרון_

פרטים :

מגיש :יגאל נאמן

תאריך :6.1.2019

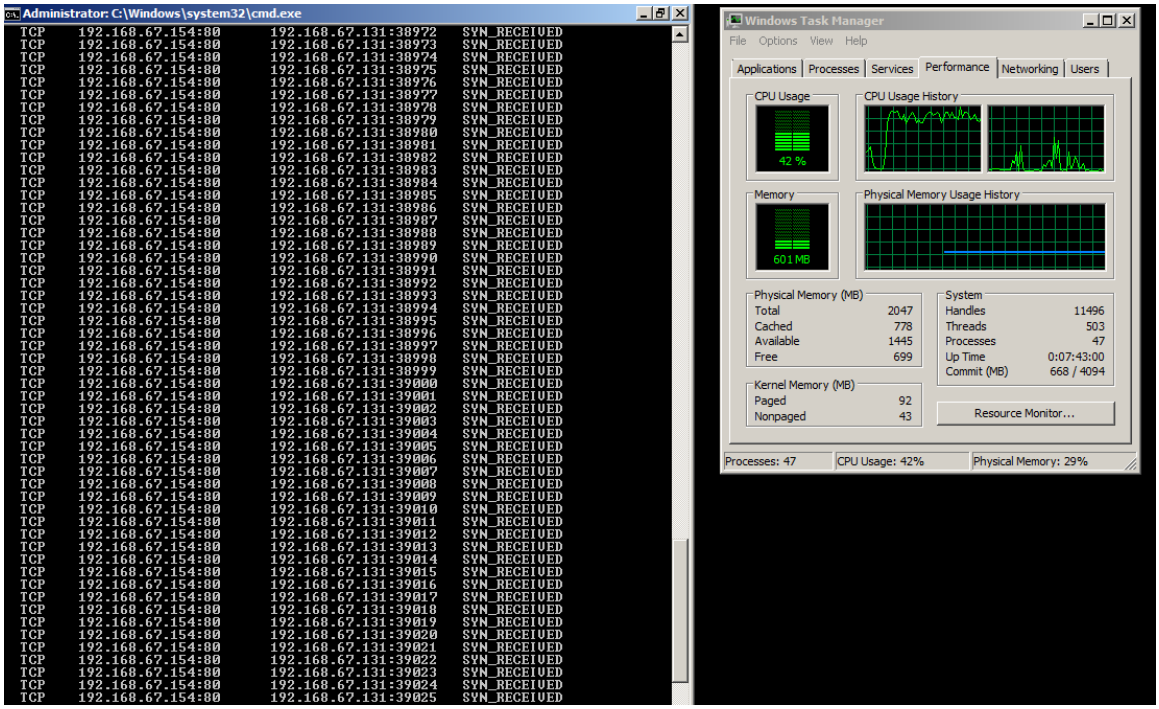
שם התרחיש :Ddos Syn Flood



איך תהליך ההתקפה נראה במחשב התוקף ב LINUX KALI :

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~#
root@kali:~# hping3 -S --flood -V www.hping3testsite.com
using lo, addr: 127.0.0.1, MTU: 65536
HPING www.hping3testsite.com (lo 127.0.0.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- www.hping3testsite.com hping statistic ---
746021 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

וכך זה נראה אצלנו דוגמא להמחשה :




ניתן להבחין גם ש ה- CPU גבוהה זה אומר ש ה- PING שהתוקף מכיל הוא מכיל גם DATA פירוש הדבר שזה ישפיע יותר על תעבורת הרשת מבחינת עומסים.

## תהליך ההתקפה:

תהליך שבו התוקף שולח בקשות בפרוטוקול http בתעבורת tcp לשרתי ה web

apache2,apache3,Apache1

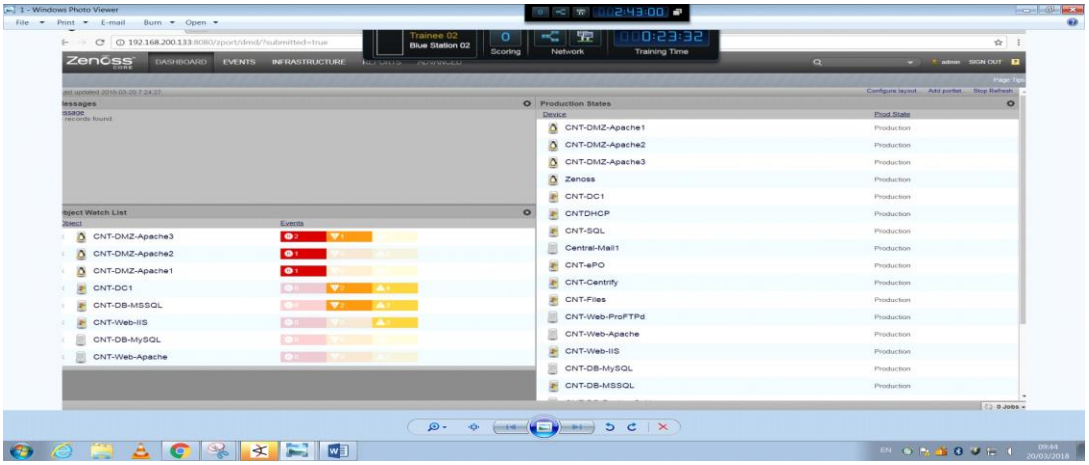
Tcp - פרוטוקול tcp

במהלך ההתקפה התוקף שולח בקשת syn לאחד השרתי apache וה apache מחזיר לו בתגובה syn+ack כלומר הוא מצפה לתשובה בחזרה ack אך הוא איננו מקבל תשובה בחזרה כתוצאה מכך הפורט תפוס והתוקף שולח הרבה בקשות בזמן קצר וכתוצאה מכך נופלים השרתים ואינם מספקים את השירותים קבלת דף html

## תהליך הזיהוי:

1)כניסה ל zenoss

בzenoss נמצא שלושת שרתי ה apache שמספקים שירותי web נפלו




לאחר מכן נכנסנו לבדוק את הזמנים של נפילת השרתים שהזמנים משמשים לנו כעוגן

השעה 9:40

2) tracker smartview -בשלב זה פילטנרו את התעוברה לפי השעה שבה השרתים נפלו וראינו כי הוא קיבל הרבה פאקטות עד למצב שבו הוא לא יכול לקבל פקטות יותר ואז מבצע drop לפקטות שמגיעות אליו

מכאן נגיע למסקנה על תהליך התקיפה שהתוקף בזמן קצר

(**וזה מרמז לנו שיש להגביל את הכמות הבקשות לשנייה** ) כי התוקף שולח הרבה בקשות ולא מחזיר ack לכן הפורטים תפוסים והדבר מונע גישה לאותם שרתי apache סוג תקיפה זאת נקראת FLOOD SYN DDOS

תהליך הגנה:

מניעה עכשווית-במידה ואנו מזהים בזמן קצר הרבה בקשות יש למנוע זאת ולהגביל את כמות הבקשות בזמן קצר (פיקוח על בקשות בזמן קצר)

c (time,idle,ms1)

for now we need to block the request milie seconds that cannot come from outside to my servers, for example:

dean 102.30.10.1 -> ping 138.1.1.200

dean 102.30.10.1 -> ping 138.1.1.200

dean 102.30.10.1 -> ping 138.1.1.200

so if the attacker use by SYN FLOOD so it (repate the ping) in the sametime 'ms0' the mean something happen over the backround,(**Abuse ping**)

so we need to take a rule to block this class 102.30.*.* by firewall/**snort** etc

תהליך הגנה מונעת:

מניעה לטווח הארוך – במידה והשרת רואה זמן המתנה ארוך מהמשתמש יעשה יסגור את הsocket (חיבור )

## הפרצות באבטחת הארגון

1)לא היה חוק שמגביל את כמות הבקשות בזמן קצר!!!

2)לא הוגדר חוק **SNORT**

## כלים שפיתחנו

בתרחיש זה לא פיתחנו איזשהו כלי או הגדרנו חוק להגבלת הבקשות

## אופן עבודת הצוות

במהלך עבודתנו חילקנו תפקידים :

1)ניגש ל zenoss וזיהה כי השרתים נפלו

2)חקר את הפאקטות ב firewall

3)נכנס לשרתים עצמם כדי לראות שאין כניסות לשרתים

4)ניהול התרחיש וחילוק תפקידים