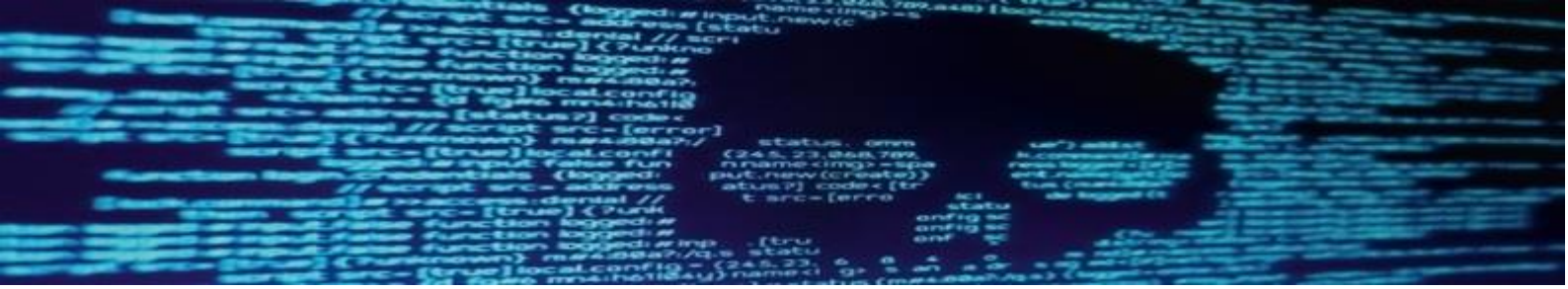


# Homework 4 - SYN FLOOD & TCP

## 1. כללי

- בחלק הראשון של מעבדה זו נלמד על חולשת פרוטוקול TCP אשר מאוד נפוץ היום, היות והקמת התקשורת מבוססת על פרוטוקול זה. בנוסף נלמד על חולשת ההצפנה SYN FLOOD והשימוש שלה בפרוטוקול TCP.

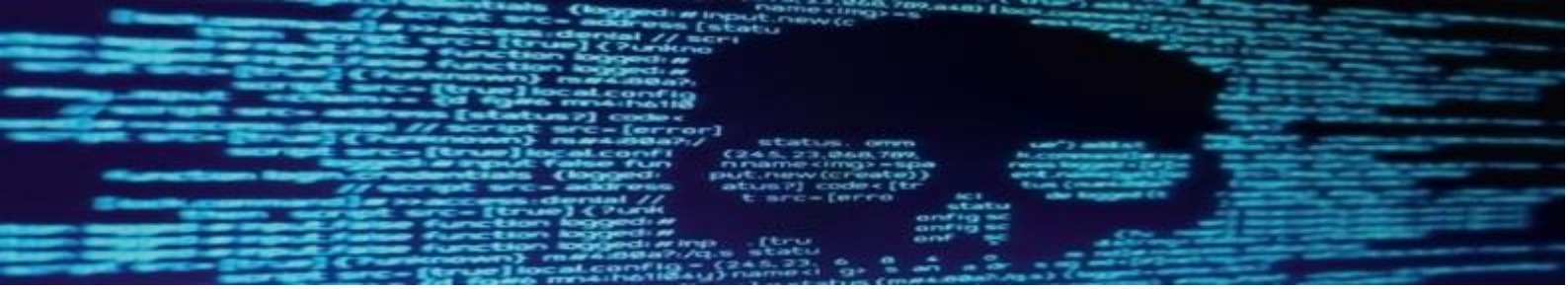
  בתקשורת נתונים, הצפנת (SYN FLOOD) SYN היא סוג של התקפת מניעת שירות (DOS) המנצלת פרצת אבטחה במנגנון הקמת הקשר של ה-TCP.
- בחלק השני נבנה סקריפט בפייתון, המבצע בצורה איטרטבית שליחה של syn packet ובכך ניצור התקפת syn flood.
- את המעבדה יש להגיש בזוגות באתר moodle בפורמט הבא:

  LAB4_SYN_ID1_ID2.pdf
- **קראו היטב את המשימות. ענו על שאלות ההכנה והשאלות במהלך הניסוי.**
- **במידת הצורך צרפו תמונות וצילומי מסך המתאימים לתשובתכם.**
- **לפני שאתם מבצעים צילומי מסך הריצו מהטרמינל את הסקריפט print_names.py (ערכו אותו כך שיכיל את השמות והת"ז שלכם). השורה צריכה להופיע בתמונה.**

```
root1@kali:~/Desktop/DHCP$ python3 print_names.py
Israel Israeli 102030405 | Dani Din 506070809 | Sun Oct  4 13:21:03 2020
```

## 2. מקורות

- https://en.wikipedia.org/wiki/Transmission_Control_Protocol
- https://searchnetworking.techtarget.com/definition/TCP#:~:text=TCP%20(Transmission%20Control%20Protocol)%20is,of%20data%20to%20each%20other.
- https://en.wikipedia.org/wiki/SYN_flood
- https://www.imperva.com/learn/ddos/syn-flood/
- https://security.radware.com/ddos-knowledge-center/ddospedia/syn-flood/



# חלק א'

## 3. שאלות הכנה

### 3.1. פרוטוקול TCP

א. מה תפקידו?

ב. באיזו שכבה במודל 7 השכבות עובד הפרוטוקול?

ג. איך מתבצעת בדיקת אמינות הנתונים? ומה קורה במידה של תקלה?

ד. מהו מבנה חבילת ה TCP ?

### 3.2. לחיצת היד המשולשת

א. הסבר\י על לחיצת היד המשולשת ושלושת השלבים שלה.

ב. איך מתבצע סגירת הקשר ?

ג. ISN-Initial Sequence Number

a. מהו ?

b. מאיפה מתחיל המספור ולמה?

### 3.3. הצפת SYN

א. הסבירו על ההתקפה:

a. מהי מנצלת?

b. איך היא פועלת?

c. מטרת התקיפה?

ב. מנו לפחות 3 דרכים להתמודדות עם ההתקפה.

### 3.4. פרוטוקול UDP

א. מה תפקידו?

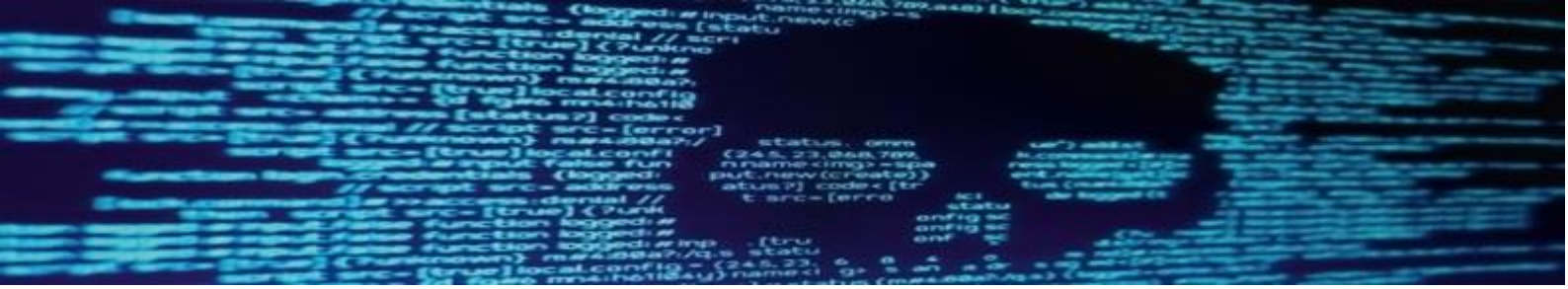
ב. באיזו שכבה במודל 7 השכבות עובד הפרוטוקול?

ג. מהי מבנה הודעת UDP?

### 3.5. Checksum

א. מהו Checksum?

ב. מה תפקידו?



# חלק ב'

## 4. מהלך הניסוי

### 4.1. שלב א' – הכנת התשתית לביצוע הניסוי

א. פתח מכונה וירטואלית: Kali – Attacker

ב. פתח מכונה וירטואלית: Kali – victim

### 4.2. שלב ב' – ייצור פקטת SYN

א. ניצור פקטת IP חדשה ונגדיר את המקור ככתובת IP רנדומלית. הסבירו למה ?

ב. נגדיר את היעד לכתובת ה-IP שאותה אנחנו רוצים לתקוף (במקרה שלנו כתובת ה - IP של הקורבן).

```
IP_Packet = IP ()
IP_Packet.src = randomIP()
IP_Packet.dst = dstIP
```

### 4.3. שלב ג' – ייצור פקטת TCP

**א.** את TCP FLAG נגדיר להיות "S".

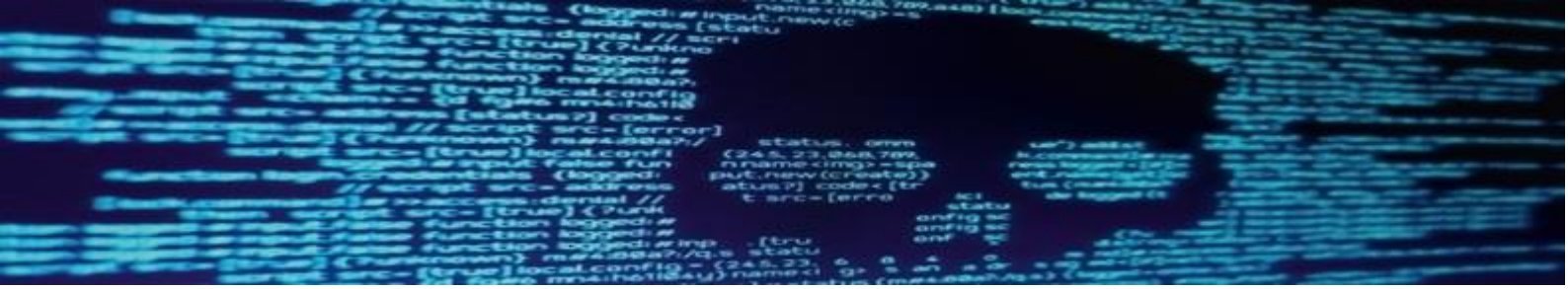
**ב.** את כתובת ה – IP של הקורבן נרשום ב – dport.

```
TCP_Packet = TCP ()
TCP_Packet.sport = randInt()
TCP_Packet.dport = dstPort
TCP_Packet.flags = "S"
TCP_Packet.seq = randInt()
TCP_Packet.window = randInt()
```

### 4.4. שלב ד' – שליחת הפקטה

שליחת הפקטה תעשה על ידי הפקודה הבאה:

```
Packet = IP_Packet/TCP_Packet
send(Packet, verbose=0)
```



### 4.5. שלב ה' – יצירת קוד פייתון וביצוע ההתקפה

**א.** מצורף קטע קוד פייתון (בשם syn_flood_attack.py) שמבצע את ההתקפה.

**ב.** עליכם להשלים את הפונקציה SYN_Flood ולאחר מכן להריץ את קטע הקוד מטרמינל התוקף ובכך להוציא לפעולה את ההתקפה.

### 4.6. שלב ו' – בדיקת ההתקפה

**א.** עליכם להסביר מה אתם מצפים לראות ?

**ב.** יש לצרף צילום מסך של התעבורה ב – WIRESHARKE , ולהסביר מה בפועל ראיתם לעומת מה שציפתם לראות ?

## 5. דו"ח מסכם

- הגישו את קטעי הקוד שכתבתם וצילומי מסך מכל שלב במעבדה.
- הסבירו באופן ברור את הפתרון בכל שלב במעבדה.