טכנו"צ סייבר - רמזים תרגיל 3

כי מצגת נראה לי יותר כיף ממסמך

בגדול אנחנו יוצרים כלי
שמאפשר להריץ כל קוד
על מחשב מרוחק

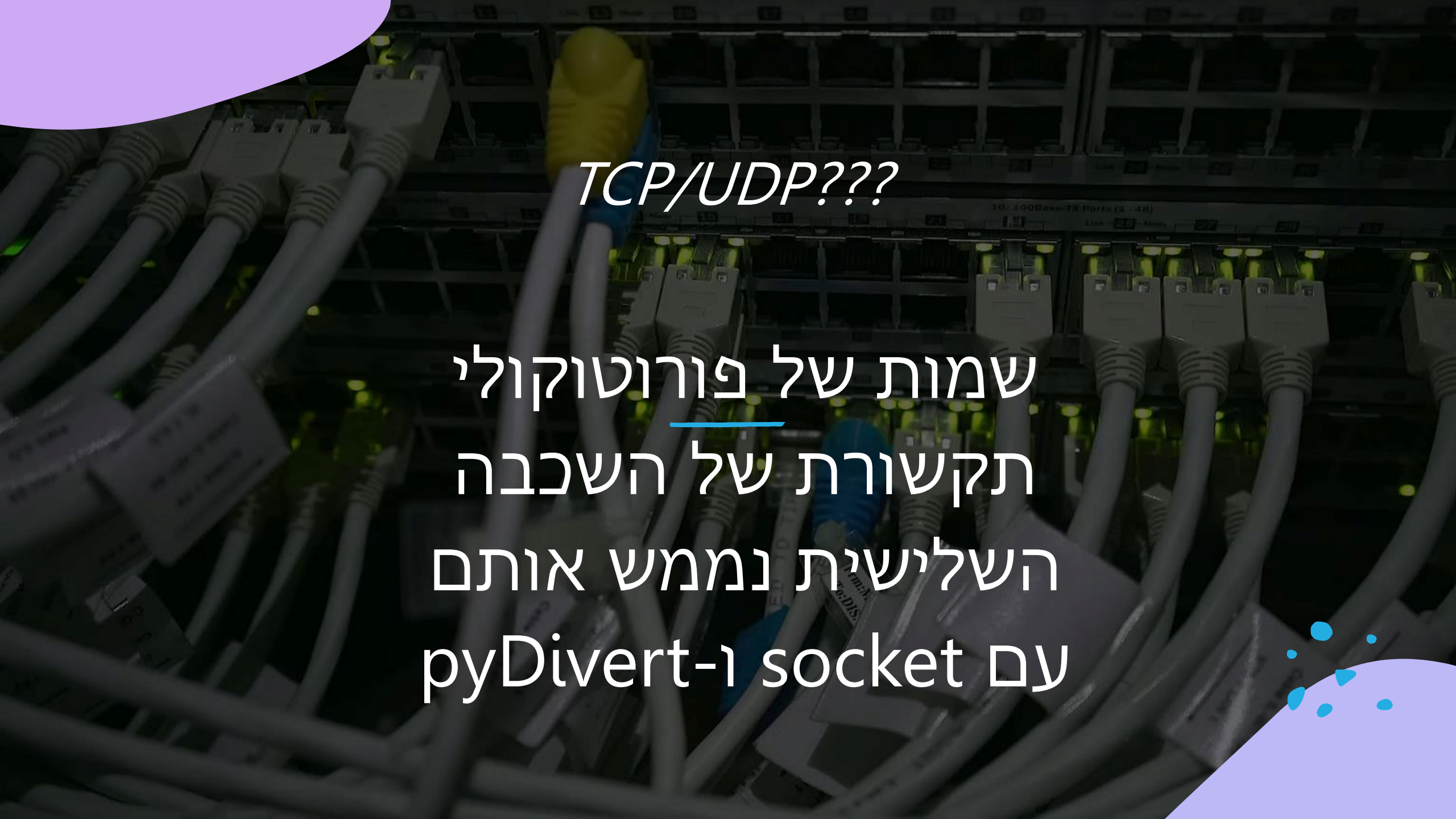
Port Knocking

פורטים הם אלמנטים שקשורים לשכבה הרביעית הם בעצם מאפשר למחשב לדעת לאיזו תוכנה לנתב את המידע שהוא קיבל מהאינטרנט. ז"א ככה המחשב יודע שהבתים שהוא קיבל עכשיו רלוונטים לכרום ולא ל-Chicken Invaders או Windows Store.

כדי לעשות port knocking אנחנו נשתמש בפרוטוקול UDP כדי לשלוח מידע לשלושה פורטים בזה אחרי זה

- 1234 -> 5678 -> 1278

כשהנוזקה תזהה את "הדפיקה המדויקת" שלוש פקטות בשלושת הפורטים היא תפתח פורט נוסף שבו היא תקשיב בפרוקטול TCP



TCP/UDP???

שמות של פורוטוקולי
תקשורת של השכבה
השלישית נממש אותם
עם socket ו-pyDivert

אמין אבל איטי – ???TCP

צד שרת

```
server_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
server_socket.bind(?)
server_socket.listen(?)
? = server_socket.accept()
```

צד לקוח

```
transmitter = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

כדי לשלוח מידע (אותו דבר בשרת)

```
transmitter.send(?)
```

כדי לקבל מידע (אותו דבר בשרת)

```
transmitter.recv(?)
```

לא אמין אבל מהיר – UDP???

צד לקוח

```
port_knock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
```

כדי לשלוח מידע

```
port_knock.sendto(?)
```

צד שרת

```
with pydivert.WinDivert(filter) as w:
    for packet in w:
        packet – פקטת המידע
```

Sockets/PyDivert??

סוקט זה כמו צינור להעברת מידע שמאפשר לקשר בין שני מחשבים (תהליכים על אותו מחשב במקרה שלנו) באמצעות כתובת IP ומספר PORT.

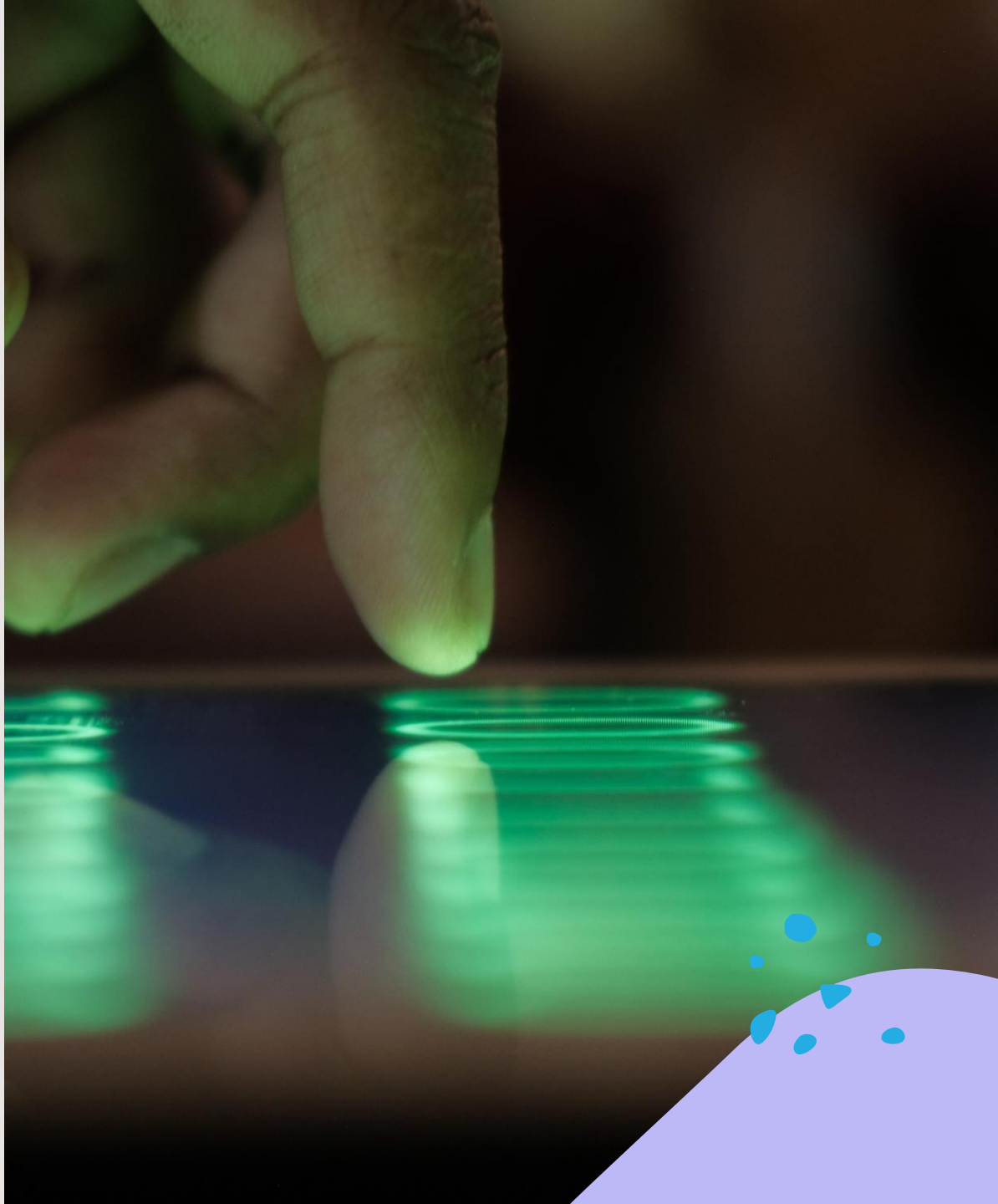
PyDivert זה מודול python של Windivert שמאפשר לאפליקציות בהרשאת מנהל לתפוס, לשנות ולהסיט פקטות (יעני להתלבש על הכבל רשת ברמה זו או אחרת ולעשות מה שבה לו עם הפקטות)

Exec?

מקבל טקסט ומאפשר להריץ את הטקסט כ-python. א מה מה, הוא לא מחזיר ערך החזרה, יעני אם עשיתם print הוא פשוט מדפיס. אז בגדול היינו רוצים שהוא יכווין מחדש את הפלט של print מהקונסול לאיזשהו קובץ. זה מה שאני חיפשתי בגוגל כדי למצוא איך עושים את זה

redirect exec to file python

אגב הבונוס המעשי לא קשה ופותר את הבעיה הזאת בצורה הרבה יותר טובה.



המלצות כלליות

בהתחשב בזה שגם השרת וגם הלקוח צריכים שלוח ולקבל הודעות ב-TCP אני ממליץ שיהיה קובץ אחד שאחראי לעשות את זה. קראתי לו protocol ויש בו פונקציית send שמקבלת socket ומידע שצריך לשלוח ופונקציית receive ששואבת את המידע מה-socket.

איך היא יודעת כמה בתים להוציא מ-socket?

דאגתי ב-send לכתוב לה דבר ראשון כמה בתים יש בהודעה – מוזמנים לחשוב על דרכים יותר מתוחכמות לבצע את השיחה בין השרת ללקוח.

בהצלחה, מוזמנים לשאול שאלות!