משימת תכנות הגנת פרוטוקולי רשת

סה״כ הנקודות בעבודה זו הינה 100 נקודות שמהווים 50 אחוז מהציון בקורס.

א. פתחו מערכת לניתוח תעבורה ב פיתון:

a. המערכת מקבלת תעבורה על interface שאתם בוחרים.
b. המערכת מחלקת את המידע ל flow לפי tuple-5. המערכת תחזיר תובנות על flow ויתר metadata של כמה מידע עבר מכל צד, איזה פרוטוקול והאם נמצאו התקפות
c. המערכת מנתחת את החבילות, מבצעת וולידציה ל
d. המערכת תעבוד כ intrusion detection system ותחפש התקפות של הזלגת מידע.
e. המערכת תנתח את המידע בצורה יעילה
f. פיתוח המערכת הינו רק בעזרת קוד מקורי שלכם. ניתן להשתמש בקוד של פרסור (parser) חבילות על מנת להוציא ולפרסר שכבות.
g. על מנת להגן – אתם צריכים לדעת להתקיף.
h. תיצרו את הפתרון ב docker ותשדרו חבילות בעזרת tcp replay.

ב. שלבים:

a. פיתוח מערכת לניתוח flow [10 נקודות]
b. פיתוח מערכת ui וסטטיסטיקה וויזואלית למידע שעובר וסכנות שאותרו [10 נקודות]
c. מחקר ו פיתוח התקפות להזלגת מידע מהארגון בתעבורת רשת ארגונית [25 נקודות]
יצירת דוח אשר מכיל את הארכיטקטורה, תכנון, גישות זיהוי ודיון על הגישות שנבחרו. (הכל באנגלית – overleaf).
d. פיתוח וולידציה ושיטות לגילוי הזלגת מידע מהארגון [30 נקודות]
כולל דוגמאות והתקפות שמצאתם, יצרתם כ unitest למערכת
e. פיתוח מערכת בסביבת דוקר [10 נקודות] הערה: במידה ונבטל את סעיף זה הנקודות יתחלקו בשווה בין סעיף (a) לסעיף (b).
f. איתור תרחיש הזלגת מידע של הבודקים [15] נקודות

ג. מה מגישים:

a. קוד (לא git) אשר מכיל את כל הקוד, unitest שנדרש לבנות את הפתרון ולבדוק אותו.
b. דוח מסכם אשר מכיל את סעיף (b).
c. הדגמת POC בבחינה פרונטלית על הקוד מול סעיף e.