**משימת תכנות הגנת פרוטוקולי רשת**

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

1. פתחו מערכת לניתוח תעבורה ב פיתון:

אנו מחפשים לטפל בזליגת מידע, הוא כבר נגנב מאדם בתוך הארגון, אנו רוצים לא לאפשר את זליגת המידע מהאדם למחוץ השרת

אנו לא יודעים איזה מידע הוא מידע שאסור לו לזלוג, שליחת המידע היא בהתאם לתקינות הפרוטוקול.

אנו רוצים לבדוק את הפרוטוקול ובמידה והוא עובר את המבחנים שלנו והוא תקין אז נאפשר שליחת המידע.

המערכת(לא שרת) מקבלת תעבורה ועליה לוודא שהפרוטוקול תקין מכל בחינה כך שכאשר פרוטוקול לא עובר את המבחנים שלנו מבחינתנו הוא עוין ולא נשלח את המידע.

* 1. המערכת מקבלת תעבורה על interface שאתם בוחרים.

לא מממשים שרת ולקוח רגילים, מממשים רק מערכת לניטור חבילות ושם עושים את הבדיקות

* 1. המערכת מחלקת את המידע ל flow לפי 5-tuple. המערכת תחזיר תובנות על flow ויתר metadata של כמה מידע עבר מכל צד, איזה פרוטוקול והאם נמצאו התקפות

<src\_ip,dst\_up,src\_port,dst\_port,protocol>, לא באמת אכפת לנו מהפרטים האלה של מי שלח, מאיפה הזרימה וכו, אנחנו בודקים נטו את המבנה של הפרוטוקול.

* 1. המערכת מנתחת את החבילות, מבצעת וולידציה ל
  2. המערכת תעבוד כ intrusion detection system ותחפש התקפות של הזלגת מידע.
  3. המערכת תנתח את המידע בצורה יעילה
  4. פיתוח המערכת הינו רק בעזרת קוד מקורי שלכם. ניתן להשתמש בקוד של פרסור (parser) חבילות על מנת להוציא ולפרסר שכבות.
  5. על מנת להגן – אתם צריכים לדעת להתקיף.
  6. תיצרו את הפתרון ב docker ותשדרו חבילות בעזרת tcp replay.

1. שלבים:
   1. פיתוח מערכת לניתוח flow [10 נקודות]
   2. פיתוח מערכת ui וסטטיסטיקה וויזואלית למידע שעובר וסכנות שאותרו [10 נקודות]
   3. 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).

* 1. פיתוח וולידציה ושיטות לגילוי הזלגת מידע מהארגון [30 נקודות]

כולל דוגמאות והתקפות שמצאתם, יצרתם כ unitest למערכת

* 1. פיתוח מערכת בסביבת דוקר [10 נקודות] הערה: במידה ונבטל את סעיף זה הנקודות יתחלקו בשווה בין סעיף (a) לסעיף (b).
  2. איתור תרחיש הזלגת מידע של הבודקים [15] נקודות

1. מה מגישים:
   1. קוד (לא git) אשר מכיל את כל הקוד, unitest שנדרש לבנות את הפתרון ולבדוק אותו.
   2. דוח מסכם אשר מכיל את סעיף (b).
   3. הדגמת POC בבחינה פרונטלית על הקוד מול סעיף e.

פורטי שרת הם קטנים מ1024

פורטים עם לקוח הם מספר רנדומלי בין 1024 ל16000~

בדיקה אופציונלית אחת

נפתח בmain קובץ .PCAP רנדומלי או מסוים ונעשה את הבדיקות עליו