**סטטוס התקדמות והכנה למחר:**

**משימות:**

1. TrafficGPT
   1. לאתר מייל של הכותבים
   2. לנסח מייל שמכיל: קראנו את המאמר, אנחנו עושות פרוייקט בתחום, אנחנו עובדות עם עמית וחן ונשמח לקבל קוד
2. Netshare
   1. לבדוק ציטוטים בscholar וב-GIT לראות אם הקוד סבבה
   2. אם לא – להרים דגל
   3. אם כן – להתחיל לרוץ על הקוד
3. Compare GPT-GAN with PentrestGPT
   1. לבדוק אם יש קוד ב- PentrestGPT
   2. אם כן לעשות בדיקה האם המאמר ברמה טובה/ הקוד עובד
   3. אם כן להתחיל לרוץ גם על זה

**עיקרי הדברים:**

1. **TrafficGPT** - מצאתי את מיילים (האמת לקח לי קצת זמן עם הסינים האלה), וניסחתי משהו - לשלוח פשוט? או שמישהו מכם מעדיף להעיף מבט לפני כן?
2. **Compare GPT-GAN with PentrestGPT**
   1. יש קוד – <https://github.com/greydgl/pentestgpt>
   2. ממה שראיתי הוא הוצג בכנס -   
      33rd USENIX Security Symposium (USENIX Security 24), 2024 שהתקיים בתאריכים 14-16/08/2024
   3. כך שאף אחד לא הספיק לצטט אותו עדיין.
3. **Netshare**
   1. היו כ-50 ציטוטים למאמר, לכן בחרנו מדגמית כמה ממאמרים החדשים יותר כדי להבין את איכות הפתרון.
   2. איכות הקוד: רב המאמרים מדברים על זה שקוד שמבוסס על GANs, כמו NetShare, משיג איכות טובה מבחינת משימות יצירת תעבורת רשת אבל יש לו כל מיני מגבלות של GANs כמו "קריסת מצב", אימון לא יציב ורגישות יתר להיפרפרמטרים. אחד המאמרים הציג את NetDiffus שהצליח להשיג "נאמנות" (באנגלית fidelity, שממה שהבנו הכוונה פה היא לתוצר שדומה יותר לתעבורה אותנטית) גבוהה ב-66.4% בנתונים שנוצרו בהשוואה ל NetShare. זה מצביע על זה ש- NetShare יחסית בסדר, אבל יש חלופות חזקות יותר בגישות חדשות יותר כמו NetDiffus.
   3. מגבלות משמעותיות:  
      ממה שהבנתי המגבלה המשמעותית של NetShare (ושל כל פתרון מבוסס GAN) היא קריסת מצב, שבה המודל נוטה ליצור פלטים פחות מגוונים. וגם דיברו על אימון לא יציב, במיוחד אם ההיפרפרמטרים לא מכוונים טוב (ממה שהבנתי יש מצב שהם התכוונו לסוג של over-fitting ל-data שהוא אומן עליו. וזה מתבטא בזה שאם נותנים לו מידע שהוא מכיר (מהאימון) הוא יעשה עבודה טובה אבל אם יתנו לו משהו חדש הוא לא יצליח).
   4. בשורה התחתונה NetShare הוא טוב יחסית לפתרון מבוססGAN (וזה נראה לי קצת עונה על מה שדיברנו על תעבורה "שיש בה שכל" שזה חלק ממה שהמודל לא מצליח כל כך לייצר).
   5. אבל זה כן הוביל אותנו ל- NetDiffus (השם בגלל שהוא מבוסס על מודלים של דיפוזיה – שאני עדיין לא יודעת מה זה בדיוק אומר) שכן אמור להביא תוצאה טוב יותר.
   6. יש קוד ל- NetDiffus - <https://github.com/Nirhoshan/NetDiffus>
   7. ייצרנו לנו מסמך מסודר עם ציטוטים מהמאמרים שגרמו לנו להבין את זה - תכלס זה 2 מאמרים שכן דיברנו על זה בהרחבה (לשאר שבדקתי לא הייתה יותר מידי "אמירה"). אנחנו יכולות לשלוח אם אתם רוצים/ נראה לכם רלוונטי.
   8. רוצות לסייג ולהגיד שהמסמך המרכזי ש"מלכלך" על NetShare הוא המאמר של NetDiffus (NetDiffus: Network Traffic Generation by Diffusion Models through Time-Series Imaging)

**התייעצות – הדבר המתבקש הוא ללכת עם NetDiffus, לוודא שגם שם אין איזה תקלה משמעותית ולהתחיל לרוץ על הקוד הזה. האם זה מקובל/ נשמע לכם כמו רעיון טוב?**