סיכום פרויקט במערכות הגנה לרשת

נושא הפרויקט: אנטי וירוס לשרת אימייל.

תיאור הפרויקט:

הפרויקט מבוסס על שרת אימייל SMTP מסוג Postfix שנכתב ופותח באמצעות שפת התכנות Python 3. בשרת קיימים שני צדדים, צד הלקוח וצד השרת כאשר צד הלקוח שולח מייל וצד השרת הוא הצד שמקבל את המייל.
ההתמקדות העיקרית בפרויקט הייתה למידה ופיתוח מעין "אנטי וירוס" אשר מתממשק עם השרת מייל וחוסם הודעות מייל שאליהן הוטמע קובץ זדוני.
על מנת לזהות קבצים זדוניים השתמשתי במאגר וירוסים "דמיוני" שכתוב בבסיס הקסדצימלי ובו כתובים מספר וירוסים שלכל וירוס יש שם, גודל, והחתימה עצמה שמזוהה עם הווירוס. בעת קבלת מייל, מתבצעת סריקה של הקובץ שהתקבל, ובמידה ומזוהה בו וירוס ההודעה נחסמת ולא מתקבלת ונשלחת הודעת שגיאה לשולח ההודעה. במידה והמייל תקין ההודעה נשלחת בהצלחה ומוצגת למשתמש.
בנוסף, כתוספת לתוכנה פיתחתי שני פיצ'רים נוספים:
1. התוכנה תחסום מיילים שבהם שם הקובץ יהיה מזוהה עם אחד מהשמות ממאגר שמות לא תקין שמוחזק בתוכנה. לדוגמא, מיילים עם קבצים ששמם יהיה "Virus" או "Spam" ייחסמו כחשד לקבצים זדוניים.
2. התוכנה תסרוק קובץ שהתקבל ותבדוק האם קיים חשד ל "File Spoofing", כלומר האם הקובץ שהתקבל, שמוצג כקובץ "Png." לדוגמא הינו בכלל קובץ הרצה "Exe." , דבר אשר ניתן לזהות על ידי סריקת החתימה של הקובץ וזיהוי לפי ה- Magic Number שלו. המייל עצמו יתקבל בהצלחה אך תוצג הודעת אזהרה למשתמש שהקובץ שהתקבל חשוד כזדוני ולכן מומלץ לא להפעילו.

מדריך להרצת הפרויקט:

המדריך הנ"ל מיועד להרצת הפרויקט במערכת הפעלה מבוססת Linux ותקינות ההוראות נבדק על Ubuntu.

ראשית, נצטרך לוודא ששפת התכנות Python 3 מותקנת אצלנו במערכת, לכן נבצע את הפקודה הבאה:

```
sudo apt-get install python3
```

כעת נתקין את התוספים שהתוכנה משתמשת בהם:

```
sudo apt-get -y install python3-pip

pip3 install puremagic
```

עכשיו אנו יכולים להריץ את הפרויקט עצמו. לצורך כך נצטרך לפתוח 2 לשוניות ב- Shell.

על הראשונה נריץ את השרת על ידי הפקודה הבאה:

```
python3 Server.py
```

על השנייה נריץ את הלקוח על ידי אחת מהפקודות הבאות: [תלוי בסוג לקוח שנרצה להריץ]

```
python3 Malicious_Client.py

# or

python3 Suspicious_Client.py

# or

python3 Normal_Client.py
```

זהו סיימנו! כעת ניתן להריץ את הפרויקט. יש לשים לב שהשרת רץ תמיד לכן כדי לסגור אותנו נשתמש ב- CTRL-C .

*את פקודות ההרצה עצמן ניתן לשלוף מקובץ טקסט שמצורף לפרויקט עם הערות וניתן לבצע "העתק-הדבק" ישירות ל- Shell לצורך נוחות הבודק.

<u>קשיים בביצוע הפרויקט:</u>

במהלך הפרויקט נתקלתי במספר קשיים אשר האריכו את זמן ביצוע הפרויקט מעבר לזמנים אשר הצבתי לעצמי וגרמו לשינוי יישום הפרויקט בהשוואה למסמך האפיון שהוגש בתחילת הסמסטר.

הקושי העיקרי שנתקלתי בו היה בחירת אופן פיתוח שרת המייל. חוסר ידע וניסיון מקדים הוביל לתקלות רבות במהלך הקמת השרת הראשוני באמצעות הענן של Amazon לדוגמא, ורק לאחר ניסיונות שונים הוחלט על פיתוח השרת ב Python. קושי נוסף היה הלמידה והמחקר SMTP ועל שפת Python שבה לא היה לי רקע מקדים אך לאחר זמן מה של למידה הצלחתי לפצות על החורים שהיו ועל הדרך הקנתי לעצמי כלים חדשים בפיתוח תוכנה.

לסיכום, למרות הקשיים והזמן שהפרויקט צרך ממני, נהנתי מאוד ללמוד נושאים חדשים במסגרת הפרויקט ולראות את התוצר שהצלחתי להביא.