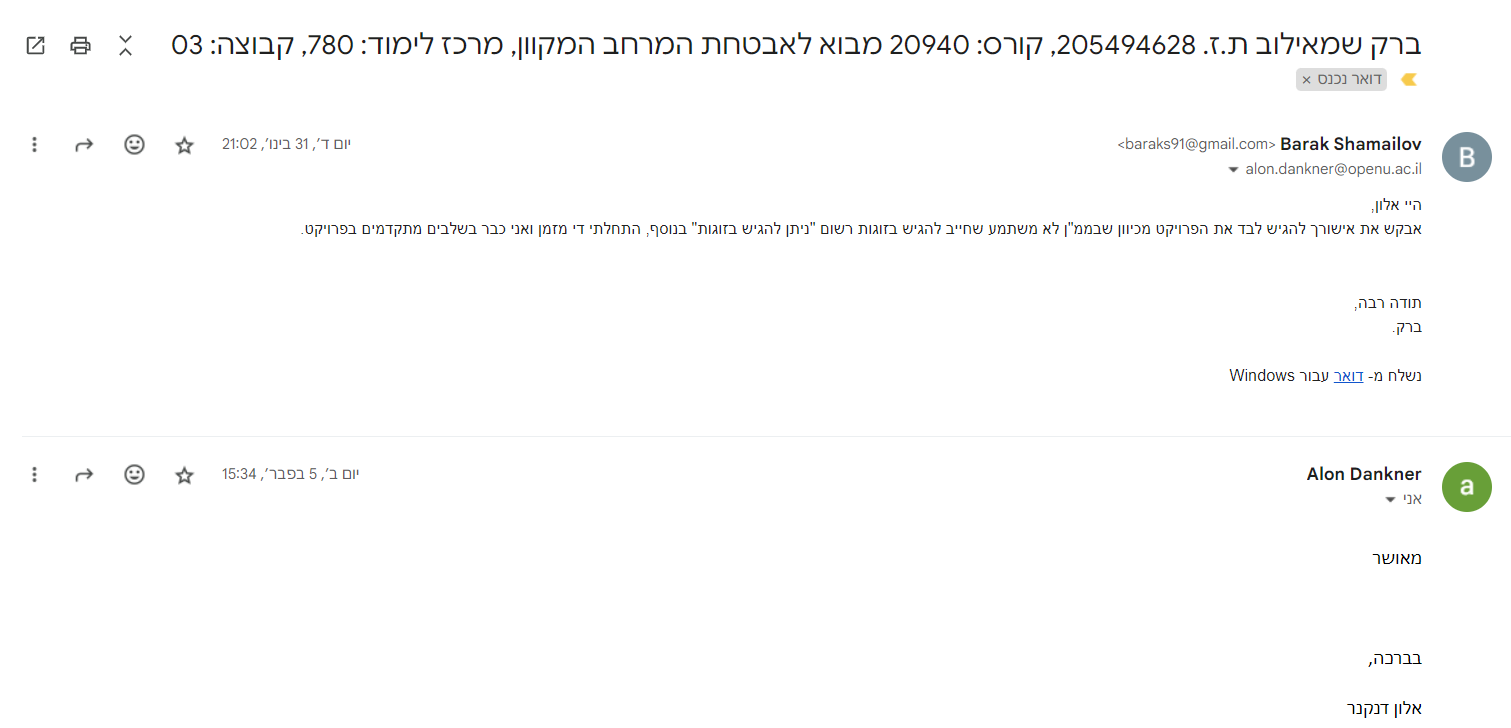
הגשת ממ"ן 16:

הערות:

* שם: ברק שמאילוב, ת"ז: 205494628, אני מגיש לבד את הפרויקט – אישור במייל (תצלום של האישור במייל)
* בחרתי לממש את הבונוס, באופן חופשי כפי שהוסבר בהרצאה ובפורום הקורס.
* הפרויקט נכתב בPython בסביבת Pycharm.
* התיקייה Crypto זו בעצם חבילת הצפנה PyCryptodome, העלתי אותה למקרה ובדיקת הפרויקט לא תהיה בסביבת Pycharm שתוכל לרוץ גם בסביבה אחרת.

סרטון הסבר:

את סרטון ההסבר העליתי גם לדרייב וגם ליוטיוב, במידה ותהיה תקלה בהרשאת צפייה לדרייב אז שתהיה אפשרות גם ביוטיוב לצפות:

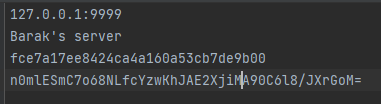
1. דרייב - <https://drive.google.com/file/d/1OKObTw1FNe8Gtu8vzn3-1k89nh1QEBLR/view?usp=drive_link>

הקישור שותף עם כתובת המייל - [alon.dankner@openu.ac.il](mailto:alon.dankner@openu.ac.il).

1. יוטיוב – <https://youtu.be/b9j_BUFr0g4>.

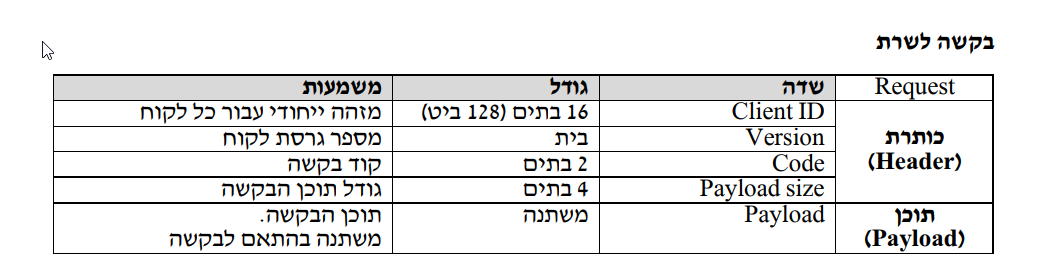
הסבר מימוש בונוס:

1. שרת ההודעות קורא את פרטי ההתחברות לשרת האימות דרך הקובץ "auth.info.txt" בשורה הראשונה של הקובץ נמצאים הIP וה-PORT של השרת האימות בצורה הבאה – 127.0.0.1:8080.
2. שרת ההודעות קורא את פרטי הIP ,הפורט שלו, את שמו, את המזהה הייחודי שלו ואת המפתח הסימטרי שלו מהקובץ msg.info.txt בצורה הבאה:



* אם הקובץ לא קיים, נזין את שם השרת שאנו רוצים דרך הקונסול ויוזנו לנתיב והIP ערכים דיפולטיביים ולאחר מכן יתבצע תהליך רישום אצל שרת האימות.
* אם הקובץ קיים לא יתבצע תהליך הרישום (מכיוון שהוא כבר רשום).

1. הלקוח קורא את פרטי ההתחברות לשרת האימות דרך הקובץ "auth.info.txt" בשורה הראשונה של הקובץ נמצאים הIP וה-PORT של השרת האימות בצורה הבאה – 127.0.0.1:8080.
2. בקשת רישום של שרת ההודעות לשרת האימות כוללת את הHeader כפי שהוגדר בממ"ן: (קוד הבקשה 1025)



1. לאחר מכן התוכן של התשובה (Payload) יכלול את הפרטים הבאים:

תוספת שלי

|  |  |  |
| --- | --- | --- |
| שדה | גודל | משמעות |
| Name | 255 בתים | מחרוזת ASCII המייצגת שם משתמש. כולל תו מסיים! ) null terminated) |
| מפתח סימטרי | 32 בתים | מפתח AES סימטרי לשרת ההדפסה (מיועד לפענוח Ticket- ים) |
| Server IP | 16 בתים | כתובת ה-IP של השרת. |
| Server Port | 2 בתים | הפורט של השרת |

* הערה: בממ"ן רשום שכתובת הIP היא 4 בתים בחרתי ב16 בתים, מכיוון שאני מייצג את הIP כמחרוזת, רציתי לוודא שאני מכסה גם כתובת IP בגודל הבא: "XXX.XXX.XXX.XXX"

1. בקשת רשימת שרתי ההודעות כוללת את הHeader במטלה שמצויין למעלהת קוד הבקשה 1026 כאשר הPayload שווה ל-0.
2. שרת האימות שומר את פרטי שרתי ההודעות בקובץ שנקרא "servers" בצורה הבאה:

IP – מייצג את הIP של שרת ההודעות.

Port – מייצג את הפורט של שרת ההודעות.

ID – מייצג את ה-ID של שרת ההודעות.

Name – מייצג את השם של שרת ההודעות.

AESKey – מייצג את המפתח הסימטרי ארוך הטווח של שרת ההודעות.

IP:Port:ID:Name:AESKey

1. כעת נתאר את התשובות לבקשות מצד שרת האימות, התשובות כוללות את הHeader כפי שמופיע בממ"ן:

תמונה שמכילה טקסט, צילום מסך, גופן, מספר

התיאור נוצר באופן אוטומטי

1. תשובה לבקשת רישום שרת ההודעות, קוד תשובה 1600 ,המשמעות רישום הצליח, התוכן של התשובה (Payload) כפי שמופיע בממ"ן:

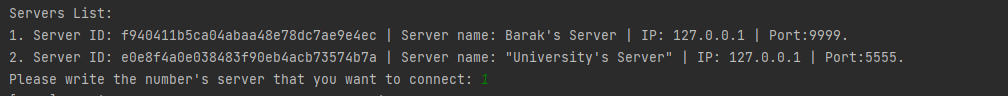
|  |  |  |
| --- | --- | --- |
| שדה | גודל | משמעות |
| Server ID/Client ID | 16 בתים | מזהה ייחודי של שרת/לקוח |

* התשובה תוחזר בהתאם למי ששלח אותה וכך גם התוכן יותאם בהתאם, לקוח או שרת.
* תוחזר גם תשובה במקרה שהרישום נכשל הקוד שלה הוא 1601.

1. תשובה לבקשת רשימת שרתי ההודעות, קוד התשובה הוא 1602 המשמעות רשימת שרתי ההודעות. התוכן של התשובה (Payload) :

|  |  |  |
| --- | --- | --- |
| שדה | גודל | משמעות |
| Server ID | 16 בתים | מזהה ייחודי של שרת |
| Server Name | 255 בתים | מחרוזת ASCII המייצגת שם משתמש. כולל תו מסיים! ) null terminated) |
| Server IP | 16 בתים | כתובת ה-IP של השרת. |
| Server Port | 2 בתים | הפורט של השרת |

1. כאשר הלקוח יקבל את התשובה משרת האימות לבקשה של שרתי ההודעות, הוא יפענח הדאטה של התשובה ולאחר מכן ידפיס למשתמש את הרשימה של השרתים בצורה הבאה ויבקש ממנו לבחור את השרת שאליו הוא רוצה להתחבר:



כפי שניתן לראות במקרה של התמונה ישנם שני שרתים ברשימה שכל אחד מהם קיבל מספר (1 ו-2) והמשתמש הזין את המספר של השרת שהוא רוצה להתחבר אליו שהוא 1. כמו כן מפורט למשתמש המידע על השרת, לאחר שהמשתמש בחר את השרת, הפרטים יעודכנו בתוכנית הלקוח לצורך התחברות לשרת ההודעות שהמשתמש בחר.