***פרוטוקול תקשורת בין שרת ולקוח:***

**דגשים**

* כל שיחה בין שרת ולקוח היא session מוצפן בפני עצמו.
* תמיד השרת הוא זה שיזום פתיחת session.
* כל session מתחיל עם החלפת מפתחות ציבוריים לצורך הצפנה.

**לחיצת ידיים להחלפת מפתחות ציבוריים ל-RSA**

מאחר והשרת יוזם את השיחה הוא ראשית ישלח את המפתח שלו, ולאחר מכן הלקוח ישלח את המפתח שלו. מדובר בלחיצת ידיים בסיסית רק לצורך החלפת מפתחות מאחר והתקשורת עוברת מעל TCP ואין כל צורך במנגנון וולידציה נוסף. לחיצת הידיים אינה מוצפנת מאחר ולא עובר מידע רגיש, הצפנת RSA היא הצפנה א-סימטרית ועם המפתח שעובר ניתן רק להצפין את המידע.

**P-KEY:<public key> (int bytes array)**

**Conversation:**

**EXEC:<command> (string)**

מטעמי אתיקה ושמירה על פרטיות, הפרויקט שלי יהווה POC ותינתן אפשרות ל-CMD בהרשאות גבוהות בלבד (אסרו עליי להריץ סקריפטים אוטומטים לאיסוף מידע וכו'). למרות זאת, עדיין בחרתי להשאיר את כותרת הפרוטוקול במידה ובהמשך אבחר להוסיף דברים נוספים, ולא סתם לשלוח את הפקודה שתבוצע בשורת הפקודה.