אבטחת תקשורת 2 – הסבר קוד והדגמה

הבעיה שבאנו לפתור:

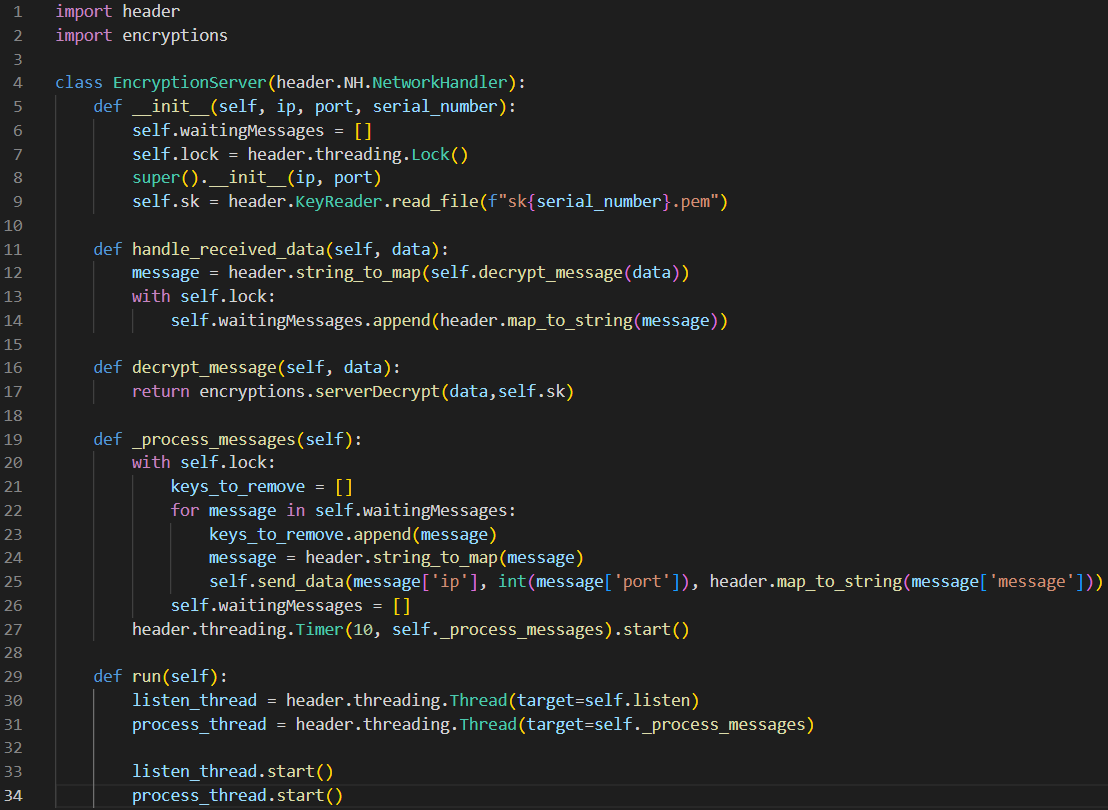
כאשר אנו גולשים ברשת המידע שאנו שולחים ומקבלים הוא מוצפן ולכן מי שמאזין לנו לא יכול לדעת מה המידע, אבל הוא כן יוכל לראות לאן אנחנו גולשים או עם מי אנו מתכתבים.

כדי לפתור את הבעיה ולתת אנונימיות מה שנעשה זה נעביר את הפקטות דרך שרתי mix שהתפקיד שלהם הוא שכאשר יוזרים פונים אליו הוא יעביר את ההודעות שלהם דרכו ובכך מי שמאזין לא יוכל לקשר בין היוזרים למידע שהם גולשים אליו (בדומה לשרת VPN):

הבעיה שנתקלנו בא היא שאם תוקף מצליח להשיג שליטה על שרת הmix האנונימיות נשברת. ולכן נשתמש בכמה שרתי mix שונים כך שעל מנת לשבור את האנונימיות התוקף יצטרך להשיג שליטה על כולם. כמובן שכל התקשורת מוצפנת ולכן תוקף מאזין לא יוכל לדלוף מידע וגם השרתים לא יוכלו לדלוף מידע מעבר למקום בוא הפקה הגיע אליו ולאן הוא ישלח אותה.

**הסבר הקוד:**

צד השרת:

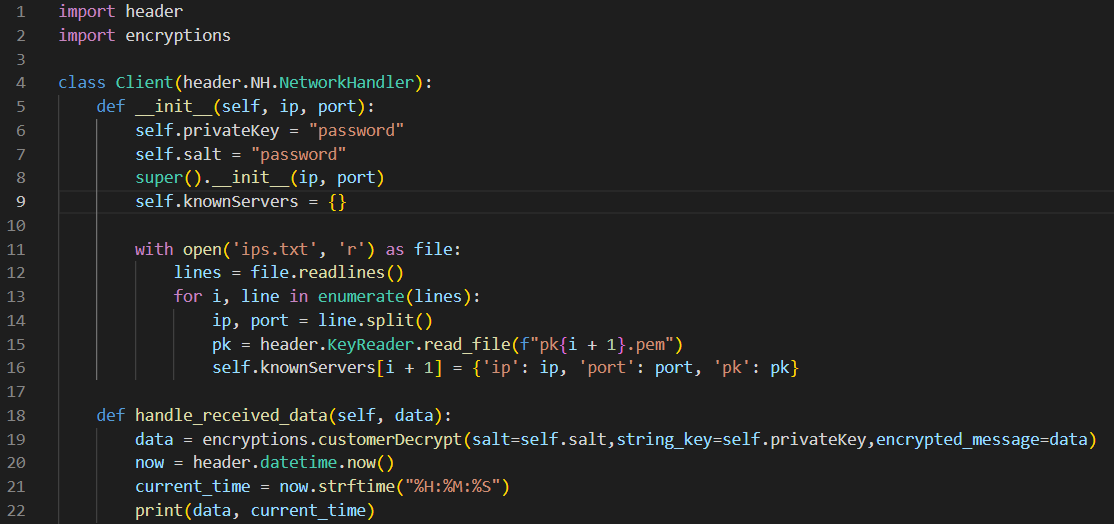


לכל שרת יש PORT כתובת IP ומספר סידורי שתפקידו להתאים את המפתח הפרטי שלו.

כאשר השרת רץ הוא עושה 2 פעולות (בפונקציה run()), מאזין לתעבורת רשת (מחכה להודעות חדשות) ובנוסף באמצעות הפונקציה \_process\_message כל 10 שניות רץ על כל ההודעות שמחכות ומעביר אותן הלאה – מה שמדמה round.

מבנה הודעה – כל server מקבל בהודעה map, אשר מכיל port, ip, message ובעצם הוא מעביר את ההודעה לכתובת הבאה, המידע של הmessage מוצפן ולכן השרת אינו יכול להשיג מידע נוסף ולשבור את האנונימיות

צד לקוח:



A computer screen shot of text

Description automatically generated

לכל לקוח יש IP וPORT בהם הוא מאזין, בנוסף יש מפתח פרטי לכל לקוח אשר מאותחל להיות מורכב כ "password", "salt" וכל לקוח יכול לשנות אותו – בנוסף באתחול, כל לקוח קורא את המפתחות הציבוריים של השרתים.

צד הלקוח מורכב משליחת הודעות וקבלת הודעות, בקבלת ההודעות כל לקוח מאזין לכתובת שלו ולפורט שלו – וכל הודעה שנשלחת הוא מדפיס ואת השעה בא התקבלה ההודעה. בצד השלוח כל לקוח מקבל קובץ הודעות מפרק את הקובץ ובעצם בונה הודעה בתוך הודעה כך שכל server במסלול יקרא אך ורק את החלק הרלוונטי אליו (המידע מוצפן ולכן המידע היחיד שהסרבר מקבל זה טקסט מוצפן ולאן להעביר אותו) ובכך בעצם הלקוח שולח הודעה שאותה כל שרת מפרק עד שמגיע ללקוח בצד השני עם ההצפנה הסימטרית. בנוסף כל הודעה נשלחת בround שנקבע לה וזמן כל round הוא 10 שניות.

**דוגמת הרצה:**

בדוגמה נשתמש בלקוח שולח ,לקוח מקבל, 2 שרתי ביניים וMITM בין הלקוחות לרשת – כלומר נשתמש באותו MITM כדי לראות את כל התעבורה שיוצאת ונכנס לכל אחד מהלקוחות:

Client – receive message

Client – send message

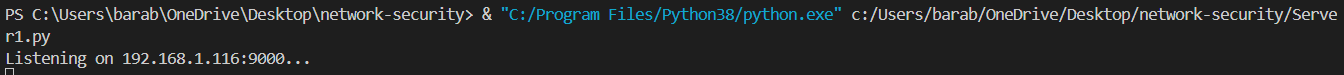
Router -MITM

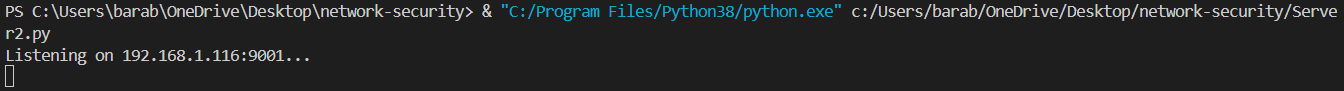
2 הלקוחות והראוטר יושבים על מכונה וירטואלית, ושרתי הmix יושבים לוקלית על המחשב

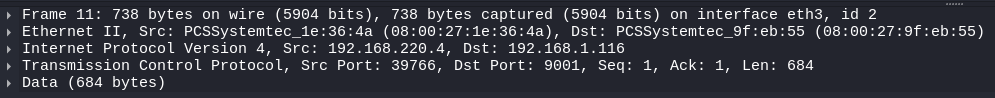
ארכיטקטורה:

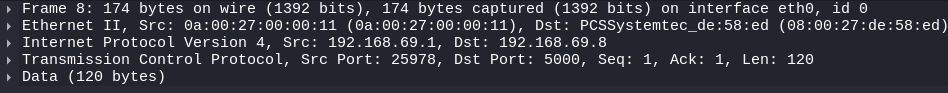
בדוגמת ההרצה נשלח הודעה מהclient הראשון לclient השני תוך כדי האזנה עם wireshark לתעבורה היוצאת והנכנסת ונראה כי אין לנו שום ידע שמעיד על שליחת הודעות בין השניים והמידע היחיד שכן נקבל בעצם זה ששני הצדדים מתקשרים עם השרתים.

ראשית נריץ את 2 השרתים:





לאחר מכן נריץ דרך המכונות client אחד אשר מאזין, ואחד אשר שולח הודעה, נראה בwireshark את הפקטות.  
ההודעה הראשונה שקולט הwireshark היא:  
מצד הלקוח השולח. ולאחר מכן לאחר זמן מסוים הwireshark קולט את ההודעה הנכנסת למחשב השני:



(גודל החבילות משתנה בגלל ההצפנה של הRSA), ובנוסף נבחין כי כל מה שהMITM יכול לראות זה ש2 היוזרים מתקשרים עם שרתי הביניים אך לא ניתן לראות שהם מתקשרים אחד עם השני.