שם: עומר אלכסנדר , ת"ז: 313703415

**ממ"ן 15**

שאלה 1

מספר דברים לא ברורים ושלא ענו עליהם בפורום, שהנחתי ככה:

1. בלי קובץ transfer.info אצל הלקוח לא ניתן להתחיל את התהליך של הלקוח.
2. אם קיים כבר קובץ me.info אז הלקוח לא יכול להירשם. [בגלל שקיום הקובץ מעיד שכבר נרשם]
3. תגובת לקוח עם 3 נסיונות קורת רק בבקשת שליחת קובץ [בדומה לדיאגרמה במטלה].

שאלה 2

יש מספר חולשות עיקריות שנובעות מההנחיות והפרוטוקול של העבודה [ללא קשר למימוש]:

1. Man in the middle [MITM] – זוהי אולי הפרצה החמורה ביותר בפרוטוקול אשר מאפשר לגורמים זדוניים לשבת על התקשורת בין הלקוח לשרת האמיתי ולחבל בה. דבר זה אפשרי בצורה פשוטה יחסית משום שאין בפרוטוקל שום שלב שמכיל מנגנון ווידוא על כך שהשרת הינו מחשב לגיטמי [מנגנון וידוא certificate כמו בTSL/SSL] ולא איזשהו שרת זדוני. דוגמאות למצבים וחולשות שיכולים לנבוע מכך:
   1. התחזות ללקוח קיים – שרת זדוני יכול בזמן בקשת שליחת מפתח ציבורי, לייצר מפתח פרטי וציבורי משלו במקום המקוריים ובכך לקבל חזרה מפתח סימטרי AES מותאם לו. לאחר שיש לו מפתח סימטרי ואת הID שלקח הוא בעצם יכול להמשיך לבצע תקשורת מול השרת בצורה נוחה כשהוא מתחזה למשתמש אחר [כמו לשלוח קבצים...].
   2. התחזות לשרת – בדומה לדוגמה הקודמת בשליחת מפתח ציבורי של הלקוח השרת הזדוני יכול להחזיר מפתח סימטרי AES שמוצפן על ידו ובכך בהמשך כשהלקוח ישלח קבצים לשרת הרגיל אז הוא יוכל לפענח אותם בעזרת המפתח שיצר עבורו.

תיקון אפשרי – על מנת למנוע התקפה מסוג כזה, ניתן להחליף את פרוטוקול החלפת המפתחות שקיים בממן לפרוטוקול החלפת מפתחות אמין יותר. כמו למשל SSL, אשר בפרוטוקול זה השרת צריך להזדהות בפני הלקוח עם הSSL certificate שלו. הcertificate הזה יתן אינדיקציה לכך שהשרת אמין ושניתן להתחבר אליו ולתקשר איתו בצורה מאובטחת. לאחר שתהליך ההזדהות והאימות יבוצע, השרת והלקוח יחליפו מפתחות הצפנה כמו שמתואר.

1. DOS – התקפת מניעת שירות עלולה להיווצר בפרוטוקול שלנו ע"י יצירת עומס חריג של השרת ובכך בעצם למנוע מלקוחות להשתמש בשירותי השרת כפי שמוצג בפרוטוקול. דבר זה אפשרי בגלל שאין שום מנגנון כמו WAF בפרוטוקול, אז ניתן לייצר עומס פניות לשרת ובכרך לגרום לו לקרוס.

תיקון אפשרי - הדרך למנוע זאת היא להשתמש במנגנון WAF או סוג של firewall אשר יחסמו מצב כזה בתקשורת של השרת.

1. עריכת קבצי טקסט שמשפיעים על התוכנית [ כמו port.info] - בגלל שהתהליכים של הפרוטוקול תלויים בקבצי טקסט שנמצאים בשני הצדדים ניתן לשנות אותם ובכך לגרום לתוכנית לבצע דברים לא רצוים למשל:
   1. למשל: ע"פ הפרוטוקול לקוח זדוני יכול לשלוח קובץ טקסט בשם port.info ולהכניס שם פורט אחר, ובכך בהפעלה הבאה של השרת בעצם הוא יפעל בפורט אחר שמשתמש זדוני הכניס לקובץ הזה.

יש מספר חולשות נוספות שנובעות מההנחיות והפרוטוקול של העבודה שהן תלויות מימוש:

1. הזרקת SQL – קבלת מידע שלא צריך להיות חשוף למשתמש לדוגמה:

query = "SELECT \* FROM Clients WHERE id = 1234 OR 1=1";, ניתן לעשות זאת למשל ע"י שליחת id = "1234… OR 1=1".

תיקון אפשרי - ניתן למנוע זאת ע"י הגבלת כל הפרמטרים שהשרת מריץ עליהם execute להיות מוגבלים לערכים ולידיים בלבד ע"פ מה שהשרת מצפה לקבל, ובכך למנוע פקודות בלתי רצויות בשרת.

1. Path traversal – גישה למקומות בזיכרון שאין כוונה שתהיה גישה אליהם. במידה והשרת שומר את הקובץ שקיבל ע"פ השם של הקובץ ומתייחס אליו כאל path אז בעצם ניתן לגשת למקומות בזיכרון של השרת, ולדרוס /למחוק וליצור קבצים.

תיקון אפשרי – ניתן למנוע זאת ע"י התייחסות לשם הקובץ רק כאל שם ובעצם השרת קובע איפה הוא רוצה לשמור את הקובץ אצלו בזיכרון ולא מקבל כקלט מהמשתמש משהו שהוא עלול להשתמש בו כpath.