ים צרניחובסקי, 327484085

הסבר המתקפה:   
במתקפה זו התוקף מצליח להשיג את ההודעות של הלקוח, ההודעות שמעניינות אותנו הן הודעה שהשרת אימות שלח ובה ticket וההודעה שהלקוח שלח לשרת הודעות על מנת ליצור קשר ראשוני.   
בקוד שמם msg1 , msg2. חלק ההודעה הראשונה הוצפנה ע״י hash של הסיסמה של הלקוח שם אפשר למצוא את המפתח המשותף שהונפק ע״י שרת האימות עבור התקשורת בין המשתמש לשרת ההודעות. התוקף עובר על רשימת סיסמאות השמורה בקובץ password\_notbook.txt לכל סיסמה עושה hash ובודק האם הפיענוח של ההודעה נותנת מפתח AES אשר מפענח את השיחה.   
כדי לבדוק זאת בודקים שהמידע הלא מוצפן או הידוע מראש (version, uuid). כאשר מוצאים את המפתח המשותף מתחזים ללקוחת ומתקשרים עם השרת הודעות.