**SMS Sniffing מסמך ייזום-**

**פרטי המגישים (קבוצה 21) :**

1. **שם : יאיר רביב , ת"ז : 316283043.**
2. **שם : ליאל ברניקר , ת"ז : 315708370.**
3. **שם : רבקה סטריליץ , ת"ז : 207911512.**

**הצגת הטכנולוגיה :**   
GSM - (global system for mobile communication)  
 זוהי טכנולוגיה המשמשת להעברת קול ומידע באופן דיגיטלי. פועלת בערוצים :   
 850MHz, 900MHz, 1800MHz, 1900MHz.

GSM עובדת בשיטת TDMA כלומר חלוקת משאבי התקשורת למשתמשים ע"פ זמן.

**למה בחרנו GSM:**

- בחרנו ללמוד וליישם התקפה על טכנולוגיה זו מכיוון שהיא רלוונטית לימינו ונוכל לעשות בה שימוש ממשי , בנוסף נתקלנו בחומר רב שהועבר בשיעורים בנושא תקשורת סלולר ומצאנו שנושא זה מעניין אותנו מאוד ומסקרן אותנו להתנסות בו.

**פגיעות/חולשה מרכזית + ההתקפה הרלוונטית:**

* נדגיש כי ההתקפה מכוונת למכשירים המשתמשים בדור 2 (2G) החולשה המרכזית שאנו מכוונים אליה היא האופן שבו מכשיר סלולרי מתחבר לBase station , קודם כל , מכשיר סלולרי מחפש את הMobile tower (BS) בעל האות החזק ביותר , בנוסף , כאשר מכשיר סלולרי מתחבר לBS , ההזדהות מתבצעת באופן "חד כיווני" בדור 2 (2G), כלומר – המכשיר הסלולרי מזדהה באמצעות הIMSI שלו , ולעומת זאת הBS אינו צריך לזהות את עצמו בפני המכשיר הסלולרי , ולכן – זיוף של BS יגרום למכשירי סלולר קרובים להתחבר לBS המזויף שלנו ויאפשר לנו לנטר את התקשורת שעוברת מ/אל הקורבן לבין האנטנה של האמיתית של הספק תקשורת.

.בעצם זוהי מתקפת MITM קלאסית על תקשורת GSM.

**תכולת העבודה:**

* העבודה שלנו תורכב מ:

1.מסמך שנכין שיפרט בצורה תיאורטית על סוג הטכנולוגיה , על החולשה הספציפית שננצל , ועל אופן מימוש המתקפה.

2.תוכנת פייתון שבאמצעות חומרה מתאימה תתחזה לBS , ותשיג מידע של הקורבנות שיתחברו לBS (בפרט תקשורת של sms).

**מדידת הצלחה:**

הצלחת העבודה תימדד ע"י:

* הבנה מעמיקה של הטכנולוגיה , חולשותיה , והאופן שבו ממומשת התקפה מתאימה שמנצלת חולשות אלו.
* הבנת השימוש בכלי תקיפה מתאים שמורכב מתוכנה וחומרה מתאימה.
* השגת המידע הנדרש ע"י שימוש בכלי התקיפה.

**רקע רעיוני למימוש המתקפה:**

* הבסיס למימוש ההתקפה הוא שימוש בחומרה מתאימה (SDR-RTL) ש"תייצג" את הBS , ותנהל את התקשורת אל מול הרכיב המתאים במכשירי הקורבנות (MS) ואל מול הBS האמיתי.
* כל זאת באמצעות שימוש בממשק המתאים UM המשתמש בפרוטוקול LAPDm.

השלב הבא בהתקפה יתבצע ע"י התוכנה , התוכנה תאזין לתקשורת העוברת אל/מ האנטנה שלנו , ותפלטר מהתקשורת המועברת פאקטות בעלות שכבת "GSM\_SMS" , ומפאקטות אלו נחלץ את תוכן ההודעות  
  
**הגנה:**כדי להגן על המכשיר נרצה לייצר את שכבת ההגנה שתדרוש הזדהות דו כיוונית ( בדומה ל3G,4G)

ביצוע הגנה זאת ימומש על ידי שמירת כל ה cell towersהמוכרים בקרבת המכשיר, באיזשהו מסד נתונים.  
ובזמן החיבור של הMS אל BS נתון נבדוק ,תחילה אם פרטי ה BS מוכרים לנו כלומר האם מופיעים במסד הנתונים. אם אכן הפרטים יופעו נדע כי הBS הינו בטוח וניתן לחיבור, אחרת נגדיר שהמכשיר יתחבר לBS עם התדר החזק ביותר שאכן מופיע במסד הנתונים   
  
**פירוט המשאבים חומרה/תוכנה:**חומרה:  
rtl-sdr device - USB dongle שסורק תקשורת סלולר בקרבת המכשיר  
תוכנה:  
מערכת הפעלה linux (תפוצת Debian)  
  
**מקור מידע:**מאמר בנושא : **GSM, התקפות והגנות**  
https://www.paladion.net/blogs/how-to-build-an-imsi-catcher-to-intercept-gsm-traffic