**מסמך אפיון לפרו ייקט במגשימים: סוס טרויאני לאנדרואיד**

**צד לקוח**

תיאור כללי

המערכת משמשת לשליטה, בקרה ואיסוף מידע על מכשירים הפועלים על מערכת ההפעלה Android.

תיחום המערכת

המערכת תפעל על מערכת ההפעלה Android. תוכנת השרת שולחת את המידע לתוכנת הלקוח כל x זמן, או בכל פעם שיש גישה לאינטרנט- TBD תוכנת השרת אוגרת את המידע עד לשליחתו אל הלקוח, ואז מוחקת אותו.

אילוצים

פיתוח בAPI Levels 9-18.

גרסאות אנדרואיד 2.2 עד 4.3.1.

**תהליכים מרכזיים**

* איסוף מידע
  1. אודות הטלפון (מספר גרסה, מספר טלפון ועוד)
  2. אנשי קשר
  3. היסטוריית שיחות
  4. אסמסים
  5. רשימת אפליקציות
  6. רשימת קבצים ותיקיות
  7. האזנה למיקרופון (כל x דקות קח דגימת קול של y דקות, או הקלט בתאריכים ... בשעות ...)
  8. האזנה לשבב NFC (האזנה אקטיבית- כל הזמן)
  9. מיקום GPS (כל x דקות קח מידע מהGPS, או הקלט את מסלול המשתמש בתאריכים ... בשעות ...)
  10. לוח שנה
  11. רשימה של קבצים שהוספו לאחרונה כמו: תמונות, וידיאו ואודיו
* שינוי מידע
  1. מחיקת קבצים
  2. הוספת קבצים
  3. מחיקת תיקיות
  4. הוספת תיקיות
  5. מחיקת אסמסים
  6. שליחת אסמסים
  7. מחיקת שיחות מהיסטוריית השיחות בפלאפון
* הפצה
  1. הדבקה ע"י אתר אינטרנט
  2. הדבקה ע"י שליחת האפליקציה לרשימת אנשי הקשר
* הסתרה
  1. במידה ויש Privilege Escalation
  2. במידה ואין Privilege Escalation
* שליחת מידע לשרת
* Privilege Escalation

**פירוט תהליכים מרכזיים**

* איסוף מידע
  1. אודות הטלפון- תחילה ישלח מידע אודות הטלפון כמו מספר גרסה, מספר טלפון, ועוד. לאחר מכן ישלח מידע אודות שינויים במידע זה.
  2. אנשי קשר- תחילה ישלחו כל אנשי הקשר (כולל המידע הנ"ל: שם פרטי ושם משפחה, מספרי טלפון, כתובת דואר אלקטרוני וארגון). לאחר מכן, ישלחו אנשי קשר חדשים או אנשי קשר שנערכו מאז העדכון האחרון.
  3. היסטוריית שיחות- תחילה תישלח כל היסטוריית השיחות ששמורה במכשיר. לאחר מכן ישלחו השיחות שהתבצעו מאז העדכון האחרון (כולל המידע הנ"ל: איש הקשר איתו בוצעה השיחה/מספר טלפון, שיחה יוצאת/נכנסת, תאריך ושעה ,משך השיחה).
  4. אסמסים- תחילה ישלחו כל האסמסים השמורים (לפי אנשי קשר ומספרי טלפון). לאחר מכן ישלחו כל האסמסים שנשלחו/התקבלו מאז העדכון האחרון (כולל המידע הנ"ל- איש קשר/מספר טלפון, אסמס יוצא/נכנס, תאריך ושעה).
  5. רשימת אפליקציות- תחילה תשלח רשימה של כל האפליקציות המותקנות על המכשיר לפי חלוקה של אפליקציות שהורדו ואפליקציות מובנות. לאחר מכן, תישלח רשימת אפליקציות שנוספו מאז העדכון הקודם.
  6. רשימת קבצים ותיקיות- תחילה תישלח רשימה של כל הקבצים והתיקיות של המכשיר המודבק (כולל המידע הנ"ל: שם הקובץ, סיומת, תאריך עריכה אחרון של הקובץ/תאריך יצירה של הקובץ). לאחר מכן תישלח רשימה של כל הקבצים החדשים שנוצרו /נערכו.
  7. האזנה למיקרופון- האזנה למיקרופון תתרחש כאשר נערכת שיחה יוצאת/נכנסת.
  8. האזנה לשבב nfc-
  9. מיקום GPS- איסוף רשימה של מיקומי הGPS הידועים (כל פעם שבעל המכשיר המודבק הדליק GPS).
  10. לוח שנה- איסוף של רשימה של כל האירועים החדשים שנוספו( עם המידע הנ"ל: זמן ומקום).
  11. רשימה של קבצים שהוספו לאחרונה כמו: תמונות, וידיאו ואודיו- רשימה של קבצים שהוספו לאחרונה (לדוגמא צולמה תמונה חדשה וכו').
  12. במקרה של השגת ROOT- יוספו גם רשימת אימיילים והיסטוריית גלישה ברשת.
* שינוי מידע- התוכנה תיכנס לדף באתר, שם ישמרו כל בקשות המשתמש, היא תשנה מידע במכשיר המודבק בהתאם לבקשות המשתמש. כל הפרטים להוספת/מחיקת מידע יהיו בבקשות המשתמש.

1. מחיקת קבצים- ימחק קובץ לפי שמו, הסיומת שלו ומיקומו.
2. הוספת קבצים- יוסף קובץ, בשם מסוים ובמיקום מסוים במכשיר המודבק .
3. מחיקת תיקיות- תמחק תיקייה לפי שמה ומיקומה (כל הקבצים/תיקיות שנמצאים בתוך תיקייה זאת ימחקו גם הם).
4. הוספת תיקיות- תוסף תיקייה לפי שם ומיקום רצוי.
5. מחיקת אסמסים- ימחק האסמס הרצוי מהמכשיר המודבק.
6. שליחת אסמסים- ישלח אסמס למספר טלפון מסוים.
7. מחיקת שיחות מהיסטוריית השיחות בפלאפון- ימחק התיעוד של שיחה מסוימת.

* הפצה
  1. הדבקה ע"י אתר אינטרנט
     + WAP push SL
  2. הדבקה ע"י שליחת האפליקציה לרשימת אנשי הקשר
     + SMS
     + email
* הסתרה
  1. במידה ויש Privilege Escalation
  2. במידה ואין Privilege Escalation
     + התחזות לאפליקציה תמימה ושימושית
     + הסתרה מהlauncher
     + הסתרה מרשימת האפליקציות
* שליחת מידע לשרת
  1. המידע מוצפן.
  2. המידע ישלח לכתובת URL בשרת.
* Privilege Escalation
  1. ע"י שימוש בexploit והשגת גישת ROOT
  2. ע"י קבלת Android Device Administrator
  3. ע"י שימוש בSU (מותקן כבר על המערכת אם המכשיר פרוץ)
  4. ע"י שימוש בADB
     + אפשור הADB והתחברות אליו מתוך הפלאפון ע"י ADB over Tcp.

**צד שרת**

תיאור כללי

המערכת מופקדת על איסוף הנתונים מהשרת והצגתם למשתמש בממשק Web

המערכת תאפשר למשתמש לשלוח פקודות לביצוע אצל השרת דרך ממשק הWeb

תיחום המערכת

המשתמש יתקשר עם תוכנת הלקוח ע"י כניסה לכתובת מסויימת דרך דפדפן אינטרנט.

תוכנת הלקוח אחראית לשמירת המידע והצגתו למשתמש בממשק נוח.

אילוצים

**תהליכים מרכזיים**

* קבלת מידע מהלקוח
* התחברות
* פעולות שמתבצעות באתר
  + פקודות משתמש (שינוי והוספת מידע)

1. מחיקת, הוספת ושינוי קבצים ותיקיות
2. הוספת ,עריכת ומחיקת אנשי קשר
3. הוספת והסרת אפליקציות
4. מחיקת, שליחת והוספת SMSים.
   * הצגת מידע שנאסף
5. הצגת מידע טכני אודות הטלפון (מספר גרסה, מספר טלפון ועוד)
6. הצגת רשימת אנשי קשר
7. הצגת היסטוריית שיחות
8. הצגת אסמסים
9. הצגת רשימת האפליקציות המותקנות
10. הצגת רשימת הקבצים והתיקיות
11. הצגת תמונות + וידיאו
12. שמיעה לקבצי הקול שהתקבלו מהלקוח, והצגת מידע לגביהם
13. הצגת הstrings שהתקבלו מהאזנה לשבב הNFC
14. הצגת המיקומים שהמשתמש היה בהם עפ"י תאריכים ושעות ע"ג המפה, אם הלקוח עוזב אזור מסויים או נכנס אל תוך אזור מסויים- הצגת התרעה TBD
15. הבלטת אנשי הקשר הפעילים ביותר
16. הבלטת הפעולות הנפוצות ביותר בשרת
17. הצגת לוח שנה ובו האירועים של הלקוח

**פירוט תהליכים מרכזיים**

* קבלת מידע מהלקוח
  + פענוח המידע
  + הכנסת המידע למסד הנתונים המתאים
* התחברות
  + המשתמש יכניס שם משתמש וסיסמא
* פעולות שמתבצעות באתר
  + פקודות משתמש (שינוי מידע)
    1. מחיקת קבצים- המשתמש יבחר שם של קובץ מרשימת הקבצים הנתונה.
    2. הוספת קבצים- המשתמש יעלה קובץ מהמחשב שלו, יבחר את השם שיינתן לו במכשיר המודבק (עם ציון הסיומת שלו, שם קובץ ייחודי) והמיקום (לפי רשימת התיקיות).
    3. מחיקת תיקיות- המשתמש יבחר תיקייה מרשימת התיקיות.
    4. הוספת תיקיות- המשתמש יבחר ומיקום ואת שם התיקייה החדשה (שם התיקייה יהיה ייחודי).
    5. מחיקת SMS-המשתמש יבחר אסמס מסוים מרשימת הSMSים.
    6. שליחת SMS- המשתמש יבחר את תוכן ההודעה (טקסט- בעל מקסימום של מספר תווים-TBD), ואת מספר הטלפון אליו תישלח ההודעה.
    7. מחיקת שיחות מהיסטוריית השיחות בפלאפון- המשתמש יבחר את תיעוד השיחה שירצה למחוק מהיסטוריית השיחות מהרשימה.
  + הצגת מידע שנאסף-