מטלת סיכום –
מעבדת התקפה

מגישים:

ניר ששון - 212174486

אופק אלון – 213101637

שלב ראשון – בחינת אפליקציית המקור ותכנון

השתמשנו ב APKTOOL על מנת לבצע UNPACK לאפליקציית הבסיס לאחר מכן עברנו עליה כדיי להבין איפה אנחנו רוצים להשתיל את הקוד, ראינו שקיים מתודה של ONCLICK ולכן הבנו שמדובר כנראה על אחד מהכפתורים במסך לאחר מכן ראינו את הקריאה למתודה GETRANDOM והבנו שלאחר הקריאה הזו כנראה שאנחנו צריכים להשתיל את הקוד.

הבנו שהצורה הכי פשוטה לכך תהיה לבצע קראיה לפונקציה אחרת בקוד לאחר הGETRANDOM שהיא בעצם הקוד שנשתול, כדיי לעשות זאת בצורה נוחה שתדרוש כמה שפחות שינויים בהעתקה של הקוד SMALI תיהיה ליצור אפליקציה חדשה עם כפתור יחיד ששמו הוא אותו שם של הכפתור שבו אנחנו מנסים "לחטוף את הפעולה שלו" ושכל התוכן הוא בפונקציה בודדת על מנת להוריד את כמות השינויים שאולי נצטרך לבצע.

שלב שני – בניית האפליקציה

בעזרת אנדרואיד סטודיו פתחנו אפליקציה חדשה עם כפתור אחד שכאשר לוחצים עליו נוצר קובץ TXT.INFORMATION המכיל מידע על הטלפון אותו רצינו להוציא, תהליך העבודה שלנו בהוצאת מידע היה קודם להוציא כמה שיותר מידע ללא שימוש בהרשאות כלל – יכלו בעיקר להוציא דברים פשוטים שהכילו אותם קלאסים כמו BUILD, PACKGEMANNGER, BATTERYMANNGER

מהם הוצאנו: מידע שקשור למכשיר כמו מודל המכשיר מי ייצר אותו מהי מערכת הפעלה ועוד מידע הנשמר בתוך BUILD הקשור למכשיר

מידע לגבי אפליקציות אחרות שקיימות כמו השם שלהם את ההרשאות שניתנות להם ועוד מידע המופיע בPACKAGEMANAGER

מהאחרון הוצאנו את אחוז הסוללה הנוכחי

בנוסף השתמשנו בשלוש הרשאות

```
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />

<uses-permission android:name="android.permission.INTERNET" />

</ "uses-permission android:name="android.permission.READ_CONTACTS>
```

השתיים הראשונות משמשות כדיי שנוכל להשתמש בWIFIMANEGER ובאמצעותו להוציא מידע על חיבור הWIFI כגון מהירות, סוג וכו...

האחרונה משמשת כדיי להוציא את שמות אנשי הקשר ומספר הטלפון שלהם מהמכשיר

שלב שלישי – השתלה

הוצאנו את ה APK של האפליקציה מאנדרואיד סטודיו לאחר מכן ביצענו אותו תהליך שעשינו לאפליקציית הבסיס עם APKTOOLS

חיפשנו את הפונקציה מהקוד והעתקנו אותה אל אפליקציית המקור לאחר מכן ביצענו שינויים בפונקציה מכיוון שהיא בנויה ל PACKAGE של האפליקציה שבנינו וצריך היה להחליף את שם הPACKAGE לשם של אפליקציית הבסיס

לאחר מכן הוספנו את הקריאה לפונקציה לאחר הקריאה לGETRANDOM

והוספנו את ההרשאות שנדרשות למניפסט ושיהיה ניתן לדבג

עשינו REPACKGE ואז חתמנו בעזרת SIGNER-APK-UBER

שלב רביעי – הרצה

גררנו את ה APK אל תוך האימולטור ונתנו לאפלקציה את ההרשאות שהיא צריכה לאחר לחיצה על כפתור הRANDOM DATE יצאנו ממנה והלכנו אל המקום בו נשמר הקובץ, וייצאנו את המידע החוצה

*בסרטון של ההדגמה הוספנו אנשי קשר רנדומלים למען שנוכל להדגים את היכולת הזאת

דוגמאות למידע שהוצאנו והסבר

שם היוסר תחת :user

מה הסוג של המשתמש תחת :type

מייצר, מודל, חברה, SDK, גרסת אנדרואיד

מידע על האפליקציה

```
(category, label, dataDir, permissions)
```

בעצם לכל אפליקציה יש שורה שזה המידע עליה

הוצאנו גם את האינטרפייסים ואיכות חיבור האינטרנט, כתובת הIP הפנימית

שם איש הקשר ומספר הטלפון

*גודל הקובץ תלוי במספר אנשי הקשר ומספר האפליקציות בסופו של דבר אנחנו הוספנו אנשי קשר אך האפליקציות הם הבסיסיות שמגיעות עם הטלפון