

מטלת הסיכום שלכם לקורס מעבדת התקפה הינה עד כחודש לאחר סוף הסמסטר 13.2.22.

**מטלת סיכום מעבדת התקפה**

במטלת הסיכום תבחרו עליכם לבנות אפליקציה באנדרואיד.

1. **גניבת מידע**:

* אתם מקבלים קובץ APK של אפליקציה תקינה. אתם נדרשים להוסיף לאפליקציה זו תוכן זדוני.
* האפליקציה התקינה הועלתה למודל, מופיעה תחת השם "אפליקציית בסיס".
* התוכן הזדוני יופעל כאשר המשתמש ילחץ על כפתור הrandom.
* מטרתו של התוכן הזדוני היא להשיג כמה שיותר מידע על המשתמש/המכשיר שיוריד את האפליקציה שלכם.
* אין הגדרה מדויקת לאלו הרשאות אתם יכולים להשתמש. אתם מוזמנים להשתמש באלו הרשאות שתרצו.
* לאחר שתכניסו את התוכן הזדוני על ידי repackaging, יש לוודא שאכן האפליקציה עומדת ביעד שלה ולא קורסת בשום שלב.
* את המידע שנגנב, תייצאו לקובץ בשם information.txt שישמר בתיקיה בה רצה האפליקציה, בצורה של הגדרה: מידע

לדוגמא...

Current username: cyber

במידה והצלחתם אוטומטית למצוא את המשתמש שרץ כרגע בפלאפון (ושמו במקרה זה הוא cyber).

או...

Sdk version: 10

אם הצלחתם להבין אוטומטית שהמכשיר/אמולטור את גרסת הsdk שהמכשיר מריץ (בריצה זו 10).

1. **הגשה:** תצטרכו להגיש קישור לגיטהאב שתפתחו לתיבת ההגשה. ב**גיטהאב** יהיו התכנים הבאים:
   1. האפליקציה הסופית שלכם, כך ששמה היא ID.apk כשID הוא מס' ת.ז. שלכם.
   2. קובץ הinfromation.txt שיצרתם.
   3. קובץ pdf שמתאר את התהליך שעשיתם.
   4. סרטון וידאו קצר של עד 5 דקות, שמתאר את הפעלת האמולטור (דרך סטודיו או מחוץ לו), הפעלת האפליקציה שלכם באמולטור, יצירת קובץ הinformation.txt, שליפת הקובץ מהאמולטור ופתיחתו בnano\gedit\notepad או כל תכנת מעבד תמלילים שתרצו. קובץ הוידאו צריך להיות בפורמט MP4.
2. **נא לשים לב שככל שתשתמשו ביותר הרשאות, האפליקציה שלכם תראה יותר זדונית. הציון יורכב מהתייחסות לכמות ההרשאות שבקשתם על מנת שהאפליקציה תרוץ מול כמות המידע שהצלחתם לגנוב.**

שאלות ותשובות

**שאלה:** מהי הדרך לבצע repackaging?

**תשובה:** המתודה מופיעה במעבדה הזו:

<https://seedsecuritylabs.org/Labs_16.04/Mobile/Android_Repackaging/>

שם מכניסים תוכן זדוני קבוע לאפליקציה, במטלה שלכם אתם קובעים איזה תוכן יוכנס.

**שאלה:** מהי הדרך הטובה ביותר לייצר תוכן זדוני?

**תשובה:** יש כמה דרכים. אם אתם יודעים לכתוב את הדברים בsmali, אשריכם. אם לא, ניתן לכתוב את הפקודות שגונבות את המידע בתוך אנדרואיד סטודיו, לקמפל וליצור APK שמכיל את התוכן הזה. לאחר מכן, לפתוח את הAPK שנוצר ע"י apktool ולקחת את התוכן שנכתב עבורכם בsmali ולהכניס אותו לאפליקציה שלכם (וכמובן לסגור מחדש את האפליקציה ולחתום עליה).