נושאים מתקדמים בזיהוי חורי אבטחה והגנת סייבר במערכות הפעלה

תרגיל 2

תאריך הגשה: 2.6.2017

הגשה ביחידים

חלק קריאה

בקורס למדנו על גישה אחת לביצוע sandbox שמתבסס על מודל אבטחה מבוסס יוזרים והרשאות למשאבים.

במערכות הפעלה אחרות קיימים מודלי אבטחה שונים וכתוצאה מכך, קיימים sandbox-ים שונים.

בחלק זה עליכם לקרוא על ה-Android security model, להבין מה העקרון שלו וכיצד אפליקציות שמשתמש מוריד ומתקין חסומות מביצוע פעולות אסורות.

עליכם להגיש קובץ בו אתם מסבירים במילים שלכם את המודל אבטחה, מה הוא מספק ומה מפתח צריך לעשות כדי לעמוד בו ולהשוות את התכולות שהוא מספק לעומת מה שנלמד בכיתה כ-sandbox במע"ה כמו Windows.

אין צורך לפרט באופן ארוך מידי, אלא להסביר באופן ברור נושאים כמו

- כיצד שפות התכנות הנפוצות משפיעה על אבטחת תוכנות
- מהו מנגנון ההרשאות של תוכנות שונות ב-Android (האם הוא מתבסס על כך שמדובר בקרנל לינוקס?)
- כיצד המודל מגביל או מקל על המפתח לבצע משימות שונות כמו תקשורת משתמש, תקשורת עם האינטרנט ועם חומרה

חומר קריאה רלוונטי

- https://source.android.com/security/overview/app-security
- https://crypto.stanford.edu/cs155/lectures/17-mobile-platforms.pdf

חלק פיתוח

נבנה תוכנת Broker גנרית שמקבלת כפרמטר תוכנה להריץ ב-sandbox, ותריץ אותה.

```
mysandbox  -torun C:\temp\target.exe
```

כאשר נריץ את התוכנה בפרמטר עם הרשאות כמה שיותר נמוכות שלא תצליח להתפרץ החוצה.

דרישות

חסימת הרשאות

התוכנה שלכם צריכה לקבל כקלט נתיב לקובץ הרצה ולהריץ אותו, כאשר התוכנה רצה במגבלות הבאות:

- התוכנה יכולה לכתוב אך ורק לתיקיה מסוימת שנוצרה במיוחד בשבילה, אותה היא תקבל כפרמטר ב-command line שלה (בנוסף לכל שאר הפרמטרים הרגילים שלה)
  כלומר כל קריאה ל-Createfile (או כל דרך אחרת ליצור קבצים) תיכשל אלא אם מדובר בקובץ תחת הנתיב המוגדר.
- התוכנה חסומה מליצור חלונות
  די מובן מאליו
- התוכנה חסומה מלתקשר עם עכבר/מקלדת
  יש לוודא שכל דרך מתועדת לקרוא מקשי מקדלת שלא מיועדים לחלו התוכנה (שלא קיים אחד כזה) לא יעבוד.

IPC

נספק לתוכנה שרצה ב-sandbox יכולת לתקשר החוצה אם הקוד מודע לזה שהוא ירוץ ב-sandbox.

שיטת המימוש פתוחה לכם, אך המימוש צריך לספק את היכולות הבאות

- יכולת גישה לקבצים כרצון ה-**broker** עבור כתיבה/קריאה
  כלומר תוכנה צריכה להצליח לבקש מה-broker גישה לקובץ מסוים (בהרשאות R/RW וכו'), יכולת לקרוא או לכתוב.
  החוקיות של למה לאפשר נתונה לשיקול דעתכם והמימוש כנ"ל.
- יכולת להציג חלון שמציג הודעה למשתמש ומקבל תשובה חזרה כטקסט
  כלומר היכולת לבקש מה-broker להציג חלון עם טקסט מה broker כך שיש אופציה למשתמש להקליד תשובה באורך כרצונו ושהתוכנה תידע לקבל את התשובה מה-broker.

הגשה

עליכם להגיש את הפרויקט באופן הבא

- הסבר על מבנה הקוד
  - כיצד ביצעתם כל חלק מהדרישות
  - בעיות פונטציאליות שזיהיתם בקוד שלכם
- קוד שרץ על Windows 7+
- תוכנה שתממש את ה-broker ובעזרתה נריץ תוכנות ב-sandbox
- ספרייה (header/lib או header/lib/dll) שמאפשר לתוכנה בתוך sandbox לתקשר החוצה

רמזים

- יש לעבוד צמוד לכלים כמו Process Monitor ו-Process Explorer כדי להבין למה משהו עובד או לא עובד.
- בעזרת windbg אפשר להסתכל בדיוק איזה הרשאות קיים לתהליך
- קוד של sandbox-ים באינטרנט לא יעזור, אבל התיעוד שלו בהחלט כן 😊
- לצרכי עבודה עם token-ים, תיעוד רלוונטי (אך לא מקיף)
  https://msdn.microsoft.com/en-us/library/windows/desktop/aa374909(v=vs.85).aspx

https://msdn.microsoft.com/en-us/library/windows/desktop/aa379316(v=vs.85).aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/aa446583(v=vs.85).aspx

- לצרכי עבודה עם IPC

https://msdn.microsoft.com/en-us/library/windows/desktop/aa366551(v=vs.85).aspx

https://msdn.microsoft.com/en-us/library/windows/desktop/aa365780(v=vs.85).aspx

- למחמירים שרוצים לבדוק את הקוד שלהם
http://s7ephen.github.io/SandKit/