תרגיל רביעי

חולשות LPE

מועד הגשה – 09.06.22

תכנות בטוח – 89509

הנחיות כלליות

- עבודה ביחידים או בזוגות בלבד.
- הפעילו שיקול דעת.

סעיפי התרגיל

1. מערכות הפעלה רבות מאפשרות למשתמשים להריץ קוד בהרשאות נמוכות.
הפרדה בין סוגי ההרשאות האפשריים ובין הרשאות של משתמשים שונים והקרנל מכילות עקרונות דומים מאוד, אך גם שונות מאוד במהותן בין מערכות הפעלה שונות.
הכינו קובץ PDF המתאר חולשה של העלאת הרשאות לוקאלית (Local Privilege Escalation, LPE) באחת ממערכות ההפעלה הבאות:
   א. אנדרואיד ומערכות מבוססות לינוקס
   ב. Windows
   ג. iOS

בנוסף, ניתן לכתוב על וריאציות של העלאת הרשאות, כגון בריחה מ-VM או מדוקר.

הנחיות לתרגיל

א. ניתן לחפש חולשות באתר זה - CVE - Search CVE List (mitre.org).
ב. מצופה שהסיכום על החולשה יהיה מעמיק ומובן. דהיינו, במידה ויש חולשה מאוד פשוטה שההשמשה שלה הייתה מאוד פשוטה, היא כנראה לא תתאים לתרגיל. מצד שני, אין צורך לבחור את החולשה המסובכת ביותר.

הנחיות להגשת התרגיל

את התרגיל יש להגיש בסבמיט לקבוצה 01. עיקר ההגשה הוא קובץ PDF מפורט המסכם את החולשה. ניתן לצרף נספחים כמו השמשה, קטע קוד חולשתי וכדומה. הסיכום צריך להיות ברור ומקיף – באופן שאדם עם רקע בסיסי יוכל לקרוא את הסיכום ולהבין מה הייתה החולשה, איזה סוג של חולשה היא הייתה, באיזה מנגנון וכיצד סגרו אותה.

בנוסף, יש להפנות ל-CVE הרלוונטי של החולשה.

כל שמות הקבצים שאתם מגישים צריכים להיות הגיוניים, ועם תווים אנגליים וסימנים בקידוד ASCII בלבד (בלי אותיות בעברית או בשפות שהן לא אנגלית) – על מנת לא לבלבל את ה-submit.

לכל תרגיל צריך להיות מצורף קובץ בשם details.txt, המכיל את תעודות הזהות של המגישים, ושמות המשתמש שלהם בסבמיט.

שימו לב שהקובץ הוא קובץ טקסט פשוט מקודד ב-ASCII על מנת שיוכלו לקרוא אותו בקלות.
פורמט מבוקש –

```
name1
id1
name2
id2
```

סטודנט שבחר להגיש את התרגיל לבד, יגיש קובץ details כמתואר בתרגילים הקודמים.

במידה ויש שאלות בנוגע לתוכן התרגיל, נא להפנות לסגל הקורס בהקדם האפשרי.

הערות

טעות לעולם חוזר.

בהצלחה!
