"הגנת סייבר במערכות מבוססות רשת" – תרגיל 3

תאריך הגשה: 02.03.2016

הגשה ביחידים או בזוגות בלבד

את כלל העבודה יש לבצע במכונה וירטואלית ללא גישה לאינטרנט אלא במצב Internal Network בלבד, פרט לגישה ל-Source Control

כלל שורות הקוד הנכתבות ב-Python צריכות לעמוד בתקן PEP8[1]

מומלץ לבצע את התרגיל תוך שימוש בכלי Source Control כלשהו (למשל github או bitbucket)

מטרת תרגיל זה ליישם את כלל הכלים אשר נלמדו במהלך הסמסטר תוך שימת דגש על:

- הכרות עם בעיות אבטחה בפרוטוקולי תקשורת
- זיהוי והבנה של חורי אבטחה בפרוטוקולי תקשורת
- אפיון ומימוש של מנגנוני הגנת סייבר להתמודדות עם בעיות אבטחה בפרוטוקולי תקשורת

להלן דוגמאות לסוגי פרויקטים אפשריים:

- הוספת מנגנון הגנה לפרוטוקול מוכר (שנלמד בכיתה) והתקפה שנלמדה כנגדו בכיתה
  - תחילה יש לממש בעזרת סקריפט את בעיית האבטחה
  - במידה ומדובר בפרוטוקול מבוסס Client-Server, יש לממש כחלק מהפרויקט גם את ה-Client עם יכולות האבטחה וגם את ה-Server עם יכולות האבטחה
  - הדגמה כי לאחר הוספת יכולות הגנת הסייבר שהחלטתם לממש ההתקפה שהדגמתם אינה עובדת יותר
  - דוגמאות:
    - Secure DHCP
      - הוספת תמיכה בפרוטוקול להתמודדות עם Rouge DHCP
    - Secure ARP
      - התמודדות עם ARP Poisoning
- הוספת מנגנון הגנה לפרוטוקול (**שלא נלמד בכיתה**)
  - תחילה יש לזהות חור אבטחה בפרוטוקול
  - יש לממש סקריפט בסביבת מעבדה (סביבת VM שלא מחוברת לאינטרנט) את בעיית האבטחה
  - במידה ומדובר בפרוטוקול מבוסס Client-Server, יש לממש כחלק מהפרויקט גם את ה-Client עם יכולות האבטחה וגם את ה-Server עם יכולות האבטחה
  - הדגמה כי לאחר הוספת יכולות הגנת הסייבר שהחלטתם לממש ההתקפה שהדגמתם אינה עובדת יותר
  - דוגמאות:
    - LDAP
    - TFTP
    - SMB

[1] https://www.python.org/dev/peps/pep-0008/

- ניתוח פאסיבי של תעבורת תקשורת וזיהוי של 4 התקפות שנלמדו בכיתה
  - יש לממש גם הדגמות לתקיפות המזוהות
- ניתוח פאסיבי של תעבורת תקשורת וזיהוי 2-3 התקפות שלא נלמדו בכיתה (כתלות ברמת מורכבותן)
  - יש לממש גם הדגמות לתקיפות המזוהות
- FW אשר ממש פונקציות אבטחה שונות כגון:
  - Statful Inspection
  - DPI
    - תמיכה בפרוטוקולים ספציפיים (למשל DNS/HTTP ועוד)
    - למשל זיהוי Tunneling על-ידי חריגה מ-RFC
  - בניית מנגנון חוקים המאפשר אפשור/חסימה של העברת נתונים בהתאם להגדרות המשתמש
- פיתוח של פרוטוקול מאובטח
  - פרוטוקול הזדהות
  - פרוטוקול מאובטח להעברת קבצים
  - פרוטוקול ניהול של רכיבי תקשורת
- **<u>כל פרויקט שאושר פרטנית</u>**

<u>הנחיות מחייבות</u>:

- כל פרויקט חייב להכיל מימוש ל שמנגנון הגנה
  - פרויקטים אשר יכילו רק מציאת חור אבטחה/מימוש חור אבטחה
- **כל קבוצה צריכה לקבל אישור לפרויקט עד לתאריך ה-24.1.2016**
- בנוסף לבדיקת קוד המערכת תערך בדיקה פרונטלית לכל אחת מהקבוצות
- ציון התרגיל יהיה מורכב מ-70% קוד שיוגש ו-30% בדיקה פרונטלית