**פרויקט למעבדה באבטחת מידע – ד"ר איתן קוך –** **etankoch@gmail.com**

**הנושא – ערוצים סמויים ב- SIP**

1. **רקע –** ערוץ סמוי , covert channel, הוא סוג של מתקפה אבטחתית היוצרת יכולת להעביר ישויות מידע בין תהליכים, ומוגדר כ"כל ערוץ תקשורת שניתן לנצל אותו ע"י תהליך לצורך העברת מידע באון המפר את מדיניות האבטחה של המערכת". הסיבה לכינוי "סמוי" היא שהערוץ מוסתר מפני מנגנון ההרשאות של מערכת המאובטחת ברמה גבוהה, מפני שהוא אינו משתמש במנגנוני העברת המידע הלגיטימיים של המערכת הנמצאים תחת בקרת מנגנון ההרשאות. רוחב הסרט של ערוץ סמוי מוגדר כמספר הביטים לשנייה שניתן להעביר בערוץ. סטגנוגרפיה (ביוונית כתב מוסתר) היא הסתרת מידע בתוך מידע אחר. SIP – Session Initiation Protocol הוא פרוטוקול איתותים ומטרתו החלפת מידע בזמן אמת המאפשר יצירת מפגש וירטואלי מעל הרשת ומאפשר מתן שירותים כגון שיחת טלפון, וידאו ועוד. זהו הפרוטוקול המוביל בעולם ה- VoIP. SIP בגרסה העדכנית 2.0 מוגדר ב- RFC3261.
2. **מטלות הפרויקט**
	1. לימוד נושא ערוצים סמויים, סטגנוגרפיה ו- SIP וסיכום קצר שלהם – 3 שבועות.
	2. אפיון ותיכון תוכנה להעברת מידע סמוי ב- SIP בהתבסס על תוכנת קוד פתוח (חופשי) של SIP, בין שני מחשבים (רגילים או וירטואלים) על גבי ערוץ איטרנט. בפועל לא נבדיל בין ערוץ סמוי וסטגנוגרפיה כהגדרתם לעיל. יודגש שהמידע הסמוי מועבר ע"י תוקף "הרוכב" על שיחת SIP לגיטימית, ללא ידיעת מבצעי השיחה הלגיטימית – 6 שבועות.
	3. קידוד התוכנה להעברת מידע סמוי, כולל יכולת להזין כקלט את המידע הסמוי לצפות בו בעת המעבר, ולוודא את קבלתו ביעד. ניתן להסתפק בהעברת מידע מצד א' ל-ב' – 10 שבועות.
	4. בדיקות, הדגמת הפרויקט, הכנת מצגת סיום – 13 שבועות.
	5. הגשת דו"ח סופי – 14 שבועות.
3. **בהצלחה!**