המרכז לחינוך סייבר
CYBER EDUCATION CENTER

תרגיל מסכם מערכות הפעלה – הזרקת קוד

ברק גונן

בתרגיל המסכם תכתבו תוכנה שמבצעת מספר שלבים נפוצים בנוזקות.

הנחיות כלליות:

- עליכם להגיש את הקוד הסופי. אין צורך להגיש קוד שלב בנפרד, הציון יתבסס על השלב אליו הגעתם במימוש.
- כל הקוד שקשור לעבודה עם סוקטים יפותח באמצעות WinAPI. אין להשתמש בספריות קוד מוכנות.
- לצורך פישוט העבודה, הריצו את השרת והלקוח על אותו מחשב. ניתן לעשות זאת באמצעות שימוש בכתובת ה-IP המיוחדת 127.0.0.1.

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

שלב א- ביצוע IAT Hooking (60 נקודות)

בצעו את התרגיל המסכם שבפרק 9, IAT Hooking.

התוכנית שלכם:

א. תבדוק אם קיים process של notepad
ב. תבצע IAT Hooking לפונקציה CreateFile
ג. תציג MessageBox עם כיתוב כלשהו

הדרכת השלבים נמצאת בספר הלימוד, עמודים 215-226

שלב ב – הוספת DLL Injection (20 נקודות)

קשה לצפות מ-Process שיעשה לעצמו IAT Hooking 😊

בצעו את שיפור ב', שבעמוד 227. למעשה ביצעתם את התרגיל הזה כבר כשעשיתם את תרגיל DLL Injection, כעת תשלבו בין התרגילים ליצירת קוד הרצה שמבצע ל-Process אחר DLL Injection ומשנה את ה-IAT שלו.

שלב ג – הוספת דיווח למפעיל מרוחק (20 נקודות)

עד כה, בכל פעם שנקראה הפונקציה CreateFile, גרמתם להופעת MessageBox. כעת תעשו משהו מעניין יותר. תפתחו Socket מול שרת ובכל פעם ש-CreateFile נקראת, תשלחו לשרת הודעה כרצונכם.

כיצד לעשות זאת?

א. לימדו איך משתמשים בסוקט לתקשורת בין שרת ולקוח. צרו קוד פשוט שמקים קשר בין לקוח ושרת ושולח הודעה מהלקוח.
ב. כחלק מה-WinMain שב-DLL, הקימו את הסוקט מול השרת, שרץ על המחשב שלנו. השרת פעיל כל הזמן וממתין ללקוח שינסה להתחבר אליו, השרת רץ כפרוסס נפרד ומאזין לכתובת 127.0.0.1 בפורט שתבחרו
ג. ה-IAT Hooking שלכם ישתמש בסוקט הפתוח לשליחת הודעה כלשהי לשרת, במקום לפתוח MessageBox כפי שעשיתם עד כה

טיפ: עליכם ללמוד לבד את הבסיס של כתיבת סוקטים. ניתן להשתמש בספר הלימוד "רשתות מחשבים" של המרכז לחינוך סייבר, אשר מסביר את הפקודות

הבסיסיות של פתיחת סוקט בשרת ובלקוח. לאחר שהבנתם את התיאוריה, רצוי להעזר בתיעוד של msdn.

בהצלחה!