מגיש: בן זמיר
benzamir1234@gmail.com

פרוייקט סיום קורס - פייתון התקפי

רקע כללי:

מערכת שליטה בתצורת reverse shell ב- tcp. מאפשרת שליטה מרחוק על מחשב היעד.
הכלי בנוי מ2 קבצים: מערכת השליטה וסוס טרויאני.

הסוס איננו מזוהה במערכות אנטיוירוס ואיננו נחסם על ידי פיירוול בזכות תכונת הreverse shell.
התעבורה מוצפנת בהצפנה סימטרית - AES.

צורת פעולה:

1. שליחת הסוס הטרויאני במסווה של תמונה. פתיחה של התמונה גורמת לסוס לעבוד ברקע ובמקביל לפתוח תמונה של כלב על מנת לא להעלות חשד.

2. הסוס ינסה להתחבר באופן אוטומטי כל 1-20 שניות (רנדומלי).

3. הפעלת מערכת השליטה. חיבור מוצלח מאפשר הרצת פקודות וקוד מרחוק עם ממשק gui.

כלים מהקורס אשר הוטמעו במערכת:

1. שליחת פקודות cmd דרך שדה טקסט ב- gui.
2. שליפת כל סיסמאות ה- wifi השמורות במערכת.
3. שיטוט בתיקיות של המחשב הנשלט.
4. הצפנת התעבורה בAES
5. שליפת ה clipboard של המחשב הנשלט

כלים נוספים:

1. שליפת מידע ונתונים על המערכת הנשלטת באמצעות ספריות פייתון
2. אתחול של המחשב הנשלט

מאפיינים:

א. שימוש ב try exception בקוד למניעת קריסה וטיפול בשגיאות

ב. ממשק קלט ופלט ב gui הכולל שורת סטאטוס ושדה טקסט נגלל שמכיל את פלט הפקודות

ג. ממשק ה gui נבנה בשימוש בסיפריית .Tkinter על מנת לייצר חיבור ולולאה של תקשורת במקביל לעבודת הממשק בוצע שימוש ב thread. החיבור עצמו מתבצע ב thread נפרד כך שממשק ה gui עדיין פעיל במהלך החיבור.

ד. המשתנה שמחזיק בסוקט הוא משתנה גלובלי וכך ניתן לגשת אליו מה thread ומבחוץ במקביל.