זיהוי פלילי

מבוא:

בתרגיל זה נתנסה בזיהוי פלילי של תוכנה זדונית מצילום זיכרון.

בתרגיל זה:

1. נבדוק מהי גרסת מערכת ההפעלה כדי שנדע אילו פקודות אפשר להפעיל על צילום הזיכרון.
2. נבדוק אילו תהליכים רצים במערכת ובאילו חיבורי תקשורת הם משתמשים.
3. ננתח תהליכים חשודים באמצעות שליפת שורת הפקודה שלהם וניתוח המחרוזות בזיכרון שלהם.
4. בסוף, נאושש את החשד שלנו ע"י העלאת שחזור קובץ ההרצה (EXE) של התהליך החשוד ל-VirusTotal.

פקודות מיוחדות

- הפקודה connscan מאפשרת לסרוק את הזיכרון בחיפוש אחר pool-ים שמתארים חיבורי TCP קיימים וכאלה שכבר לא קיימים.
- הפקודה sockets מאפשרת לבצע מעבר על רשימה מקושרת שמתארת את ה-socket-ים הפתוחים, חלקם יכולים להיות מחוברים וחלקם – לא. הפקודה קיימת רק במערכות הפעלה XP ו-2003.
- הפקודה cmdline מציגה את שורת הפקודה עמה הורץ כל אחד מהתהליכים במחשב. בפרט, בשורת הפקודה ניתן למצוא את הנתיב המלא של התוכנות שרצות.

הוראות:

יש לענות על השאלות הבאות. אחרי כל תשובה יש לכתוב את שורת (או שורות) הפקודה שהורצה כדי לענות על השאלה.

1. מהי גרסת מערכת ההפעלה שצולמה בצילום הזיכרון?
2. מהו מספר התהליך ששמו "reader_sl.exe"? מהו מספר התהליך שיצר אותו?
3. מהי כתובת הIP של המחשב שזכרונו צולם?
4. לאילו שתי כתובות IP ולאילו PORTים התבצע חיבור מהמחשב שזכרונו צולם?
5. לאילו כתובות IP ולאיזה PORT המחשב היה מחובר בזמן הצילום?
6. בהתאם לשורת הפקודה, מה שם החברה שפיתחה את התוכנה "reader_sl.exe"?
7. שמור את הזיכרון של התהליך "reader_sl.exe" והוצא את המחרוזות ששמורות בו. מהי הכתובת ששמורה מיד לפני bankofamerica.com?
8. שמור את זיכרון התהליך כקובץ EXE והעלה אותו ל-VirusTotal.com. איזו תווית McAfee נותן לקובץ EXE הזה?

הוראות הגשה

1. יש להגיש קובץ PDF שמכיל תשובות לשאלות 1-8.
2. רק נציג אחד מהקבוצה צריך להגיש.
3. שם הקובץ צריך לכלול את מספרי ת.ז. של כל חברי הקבוצה.

בהצלחה!