מגישים: שרון דניאלי 305053217 וספיר מלצקי 308427806

מיני פרויקט בנושאים באבטחת רשתות

תוכנית העבודה

התרחיש:

החדרת קובץ זדוני למערכת סגורה (כגון חברות פרטיות) דרך מערכת חיצונית (מייל).

בניית כלי בהתאם לצד המשתמש בו מבצע אחד מהדברים הבאים:

1. בהינתן מידע ותמונה מטמין את המידע (הקובץ) בתמונה.
2. בהינתן תמונה בלבד מחלץ את המידע שהוטמן.

הכלי מאפשר להחדיר למערכות שונות קובץ שמתנהג כמו תמונה אך בעצם מכיל מידע נוסף שמצליח להטעות אותן כי מדובר בתמונה בלבד. לתוקף (מקבל התמונה) יש גישה למערכת הסגורה אליה ישלח הקובץ אל מייל של החברה ובאמצעות הכלי יוכל לפתוח את התוכנית הזדונית. כיוון שהקובץ מוטמן בתמונה מערכות אבטחת החברה לא יזהו שמוגדר במידע זדוני.

המטרה: העברת מידע באופן סמוי (למשל קובץ זדוני) וגישה אליו על ידי שימוש בכלי שפיתחנו. נתעמק באופן הסתרת התוכנית בתמונה. מטרתנו היא העברת התוכנית הזדונית ללא חשד של מערכות אחרות דרכה היא עוברת.

אבני דרך / יעדים:

1. הכרות בסיסית של תחום עיבוד תמונה והשתלת מידע בתמונה.
2. הכרות עם python ועם הספריות הרלוונטיות.
3. אנו מניחים שיש בידינו דרך התקשרות עם המערכת המותקפת (למשל מייל של החברה) ואיש קשר מתוך המערכת שמודע לתוכנית הזדונית. יחד עם זאת, ללא הנחה זו אנו עשויים להתקשות בביצוע המשימה שכן המידע יגיע ליעד אך לא יופעל.
4. יצירת סביבת עבודה מתאימה לצורך מימוש עתידי של הפרצה.
5. כתיבת הכלי עצמו.
6. תאריך ההגשה 8/2/2020

האתגר: יצירת קובץ שנראה כתמונה תמימה והחדרתו למערכת סגורה.

אתגר נוסף שיכול להיות שהתמונה כן הועברה והגיעה ליעד אך הכלי שפיתחנו לא יכול להמצא במחשבי החברה. למקבל ישנה גישה למחשב במערכת שאותה אנו מנסים לעקוף, אך לכלי שבנינו אין אפשרות גישה מתוך המערכת. נוכל גם ללא שימוש בכלי לפתוח את הקובץ שמוסתר בתוך התמונה על ידי מערכות חוקיות שמאפשרות זאת כמו winrar. כמו כן נצטרך להניח שהמקבל יודע על האופן בו הקובץ הוטמן בתמונה.

חוזקות:

- בפעולה פשוטה ולא מודעת של המערכת המותקפת, נוכל להעביר את התמונה יחד עם התוכנית הזדונית. המקבל של התמונה יוכל לקבל גישה אל הקובץ המוסתר ולבצע הרצה של הווירוס במערכת המותקפת.
- ניתן להוסיף מידע על גבי קובץ התמונה מבלי להשפיע על נראות התמונה על המסך מה שמהווה יתרון להסתרת הפעולה המתוכננת מהמותקף.

תיעוד העבודה

תיאור הכלי ותיעוד הקוד

הכלי מבצע אחד מהדברים הבאים:

1. בהינתן מידע ותמונה מטמין את המידע (הקובץ) בתמונה.
2. בהינתן תמונה בלבד מחלץ את המידע שהוטמן.

בעת הרצת הכלי מופיע התפריט הבא:

```
Please enter your choose -
 create malicious image: 1
 extract file from image: 2
```

מקרה 1: קבלת תמונה וקובץ:

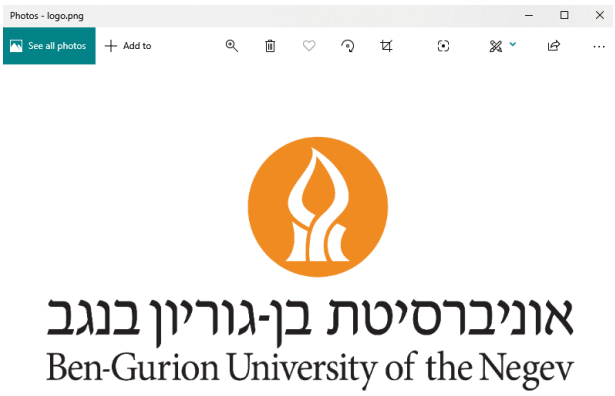
בהינתן path לתמונה וpath לקובץ, נכניס את הקובץ לתוך התמונה באמצעות השלבים הבאים:

```
Please enter your choose -
 create malicious image: 1
 extract file from image: 2
 1
Enter path of the file you want to hide:
C:\Users\מיכל\Downloads\virus-setup.exe
Enter path of the image should be cover:
C:\SHARON\University\Projects\logo.png
```

התמונה המקורית שקיבלנו היא בגודל ההתחלתי:

logo	23/01/2020 18:49	PNG File	162 KB

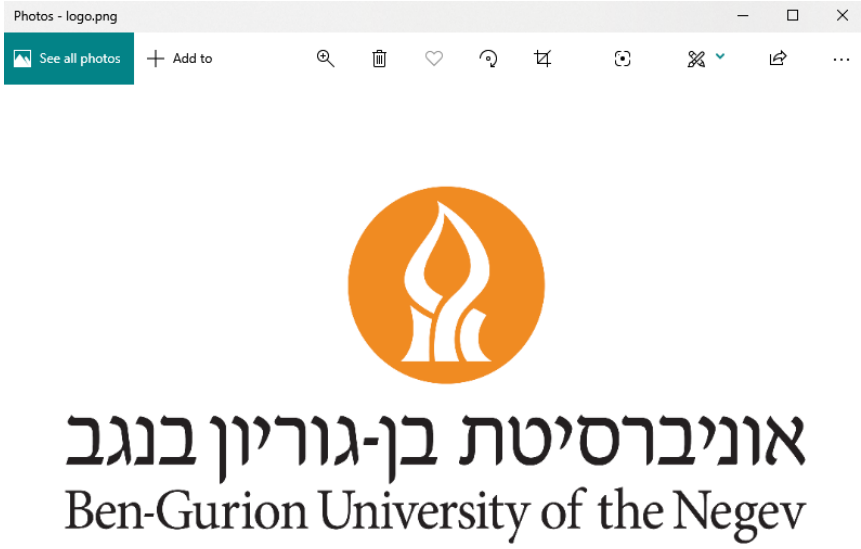
ונראית כך:



בשלב הבא נשלב באופן בינארי את הקובץ המוטמן ביחד עם קובץ התמונה ואז נקבל קובץ תמונה חדש, שנראה כמו הקודם אך מכיל בתוכו את המידע הנוסף. נוכל לראות זאת בגודל התמונה שהשתנה:

logo	23/01/2020 18:49	PNG File	9,698 KB

אך עדיין בפתיחתה, נראית אותו הדבר:



⤢

<u>מקרה 2: חילוץ המידע המוטמן מהתמונה:</u>

בהינתן התמונה עם המידע המוטמן, נפרק את קובץ התמונה ונחלץ את הקובץ הנוסף שהועבר יחד איתה:

```
Please enter your choose -
 create malicious image: 1
 extract file from image: 2
 2
Enter path of the image should be cover:
C:\SHARON\University\Projects\logo.png
```

כעת בתיקייה בה הייתה התמונה נוסף הווירוס וזמין להרצה:

logo	23/01/2020 18:49	PNG File	9,698 KB
virus-setup	23/01/2020 19:03	Application	9,536 KB

מענה למטרה

הכלי הוא דרך המימוש של המטרה: העברת מידע באופן מוסתר ממערכות ההגנה.
למשל קובץ מזיק לא היה יכול לעבור באופן ישיר במייל כי היה מתגלה על ידי המערכת, אך קובץ שמוטמן בתוך תמונה ונראה כאילו מועברת בהודעה תמונה "תמימה" עובר את מערכות הסינון.
כיוון שזה בדיוק מה שהכלי עושה הוא מממש עבורנו את המטרה.

בעיות

במקור, רצינו שבעת פתיחת התמונה הקובץ המוטמן בה יחל לרוץ. אך לאחר מחקר מעמיק בנושא הבנו כי תוכנית כזו היא מורכבת ודורשת שליטה בתחום. לכן החלטנו שאפשר לצמצם את המקרים בהם ישתמשו בכלי המקורי, בכך שקיים איש קשר בצד השני המודע לקיום התוכנית הזדונית והוא יהיה אחראי להרצתה.
כלומר הדבר המרכזי שהשגנו זה **החדרת הקובץ הזדוני** אל המערכת בה אנו רוצים לפגוע. הצעד הנוסף הוא הרצה שלו – שמתבצע על ידי גורם נוסף. נדגיש כי ייתכן וקיימת דרך שהחילוץ וההרצה של התוכנית הזדונית המוטמנת בתמונה תבוצע ללא התערבות אדם נוסף, אך החלטנו על הפתרון שתיארנו.

חוזקות הכלי

- הכלי מייצר קובץ תמונה חדש, הנראה זהה בסיומת ובתצוגה מלבד גודל התמונה המקורי. מה שאינו מעלה חשד אצל מקבל שאינו יודע על המטרה האמיתית שלה.
- פלט הכלי (התמונה עם המידע המוטמן) יכול להתקבל לכל מערכת הפעלה.

חולשות הכלי

- גודל התמונה וגודל הקובץ הזדוני צריכים לשמור על פרופורציה מסוימת. כלומר אם התמונה מאוד קטנה והקובץ מאוד גדול אז החיבור הבינארי ייכשל. אך ניתן תמיד למצוא תמונה אחרת בגודל מתאים שתענה על המטרה של הטמנת המידע הרצוי.

<u>סביבת עבודה והנדסה סביבתית</u>

המטרה היא שאם הקובץ המכיל את המידע המוטמן יגיע אל אדם אחר העובד בחברה ולא לאיש הקשר (התוקף) מתוך החברה הם לא ידעו שמדובר בקובץ זדוני ולא יהיו מודעים לכך שניתן לחלץ מהתמונה מידע נוסף. כלומר רק אדם היודע על ייעודה האמיתי של התמונה ידע לנסות ולגשת אל המידע שנמצא בה.

בנוסף, כיוון שהכלי שפיתחנו נועד להטעות את המערכות האבטחה הוא אינו דורש התעסקות מעמיקה נוספת בתחום הsocial engineering.

הרצת התוכנית שכתבתנו ויצירת הקובץ הזדוני נתמכים על מערכת הפעלה מסוג windows, אבל הגבלה זו לא חלה על המחשב המותקף שיפתח את התוכנית הזדונית. כל מחשב וכל מערכת הפעלה שמקבלת את התמונה ותומכת בwinrar תוכל לחלץ את המידע המוטמן. כך נוכל להעביר את המידע בין מערכות הפעלה שונות.

<u>הרצת התוכנית</u>

לשם הרצת התכנית נדרש במחשב המייצר את הקובץ הזדוני פייתון גרסא 3.6 ומעלה.
הקובץ ניתן להורדה מהגיט שלנו: https://github.com/dsharonbgu/netse201

יש להוריד את התיקייה (באמצעות git clone) ולהריץ את הקובץ ע"י פתיחת ה-command בתיקייה והרצת הפקודה: "python out_mini.py".
המחשב התוקף (שנמצא ברשת הפנימית אליה אנו רוצים לחדור) יכול לפתוח את הקובץ הזדוני ע"י מ-2 האפשריות הבאות: באמצעות התכנה שבנינו (ע"י בחירה באפשרות זו בתפריט) ואז הקובץ יחולץ לתיקייה של התמונה או ע"י פתיחת התמונה באמצעות winrar. כלומר, מקש ימני על הקובץ=> פתיחה באמצעות=> winrar.