**תוכנית עבודה – מיני פרויקט במערכות הגנה לרשת:**

יובל עמרמי 316417591

יעל ינאי 316418656

רקע לפרויקט: אחת מסוגי ההונאות הנפוצות ברשת היא phishing – גניבת מידע רגיש מהמשתמש על ידי התחזות.

לרוב, תישלח למשתמש הודעה על ידי אתר מוכר או חתומה בשם של אדם המוכר לו, בה יש קישור לאתר אחר. באתר שאליו המשתמש יועבר לרוב יתבקש להזין פרטים אישיים/ לשנות סיסמא/ לאמת אשראי וכו'. פרטי המשתמש יועברו (ללא אישור המשתמש) לגורם זר שיוכל לעשות בהם שימוש כרצונו.

ההנחה ב- phishing היא שהמשתמש בוטח בנמען ממנו הגיע הקישור ולכן לא יחשוד בדבר בעת כניסה אליו.

פעמים רבות גם האתר אליו מועבר המשתמש הוא אתר שדומה מאוד לאתר אמיתי שהמשתמש מכיר ולכן הוא לא יחשוד בדבר (לדוגמא, אתר ה"מתחזה" לאתר של בנק מוכר).

רעיון הפרויקט: הרעיון שלנו ייתן מענה לסיטואציות שכאלה על ידי תוסף מובנה לדפדפן chrome שיזהה אתרים זדוניים לפני כניסת המשתמש אליהם, יאמת קישורים שהמשתמש עלול להיכנס אליהם ויתריע למשתמש במידה ונתקל בכתובת חשודה.

מטרה ויעדים לפרויקט: ברצוננו להגן על משתמש מפני לינקים חשודים ברשת.

נבצע ווידוא שהכתובת אליה המשתמש רוצה להיכנס היא תקנית ומוכרת, על פי קריטריונים שנגדיר מראש.

בנוסף, במהלך הפרויקט נרצה ללמוד ולהכיר יותר טוב את עולם הגנת הרשתות ולהבין איך phishing פועל.

תוך כדי כתיבת הקוד ומימוש האלגוריתם נרצה להבין את זרימת הנתונים ברשת בעת לחיצה על קישור ומעבר לאתר אחר.

בסופו של הפרויקט נרצה להציג תוסף עובד, שאכן מתריע מפני אתרים זדוניים ונותן למשתמש, לאחר שקיבל את המידע, את האפשרות להחליט אם לגשת אליהם או לא.

תרחישים אפשריים בעת לחיצה על לינק אליהם נתייחס:

* לינק תקין – לא צריכה לקפוץ שגיאה, ממשיכים כרגיל.
* לינק זדוני – קופצת שגיאה למשתמש. חסימת גישה (האתר לא ייפתח ברקע) ורק אם המשתמש בוחר לאשר ולהיכנס בכל זאת – מעבר לאתר.

אתגרים וקשיים במימוש הפרויקט:

* על מנת לאמת את נכונות הקישור אליו נכנסים יש לבחור שיטה להגדרת אתר כאתר בטוח לכניסה.

נגדיר 2 אפשרויות למימוש האימות:

* + תחזוקה של רשימת "אתרים טובים", ניתן לגשת רק לאתרים שנמצאים בה וחסימת כל אתר שלא ברשימה.

הקושי המרכזי בגישה זו יהיה התייחסות לעובדה שהרשימה צריכה להיות דינמית, גדלה עם הזמן, לפי מידע נוסף שנצבר באלגוריתם. מעבר לכך, יש לדאוג לכך שחווית המשתמש לא תואט ותפגע משמעותית.

* + חיפוש ברשת (על ידי האלגוריתם) של האתר כדי לאשר את "זהותו", כלומר, לקבוע אם זדוני או לא.

הקושי המרכזי בגישה זו יהיה זיהוי של אתר תקין כתקין ואתר זדוני כזדוני (אם לא, ויקרה מצב בו נזהה אתר זדוני כתקין - המשתמש עלול להיפגע). בנוסף, נצטרך להגדיר שיטה לזיהוי מילה/ות החיפוש הרלוונטית – כלומר נצטרך להגדיר מה יש לחפש באינטרנט כאשר האלגוריתם נתקל בקישור (רצף תווים מתוך ה- URL עצמו/ מילים שמופיעות "מסביב" לקישור באתר...).

* הגדרת אתרים זדוניים ובדיקת המערכת מולם. בדיקות האם התוסף שנבנה יצליח לזהות אתרים זדוניים ברמה מספקת. הגדרה של רמה סבירה של זיהוי אליה נרצה להגיע.
* אתגרים טכנולוגיים – שימוש בטכנולוגיות חדשות ולא מוכרות לנו, למידה על תהליכי זרימת נתונים ברשת, התאמת הטכנולוגיות לפתרון הבעיה המוצגת.
* שמירה על חווית משתמש בעת גלישה ברשת.

חוזקות התוצר המוגמר:

* זמינות – לא נדרש מהמשתמש לפתוח תוכנה או אתר נוסף במקביל לעבודתו במחשב, פועל על הדפדפן שבשימוש.
* אם יעיל ומהיר אז אין כמעט פגיעה בחוויית משתמש.
* שמירה על משתמש מטעויות שלעיתים נגרמות מחוסר ערנות (לחיצה על קישור ש"נראה אמין" והגיע כהודעת מייל, או מתוך אתר מוכר).
* הגנה על אוכלוסיות שמועדות יותר ל"נפילה" לטעויות כאלו (אנשים מבוגרים, ילדים...).

אבני דרך + לוח זמנים:

* הכרות עם הטכנולוגיות הרלוונטיות.

יבוצע עד ל- 01/04/2021.

* הכרות ואפיון עולם התוכן - סוגי האתרים הזדוניים הקיימים, כיצד מבוצע המעבר בין אתרים שונים (לחיצה על לינקים, פתיחה אוטומטית...), זיהוי ההבדלים בין אתרים תקינים לאתרים זדוניים.

יבוצע עד ל- 01/04/2021.

* בחירת שיטות מימוש ואימות אמינות האתר ונכונות האלגוריתם.

יבוצע עד ל- 01/05/2021.

* בניית תשתית עבור התוסף לדפדפן.

יבוצע עד ל- 01/05/2021.

* כתיבת אלגוריתם לזיהוי אתרים זדוניים + מתן הרשאות מתאימות לאלגוריתם כך שיוכל לזהות ולגשת לקישורים שמופיעים בתוך אתרים. כתיבת לוגיקה של זיהוי מילות מפתח באתרי המקור והשוואה מול הלינק.
  + במידת הצורך, לפי ביצועי האלגוריתם בעת בדיקה שלו, נדרש להבין כיצד ניתן לשאוב מידע מתוך חיפוש ב- Google ובנוסף מתוך האתר בו מתבצעת הגלישה. זאת לשם ווידוא אמינות הקישור אליו המשתמש רוצה לגשת.

יבוצע עד ל- 01/06/2021.

* בדיקת נכונות וביצוע tests לתוסף.

יבוצע עד ל- 15/06/2021.

* כתיבת דו"ח סיום לפרויקט, הסקת מסקנות והפקת לקחים.

יבוצע עד ל- 30/06/2021.

הטכנולוגיות בהן נשתמש: עבור מימוש הפרויקט נכתוב תוסף לדפדפן chrome.

* התוסף ייכתב ב- JavaScript, HTML.
* עבור הלוגיקה של האלגוריתם נשתמש ב- JavaScript, ובנוסף ב- python במידת הצורך.