יאנה אורחוב – 321112591

עמית מעוז - 206197717

**תיעוד סופי - מיני פרויקט:**

**מסמך תיעוד זה מכיל:**

1) תיאור הפרויקט – נושא וחלקים

2) תיאור קבצי ההגשה

3) קשיים ודרכי התמודדות

4) הסבר נלווה לסרטון הסימולציה

**1) תיאור הפרויקט:**

**נושא הפרויקט:**

תקיפת phishing בתצורת man in the middle – גניבת נתוני ההתחברות (יוזר וסיסמא) של משתמשי ה-submission system האוניברסיטאית ושמירתם בקובץ הנגיש לתוקף ללא ידיעת המשתמשים.

במסגרת התקיפה נרצה להוביל את המשתמשים לדף נחיתה מזויף בעל נראות זהה לחלוטין לדף ההתחברות של מערכת ה-submission. האתר הנ"ל יהווה למעשה מעין Proxy – יבצע מעבר של המשתמש לאתר ה-submission המקורי באמצעות פרטי ההתחברות שהזין, תוך שמירה שלהם לקובץ צדדי.

**המטרה המרכזית** היא שמירת נתוני ההתחברות של כמה שיותר משתמשי המערכת, ללא ידיעתם.

\* נציין שהבחירה שלנו במערכת ה-submission של האוניברסיטה אינה מחייבת , והתקיפה ניתנת ליישום על מערכות שונות בהן מבוצע תהליך login, תוך ביצוע התאמות קלות.

**תיאור חלקי הפרויקט:**

**החלק הראשון** - יצירת קוד QR אשר סריקה שלו באמצעות מכשיר mobile מובילה להעתק מזויף של דף התחברות למערכת ה-submission. פניה לקהל הסטודנטים באמצעות חלוקת עלונים ברחבי הקמפוס שעל גביהם ה-QR ימצא, אשר יציעו התחברות זריזה למערכת ה-submission.

**החלק השני** - יצירת ההעתק המזויף של דף ההתחברות ל-submission, אשר יגרום לקרבנות לחשוב שהם גולשים במערכת המוכרת וישכנע אותם להזין את פרטי ההתחברות שלהם.

**החלק השלישי** - שמירה של הנתונים שהמשתמש הזין בקובץ צדדי והעברתו לאתר המקורי.

**2) תיאור קבצי ההגשה**

הפרויקט מוגש כקובץ zip המכיל את הפרטים הבאים:

- תיקייה בשם qrCode המכילה את ה-source code היוצר את ה-QR.

- תיקייה בשם submission\_html המכילה את הקבצים הרלוונטיים ליצירת דף הנחיתה המזוייף.

- קובץ README המתאר בקצרה את חלקי הקוד הרלוונטיים.

- סרטון סימולציה של התקיפה בשם Mini\_Project\_Attack\_Simulation.mp4

- תכנית עבודה לפרוייקט

- מסמך זה (תיעוד סופי של הפרוייקט)

- מסמך הצהרת מקוריות

**3) קשיים ודרכי התמודדות:**

1. **פיתוי הקורבן אל האתר המזויף** – האתגר הראשוני בתהליך התקיפה הוא הבאת המשתמשים לאתר המזויף באופן שלא יעורר חשד. אפשרות נאיבית היא למשל שליחת קישור במייל לקורבן, אך בחירה בדרך עלולה להעלות קשיי אמינות בדבר הגורם השולח, תוכן המייל, וכו’.

בחרנו להתמודד עם מכשול זה באמצעות **שימוש בקוד QR** – כלומר , חלוקת עלונים ברחבי הקמפוס שיציעו התחברות מהירה למערכת ה-submission ע"י סריקת קוד QR מצורף.

הסיבה העיקרית לבחירה זו היא ניצול החולשה הטבעית של קודי QR – קשה עד בלתי אפשרי לאדם מן המניין להבדיל בין קוד benign לבין קוד malicious. בנוסף, בעידן של ימינו (ובפרט בעידן הקורונה) הולך וגובר השימוש בקודי QR (לעתים אפילו לביצוע פעולות רגישות כמו תשלום), ומכאן נובע חיזוק נוסף לאמינותם.

2. **אמינות האתר המזויף –** לאחר שהצלחנו להביא את הקורבן אל האתר המזויף, עולה האתגר של שכנוע הקורבן כי הוא גולש באתר ה-submission המוכר לו על מנת שיזין את פרטי ההתחברות שלו.

**דרכי התמודדות:**

**נראות** – עלינו ליצור את האתר המזויף כך שמבחינה ויזואלית יהיה בעל נראות זהה לחלוטין לאתר המקורי.

**קישור לאתר המקורי**- על מנת לייצר תחושת "חלקות" בתהליך מצד הקורבן, נבצע במקביל לשמירת נתוני המשתמש את בקשת ההתחברות בשמו אל מול השרת המקורי של המערכת, ובעקבותיה יועבר לאתר הsubmission המקורי כפי שציפה.

\* נציין שתי סוגיית אמינות נוספות בנושא זה. הראשונה נוגעת לשימוש ב-cookies המכילים את פרטי ההתחברות. במהלך תהליך ההתחברות השגרתי מרבית הדפדפנים מציעים מילוי אוטומטי של פרטי ההתחברות, שירות הדורש אימות קודם מול השרת המקורי ולכן אינו אפשרי מצד האתר המזויף שלנו. החשש בצד התוקף הוא שמשתמשים חדי עין יבחינו בהיעדר השירות הזה והדבר יעורר חשד באמינות התהליך. במסגרת התקיפה שאנו מציעים לא נתמודד עם סוגיה זו בשל מורכבותה.

הסוגיה השנייה נוגעת לכתובת האתר המזויף. בכדי לא לעורר חשד מצד הקורבן, יש לרכוש דומיין בעל כתובת דומה ככל הניתן לכתובת של המערכת אליה התוקף מבקש להתחזות.

3. **שמירת הנתונים לקובץ בצד התוקף** – יש למצוא פתרון למיקום הקובץ אליו יכתבו הנתונים, כך שיהיה נגיש לתוקף. **התמודדות:** הכתיבה מתבצעת למסמך google sheets שנוצר מראש על ידי התוקף ויהיה נגיש בפניו. השמירה בצד התוקף של פרטי ההתחברות נעשית רק כאשר המשתמש מזין את פרטי ההתחברות הנכונים שלו.

**4) הסבר נלווה לסרטון הסימולציה**

להגשה מצורף סרטון קצר המתאר את מהלך התקיפה. הסרטון מחולק ל-2 חלקים:

* בחלק הראשון מודגמת יצירת קוד ה-QR על ידי התוקף – נעשית בפשטות ע"י פתיחת הקובץ sumbissionQRnetsec/qrCode/main.py, עריכת הפרמטר לפונקציה pyqrcode.create כך שיכיל את כתובת האתר הזדוני והרצה של התכנית.

נציין שבסרטון ערך הפרמטר הנ"ל הוא כתובת לוקאלית של האתר הזדוני לשם המחשה. בפועל, על התוקף יהיה לרכוש דומיין בעל כתובת דומה ככל הניתן לכתובת של המערכת אליה הוא מנסה להתחזות.

* - בחלק השני מתוארת התקיפה עצמה. ניתן לראות בסרטון שני חלונות פתוחים. החלון הימני ממחיש את מה שמתרחש בצד הקורבן, והשמאלי את צד התוקף.

תחילה, הקורבן מבצע סריקה של קוד ה-QR. לשם נוחות הצילום, המחשנו בסרטון את הסריקה בעזרת פלטפורמה אינטרנטית שמאפשרת העלאה של קובץ התמונה של ה-QR ומבצעת פענוח של ה-url המקודד בו, ולכן היה עלינו להעתיק את הכתובת המפוענחת לשורת הכתובות בדפדפן. בפועל, אנחנו מצפים שהקורבן ישתמש באפליקציה במכשיר ה- mobile שלו וה-redirection יבוצע בצורה אוטומטית (מרבית אפליקציות הסריקה ל- mobile מבצעות זאת).

בהמשך, הקורבן מזין את פרטי ההתחברות שלו בדף הנחיתה המזויף, וכאשר הוא לוחץ על כפתור ok לביצוע ההתחברות, ניתן לראות שהוא אכן מועבר למערכת ה-submission (המקורית) ושבמקביל פרטי ההתחברות שלו נשמרים במסמך google sheets בצד התוקף.