יאנה אורחוב – 321112591

עמית מעוז - 206197717

**תוכנית עבודה למיני פרויקט:**

**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:** שמירת נתוני ההתחברות של כמה שיותר משתמשי המערכת, ללא ידיעתם.

**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.

**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’. לכן,נבחר להתמודד עם מכשול זה באמצעות **שימוש בקוד QR** – נחלק 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.

\* סוגיית אמינות נוספת בנושא זה 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.

3. **שמירת הנתונים לקובץ בצד התוקף** – יש למצוא פתרון למיקום הקובץ אליו יכתבו הנתונים, כך שיהיה נגיש לתוקף. **התמודדות:** נבצע כתיבה למסמך google sheets שנוצר מראש על ידי התוקף ויהיה נגיש בפניו.

**לו"ז עבודה ואבני דרך:**

|  |  |  |
| --- | --- | --- |
|  | **התחלת עבודה** | **דדליין** |
| כניסה אל עולם החולשות , קריאה על חולשות קיימות ומקרים מעניינים. מעבר על הCVE-ים הקיימים | 1.11.20 | 1.12.20 |
| בחירת נושא לפרויקט – התמקדות בחולשה או שתיים שמעניינות אותנו במיוחד ועשויות להתאים לפרויקט. | 1.11.20 | 1.12.20 |
| הבנה לעומק של החולשה שנבחרה לצורך מימושה, ובניית תרחיש תקיפה המשלב שבירת פרדיגמה ו-social engineering | 1.11.20 | 1.12.20 |
| הקמת העתק לאתר submission בעל נראות זהה לאתר המקורי | 1.12.20 | 1.1.21 |
| מימוש שמירת נתוני המשתמשים, בחירת מיקום הקובץ | 1.12.20 | 1.1.21 |
| יצירת QR המוביל לאתר הזדוני | 1.12.20 | 1.1.21 |
| יצירת עלונים משכנעים בצירוף קוד הQR אשר יגרמו לאנשים לסרוק | 1.12.20 | 1.1.21 |
| בדיקות של הפרויקט על מספר משתמשים | 1.1.21 | 15.1.21 |
| העלאה של הפרויקט לאוויר ויצירת קבצי תיעוד | 1.1.21 | 15.1.21 |
| הגשת הפרויקט | לכל המאוחר 15.1.21 |  |