**המחלקה להנדסת תוכנה**

**קונפיגורציה ואבטחת הרשת הביתית**

**חיבור זה מהווה חלק מהדרישות לקבלת**

**תואר ראשון בהנדסה**

**מאת**

**יועד שירן**

**ליאור ספיר**

**תמוז התשע"ז יולי 2017**

**המחלקה להנדסת תוכנה**

**קונפיגורציה ואבטחת הרשת הביתית**

**חיבור זה מהווה חלק מהדרישות לקבלת**

**תואר ראשון בהנדסה**

**מאת**

**יועד שירן**

**ליאור ספיר**

**מנחה אקדמי: דר' מרים אללוף אישור: תאריך:**

**רכז הפרויקטים: דר' יגל ראובן אישור: תאריך:**

**מערכת ניהול פרויקט ובקרת תצורה**

|  |  |  |
| --- | --- | --- |
| **#** | **מערכת** | **מקום** |
| **1** | **מאגר קוד** |  |
| **2** | **יומן** |  |
| **3** | **ניהול פרויקט** | **github** |
| **4** | **הפצה** |  |
| **5** | **סרטון** |  |

**תקציר**

פרויקט זה מספק כלי עזר לשליטה ומחקר על אבטחת נתבים בייתים.

בכל רשת ביתית שמתחברת לאינטרנט, מותקן רכיב חומרתי הנקרא "נתב".

עיקר המחקר והעבודה בפרויקט, מתמקד באבטחתו וקביעת תצורתו מחדש.

נתב (Router) – הוא רכיב תקשורת מחשבים שנועד לקביעת נתיבן והפצתן של חבילות נתונים ברשתות תקשורת נתונים.

הצורך בפרויקט, נדרש מכוח חולשת אבטחת הרשת הביתית, שאינה עמידה לאיומי פריצה המתקדמים ומשתכללים בכל עת. ברקע העבודה לפיתוח הגנת הרשת הביתית, גורמים מסוימים פועלים להכשלה ולגילוי חורים באבטחתה. תוצר עבודתנו מספק מחקר, תוכנת אבטחה ומוצר אפליקטיבי שמגבירים את רמת האבטחה, תוך יכולת קביעת הגדרות חדשות לרשת הביתית.

כל רשת ביתית המאפשרת רשת אלחוטית (WIFI) בתקן 802.1X, חשופה למתקפות חדירה וגילוי. במסגרת אבטוח הנתב, כשהוא נושא גדול ועמוס שמלא במחקר ועשיה ואין באפשרותנו לכסות את כל היבטיו, הגדרנו בפרט את הפלג בו נרצה לעסוק ולהתמקד באבטחה – כניסה ואימות המשתמש ברשת אלחוטית ביתית. בתחילת עבודתנו, הצבנו לעצמנו את המטרה להגנה מפני מתקפת Brute Force. עם המחקר והעשייה לסלילת הפתרון, יצרנו ארסנל להגנת מתקפות נוספות, שלא שמנו ביעדנו לפתור אותם.

Brute Force – הינו אלגוריתם שמטרתו הוא פיצוח סיסמאות כניסה למחשב או רשת אלחוטית, באמצעות ניסיון להיכנס עם כל הסיסמאות האפשריות, עד להצלחה. ניתן להפעיל את המתקפה על כל רשת ביתית שעובדת על תקן IEEE802.

הטכניקה אינה יעילה, מכיוון שמספר הצירופים הוא עצום. זמן פעולת האלגוריתם עד לפיצוח הסיסמא יכול להיות בלתי מוגדר או מוגבל ולכן אינו מספק פתרון יעיל לפריצה כשהוא לעצמו. על מנת לשפר את האלגוריתם משתמשים ב "מילון סיסמאות" – מילון שמכיל צירופים נפוצים ושכיחים המופעים בסיסמאות בדרך כלל. מילון סיסמאות מייעל את זמן הפריצה באופן משמעותי.

במסגרת הפרויקט חקרנו את המתקפה הפוגעת באבטחה, ישמנו פתרון לחדירת הכניסה של גורם שאינו רצוי ברשת הביתית ופיתחנו מוצר לשלוט על תצורת הנתב הביתי דרך מכשיר אנדרואיד, מוצר שעוד איננו קיים בעולם עת לזמן כתיבת המסמך!

ע"י אימות מחדש נוכל למנוע את מתקפת הBrute Force, אימות נוסף ואפליקציה שיוכלו לזהות את המתקפה ואת התוקף ולמנוע ממנו מלהתחבר לרשת.

הצהרה:

הפרויקט נעשה בהנחיית ד"ר אללוף מרים,

המכללה האדמית להנדסה ירושלים – המחלקה להנדסת תוכנה.

החיבור מציג את עבודתי האישית ומהווה חלק מהדרישות לקבל תואר ראשון בהנדסה

תודות

תוכן העניינים

מילון מונחים, סימנים וקיצורים

נתב - Router

1. **מבוא**

הבאנו כי ניתן לפרוץ את הרשת הביתית ולהתחבר לאינטרנט על גבי שירות שניתן למישהו אחר.

ישבנו וחקרנו כיצד ניתן להגן על רשת ביתית מפני חדירת גורם זר במהלך הפרויקט התחלנו לבצע מחקר על דרכי חדירה לרשת האלחוטית ועלינו על מתקפה שנקראת Brute Force.

במהלך המחקר גילנו כי יש תהליך התחברות מורכב לשרת המערב הצפנות מסובכות מעולם האבטחה אך עם זאת קיים כלי נפוץ מאוד הנקרא Air Crack . הכלי מסוגל לנחש את הסיסמה של הרשת האלחוטת בעזרת תהליך פריצה מסוים. עם כל סוגי האבטחה הקיימת על הרשת האלחוטית עדיין ניתן לפרוץ אותה ביותר קלות. בפרויקט זה אנו נציע דרך להתגונן מפני הפריצה לרשת האלחוטית וזיוף תהליך האימות.

נציג בפרויקט זה 2 מוצרים שפיתחנו על מנת לפתור את בעית האבטחה הקיימת.

מוצר 1 – מוצר זה מוצר תוכנתי היושב על מחשב ברשת ונקרא שרת אימות. תפקידו לאמת את המשתמש החדש ברשת האלחוטית.

הצורך במוצר זה הינו לעקוף את בעית האבטחה הקיימת ברשת אלחוטית ולפתח תהליך אימות חדש.

מוצר 2 – אפילקציה להגדרת מאפייני הנתב מחדש.

הצורך במוצר הזה נובע מהצורך לקבל את נתוני הנתב כפי שהם על מנת לקבוע את מאפייני הנתב בצורה נוחה ולקבל מידע אשר מאפשר לנו לזהות אנומליה ברשת האלחוטית.

מוצר זה אינו קיים היום בשוק. והוא מהווה פריצת דרך בתחום האנדרואיד ונוגע בשליטה מרחוק וקנפוג הנתב.

אחת מהמתקפות הקיימות בעולם הסיבר היא מתקפת Brute Force

* 1. רשת ביתית - היא רשת טלקומוניקציה המאפשרת העברת נתונים.

מכשירים המחוברים לרשת המחשבים מעבירים זה לזה נתונים על גבי חיבורים להעברת נתונים.



איור 1 : רשת WIFI מסוג personal המבוססת על תקן IEEE802

הרשת הביתית שאנו נתמקד בפרויקט היא רשת שעובדת לפי מודל הOSI העובדת על תקן IEEE802.1X .

מודל הosi מתבסס על חלוקת תפקידים בין פרוטוקולי תקשורת שונים. כאשר בכל פרוטוקול ישנם מספר חוקים מוסכמים שמגדירים את האופן שבו מבצע הפרוטוקול את תפקידו לטובת כלל תהליך התקשורת ובמקרה של הפרויקט שלנו, תהליך האימות לשלב האימות ברשת.

רשת WIFI מסוג personal היא רשת שקל יותר לעבוד איתה מהסיבה שהיא לא תלויה ברכיבים שמגודרים מחוץ לנתב. תהליך האימות ברשת personal קל, יעיל ונפוץ ברשתות WIFI ביתיות.

1.2



**הבעיה**

היום ניתן להאזין לכל המידע העובר ברשת אלחוטית העובדת על תקן IEEE802.

ברגע שניתן לראו

**המחקר**

**הפתרון המוצע**

**2 פרויקטים**

Abstract

***עמוד השער הפנימי באנגלית - דף דוגמה***

**Software Engineering Department**

**Project Name**

**by**

**Student Name**

**Academic Supervisor:**

***עמוד הכריכה*** *לדו"ח סיום פרויקט הגמר (אנגלית) - דף דוגמה*

**Software Engineering Department**

**Project Name**

**by**

**Student Name**

**July 2015 (civil date) Tamuz 5775 (Hebrew date)**