**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 לראות את התעבורה ברשת, המידע שלנו נחשף לגורמים זרים.

אין בידינו אפשרות שהמידע לא ייחשף לגורמים זרים אבל יש אפשרות להצפין את המידע ולהכריז על מפתח סימטרי משותף בין הנתב למשתמש.

ברגע שיש לנו מפתח משותף בין הנתב למשתמש, לגורם זר יהיה מאוד קשה לנתח את המידע ולהאזין לו בצורה שוטפת. ולכן לגורם זר יהיה אינטרס להבין מהו המפתח המשותף בשביל להאזין למידע העובר ברשת.

בשביל שהגורם זר ישיג את המפתח המשותף הוא יצטרך להתחזות למשתמש רגיל שמנסה לעבור את שלבי האימות של הנתב.

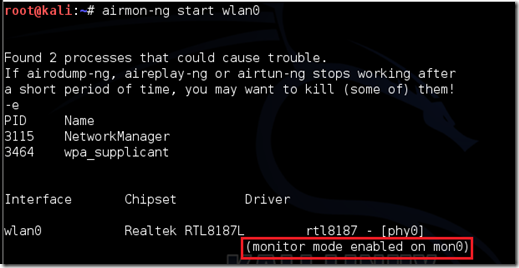
ברגע שהגורם הזר יעבור את שלב האימות הוא יהיה חלק מהרשת ויוכל להאזין לכל המידע העובר ברשת.

אנו בפרויקט זה נסביר כיצד גורם זר משיג את המפתח של הנתב ונהיה חלק מהרשת ונחקור את הבעיה בשביל למצוא לה פתרון.

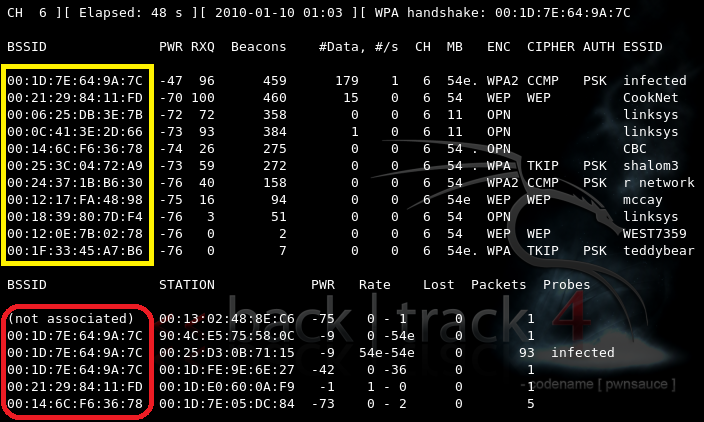
השאלה הראשונה שעולה, כיצד גורם זה יכול להאזין לרשת?

תשובה: יש היום המון כלים חינמים שניתן לראות את תעבורת הרשת. הכלי הנפוץ ביותר נקרא Air Crack והוא מחולק למספר tools.

הכלי הראשון שלו נקרא airmon-ng שהוא השלב הראשון לצורך האזנה לרשת. הוא פותח ממשק וירטואלי על כרטיס רשת האלחוטי שדרכו נוכל להאזין לתעבורת הרשת.



אחרי שפתחנו ממשק וירטואלי, נשאר רק להאזין לרשת, הכלי השני של air crack נקרא airodump-ng שבעזרתו אנו יכולים לראות את כל תעבורת הרשת (beacons)



החלק שמסומן בצהוב מייצג את הכתובות MAC של הנתבים עם הפרטים עליהם

החלק שמסומן באדום מייצג את הכתובות MAC של המשתמשים שמחוברים לנתבים.

נכון לעכשיו, לגורם זר יש את כל המידע ההתחלתי שהוא צריך לצורך מציאת רשת להאזנה.

בשלב הבא, הגורם הזר יחפש רשת פוטנציאלית שהוא ינסה להתחבר אליה.

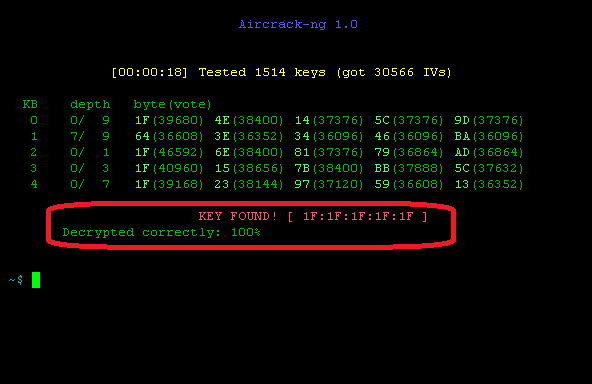
הוא יחפש משתמש שמחובר לאחת הרשתות, הוא יסתכל בחלק שמסומן באדום ויחפש את הכתובת של הנתב שאליה המשתמש מחובר.

השאלה שנייה שעולה : כיצד הגורם הזר יכול להחדיר פקטה שתגרום לאימות מחדש (תוך כדי שהוא מאזין לרשת)?

תשובה : ברגע שהגורם הזר מצא משתמש שמחובר לאחת הרשתות הוא יאזין לנתב הספציפי שהוא בחר ויחדיר פקטה לנתב (injection) ע"י הפקודה aireplay-ng שתגרום לאימות מחדש של המשתמש לרשת. (למעשה aireplay-ng מזייף פקטה שמתחזה למשתמש שהוא חלק מהרשת וגורמת לנתב להאמין שהמשתמש נותק ומנסה לבצע אימות מחדש).

ברגע שהמשתמש יבצע אימות מחדש לנתב, פקטת האימות תשמר אצל הגורם הזר ומה שנשאר זה רק לנתח את שלב האימות והסיסמה שבתוכו בעזרת הכלי Aircrack-ng.

Aircrack-ng מריץ מילון סיסמאות על פקטת האימות (brute force) עד שהוא מנחש את הסיסמה הנכונה לרשת



לאחר מחקר ארוך הגענו למסקנה שהחולשה של האימות ברשת נמצא בשלב שנקרא 4 way handshake.

(צריך לפרט על השלב?)

Aircrack-ng מדמה סביבה וירטואלית של תהליך ה4 way handshake במצב offline עד שהוא מוצא את הסיסמה.

ולכן בפרויקט זה נחקור וננסה להציע פתרונות לשלב האימות ברשת בשביל שגורם זר לא יצליח לחדור.

**המחקר**

אחרי מחקר ארוך מצאנו שהחולשה נמצאת בתהליך האימות וניסנו להציע פתרונות אחרים לשלב האימות

* כיצד מתבצע האימות ברשת
* תקנים לאימות ברשת
* קנפוג מחדש של הנתב (לצורך הגדלת האבטחה)
* שילוב שרת שיבצע את האימות לרשת

**הפתרון המוצע**

בפרויקט זה הגענו למסקנה שאנו חייבים לשנות את דרך האימות לנתב, להגדיר קונפיגורציה חדשה ולהוסיף בקרה (אפליקציה) שתבדוק אם מישהו הצליח לחדור לנתב.

הפתרון שלנו מחולק ל2 חלקים:

בחלק הראשון – בגלל חולשת הנתב בשלב האימות, חקרנו והבנו שאנו צריכים לבנות שיטת אימות חדשה.

התחלנו לחקור את שיטות האימות לנתבים ביתיים והבנו שיש מספר שיטות:

1. Wep
2. Wpa personal
3. Wpa2 personal
4. Wpa enterprise
5. Wpa2 enterprise

לכל אחת מהשיטות יש צורת אימות שונה.

חקרנו בשלב ההצעה/האב טיפוס את כל אחת מהשיטות הנ"ל והגענו למסקנה שהשלב היעיל ביותר שאנו יכולים לפתח ולשפר אותו הוא enterprise.

ההבדל העיקרי בין רשת מסוג personal לרשת מסוג enterprise ששיטת האימות שונה.

שיטת האימות ברשת personal היא מסוג passphrase – כלומר הצפנה על סיסמה ארוכה (ccmp/tkip) ע"י אלגורתים aes/rc4 ורשת מסוג personal עובדת על תקן ieee802.1n.

שיטת האימות ברשת enterprise היא זהה לרשת personal רק שהתקן משתנה לieee802.1X.

ההבדלים בין התקנים

Ieee802.1n – מאפשר את תהליך ה4 way handshake בתוך הנתב.

Ieee802.1x – מאפשר את תהליך האימות בשרת חיצוני (AS).

לאחר המחקר הממושך הבנו שכדאי לנו לעבוד על תקן ieee802.1x שתומך ברשת enterprise מהסיבה שאנו יכולים לבנות את שלב האימות ולשנות אותו ובכך להגביר את האבטחה על רשת ביתי.

-תהליך בניית הAS

בשלב הראשון של בניית השרת הAS היינו צריכים לפתוח socket ולהאזין לפרוטוקול UDP מהסיבה שנתב שעובד על תקן IEE802.1X עובד על פרוטוקול UDP.

בשלבי השני – היינו צריכים לדעת איך לקבל בקשה ולכן השתמשו בפונקציית recvfrom הנמצאת בספריית sys/socket.h.

בשלב השלישי – היינו צריכים לדעת לנתח ולקרוא את הבקשה (בשביל למנוע הודעות injection) ולכן בנינו שני פונקציות עיקריות, אחת שמדפיסה את הבקשה לתוך קובץ והשנייה בודקת שהמידע התקבל עומד בתקנים של rfc-2865.

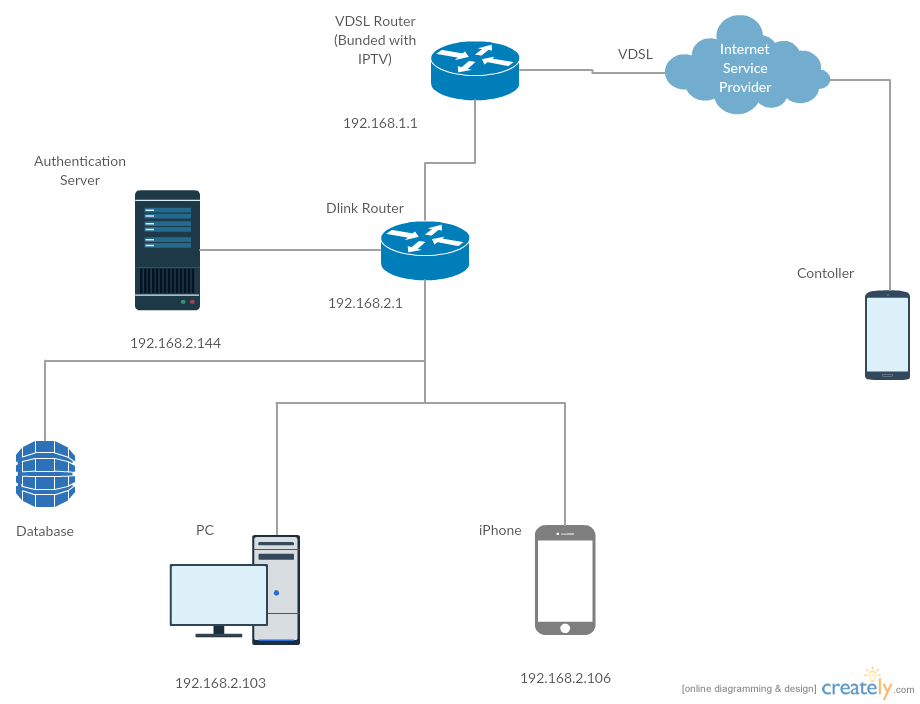
בשלב הרביעי היינו צריכים לזהות את סוג הבקשה – אם הבקשה היא request היינו צריכים לבנות פקטת אימות מסוג challenge ואם פקטת אימות היא מסוג challenge היינו צריכים לבנות פקטת accept/reject.

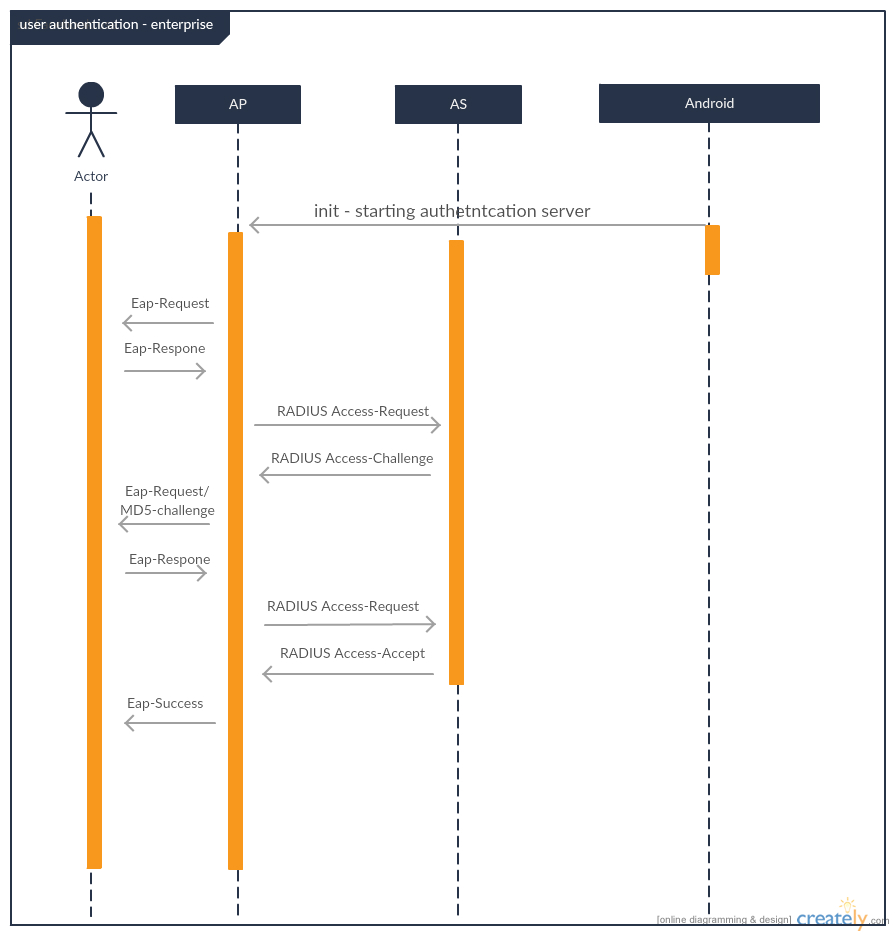
בשלב החמישי היינו צריכים להצפין את פקטת האימות שהתקבלה ולכן השתמשו בספריית libssl מתוך המערכת שיודעת להצפין בעזרת md5/hmac.

בשלב האחרון היינו צריכים לשלוח את פקטת האימות לAP.

בחלק השני – בנינו אפליקציה שיודעת לקרוא את נתוני הנתב ולקנפג אותו מרחוק. (פותחת שני sockets TCP/UDP, TCP לחיבור דרך telnet וUDP בשביל להסתנכרן עם הAS)

ארכיטקטורה





**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)**