Evil Twin Attacks

מגישים:

דביר אברהמי - 207029364
נדב קיסר - 207229477
הראל עזרא - 318926854

תקציר:

בשנים האחרונות גדל השימוש ברשתות אינטרנט אלחוטיות - Wifi - Wireless Access Point.

מתקפת התאום הרשע - evil twin מהווה יישום של התקפה קלאסית לעולם הסייבר האלחוטי מסוג Rogue-AP המתבצעת על רשת Wifi. העיקרון פשוט, המתקפה יוצרת רשת Wifi מזוייפת, וגורמת למשתמשים להתחבר אל רשת ה Wifi המזוייפת ובכך למעשה התוקף מתיישב על תעבורת הרשת בין הרשת אל המשתמש וכך יכול לגשת אל מידע רגיש. נציג רקע והסבר על המתקפה וכלי למימוש המתקפה בשפת Python ובעזרת הספרייה Scapy.

רקע:

מהי Evil Twin Attack?

מתקפת evil twin עובדת כך שהתוקף מקים רשת Wifi מזוייפת וגורם למשתמשים להתחבר אל הרשת ה Wifi המזוייפת במחשבה שהם מתחברים אל רשת שהם סומכים עליה וזאת במקום שיתחברו אל הרשת האמינה. לאחר שהמשתמש מתחבר אל הרשת המזוייפת ניתן בעזרת מגוון כלים לגשת למידע המועבר בדרך הרשת המזויפת כגון סיסמאות, כרטיסי אשראי ופרטים אישיים. אפשר ליצור רשת מזוייפת בעזרת כל מכשיר בעל יכולת אינטרנט ותוכנה זמינה. המתקפה שכיחה יותר ברשתות Wifi ציבוריות שמאובטחות פחות ויותר פגיעות.

המתקפה בעצם מאפשרת לרמות את המשתמש ע"י הוספת access point בעל שם רשת (SSID) זהה לAP האמיתי ולגרום למשתמש להתחבר לAP המזוייף במקום לAP המקורי. את הAP המזוייף מכנים Rogue AP.

תקן IEEE 802.11 והפגיעות שלו

תקן 802.11 הוא שם כולל למשפחה של תקנים לתקשורת אלחוטיות ברשתות מקומיות - WLAN. כאשר משתמש מתחבר לAP, נעשה זיהוי. המידע היחיד שמועבר בזיהוי הוא שם הרשת - SSID וכתובת הMAC. כתוצאה מכך ניתן דיי בקלות לייצור כתובת רשת מזוייפת עם אותו השם כמו של הרשת המקורית – SSID וכך תהליך ההתחברות אל הרשת המזוייפת לפי תקן 802.11 יעבוד כרגיל, והמשתמש לא יחשוד בכלום. בנוסף יש קושי בתקן לאמת את זהות שולחי החבילות ולכן ניתן לזייף חבילת ניתוק מהרשת המקורית עליה נסביר בהמשך.

איך עובדת המתקפה?

בדרך כלל, אלא אם כן הוגדר אחרת AP, יפרסם את שם הרשת (SSID) ע"י שליחת פקטת Beacon. המשמעות היא שכל מי שנמצא בסביבת הAP מודע לקיום הרשת האלחוטית. המשתמש ינסה להתחבר אוטומטית לAP המפרסם SSID מסוים במידה ובעבר המשתמש התחבר לאותה רשת עם (SSID) זהה ובהנחה, כמובן, כי ההגדרה להתחברות אוטומטית לא

השתנתה. פה המקום לציין שהמשתמש מתחבר לפי אותו מנגנון שהוגדר עבור אותו SSID , כלומר אם בעת ההתחברות הראשונית היה נדרש עבור SSID מסוים לספק סיסמא תוך שימוש במנגנון WEP , WPA2 או כל מנגנון אחר, אזי בכל פעם שהמשתמש יזהה כי קיימת רשת Wifi באזור עם אותו SSID ,היא תנסה להתחבר אליו תוך כדי הפעלת מנגנון האבטחה אשר הוגדר לרשת זו.

לפיכך, אם עבור רשת מסוימת המשתמש הוגדר להתחבר בעבר באמצעות סיסמא, במידה ונשנה בAP את ההגדרות עבור אותה רשת כך שלא תידרש סיסמא, המשתמש לא יתחבר לאותו AP, מאחר ומנגנון ההזדהות הדו-צדדי לא יעבוד הAP לא יצליח לעבור תהליך אימות מול המשתמש מאחר ואין בידו את הסיסמא / מפתח המוגדר. במידה והמשתמש היה מחובר לAP עם SSID מסוים אבל הוא קולט שידור בעוצמה גבוהה יותר מAP אחר עם אותו SSID, המשתמש ינסה להתחבר לAP החדש. עובדה זו מאפשרת לממש את ההתקפה Evil twin.

<u>שלב 1: מציאת מיקום ורשת לזיוף, ומשתמש לתקיפה</u>

בשלב הראשון נרצה למצוא מקום שיש בו רשת Wifi שיכולה להיות פגיעה. זה יכול להיות רשת ביתית אך עדיף רשת מרכזית חינמית כך שנוכל לזייף אותה ולקבל הרבה מידע. זה יכול להיות מקומות כמו ספריות, בתי קפה או אוטובוסים. במקומות ציבוריים יכולים להיות גם מספר AP שונים בעלי אותו שם מה שיקל על התוקף לזייף את הרשת ולקבל משתמשים שיתחברו. לאחר בחירת מיקום נרצה לבצע סריקה על מנת לאתר רשתות Wifi באזור, ונרצה לבחור משתמש שאותו נתקוף.

<u>שלב 2: הקמת רשת Wifi AP מזויפת</u>

בשלב שני נרצה לבנות ולהקים את הרשת שלנו ובעצם ליצור AP בעל אותו שם SSID לרשת המקורית. אפשר להשתמש בכל מכשיר שקיים בו רכיב Wifi כמו סמארטפונים, מחשבים ראוטרים וכו. יכול להיות גם שנרצה להשתמש במכשירים מגדילי טווח קליטה הנקראים Wifi Pineapple. משתמשים המחוברים אל הרשת אינם יודעים לזהות האם הרשת הנ"ל היא המקורית או המזוייפת.

<u>שלב 3: חיבור משתמשים אל הרשת המזוייפת</u>

בשלב השלישי נרצה לחבר אל הרשת המזוייפת שייצרנו משתמשים. נרצה לגרום למשתמשים להתנתק מהרשת המקורית, לייצר עוצמת שידור גבוהה של הרשת המזוייפת וקרובה אל המשתמשים למטרת התקיפה, מה שיגרום למשתמשים להתחבר בחיבור מחדש אל הרשת בעלת העצימות הגבוהה ביותר, ולכן אם הרשת המזוייפת תהיה החזקה ביותר המשתמשים יתחברו אליה. הניתוק נעשה בעזרת שליחת פקטת deauth שגורמת למשתמשים להתנתק מהרשת המקורית. פקטה של ניתוק לקוח מרשת לא דורשת שום אימות, ולכן כל אחד יכול לנתק כל אחד מהרשת בקלות, רק צריך לזייף את הפקטה כך שתראה כאילו הsource הוא הAP.

<u>שלב 4: יצירת captive portal מזוייף</u>

לרוב, לפני שמתחברים לרשתות Wifi במקומות ציבורים מובלים אל captive portal שבו נצרך למשל לאשר הגדרות שימוש או לשלוח מידע מסויים וכו. בשלב הרביעי נרצה לשלוח את המשתמשים שלנו אל captive portal שיהיה דומה לרשת המקורית, שבו הם יצטרכו למסור מידע אותו נרצה לגנוב. באותו אופן, במידה ונרצה לתקוף משתמש שמחובר לרשת מוגנת, נוכל בדרך זו לקבל את הסיסמה אל הרשת המוגנת.

שלב 5: גניבת מידע

לאחר שמשתמשים התחברו אל הרשת המזוייפת שיצרנו, אנחנו יכולים בעזרת מגוון כלים לשלוט ולגשת למידע שעובר בינם לבין האינטרנט ולגנוב להם סיסמאות כניסה, כרטיס אשראי, פרטים אישיים וכו'.

נזק:

פוטנציאל הנזק הוא עצום שכן לאחר מימוש התקיפה התוקף בעצם יושב על הקו שבין המשתמש לרשת האינטרנט ולמעשה יש לו גישה מלאה לכל התעבורה העוברת שם. להלן מספר אופציות תקיפה שניתן לעשות לאחר מימוש evil twin.

1. גניבת סיסמאות בעזרת הפניית המשתמשים לאתרי אינטרנט שונים כך שיצטרכו להזין סיסמה לאתר כלשהו (captive portal).
2. הפניה לאתר המכיל קוד זדוני שינסה לנצל חולשות בדפדפנים ויוכל להתקין על מחשב המשתמשים וירוסים ותולעים.
3. כאשר המשתמש מתחבר לאתר שלישי (שרת) כמו ארגון פנימי או אתר אותו הוא מנהל נוכל לפרוץ לארגון ולמידע שבו.
4. ביצוע sniffing - האזנה על התקשורת העוברת בין המשתמש לרשת האינטרנט וגניבת מידע רגיש.

הגנות נגד המתקפה:

מתקפת evil twin יכולה להיות קשה לזיהוי במיוחד כאשר מתחברים לרשת Wifi ציבורית, איך ישנם מספר דברים שניתן לעשות בנידון.

החלק החשוב ביותר בהגנה מפני מתקפות סייבר הוא מודעות. כאשר אדם מודע לסכנות התקיפה הקיימות באינטרנט הוא ניזהר יותר משיתוף מידע ומשאבים. בנוסף כאשר אנחנו מחוברים ברשת ציבורית צריך לא לשתף מידע רגיש ולא להתחבר לחשבונות אישיים. ניתן לבדוק שאנחנו מחוברים ברשת הביתית שלנו אל הרשת המקורית ולבטל את החיבור האוטומטי במכשיר. ניתן גם להשתמש בתעבורת VPN מוצפנת ע"י כך שה VPN מצפין את המידע לפני שתוקפים יכולים לראות אותו, לא משנה באיזה רשת גולשים.

ישנם שיטות הגנה חזקות יותר כמו WifiHop, כלי של המשתמש שעוזר לזהות את הAP. אסטרטגיית זיהוי הנקראת רצועת הקשר המגבילה שמאשרת AP לפי מיקום ועוד.

מימוש המתקפה:

את המתקפה מימשנו בשפת python ובעזרת הסיפריה scapy. מצורף דו"ח וסרטון המדגימים את מימוש התקיפה.

ניתן לראות את הקודים והקבצים הרלוונטיים בגיט בכתובת:
https://github.com/Harel-ezra/Evil-Twin-Attack

סיכום:

לסיכום, בפרויקט זה הצגנו את תקיפת התאום הרשע - evil twin, יצרנו רשת Wifi מזויפת וגרמנו למשתמש להתחבר אליה ובכך יצרנו גישה אל התעבורה בינו לבין רשת האינטרנט, וכך למעשה ניתן לגנוב מידע רגיש. במימוש שלנו הוא הופנה ישר אל captive portal המבקש ממנו מידע אישי.

מקורות:

https://link.springer.com/content/pdf/10.1007/978-3-642-23822-2_2.pdf

https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.172.7083&rep=rep1&type=pdf

https://dl.acm.org/doi/abs/10.1145/2642687.2642691

https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.139.3736&rep=rep1&type=pdf

https://www.kaspersky.com/resource-center/preemptive-safety/evil-twin-attacks

https://www.pandasecurity.com/en/mediacenter/security/what-is-an-evil-twin-attack/

https://www.ericgoldman.name/en/2009/evil-twin-attack-demonstration/