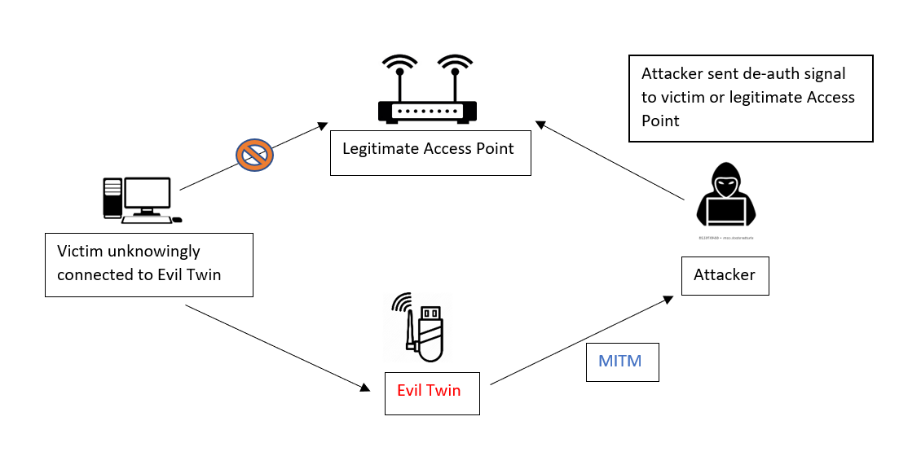
בס"

מסמך יזום

**נושא**

פיתוח ובניית מערכת התקפת Evil twin על מנת להשיג פרטי אשראי כאשר לקוח מתחבר לרשת WIFI ציבורית ברשות שדות בתעופה.



**מוטיבציה**

כיום רשתות WIFI ציבוריות פרוסות כמעט בכל מקום , בין אם בבתי קפה , אוניברסיטאות קניונים בתי חולים שדה תעופה וכו' , כאשר הצורך הבסיסי הוא גלישת אינטרנט . בעידן של היום הצורך ב-WIFI גדול , כל האנשים מחפשים בכל מקום אפשרי חיבור לWIFI בכדי לשתף ברשתות החברתיות , או בכדי להתכתב באפליקצייתwhatsapp , מבלי לבדוק או לדעת האם הרשת הינה רשת תקינה או רשת מזויפת.

כלונו יודעים כי יש כמה רשתות WIFI אשר מציעות ללקוחות אפשרות של גלישה ברשת שלהם בתשלום עבור הגלישה , ולכן צריך להכניס פרטי תשלום בכדי לבצע רכישה , לא כולם יודעים האם בטוח לרכוש או להכניס פרטי אשראי כיוון שיש המון חברות שמציעות רכישה אינטרנטית , כגון ASOS , eBay , אשר הינם חברות בטוחות לרכישה .

הסיבה שבחרנו בתקיפת רשת WLAN היא מפני שזו דרך תקשורת אשר ניתן דרכה לאתר את תעבורת הרשת , וכך להשיג מידע לגבי משתמשים , ובכך לתקוף את אותם המשתמשים.

**שלבי המתקפה**

* סריקת הרשתות הזמינות
* בחירת הרשת אותה נרצה לזייף
* לבדוק מי הם הלקוחות אשר מחוברים לאותה הרשת
* התקפת ביטול האימות (Deauthentication attack) ובכך להפיל את המכשיר שאותו נרצה לתקוף
* יצירת נקודת גישה מזויפת (FakeAP) שמחקה את הרשת המקורית
* נוצר שרת DHCP ב - FakeAP
* נוצר שרת DNS אשר מפנה את כל הבקשות למארח
* web server עם הממשק שנבחר מושק
* הלקוח מתחבר ל- FakeAP ומנתב מחדש לאתר הזדוני
* הלקוח מזין את פרטי האשראי שלו בכדי לרכוש חבילת אינטרנט , והנתונים נשמרים ב-DB

**שיטת הגנה**

* בכדי להגן על המשתמש קצה , אנחנו נפעיל בדיקה אם המשתמש מקבל המון פאקטות סימן לתקיפת Deauthentication attack . המשתמש יקבל התראה כאשר הוא מותקף.

**כלים**

* [Kali Linux](https://rootsh3ll.com/rwsps-installing-and-configuring-kali-linux-ch1pt2/)
* scapy
* dnsmasq
* hostapd
* Python3
* 2 כרטיס רשת

**מקורות**

* <https://www.thepythoncode.com/code/building-wifi-scanner-in-python-scapy>
* <https://www.thepythoncode.com/article/building-wifi-scanner-in-python-scapy>
* <https://www.digitalwhisper.co.il/files/Zines/0x22/DW34-4-EvilTwinAttacks.pdf>
* <https://rootsh3ll.com/evil-twin-attack/>
* <https://duthcode.com/Blog/blogPostContent.php?post=deauthentication-attack-using-kali-linux-18>
* <https://www.pentesteracademy.com/course?id=14>