מסמך ייזום

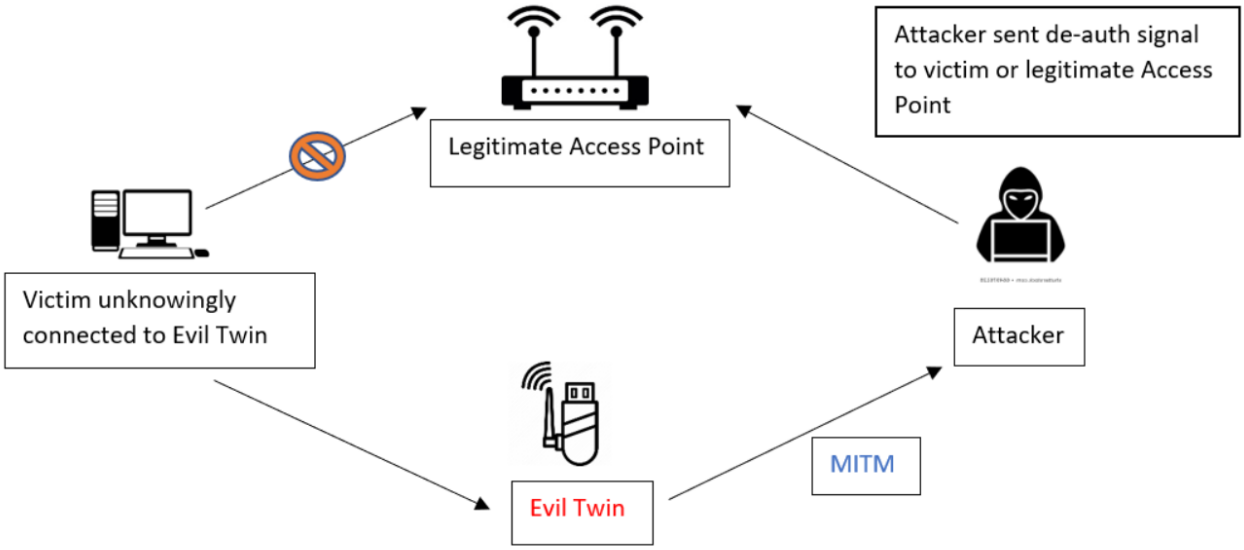
שמות המגישים	
שם ומשפחה	**ת.ז.**
דניאל ספריגין	207682493
אלי חיימוב	308019306

תוכן עניינים

רקע

<u>תאום מרושע:</u>

תאום רע (Evil Twin) היא מתקפה בה התוקפים מגדירים את המכשיר או המערכת שלהם כנקודת גישה תאומה או דומה ומעבירים את הקורבנות להתחבר דרך נקודת גישה מזויפת זו. כאשר הקורבן מחובר, ההאקר/ התוקף יכול לרחרח את הרשת, לתפוס את התקשורת ולעשות ניסיון נוסף להתקפות כמו: ביטול אימות ברשת אלחוטית (Wi-Fi Deauthentication attack), אדם בתווך (Man in the middle), חטיפת שיחה (session hijacking), התקפות DNS או דיוג (phishing). ניתן להגן על המשתמשים והעובדים מפני התקפות כאלה על ידי חיבור כל מחשבי הלקוח לנקודות גישה רשמיות עם פרטים מאומתים ויישום טכניקות הצפנה בערוץ התקשורת.



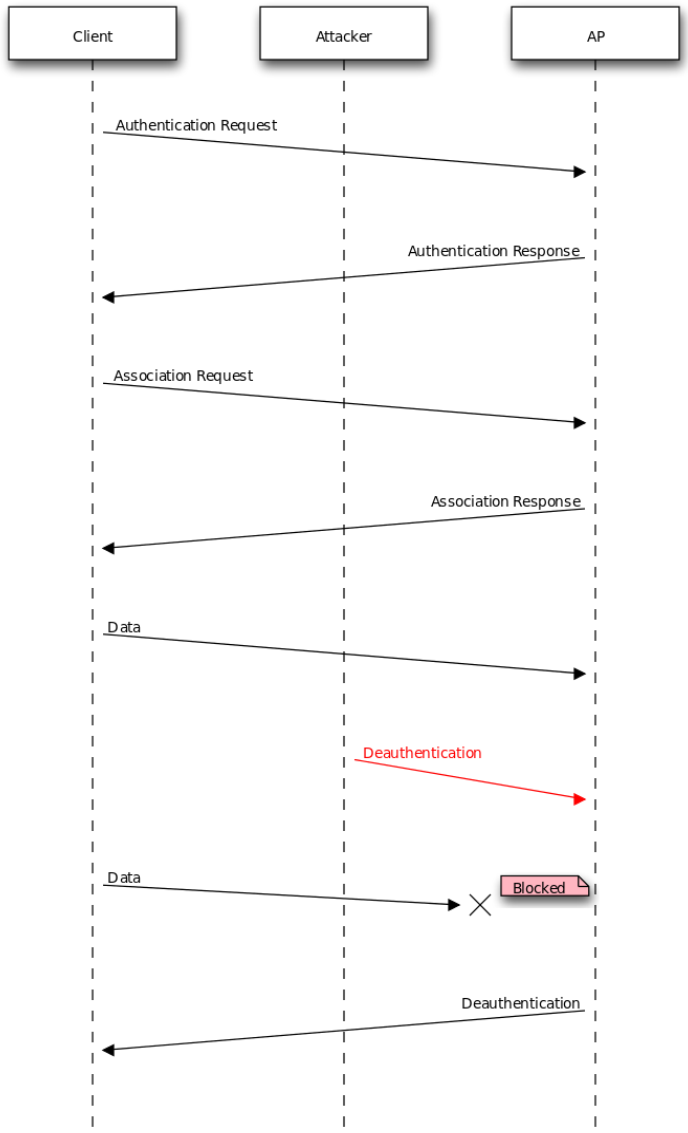
<u>התקפת ביטול אימות ברשת אלחוטית:</u>

התקפת ביטול אימות ברשת אלחוטית, **Wi-Fi Deauthentication Attack**, נחשבת להתקפת מניעת שירות ומטרתה לשבש את התקשורת בין משתמש הקצה לנקודת הגישה האלחוטית.

בהתקפה זו, שולח התוקף מנות (packets) לניתוק כל המשתמשים המחוברים אל נקודת הגישה האלחוטית ומנצל זאת למספר מטרות:

- זיהוי מזהה רשת (ESSID) מוסתר.
- לכידת לחיצות ידיים (HandShakes) בפרוטוקול <u>WPA</u>/<u>WPA2</u> ואילוץ המשתמש לבצע אימות מחדש.
- יצירת בקשות <u>ARP</u> זדוניות.

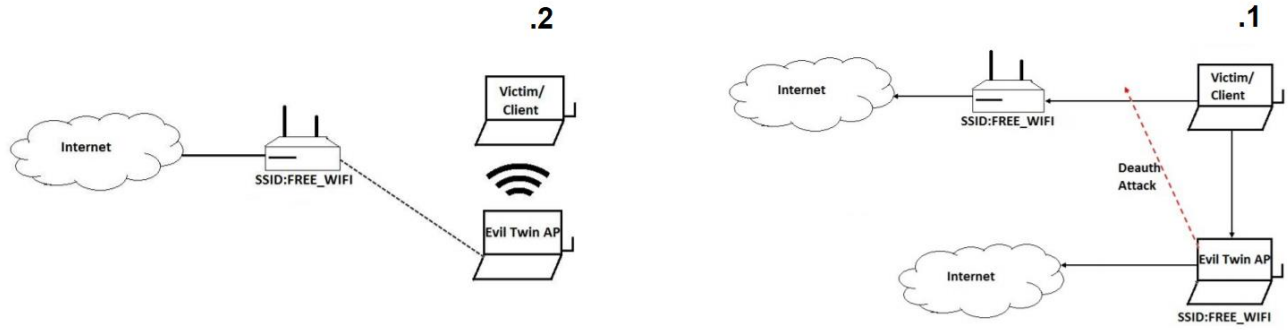
התקפה זו היא חסרת תועלת אם אין משתמשים המחוברים אל נקודת הגישה האלחוטית. לשם ביצוע התקפה זו על התוקף לדעת את כתובת ה-<u>MAC</u> של הקורבן ואת שם נקודת הגישה האלחוטית.



מוטיבציה

המוטיבציה שלנו בבחירת נושא זה היא להצליח לנתק אדם מהרשת האלחוטית אשר מחובר אליה (ע"י התקפת ביטול אימות ברשת אלחוטית) ולנסות לגרום לו לעבור לרשת הזהה שלנו (תאום מרושע).

מוטיבציה



תכנון וקביעת מטרות תקיפה

<u>תכנון:</u>
לאחר התעמקות בנושא הגענו למסקנה שהמשאבים הנצרכים לביצוע המשימה, הם:

<u>תוכנה:</u>
א) linux kali
ב) sniffing traffic

<u>חומרה:</u>
א) רכיב WIFI (מכשיר אלחוטי (ומנהל התקן) עם יכולות מצב צג).

<u>מטרות:</u>
1) התקפת מניעת שירות. כאשר אנו נתחבר לרשת, נעקוב אחר המשתמשים ברשת ונתקוף אותם על ידי שליחת פקטות לניתוק החיבור.
2) לחיצת היד בפרוטוקול <u>WPA</u>/<u>WPA2</u> מאפשרת ללקוח, שהפלנו את רשתו, בחירה אוטומטית של שיטת התקשרות עם הרשת הזדונית החדשה שיצרנו.
3) ניסיון להשגת נתונים רגישים/ פרטיים מצד הלקוח המחובר לרשת שלנו.

**הערות: במידה ולא נצליח להשיג את פרטיו של הלקוח המחובר לרשתנו, ננתק החיבור ונפסיק פעולתו.

כלים, אמצעים ושיטות
לכתיבת התוכנה: ● Python ● Scapy ניתן לאבחן תקשורת אלחוטית בעזרת מספר כלים: ● Aircrack-ng ● Scapy ● MDK3 ● Void11 ● Zulu WiFi Tool ● Airmon-ng, Airodump-ng, Airplay-ng

מקורות מידע
מתקפת evil twin: https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks) https://www.simplilearn.com/explain-types-of-wireless-attacks-tutorial https://www.thecybersploit.com/2019/12/Hacking-WPA2-Wi-Fi-password-using-Evil-Twin-Attack.html התקפת מניעת שירות: https://he.wikipedia.org/wiki/%D7%94%D7%AA%D7%A7%D7%A4%D7%AA_%D7%9E%D7%A0%D7%99%D7%A2%D7%AA_%D7%A9%D7%99%D7%A8%D7%95%D7%AA

התקפת ביטול אימות ברשת אלחוטית:

https://he.wikipedia.org/wiki/%D7%94%D7%AA%D7%A7%D7%A4%D7%AA_%D7%91%D7%99%D7%98%D7%95%D7%9C_%D7%90%D7%99%D7%9E%D7%95%D7%AA_%D7%91%D7%A8%D7%A9%D7%AA_%D7%90%D7%9C%D7%97%D7%95%D7%98%D7%99%D7%AA

הסבר על סוג ההתקפה וחיבור הלקוח לרשת:

https://www.youtube.com/watch?v=O1TpBjoiLe4

https://www.youtube.com/watch?v=Kb7qe5wlLKU