מסמך ייזום

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

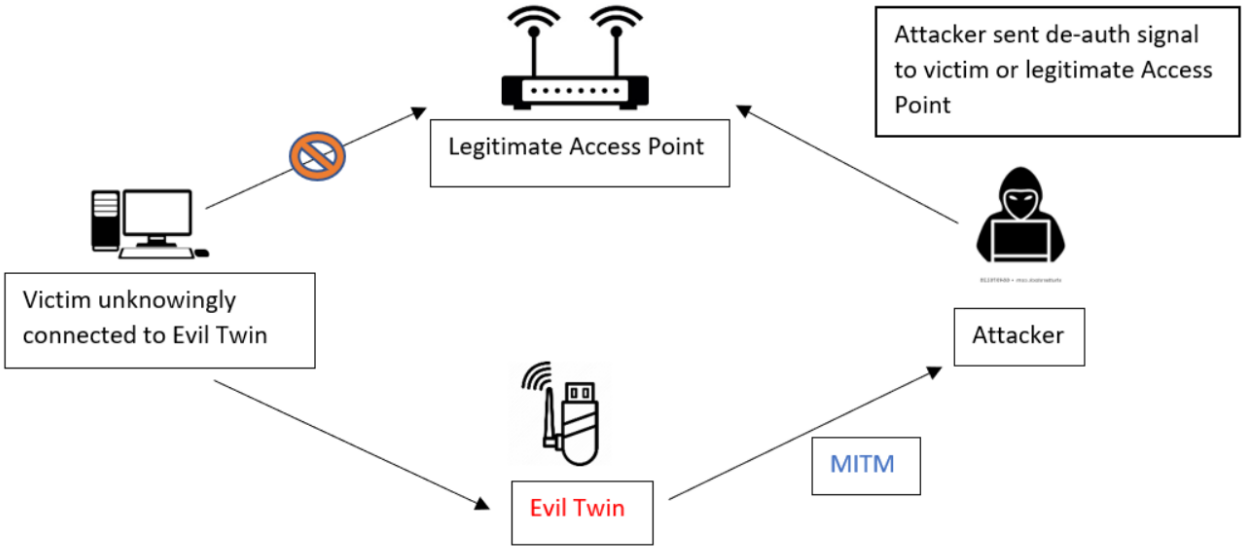
תוכן עניינים

רקע

<u>תאום מרושע:</u>

תאום מרושע (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.

בנוסף, מתקפה זו פועלת על ידי ניצול העובדה שרוב המחשבים והטלפונים יראו רק את "השם" או ה- ESSID של רשת אלחוטית. זה למעשה מקשה מאוד על הבחנה בין רשתות עם אותו שם וסוג של הצפנה. למעשה, לרשתות רבות יהיו כמה נקודות גישה מרחיבות רשת, וכולן משתמשות באותו שם כדי להרחיב את הגישה מבלי לבלבל משתמשים.
איך המתקפה עובדת? יוצרים נקודה חמה/גישה של Wi-Fi במכשיר (טלפון) וקוראים לה בדיוק כמו לרשת הביתית שלכם. נשים לב שקשה להבחין בהבדל בין שתי הרשתות או שמכשירכם עשוי פשוט לראות את שניהם באותה רשת. כלי לרחרוח רשת כמו Wigle Wifi באנדרואיד או Kismet , יכולים לראות בבירור את ההבדל בין הרשתות הללו, אך למשתמש הממוצע, הרשתות הללו ייראו אותו דבר.
זה עובד נהדר בשביל להערים על משתמש להתחבר אם יש לנו רשת עם אותו שם, אותה סיסמה ואותה הצפנה, אבל מה קורה אם אין בידינו את הסיסמא עדיין? לא נוכל ליצור רשת שתערים את המשתמש להתחבר אוטומטית, אך נוכל לנסות התקפה הנדסית חברתית (social engineering attack) כדי לנסות להכריח את המשתמש למסור לנו את הסיסמה על ידי הוצאתו מהרשת האמיתית.



שימוש במתקפת פורטל שבוי (Captive portal attack):

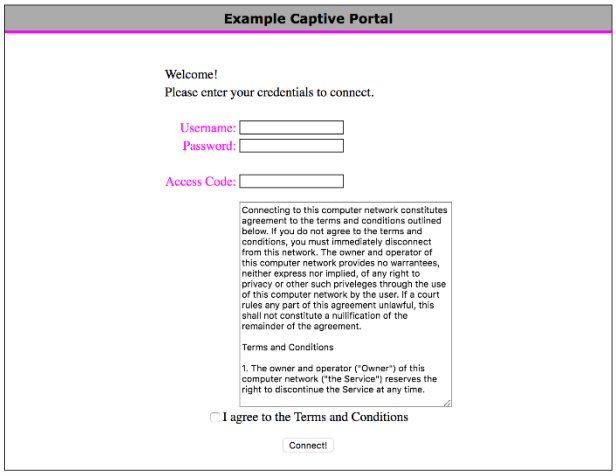
אחת המתקפות הנפוצות במתקפה "תאום מרושע" היא "פורטל שבוי".
במתקפה זו, משתמש התוקף במסגרת ההתקפה האלחוטית של Airgeddon כדי לנסות לאלץ את המשתמש להתחבר לרשת פתוחה בעל אותו השם כמו לרשת אשר עליה סומכים. פורטל שבוי דומה למסך שרואים כשאנשים מתחברים לרשת פתוחה בבית קפה, במטוס או בבית מלון. מסך זה, שמכיל תנאים והגבלות, הוא דבר שאנשים רגילים לראותו, והתוקף משתמש בזה לטובתו כדי ליצור דף דיוג (פישינג) שנראה כאילו הנתב מתעדכן.

הדרך בה התוקף מרמה את הקורבן לעשות זאת היא על ידי הצפת רשת המהימנה שלו במנות ביטול אימות (ע"י התקפת ביטול אימות ברשת אלחוטית), ובכך לא ניתן להתחבר לאינטרנט באופן רגיל. כאשר הקורבן מתמודד עם חיבור אינטרנט שמסרב להתחבר ולא יאפשר גישה לאינטרנט כלשהו, הקורבן יגלה רשת Wi-Fi פתוחה עם אותו שם לרשת שאליה לא הצליח להתחבר ויניח שזה מה שהיה קשור לבעיה.

עם התחברות לרשת, הקורבן יופנה לדף התחזות המסביר כי הנתב עודכן ודורש סיסמה כדי להמשיך. אם הקורבן אכן נמנע, הוא יזין את סיסמת הרשת, אך זה לא מסתיים בזאת. אם הקורבן מתעצבן מאי הנוחות הזו ומקליד את הסיסמה השגויה, על התוקף לוודא שיוכל להחזיר הודעת שגיאה מפני סיסמא שגויה בהשוואה לסיסמא הנכונה. לשם כך יש ללכד תחילה את לחיצות הידיים מהרשת, כך שיוכל לבדוק כל סיסמה שהקורבן נותן לו ולומר מתי אכן נכנסת הסיסמא הנכונה.

יישום פורטל שבוי: ניתוב מחדש של HTTP (HTTP redirect):

שיטה נפוצה היא להפנות את כל התעבורה באינטרנט לשרת אינטרנט, המחזיר הפניה מחדש של HTTP לפורטל שבוי. כאשר מכשיר מודרני המותאם לאינטרנט מתחבר לראשונה לרשת, הוא שולח בקשת HTTP לכתובת אתר לזיהוי שהוגדרה מראש על ידי הספק שלה ומצפה לקוד סטטוס HTTP של 200. אם המכשיר מקבל קוד סטטוס HTTP 200, היא מניחה שיש לה גישה לאינטרנט ללא הגבלה. ההנחיות לפורטל הכבוש מוצגות כאשר אתה מסוגל לתפעל את הודעת ה- HTTP הראשונה הזו כדי להחזיר קוד סטטוס HTTP של 302 (הפניה מחדש) לפורטל השבוי שתבחר.



שימוש בהתקפה הנדסית חברתית (Social engineering attack):

על מנת שהתקפה זו תעבוד, יש לעמוד בכמה דרישות מפתח. ראשית, התקפה זו דורשת מהמשתמש לעשות כמה דברים בורים. אם היעד שהתוקף בוחר ידוע כמנוסה בטכנולוגיה, יתכן שהתקפה הזו לא תעבוד. משתמש/קורבן מתקדם, או כל מי שיש לו הכשרה בנושא מודעות בנושא אבטחת סייבר, יבחין בהתקפה זו בעיצומה ואולי יהיה מודע לכך שמדובר בהתקפה קרובה יחסית. כנגד מטרה מוגנת היטב, ניתן לצפות שתוקף זה יתגלה ואפילו מיקומי לצורך מציאתו. שנית, על הקורבן להיות מאומת בהצלחה מרשתו, ולהיות מתוסכל מספיק כדי להצטרף לרשת פתוחה לא ידועה לחלוטין שרק הופיעה משום מקום ויש לה אותו שם של הרשת שהוא מכיר וסומך עליה. יתר על כן, ניסיון להתחבר לרשת זו (ב- macOS) אפילו מניב אזהרה כי בפעם האחרונה שהרשת הייתה מחוברת, היתה לה הצפנה מסוג אחר.
לבסוף, על הקורבן להזין את סיסמת הרשת לדף הדיוג/מתחזה (פישינג) אליו הוא מופנה ולראות עמוד/ הודעה מסויימת לאחר שהצטרף לרשת הפתוחה שיצר התוקף. יש הרבה רמזים שהקורבן יכול להבחין בהם ולהבין שהדף מוטעה וזו מתקפה, כגון: שפה לא נכונה, איות שגוי, מבנה מוזר וכדומה. מכיוון שדפי הנתב בדרך כלל נראים די מכוערים, יתכן ופרטים אלה לא יבלטו בפני רב הקורבנות שאינם בקיאים בנראות דף הניהול של הנתב שלהם.

דיוג (Phishing):

באבטחת מידע, דיוג או פישינג הוא ניסיון לגניבת מידע רגיש על ידי התחזות ברשת האינטרנט. המידע עשוי להיות, בין היתר, שמות משתמש וסיסמאות או פרטים פיננסיים. פישינג מתבצע באמצעות התחזות לגורם לגיטימי המעוניין לקבל את המידע. לרוב שולח הגורם המתחזה הודעת מסר מיידי או דואר אלקטרוני בשם אתר אינטרנט מוכר, בה מתבקש המשתמש ללחוץ על קישור .לאחר לחיצה על הקישור מגיע המשתמש לאתר מזויף בו הוא מתבקש להכניס את הפרטים אותם מבקש המתחזה לגנוב.

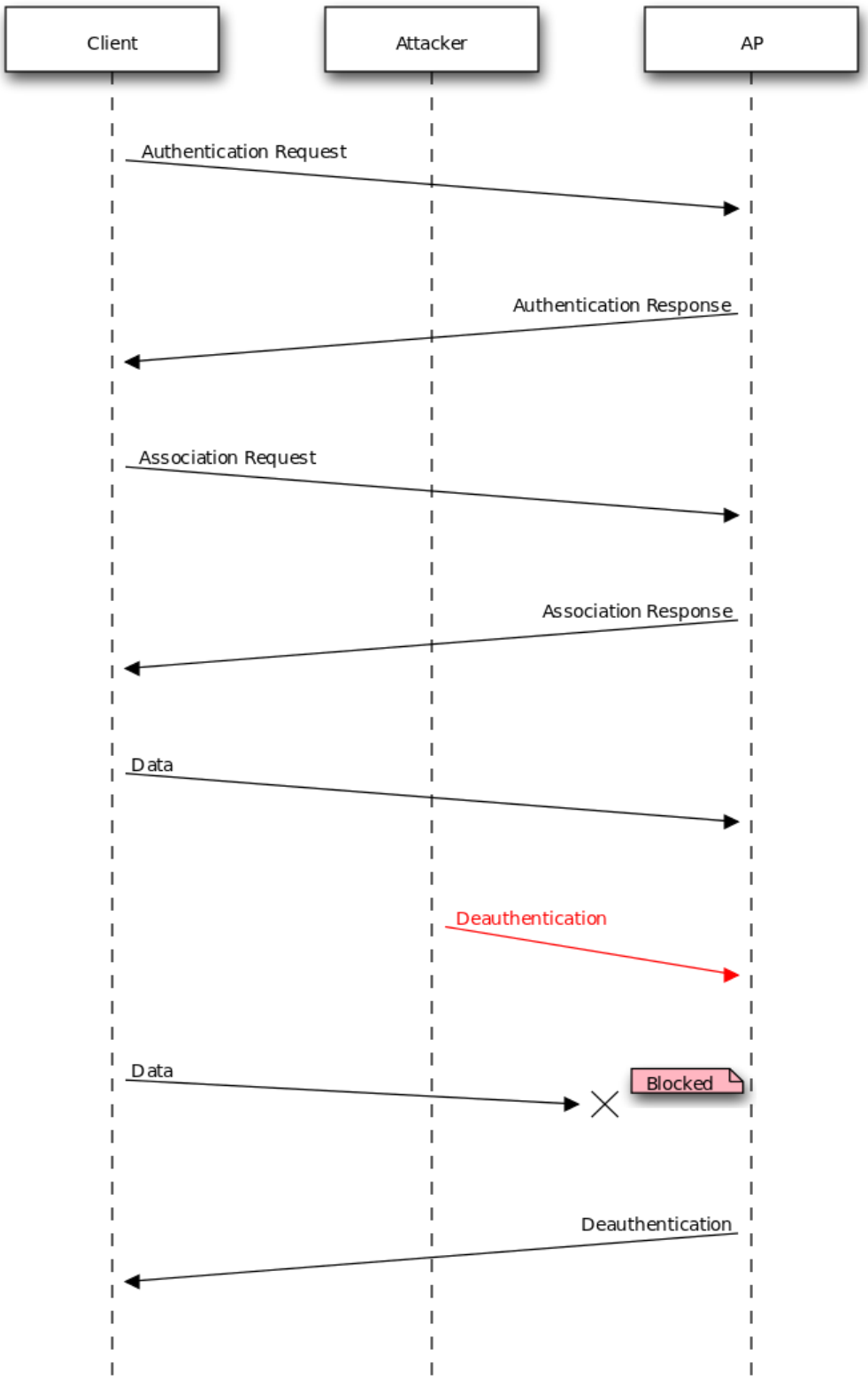
התקפת ביטול אימות ברשת אלחוטית (Wi-Fi Deauthentication Attack):

התקפת ביטול אימות ברשת אלחוטית, 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 WPA/WPA2 ואילוץ המשתמש לבצע אימות מחדש.
- יצירת בקשות ARP זדוניות.

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


Client
Attacker
AP
Authentication Request
Authentication Response
Association Request
Association Response
Data
Deauthentication
Data
Blocked
Deauthentication

מוטיבציה

המוטיבציה שלנו בבחירת נושא זה היא להצליח להשיג נתונים רגישים על הרשת האלחוטית של בית האירוח (לדוגמא: בית מלון/ אכסניה וכו') ושל הנתקף, כגון: פרטי התחברות לרשת האלחוטית של בית האירוח (סיסמא) ופרטי אמצעי תשלום (פרטי האשראי) לצורך האימות, של הנתקף, ע"י מתקפה נפוצה בשימוש "התאום המרושע", בשם: "פורטל לכוד".
בכדי להשיג נתונים אלו, מטרתינו העיקרית לנתק הנתקף מנקודת גישתו (רשת האלחוטית) של בית האירוח, אשר אליה מחובר (ע"י התקפת ביטול אימות ברשת אלחוטית) ולחברו לנקודת הגישה (רשת אלחוטית) המזויפת/זהה שיצרנו, כמתואר בשימוש "התאום המרושע".
ברגע שהנתקף יתחבר לרשתינו האלחוטית, יקושר מיידית לעמוד/אתר (כפי שמקובל בימינו בבתי האירוח השונים) שיצרנו, המשמש כמעין "צומת" (פישינג), למסירת הפרטים הרגישים ואימות ולהתחברות לרשתינו האלחוטית.

<u>הרחבת תיאור המוטיבציה:</u>

אורח מתחבר לרשת האלחוטית של בית אירוח ספציפי, התוקף מנתק גישתו לרשת זו וגורם לאורח להתחבר לרשת המזויפת שיצר. עם ניסיון נוסף להתחברותו לרשת האלחוטית, יועבר האורח מיידית לאתר (פישינג) אשר יידרש ממנו להזין את הפרטים הרגישים (פרטי האשראי איתם שריין את מקומו וסיסמת הרשת האלחוטית של בית אירוח זה) לצורך אימות והתחברות לרשת האלחוטית של התוקף. בסיום תהליך זה, יתחבר האורח לרשת זו, והתוקף יקבל את כל הפרטים הנדרשים, כמתואר במתקפת "פורטל לכוד".

<u>יישום המוטיבציה:</u>

<u>שלב 1. ביטול אימות ומניעת שירות:</u>
<u>סיבת הביצוע:</u> ניתוק הקורבן מהרשת אשר מחובר אליה בכדי לחברו לאחר מכן לרשת המזויפת של התוקף.
<u>אופן הביצוע:</u> הצפת רשת הקורבן במנות (פאקטות) ביטול אימות ע"י התקפת ביטול אימות ברשת אלחוטית, לניתוקו מהרשת.

<u>שלב 2. התאום המרושע:</u>
<u>סיבת הביצוע:</u> ליצירת נקודת גישה מזויפת וחיבורו של הקורבן לרשת זו.
<u>אופן הביצוע:</u> יצירת נקודת גישה של Wi-Fi במכשיר והענקת שם זהה לרשת, סיסמא ואותה הצפנה, במידת הצורך.
**כלי עזר לקבלת סיסמת הקורבן הוא: התקפה הנדסית חברתית.

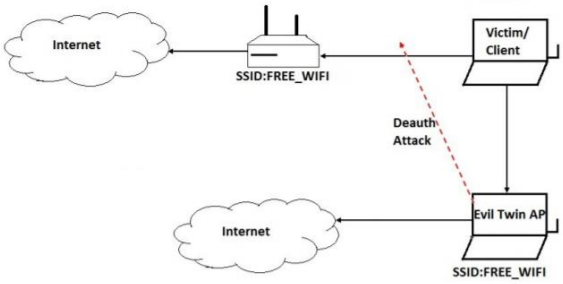
מוטיבציה

שלב 3. פורטל שבוי:
סיבת הביצוע: הכנסת הקורבן לאתר המתחזה (פישינג) והזנת הפרטים הרגישים.
אופן הביצוע: יצירת דף מתחזה (הקפדה ליצירת דף אמין) עם מילוי תוכן הפרטים הרגישים וניתוב מחדש של HTTP (תיאור היישום פורט ברקע מסמך הייזום) של הקורבן לעמוד/אתר המתחזה להזנת הפרטים.

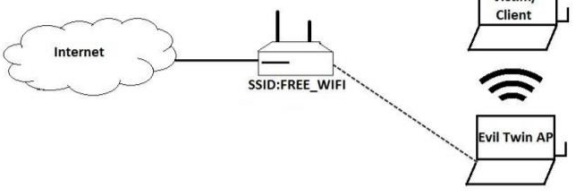
שלב 4. פישינג:
סיבת הביצוע: ניסיון לקבלת מידע רגיש מהאורח, כגון: סיסמת בית האירוח או פרטי האשראי של האורח (הקורבן).
אופן הביצוע: התחזות לדף/אתר בית האירוח לאימות סיסמא לקבלת הרשת האלחוטית ופרטי אמצעי תשלום האורח (הקורבן). נחלק הביצוע הנ"ל לשני מקרים:

1. במידה והקורבן מאזין סיסמא שגויה לרשת בית האירוח אשר קיבל/השיג או פרטי אשראי שגויים (כגון: מעט מספרים במספר האשראי), תצוץ הודעת שגיאה (השגת הסיסמא המקורית של רשת בית האירוח ע"י התקפה הנדסית חברתית) שתיתן לאורח אפשרות הזנה נוספת, וכך עד שיזין את פרטיו (או לכל הפחות את סיסמת הרשת האמיתית) ויעבור למקרה 2 או יתייאש ויצא.
2. במידה והזין הכל כנדרש, יחובר האורח לרשת המזויפת או יקבל הודעת שגיאה שרשת בית האירוח נפגעה מסיבות מסויימות וישר ינותק, כאשר התוקף כבר אוחז בפרטים לניצול/שימוש למטרות היעד השונות.

.1



.2



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 Wi-Fi / מתאם רשת אלחוטית (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 Wi-Fi Tool ● Kismet

- Airgeddon ,Airmon-ng, Airodump-ng, Airplay-ng

מקורות מידע

מתקפת "התאום המרושע" (Evil twin) ופורטל שבוי (Captive portal):

https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)

https://en.wikipedia.org/wiki/Captive_portal

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

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/

התקפת הנדסית חברתית (Social engineering attack):

https://he.wikipedia.org/wiki/%D7%94%D7%A0%D7%93%D7%A1%D7%94_%D7%97%D7%91%D7%A8%D7%AA%D7%99%D7%AA_(%D7%90%D7%91%D7%98%D7%97%D7%AA_%D7%9E%D7%99%D7%93%D7%A2)

דיוג (Phishing):

https://he.wikipedia.org/wiki/%D7%93%D7%99%D7%95%D7%92

התקפת מניעת שירות (Wi-Fi Deauthentication Attack):

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