קובץ סיכום – הגנת רשתות

# הקדמה

רשת אלחוטית מבוססת Wi-Fi הינה רשת המאפשרת לחבר בין ציוד קצה כגון: מחשבים ניידים, פלאפונים חכמים וכו' לבין רשת אחרת (קווית או אלחוטית) תוך שימוש בתווך אלחוטי.

במידה ומעוניינים לעבוד במצב Infrastructure נדרש להתקין Access-Point המשמש כנקודת המעבר בין הרשתות . תפקיד ה- Access-Point הינו לנהל את הרשת האלחוטית ע"י התווך האלחוטי בין הצרכנים השונים ולקשר בין תחנת הקצה (הצרכן) לרשת.

# תיאור ההתקפה

בדרך כלל, אלא אם הוגדר אחרת, Access-Point יפרסם את שם הרשת (SSID) ע"י שליחת Beacon מתאימה, כאשר ההודעה נשלחת כ-Broadcast עקב מאפייני התווך האלחוטי.

המשמעות היא שכל מי שנמצא בסביבת ה-AP מודע לקיום הרשת האלחוטית. תחנת הקצה תנסה להתחבר אוטומטית ל-AP המפרסם SSID מסוים במידה ובעבר המשתמש התחבר דרך תחנת הקצה לאותה רשת עם SSID זהה (בהנחה כי ההגדרה להתחברות אוטומטית לא השתנתה)

פה המקום לציין שתחנת הקצה תתחבר 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 תפעם שתחנת הקצה תזהה כי קיימת רשת Wi-Fi באזור עם אותו SSID, היא תנסה להתחבר אליו תוך כדי הפעלת מנגנון ההבטחה אשר הוגדר לרשת זו.

# כלים

* **Hostapd** - מאפשר פתיחת רשת אלחוטית (משנה mode של adapter ל master)
* **Dnsmasq** - DHCP & DNS Server (localhost port 53 and 67).  
  צריך שרת DHCP בשביל חלוקת אייפי למשתמשים ברשת.  
  צריך שרת DNS בשביל לקבל תשובות על כתובות אייפי או דומיינים.
* **Bash** - רוב ההתקפה שלנו נעשית בעזרת פקודות קצרות. כל חלק בעבודה, קיים לו סקריפט .sh בשבילו, וחסר רק להריץ אותו.
* **Python** - בעיקר לכתיבת הכלי עצמו, וכתיבת ה deauth שלנו
* **PHP, HTML**- בשביל אתר ה-Phishing

# מימוש ההתקפה

השלבים למימוש ההתקפה הם:

1. התוקף צריך לבחור ESSID (שם רשת) אותו הוא רוצה לתקוף.
2. הכלי יוצר AP זהה ב- ESSID לרשת המותקפת עם אות גבוה.
3. התוקף בוחר לנתק מהרשת המקורית את כלל המשתמשים וכך לגרום להם להתחבר באופן אוטומטי לרשת המזויפת שהוא פתח.
4. בעזרת שינוי בנתיבי ה- DNS ושימוש ב- Apache כלל המשתמשים המתחברים באופן אוטומטי לרשת המזויפת כאשר יגלשו באינטרנט יגיעו לאתר המבקש מהם סיסמא לרשת וכך התוקף מצליח לקבל את הסיסמא לרשת המקורית.
5. התוקף יכול להשתמש בסיסמא זו על מנת להתחבר לרשת המקורית ולנסות לפרוץ לקונפיגורציה של הראוטר.

# מושגים חשובים:

מדוע להשתמש ב 2 כרטיסי רשת?

אחד, בשביל Deauth. השני, בשביל להריץ AP.

כרטיס רשת לא יכול לעשות את שניהם ביחד.

(כי כשהוא במצב AP הוא ב Master Mode וכשהוא ב Deauth הוא במצב Monitor Mode).

# Deauthentication attack

התקפת ביטול אימות ברשת נחשבת להתקפת מניעת שירות ומטרתה לשבש את התקשורת בין משתמש הקצה לנקודת הגישה האלחוטית. בהתקפה זו, שולח התוקף חבילות לניתוק כל המשתמשים המחוברים אל נקודת הגישה האלחוטית ומנצל זאת למספר מטרות:

1. זיהוי מזהה רשת (ESSID) מוסתר.
2. לכידת לחיצות ידיים (HandShakes) בפרוטוקול WPA/WPA2  ואילוץ המשתמש לבצע אימות מחדש.
3. 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.

מושגים לחזור עליהם

* 802.11
* Beacon
* Response requests
* Addr1 addr2 addr3
* Frame