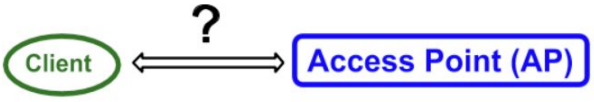
סדר פעולות עבור Evil twin

תום סואד

1. נרצה לסרוק את הרשת על מנת למצוא AP-ים בסביבה.
ניתן לעשות זאת בעזרת - airodump, או לעשות sniffer שמחפש Beacon packets (לכתוב קוד ב-scapy).

לאחר שמצאנו AP, נראה את השם שלו ואת ה-MAC address שלו -- הוא יהיה הtarget שעליו נבצע את ההתקפה.

2. נרצה לבדוק האם מחובר Client ל-AP. אם אין מישהו מחובר - אין טעם לתקוף את אותו AP.



נרצה "לתפוס" פאקטות שנשלחות באוויר ולפלטר אותן. נחפש פאקטה שבה ה-source או ה-destination הוא הכתובת MAC של ה-AP שמצאנו בהתחלה. בנוסף, נצטרך לבדוק שהפאקטה שתפסנו היא לא Beacon, נעשה זאת בעזרת בדיקה שהשליחה שלה לא הייתה ב- broadcast (כלומר, **לא** נרצה שבכתובת MAC יהיה כתוב *FF:FF:FF:FF:FF:FF*).
אם הצלחנו למצוא פאקטות כאלו - מצאנו Client, ואפילו יש לנו את הכתובת MAC שלו (לפי ה-source/destination של החבילה שמצאנו).

❖ המטרה הבאה היא לנתק את הקשר בין ה-AP ל-Client, כדי שבהמשך ה-Client יתחבר אלינו (ל-Evil twin).

3. נרצה להכין את ה"סביבה" שלנו - להרים את ה-Evil AP שלנו.

נשים לב שנרצה להרים Evil Twin AP עם אותו השם כמו ה-AP שמצאנו, כדי שה-Client יחשוב שאנחנו אותו אחד.

4. בשלב הבא נרצה לגרום לניתוק בין ה-AP ל-Client.

כדי לגרום לניתוק נצטרך לשלוח פאקטות מסוג - deauthentication. נרצה לדמות בקשת התנתקות אמיתית, לכן נבנה 2 הודעות כאלו, אחת "נשלחת" מה-AP ל-Client, והשנייה "נשלחת" מה-Client ל-AP. כך הש-AP יחשוב שה-Client

רוצה להתנתק, ולהיפך. את ההודעות האלו נשלח ב-loop, כדי שאם הם ינסו לעשות ׳התחברות מחדש׳, הם שוב יקבלו הודעת ניתוק מהצד השני, ולא יצליחו לבצע את ה׳חיבור מחדש׳.
בסופו של דבר, אנחנו סומכים על כך שה-Client יחשוב שיש משהו לא תקין עם ה-AP, ופשוט ינסה להתחבר לרשת שיש לה את אותו השם - שזה בעצם ה-ET. וכמובן שהוא יצליח 😈.
לאחר שה-Client מתחבר אלינו, אפשר להפסיק לשלוח את ההודעות ל-AP הטוב.

עוד דרך היא שניתן לעשות DoS attack ל-AP, ובעצם למנוע מה-Client גישה ל-AP.

❖ עבור השלבים עד עכשיו אנחנו צריכים 2 כרטיסי רשת.
<u>כרטיס 1</u> - עבור מציאת AP בסביבה (שלב 1), נעשה זאת על-ידי כך שנשים את כרטיס הרשת ב-monitor mode והוא יסרוק את הרשת. ועבור ניתוק הקשר בין הAP לClient (שלב 4).
<u>כרטיס 2</u> - עבור ה-Evil Twin שלנו.

5. ה-Evil Twin שלנו צריך לספק 3 דברים:
1). **DHCP server** - כאשר Client מתחבר, השרת הזה מביא לו הקצאה לכתובת IP, ואת כל הקונפיגורציות הדרושות. זה משהו שאנחנו צריכים להרים.
2). **DNS** - הוא ממיר לנו את ה-URL לכתובת IP המתאימות. במקרה של ההתקפה, אנחנו נרצה שהוא יוביל את ה-Client ל-web server שיכיל אך ורק דף נחיתה שאנחנו נבנה אותו, לא משנה איזו כתובת URL המשתמש מכניס.
3). **Web server** - זה גם משהו שאנחנו צריכים להרים, לדוגמא apache/apache2. אנחנו נרצה web server שלנו יכיל אך ורק דף נחיתה שאנחנו נבנה.

6. נרצה להשיג את הסיסמא של ה-AP הטוב מהדף נחיתה שלנו. לכן נרצה לדמות אתר אמיתי, לדוגמא אתר של LINKSYS , ולרשום שהראוטר צריך איפוס, וצריך לשים את הסיסמא כדי לאפס אותו. ולאחר שה-Client יכניס את הסיסמא, אנחנו נוכל לשמור אותה.
מכאן יש כמה אופציות -
- ניתן ״לשחרר״ את ה-Client, ובעצם יש לנו את הסיסמא של ה-AP. העיקר שאנחנו השגנו מידע 🙃.
- ניתן להתחבר ל-AP, כאילו אנחנו ה-Client, ואז להיות Man In The Middle. וככה ניתן לראות את כל התקשרות שעוברת בין ה-Client ל-AP. במקרה הזה יכול להיות לנו יותר מידע 😇.
- ועוד מלאן אופציות - just google it.

בהצלחה!! 🤓