23 פרויקט: חטיפת חבילות ARP עם WireShark

אנחנו הולכים להסתכל על תעבורת רשת חיה עם WireShark ולראות אם אנחנו יכולים לתפוס בקשות ARP ותגובות.

WireShark הוא כלי מצוין לחטיפת חבילות רשת. הוא נותן לך דרך לעקוב אחרי חבילות שמח crosses את הרשת המקומית.

נקים פילטר ב-WireShark כך שנחפש רק חבילות ARP שמגיעות אל וממכונות ספציפיות שלנו, כך שלא נצטרך לחפש מחט בערימת שחת.

23.1 מה ליצור

מסמך שיכלול 4 דברים:

- את כתובת ה-MAC של החיבור הפעיל שלך.
- את כתובת ה-IP של החיבור הפעיל שלך.
- תפס צילום חבילה קריא לאדם של בקשת ARP.
- תפס צילום חבילה קריא לאדם של תגובת ARP.

פרטים בהמשך!

23.2 שלב אחרי שלב

הנה מה שאנחנו נעשה:

חפש את כתובת ה-MAC שלך
המחשב שלך עשוי להכיל מספר ממשקי Ethernet (למשל אחד עבור WiFi ואחד עבור חיבור חוטי – חיבור ה-Ethernet בצד).
מאחר שכנראה אתה משתמש כרגע ב-WiFi, חפש את כתובת ה-MAC עבור ממשק ה-WiFi שלך. (ייתכן שתצטרך לחפש באינטרנט איך לעשות זאת.)
בשני שלבים אלו, תוכל למצוא את המידע עם הפקודה הזו ב-Unix:

bash
Copy code
```
ifconfig
```

ובפקודה הזו ב-Windows:

bash
Copy code
```
ipconfig
```

חפש את כתובת ה-IP שלך
שוב, אנחנו רוצים את כתובת ה-IP של ממשק הרשת הפעיל שלך, כנראה מכשיר ה-WiFi שלך.

השק את WireShark
בזמן הפעלת WireShark לראשונה, הקם את WireShark כך שיתבונן במכשיר ה-Ethernet הפעיל שלך. ב-Linux, זה עשוי להיות wlan0, ב-Mac זה יכול להיות en0, וב-Windows זה כנראה פשוט Wi-Fi.

הקם פילטר הצגה ב-WireShark כך שיחפש רק חבילות ARP שמגיעות אל וממכונתך. הקלד את זה בשדה הפילטר בחלק העליון של החלון, ממש מתחת לכפתור הסנפיר הכחול:

bash
Copy code
```
[arp and eth.addr==[your MAC address
```

אל תשכח ללחוץ על ENTER אחרי הקלדת הפילטר.

התחל בלכידת החבילות על ידי לחיצה על כפתור הסנפיר הכחול.

מצא יותר כתובות IP על תת-ההרשת שלך
לסעיף הזה לא משנה אם יש מחשב בכתובת ה-IP המרוחקת, אך זה נחמד אם יש. עקוב אחרי יומן WireShark במשך זמן מה כדי לראות אילו כתובות IP נוספות פעילות על הרשת המקומית שלך.

ה-IP שלך בשילוב עם מסכת תת-ההרשת הוא מספר תת-ההרשת שלך. נסה לשים מספרים שונים עבור חלק ה-host. נסה את שער ברירת המחדל שלך (חפש באינטרנט איך למצוא את שער ברירת המחדל במערכת ההפעלה שלך).

בפקודה, פינג לכתובת IP אחרת ברשת המקומית שלך:

bash
Copy code
```
[ping [IP address
```

(לחץ CONTROL-C כדי להפסיק את הפינג.)

בפינג הראשון, האם ראית חבילות ARP עוברות ב-WireShark? אם לא, נסה כתובת IP אחרת בתת-ההרשת, כפי שצויין למעלה.

לא משנה כמה פינגים תשלח, תראה רק תגובה אחת של ARP. (תראה בקשה אחת לכל פינג אם לא קיבלת תגובות!) זאת מכיוון שאחרי התגובה הראשונה, המחשב שלך שומר את תגובת ה-ARP במטמון ולא צריך לשלוח אותן שוב!

אחרי דקה או חמש, המחשב שלך אמור לפוג את הרשומה במטמון ה-ARP, ותקבל עוד חילופי ARP אם תפינג את אותה כתובת IP שוב.

רשום את הבקשה והתגובה
בקו הזמן, בקשת ה-ARP תיראה משהו כזה (עם כתובות IP שונות כמובן):

Copy code
```
ARP 60 מי יש לו 192.168.1.230? אמר ל-192.168.1.1
```

אם הכל הלך כשורה, תראה תגובה כזו:

bash
Copy code
```
192.168.1.230 ARP 42 נמצא ב-ac:d1:b8:df:20:85
```

[אם אינך רואה כלום, נסה לשנות את פילטר ההצגה כך שיחפש רק "arp". עקוב אחרי היומן במשך זמן מה כדי לראות אם אתה רואה זוג בקשה/תגובה.]

לחץ על הבקשה וצפה בפרטים בתחתית המסך. פתח את פאנל ה-"Address Resolution Protocol (request)".

לחץ עם הכפתור הימני על כל שורה בפאנל הזה ובחר "Copy->All Visible Items".

הנה בקשה לדוגמה (מועתקת לאורך שורות):

less
Copy code
```
[...] Frame 221567: 42 bytes on wire (336 bits), 42 bytes captured
[...] Ethernet II, Src: HonHaiPr_df:20:85 (ac:d1:b8:df:20:85), Dst:
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HonHaiPr_df:20:85 (ac:d1:b8:df:20:85)
    Sender IP address: 192.168.1.230
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.148
```

לחץ על התגובה בקו הזמן. העתק את המידע של התגובה באותו אופן.

הנה תגובה לדוגמה (מועתקת לאורך שורות):

less
Copy code
```
[...] Frame 221572: 42 bytes on wire (336 bits), 42 bytes captured
[...] Ethernet II, Src: Apple_63:3c:ef (8c:85:90:63:3c:ef), Dst:
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
```

```
                                        (Opcode: reply (2
   (Sender MAC address: Apple_63:3c:ef (8c:85:90:63:3c:ef
                        Sender IP address: 192.168.1.148
(Target MAC address: HonHaiPr_df:20:85 (ac:d1:b8:df:20:85
                        Target IP address: 192.168.1.230
```