ARP Spoofer

הקדמה – מה זה ARP Spoofing

בכל מחשב יש טבלאות של פרוטוקול ARP, אשר ממפות בין כתובות IP ל-MAC של מחשבים שנמצאים באותה רשת. כל רשומה כזאת נשמרת לזמן מוגבל, בדרך כלל כמה שניות עד דקה.

תקיפה זו היא מימוש ל- ARP poisoning, שבה התוקף מרעיל את הטבלה הנ"ל של הקורבן וגורם לו לחשוב שמחשב מסוים הוא מחשב אחר, או בכלל מחשב שלא קיים ברשת.

המתקפה מנצלת את העובדה שפרוטוקול ARP הוא **מאוד** פושט ולא מצבע **שום** בדיקות תקינות ואמינות – התוקף שולח כל מספר שניות (אשר קטן מהזמן שאחריו שהרשומה תימחק) הודעה מסוג תגובת ARP לקורבן ושמה כתוב שהוא (=התוקף) מחשב אחר (לדוגמא - הנתב). הקורבן בתמימותו מכניס את התשובה שקיבל לטבלה שלו – וזהו.

מהמימוש המתבקש של תקיפה זו, אפשר לממש Man In The Middle – MITM[1], וכך להתחזות ל-gateway ובכך להעביר את כל המידע בין הקורבן לשאר האינטרנט דרך התוקף. והתוקף יכול לעשות מה שהוא רוצה עם מידע זה.

בתרגיל זה לא מימשנו MITM, אלה רק את הרעלה של הטבלאות.

אופן הפעולה

ראשית, השתמשנו בספרייה `argparse` על מנת לקלוט ולפרסר את פרמטרי השורה, ואת זה ניתן למצוא בפונק' `get_args()`.[2]

לאחר מכן, אתחלנו אובייקט חדש שיצרנו, אשר מנהל את ההתקפה, ואליו שלחנו את כל הפרמטרים שהמשתמש הכניס. מכיוון שחלקם אופציונליים ואינם חובה, יכול להיות שאותם פרמטרי שורה יהיו `None` – טיפלנו בכך בבנאי האובייקט.[3]

הפונק' `start()`[4] מבצעת את התקיפה בלולאה אין סופית ומדפיסה למשתמש את סטטוס הפעולה.

אם המשתמש בחר באפשרות Full Duplex[5] – אזי ישלחו שני הודעות *הרעלה* – אחת לקורבן, ואחת למי שהתוקף בחר להתחזות אליו.

אחרת – תשלח הודעת *הרעלה* רק לקורבן.

- בהודעת הרעלה שנשלחת לקורבן[6]:

  אנחנו מתחזים למחשב שהמשתמש בחר, זאת אומרת – אומרים שכתובת ה-MAC של במחשב שכתובת ה- IP שלו מופיע בפרמטר `src` – היא כתובת ה-MAC של התוקף.

- בהודעת הרעלה שנשלחת למחשב שכתובת ה- IP שלו מופיע בפרמטר `src`[7]:

  אנחנו מתחזים לקורבן, זאת אומרת – אומרים שכתובת ה-MAC של הקורבן – היא כתובת ה-MAC של התוקף.

---

[1] כדי להצליח לעשות תקיפה זו (MITM) צריך לעשות 2 דברים:
a. להרעיל את טבלת ה-ARP של ה-gateway ולהגיד שכתובת ה-MAC של הקורבן היא ה-MAC של התוקף.
b. לאפשר תקשורת בין הקורבן לעולם האמיתי, כלומר: כל הודעה שהקורבן רוצה לשלוח ל-gateway – אז באמת להעביר אותה אליו, וכנ"ל הפוך.

[2] שורות 13-28

[3] שורות 36-55

[4] שורות 68-86

[5] הבדיקה לכך – נעשית בשורה 77

[6] הבנייה של הודעה זו נעשה ע"י הפונק' send_fake_arp_replay, שורות 95-109

[7] הבנייה של הודעה זו נעשה ע"י הפונק' send_fake_arp_replay, שורות 95-109

צילומי מסך

ראשית, כדי להוכיח שאכן התקיפה צלחה – כתובת ה-MAC של המחשב שלי היא 50-9A-4C-09-66-58 כפי שניתן לראות בצילום מטה:

```
C:\Users\shachar>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-C1IIBNN
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter ⎫⎫ Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (5) I219-LM
   Physical Address. . . . . . . . . : 50-9A-4C-09-66-28
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f134:c142:6d1:36e2%5(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.30(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : ??? 07 ?????? 2020 18:08:30
   Lease Expires . . . . . . . . . . : ??? 07 ?????? 2020 21:34:26
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 72391244
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-2C-D8-1B-50-9A-4C-09-66-28
   DNS Servers . . . . . . . . . . . : 213.57.22.5
                                       213.57.2.5
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

צילום מ-wireshark (במכונה התוקפת) שמוכיח ששני הודעת *ההרעלה* הצליחו:

2.946746	XiaomiCo_c9:bb:49	Dell_09:66:28	ARP	60	192.168.1.29 is at 0c:98:38:c9:bb:49
2.951545	AskeyCom_2e:59:28	Dell_09:66:28	ARP	60	192.168.1.1 is at 7c:b7:33:2e:59:28
3.009634	Dell_09:66:28	AskeyCom_2e:59:28	ARP	42	192.168.1.29 is at 50:9a:4c:09:66:28 (duplicate use of 192.168.1.1 detected!)
3.013221	AskeyCom_2e:59:28	Dell_09:66:28	ARP	60	192.168.1.1 is at 7c:b7:33:2e:59:28
3.151635	XiaomiCo_c9:bb:49	Dell_09:66:28	ARP	60	192.168.1.29 is at 0c:98:38:c9:bb:49
3.198290	Dell_09:66:28	XiaomiCo_c9:bb:49	ARP	42	192.168.1.1 is at 50:9a:4c:09:66:28 (duplicate use of 192.168.1.29 detected!)
6.222716	XiaomiCo_c9:bb:49	Dell_09:66:28	ARP	60	192.168.1.29 is at 0c:98:38:c9:bb:49
6.275268	Dell_09:66:28	AskeyCom_2e:59:28	ARP	42	192.168.1.29 is at 50:9a:4c:09:66:28 (duplicate use of 192.168.1.1 detected!)
6.278788	AskeyCom_2e:59:28	Dell_09:66:28	ARP	60	192.168.1.1 is at 7c:b7:33:2e:59:28
6.337531	Dell_09:66:28	XiaomiCo_c9:bb:49	ARP	42	192.168.1.1 is at 50:9a:4c:09:66:28 (duplicate use of 192.168.1.29 detected!)
9.402583	XiaomiCo_c9:bb:49	Dell_09:66:28	ARP	60	192.168.1.29 is at 0c:98:38:c9:bb:49
9.407698	Dell_09:66:28	AskeyCom_2e:59:28	ARP	42	192.168.1.29 is at 50:9a:4c:09:66:28 (duplicate use of 192.168.1.1 detected!)
9.411681	AskeyCom_2e:59:28	Dell_09:66:28	ARP	60	192.168.1.1 is at 7c:b7:33:2e:59:28
9.465043	Dell_09:66:28	XiaomiCo_c9:bb:49	ARP	42	192.168.1.1 is at 50:9a:4c:09:66:28 (duplicate use of 192.168.1.29 detected!)

באדום – הרעלה של הקורבן

בכתום – הרעלה של המחשב שכתובת ה- IP שלו מופיע בפרמטר `src`.

קצב ריענון טבלת המטמון של ARP בווינדוס ולינוקס

- **Unix:** נתחיל מהדבר הברור שכאשר ההודעה נשלחת אחת לשניה –התקיפה עובדת.

  לכן ניסינו לתת תחום גדול באופן יחסי – 100 שניות בין הרעלה להרעלה:

  ראינו בהתחלה שאכן זה אבל, אבל אחרי בערך דקה – האינטרנט חזר לעבוד.

  לכן הורדנו את זמן ההמתנה ל-50 שניות – ראינו כי התקיפה עובדת.

  העלנו את הdelay ל-70 שניות – התקיפה לא צלחה.

  הורדנו חזרה ל-60 – והתקיפה עבדה.

  מסקנה מתבקשת: זמן ריענון הטבלה של ARP ב-Unix עובד על כ-60 שניות.

  - חיפשנו בגוגל ומצאנו כי אכן הזמן בגרסה שלנו של unix זמן הרענון הוא אכן 60 שניות. את הפקודה שסיפרה לנו כך ואת הפלט שלה ניתן לראות בתמונה שלמטה:

```
root@kali:~# cat /proc/sys/net/ipv4/neigh/default/gc_stale_time
60
```

- **Windows:** נתחיל מהדבר הברור שכאשר ההודעה נשלחת אחת לשניה –התקיפה עובדת.

  לכן ניסינו לתת תחום גדול באופן יחסי – 100 שניות בין הרעלה להרעלה:

  ראינו בהתחלה שאכן זה אבל, אבל אחרי בערך דקה – האינטרנט חזר לעבוד.

  לכן הורדנו את זמן ההמתנה ל-50 שניות – ראינו כי התקיפה עדיין עובדת רק בשניות הראשונות.

  הורדנו עוד את ה-delay ל-20 שניות – והתקיפה עבדה.

  העלנו את הdelay חזרה ל-40 שניות – התקיפה לא צלחה.

  הורדנו חזרה ל-30 – והתקיפה עבדה.

  מסקנה מתבקשת: זמן ריענון הטבלה של ARP ב-Windows עומד על כ-30 שניות.

  - חיפשנו בגוגל ומצאנו כי אכן הזמן בגרסה שלנו של Windows זמן הרענון הוא מעוד קרוב ל-30 שניות. את הפקודה שסיפרה לנו כך ואת הפלט שלה ניתן לראות בתמונה שלמטה:

```
C:\Windows\system32>netsh interface ipv4 show interfaces

Idx     Met         MTU          State                Name
---  ----------  ----------  ------------  ---------------------------
  1          75  4294967295  connected     Loopback Pseudo-Interface 1
  5          35        1500  connected     ??Ethernet
  6          25        1500  connected     Npcap Loopback Adapter
 13          25        1500  connected     VirtualBox Host-Only Network
```

ואם נבחר בכרטיס ספציפי – נוכל לקבל עליו פרטים ובניהם, את הזמן שהרשומות בטבלה נכונות:

```
C:\Windows\system32>netsh interface ipv4 show interfaces 5

Interface ??Ethernet Parameters
----------------------------------------------
IfLuid                             : ethernet_32769
IfIndex                            : 5
State                              : connected
Metric                             : 35
Link MTU                           : 1500 bytes
Reachable Time                     : 29000 ms
Base Reachable Time                : 30000 ms
Retransmission Interval            : 1000 ms
DAD Transmits                      : 3
```