תרגיל arpspoof

אריאל בר כליפא 214181604

ידידיה מרשה 213661499

1. נבנה
2. עובד כנגד מכונת לינוקס וירטואלית (NAT אם משתמשים בוויפיי של המכון) וגם כנגד ווינדוס ב bridged adapter.
3. **בלינוקס:** יש משתנה הקרו **base_reachable_time** אשר שולט בזמן התקינות של כל כניסה בטבלת הARP כאשר הערך הדיפולטיבי שלו הוא 30 שניות.

```
┌──(kali㉿kali)-[~]
└─$ cat /proc/sys/net/ipv4/neigh/eth0/base_reachable_time
30
```

הזמן בפועל משתנה באופן אקראי בתלות במשתנה הנ"ל באופן הבא:

Base / 2 < timeout < 3*Base / 2

אצלינו בניסוי יצא 34 שניות בערך.

3	0.034122004	PcsCompu_7d:eb:6e	PcsCompu_a2:4f:4b	ARP	42	10.7.7.254 is at 08:00:27:7d:eb:6e
9	34.143004554	PcsCompu_a2:4f:4b	PcsCompu_7d:eb:6e	ARP	60	Who has 10.7.7.254? Tell 10.7.0.196

לכן המקסימום delay המומלץ ע"מ להבטיח שהtarget לא יבקש מהרשת את כתובת הMAC של הsrc הוא 14 שניות (עם טווח ביטחון של שניה אחת).

בווינדוס: התנהגות דומה. גם הערכים הדיפולטיבים למשתנים הנ"ל אותו הדבר.