המקרה המוזר של ה ping6 בשעת לילה

היי, שמי בוב ויש לי שאלה.

- לאחרונה למדתי על פרוטוקול ND שמשתמשים בו בעולם ה ipv6.
אחד מהדברים הנחמדים שיש בפרוטוקול הזה הוא שתי הודעות NS ו NA והייתי אומר שהתפקיד המקביל שלהם בעולם ה ipv4 הם ARP request ו ARP response בהתאמה.

- חשבתי שאם אוכל לשלוח לאליס הודעת NA שאומרת "היי, הכתובת ipv6 שלי נמצאת בכתובת הפיזית 13:33:33:33:33:37", אז מעתה כל הודעה שהיא תרצה לשלוח לי (אנחנו באותה רשת פיזית) תקבל את כתובת ה dst MAC הנ"ל, וההודעה שלה לא אמורה להגיע אלי.

כי זה מה שקרה ב ipv4 עם ARP spoofing, והייתי בטוח שזה גם מה שיקרה כאן.. אבל.. לא.

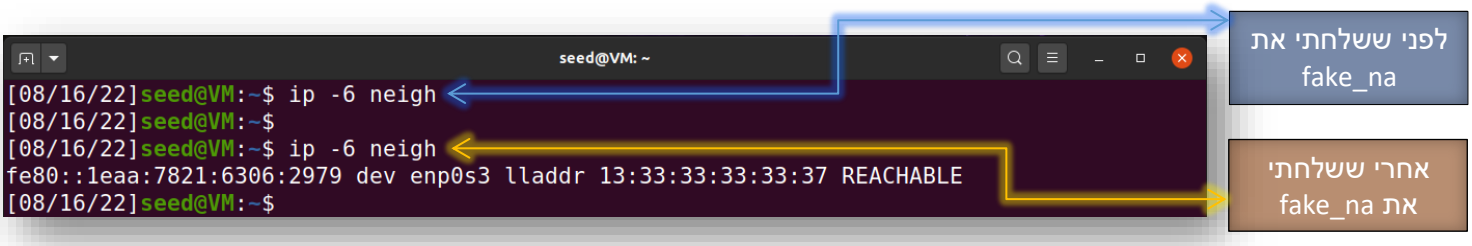
- לפני שאתחיל לתאר את מה שקרה, חשוב שתדעו שזה היה מצב הרשת:

- בנספחים בסוף המסמך צירפתי צילומי מסך של ifconfig מהמחשבים שלי ושל אליס.

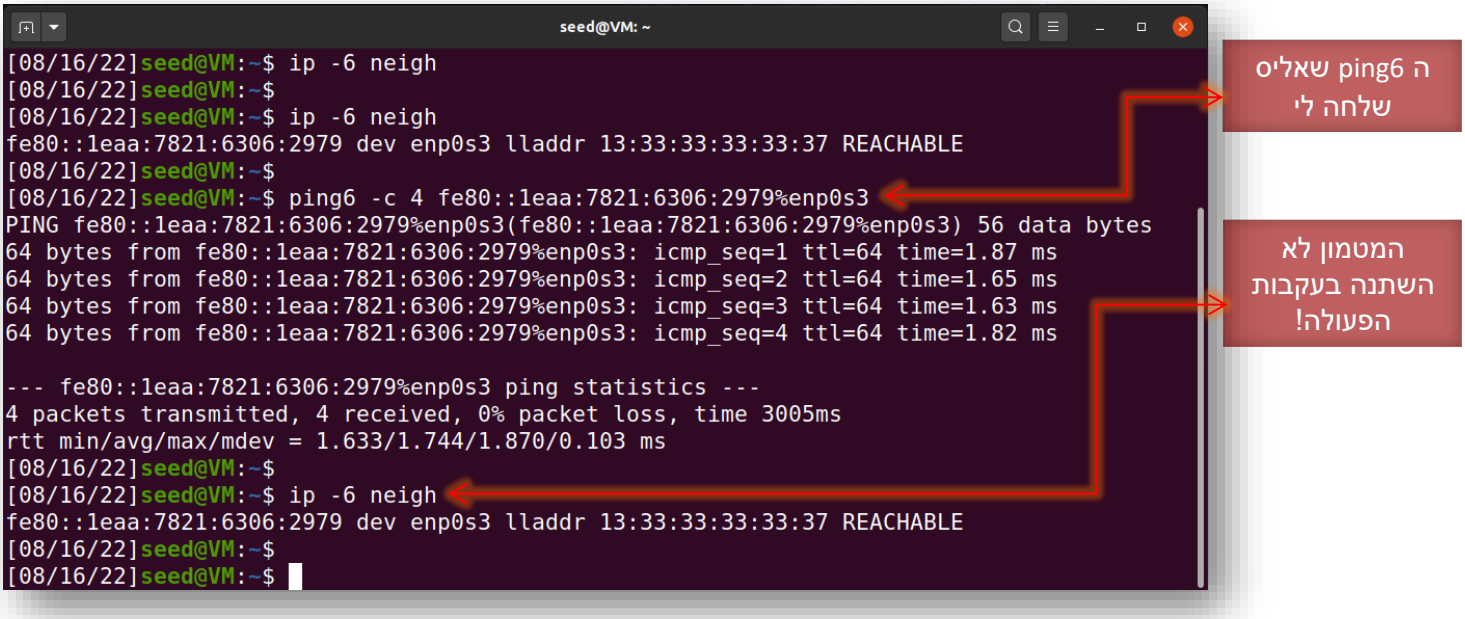
- הכנתי עם scapy פקטת NA מזויפת וקראתי לה fake_na. אלה הם הפרטים שלה:

```
>>> fake_na.show()
###[ IPv6 ]###
  version= 6
  tc= 0
  fl= 0
  plen= None
  nh= ICMPv6
  hlim= 255
  src= fe80::1eaa:7821:6306:2979
  dst= fe80::43cc:ca2f:ae1f:dbed
###[ ICMPv6 Neighbor Discovery - Neighbor Advertisement ]###
     type= Neighbor Advertisement
     code= 0
     cksum= None
     R= 0
     S= 1
     O= 1
     res= 0x0
     tgt= fe80::1eaa:7821:6306:2979
###[ ICMPv6 Neighbor Discovery Option - Source Link-Layer Address ]###
        type= 2
        len= 1
        lladdr= 13:33:33:33:33:37

>>>
```

- ואז שלחתי אותה עם הפקודה send(fake_na)
- ניתן לראות כעת **שזכרון המטמון של אליס**, השתנה כמו שרציתי:



- כדי לבדוק שאליס באמת כבר לא יכולה לפנות אלי, ביקשתי ממנה לעשות אלי ping6.
בתמונה הבאה היא המשך ישיר של התמונה הקודמת (היא חתוכה), לכן לא אסביר את השורות הראשונות.



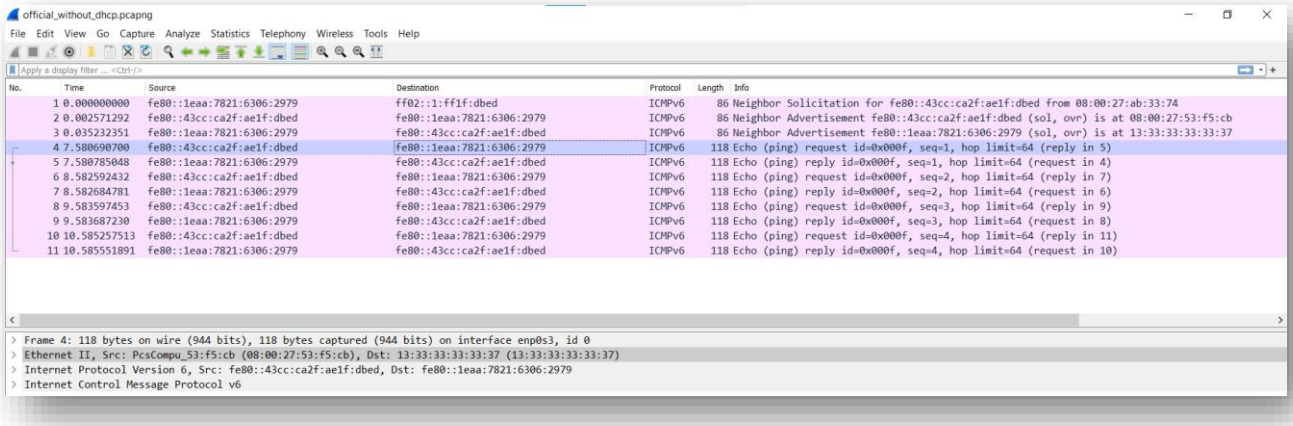
- אז בניגוד לכל הציפיות שלי, לכל ארבעת ה Echo requests התקבלה תשובת Echo replay.
- הייתי יכול לחשוב שהזכרון מטמון התעדכן כנראה כדי לבצע את פעולת ה ping6, אבל (למרבה החוצפה) הוא נשאר "שגוי".

- הייתי יכול לחשוב גם שאולי הפקטות של ה echo requests נשלחו דרך ה mac הנכון בכל זאת ואולי טעיתי בהארכה שלי שמה שיש בזכרון המטמון זה מה שבסוף יצא החוצא.
ובכן, טעיתי. וכמו שתדגים התמונה הבאה – אשכרה כל ה pings נשלחו לכתובת dst MAC המזוייפת.

- קצת הקדמה לקראת תמונת המצב דרך wireshark (זהה עבורי ועבור אליס ומצורפות ההקלטות בנפרד)

ההקלטה מראה רק פקטות icmpv6 ומלווה את כל התהליך החל משליחת ה fake_na ועד אחרי שאליס בודקת מה מצב הזיכרון מטמון שלה לאחר הפינגים.
ישנם 11 פקטות:

- 2 ראשונות מבררות מה ה mac של אליס, כי scapy צריך להשלים בעצמו את שכבת הקו. זה נעשה באמצעות מנגנון ה ns ו- na.
- פקטה שלישית היא ה fake_na בכבודו ובעצמו
- 8 הפקטות האחרונות הן ארבעה זוגות של בקשה & תגובה על כל אחד מארבעת ה pings.



- בחרתי לא להעמיס הפעם עם חיצים.
יש לשים לב לפקטה מספר 4, שהיא echo request שכתובת ה dst MAC היא 13:33:33:33:33:37
ולפקטה מספר 5 שמהווה את התגובה לאותו פינג.
  - הסיפור הזה חוזר על עצמו בכל אחד משלושת הפינגים הבאים.

והרי השאלה שלי:

עזבו אפילו לקבל ולהסניף חבילות **שלא אמורות להגיע אלי** (שוב, סתכלו על כתובת ה mac של היעד..)

מה פתאום נוצר echo replay על זה?!

זה גם קרה ששמתי כתובת mac כמו 10:10:10:10:10:10

מה אני מפספס פה?

קשה להמשיך לחקור כשכל מה שלמדתי עד כה קורס לתוך עצמו ונעלם 😊

אשמח לעזרה,

בוב.

נספחים

- ifconfig דרך המחשב של בוב

```
seed@VM: ~
[08/16/22]seed@VM:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:32:6b:68:5c  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fe80::1eaa:7821:6306:2979  prefixlen 64  scopeid 0x20<link>
        inet6 fd17:625c:f037:2:ee60:5dd5:ed61:68d5  prefixlen 64  scopeid 0x0<global>
        inet6 fd17:625c:f037:2:53c:cf3a:2291:f6a0  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:ab:33:74  txqueuelen 1000  (Ethernet)
        RX packets 14264  bytes 20327649 (20.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4246  bytes 343181 (343.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1400  bytes 95314 (95.3 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1400  bytes 95314 (95.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[08/16/22]seed@VM:~$
```

- ifconfig דרך המחשב של אליס

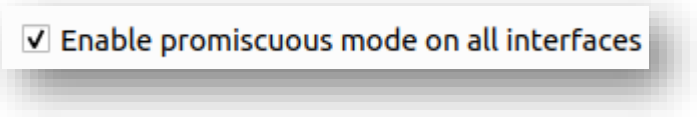
```
seed@VM: ~
[08/16/22]seed@VM:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:6a:81:db:05  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet6 fd17:625c:f037:2:8633:8a0:c9c:908d  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::43cc:ca2f:ae1f:dbed  prefixlen 64  scopeid 0x20<link>
        inet6 fd17:625c:f037:2:bc4d:8816:4ed4:f890  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:53:f5:cb  txqueuelen 1000  (Ethernet)
        RX packets 1836  bytes 275739 (275.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 719  bytes 118728 (118.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 898  bytes 64867 (64.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 898  bytes 64867 (64.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[08/16/22]seed@VM:~$
```

תשובה

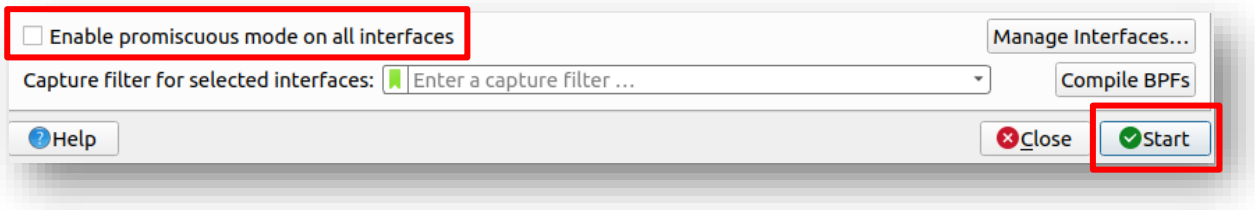
שלום בוב,

כרטיס הרשת שלך נמצא במצב promiscuous.

שים לב לסימון V בהגדרות ב wireshark:



כל שעליך לעשות הוא להוריד את ה V וללחוץ על start:



בהצלחה,

איב תעשיות רשע בע"מ