**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

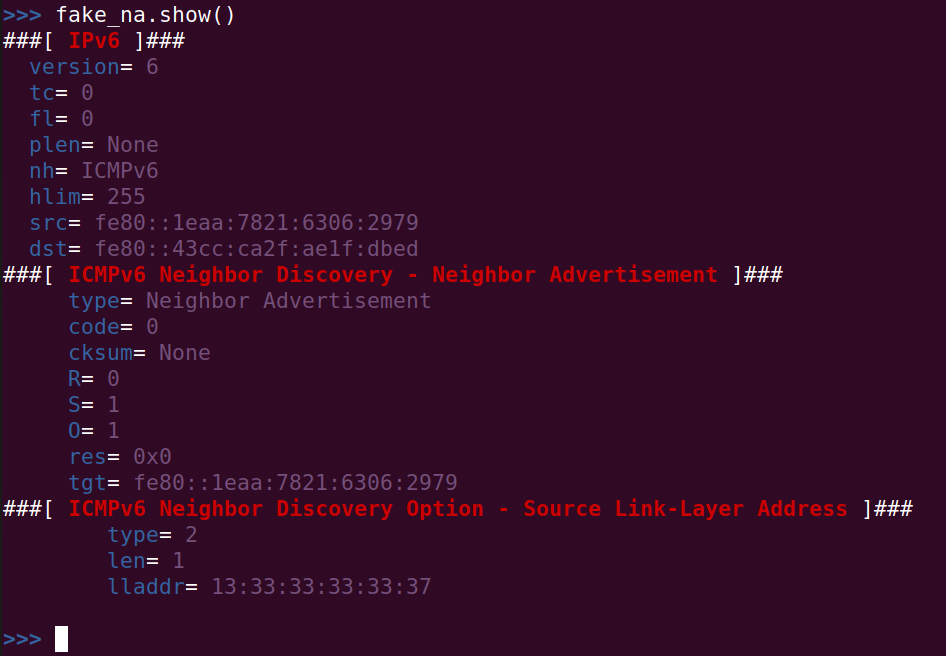
אומר שהתפקיד המקביל שלהם בעולם ה ipv4 הם ARP request ו ARP response בהתאמה.

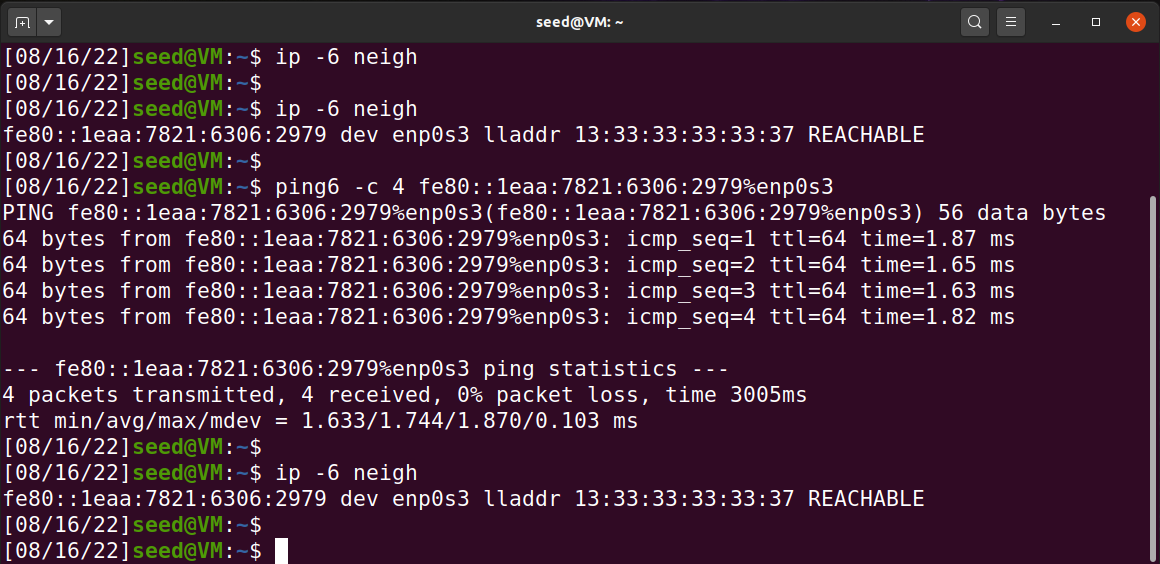
* חשבתי שאם אוכל לשלוח לאליס הודעת NA שאומרת "היי, הכתובת ipv6 שלי נמצאת בכתובת הפיזית 13:33:33:33:33:37", אז מעתה כל הודעה שהיא תרצה לשלוח לי (אנחנו באותה רשת פיזית) תקבל את כתובת ה dst MAC הנ"ל, וההודעה שלה לא אמורה להגיע אלי.

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

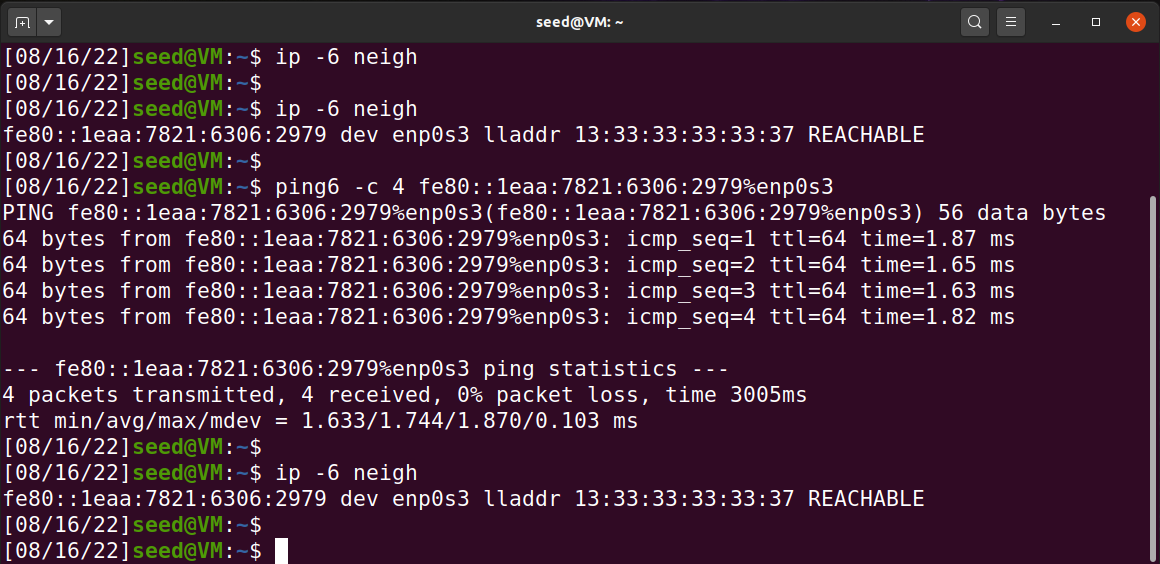


לפני ששלחתי את fake\_na

אחרי ששלחתי את fake\_na

* כדי לבדוק שאליס באמת כבר לא יכולה לפנות אלי, ביקשתי ממנה לעשות אלי ping6.

(התמונה הבאה היא המשך ישיר של התמונה הקודמת (היא חתוכה), לכן לא אסביר את השורות הראשונות)



המטמון לא השתנה בעקבות הפעולה!

ה ping6 שאליס שלחה לי

* 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)

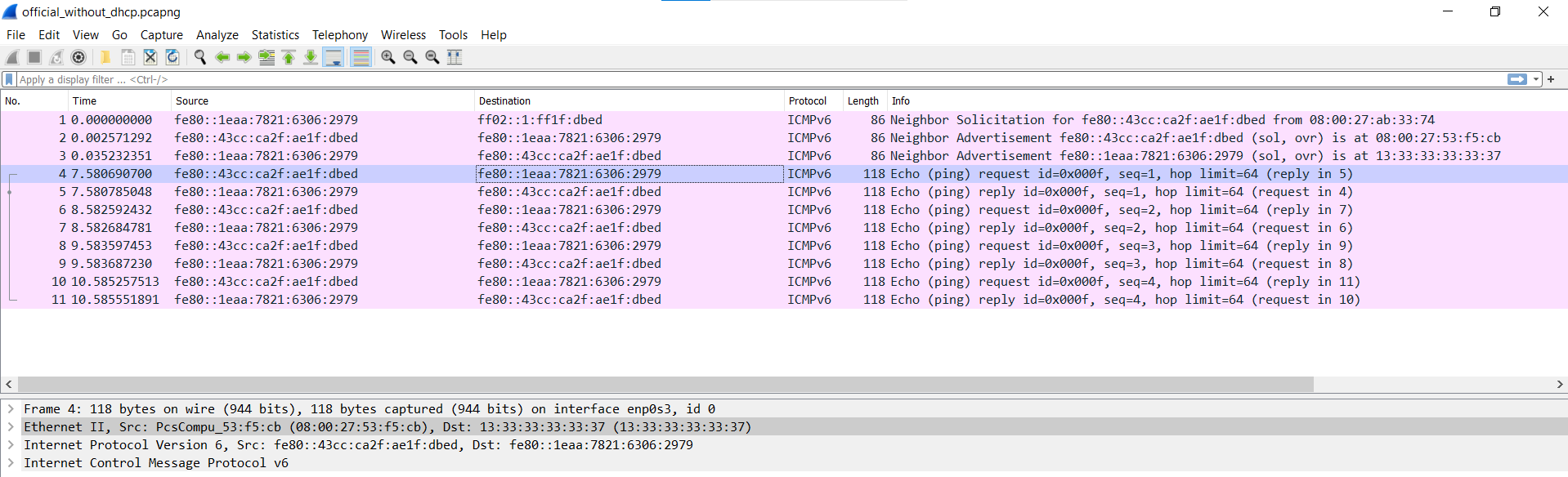
ההקלטה מראה רק פקטות icmpv6 ומלווה את כל התהליך החל משליחת ה fake\_na ועד אחרי שאליס בודקת מה מצב הזיכרון מטמון שלה לאחר הפינגים.

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?

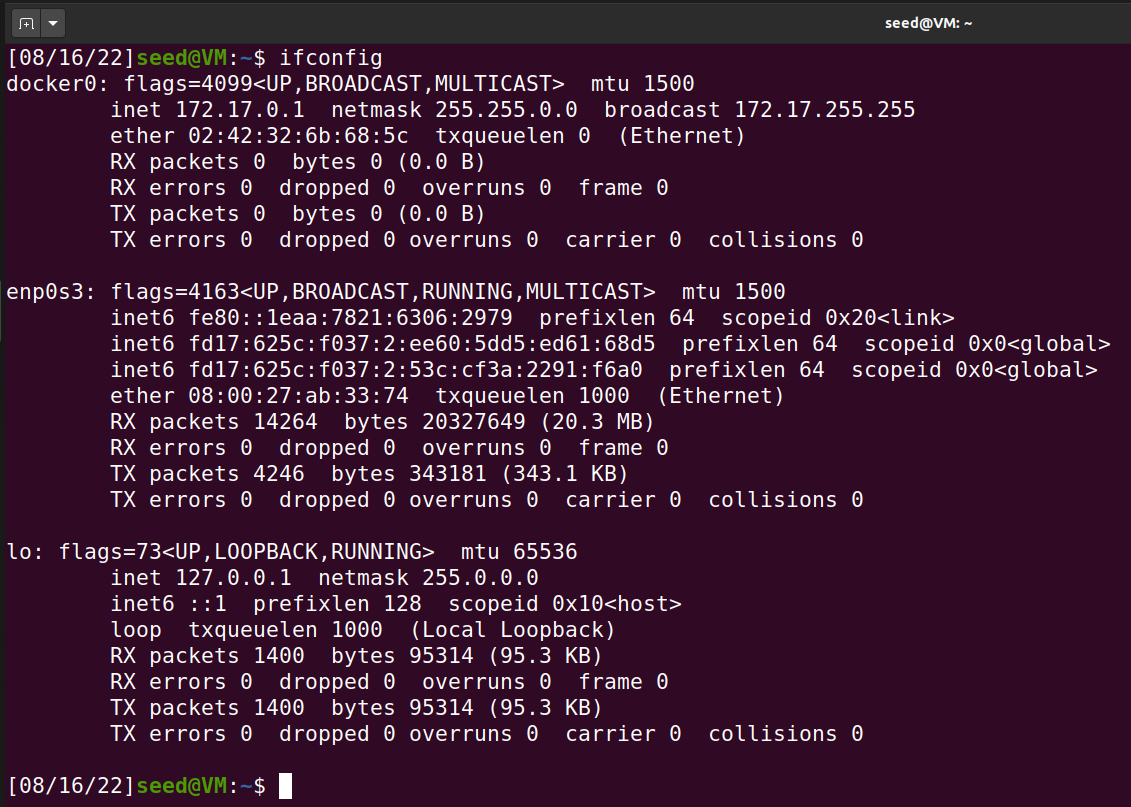
קשה להמשיך לחקור כשכל מה שלמדתי עד כה קורס לתוך עצמו ונעלם 😊

אשמח לעזרה,

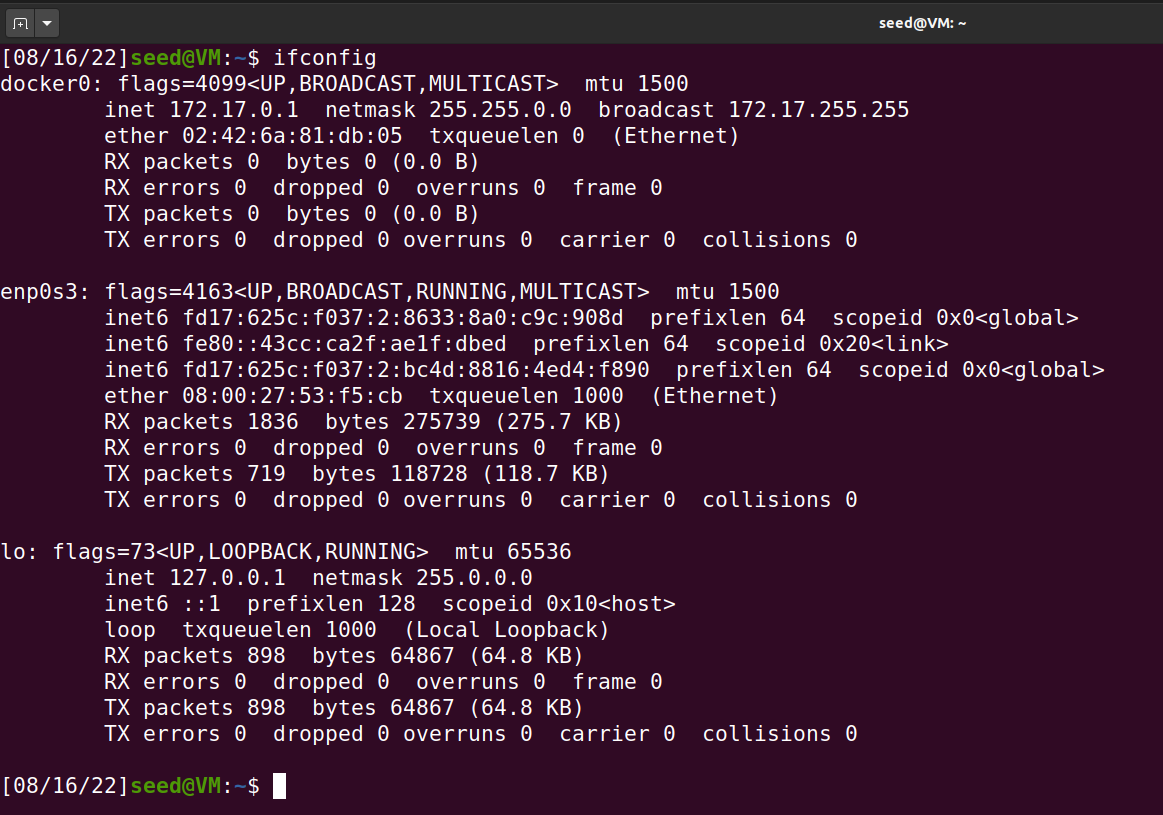
בוב.

**נספחים**

* ifconfig דרך המחשב של בוב



* ifconfig דרך המחשב של אליס



**תשובה**

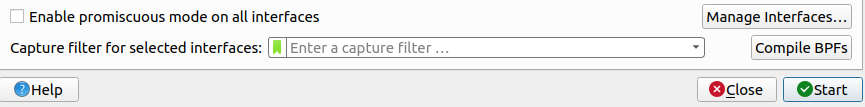
שלום בוב,

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