הורעלתי שוב ולאף אחד לא אכפת

לא לדאוג אין צורך באמבולנס..

היי. שמי אליס. אני עצבנית. ומסתבר שבנוסף לכל הצרות יש לי גם זכרון גרוע, שוב. (זכרון מטמון. לא צוחקת.)

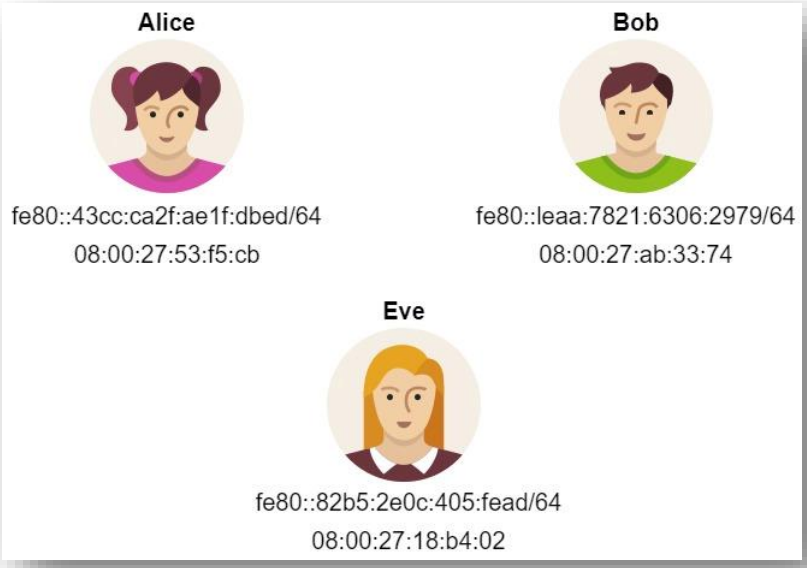
בגדול מה שקרה זה שאחרי שאיב הרסה לבוב את הצעת הנישואין שלו אלי (לינק לכתבה שמתעדת את המקרה המתועב https://github.com/SimchaTeich/MITM)

דיברנו ביננו והגענו למסקנה ש ARP לא מספיק מאובטח והגיע הזמן להגר מהר ל ipv6.

הבטיחו לנו שהוא מאובטח ואין אופציה ל ARP poisoning וכל השטויות האלה.

כן. ממש.

לפני שאספר על מה שקרה כדאי שתעיפו מבט על מצב הרשת שאני נמצאת בה:



אחרי הצעת הנישואין הטראומתית, כל לילה לפני שאני נרדמת וכל יום איך שאני קמה בבוקר אני בודקת את זכרון המטמון שלי.

למרבה הזוועה זה מה שקידם את פני הבוקר:

```
[08/18/22]seed@VM:~$ ip -6 neigh
[08/18/22]seed@VM:~$
[08/18/22]seed@VM:~$ ip -6 neigh
fe80::82b5:2e0c:405:fead dev enp0s3 lladdr 08:00:27:18:b4:02 DELAY
fe80::1eaa:7821:6306:2979 dev enp0s3 lladdr 08:00:27:18:b4:02 REACHABLE
[08/18/22]seed@VM:~$
```

אתמול בלילה

היום בבוקר

לפני שהלכתי לשון אתמול ניקיתי את הזכרון מטמון עם הפקודה sudo ip -statistics neigh flush dev enp0s3

ולכן אתמול בלילה הלכתי לישון כשהזכרון נקי.

בבוקר ניתן לראות שיש שתי רשומות.

הראשונה – דווקא בסדר. זה בסך הכל מספר לי על איב, והפרטים שלה תקינים (ראו שוב תמונת רשת)

השניה – ממש לא כיפית ומזכירה לי דברים שאני מעדיפה לשכוח. יש שם קישור בין כתובת ה ipv6 של בוב לכתובת ה mac של איב.

הדבר הראשון שעשיתי (אחרי קורס מעבדת הגנה :) היה ללכת להסנפות, כי אני מתה על להסניף מתוך שינה, ואחרי כמה פעולות נקיון גיליתי גם את הפקטות שאחראיות על הבלאגן הזה (הקלטה מצורפת בנפרד):

Source	Destination	Protocol	Length	Info
fe80::1eaa:7821:6306:2979	fe80::43cc:ca2f:ae1f:dbed	ICMPv6	65	Echo (ping) request id=0x0001, seq=1, hop limit=64 (reply in 4)
fe80::43cc:ca2f:ae1f:dbed	ff02::1:ff06:2979	ICMPv6	86	Neighbor Solicitation for fe80::1eaa:7821:6306:2979 from 08:00:27:53:f5:cb
fe80::1eaa:7821:6306:2979	fe80::43cc:ca2f:ae1f:dbed	ICMPv6	86	Neighbor Advertisement fe80::1eaa:7821:6306:2979 (sol, ovr) is at 08:00:27:ab:33:74
fe80::43cc:ca2f:ae1f:dbed	fe80::1eaa:7821:6306:2979	ICMPv6	65	Echo (ping) reply id=0x0001, seq=1, hop limit=64 (request in 1)
fe80::1eaa:7821:6306:2979	fe80::43cc:ca2f:ae1f:dbed	ICMPv6	86	Neighbor Advertisement fe80::1eaa:7821:6306:2979 (sol, ovr) is at 08:00:27:18:b4:02

- פקטה ראשונה: בוב שלח לי ping6, כלומר echo requests
- פקטה שניה + שלישית: אני מבררת עם NS ו NA מה ה mac של בוב כדי לענות לו echo replay
- פקטה רביעית: אני עונה לבוב echo replay
- פקטה חמישית: בוב שולח לי (שוב, משום מה) פקטת NA שמספרת לי שהכתובת MAC שלו היא כמו של איב. (שימו לב להבדלים בין הפקטות השלישית והחמישית)

אז היה לי קצת חשוד מה פתאום בוב שולח לי ping6 באמצע הלילה, במיוחד אחרי המקרה המוזר שקרה לו.

ולכן שלפתי עם סקאפי את הפקטה הראשונה מתוך ה- pcap, הדפסתי אותה, וגיליתי את הדברים הבאים:

איב היא המקור האמתי בכלל!

ובשיא החוצפה היא מזייפת חבילה בשם בוב

```
>>> fake_ping6.show()
###[ Ethernet ]###
  dst= 08:00:27:53:f5:cb
  src= 08:00:27:18:b4:02
  type= IPv6
###[ IPv6 ]###
     version= 6
     tc= 0
     fl= 0
     plen= None
     nh= ICMPv6
     hlim= 64
     src= fe80::1eaa:7821:6306:2979
     dst= fe80::43cc:ca2f:ae1f:dbed
###[ ICMPv6 Echo Request ]###
        type= Echo Request
        code= 0
        cksum= None
        id= 0x1
        seq= 0x1
        data= 'hey'

>>>
```

כלומר מה שקרה כאן זה שאיב זייפה ping6 בשם בוב ושלחה אותו אלי.

אז המחשב שלי רצה לענות echo replay לבוב, ולכן הפקטה השניה והשלישית מוצאות את ה mac שלו.

הפקטה הרביעית כמו שאמרנו זה ה echo replay שלי לבוב.

לכן נותר לי לחשוד בפקטה החמישית, שבה בוב אומר לי שה mac שלו הוא כמו של איב.

לכן גם פה חילצתי עם scapy את הפקטה החמישית והדפסתי.

ואז הבנתי מה קרה פה:

- איב זייפה ping6 בשמו של בוב
- ואז איב זייפה na שיגרום לשינוי רשומה אצלי, כך שהכתובת mac של בוב שמקושרת ל ip שלו תהיה הכתובת שלה.

ולכן יש לי כמה שאלות:

איפה תחנת המשטרה הקרובה? אני מתה שאיב תהיה מאחורי סורג ובריח.

למה איב לא יכלה פשוט לשלוח רק fake_na? למה היא היתה צריכה גם לזייף ping6 לפני התהליך.

תשובה

היי אליס.

אתייחס ברשותך רק לשאלה השניה.

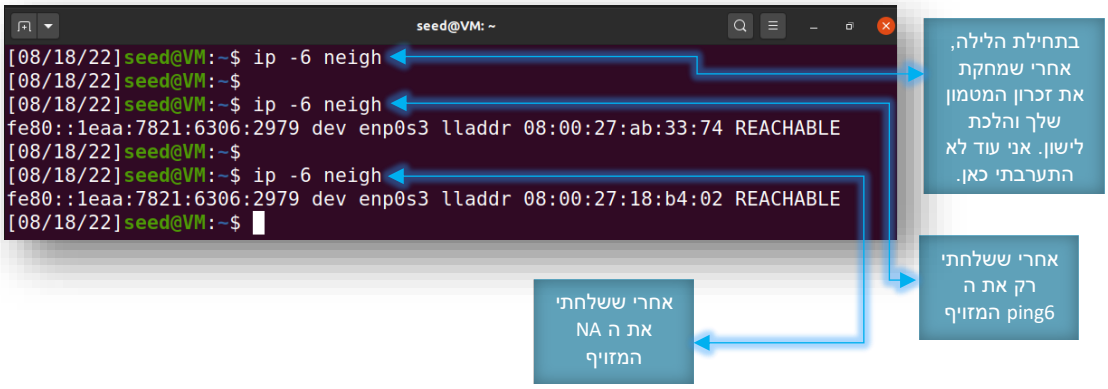
הייתי צריכה לזייף קודם ping6 בשם בוב, כדי שלפני שתעני לו echo replay תיווצר אצלך רשומה שמתארת את הקישור בין ה ip של בוב ל mac האמיתי שלו. (לזה אחראיות פקטות 2 ו 3 בהסנפה שלך)

רק אחרי שהרשומה האמיתית תהיה קיימת, ה fake_na שלי יהיה בכוחו לשנות אותה לצרכי התמימים לגמרי.

- אם לא תהיה קיימת רשומה עם ה ip של בוב, ה fake_na לא יצליח ליצור אותה בעצמו.

כדי להסביר יותר טוב,

כך נראה זכרון המטמון שלך במהלך ~~המתקפה~~ הניסוי שלי:



אה איך נכנסתי לך לטרמינל כדי להראות פה את התהליך הנ"ל את שואלת?

פשוט תמשיכי את החיים שלך כרגיל ואל תתרידי את עצמך עם שאלות מטופשות.

באהבה,

איב תעשיות רשע בע"מ