**הורעלתי שוב ולאף אחד לא אכפת**

די נמאס לי.

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

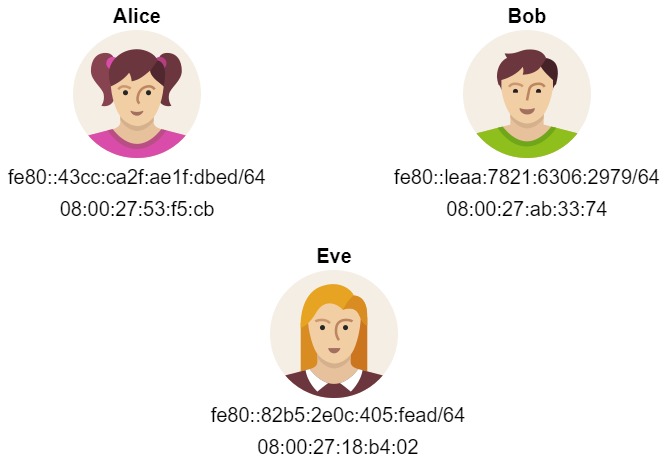
בגדול מה שקרה זה שאחרי שאיב הרסה לבוב את הצעת הנישואין שלו אלי (לינק לכתבה שמתעדת את המקרה הנפשע <https://github.com/SimchaTeich/MITM>)

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 אני בודקת ואז מוחקת את זכרון המטמון, וכל יום איך שאני קמה בבוקר אני בודקת את זכרון המטמון שלי שוב.

למרבה הזוועה זה מה שקידם את פני הבוקר:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

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):תמונה שמכילה שולחן

התיאור נוצר באופן אוטומטי

* 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:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

ובשיא החוצפה היא מזייפת חבילה בשם בוב

איב היא המקור האמתי בכלל!

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.

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

וכאן היא מספרת ש ip של בוב מקושר ל mac שלה

שוב איב היא המקור האמיתי!

ושוב היא מזייפת את החבילה בשם בוב

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 אליך איב:**

* איך את חיה עם עצמך? לא מספיקה לך הפעם הקודמת?
* למה את לא יכולה פשוט לשלוח רק fake\_na? למה את היית צריכה גם לזייף ping6 כחלק מהתהליך?

**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:

תמונה שמכילה טקסט

התיאור נוצר באופן אוטומטי

בתחילת הלילה, אחרי שמחקת את זכרון המטמון שלך והלכת לישון. אני עוד לא התערבתי כאן.

אחרי ששלחתי את ה NA המזויף

אחרי ששלחתי רק את ה ping6 המזויף

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

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

באהבה,

איב תעשיות רשע בע"מ