בס"ד

המדריך הרעיל למרעיל

שלום לכולם, כאן איב נשיאת הארגון הממשלתי הצפון קוריאני *איב תעשיות רשע בע"מ*.

ואם אתם קוראים את זה סימן שאני מתה.

בשם השליט הבלתי מעורער שלנו התחזיתי במשך תקופה לחבר'ה של המתנגדים לשלטון וחברתי לאליס ובוב מובילי המאבק לשחרור צפון קוריאה.

במהלך ניטור התעבורה הסודי שלהם כמעט נתפסתי כמרגלת המלכותית, אבל הודות לתושייה ולאומץ הנהוגים אצלנו במלכות הצפון קוריאנית הפעלתי את כישורי המשחק שלי וגרמתי להם להאמין שהכל קרה כיוון שאני מאוהבת בבוב, דבר שהוביל לבסוף לפרסום הכתבה הלא מחמיאה שהוציאו המתנגדים לממשל (ראו כאן: https://github.com/SimchaTeich/MITM) שמתחילה בשקר בו אני מאוהבת בבוב ומסתיימת בשקר שאמר שהתחתנתי עם בוב והפכתי לקרפדה.

טוב אז קרפדה אני לא, אבל לפחות הם לא חושדים בי יותר, ולכן הורדתי פרופיל ושמרתי על קשר עם בוב ואליס. (כל מה שצריך לעשות אצלם זה לומר "סליחה" חחחחחח אני מתה!)

הנקודה היא שלמרות הקשר ששמרתי איתם כבר לא הצלחתי לנטר את השיחות ביניהם.

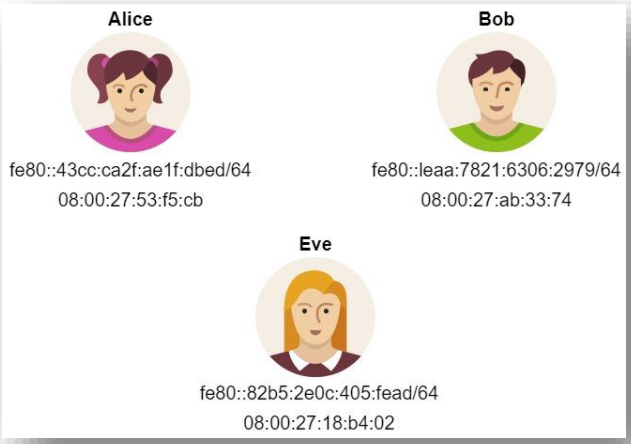
עד אתמול בערב, כשבוב פנה אלי עם הבעיה שלו עם ה ping6,
(https://github.com/SimchaTeich/IPv6/tree/main/MITMv6/1%20-%20Bob%20story) והבנתי שהם עברו ל ipv6 במחשבה הטיפשית שהוא יותר בטוח. אני חושבת שבוב ניסה לבדוק בעצמו אם ניתן להרעיל את הזכרון של אליס בipv6 כדי ללמוד על הדרכים בהם אני פועלת ולוודא שאני לא אהיה מסוגלת לעשות זאת כמו ב ipv4.

אז מכאן זה כבר היה די קל, כל מה שהיה עלי לעשות הוא לכתוב כלי שמרעיל את אליס ובוב, ולהמשיך להאזין לאליס ובוב ולהעביר את כל המידע לקים ג'ון און, השליט הבלתי מעורער של מלכותינו שיחליט לאיזה סוג של חופשה לשלוח אותם.

למרבה הצער הבוקר גם אליס פנתה אלי
(https://github.com/SimchaTeich/IPv6/tree/main/MITMv6/2%20-%20Alice%20story) ולא הסתירה את זעמה וחשדה ששוב אני מחטטת לה בזכרון מטמון. אמרתי לה שאני בסך הכל עושה ניסוי ושלא תטריד את עצמה בשאלות. מקווה שזה הרגיע אותה.

אז זאת תמונת הרשת שלי

בס"ד

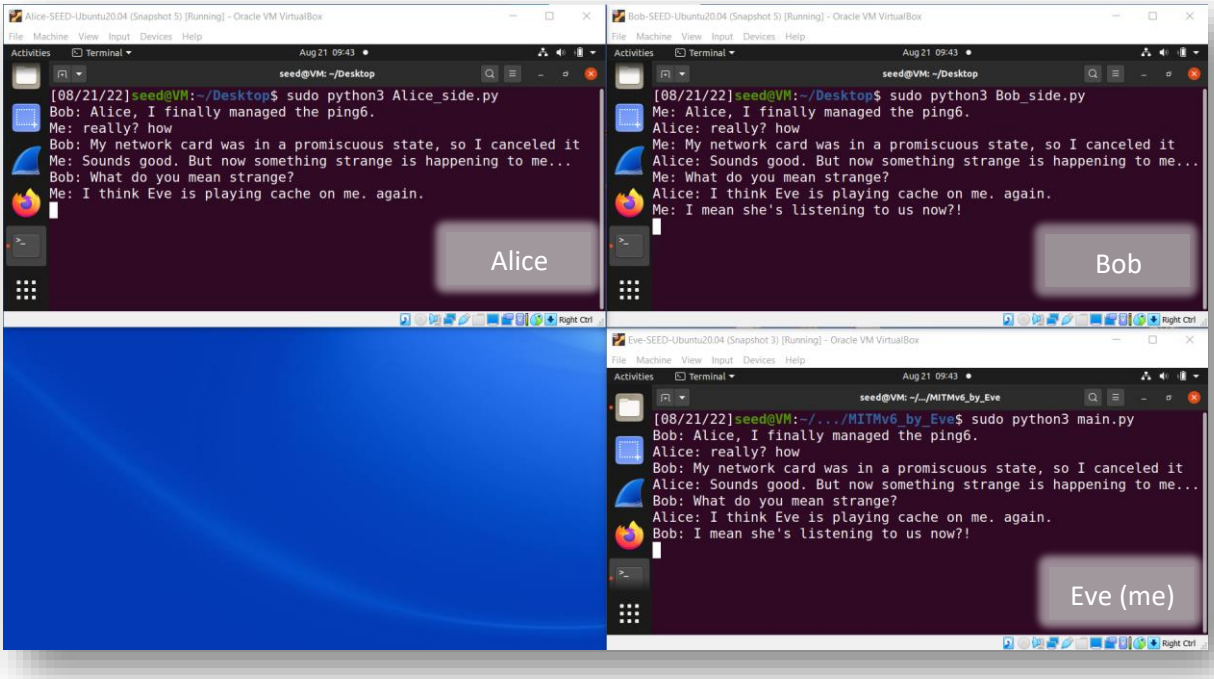


לא אתאר בפירוט כיצד הפעלתי את התקיפה, כי כל מה שעשיתי היה להרעיל שוב את זכרונות המטמון של שני הצדדים, ומה שעשיתי לצד של אליס (ובהתאמה גם לבוב) מתואר בשאלה שהיא שלחה לי קודם.

כן אומר שהפעלתי הרעלה של שני הצדדים בלולאה, ובמקביל סיננתי מהתעבורה שלי רק חבילות שעוברות בין אליס לבוב ולהפך, הדפסתי את התוכן שלהם ושלחתי כל חבילה ליעד הנכון שלה. מצורף סקריפט בנפרד.

אבל אז,

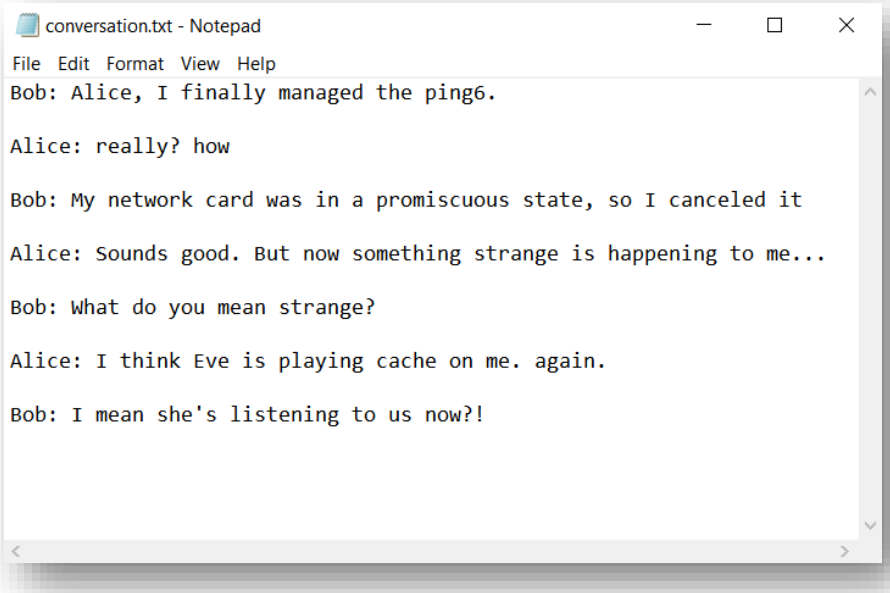
זאת השיחה שהאזנתי לה.



--סודי ביותר--

בס"ד

הוצאתי את התוכן לקובץ טקסט, על מנת לפשט את העניין:



וזהו.

בזמן שאני נסה לי על נפשי מצאתי זמן להרהר והגעתי למסקנות הבאות:

...

סוף.

--סודי ביותר--