מטלה 1 – הגנת פרוטוקולי תקשורת תשפ"ב סמסטר ב – אוניברסיטת אריאל בשומרון

הערה: המרצה מרדכי אישר את מה שעשינו, זה לא מה שכתוב במעבדה אחד לאחד 😊

מצורפת ההוכחה:

המטרה:

Man In The Middle, באמצעות ARP Poisoning.

הרקע:

Eve מאוהבת קשות ב Bob, שמאוהב קשות ב Alice.

(לא, זה לא יחס טרנזיטיבי כי Eve דווקא שונאת את Alice... :)

באחד הימים Bob החליט להציע נישואים ל Alice, אבל בדרך מקורית – בצ'אט.

כיוון ש Eve ו Bob חברים טובים, הוא סיפר לה על התכנית שלו, והיא מצידה החליטה לנצל את כישוריה הזדוניים ולחבל בהצעת הנישואים של Bob!

היא תשבור את השיחה בין שרת הצ'אט ל Alice, כך שכל ההודעות בשיחה הפרטית ביניהם יעברו דרכה, וחוץ מזה שהיא תראה אותם - היא גם תגרום להם להשתנות כך ש bob לא יצליח להציע נישואים וכל תקוותיו תיעלמנה.

אח"כ Eve תיכנס לצ'אט, תנצל את שברון הלב של Bob, ותציע לו נישואים איתה 😊

בעינינו הסיפור מרגש, הקוראים מתבקשים להזיל דמעה.

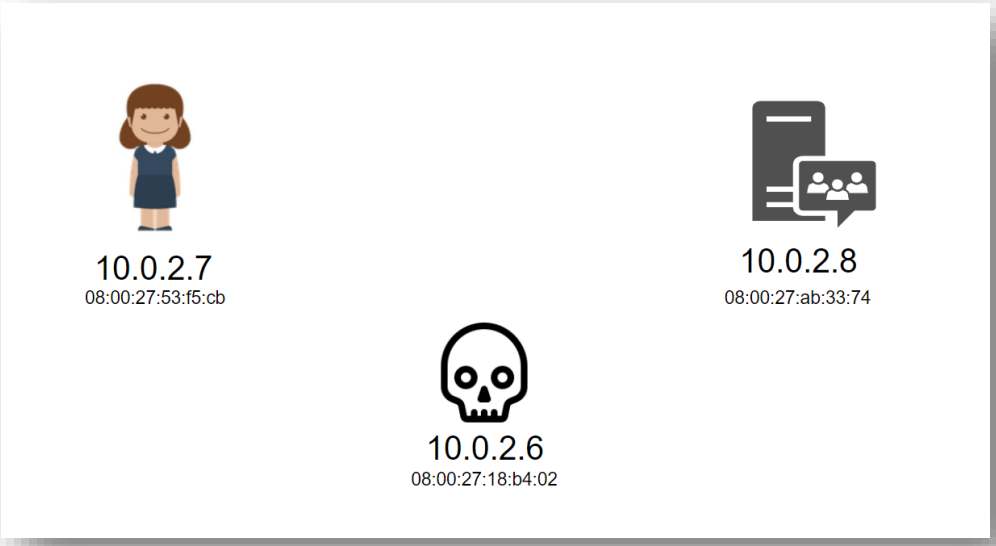
בעמודים הבאים יבוא פירוט נרחב של תיעוד התקיפה.

פירוט הרשת בה מתבצעת התקיפה:

- התקיפה תיעשה על 3 מכונות וירטואליות ubuntu20.04 של מעבדות SEED, שיושבות באותה רשת פנימית.
  - על מכונה אחת יהיו שרת הצ'אט ו Bob (השרת יכול להיות גם במכונה נפרדת, זה לא באמת משנה)
  - על מכונה שניה תהיה Alice,
  - ועל המכונה השלישית תשב Eve, בתפקיד התוקף.

- מערכת הצ'אט הנתקפת היא המערכת אותה כותבי שורות אלו בנו בפרויקט סיום של קורס תקשורת ומחשוב תשפ"ב סמסטר א. היא טובה עבור המשימה כי הפרוטוקול שלה טקסטואלי ואין הצפנת קצה לקצה. ניתן למצוא את האפליקציה כאן: https://github.com/SimchaTeich/Simple-Chat.git

- להלן סקיצה של הרשת, עם הפרטים האמיתיים שלה:

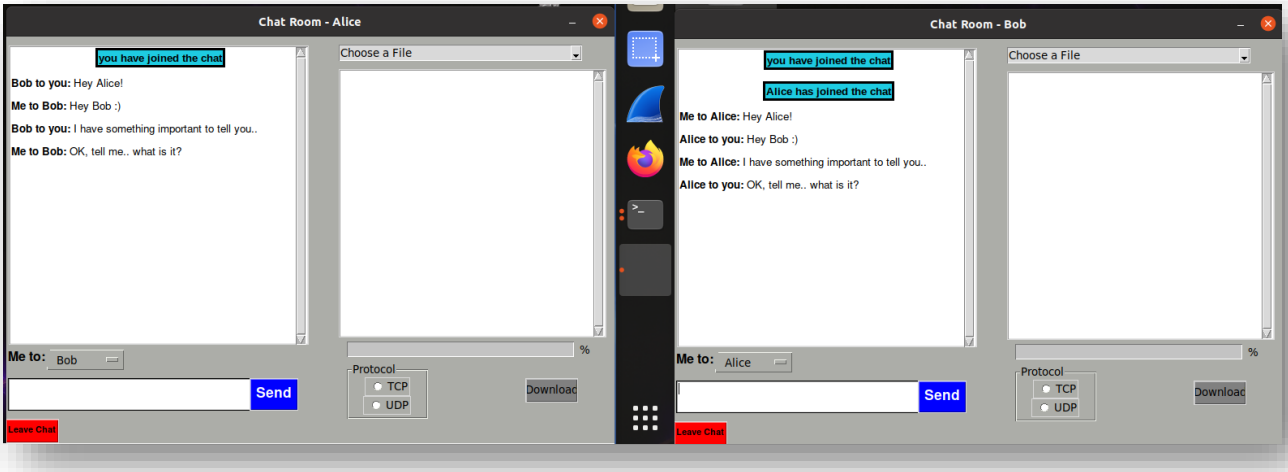


- מיותר לציין מי Alice, מי היא Eve, ומי שרת הצ'אט. נותר לברר איפה בוב.
- תשובה: לא אכפת לנו. כי המתקפה תיעשה על החיבור בין Alice לשרת הצ'אט.
- על מנת לצמצם את כמות צילומי המסך לצרכי הבהרה, וגם כדי לא לפתוח מכונה וירטואלית רביעית, Bob יישב על אותו מחשב עליו מורץ שרת הצ'אט. ולכן בצילומי המסך נראה שני ממשקי צ'אט.

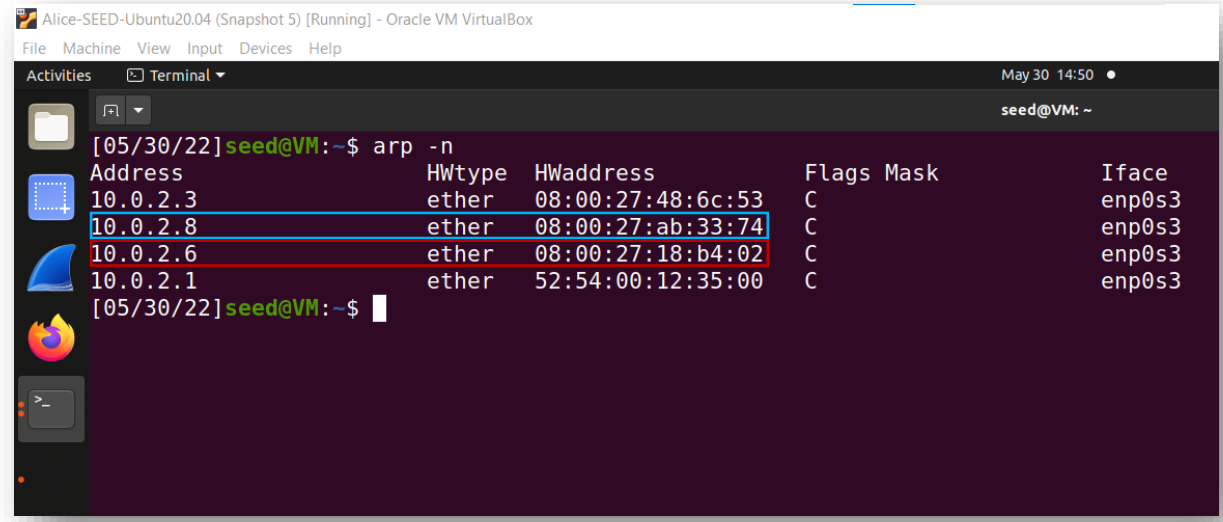
- **הערה:** בצילומי המסך הבאים, הסדר של המכונות הוירטואליות בצילומים הוא אותו הסדר של התמונה לעיל. כלומר, המכונה של Alice תמוקם משמאל למעלה, המכונה של השרת+ Bob תמוקם מימין למעלה, ו Eve, שהיא התוקפת, במיקום של הגולגולת.

כך מתחילה שיחה נורמלית:

- Bob מתחבר לצ'אט, ולאחריו מתחברת Alice.
- והם מתחילים שיחה ביניהם (נא לקרוא אותה)



- בשלב הזה, Eve (שבתמונה למעלה לא מופיעה), נכנסת לתמונה.
- היא תרעיל את זכרון המטמון של ARP אצל Alice ואצל השרת. מצורפת תמונה של זכרון המטמון של אליס טרום ברגע זה, טרום ההתקפה:

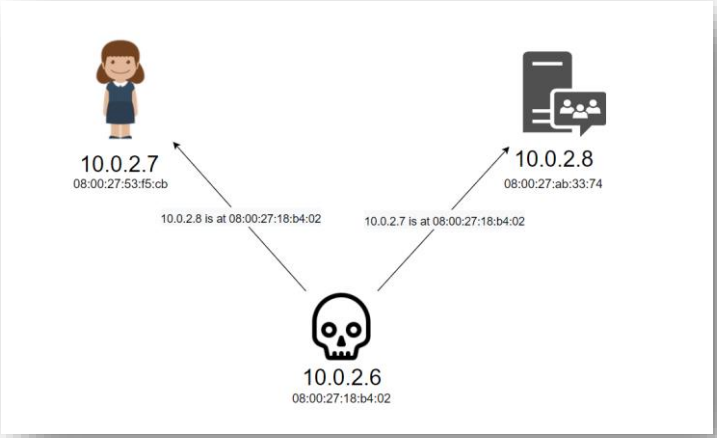


- הכתובות בכחול הן של השרת, והכתובות באדום הן של ה attacker, שכרגע הוא רק נמצא ברשת ועוד לא עושה כלום.

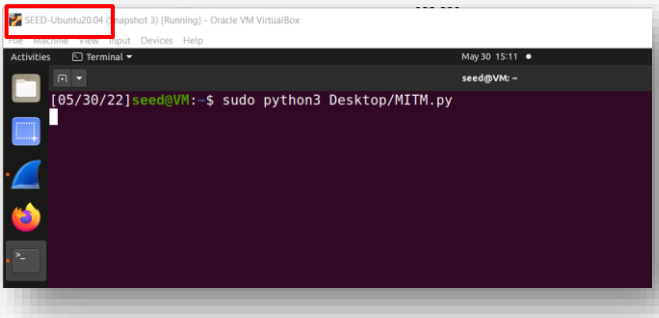
- כאמור, התוקפת Eve תשלח עכשיו שתי ARP Replay על מנת להרעיל את זכרונות המטמון ARP של Alice ושל השרת.

הרעלת זכרון המטמון של ARP:

- מצורפת כעת סקיצה של ההרעלה (הקוד יצורף בנפרד):

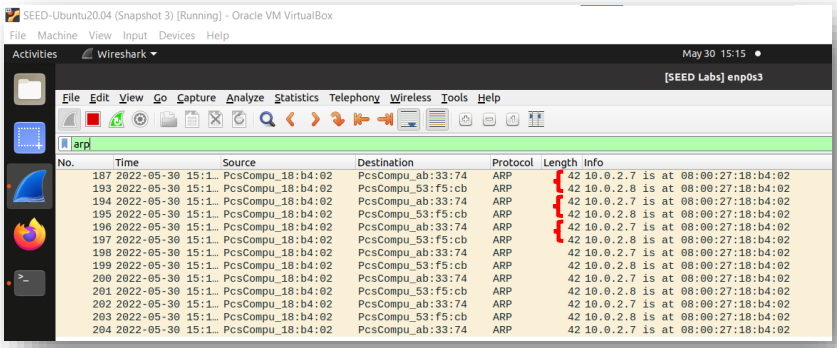


- כעת, Eve תפעיל את התכנית שלה (תרתי משמע :)
  - להלן תמונה של הפעלת התכנית מהמחשב של Eve:



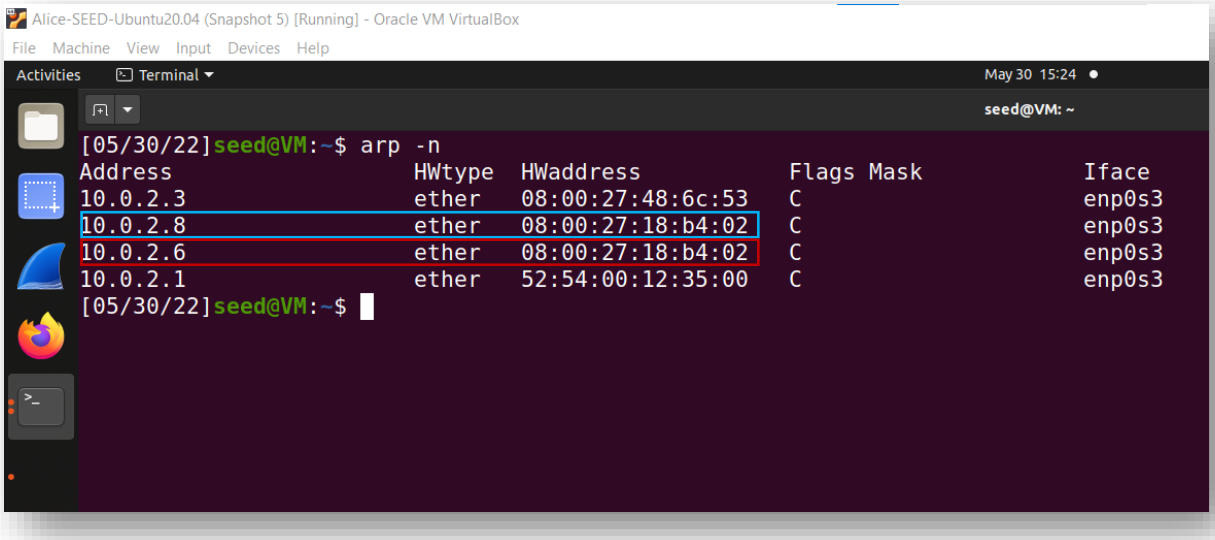
הריבוע באדום נועד להדגיש שאין מדובר במכונה של Alice או של השרת שזה קורה עליהן, אחרת היו מופיעים שם השמות Alice ו- Bob בהתאמה. בקיצור – מדובר במחשב של Eve.

- מתוך ה Wireshark של Eve, ניתן לראות כעת הרעלה מסיבית של שני הצדדים:



- ההרעלה מתבצעת כל 10 שניות, וניתן לראות את אותן הפקטות כמו בסקיצה שחוזרות על עצמן.
- עכשיו ניתן להסתכל על זכרונות המטמון ולוודא שאכן ההרעלה הצליחה.

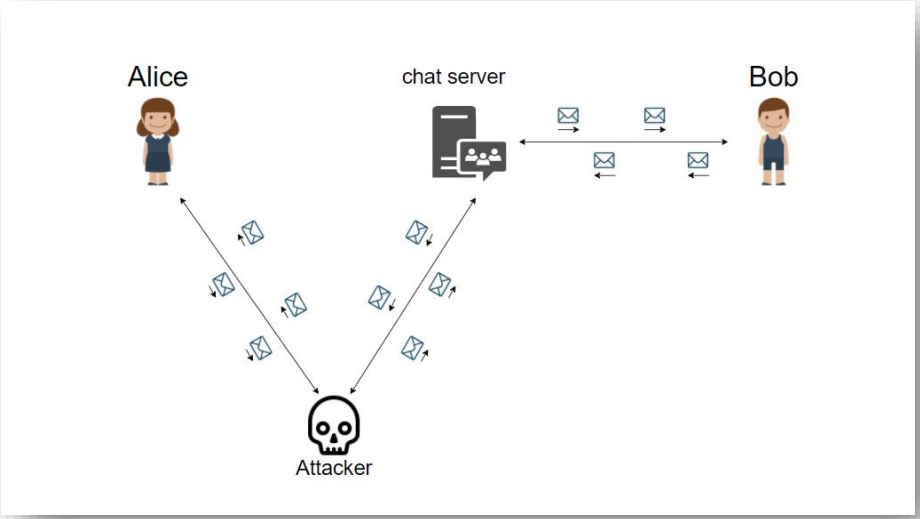
אז בהשוואה למצבה הקודם של Alice, זה המצב שלה עכשיו:



- וכמו קודם, הכתובות בכחול הן של השרת, והכתובות באדום הן של ה attacker, אבל לאחר ההרעלה.

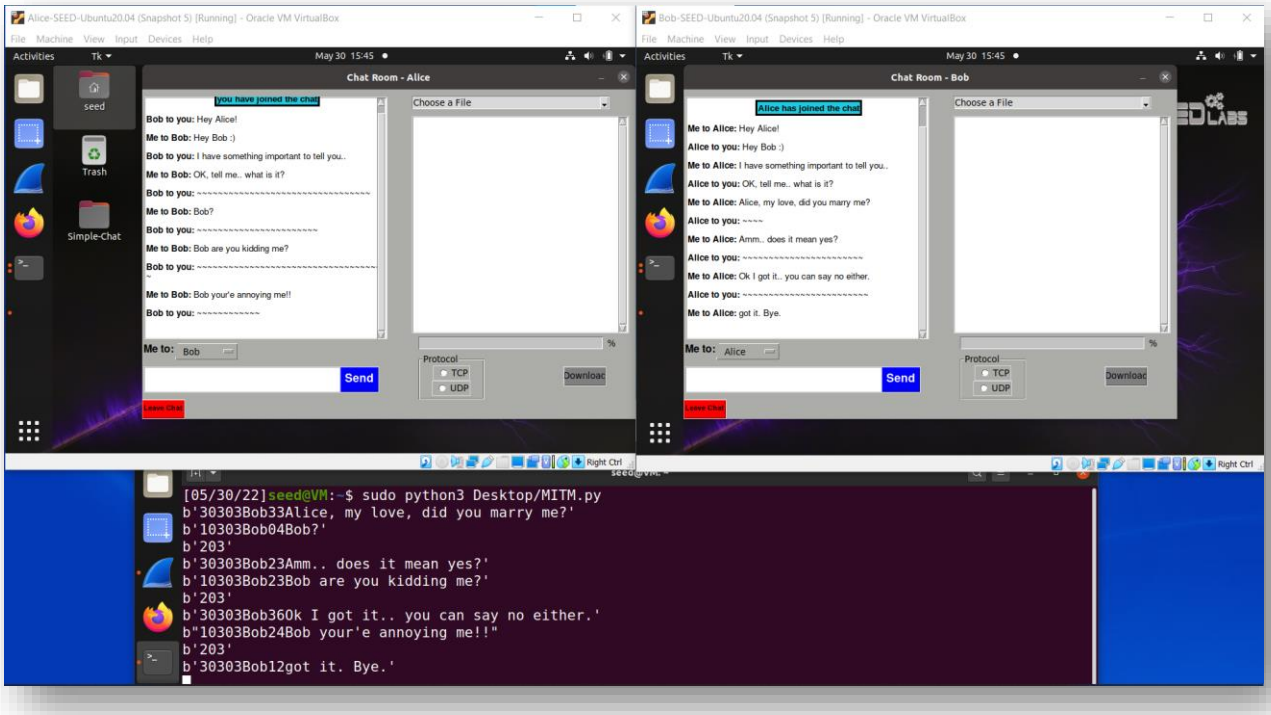
שיבוש החבילות שעוברות דרך התוקף

- ניזכר היכן היינו – Bob עמד להציע נישואין ל Alice.
- רגע לפני שזה קרה, Eve ניתבה את התעבורה כך שהיא תעבור דרכה:



- כעת, על פי התכנה, כל חבילה שתעבור מ Bob ל Alice וכן להיפך תגרום לשני דברים:
  - הדפסת התוכן האמיתי שמועבר בשיחה.
  - שיבוש התוכן האמיתי וזיוף ההודעות בין הצדדים.

- וכך, נהרסה לחלוטין הצעת הנישואין המרגשת:



- **הערה:** בפרוטוקול האפליקטיבי, חוץ מהתוכן המוצג במסך הצ'אט יש עוד פרטים (רואים את הפרוטוקול ממש במסך של התוקף, שיכול אם הוא רוצה לתעד את ההודעות הסודיות ללוג. ההודעות סודיות אגב כי זה הצ'אט על מצב פרטי), כדי שהתכנה שמציגה את ההודעות תדע מה להציג.
התווים ששונו בשיחה הם רק התווים של השיחה, כלומר מה שהמשתמשים ממש מקלידים על מנת לשלוח.

- **הערה:** הקוד וקובץ ה pcap מצורפים בנפרד.

- **הערה:** הסיפור נגמר בזה ש Bob יצא מדוכא ומצולק, והתחתן בסוף עם Eve שהפכה לקרפדה בנשיקה הראשונה. ככה זה עם נסיכות.