**תרגיל arp spoof detection (+האופציה לבונוס)**

בחרנו שלוש שיטות יעילות לזיהוי ההתקפה, ושילבנו בשביל הבונוס הגנה.

כאשר על פי שיטה מסוימת זוהתה התקפה, דגל ייחודי מורם, כאשר יש thread שרץ הבודק אם הורמו 2 דגלים.

שיטה 1- אנו מסניפים תעבורת ARP וכאשר נתפסת הודעת is at בצורה פשוטה נרכיב הודעת who has מתאימה לשם אימות (אנו מחליטים לא לסמוך על הis at המתקבלים). התשובה שמגיעה עבור מה ששלחנו עוברת השוואה אל מול הis at החשוד ואם היא זהה לו אזי לא יורם דגל, אחרת יורם הדגל. שיטה זו כמובן גורמת לתשובות הארפ המגיעות אלינו לעדכן את הטבלה במידע אמין וכך "על הדרך" אנו כבר דואגים להגנה בכך שההתקפה עוברת שיבוש.

שיטה 2- שיטה זו מורכבת משני תרחישים: באם הקוד מורץ על לינוקס, בעזרת שימוש בarp\_table אנו בודקים האם יש בטבלת הarp 2 שורות עם אותו מאק אך ip שונה. במקרה כזה יורם דגל.  
באם הקוד אינו מורץ על לינוקס, נסניף פקטות is at ונאחסן אותן במאגר משלנו (לאחר בדיקה אם פקטה כבר קיימת במאגר או לא). בתרחיש הזה האחסון יהיה בdictionary בו המפתח הוא דווקא הip והמאק הוא הערך.  
זאת מפני שהמאגר שלנו נבנה רק באמצעות is at וכדאי שנחפש קודם אחר ip במאגר השווה לזה בפקטה שקיבלנו ואם המאק שונה אז סימן שקיבלנו "המידע" על שני צירפוי מאק ואייפי שונים מה שגורם לנו להרים דגל.

שיטה 3- בשיטה זו עבור is at שמתקבל נשלח הודעת "פינג" לצירוף המאק והאייפי המוצהר בis at .  
אם תתקבל תשובה, סימן שהצירוף נכון ומחשב שכזה באמת קיים כך שניתן להניח שבהודעה זו לא מנסים לרמות אותנו. אם לא נקבל תשובה חזרה, זה מחשיד מאוד ולכן יורם דגל.

הסבר (וגם הסבר לבונוס): כאשר הורמו לפחות 2 דגלים, נפסיק את ריצת שיטות הזיהוי ונעבור לתחזוק הגנה. ההגנה דומה מאוד ומתבססת על שיטת הזיהוי מספר 1. פקטות is at מוסנפות, ופקטות who has נשלחות למאק המקור המוזכר בהן. וכך, המחשב בעל המאק המדובר יחזיר לנו תשובה שהיא תהיה לגיטימית כמובן (מפני שפקטות ארפ מועברות בשכבה 2 על פי מאק, והמידע בחלק הארפ של הפקטה ממולא על פי האינפורמציה שסופקה בחלק הארפ של פקטת הwho has) ותעדכן את הטבלה שלנו במידע נכון, מה שיילחם בעדכונים הכוזבים של התוקף ויהרוס את יעילות ההתקפה.  
**שיטות הזיהוי שלנו ואופן פעולת הקוד הינם מהירים ויעילים ונבדקו על ידינו כנגד כלי הspoof שבנינו בתרגיל הקודם, כמו כן חלק ההגנה שעשינו בתור בונוס באמת משבש את ההתקפה.**

תשובה לשאלה האם ייתכן false positive בקוד שלנו: לאחר שחקרנו את פעולתנו ומקרי קצה שונים החלטנו לענות על שאלה זו כך: כעיקרון בקוד שלנו לא ייקרה false positive שכן שיטה 1 ושיטה 3 עובדות על קבלת תשובות ממקורות לגיטימיים ועובדות בצורה מהירה מאוד כך שלא סביר בעליל שייתקבלו תשובות מכתובות אייפי שצומדו בזמן כה קצר למאק שונה. רק שיטה 2 עלולה להטעות במקרים מסוימים וספציפיים ובמיוחד כאשר התרחיש הוא מערכת לינוקס כאשר למחשב מסוים יש שתי כתובות אייפי, אך הקוד שלנו כמובן לא מסתפק בדגל מורם יחיד ולכן גם לא יהיה false positive.