**עבודת גמר – sniffing and spoofing**

**מגישים:** אריאל יפעי ומוטי דהרי.

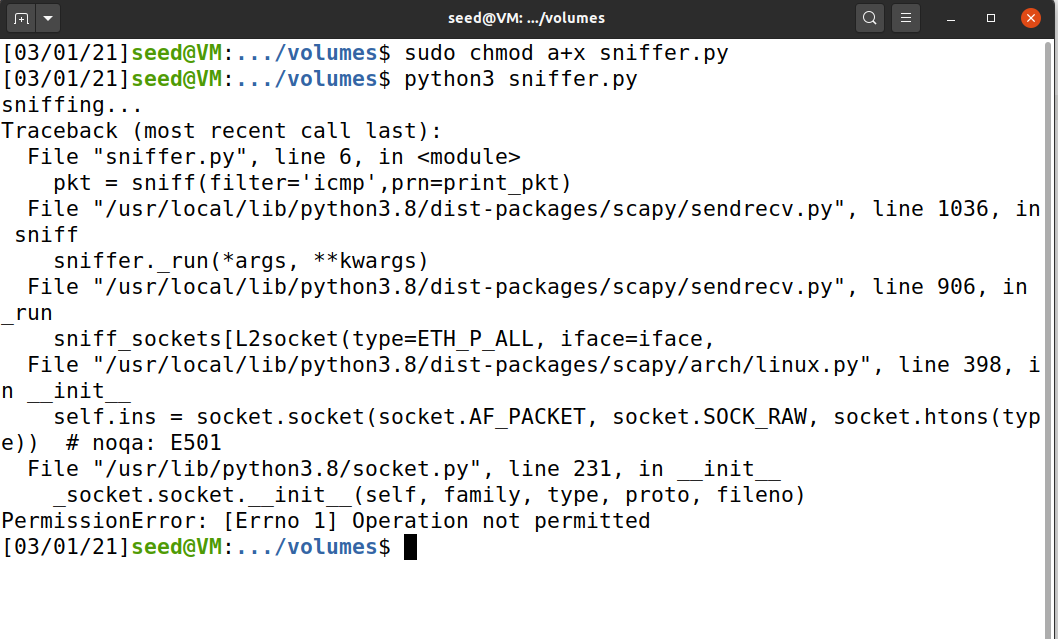
התקנו את SEEDvm בvirtualbox עדכנו את כל התוספים שהיה צריך ולאחר מכן בנינו סניפר בפייתון.

1.1A: התבקשנו להריץ את הסניפר בלי הרשאות אדמין ועם הרשאות אדמין ולראות מה קורה, הרצנו בטרמינל אחד את הסניפר שלנו ובשני את הפקודת ping לאתר של גוגל.

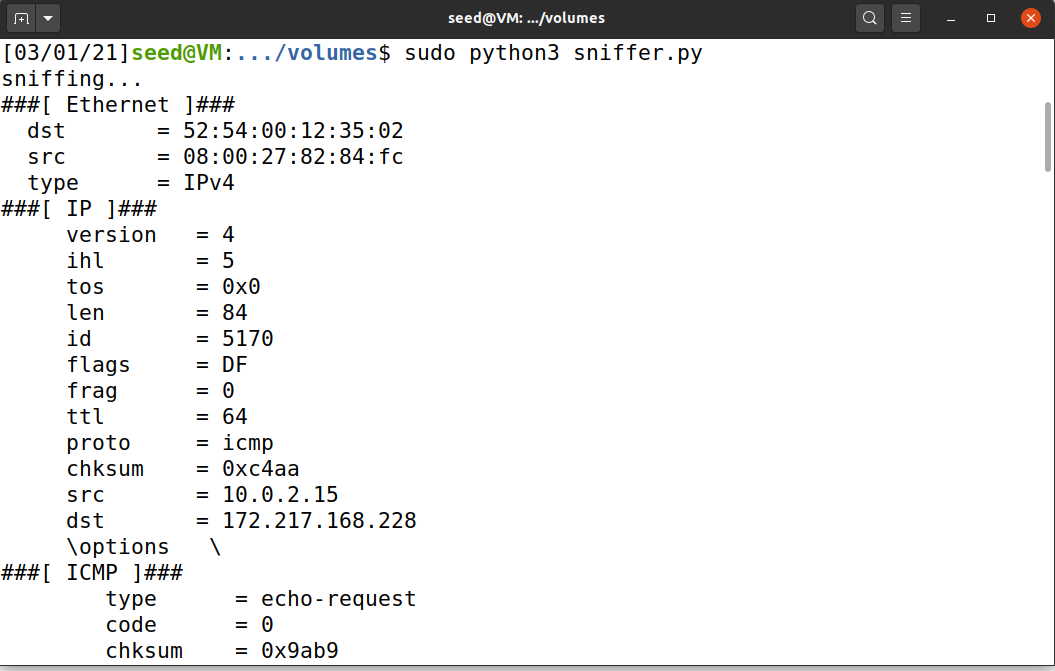
הסניפר:



הרצה בלי הרשאות אדמין:

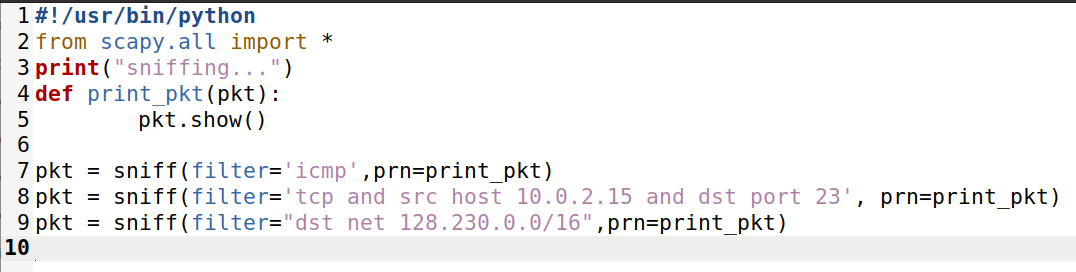


הרצה עם הרשאות:

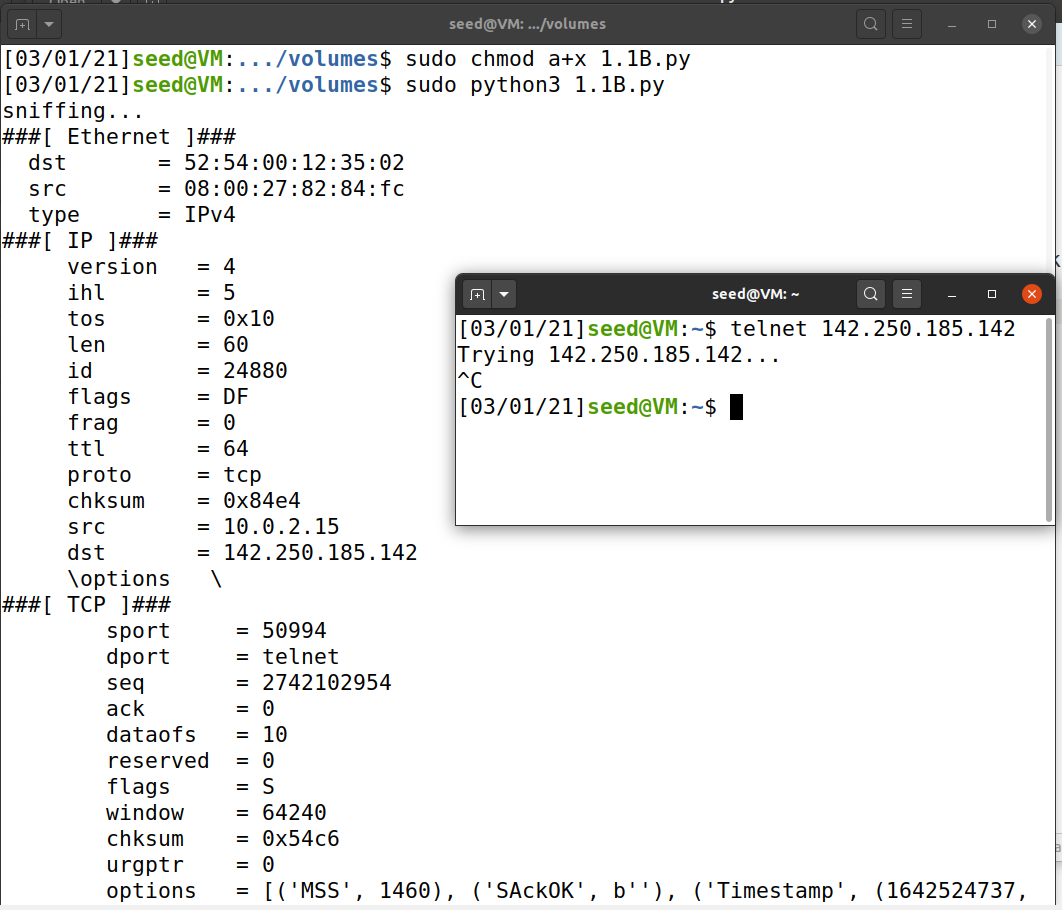


הצלחנו לתפוס פקאטות!

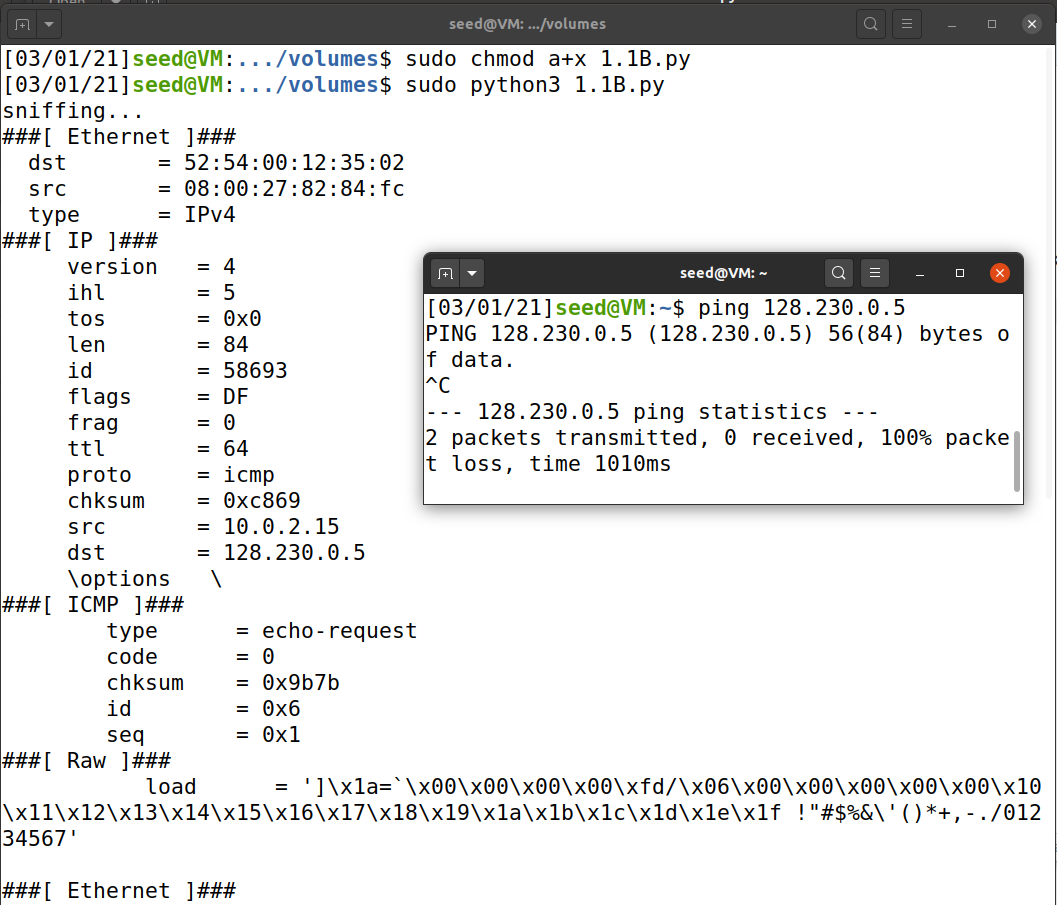
1.1B: התבקשנו להוסיף עוד פילטרים לסניפר שלנו.



תפיסת פקטת TCP:



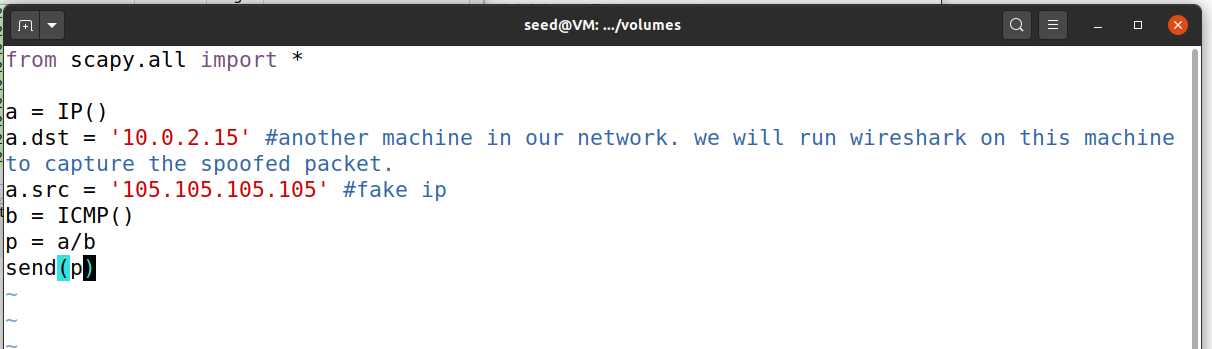
תפיסת פקטה מ subnet:



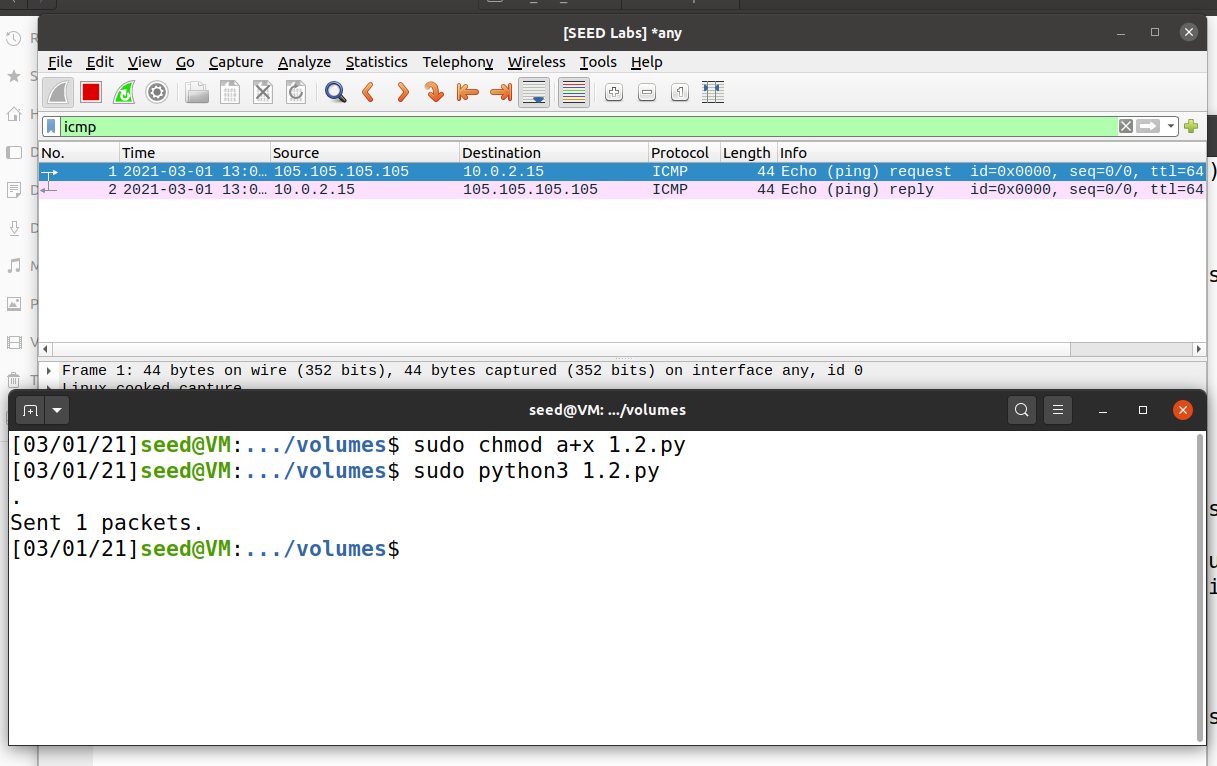
1.2:

אנחנו צריכים לעשות spopfing לפקטת icmp לכן אנו נשלח באמצעות scapy פקטת ping מip שהוא לא של האינטרפייס שאנחנו משתמשים לאינטרפייס אחר ברשת שלנו ואנו נבדוק בwireshark שאכן האינטרפייס השני לא רואה שהפקטה נשלחה מהאינטרפייס השני.

הקוד:



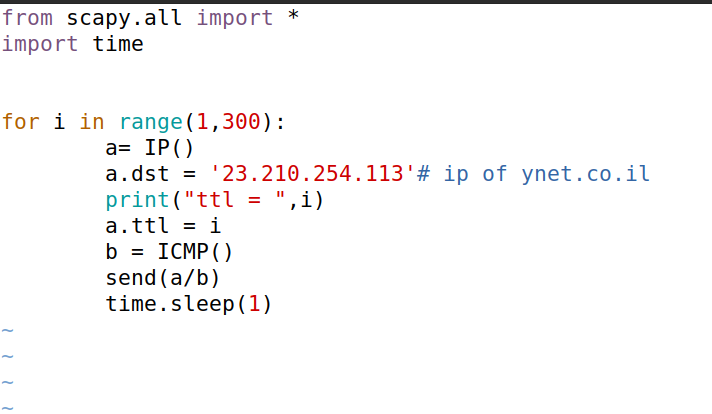
התהליך:



ואכן זה נשלח מהip של המזוייף ונשלח response למזוייף.

1.3:

התבקשנו לבדוק כמה ראוטרים אנו עוברים עד שאנו מגיעים ליעד,ע"פ ההדרכה עלינו להגביל את זמן החיים של הפקטה ולראות בכל פעם שיש לה error מסוג time-to-live has exceeded (הזמן שלה נגמר אך ללא השלמת המשימה) נבדוק באיזה ip של ראוטר היא עצרה, נרוץ בלולאה וכל פעם נעלה את הttl באחד ונספור כמה ip שונים אנו עוברים עד שאנחנו כבר לא מקבלים שגיאה.



קיבלנו 13 הודעות שגיאה מ13 ראוטרים שונים כלומר עברנו 13 ראוטרים עד היעד.

