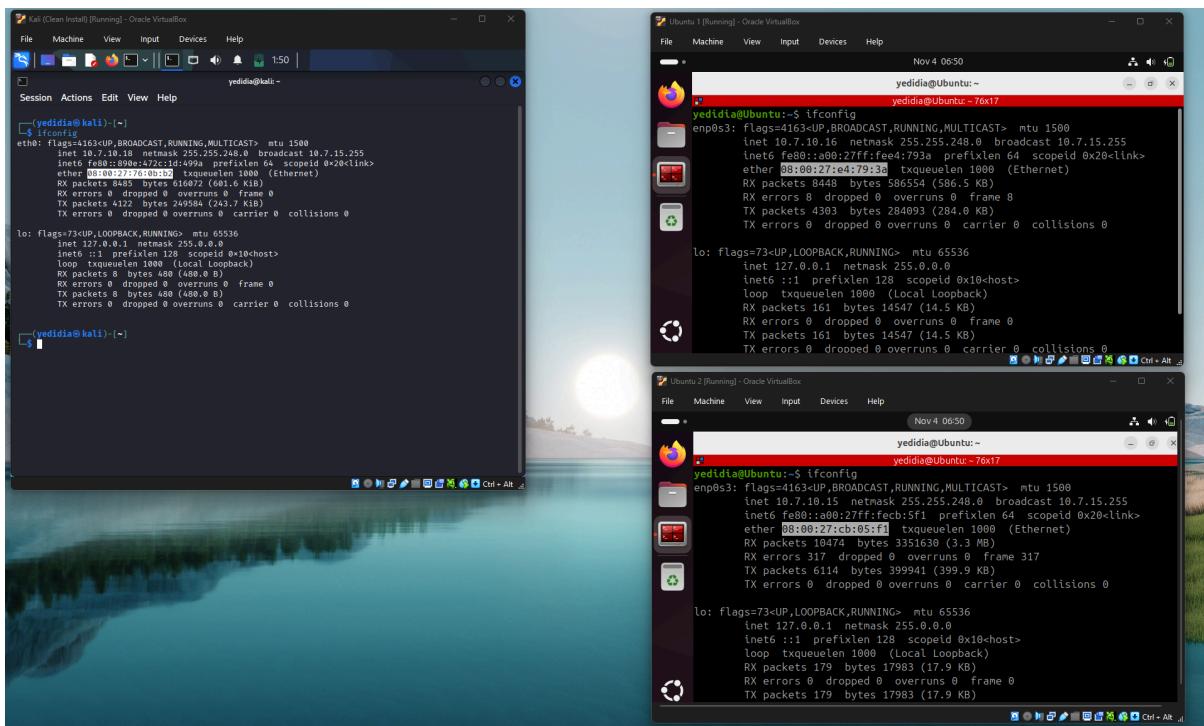


תרגיל 2 - ARP Spoofing

- ידידה בקורדזה 332461854
- מאיר קרומבי 214736688

בתרגיל זהה יצרנו קרייפט בפייתו שמאפשר לנו לבצע התקיפות ARP "ולעבוד" על מחשבים שונים ברחבי רשת LAN בכר שנגרים להם להאמין שהמחשב שלנו הוא מישחו שהוא לא ידי שליחת הודעת ARP Reply שאומרות שהמחשב עם כתובת MAC של התקוף הוא המחשב בעל כתובת IP שאנו חנו רוצים להתחזות אליה.

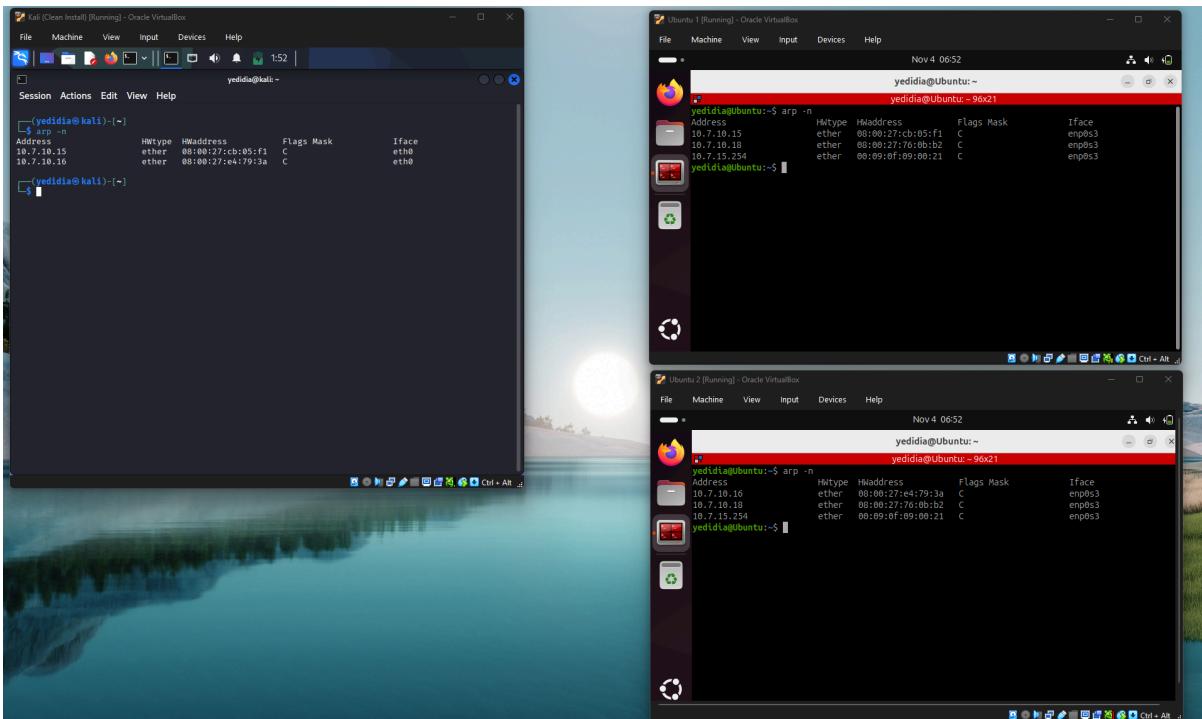
נפעיל 3 מכונות ב-VirtualBox, אחד עבור התקוף ו-2 נוספים עבור הפרטים שנעבד עליהם.
להלן תמונה המציג כל אחד מהמחשבים



או בתיאור פשוט:

התוקף	פרaicir 2	פרaicir 1
כתובת MAC	08:00:27:76:0b:b2	08:00:27:76:0b:b2
כתובת IP	10.7.10.18	10.7.10.15
כתובת gateway		10.7.15.254

נ裏 את פקודות ח-arp כדי לראות את המיפוי של כל אחד מהמחשבים:

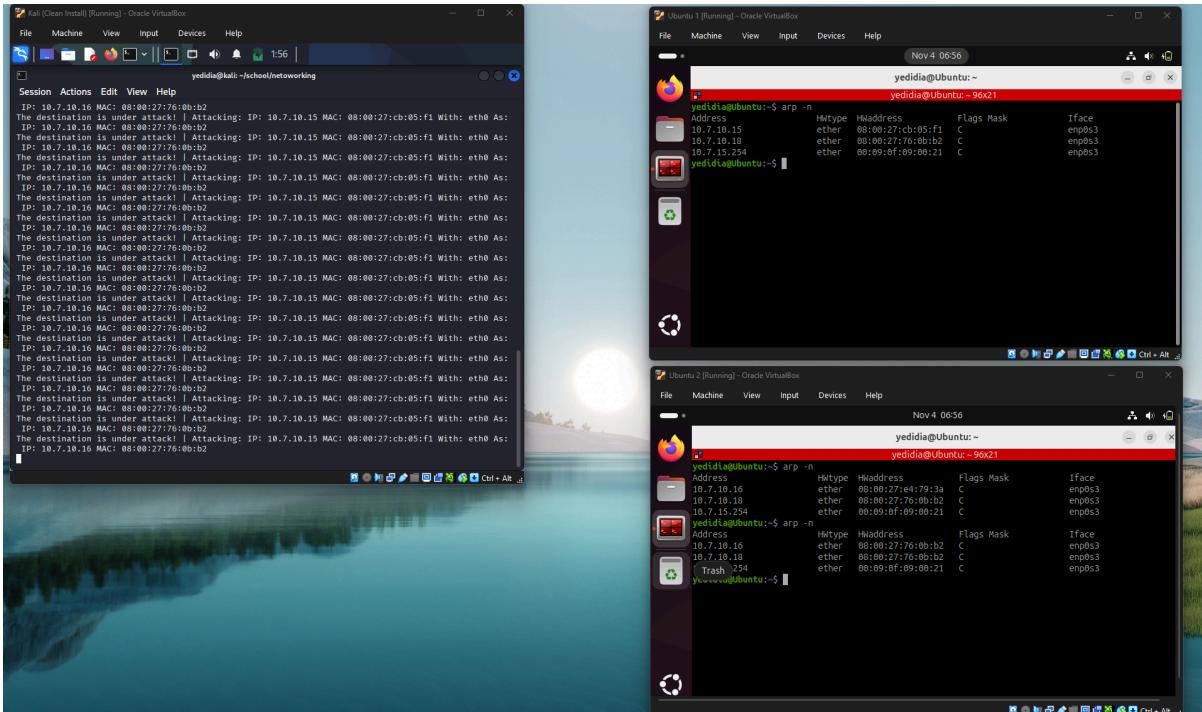


כלומר ניתן לראות שהמייפויים של כתובות MAC למכשירים לפי כתובות IP תקין. בעת נחילה לפקש את העניינים, בשלב הראשון נרצה לגרום למחשב השני להכיר במחשב התקוף אליו הוא המחשב המקורי. ככלומר, הנשלח מההתקוף והודעת למחשב השני, שמכילה פקעת ARP Reply שכתובת IP מקורה שלה הוא הכתובת IP של המחשב המקורי, ואילו כתובת MAC שבאותה פקטה תהיה כתובת MAC-ה של המחשב התקוף.

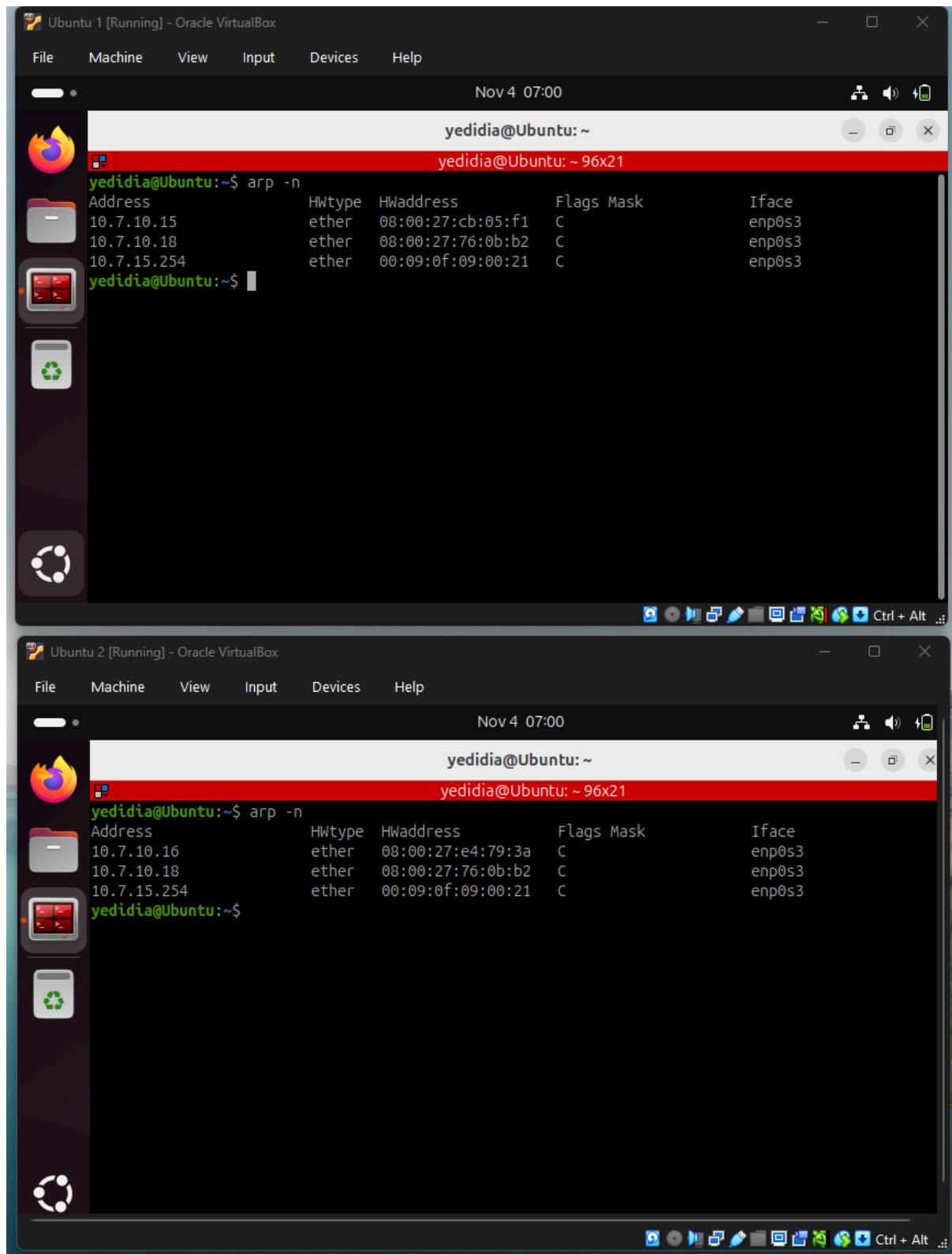
נריץ את הפקודה הבאה:

`sudo python3 ./arp_spoof.py -s 10.7.10.16 -t 10.7.10.15`

וכפי שאפשר לראות, אכן הטבלה השתנתה אצל הפראייר השני:



כעת כתובות 10.7.10.16 מוגדרת עם כתובת ה-MAC של המחשב התוקף.
עד כה, זה היה לכיוון אחד. כתעת נרצה גם לעדכן את כתובת ה-MAC של הפהאייר הראשון.
לכוארה נוכל לבצע את זה על ידי הרצת סקרייפט נוסף כך שנחננו הופכים את כתובת Src וה-target Able
בתוך הסקרייפט שיצרנו ניתן לבצע את הפעולה הפешטה הזאת עם ידי הוספה הדגל `-w`
נכבה את הרצת הסקרייפט, ונבחן את המצב שוב מהתחלה:



וכעת, נריץ את הפקודה הבאה:

```
sudo python3 ./arp_spoof.py -s 10.7.10.16 -t 10.7.10.15 -gw
```

ולבסוף התוצאה:

The figure consists of three side-by-side screenshots of terminal windows from different operating systems. The top-left window is from Kali Linux (Ubuntu 12.04) and shows the command being run. The other two windows are from Ubuntu 14.04. The middle window shows the output of 'arp -n' before the attack, and the bottom window shows the output after the attack has been run. Both show the MAC addresses of the target and gateway interfaces.

Interface	Address	Hwtype	Hwaddress	Flags	Mask	Iface
eth0	10.7.10.16	ether	00:00:27:e4:79:3a	C	enp0s3	
eth0	10.7.10.18	ether	00:00:27:76:0b:b2	C	enp0s3	
eth0	10.7.10.254	ether	00:09:0f:09:00:21	C	enp0s3	

Interface	Address	Hwtype	Hwaddress	Flags	Mask	Iface
eth0	10.7.10.16	ether	00:00:27:e4:79:3a	C	enp0s3	
eth0	10.7.10.18	ether	00:00:27:76:0b:b2	C	enp0s3	
eth0	10.7.10.254	ether	00:09:0f:09:00:21	(Incomplete)	enp0s3	

וכפי שניתן לראות, הגדרנו את כתובת ה-MAC של המחשב התקוף בטלנות של המחשבים הנתקפים. אצל המחשב הראשון הגדרנו את כתובת ה-MAC בטבלה תחת ההגדרה של הנתונים של המחשב השני (בעל כתובת ה-IP של 10.7.10.15) ואילו במחשב השני הגדרנו את כתובת ה-MAC של התקוף בטבלה תחת הגדרת הנתונים של המחשב הראשון (בעל כתובת ה-IP של 10.7.10.16).

נ.ב. ניתן לראות זאת במושך כי כתובת המחשב התקוף היא 10.7.10.18 ונitin לראות כי כתובת ה-MAC שלו דומה לשתייה בהתקפה.

כעת נרצה לבדוק מה אורך הדילאי - התשובה היא שאין תשובה חד משמעית. יש טימר כלשהו קבוע שהמערכת מגדרה אבל יש משתנים שכל פעם מתווספים אליו כמו ג'יטר ומצב הקרייה (הוא משתנה בין לינוקס ווינדוס אבל בקAli הוא 30 שניות) ולכן אין תשובה חד משמעית.