**יסודות לאבטחת רשתות – תרגיל 1 – DHCP Starvation**

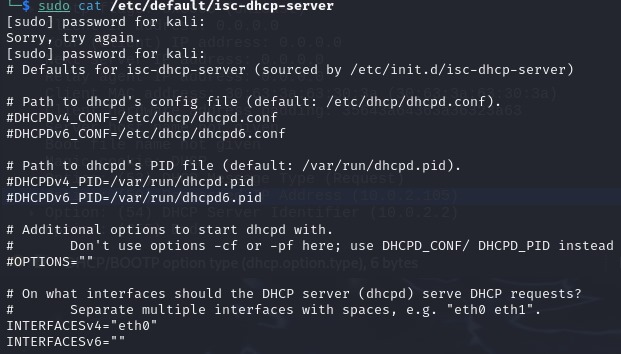
**מגישים:** אוריאל דולב 215676560, יהל קולר 214737728

Setup:

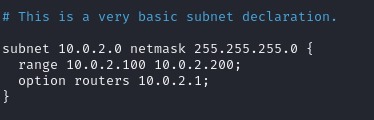
יצרנו שתי מכונות kali, אחת עבור ה-dhcp server והשניה עבור התוקף (ועבור בדיקה שאכן התקיפה עבדה ע"י בקשת כתובת ip ללא מענה לאחר הרצת התקיפה).

לאחר מכן, קינפגנו את ה-dhcp server באופן הבא:

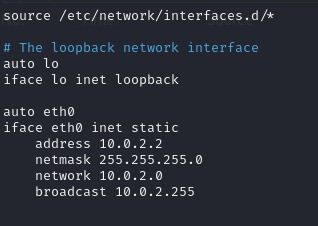
1. הגדרנו ל-dhcp את ה-default interface דרכו הוא יתקשר (eth0 במקרה שלנו) בקובץ /etc/defaults/isc-dhcp-server



1. הגדרנו את הערכים הרלוונטיים של ה-subnet בה ה-dhcp פועל ואת מרחב הכתובות אותן הוא יכול לחלק ברשת בקובץ /etc/dhcp/dhcpd.conf

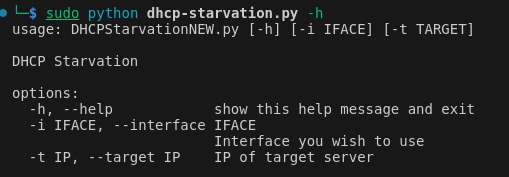


1. מכיוון שאנחנו פועלים ברשת פנימית, אין עוד dhcp servers והמכונה של ה-dhcp server צריכה בכל זאת לקבל ip איכשהו (הבהרה: כשלא עשינו את זה, זה כן עבד אבל לקח ל-server המון זמן לענות לבקשות. אנחנו משעירים שהסיבה לכך היא שלאחר קבלת הבקשה השרת ניסה להבין מה הכתובת שלו כדי להחזיר תשובה ובעצם היה צריך לבקש מעצמו את ה-ip מה שלקח זמן). אז הגדרנו לשרת ה-dhcp כתובת ip סטטית ברשת שלנו בקובץ /etc/network/interfaces



התקיפה:

הגדרות כלי התקיפה:

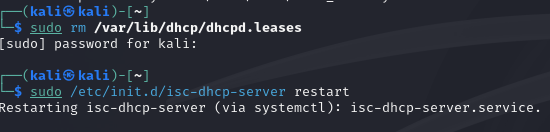


מהלך התקיפה יהיה כדלהלן:

1. נשלח בקשת DHCP פיקטיבית מבמחשב שלנו ונשתמש ב-OFFER שקיבלנו בחזרה כדי לדעת את ה-subnet mask, ובמקרה שלא קיבלנו ב-command line את ה-target, נשתמש ב-IP של ה-server שענה ראשון לבקשת ה-Discover.
2. על פי הגדרות ה-subnet, נרוץ על כל הכתובות ברשת המקומית ועבור כל אחת, נשלח בקשת DISCOVER ובקשת REQUEST עבור ה-IP המבוקש עם MAC פיקטיבי רנדומלי. (גילינו שעבור כתובות IP שלא נמצאות בקובץ הleases של השרת, הוא לא מאפשר לקבל אותן אלא אם מגיע ביחד עם הREQUEST גם בקשת DISCOVER).
3. כתוצאה מכך, השרת יאתחל lease עבור כל אחת מכתובות הMAC הפיקטיביות, עבור הIP שהיא ביקשה (בהנחה והכתובת הזאת פנויה) ובעצם, כל הכתובות שהשרת יכול לספק יתפסו, ולא יתאפשר ללקוחות אחרים לגשת אליו (הוא לא ישלח OFFER כתגובה לDISCOVERים).

הדגמת המתקפה:

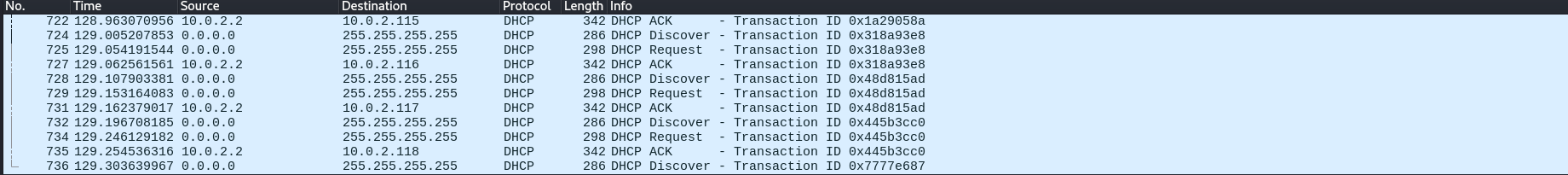
1. ראשית, למען הסדר, נמחק את קובץ ה-leases ונאתחל את השרת:

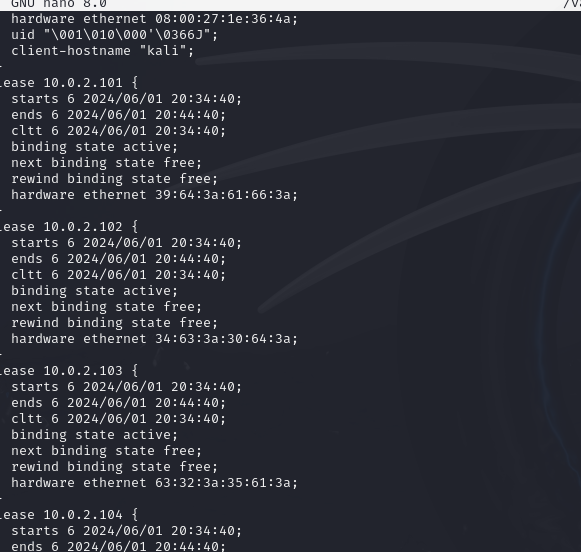


לאחר מכן, נפתח את התוקף ונפעיל אותו לתקוף את השרת:

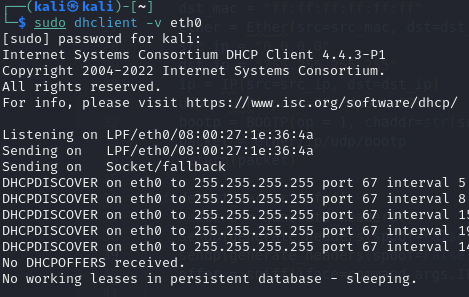


נסתכל ב-wireshark ונראה שנשלחות להן הבקשות והן מקבלות תשובה:



ולאחר שהוא סיים נוכל להסתכל בleases ולראות שהוא תפס את הכל:  


ואם עכשיו ננסה להשיג כתובת חדשה מהשרת:

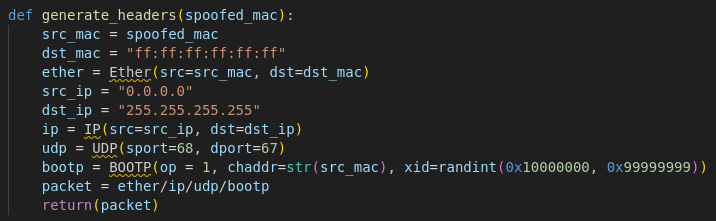


הוא ממשיך לנסות ולא מקבל תשובה.

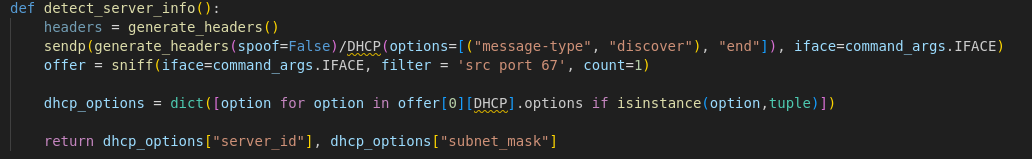
כלומר הצלחנו לתקוף את השרת ולמנוע את שירות ה-DHCP.

הסבר הקוד:

1. ראשית – יש לנו פונקציה שמטפלת בכל השכבות ומאפשרת לנו לדאוג רק ל-DHCP.



1. לאחר מכן אנחנו משיגים את המידע על השרת, הוא ישמש כדי לדעת את טווח הכתובות לתקוף וכדי לדעת את ה-target במקרה ולא הגדרנו אותו.



1. אנחנו מגדירים את התקיפה: אנחנו נרוץ על כל אחד מהכתובות שנתונות לנו(במקרה של persist יהיה מדובר בכתובות שהגשנו ובמקרה של הattack מדובר פשוט בכל הכתובות ברשת) אם זאת הפעם הראשונה שאנחנו תוקפים אנחנו נבצע discover ונבקש את הIP שהוא נותן לנו, אחרת נרוץ על הכתובות שכבר יש לנו וכל פעם נחדש אותן.



1. ולאחר מכן מתקיפים את המטרה הרצויה: נתחיל מלתקוף את כל הכתובות ברשת ונשמור את צמדי ה-mac/IP שהצלחנו להשיג, ואם אנחנו תוקפים במצב persist אנחנו נבקש את הכתובות הללו בכל פעם שה-lease ייגמר.

