**מטלת הרצה 1 : הרעלת ARP** ARP cache poisoning attack, גרסה 2.2

קישור למעבדה : https://seedsecuritylabs.org/Labs\_20.04/Files/ARP\_Attack/ARP\_Attack.pdf

<https://seedsecuritylabs.org/Labs_20.04/Networking/ARP_Attack/>

יש להריץ את המעבדה ולהגיש דו"ח+צילומי מסך, ע"פ הנחיות כלליות להגשת דו"ח משימה :

יש לודא טקטס קריא גם בתמונות. יש לצרף קוד פיתון מתועד כולל שמות המגישים. יש להגיש גם רשימת קבצים מוגשים.

צילומי המסך יהיו קריאים וממוספרים. (מספר רץ ואו שם משמעותי לכל צילום )

צילומים ושירטוטים יוגשו הן ב תוך דו"ח והן בנפרד. הגשה עי קובץ ZIP במודל. דוח במסמךMSWORD DOCX .

יש לתת שמות משמעותיים למחשבים , ל DOCKER IMAGES ולinterfaces . Attacker, Victim etc

כל תת משימה : תתחיל עם כותרת ותכלול תיאור מיבני של 4 פיסקאות:

**.1) מבוא : רקע תאורטי קצר**

שרטוט רשת התקשורת +כתובות + פרוט ציודים (עם שמות משמעותיים ע"פ תפקיד)

תאור קצר של כל הצעדים והפעולות שהתבצעו ,כולל קוד פיתון מתועד.

מטרות ומטרות הצעדים , תוצאות שהתקבלו מול תוצאות מצופות.

**2) תיעוד ביצוע המשימה :**   
 כולל צילומי מסך עם הסבר , סימון תוצאות והדגשות בצילומי המסך.

יש לרשום לכל צילום מסך לאיזה צעד ולאיזה מחשב/ציוד/דוקר שייך והאם לפני ביצוע ואו אחרי ביצוע.

מסקנות.   
  
**3) סיכום השלב** . יש לתת מענה קצר ל :   
 האם הושגה המטרה ?

איך וידאתם בדקתם (פקודות + פלט) את השגת המטרות.   
 מומלץ תיעוד עם WireShark . יש לשמור קבצי Pcap   
 האם זה תואם לתיאוריה ?  
 האם היו קשיים מיוחדים וכיצד התגברתם עליהם?

**4) מבט להמשך:**   
 יש להציע נקודות נוספות לבדיקה או בדיקה מתקדמת יותר במסגרת תת-תחום זה.

**הערות בנוגע ל תוכנות:   
יש אופציה לצילום מסך של מכונה בתוך תפריטי ה VirtuakBox**

**צריך ללמוד לעבוד עם דוקרים.**

**ניתן להוריד תוכנת Visio מלאה עם רשייון מפורטל הסטודנטים של AZURE תחת סעיף Educational Software .**

**בהצלחה מרדכי ח**