**דומנטציה - ARP Spoofing**

פרוטוקול ARP: ממפה כתובות IP לכתובות MAC ברשת המקומית (LAN)

ARP Spoofing: התקפה המנצלת את חוסר האימות ב – ARP על ידי שליחת הודעות ARP response **מזויפות רבות.** הודעות אלו גורמות לקורבנות לקשר כתובת IP עם כתובת MAC מזויפת.

תוצאות של ההתקפה:

* מניעת שירות DOS
* Session hijacking
* MITM

מימוש: שליחת הודעות ARP Response מהתוקף לקורבן המכילות את כתובת ה-IP של ה-Default Gateway אך עם כתובת ה-MAC של התוקף ל-MITM מלא נדרש גם זיוף כלפי ה-Gateway.

שימוש בסיפריית scapy מאפשרת שימוש נוח בממשקי הרשת הסנפה שליחה של חבילות ניתוח שדות החבילה ושימוש פשוט פרוטוקולים.

מדוע שולחים כמות גדולה של ARP Response מזויפות?על מנת לשמור על הcache של הקורבן במצב הרצוי

**אלטרנטיבה? להאזין לבקשות ARP ברשת ולהגיב עליהן כמובן עם שינוי הפקטה להתאים אותה לspoof הרצוי בדרך זו נוכל להסתיר משמעותית את המתקפה גם באמצעות שליחת כמות הגיונית של בקשות**

**אז למה לא? זה עובד פחות טוב קצב השליחה לא מהיר מספיק והנמען האמיתי מספיק להגיב ובכך הקשר נמנע בצורה חלשה יותר**

A screenshot of a computer program

AI-generated content may be incorrect.

תוצאה – לאחר שביצאתי spoof דרך מכונת kali linux באמצעות הכלי שיצרתי על מכונת וינדואוס 10 אפשר לראות

ה – Ip של הdefault gateway כלומר הנתב שהכיל כתובת mac כלשהי בהתחלה השתנה לכתובת הmac של מכונת הלינוקס שלי (התוקף)

