רשתות מחשבים מתקדם

תרגיל – פיתוח DNS Enumeration באמצעות Scapy

במשימה זו תממשו סקריפט פייתון שמבצע DNS enumeration

הסקריפט יקבל כפרמטר את שם הדומיין (לא באמצעות פקודת input). לדוגמה הרצת סקריפט תראה כך:

dnsenum.py jct.ac.il

הערה: ניתן לבצע את כל התרגיל אך ורק על IPv4, המטרה היא הדגמת הידע שלכם.

מוזמנים כמובן להוסיף גם IPv6 כרצונכם 😊

שלב א – מציאת שרת ה-DNS של ה-domain המבוקש

שאילתות מסוג SOA – Start Of Authority – מכילות מידע ניהולי על הדומיין.

לדוגמה, להלן מענה לשאילתא שבוצעה על jct.ac.il:

```
C:\Users\BARAK>nslookup -type=SOA jct.ac.il
Server:  UnKnown
Address:  2a0d:6fc2:131c::1

Non-authoritative answer:
jct.ac.il
        primary name server = dns.jct.ac.il
        responsible mail addr = hostmaster.jct.ac.il
        serial  = 2024022900
        refresh = 43200 (12 hours)
        retry   = 7200 (2 hours)
        expire  = 2419200 (28 days)
        default TTL = 86400 (1 day)
```

באמצעות scapy, צרו פקטת DNS מסוג SOA. הוציאו מהתשובה את שרת ה-DNS של ה-domain המבוקש.

שלב ב – התנסות בכלי dnsmap

יש להשתמש ב-linux או ב- WSL (מומלץ עקב פשטות ההתקנה).

הורידו את הכלי dnsmap, המשמש בודקי חדירות (pentesters). קיראו למה הוא משמש. השתמשו בו תוך כדי הסנפת wireshark.

```
sudo apt install dnsmap

dnsmap jct.ac.il
```

חיקרו את ההסנפה וענו לעצמכם על השאלה- כיצד הצד המקבל יודע אם הדומיין המבוקש קיים או לא?

שלב ג – הכנת קובץ עם אפשרויות לניסוי

הורידו את הקבצים dnsmap.h ואת wordlist_TLAs.txt

https://github.com/makefu/dnsmap/blob/master/dnsmap.h

https://github.com/makefu/dnsmap/blob/master/wordlist_TLAs.txt

העתיקו מהם לתוך קובץ בעל שם כרצונכם את מילות הניסוי המבוקשות. אתם יכולים להוסיף מילות ניסוי כרוחכם הטובה.

שלב ד – יצירת סקריפט פייתון dnsenum

צרו סקריפט פייתון שמשתמש בקובץ עם מילות הניסוי שיצרתם כדי לבצע מיפוי של דומיין נבחר ומיצאו אילו שרתים יש בו, ומה כתובות ה-IP שלהם.

לטובת קבלת ניקוד מלא:

- שם הדומיין המבוקש יתקבל כפרמטר לסקריפט, לא באמצעות הפונקציה input
- עליכם לפנות לשרת ה-DNS של ה-domain המבוקש, כפי שמצאתם בסעיף א. לא לשרת DNS כללי כלשהו (נסו ותווכחו שיש הבדלים בתשובות)
- לכל שם של שרת הקיים ב-domain המבוקש עליכם להדפיס את שם השרת ואת כתובות ה-IP גרסא 4 שלו
- עליכם להוציא את כלל כתובות ה-IP שיש לשרת מסויים. לדוגמה, חקירה של jct.ac.il צריכה להראות כי לשרת mail.jct.ac.il ישנן מספר כתובות IP

בהצלחה!