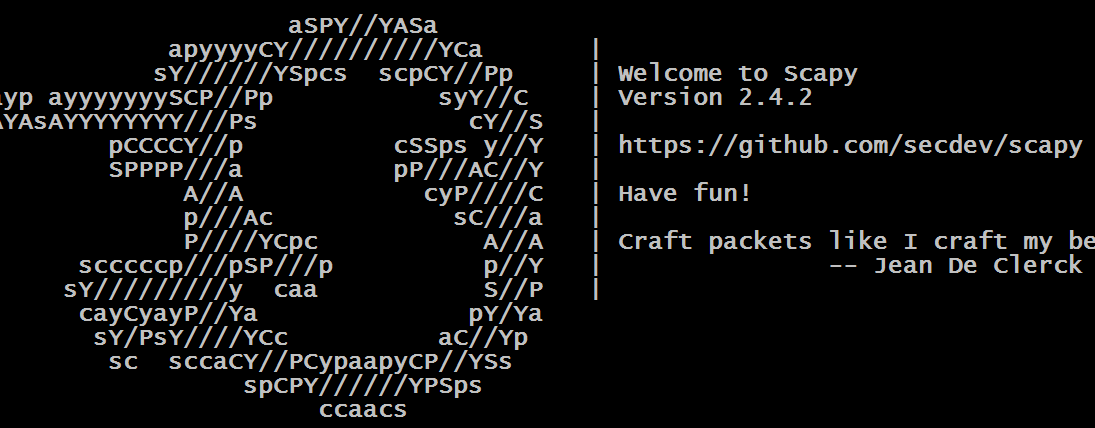
שיעור 6 – סקאפי

**להכיר את סקאפי מקרוב**

בתרגיל זה נתחיל לשחק עם הטרמינל של סקאפי. נעבוד על הסנפה בסיסית ועל בניית חבילות פשוטות ושליחתן.

1. **פתיחת הטרמינל של סקאפי**
2. במסך ההפעלה (Start->Run) יש לכתוב scapy.
3. אם זה לא עובד, נסו להיכנס ל-cmd ולכתוב שם scapy.
4. אם זה עדיין לא עובד – קראו למדריכ/ה.
5. המסך הבא אמור להופיע:



1. **יצירת הודעת IP**
2. הציגו את רשימת כל הפרוטוקולים באמצעות ls.
3. כתבו שלושה פרוטוקולים שאתם מזהים אשר למדנו עליהם השנה.

|  |
| --- |
| UDP, TCP, IP |
|  |

1. בעזרת פקודת ls, בדקו מהם השדות בפרוטוקול IP.
2. צרו הודעה (שכבה) של IP ושימו אותה במשתנה חדש בשם ipmsg.
3. בעזרת הפונקציה show, צפו מה יש בתוך ההודעה.
4. מהן הכתובות שסקאפי הכניס בצורה אוטומטית לתוך הודעת ה-IP?

|  |
| --- |
| 127.0.0.1 לכתובות מקור ויעד |
|  |

1. אחת מהכתובות כאן נכונה והגיונית, ואילו השניה חסרת משמעות. הסבירו מדוע לדעתכם זה כך.

|  |
| --- |
| לי שתי הכתובות היו אותו הדבר, אבל הכוונה היא (אני מנחש) שאנחנו לא יודעים את היעד לכן אין לכתובת הזו משמעות- אנחנו צריכים להכניס אותה אבל המקור הוא פשוט אנחנו |
|  |

1. נסו לשנות את כתובת היעד, לכתובת IP / דומיין של גוגל. מהי הפקודה שהקשתם כדי לשנות את כתובת היעד? ואיך בדקתם שהשינוי אכן הצליח?

|  |
| --- |
| ipmsg.dst = "142.250.186.142"  ipmsg.show() |
|  |

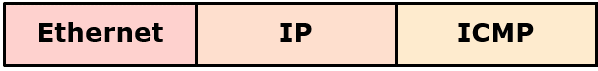
1. שנו את שדה ה-TTL ל-128 באותה צורה.

|  |
| --- |
| Ipmsg.ttl = 128 |
|  |

1. כעת יש לנו שכבת IP מוכנה לשליחה לגוגל!
2. **יצירת הודעת ICMP**
3. באותה צורה שעבדנו עם שכבת IP, צרו הודעת ICMP ושמרו אותה למשתנה icmpmsg.
4. כזכור, ב-ICMP יש מגוון סוגי הודעות. אנחנו מעוניינים ליצור הודעה מסוג Echo Request (הלא הוא בקשת פינג). בדקו שהחבילה שברשותכם היא אכן מסוג זה.
5. **יצירת הודעת Ethernet**
6. צרו הודעת Ethernet (נקרא Ether בסקאפי) ושמרו אותה למשתנה גם כן.
7. מהן הכתובות MAC שנמצאות כעת בהודעה?

|  |
| --- |
| כתובת ברודקאסט ביעד והכתובת שלנו במקור |
|  |

1. אל תשנו את הכתובות – הן ישתנו לבד בהמשך.
2. **יצירת חבילה שלמה**
3. כעת נרצה לייצר הודעת ICMP שלמה הכוללת את כל השכבות – Ethernet + IP + ICMP.



1. יש לחבר את 3 המשתנים בעזרת האופרטור **/** ולשמור את התוצאה במשתנה fullmsg.
2. כעת נצפה בנתונים של fullmsg. מה קרה לכתובות ה-MAC בשכבת הקו כעת? מדוע לדעתכם רק עכשיו התעדכנו כתובות ה-MAC?

|  |
| --- |
| הכתובת מאק השתנתה (כנראה לזו של הראוטר) כי שינינו את היעד של החבילה (האייפי כרגע) והחבילה צריכה מאק חדש |
|  |

1. **שליחת החבילה וקבלת תשובה**
2. מכיוון שהחבילה שלנו היא בשכבה 2, נשתמש בפונקציית השליחה **srp1.**

(אם החבילה שלנו היתה בשכבה 3 (מתחילה מ-IP), היינו משתמשים בפונקציה sr1.)

1. בעזרת srp1, שלחו את החבילה ואספו את התשובה למשתנה ans.
2. הציגו את הפרטים על החבילה שחזרה בעזרת show() ו-summary(). מהי הודעת ה-ICMP שחזרה מגוגל (מהו שם ההודעה)?

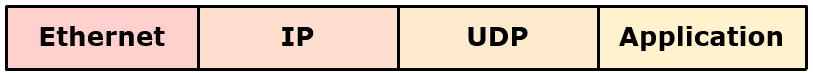
|  |
| --- |
| זה לא עבד לי עד שהוספתי טקסט רנדומלי כעוד שכבה בהודעה. שם ההודעה היה echo-reply |
|  |

1. **שליחת הודעה עם TTL נמוך**
2. צרו חבילה זהה לסעיף הקודם מלבד שינוי אחד – שימו TTL נמוך, למשל 3.
3. שלחו את החבילה. מה קיבלתם בתשובה?

|  |
| --- |
| time-exceeded ttl-zero-during-transit |
|  |

1. **שליחת הודעה לשרת ההדים**

כעת נרצה ליצור עם פרוטוקול טקסטואלי מעל UDP. לשם כך מבנה החבילה שלנו צריך להיות כזה:



כדי להוסיף טקסט חופשי בתור פרוטוקול, פשוט נוסיף שכבה שהיא סטרינג בלבד. למשל

**Fullmsg = Ether() / IP() / UDP() / “Helllllo!”**

כתבו הודעה לשרת 34.218.16.79 בפורט 100, ושלחו לו את שמכם. האם הצלחתם לקבל תשובה?  
כתבו איזה פקודה עליכם לכתוב כדי להדפיס את הטקסט שחזר מהשרת:

|  |
| --- |
| לא הצלחתי לקבל תשובה שהיא לא שגיאה, הוא כתב לי שהפורט ביעד הוא unreachable |
|  |

לא הצלחתם לקבל תשובה ואתם רואים רק הרבה נקודות? נסו לבדוק את אחת מהבעיות הנפוצות הבאות:

|  |  |
| --- | --- |
| **בעיה** | **פתרון** |
| בדקו מהו פורט המקור בחבילה שיצרתם. אם הוא 53 (domain) הרי ש-scapy קבע אותו אוטומטית ל-DNS וזה לא מאפשר לסקאפי לקבל את התשובה. | קבעו בעצמכם את פורט המקור למספר אקראי לבחירתכם. בחרו מספר גדול בן 4-5 ספרות. |
| יש מספר ממשקי רשת זמינים ויכול להיות שסקאפי משתמש בממשק הלא נכון. | בדקו את src ip של החבילה שיצרתם. האם זה ה-src ip של הרשת wifi שאתם רוצים להשתמש בה? אם לא, לכו למסך ממשקי הרשת (start->run-> ncpa.cpl) ובצעו disable לכל הממשקים שאינם ה-Wifi שלכם. |

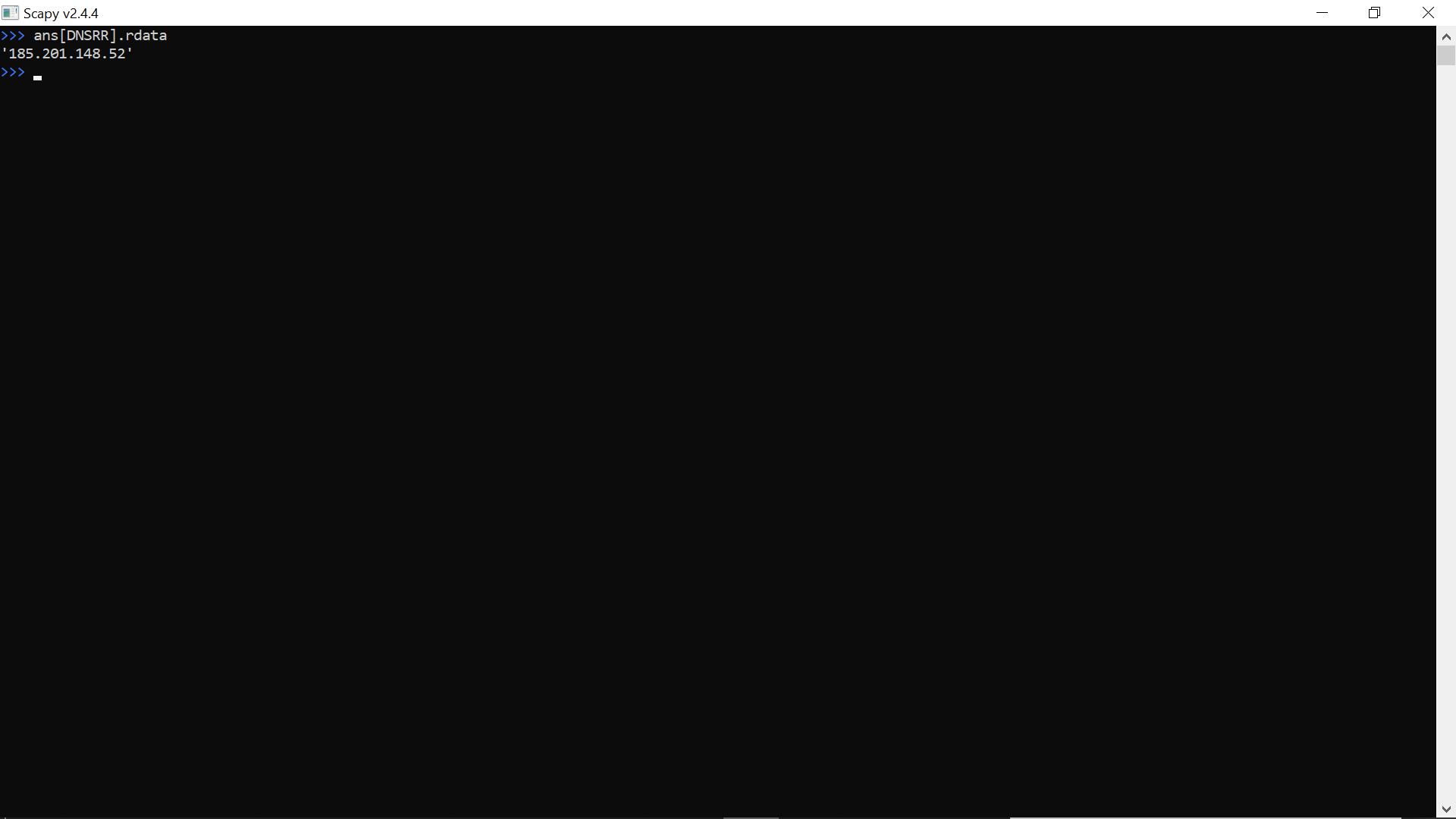
1. **שליחת בקשת DNS**

כעת ניצור בקשת DNS ונשלח אותה באמצעות סקאפי. בעזרת בקשת ה-DNS ננסה למצוא את ה-IP של האתר **cyber.org.il**.

חשבו מהו המבנה הנכון של חבילת DNS וצרו אותו. הוסיפו את הנתונים הנחוצים לכל השכבות – IP יעד בשכבת הרשת, פורט מקור ויעד בשכבת התעבורה, ופרטים על השאילתא בשכבת ה-DNS. כדי ללמוד אילו נתונים בדיוק יש להוסיף ל-DNS, היעזרו בגוגל.

נסו לשלוח את החבילה שלכם לשרת ה-DNS של גוגל – 8.8.8.8. האם התקבלה תשובה?

חפשו היכן נמצא המידע המעניין של התשובה, כלומר ה-IP של cyber.org.il, והדפיסו אותו לבדו. לסעיף זה, אל תיעזרו בגוגל! צרפו צילום מסך של פקודה המדפיסה את ה-IP לבדו.



1. **איסוף של ציטוטים יומיים**

שרת ה-UDP הנמצא בכתובת djxmmx.net (פורט 17) מספק ציטוט מפורסם לכל דורש (לא משנה מה כותבים בבקשה עצמה). כתבו קוד פייתון בתוך הטרמינל של סקאפי, אשר מבקש 10 ציטוטים ברצף (בעזרת לולאה), ומדפיס את כולם למסך.  
טיפ: אם תרצו שלא יודפס שום דבר למסך מלבד הדפסות שלכם, השתמשו ב:

**ans = srp1(fullmsg, verbose=0)**

1. **פענוח JSON משרת UDP**

את התרגיל הבא נבצע בקובץ פיתון py ולא מהטרמינל. לשם כך נכתוב את הייבוא הבא בראשית הקובץ:

**from scapy.all import \***

שאר הפקודות עובדות בדיוק אותו דבר כפי שהתנסינו בטרמינל.

שרת ה-UDP הנמצא בכתובת 34.222.145.150 (פורט 789), מקבל את תאריך הלידה שלכם, ומחזיר מידע מעניין עליו, בפורמט של JSON.

בקשות לשרת צריכות לכלול את המידע הבא בשכבת האפליקציה:

**Day=11,Month=23**

כתבו תכנית אשר קולטת מהמשתמש את תאריך הלידה שלו ופונה לשרת. בעזרת הספריה json, היפכו את המידע לטיפוס של פיתון כך שיהיה לכם נוח לעבוד איתו. הדפיסו למשתמש את המשפט הבא:

Hey there, you were born in 12/12 – it’s the same birth date as Michael Jordan (age 56) and Barack Obama (age 61)! On your birth date in the year 2000 this happened: The release of Abbey Road album by the Beatles.

**\* שימו לב** שאנחנו לא מדפיסים את כל המידע שקיבלנו אלא רק שני אנשים ואירוע אחד מתוכו.