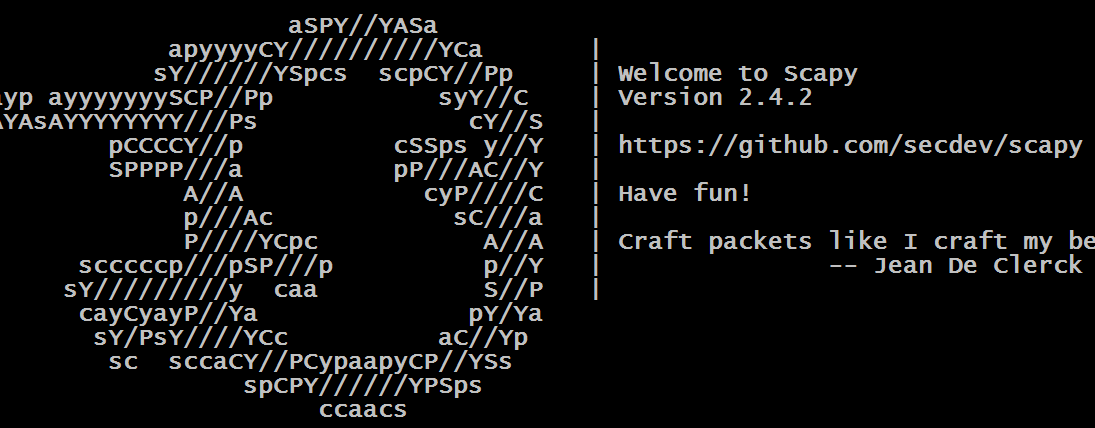
שיעור 6 – סקאפי

**להכיר את סקאפי מקרוב**

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

**לפני התחלת התרגיל יש לוודא כי סקאפי 3 הותקן כראוי, לפי ההוראות בשיעור 6 ב-EDU.**

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 למדריך.
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.

|  |
| --- |
|  |
| תשובה |

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?

|  |
| --- |
| Src IP = 10.0.0.3 (local ip address, depends on my Wifi) Dst IP = 127.0.0.1 |
| תשובה |

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

|  |
| --- |
| הכתובת מקור היא באמת הכתובת של המחשב שלי, אבל הכתובת יעד היא הכתובת של localhost. זה כך כי סקאפי לא יכול לדעת לאן אני רוצה לשלוח את החבילה... |
| תשובה |

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

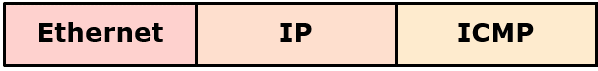
|  |
| --- |
| ipmsg.dst =”google.com”  כדי להציג כתבתי ipmsg.dst או ipmsg.show() |
| תשובה |

1. שנו את שדה ה-TTL ל-128 באותה צורה.

|  |
| --- |
| ipmsg.ttl = 128 |
| תשובה |

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?

|  |
| --- |
| dst= ff:ff:ff:ff:ff:ff (BROADCAST)  src= 00:00:00:00:00:00 |
| תשובה |

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

|  |
| --- |
| הכתובות MAC עכשיו אמיתיות!  מכיוון שהיעד ב-MAC תלוי ביעד הסופי שלי ב-IP. כעת סקאפי יכל לראות שהיעד הסופי שלי הוא לא בסאבנט שלי, ולכן הכתובת DST MAC היא ה-MAC של הראוטר שלי. |
| תשובה |

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.)

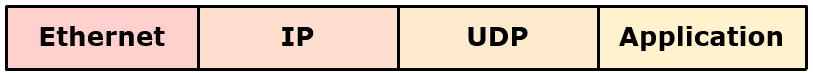
1. בעזרת srp1, שלחו את החבילה ואספו את התשובה למשתנה ans.
2. הציגו את הפרטים על החבילה שחזרה בעזרת show() ו-summary(). מהי הודעת ה-ICMP שחזרה מגוגל?

|  |
| --- |
| Echo-reply |
| תשובה |

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 בהודעת ICMP |
| תשובה |

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:

>> msg = Ether() / IP(dst="34.218.16.79") / UDP(sport=1123,dport=100) / ”Yossi”

>> ans = srp1(msg)

|  |
| --- |
| ans[Raw].show() |
| תשובה |

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.

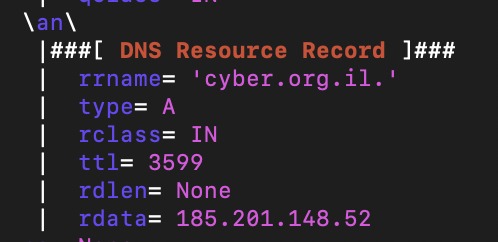
חשבו מהו המבנה הנכון של חבילת DNS וצרו אותו. הוסיפו את הנתונים הנחוצים לכל השכבות – IP יעד בשכבת הרשת, פורט מקור ויעד בשכבת התעבורה, ופרטים על השאילתא בשכבת ה-DNS. כדי ללמוד אילו נתונים בדיוק יש להוסיף ל-DNS, היעזרו בגוגל.

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.

תשובה:

>> msg = Ether() / IP(dst="8.8.8.8")/UDP(sport=3223,dport=53)/DNS(rd=1,qd=DNSQR(qname="cyber.org.il"))

>> ans = srp1(msg)

1. **איסוף של ציטוטים יומיים**

שרת ה-UDP הנמצא בכתובת djxmmx.net (פורט 17) מספר ציטוט לכל דורש. כתבו קוד פייתון בתוך הטרמינל של סקאפי, אשר מבקש 20 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)**

for i in range(20):

ans = srp1(fullmsg, verbose=0)

print(ans[Raw])