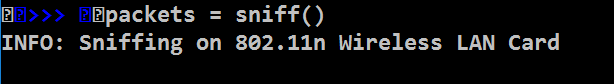
שיעור 07 – הסנפות עם סקאפי

**מסניפים בטרמינל סקאפי**

בתרגיל זה נכיר את פונקציית ההסנפה של סקאפי מתוך הטרמינל. נתנסה בעבודה עם החבילות שחוזרות מההסנפה, ונלמד כיצד מוצאים את מה שבאמת מעניין אותנו בתוך ההסנפה.

1. **משחקים קצת עם הסנפה של סקאפי**
2. פתחו את הטרמינל של סקאפי.
3. התחילו הסנפה באמצעות הפקודה

**packets = sniff()**

1. המסך הבא אמור להופיע:
2. בזמן שההסנפה מתבצעת, גלשו לאתר שלא נכנסתם אליו מזמן, למשל cnn.com.
3. חכו כ-20 שניות ולאחר מכן עצרו את ההסנפה עם Ctrl+C.
4. בעזרת הקשה של packets ו-packets.show() צפו בסיכום של ההסנפה וכתבו:

|  |
| --- |
| מספר חבילות TCP =  מספר חבילות UDP =  מספר חבילות כולל = |
| *תשובה* |

1. **ניתוח ההודעה הראשונה שהוסנפה**
2. שמרו במשתנה חדש את החבילה הראשונה שהוסנפה.
3. מהי החבילה הזאת? מהן השכבות (הפרוטוקולים) בחבילה הזאת?

|  |
| --- |
|  |
| *תשובה* |

1. האם זו חבילה נכנסת או יוצאת? איך הבנתם זאת?

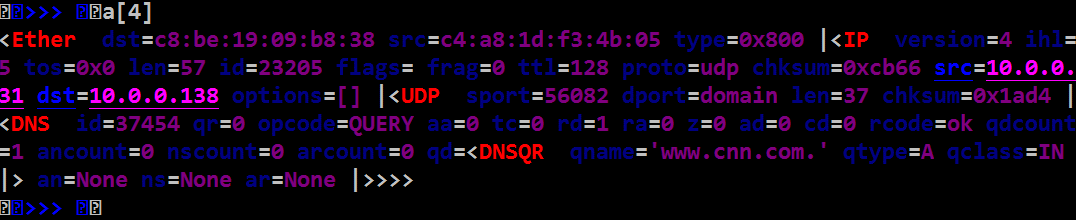
|  |
| --- |
|  |
| *תשובה* |

1. מהו הפרוטוקול בשכבת האפליקציה? (רמז: סקאפי לרוב לא מזהה בעצמו את שכבת האפליקציה)

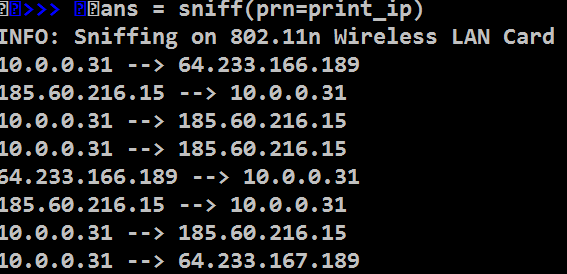
|  |
| --- |
|  |
| *תשובה* |

1. **מאתרים את חבילת ה-DNS**
2. כעת נרצה למצוא בעצמנו את חבילת ה-DNS שנשלחה ל-cnn.com. אם נרצה לעשות זאת ידנית, לעבור חבילה חבילה, זה יקח לנו שנה. חשבו על דרך מהירה יותר למצוא את כל חבילות ה-DNS בהסנפה. כתבו את הקוד שהקשתם כאן:

|  |
| --- |
| dns\_list = []  for p in packets:  if DNS in p:  dns\_list.append(p) |
| *תשובה* |

1. לאחר שהצלחתם למצוא את החבילה המיוחלת, צרפו צילום מסך שלה.
2. כעת כתבו שורה המדפיסה רק את האתר אשר ביקשנו משרת ה-DNS (המידע נמצא בתוך שכבת ה-DNS של החבילה שמצאנו).

|  |
| --- |
| dns\_list[4][DNSQR].qname |
| *תשובה* |

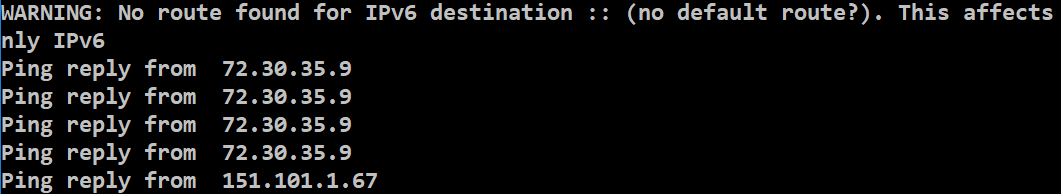
1. **שימוש בפונקציית עיבוד חבילות prn**
2. צרו פונקציה לעיבוד חבילות אשר מקבלת חבילה, ומדפיסה את IP המקור ו-IP היעד שלה בצורה כזאת: 10.0.0.1 -> 12.2.12.1 קראו לפונקציה print\_ip.  
   (אם שכחתם איך נקראים השדות של פרוטוקול IP, פשוט עיינו באחת מהפאקטות שברשותכם!)
3. בצעו הסנפה ללא הגבלת כמות, והוסיפו את הפונקציה שלכם בתור פרמטר prn.
4. בדקו שאכן אתם רואים את הפלט של כתובות ה-IP בצורה כזאת:  
   

def printer(packet):

if IP in packet: אם לא נכתוב את התנאי, התוכנה תקרוס באיזשהו שלב כאשר לא תהיה שכבת IP

print (packet[IP].src,"-->",packet[IP].dst)

ans = sniff(prn=printer)

1. **שימוש בפונקציית סינון + פונקציית עיבוד**
2. כעת נעבור לעבוד בקובץ קוד של פיתון.
3. בסעיף זה, ניצור פונקציות סינון ועיבוד המתייחסות רק ל-Ping אשר יוצאים מהמחשב שלנו.
4. צרו פונקציית סינון המסננת חבילות שיש בהן שכבת**ICMP** מסוג **Echo Reply.**(כדי לדעת איך לעשות את זה, מומלץ לבצע הסנפה בזמן שאתם מבצעים ping ולחקור חבילה אחת כזאת).
5. צרו פונקציית עיבוד אשר מדפיסה עבור כל חבילה כזאת את כתובת ה-IP ממנה היא הגיעה, בצורה הבאה :" Ping reply from <IP>"
6. התחילו הסנפה, ופתחו CMD נפרד ובצעו בו בקשות ping לאתרים לבחירתכם.
7. בדקו שאכן אתם רואים את הפלט מתעדכן בצורה כזו:

from scapy.all import \*

def filter(packet):

return (ICMP in packet and packet[ICMP].type==0)

def printer(packet):

print ("Ping reply from ", packet[IP].src)

ans = sniff(lfilter=filter, prn=printer)