Scapy

1 עבודה אינטראקטיבית – Scapy

1.1 הרצת scapy

פתחו את חלון ה command line

- הריצו את scapy

```
C:\Users\Ayelet Mashiah>
C:\Users\Ayelet Mashiah>
C:\Users\Ayelet Mashiah>
C:\Users\Ayelet Mashiah>
C:\Users\Ayelet Mashiah>
C:\Users\Ayelet Mashiah>
C:\Users\Ayelet Mashiah>
C:\Users\Ayelet Mashiah>
C:\Users\Ayelet Mashiah>scapy
```

-

```
INFO: Can't import matplotlib. Won't be able to plot.
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
WARNING: Wireshark is installed, but cannot read manuf !
WARNING: No route found for IPv6 destination :: (no default route?)
INFO: Can't import python-cryptography v1.7+. Disabled WEP decryption/encryption. (Dot11)
INFO: Can't import python-cryptography v1.7+. Disabled IPsec encryption/authentication.

                    aSPY//YASa
             apyyyyCY//////////YCa       |
            sY//////YSpcs  scpCY//Pp     | Welcome to Scapy
 ayp ayyyyyyySCP//Pp           syY//C    | Version 2.4.3rc3
 AYAsAYYYYYYYY///Ps              cY//S   |
         pCCCCY//p          cSSps y//Y   | https://github.com/secdev/scapy
         SPPPP///a          pP///AC//Y   |
              A//A            cyP////C   | Have fun!
              p///Ac            sC///a   |
              P////YCpc           A//A   | Craft packets before they craft
       scccccp///pSP///p          p//Y   | you.
      sY/////////y  caa           S//P   |                     -- Socrate
       cayCyayP//Ya              pY/Ya   |
        sY/PsY////YCc           aC//Yp
         sc  sccaCY//PCypaapyCP//YSs
                  spCPY//////YPSps
                       ccaacs
                                   using IPython 7.6.1
>>>
```

יופיעו מספר warnings אל תיבהלו, הכל בסדר....

1.2 הסנפה

הסנפה ב scpay מופעלת באמצעות הפקודה sniff . הפקודה מקבלת כפרמטר את מספר הפקטות שנרצה להסניף ומחזירה מחזירה סוג של dictionary ובו סוג הפרוטוקול הוא המפתח ומערך של רשומות מהפרוטוקול הוא הערך.

כתבו ב scapy:

packets = sniff(count=2)

```
>>> packets=sniff(count=2)
>>>
```

נבדוק את packets

הקלידו את הפקודות הבאות וכיתבו עבור כל פקודה מה התוצאה (הפלט)

פקודה	תוצאה
packets	
packets.show()	
Packets[1]	
Packets[1].show()	
packets[TCP]	
packets[TCP].show()	
packets[Ether]	
Packets[Ether].show()	

נסו להבין:

1. מה ההבדל בין הדפסה רגילה לפקודה show()
2. מה משמעות הגישה לפקטות עם סוגריים מרובעים ובתוכם מספר
3. מה משמעות הגישה לפקטות עם סוגריים מרובעים ובתוכם שם הפרוטוקול
4. מה יודפס בפקודה packets[TCP][0].show()

1.3 Fiilter

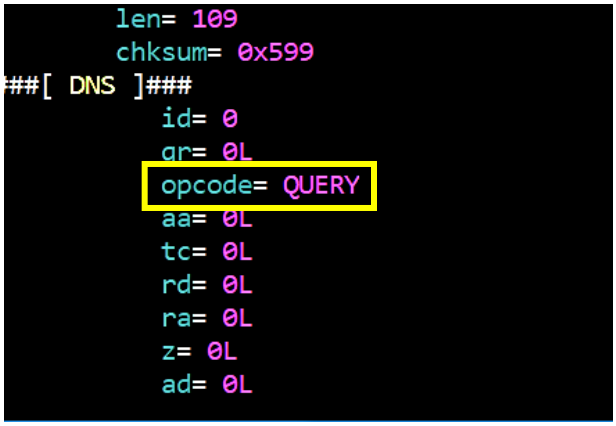
הגיע הזמן שנכתוב קצת קוד. נגדיר פרוצדורה שמקבלת פקטה ומחזירה True *אם היא מכילה הודעת* DNS

```
>>> def include_dns(p):
>>>     return DNS in p
```

כעת נורה ל sniffer שלנו להשתמש בה
נכתוב

```
>>>packets = sniff(count=5, lfilter=include_dns)
```

ומה קיבלנו? הדפיסו את התוכן של ההודעה הראשונה איך תעשו זאת?



1.4 קריאת ערכי השדות

```
>>> packets[0][DNS].opcode
0L
>>>
```

כעת אנו יודעים ששדה ה opcode מורה על QUERY אבל מה אבל מה ערכו המספרי? איך נגלה אותו?

>>> packets[0][DNS].opcode → opcode

ידפיס את ערכו המספרי של השדה
(ה L מציין שהמספר הוא integer (Long))

כלומר כשבזיכרון המחשב בפקטה שמור 0, scapy בפקודה show מציג שההודעה היא Query

1.5 תרגיל

השתמשו בכלים שרכשתם עד כה והסניפו 4 פקטות מסוג DNS. וודאו שהן מסוג Query ושהשדה qtype מורה על ערך A . שימו לב – השדה qtype יושב מתחת לכותרת ###[DNS Question Record]### והגישה אליו היא: packets[0][DNSQR].qtype, כלומר כדי לגלות את ערכו המספרי עליכם להדפיס :

```
>>> packets[0][DNSQR].qtype
```

<u>הדרכה:</u>

- הדפיסו את ערך השדה qtype בשכבה DNSQR עבור פקטה p שה ראיתם בעזרת p.show() שערכו A. זיכרו מה הערך המספרי שמייצג את A
- הגדירו בפעולה include_dnsqrA(p) המחזירה אמת עבור פקטות שמכילות את השכבה DNSQR ושהשדה p[0]{DNSQR].qtype מכיל את המספר המייצג את A

1.6 שימוש בתוצאות ההסנפה

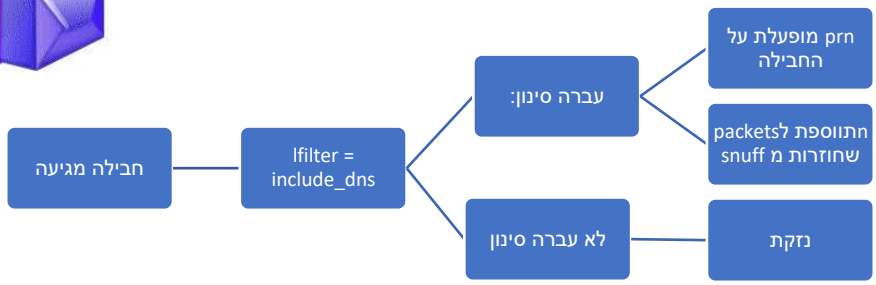
נניח ונרצה להדפס את תוצאות ההסנפה שלנו – לדוגמא את שמות ה domains שנשלחו לשרת ה DNS. לשם כך נוסיף פרוצדורה חדשה print_dns_domain.

```
>>>  def print_dns_domain(p):
...  print (p[DNSQR].qname)
```

נשתמש בפרמטר prn בקריאה ל sniff שמשמעותו היא: בצע את הפרוצדורה ששמה כתוב ב prn על הפקטות שעברו את ה filter (שערכו נמצא ב lfilter)

```
>>> pp=sniff(count=4, lfilter=dns_qrA, prn=print_dns_domain)
b'www.google.com.'
b'www.google.com.'
b'www.google.com.'
b'www.google.com.'
>>>
```

1.7 סיכום התהליך



2 Scapy – שימוש כספרייה

ניתן להשתמש ב Scapy כסיפרייה. לשם כן פתחו פרוייקט חדש ב paycharm ויבאו את Scapy.

כתבו בראש הקובץ:

```
from scapy.all import *
```

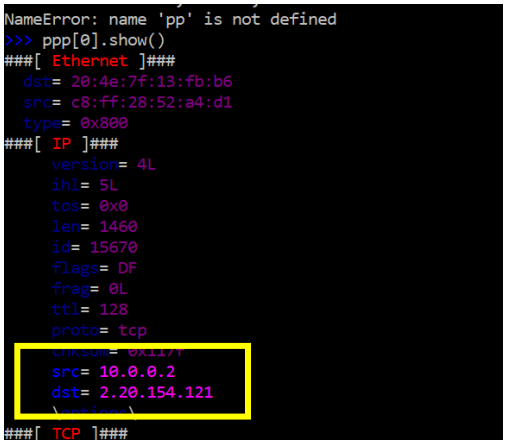
- כתבו פעול לסינון בשם Include_http שמקבלת פקטה ומחזירה אמת אם זו פקטת HTTP.
נשים לב ש scapy לא נותן ייצוג לשכבת האפליקצייה. את כל מה שמגיע בה הוא שומר ב"שכבת" Raw בשדה load ולא מציג את תוכנו בצורה מסודרת כמו בשאר השכבות. לכן נאלץ לזהות את הפרוטוקול בעצמנו.
נבחר לזהות פקטות שמתחילות ב GET.

לכן נגדיר:

```
def include_http(p):
    return Raw in p and p[Raw].load[:3] == b'GET'
```

נשים לב שיש מה שיושב ב-load הוא מסוג byte array

- print_urlandhost פעולת הדפסה שמקבלת פקטת HTTP ומדפיסה את ה IP אליו היא נשלחת.
באיזו שיכבה יהיה ה IP? באיזה פרוטוקול נשתמש על מנת לקבל אותו? נבחן תוכן של פקטת ב scapy



ה IP של היעד יושב תחת הפרוטוקול IP או תחת הפרוטוקול IPv6 בשדה dst
לכן הפעולה שלנו צריכה להיות:

```
def print_urlandhost(p):
    if IP in p:
        print(p[IP].dst)
    else:
        print(p[IPv6].dst)
```

- כתבו כעת את הפעולה my_sniffs שמזומנת מ main והריצו בה את ההדפסה שתדפיס 5 כתובות ip אליהן נשלחו הודעות Get. השתשו בפעולה sniff. מה יהיה ה filter? מה תהיה פעולת ההדפסה?

- נרחיב כעת את ההדפסה ונוסיף את ה url שנשלח עם הבקשה. באיזו פעולה תשנו את ההדפסה? איפה תמצאו את ה url? איך תחלצו אותו?
שנו את התוכנית שלכם כך שיודפס **גם** ה url.

העלו ל moodle את התכנית שכתבתם

בהצלחה