



# Scapy

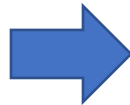
## 1 Scapy – עבודה אינטראקטיבית

### 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>scapy
```



```

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
ayp ayyyyyySCP//Pp sy//C
AYAsAYYYYYYYYY//Ps cY//S
pCCCCY//p cSSps y//Y
SPPPP//a pP//AC//Y
A//A cyP///C
p//Ac sC///a
P///YCpc A//A
scccccp///pSP//p p//Y
sY/////////y caa S//P
cayCyayP//Ya pY/Ya
sY/PsY///YCc aC//Yp
sc sccaCY//PCypaapyCP//YSs
spCPY/////////YPSps
ccaacs

Welcome to Scapy
Version 2.4.3rc3
https://github.com/secdev/scapy
Have fun!
Craft packets before they craft you.
-- Socrate

using IPython 7.6.1
>>>

```

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



## 1.2 הסנפה

הסנפה ב scapy 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)

תוצאה	פקודה
	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()



Fiilter 1.3

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?

```
len= 109
checksum= 0x599
###[ DNS ]###
  id= 0
  qr= 0L
  opcode= QUERY
  aa= 0L
  tc= 0L
  rd= 0L
  ra= 0L
  z= 0L
  ad= 0L
```

## 1.4 קריאת ערכי השדות

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

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

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

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
```

הדרכה:

- 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

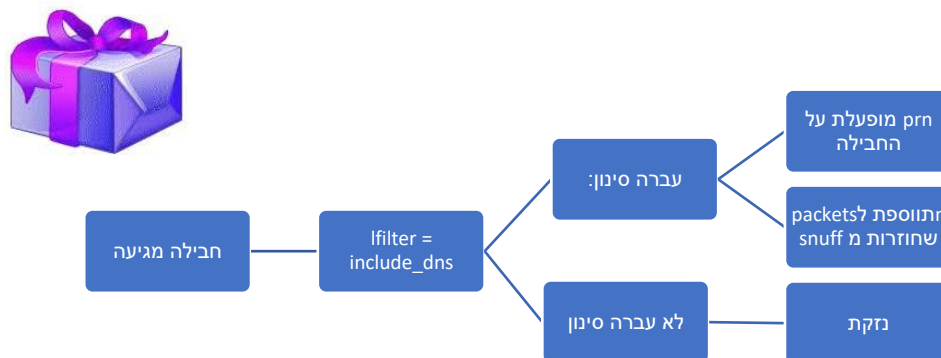
נניח ונרצה להדפס את תוצאות ההסנפה שלנו – לדוגמא את שמות ה domains שנשלחו לשרת ה DNS. לשם כך נוסיף פרוצדורה חדשה print\_dns\_domain.

```
>>> 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 ifilter)

```
>>> 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 כספרייה. לשם כך פתחו פרוייקט חדש ב paycharm וצרו קובץ חדש בשם scpy.py. ויבאו את Scapy לקובץ בצורה הבאה:

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

כתבו בראש הקובץ:

נרצה לכתוב תוכנית שמסננת פקטות http ומדפיסה את ה ip אליהן נשלחו ואת המשאב אותו הן מבקשות  
נחלק את הכתיבה לכמה חלקים

- **הפילטר** - כתבו פעולה לסינון בשם include\_http שמקבלת פקטה ומחזירה אמת אם זו פקטת HTTP. נשים לב ש scapy לא נותן ייצוג לשכבת האפליקציה. 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

- **הדפסה** – כתבו פעולת הדפסה בשם print\_urlandhost 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

```

NameError: name 'pp' is not defined
>>> ppp[0].show()
###[ Ethernet ]###
  dst= 20:4e:7f:13:fb:b6
  src= c8:ff:28:52:a4:d1
  type= 0x800
###[ IP ]###
  version= 4L
  ihl= 5L
  tos= 0x0
  len= 1460
  id= 15670
  flags= DF
  frag= 0L
  ttl= 128
  proto= tcp
  checksum= 0x1777
  src= 10.0.0.2
  dst= 2.20.154.121
  \end{packet}
###[ TCP ]###

```

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

```

def print_urlandhost(p):
    print(p[IP].dst)

```

- כתבו כעת את הפעולה my\_sniffs שמזמנת 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 המשאב שנשלח עם הבקשה. באיזו פעולה תשנו את ההדפסה? איפה תמצאו את המשאב? איך תחלצו אותו? שנו את התוכנית שלכם כך שיודפס גם המשאב. פורמט ההדפסה ip – resource לדוגמא:

```

158.106.133.146 -- /
158.106.133.146 -- /fld/gifts.php
158.106.133.146 -- /fld/dolls.php
158.106.133.146 -- /fld/index.php
158.106.133.146 -- /fld/ice.php

```

העלו ל moodle את התכנית שכתבתם לאחר שתעבור את הטסט האוטומטי

בהצלחה