Python Scapy

Scapy is a packet manipulation tool

for computer networks,

it was written in Python and can

forge => fake, change

decode => solve

send => forward

and capture => catch

network packets

with very easy API.

It is a very powerful interactive packet manipulation program,

as it can replaces most classical networking tools, such as

hping => DoS command Linux,

arpspoof => ARP address changing command,

arping => ping arp,

and even some parts of basic packet analyzing SW

Nmap, scanning tool

tcpdump, packet analyzing tool

tshark, packet analyzing tool

Download and Installation

https://scapy.readthedocs.io/en/latest/installation.html

1. Install Python 3.7+.
2. Download and install Scapy.
3. Follow the platform-specific instructions (dependencies).
4. (Optional): Install additional software for special features.
5. Run Scapy with root privileges.

Each of these steps can be done in a different way depending on your platform and on the version of Scapy you want to use.

Follow the platform-specific instructions for more detail.

Scapy versions

Note

Scapy 2.5.0 was the last version to support Python 2.7 !

Scapy version	2.3.3	2.5.0	>2.5.0
Python 2.2–2.6	☐	☐	☐
Python 2.7	☐	☐	☐
Python 3.4–3.6	☐	☐	☐
Python 3.7–3.11	☐	☐	☐

Installing Scapy v2.x

Window Python Scapy Installation

https://www.rootinstall.com/tutorial/how-to-install-scapy-on-windows/

Scapy runs natively on Linux, and on most Unixes with `libpcap` and its Python wrappers and the same code base works for both Python versions (3 and 2).

However, if you're on Windows, you need to do additional stuff in order to make it work.

Before we get started, make sure you have Python 3.4+ installed on your Windows machine, in the following section, we'll install npcap.

Installing Scapy

Now that you have Npcap installed, you have to install Scapy, it is pretty straightforward and you can do it using the following command in the command line:

```
$ pip3 install scapy
```

After you've done that, make sure you have it installed:

```
C:\Users\STRIX>python
Python 3.6.6 (v3.6.6:4cf1f54eb7, Jun 27 2018, 03:37:03) [MSC v.1900 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import scapy
>>> scapy.__version__
'2.4.3'
```

Example of Python code to handle Scapy

This code is for capturing raw signal of packet

```
from scapy.all import *

from scapy.arch.windows import IFACES


import time

n = 50

iface = "Intel(R) Ethernet Connection (7) I219-V"

IFACES.show()


def cap():

    for i in range(0, n):

        packet = sniff(iface=iface, count = 6)

        data = (packet[0].payload)


        #packet.show()


        src_ip = packet[0][1].src

        dst_ip = packet[0][1].dst

        nowtime = time.strftime('%c', time.localtime(time.time()))

        print('\033[95m'+'[ '+nowtime+' ]
'+'\033[92m'+src_ip+'\033[94m'+" -> "+'\033[92m'+dst_ip+' \033[96m'+
str(data)) #data

cap()
```

The variable n is the number of iterations =>REPEATION

iface is the network interface to capture