

LAB

5

Scanning with Scapy and NMAP

By the end of this section, you should be able to:

- Use Scapy, a packet manipulation tool for scanning.
- Use Nmap for Scanning and Enumeration.

5.1 Introduction to Scapy

5.1.1 Scapy

Scapy is known as a packet manipulation tool for computer networks. Scapy is written using python by Philippe Biondi. It can be used to craft network packet, send the packet to another network node or host and use to capture the replied packets. Scapy can be used to develop other network tool such as scanning tool, tracerouting tool, probing tool, unit tests tool, attacks tool, network discovery tool and packet generator.

Scapy provides a Python interface into libpcap, (WinPCap/Npcap on Windows), in a similar way to that in which Wireshark provides a view and capture GUI. It can interface with a number of other programs to provide visualisation including Wireshark for decoding packets, GnuPlot for providing graphs, graphviz or VPython for visualisation, etc.

5.1.2 Installing Scapy in python environment

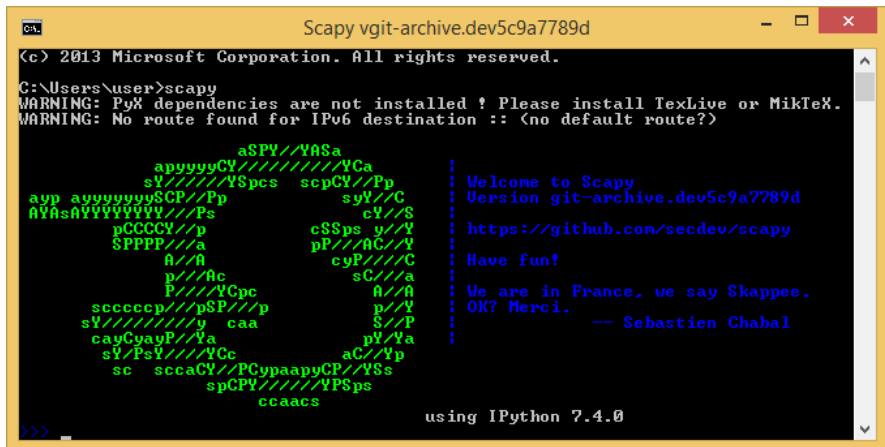
1. To start installing scapy, the following requirement is needed
 - Python 3.6 and above
 - Npcap: the latest version
 - pip install matplotlib
 - pip install PyX
2. Once these requirement is fulfill, it is time to installed scapy
3. Go to the scapy github and download the latest scapy.
4. On your console or terminal, locate the downloaded scapy form github folder and browse through the folder that contain setup.py.
5. Type the command below

```
prompt#> python setup.py install
```

6. Once the installation finish, you are ready to use scapy.

5.1.3 Using scapy for basic ping command.

1. To start using scapy just type `prompt#>scapy` on the console or terminal. Figure 1 will be displayed on your console.



```
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\user>scapy
WARNING: PyX dependencies are not installed ! Please install TexLive or MikTeX.
WARNING: No route found for IPv6 destination :: (no default route?)

      aSPY//YASa
    ap9999CY//YCa
  sY///YSpCs  scpCY//Pp
aYp a9999999SCP//Pp  syY//C
AYAsAY9999999//Ps  cY//S
      pCCCY//p      cSSps p//Y
    SPFP//a      pP//AC//Y
      A//A      cyP//C
      p//Ac      sC//a
      P///YCpc      A//A
    scccccpSP//p      p//Y
  sY///y caa      S//P
  cayCyayP//Ya      pY//Ya
  sY/PSY//YCc      aC//Yp
  sc  sccaCY//PCypaap9CP//YsS
      spCPY///YPSps
      ccaacs

Welcome to Scapy
Version git-archive.dev5c9a7789d
https://github.com/secdev/scapy
Have fun!
We are in France, we say Skappee.
OK? Merci. -- Sebastien Chabal

using IPython 7.4.0
```

Figure 1: Scapy Console in windows.

2. Type the following commands to start basic training on scapy, observe each output.

- Built a packet using

```
PH=IP( )
```

- Showing the content of a packet

```
PH.display()
```

- setting a value in the packet e.g. setting a destination of the packet

```
PH.dst="Your destination/ target IP address"
```

- Displaying the packet content will have a different value

```
PH.display()
```

3. To send a packet for example an ICMP packet the following command is use. Observe each output.

The '/' operator has been used as a composition operator between two layers. When doing so, the lower layer can have one or more of its defaults fields overloaded according to the upper layer.

Sending a packet in ICMP

```
TPH = ICMP()  
pingtool=sr1(PH/TPH, retry=2,timeout=1)  
pingtool.display()
```

4. Use a different IP address in `PH.dst="different IP"` that belong to a Windows and Linux host and see the difference display ().
5. Use an IP that is not belong to any host and observed the display.

Task 1



using Scapy in python.

1. Create a python script name ping.py and write the script below.

```

from scapy.all import *
ans=input("Enter target IP ? : ")
PH=IP()
TPH=ICMP()
PH.dst=ans
reply=sr1(PH/TPH, retry=1, timeout=1)

if reply==None:
    print(" ***** ")
    print(" HOST UNREACHABLE")
    print(" ***** ")
else :
    print(" ***** ")
    print(reply.summary())
    print(" ***** ")

```

2. To run the script type python ping.py



- This activity need a python to be install in the computer. For kali linux it have been preinstall in the kali

Review Question



Developed a python script that able to :-

1. Scan a host and determined whether the host is a Linux Host or a windows Host
2. Scan a range of IP and return whether the host is alive or not.
3. Using TCP() instead of ICMP() to scan a range of port.

5.2 Introduction to Nmap

5.2.1 Nmap

Nmap is an acronym for network mapper, an open source tool for network scanner that is developed by Gordon Lyon. Nmap can be used to discover host, services offered by a host and operating system running on a host. Among the features Nmap provide are:-

- Host discovery
- Port scanning
- Version detection
- OS detection
- Scriptable interaction with the target packets,

5.2.2 Basic Nmap Command

1. Install Nmap from <https://nmap.org/>
2. Once install open a command console or terminal
3. To use the option can be used in nmap type on the command prompt

```
admin#> nmap
```

4. To start a basic network scan for a target host, the list of command are :

Scan a single IP	nmap 192.168.1.1
Scan a host	nmap www.testhostname.com
Scan a range of IPs	nmap 192.168.1.1-20
Scan a subnet	nmap 192.168.1.0/24
Scan from a text file	nmap -iL list-of-ips.txt

5. To scan a specific port on a host :

Scan a single Port	nmap -p 22 192.168.1.1
Scan a range of ports	nmap -p 1-100 192.168.1.1
Scan 100 common ports (Fast)	nmap -F 192.168.1.1
Scan all 65535 ports	nmap -p- 192.168.1.1

6. Scanning can be done in several mode depending on the objective the scanning is done. The following command are several different mode scanning can be done using nmap.

Scan using TCP connect

```
nmap -sT 192.168.1.1
```

Scan using TCP SYN scan (default)

```
nmap -sS 192.168.1.1
```

Scan UDP ports

```
nmap -sU -p 123,161,162 192.168.1.1
```

Scan selected ports - ignore discovery

```
nmap -Pn -F 192.168.1.1
```

Review Question



Scanning a windows and linux OS :-

1. Scan a host with a Linux Host or a windows Host
2. Captured the scanning activity through a network traffic capturing tool (Preferably Wireshark) in the target host
3. Observed the captured traffic network and investigate each packet. .