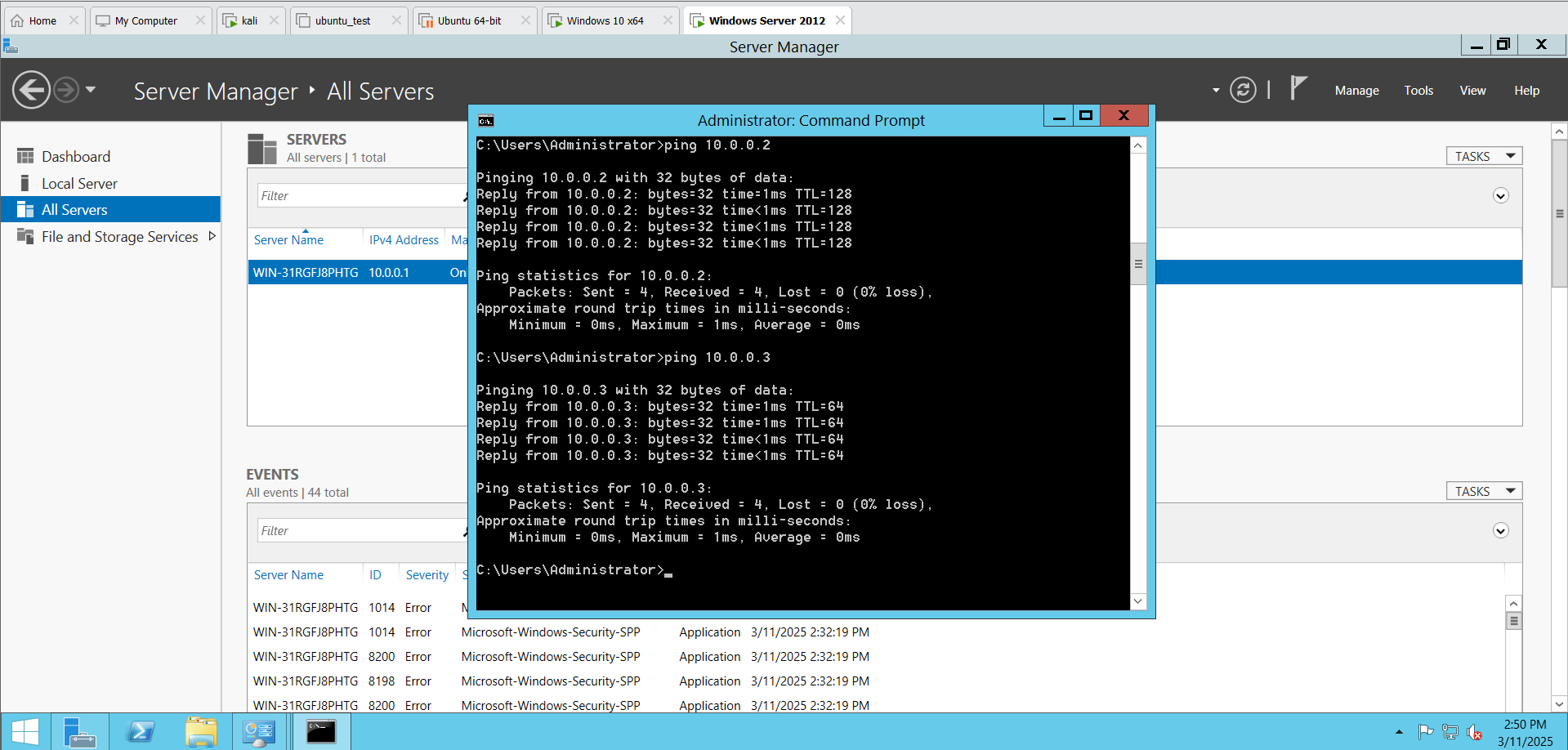
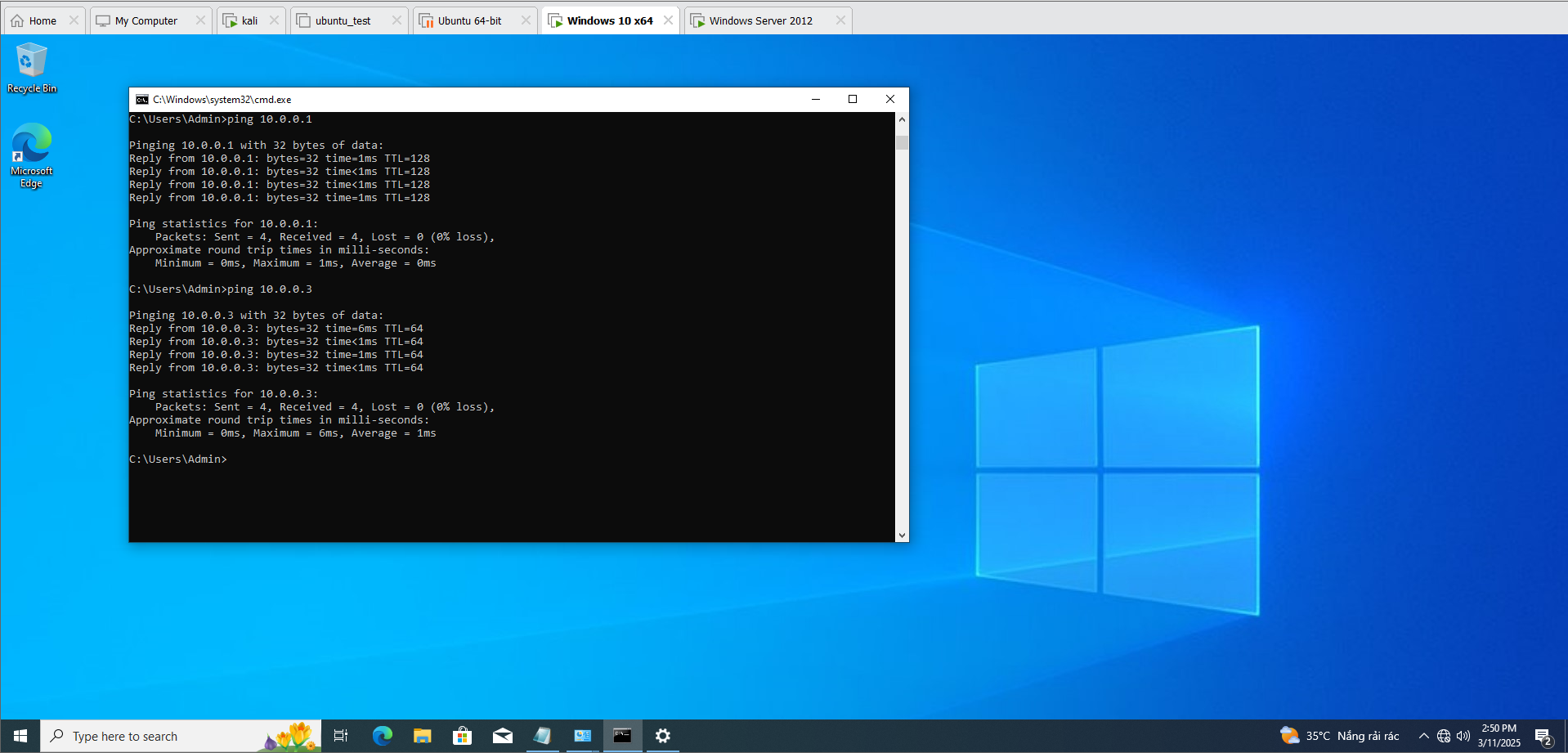
2033225505 – Trần Hoàng Huyền Trân

1. Thiết lập môi trường

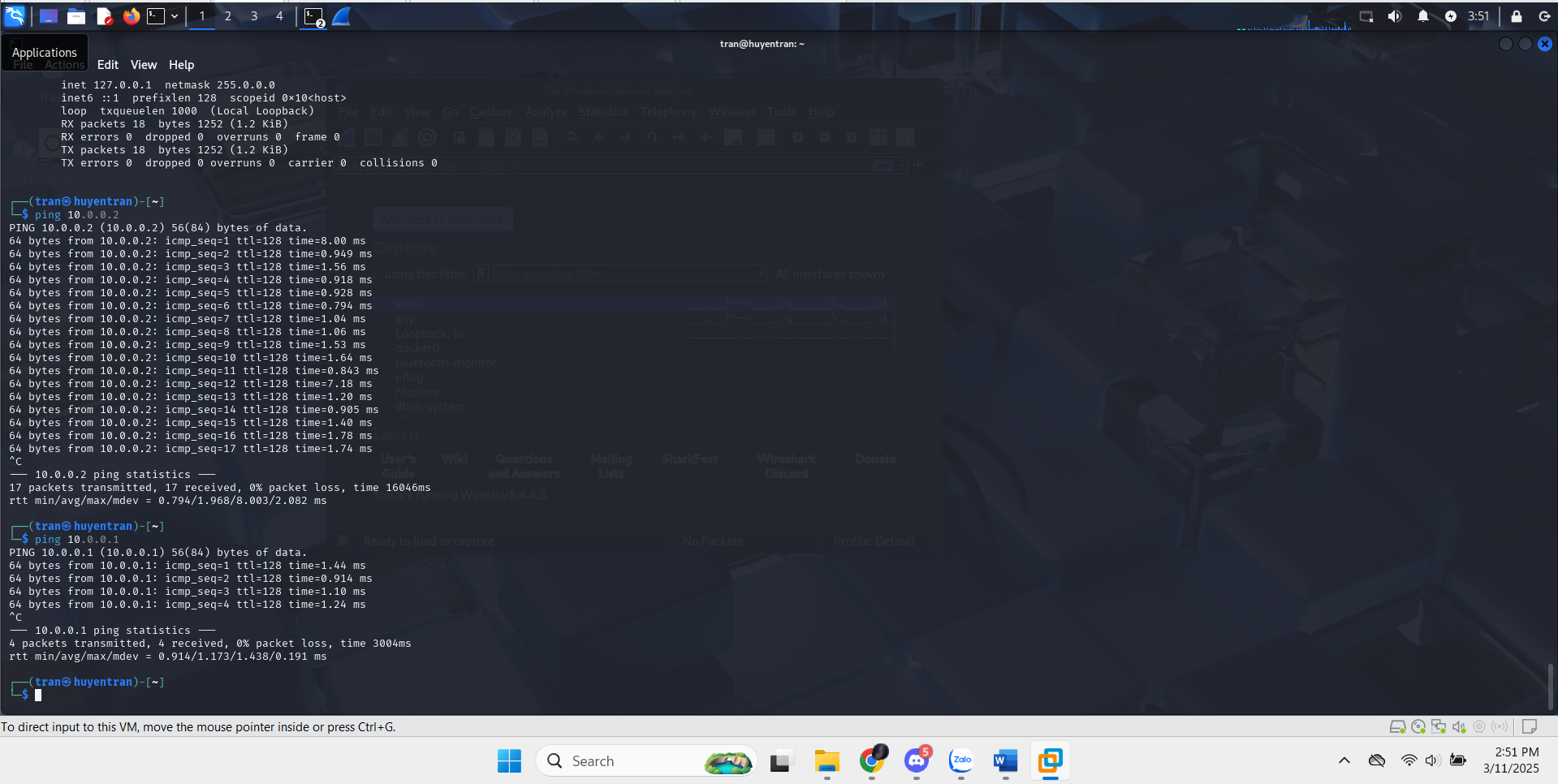
* Ping thành công từ máy server => máy client



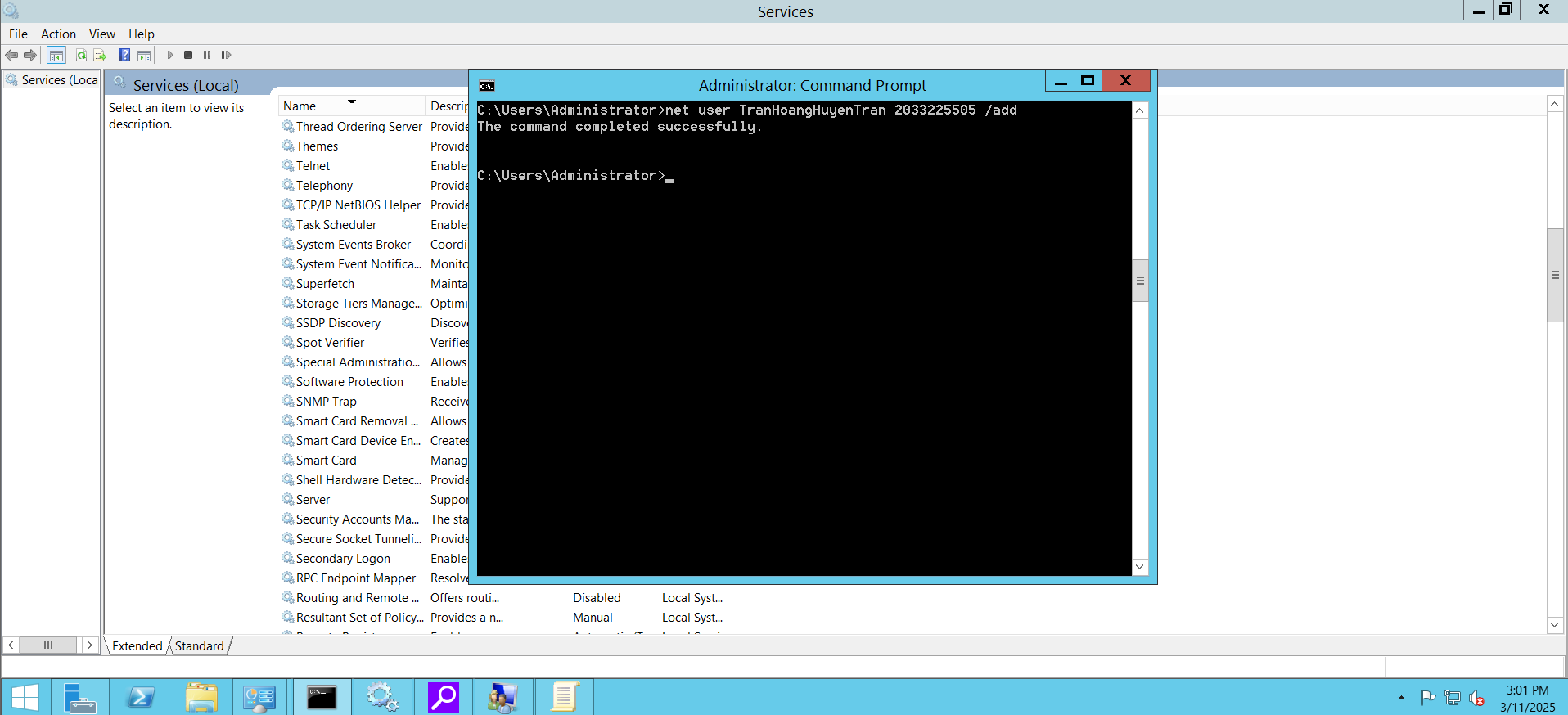
* Ping thành công từ máy client => máy server và máy kali



* Ping thành công từ máy kali => máy server + máy client



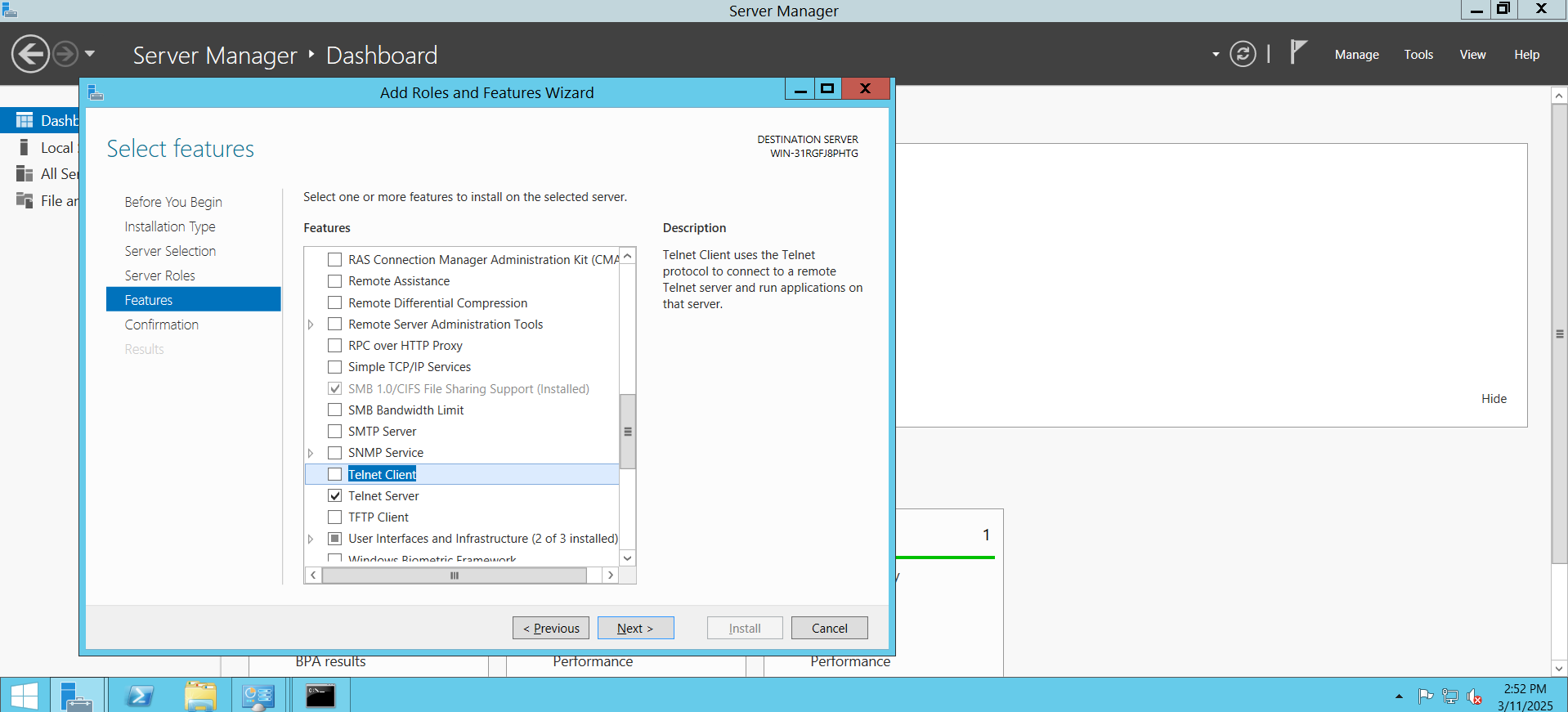
* Tạo 1 tài khoản với username = TranHoangHuyenTran và password = 2033225505



1. Bắt gói tin dùng Telnet

***Bước 1***: Bật dịch vụ Telnet trên máy chủ Windows Server.

* Cài đặt gói Telnet Server trên máy server

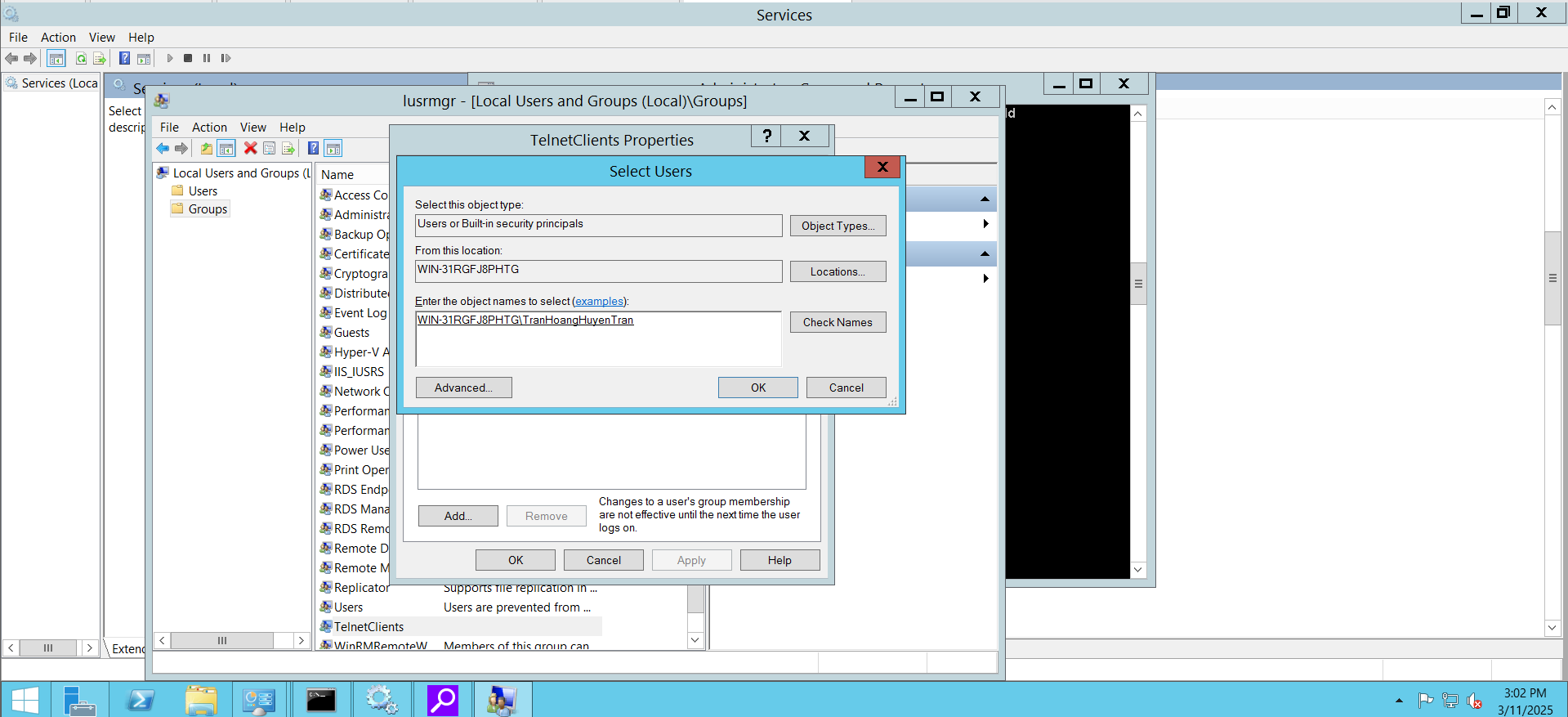


* Vào Start > Run > Gõ services.msc > Bật dịch vụ Telnet

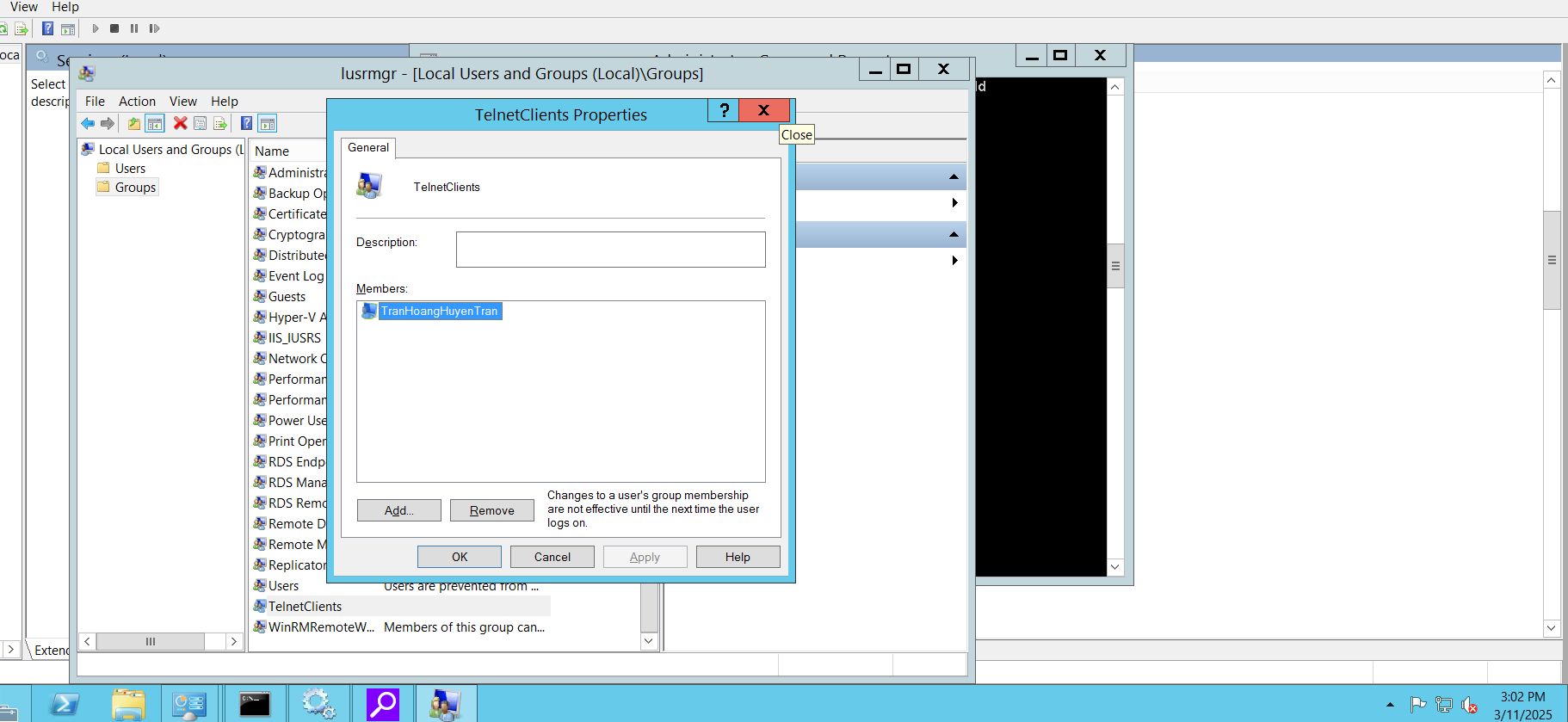


***Bước 2***: Thêm user Telnet vào TelnetClient Group tại server

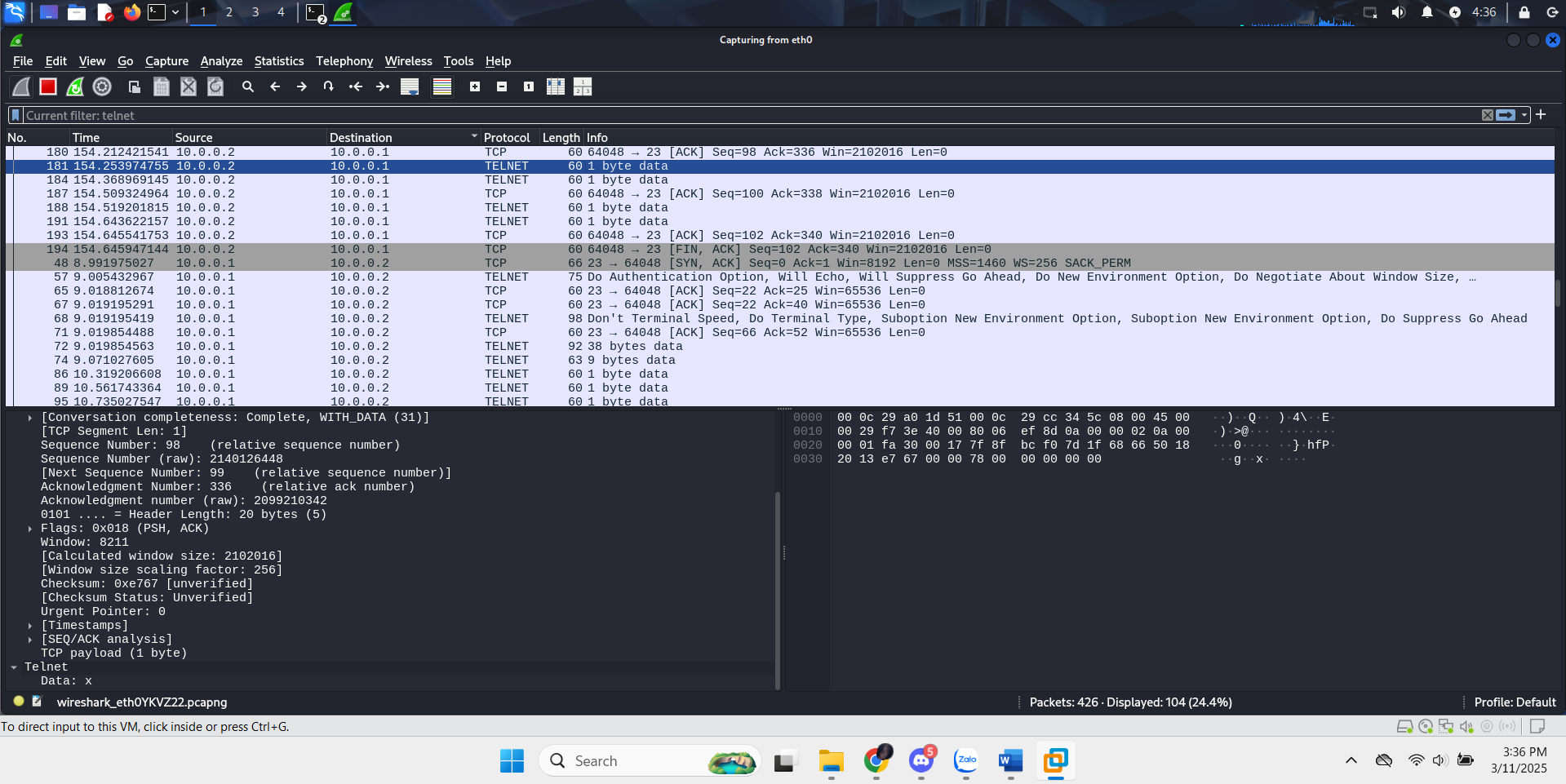
* Để cấp quyền cho Client có thể truy cập vào Server với user trên cần thêm user vào TelnetClients Group. Vào Local User and Group tại server bằng cách vào Run > gõ mmc lusrmgr.msc > Chọn TelnetClients Group và thêm user như sau:



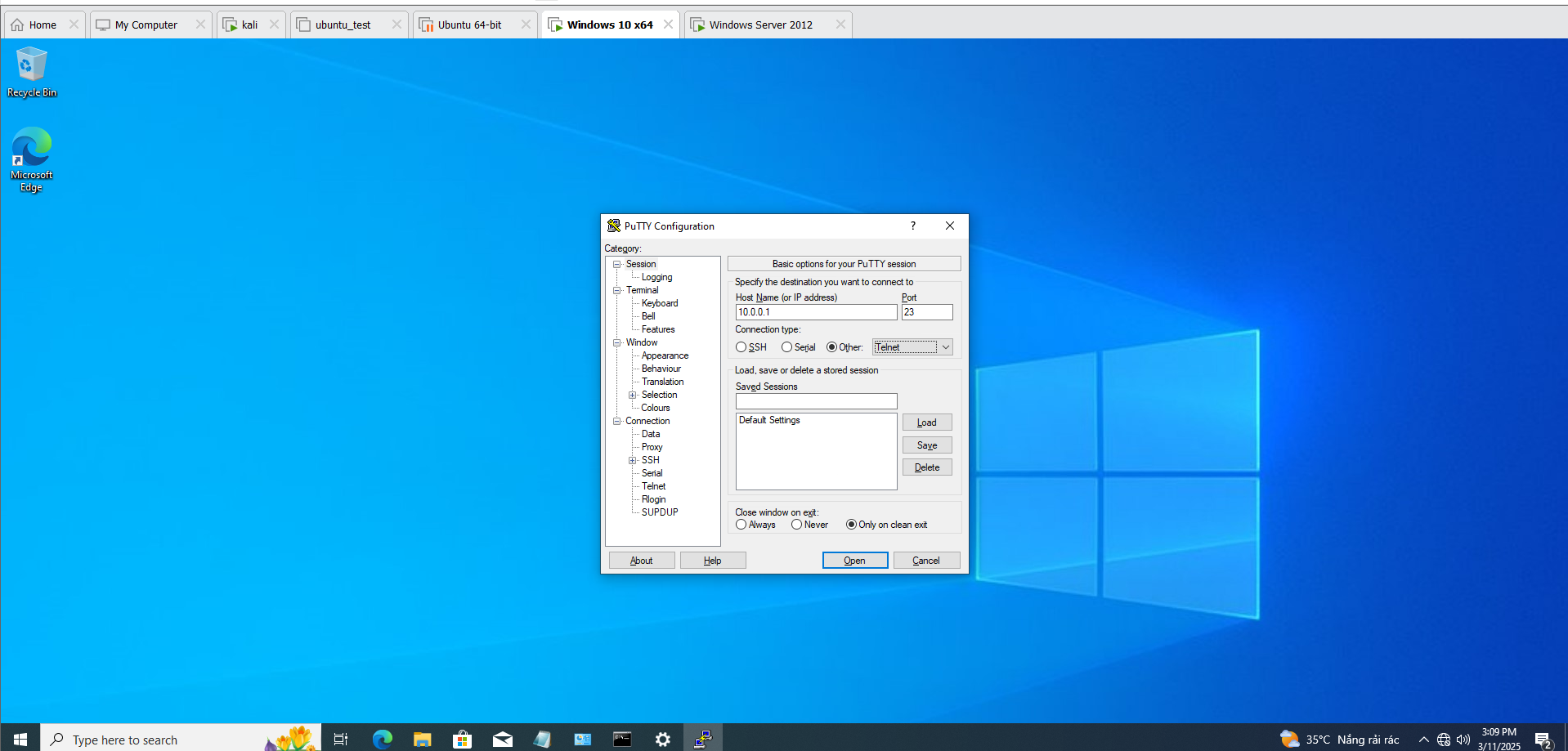
* Thêm user thành công



***Bước 3***: Tại máy Attacker, bật Wireshark (mạng eth0) để theo dõi và bắt gói tin.



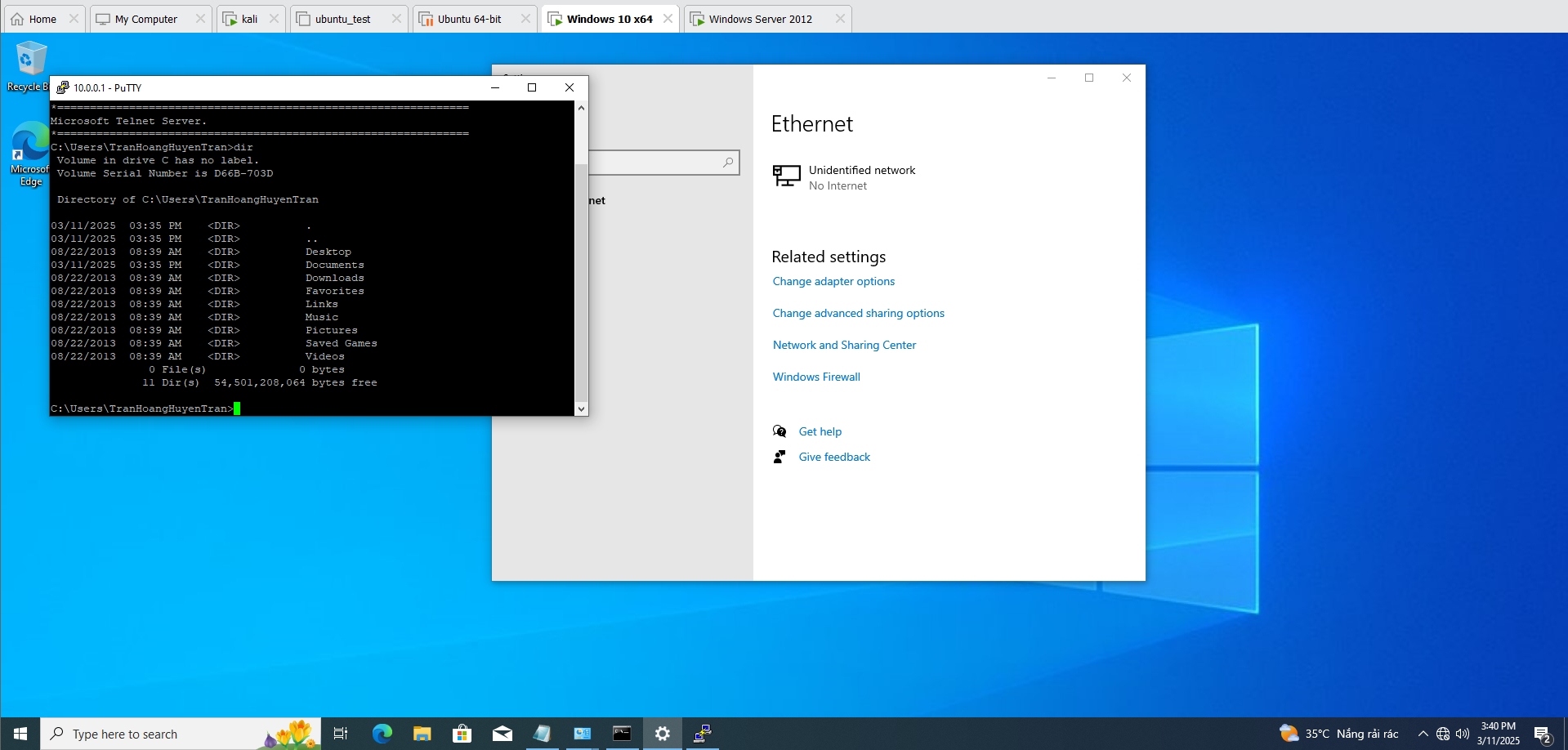
***Bước 4***: Tại máy Client, dùng Putty hoặc Command Prompt kết nối đến Server bằng Telnet với tài khoản đã tạo ở bước 1 và thực hiện một số thao tác cơ bản như xem, tạo thư mục (dir, mkdir).



* Đăng nhập với tài khoản của máy server

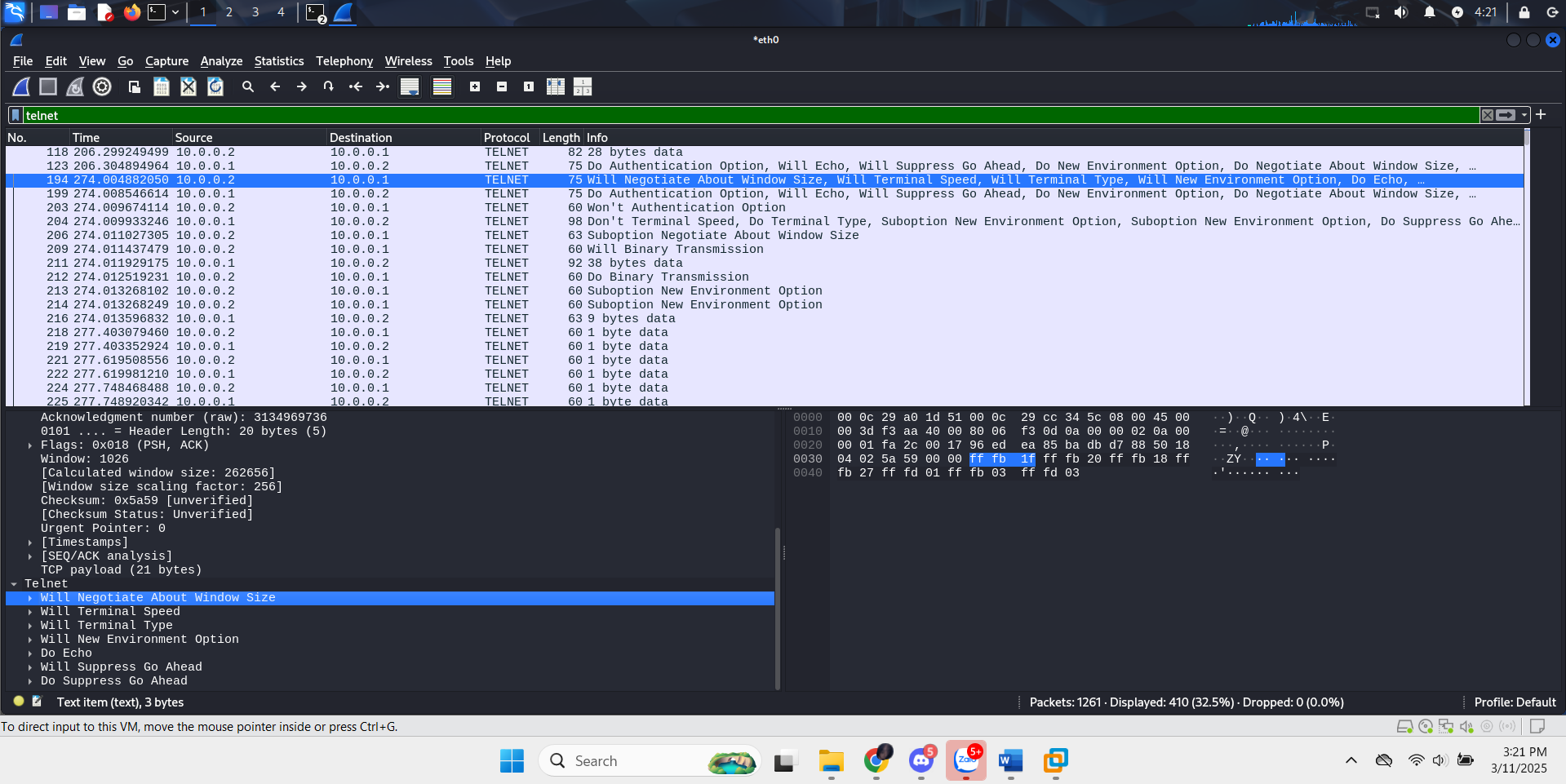


* Login thành công

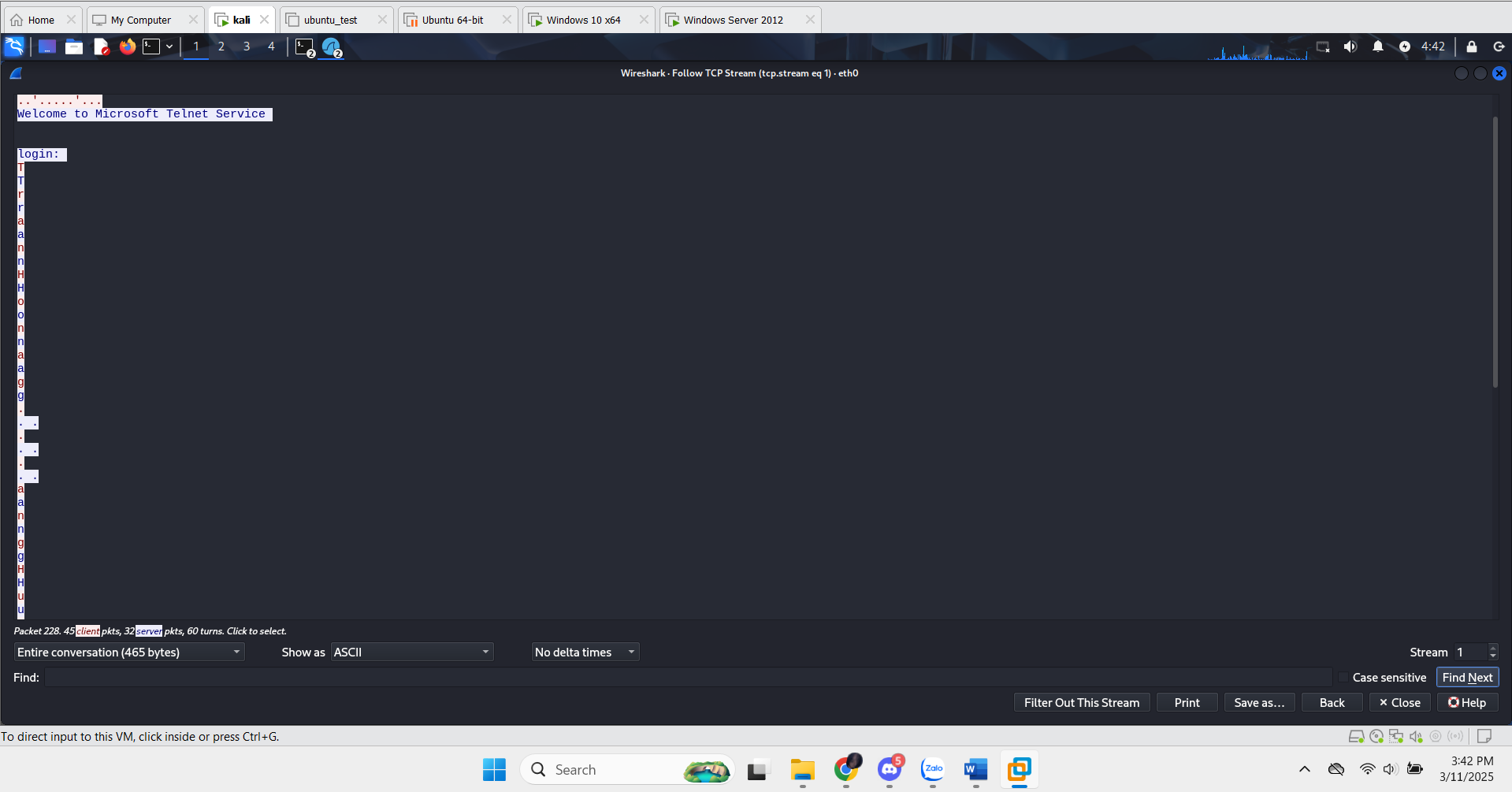


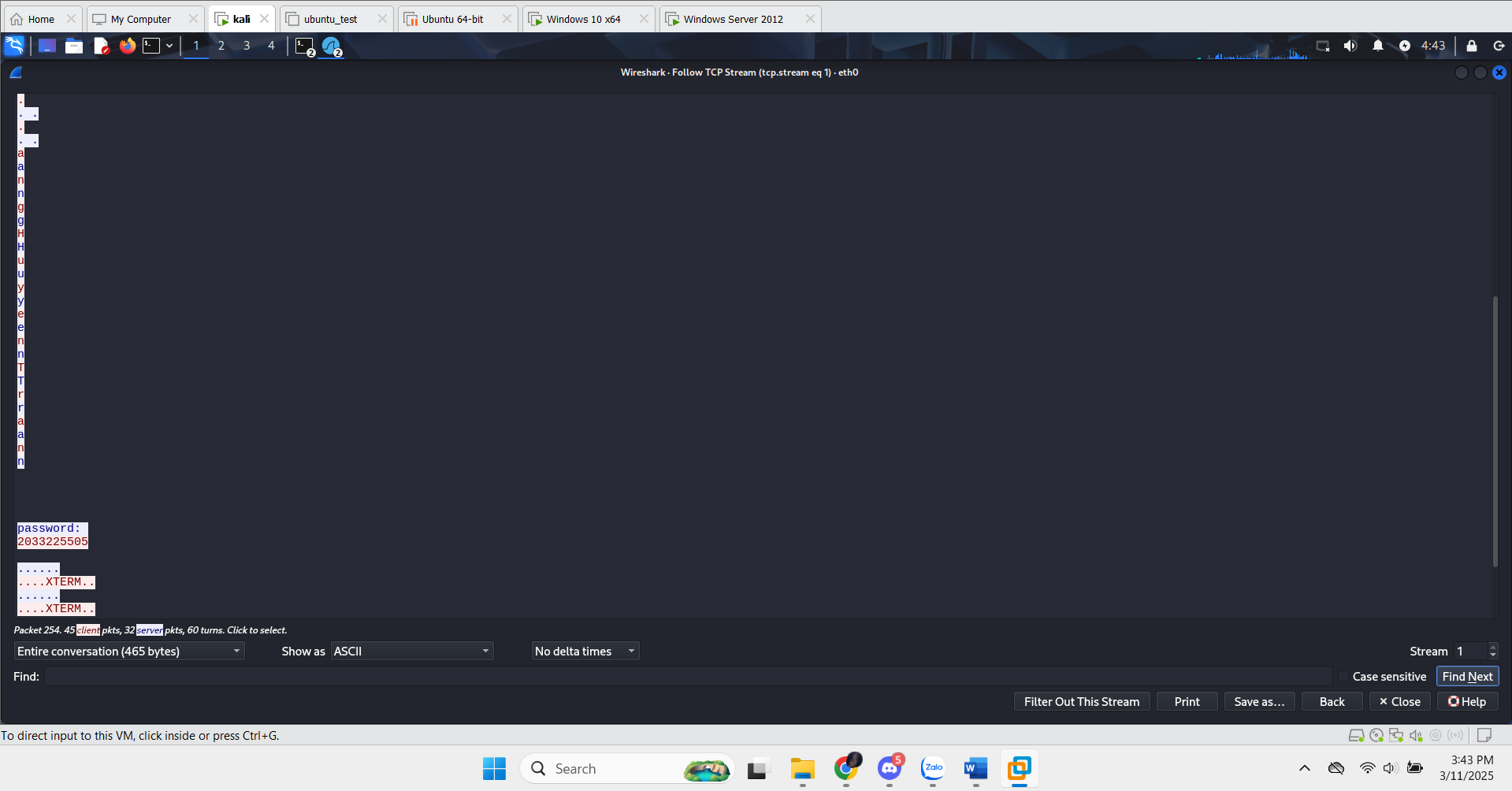
* Có thể thực hiện các lệnh với máy server

***Bước 5***: Dừng bắt gói tin ở máy Attacker, tìm thông tin đăng nhập qua các gói tin và phân tích các dữ liệu trao đổi giữa Client và Server.



* Gói telnet mà Wireshark bắt được
* Ta có thể click chuột phải vào gói telnet kia vào chọn vào Follow > TCP Stream. Ta có thể thấy được nội dung như username, password mà máy client nhập khi telnet qua máy server

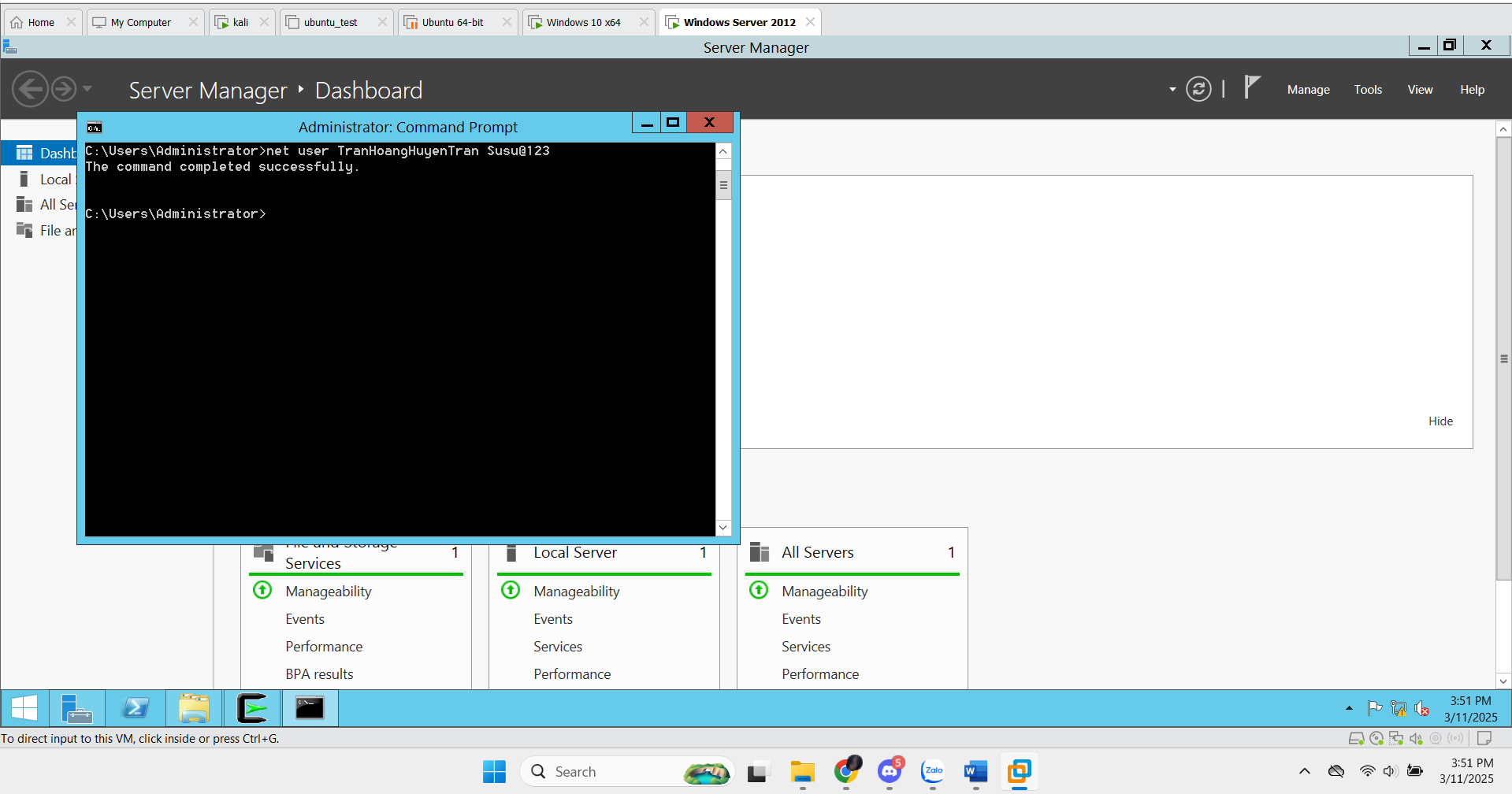




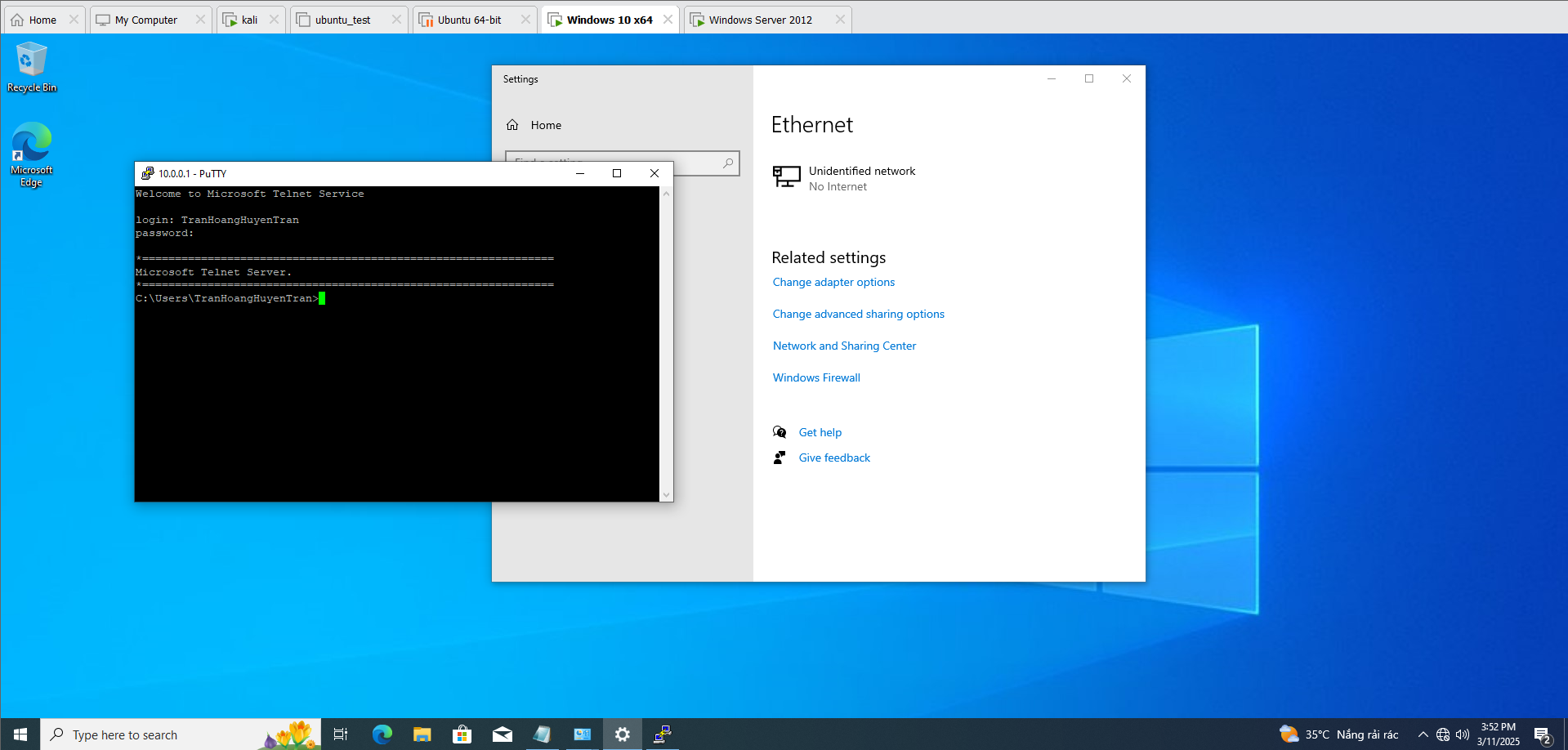
* Ta bắt được username: TranHoangHuyenTran và password: 2033225505

***Bước 6***: Thay đổi mật khẩu tài khoản đã tạo ở bước 3 thành mật khẩu phức tạp hơn (>10 ký tự, gồm chữ, số và ký tự đặc biệt). Lặp lại quá trình từ bước 3 đến bước 5 với mật khẩu vừa thay đổi.

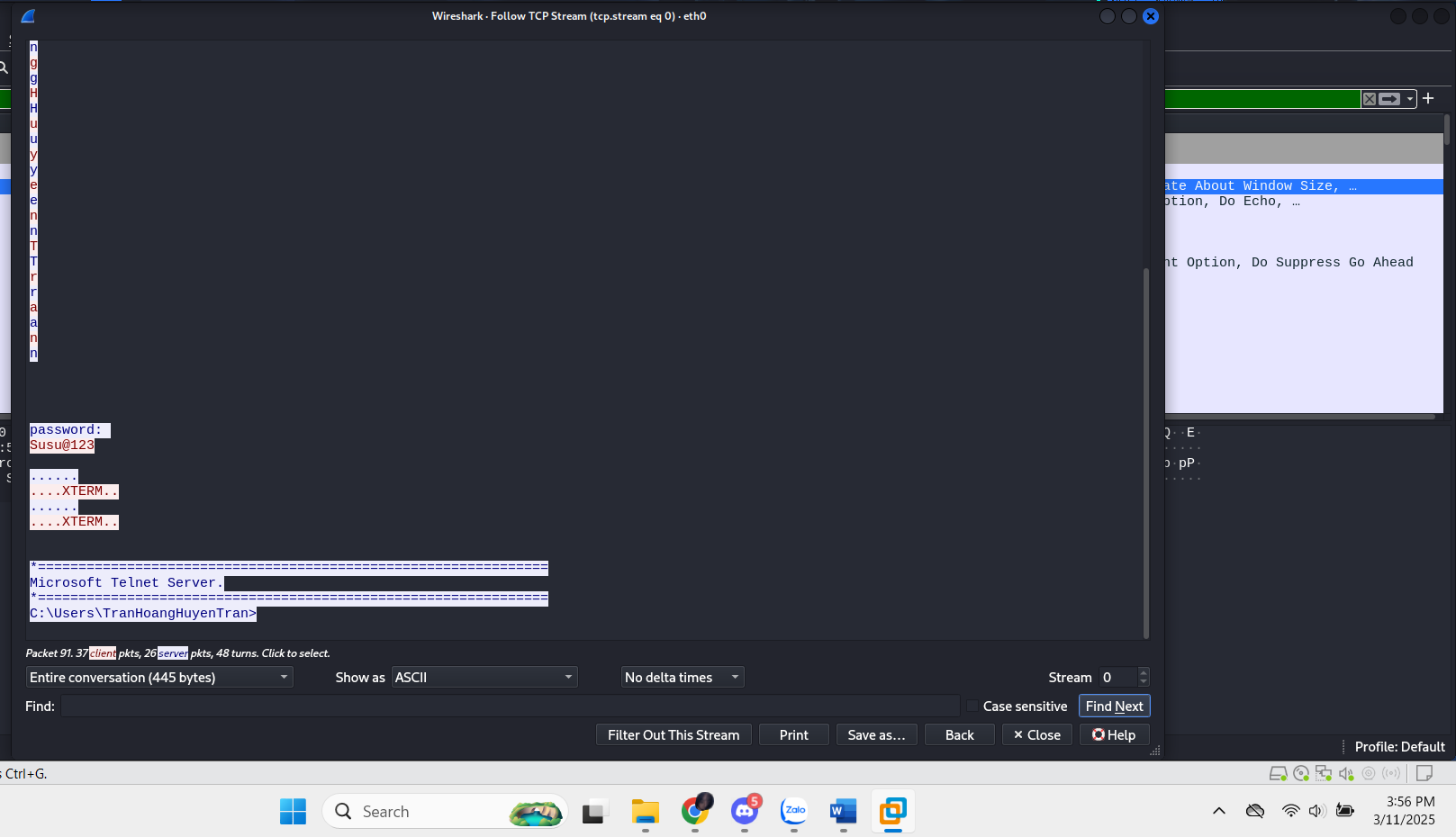
* Đổi password ở máy server



* Bật Wireshark và tiến hành login lại với telnet



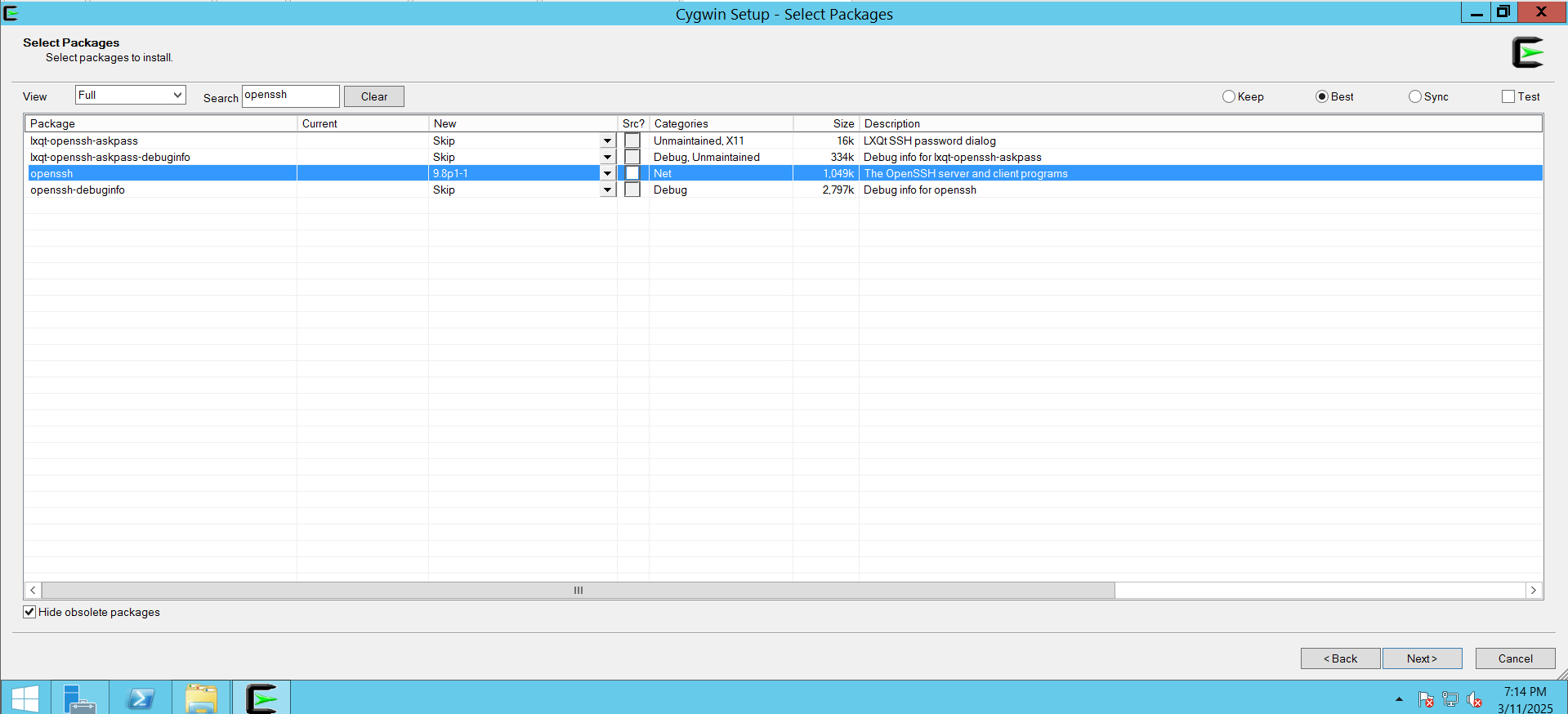
* Login lại với password: Susu@123



* Wireshark bắt được gói tin và xem được password

1. Bắt gói tin khi sử dụng SSH

***Bước 1:*** Cài đặt Cygwin để thiết lập SSH server tại máy chủ. Tiến hành cài đặt bình thường.

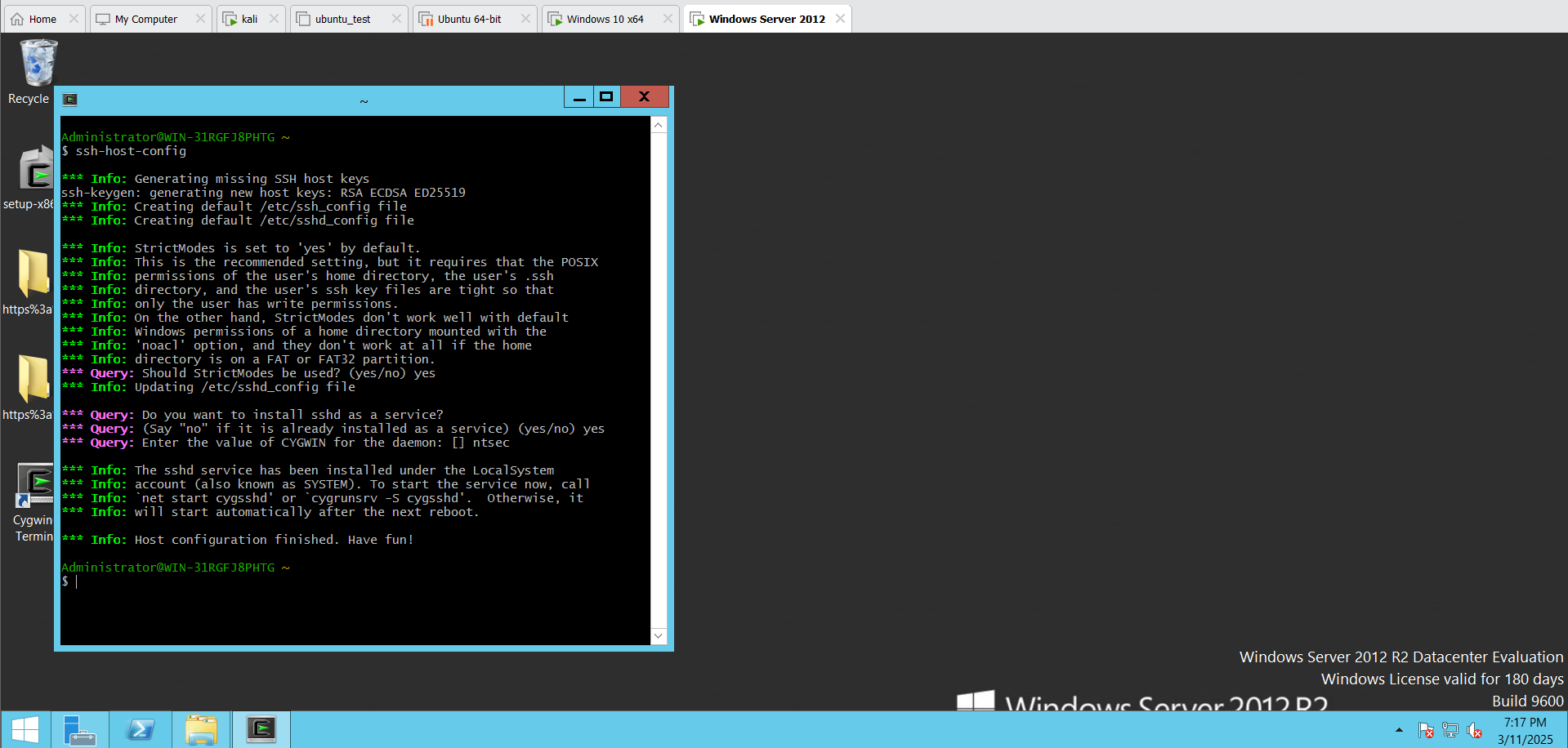


* Cần chọn gói openssh, chọn 9.8p1-1

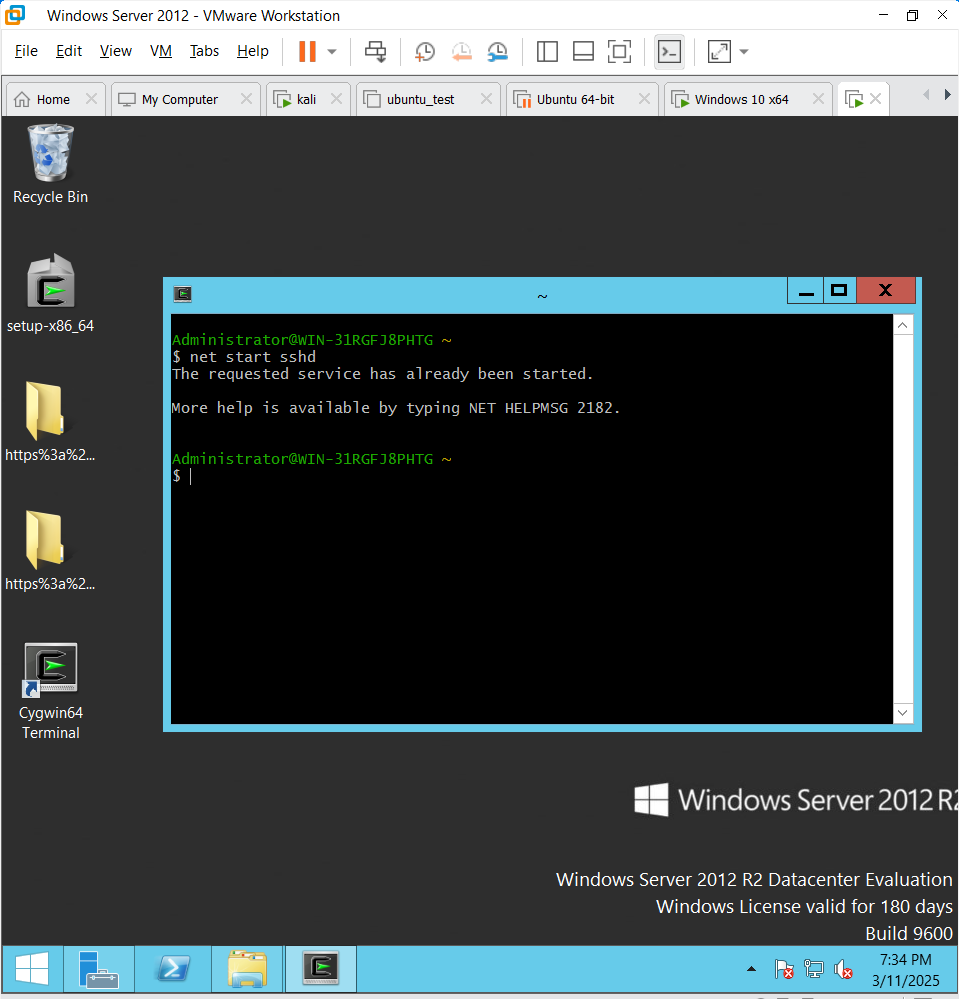
***Bước 2:*** Cấu hình và khởi động SSH server

Mở Cygwin Terminal > Cấu hình SSH server bằng lệnh **ssh-host-config**

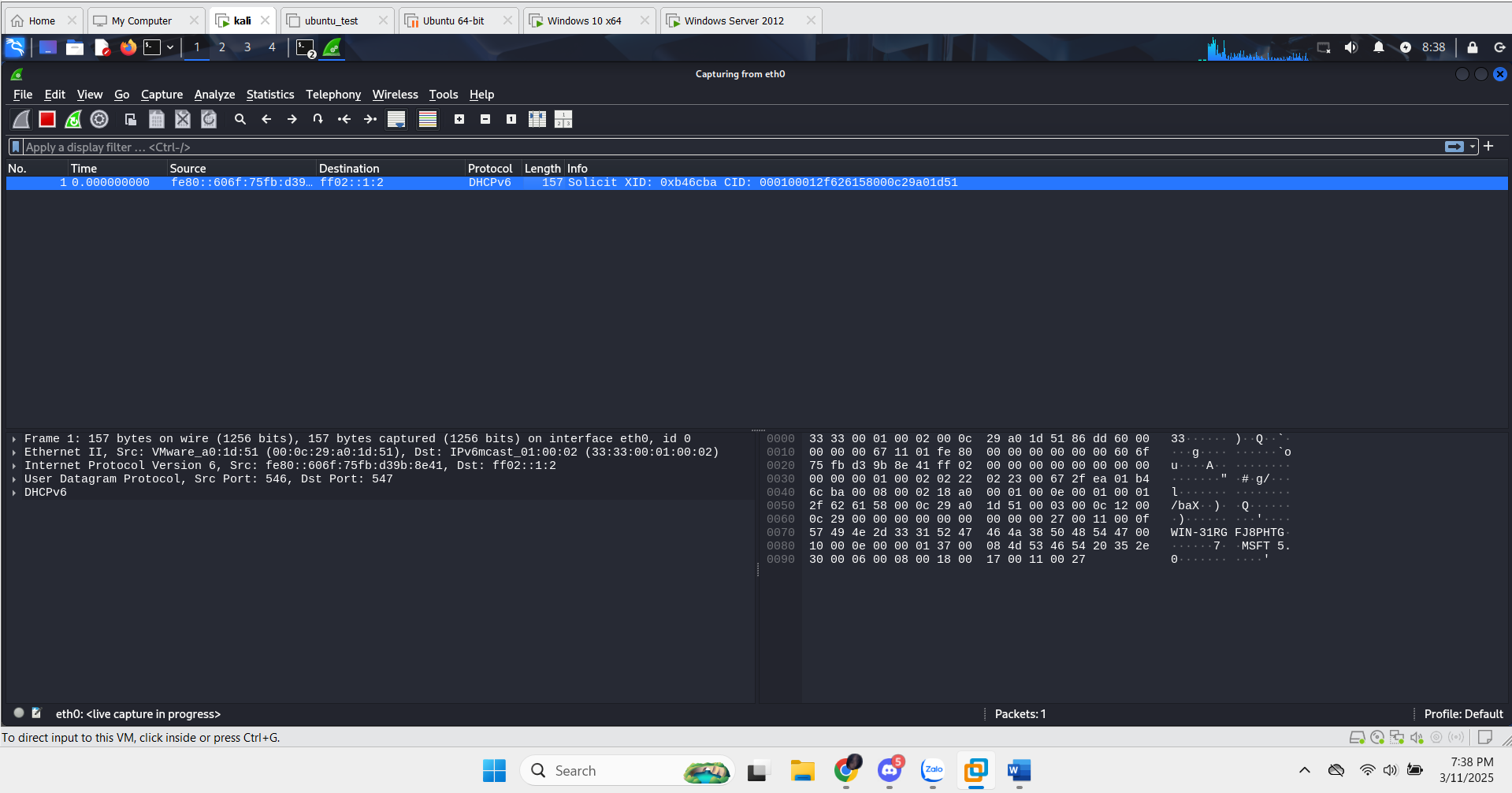
Chọn Yes ở các query, thực hiện việc cấu hình như sau:



* Nhập lệnh “net start sshd”

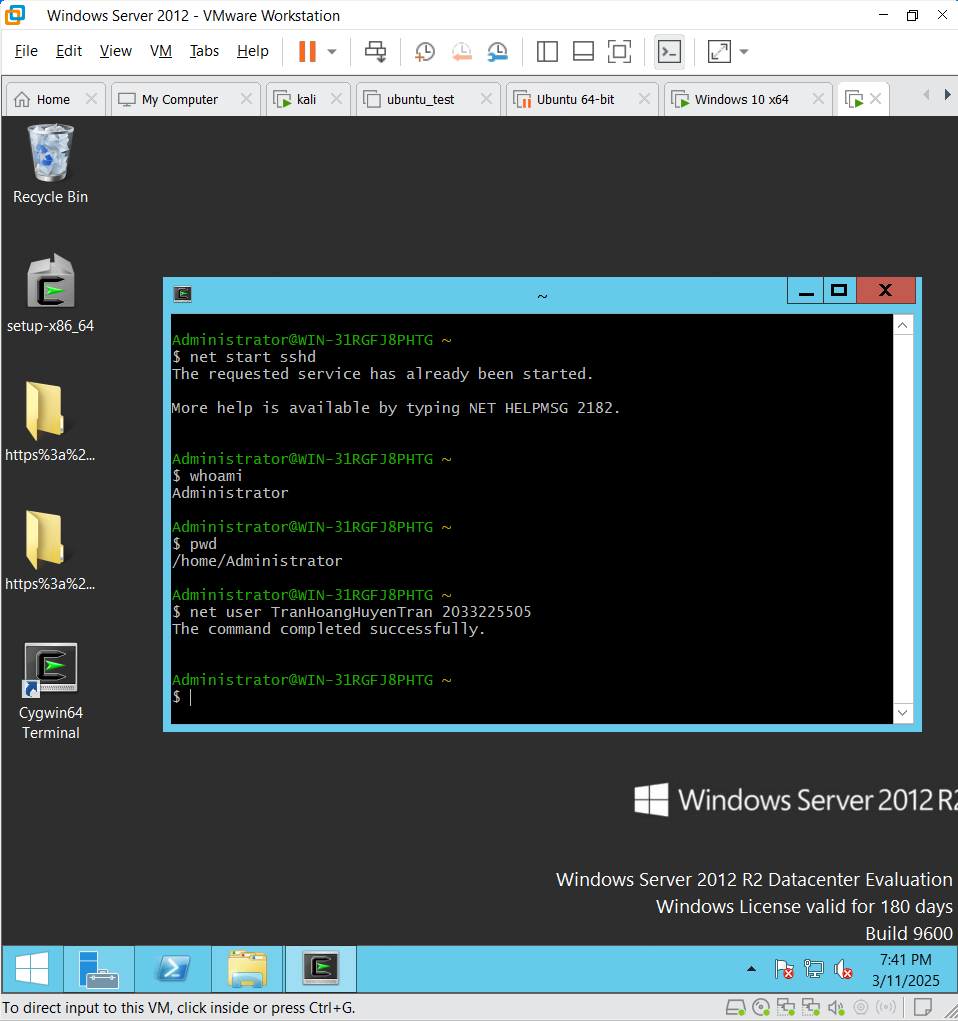


**Bước 3**: Tại máy Attacker, bật Wireshark để theo dõi và bắt gói tin

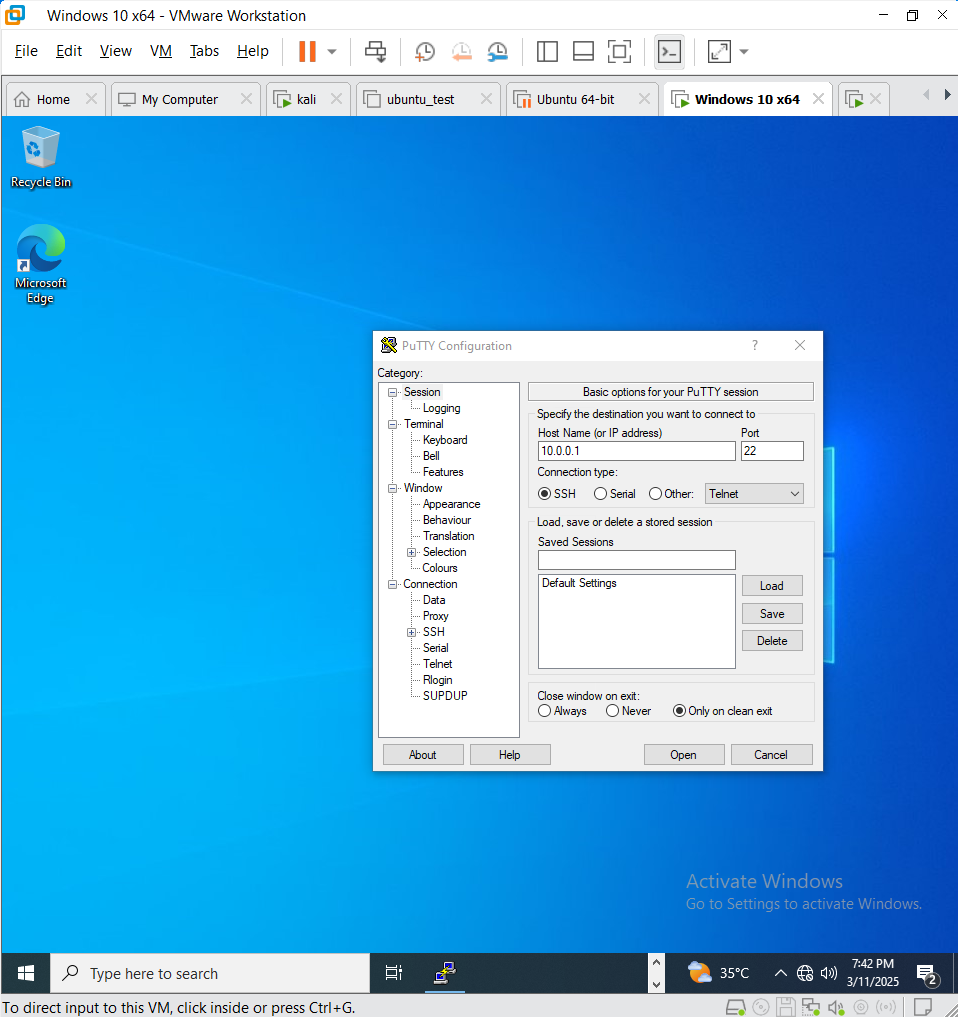


**Bước 4**: Thay đổi mật khẩu tài khoản ở Server đơn giản như ở phần 1. Tại máy Client, dùng Putty kết nối đến Server bằng SSH với tài khoản trên.

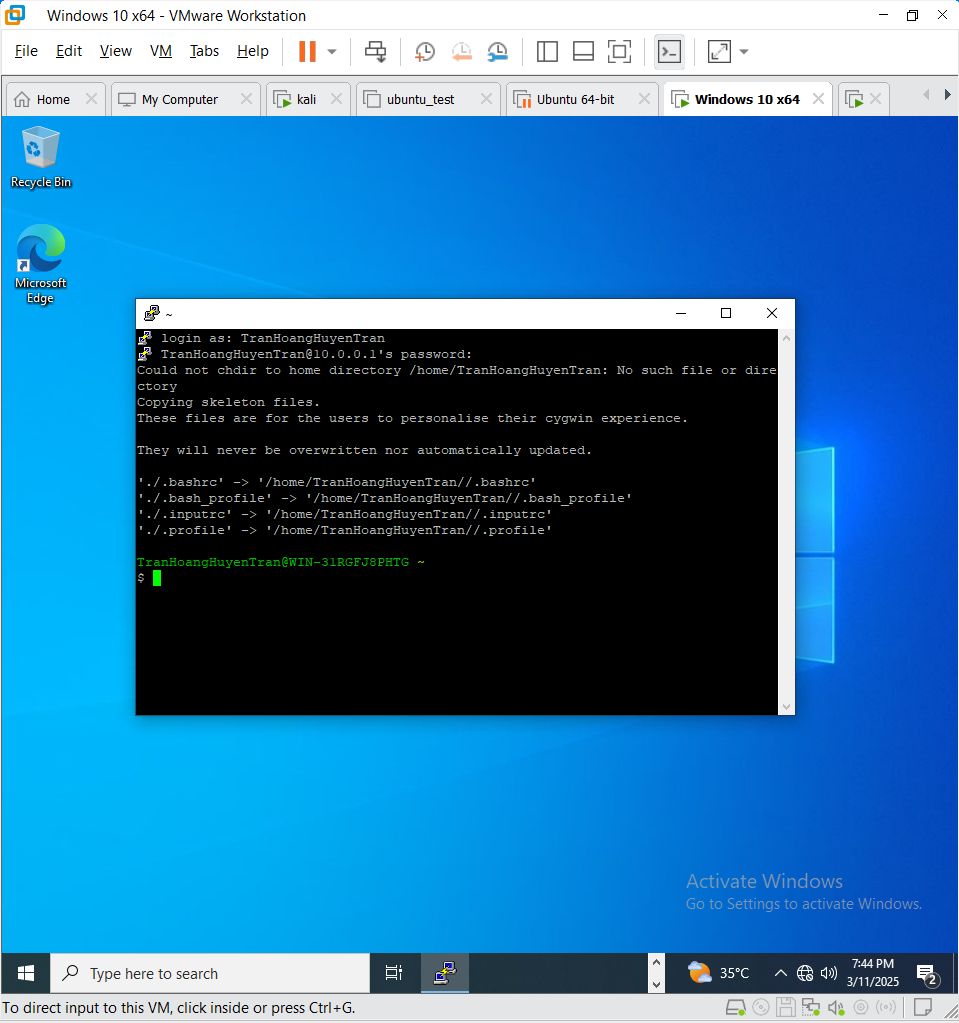
* Thay đổi mật khẩu lại thành MSSV ở máy server



* Dùng putty kết nối với ssh



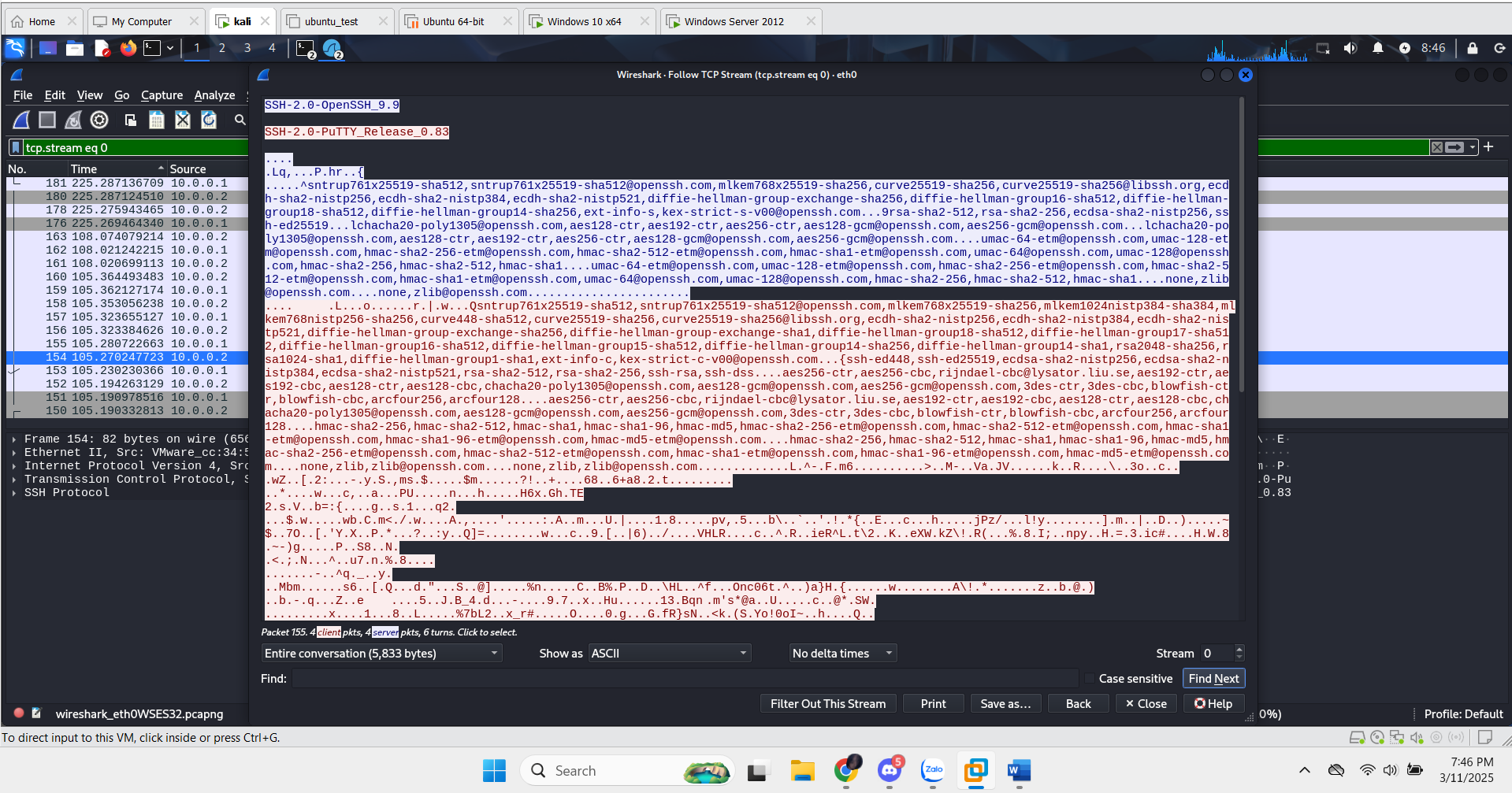
* Login như bình thường với password mới



**Bước 5**: Dừng bắt gói tin ở máy Attacker, kiểm tra và phân tích thông tin

đăng nhập và dữ liệu trao đổi giữa Client và Server.

* Kết quả nhận được là thông tin đã được mã hóa



1. Trả lời câu hỏi

* Telnet và SSH là gì và được ứng dụng trong trường hợp nào?
  + Telnet (TELecommunication NETwork) là một giao thức mạng dùng để điều khiển từ xa một thiết bị (thường là server hoặc router/switch) thông qua kết nối dòng lệnh (command line). Thường được dùng trong các trường hợp như là quản lí các thiết bị mạng cũ, kiểm tra các port dịch vụ,... đa phần là trong mạng LAN
  + SSH (Secure Shell) là một phiên bản bảo mật cao cấp hơn của Telnet, cho phép kết nối và điều khiển từ xa một cách an toàn. Thường được dùng trong các trường hợp như là quản trị máy chủ từ xa, tự động hóa kết nối từ xa bằng SSH Key,...
* So sánh Telnet và SSH:
* Bảo mật:
  + Telnet: Không mã hóa dữ liệu, dễ bị nghe lén.
  + SSH: Mã hóa toàn bộ dữ liệu, bảo mật cao.
* Truyền dữ liệu:
  + Telnet: Văn bản thuần (plain text).
  + SSH: Dữ liệu được mã hóa.
* Xác thực:
  + Telnet: Dùng tài khoản và mật khẩu, không an toàn.
  + SSH: Dùng mật khẩu hoặc cặp khóa công khai – riêng (key pair).
* Truyền file:
  + Telnet: Không hỗ trợ.
  + SSH: Hỗ trợ SCP, SFTP – truyền file an toàn.
* Tunneling/Port forwarding:
  + Telnet: Không hỗ trợ.
  + SSH: Có hỗ trợ, giúp bảo mật kết nối ứng dụng.
* Tính năng:
  + Telnet: Đơn giản, chỉ điều khiển từ xa.
  + SSH: Đa năng, hỗ trợ script, tự động hóa.
* Cổng mặc định:
  + Telnet: Port 23.
  + SSH: Port 22.
* Sử dụng:
  + Telnet: Dùng trong mạng nội bộ, kiểm tra cổng.
  + SSH: Dùng trong quản trị hệ thống, làm việc từ xa an toàn.
* Khi sử dụng SSH, còn có cách nào để đăng nhập ngoài cách dùng username và mật khẩu truyền thống?
  + Có, còn có thể đăng nhập bằng cách sử dụng cặp khóa công khai – khóa riêng (public key – private key). Đây là phương pháp an toàn và phổ biến hơn.