



# 1 Lab

## Bắt gói tin Telnet - SSH

Examining SSH & Telnet in Wireshark

**Thực hành An toàn Mạng máy tính**

GVTH: Nguyễn Thanh Hòa

Học kỳ I – Năm học 2016-2017

**Lưu hành nội bộ**

## A. TỔNG QUAN

### 1. Mục tiêu

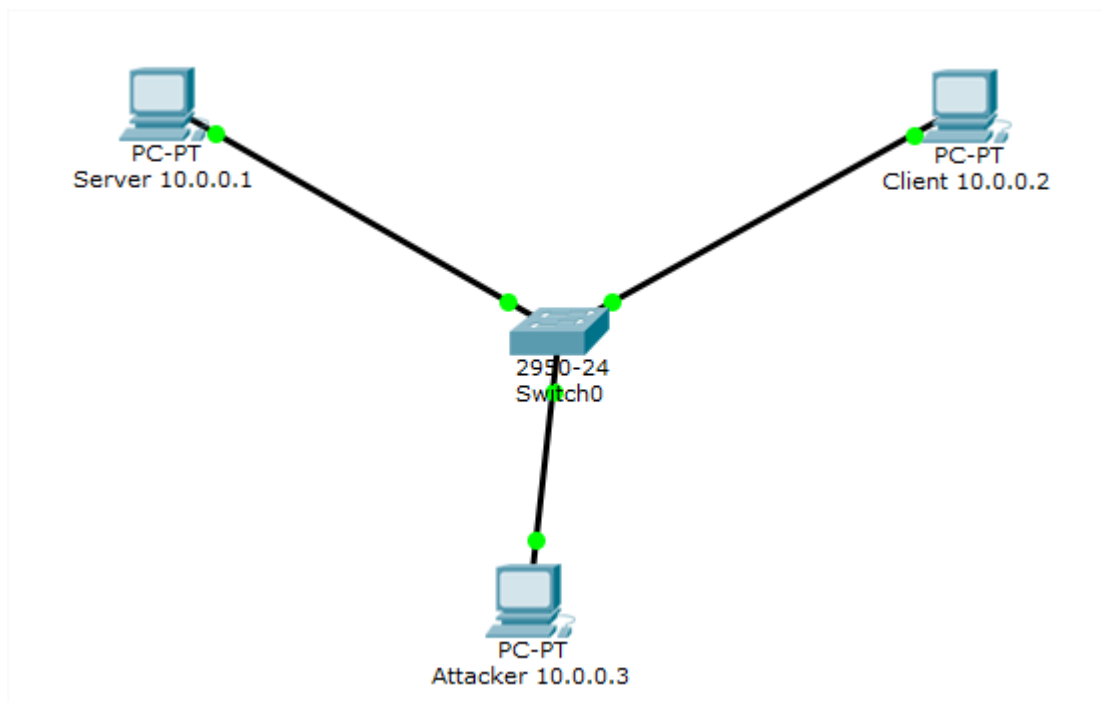
- Giả lập mạng Telnet – SSH Client/Server.
- Tìm hiểu cơ chế bắt gói tin bằng Wireshark.

### 2. Kiến thức nền tảng

- Kiến thức về Telnet/SSH.
- Thiết lập mô hình mạng.
- Sử dụng Wireshark.

### 3. Kịch bản

Giả lập mô hình mạng như sau:



Hình 1. Mô hình cho Lab01

Người dùng (Client) kết nối vào máy chủ (Server) trong cùng mạng nội bộ thông qua giao thức Telnet hoặc SSH để có thể truy cập và thao tác tại máy server với tài khoản được cấp. Một Attacker đã truy cập được vào cùng mạng này và quá trình kết nối và trao đổi dữ liệu giữa Client và Server liệu còn an toàn?

### 4. Môi trường & công cụ

Các máy tính được kết nối với nhau như Hình 1:

- 1 Máy chủ **Windows Server 2008**.
- 1 Máy Client Windows có phần mềm Putty.
- 1 Máy Attacker Windows tham gia bắt gói tin có phần mềm Wireshark.

Các công cụ sử dụng:

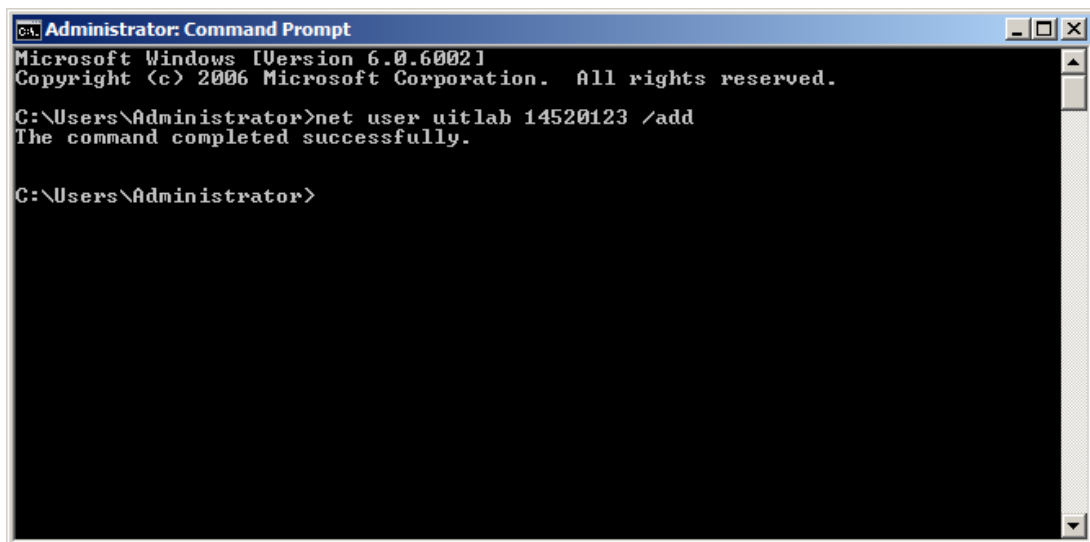
- VMWare (<http://www.vmware.com/>)
- Wireshark (<https://www.wireshark.org/>)
- Putty (<http://www.putty.org/>)
- Cygwin (<https://cygwin.com/>)

## B. THỰC HÀNH

### 1. Thiết lập môi trường

- Thiết lập mô hình mạng như *Hình 1* bằng các máy ảo VMWare hoặc Virtual Box. Kiểm tra các máy đã kết nối với nhau hay chưa bằng lệnh **ping**.
- Cài đặt **Wireshark** trên máy Attacker, **Putty** trên máy Client.
- Tại máy chủ, tạo một tài khoản với username = Tên sinh viên, mật khẩu = MSSV.

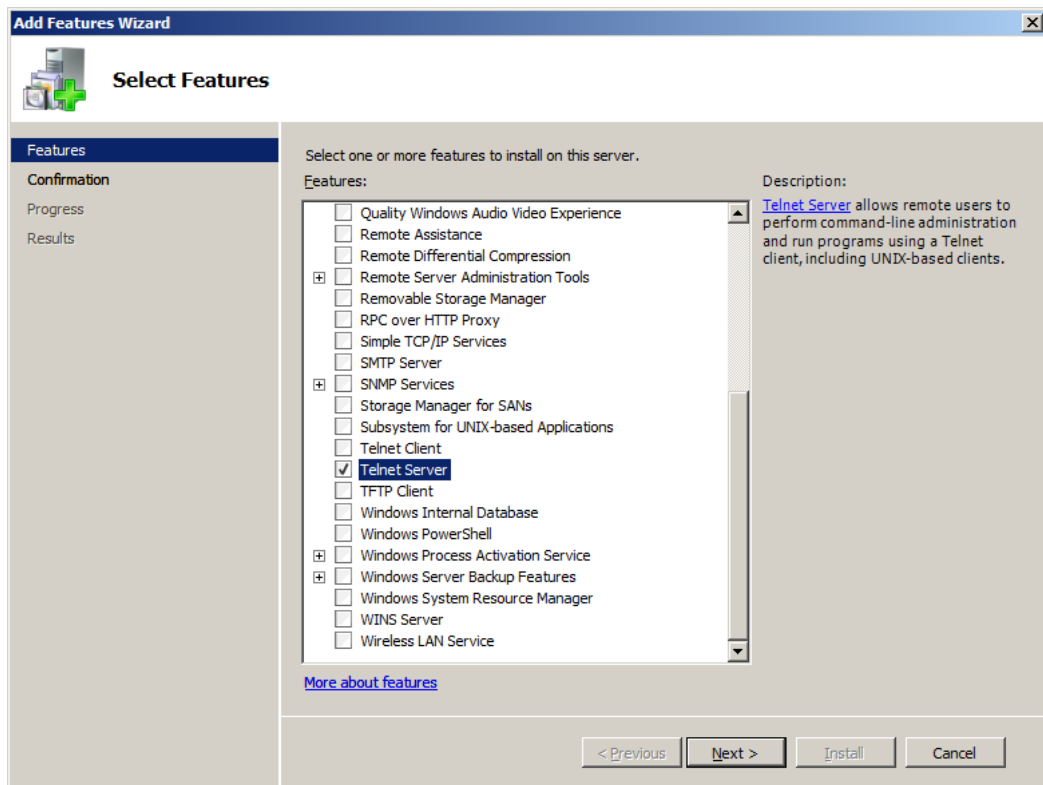
Có nhiều cách tạo tài khoản khác nhau. Ví dụ tạo tài khoản **uitlab/14520123** bằng Command Prompt với lệnh: `net user uitlab 14520123 /add`



Hình 2. Tạo tài khoản *uitlab / 14520123* bằng *Command Prompt*

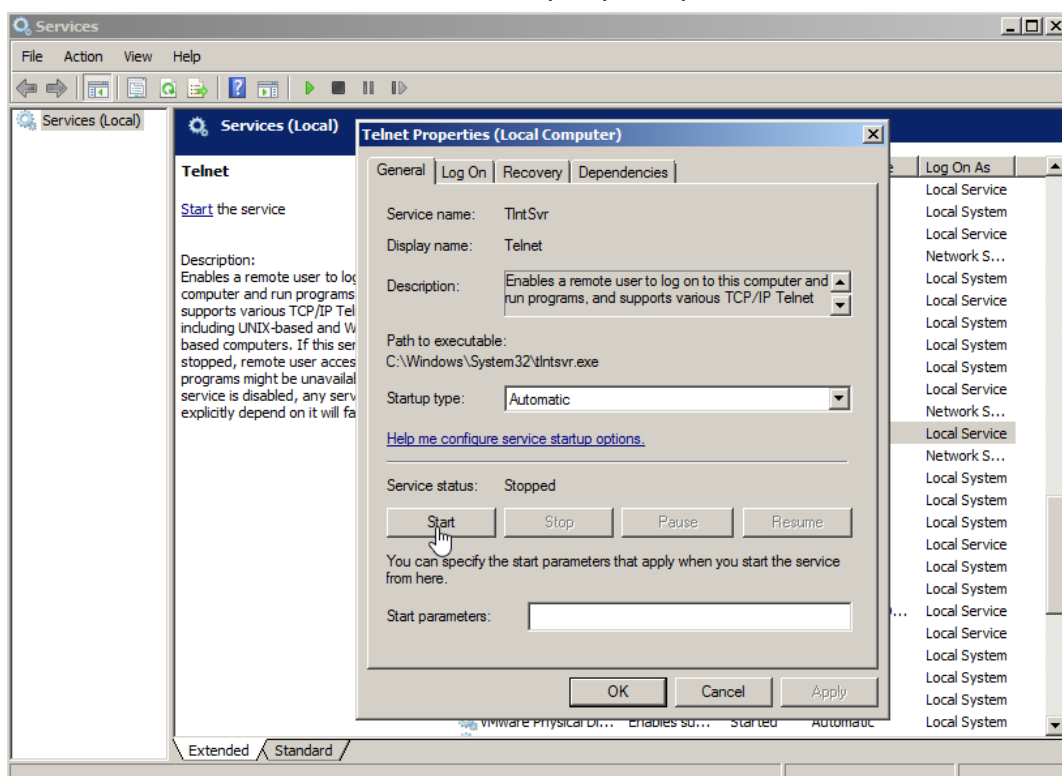
### 2. Bắt gói tin khi sử dụng Telnet

- **Bước 1:** Bật dịch vụ Telnet trên máy chủ Windows Server.
- + Nếu máy chủ chưa có feature Telnet, ta vào **Server Manager** > **Features** > Chọn **Add Feature** > Chọn **Telnet Server** và tiến hành **Install**.



Hình 3. Cài đặt Telnet Server

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

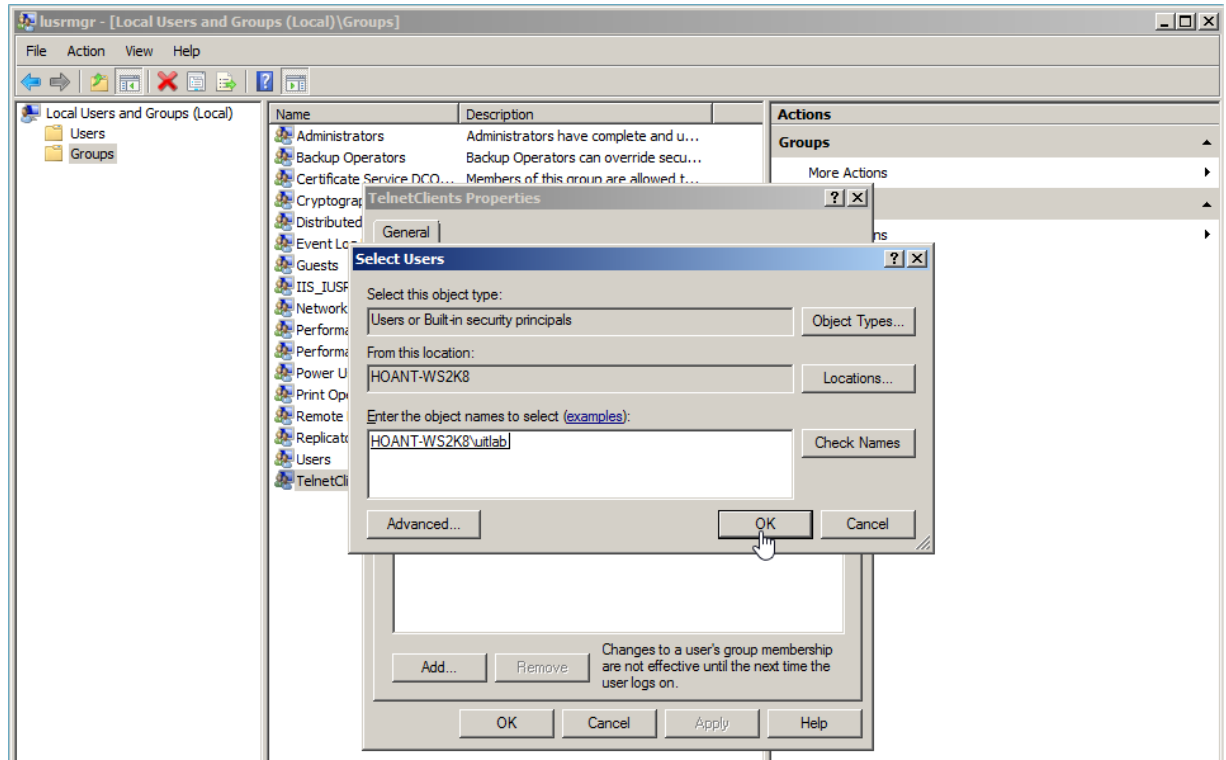


Hình 4. Khởi động dịch vụ Telnet

+ Kiểm tra Telnet server (*tlntsvr.exe*) đã hoạt động chưa bằng lệnh **netstat -ab**

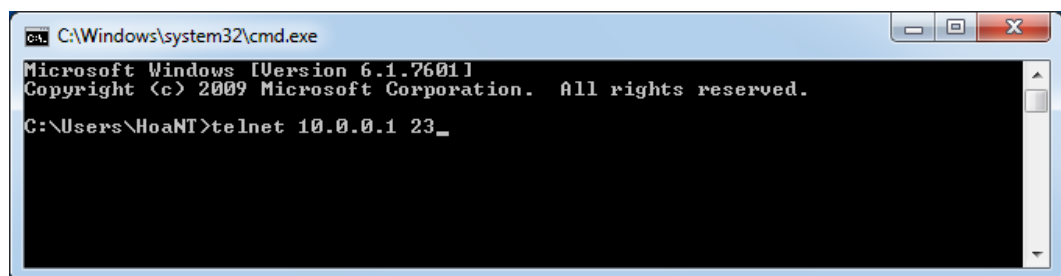
- **Bước 2:** Thêm user Telnet vào TelnetClient Group tại server

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:

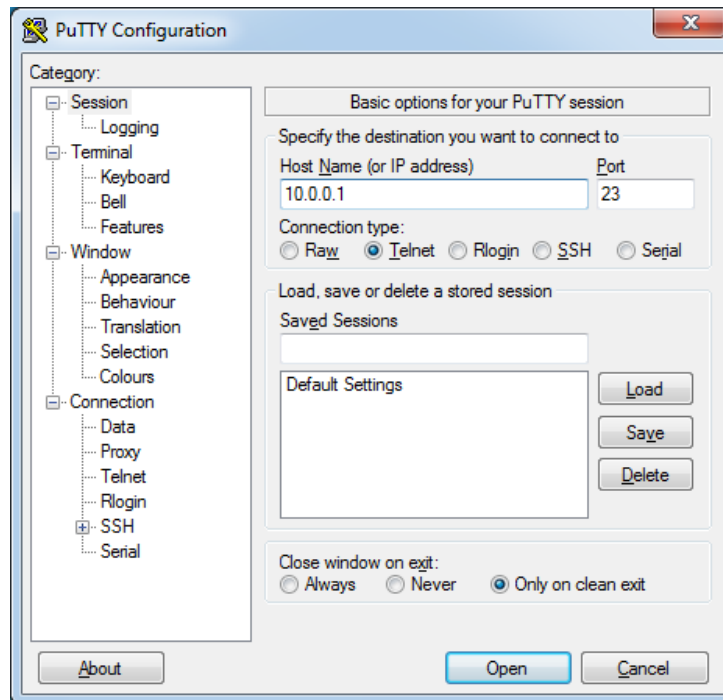


Hình 5. Thêm user utlab vào TelnetClients

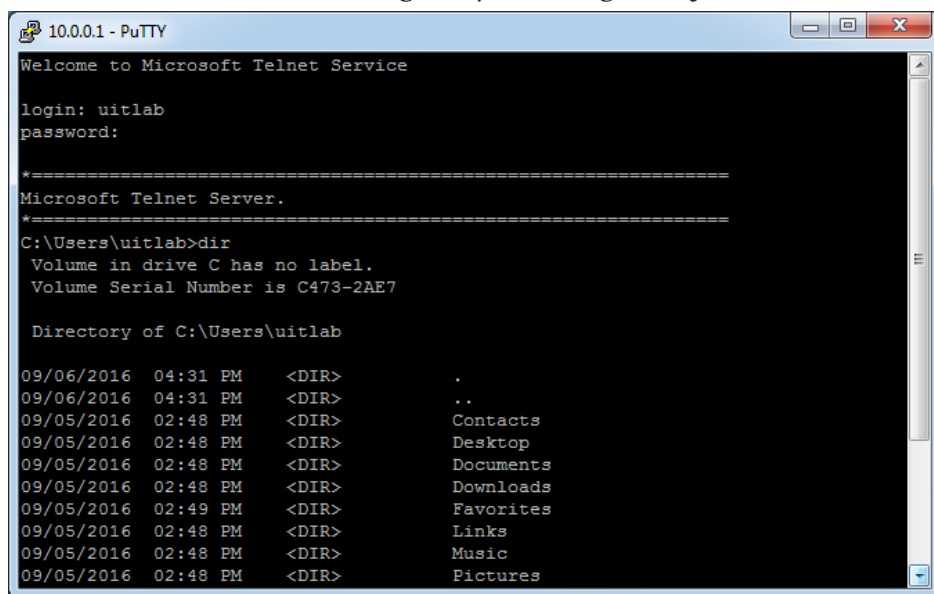
- **Bước 3:** Tại máy Attacker, bật Wireshark để theo dõi và bắt gói tin.
- **Bước 4:** Tại máy Client, dùng Putty hoặc Command Prompt kết nối đến Server bằng Telnet với tài khoản đã tạo ở bước 1 và thực hiện một số thao tác cơ bản như xem, tạo thư mục (dir, mkdir).



Hình 6. Đăng nhập sử dụng Command Prompt

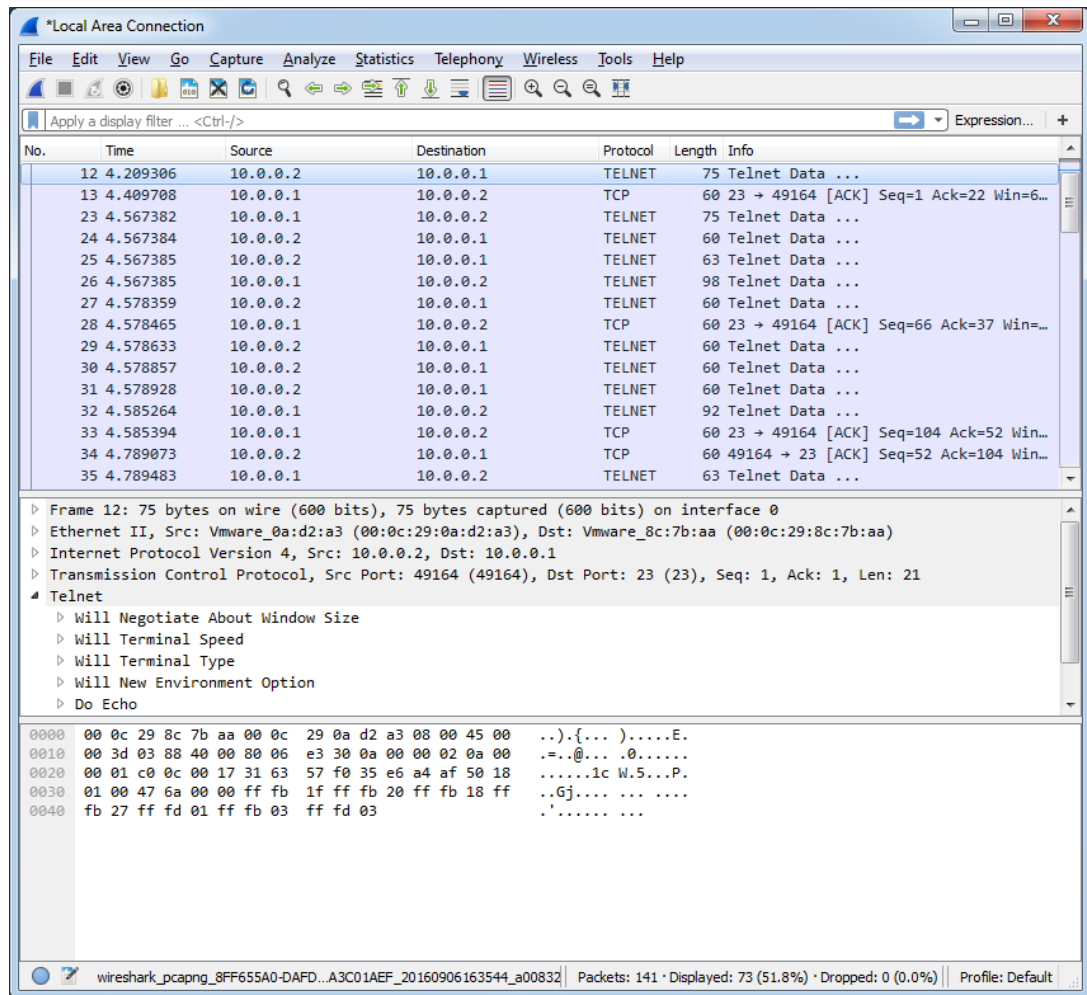


Hình 7. Đăng nhập sử dụng Putty



Hình 8. Telnet thành công vào 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.



Hình 9. Kết quả thu thập được sau khi bắt gói tin

- **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).

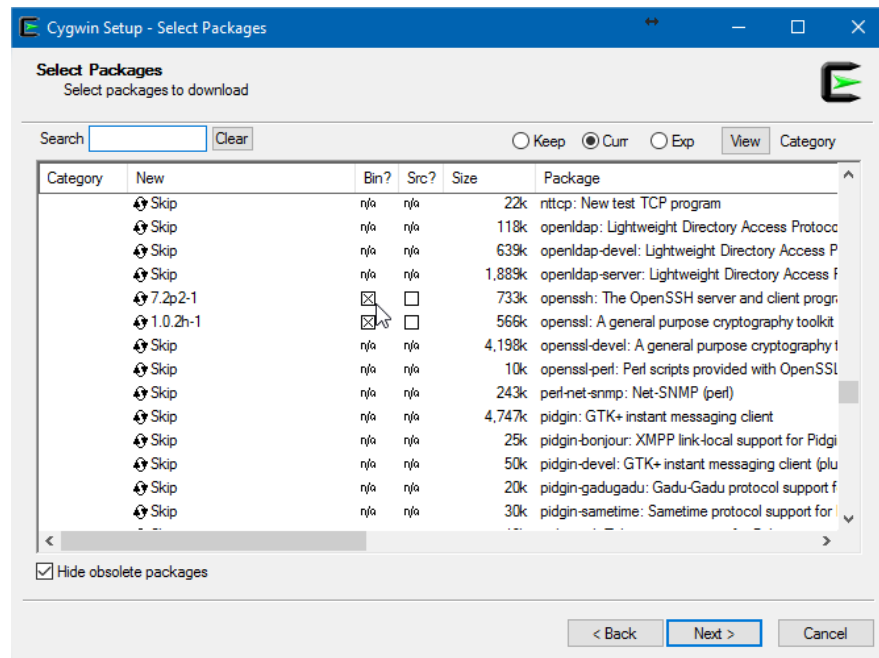
Lặp lại quá trình từ bước 3 đến bước 5 với mật khẩu vừa thay đổi. <sup>[1]</sup>

### 3. 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.

**Lưu ý:** Ở bước Select Packages, mở thẻ Net và chọn gói openssh để cài đặt.

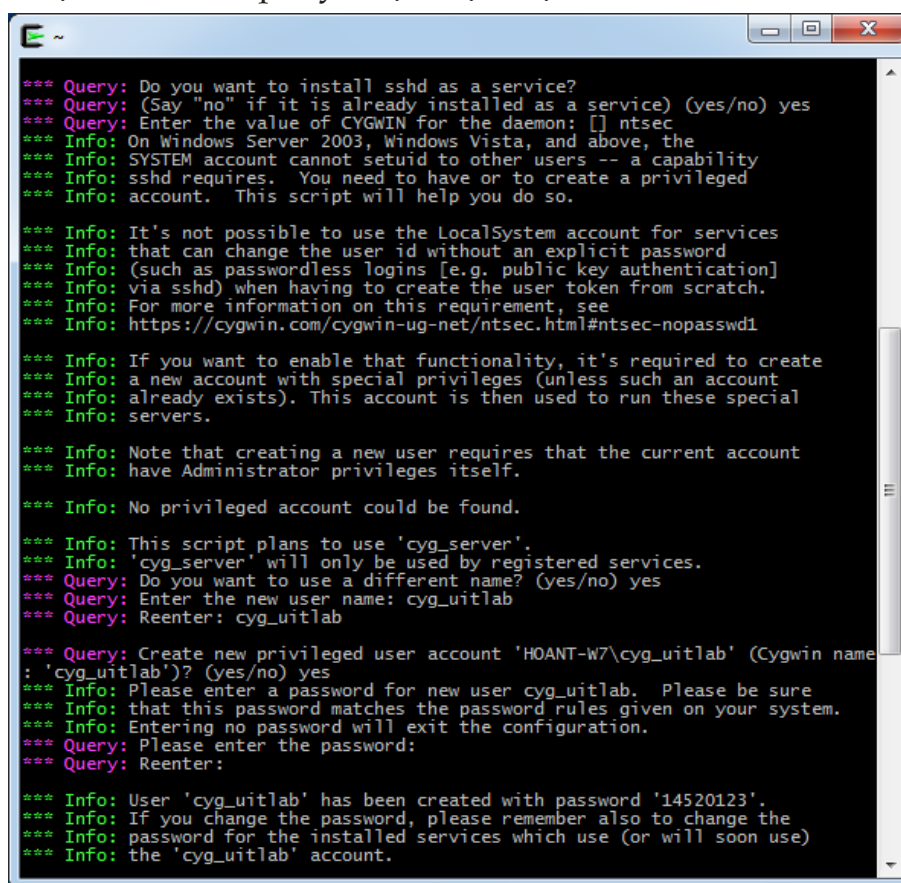


Hình 10. Lưu ý chọn gói openssh (quan trọng)

## ▪ Bước 2: Cấu hình và khởi động SSH server

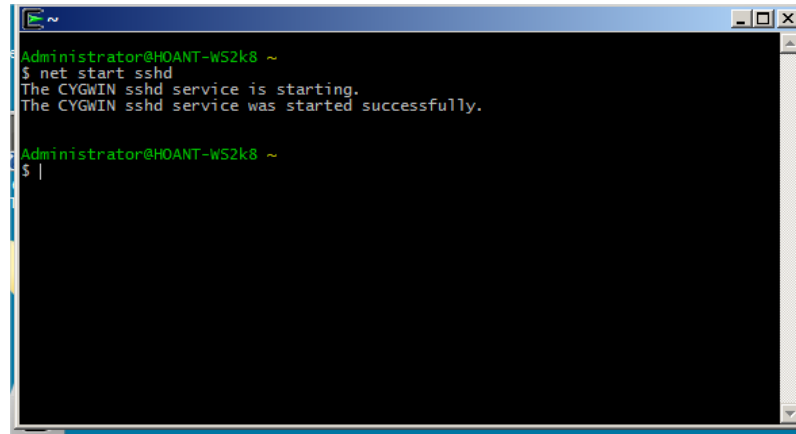
Mở Cygwin Terminal > Cấu hình SSH server bằng lệnh `ssh-host-config` <sup>[2]</sup>.

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



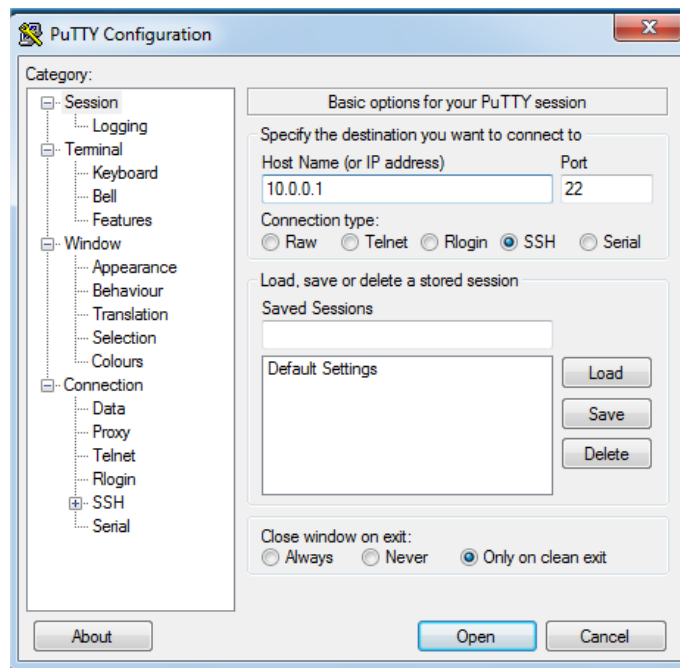
Hình 11. Cấu hình ssh-host-config



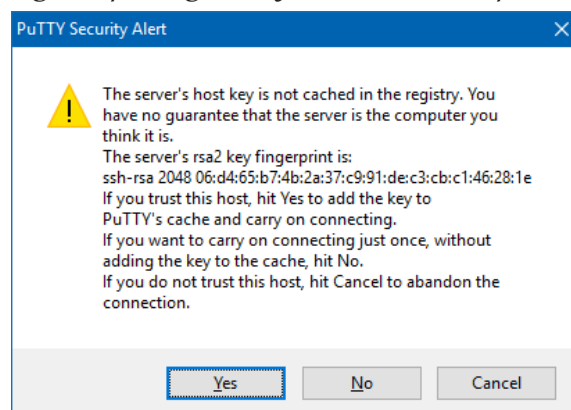


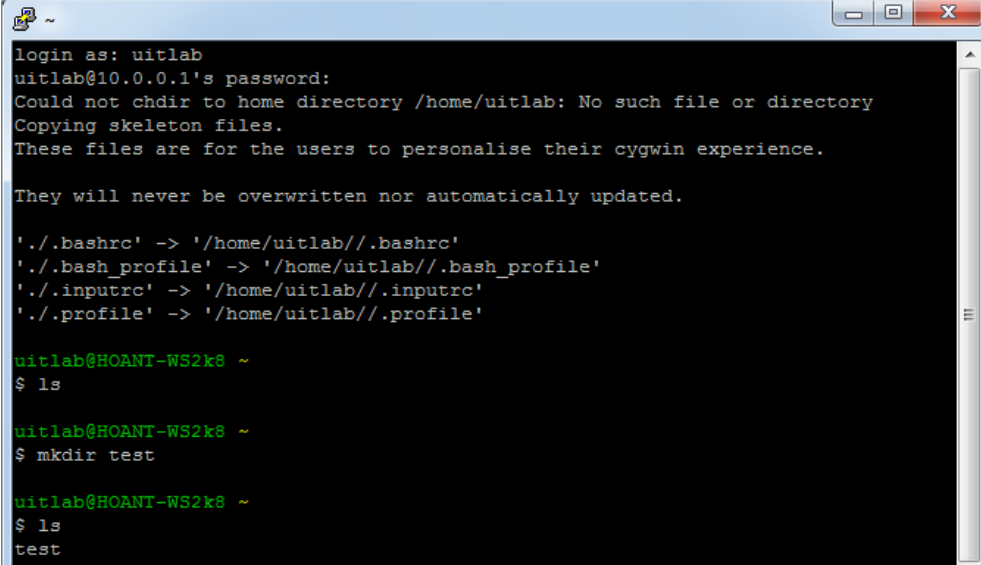
Hình 12. Sau khi cấu hình, khởi động SSH server bằng lệnh `net start sshd`

- **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.



Hình 13. Đăng nhập bằng Putty, chọn Yes ở hộp thoại tiếp theo





```

login as: uitlab
uitlab@10.0.0.1's password:
Could not chdir to home directory /home/uitlab: No such file or directory
Copying skeleton files.
These files are for the users to personalise their cygwin experience.

They will never be overwritten nor automatically updated.

'./bashrc' -> '/home/uitlab/./bashrc'
'./bash_profile' -> '/home/uitlab/./bash_profile'
'./inputrc' -> '/home/uitlab/./inputrc'
'./profile' -> '/home/uitlab/./profile'

uitlab@HOANT-WS2k8 ~
$ ls

uitlab@HOANT-WS2k8 ~
$ mkdir test

uitlab@HOANT-WS2k8 ~
$ ls
test

```

Hình 14. Đăng nhập với tài khoản uitlab

- **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.

## C. CÂU HỎI

Sau quá trình thực hành và nắm được các kiến thức nền tảng, sinh viên trả lời các câu hỏi sau:

1. Telnet và SSH là gì và được ứng dụng trong trường hợp nào?
2. So sánh Telnet và SSH.
3. Khi sử dụng SSH, còn có cách nào để đăng nhập ngoài cách dùng username và mật khẩu truyền thống? *Thực hiện demo minh họa nếu có thể.*

## D. YÊU CẦU

- Sinh viên tìm hiểu và thực hành theo hướng dẫn. Có thể thực hiện theo nhóm (2 sinh viên/nhóm) hoặc thực hiện cá nhân. Đăng ký nhóm cố định từ buổi 1.
- Sinh viên báo cáo kết quả thực hiện và nộp bài gồm:

### - Báo cáo:

- + Trình bày trong file Word (.doc, .docx) hoặc .PDF theo mẫu có sẵn tại courses.
  - + Đặt tên theo định dạng: [Mã lớp]-LabX\_MSSV1-Tên SV1\_MSSV2-Tên SV2
- Ví dụ: [NT101.H11.1]-Lab1\_14520000-Viet\_14520999-Nam.

### - Video:

- + Quay lại quá trình thực hiện Lab của sinh viên.
- + Upload lên Youtube.com và chèn link vào đầu báo cáo theo mẫu.

Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.

Nộp file báo cáo trên theo thời gian đã thống nhất tại [courses.uit.edu.vn](http://courses.uit.edu.vn).

**Đánh giá:** Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt và đóng góp tích cực tại lớp.
- Video trình bày trực quan, dễ hiểu.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.*

## **E. THAM KHẢO**

[1] Demo Cấu hình Telnet Server:

[https://www.youtube.com/watch?v=eDW7N\\_v4dxg&feature=youtu.be](https://www.youtube.com/watch?v=eDW7N_v4dxg&feature=youtu.be)

[2] Cài đặt Cygwin trên Windows Server 2008

[http://wiki.nikoforge.org/Cygwin\\_installation\\_on\\_a\\_Windows\\_Server\\_2008R2](http://wiki.nikoforge.org/Cygwin_installation_on_a_Windows_Server_2008R2)

**HẾT**