

BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG  
TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG TP.HCM  
KHOA: HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM



**BÀI LAB CÁ NHÂN  
AN TOÀN BẢO MẬT MÁY TÍNH VÀ HỆ THỐNG**

Giáo viên hướng dẫn: **ThS. Phạm Trọng Huynh**

Sinh viên thực hiện: **Lê Thị Bảo Yến**

Lớp: **08\_DH\_CNPM**

Khóa: **08**

*TP. Hồ Chí Minh, Tháng 5 Năm 2023*

## MỤC LỤC

<b>LAB 01: BẮT GÓI TIN TELNET – SSH.....</b>	1
A. Thực hành .....	1
1. Thiết lập môi trường.....	1
2. Bắt gói tin khi sử dụng Telnet .....	2
3. Bắt gói tin khi sử dụng SSH .....	8
B. Trả lời câu hỏi.....	18
1. Telnet và SSH là gì và được ứng dụng trong trường hợp nào?.....	18
2. So sánh Telnet và SSH.....	18
3. Khi sử dụng SSH, còn có cách nào để đăng nhập ngoài cách dùng username và mật khẩu truyền thống? .....	20
<b>LAB 02: KEYLOGGER TRÊN PC VÀ ĐIỆN THOẠI.....</b>	21
A. Thực hành .....	21
1. Thủ nghiệm Keylogger đơn giản với REFOG Free Keylogger.....	21
B. Trả lời câu hỏi .....	24
1. Nêu biện pháp phòng tránh, cách phát hiện Keylogger trên máy tính - điện thoại.....	24
2. Tìm thêm và giới thiệu một số loại Keylogger trên máy tính - điện thoại khác. ....	27
<b>LAB 03: THIẾT LẬP MÔ HÌNH TƯỜNG LỬA SOPHOS UTM .....</b>	37
A. Thực hành .....	37
1. Thiết lập máy chủ Domain Controller.....	37
2. Cài đặt và cấu hình máy Firewall Sophos UTM .....	44
B. Trả lời câu hỏi .....	60

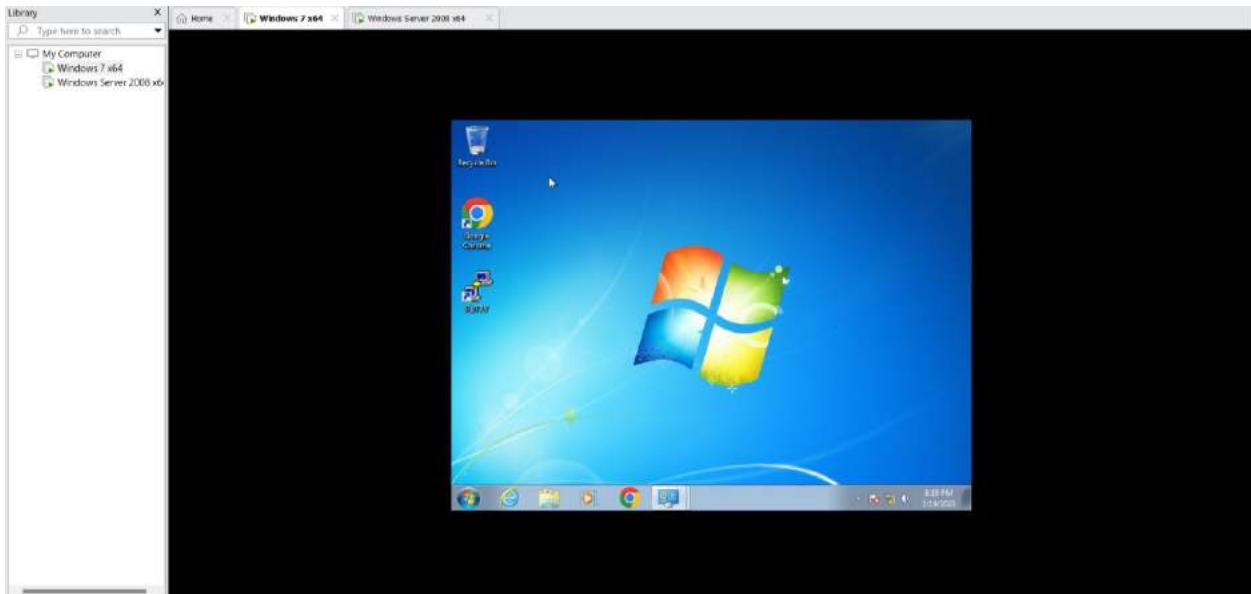
<b>1. Nêu nguyên tắc hoạt động của Firewall Sophos UTM và Domain Controller trong mô hình mạng đã thiết lập trong bài lab.</b>	60
<b>LAB 04: THIẾT LẬP RULES TƯỜNG LỬA SOPHOS UTM</b>	62
<b>A. Thực hành</b>	62
<b>2. Thiết lập một số kịch bản quy định về chính sách với tài khoản tại Domain ..</b>	71
<b>LAB 05: TƯỜNG LỬA SOPHOS UTM: XÂY DỰNG CHÍNH SÁCH WEB</b>	79
<b>A. Tổng quan</b>	79
<b>B. Thực hành</b>	79
<b>1. Tổng quan về xây dựng chính sách bảo vệ truy cập web.....</b>	79
<b>3. Kiểm tra kết quả &amp; ứng dụng .....</b>	89
<b>LAB 06: TƯỜNG LỬA SOPHOS UTM: CHÍNH SÁCH ỦNG DỤNG .....</b>	99
<b>A. Tổng quan</b>	99
<b>B. Thực hành</b>	99
<b>1. Tổng quan về xây dựng chính sách kiểm soát ứng dụng .....</b>	99
<b>2. Xây dựng bộ chính sách kiểm soát ứng dụng và triển khai CA (HTTPS) .....</b>	101
<b>3. Kiểm tra kết quả &amp; ứng dụng .....</b>	107
<b>LAB 07: LOCAL DNS ATTACK .....</b>	111
<b>A. Môi trường .....</b>	111
<b>B. Thiết lập IP tĩnh cho cả 3 máy.....</b>	111
2.1. Install and configura the DNS server.....	114
2.2. Cấu hình máy User .....	122
2.3. Attacker.....	124
2.4. Ta sử dụng lệnh dig www.example.com trên máy User để xem một vài thông tin về domain www.example.com .....	126

3.1. Attacker have already compromised the victim's machine.....	127
3.2 Directly Spoof Response to User .....	128
3.3 DNS server Cache Poisoning.....	130
<b>ĐỘ AN TOÀN CỦA HỆ CHỮ KÝ ELGAMAL .....</b>	<b>132</b>
<b>I. Hệ chữ ký Elgamal là gì? .....</b>	<b>132</b>
1.1 Tổng quan .....	132
1.2 So sánh với các hệ mã hóa khác .....	132
<b>II. Cách tạo chữ ký số trong hệ thống ElGamal.....</b>	<b>133</b>
2.1 Tạo khóa .....	133
2.2 Tạo chữ ký .....	133
2.3 Xác minh chữ ký.....	133
<b>III. Demo.....</b>	<b>134</b>

## LAB 01: BẮT GÓI TIN TELNET – SSH

### A. Thực hành

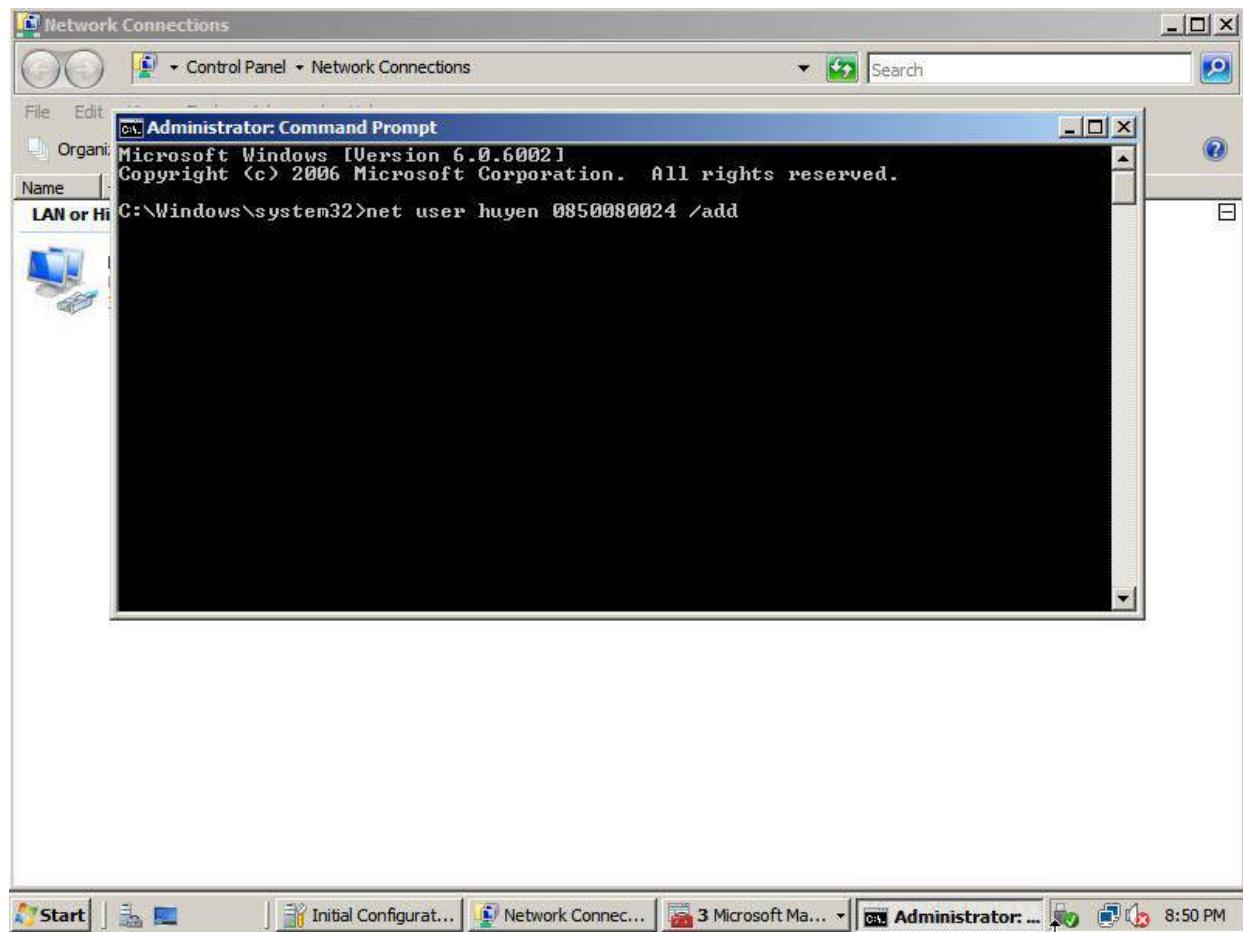
- Một máy chủ Window Server 2008
- 1 Máy Client Windows có phần mềm Putty
- 1 Máy Attacker Windows tham gia bắt gói tin có phần mềm Wireshark.



#### 1. Thiết lập môi trường

Tại máy chủ, tạo một tài khoản với username = Tên sinh viên, mật khẩu = MSSV.

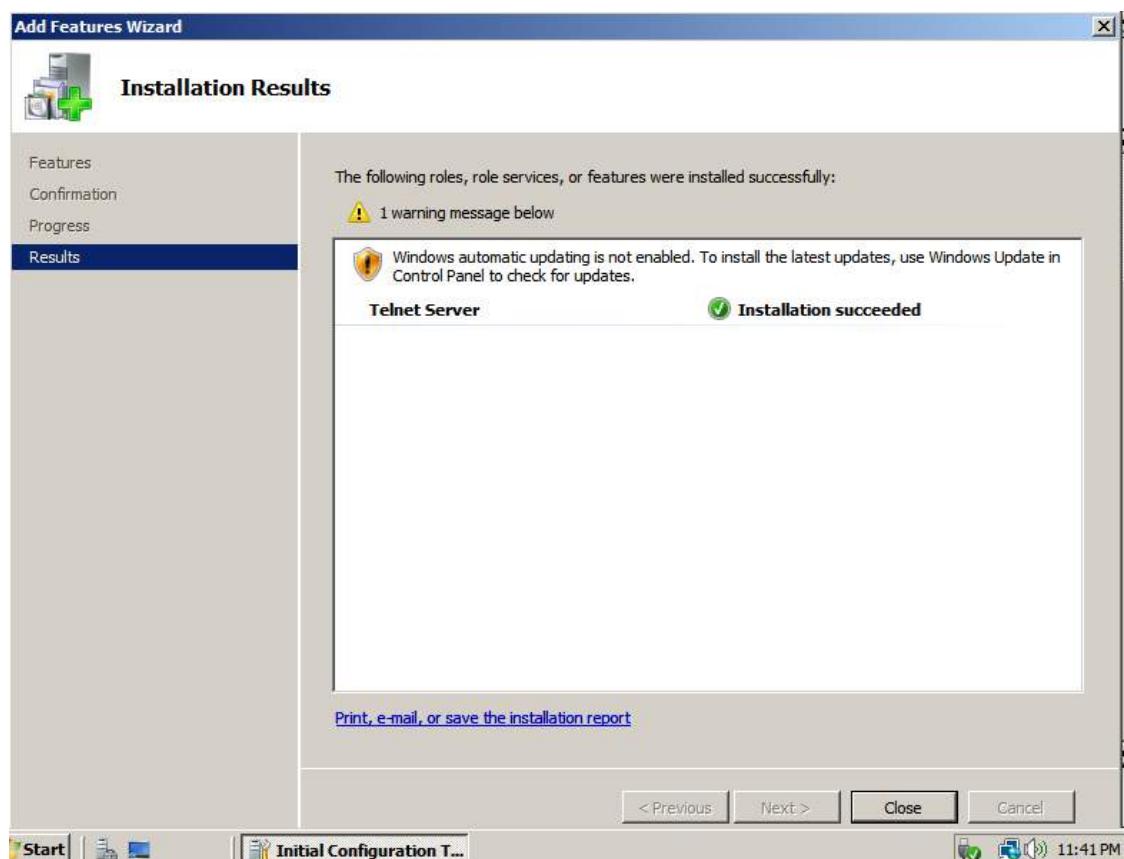
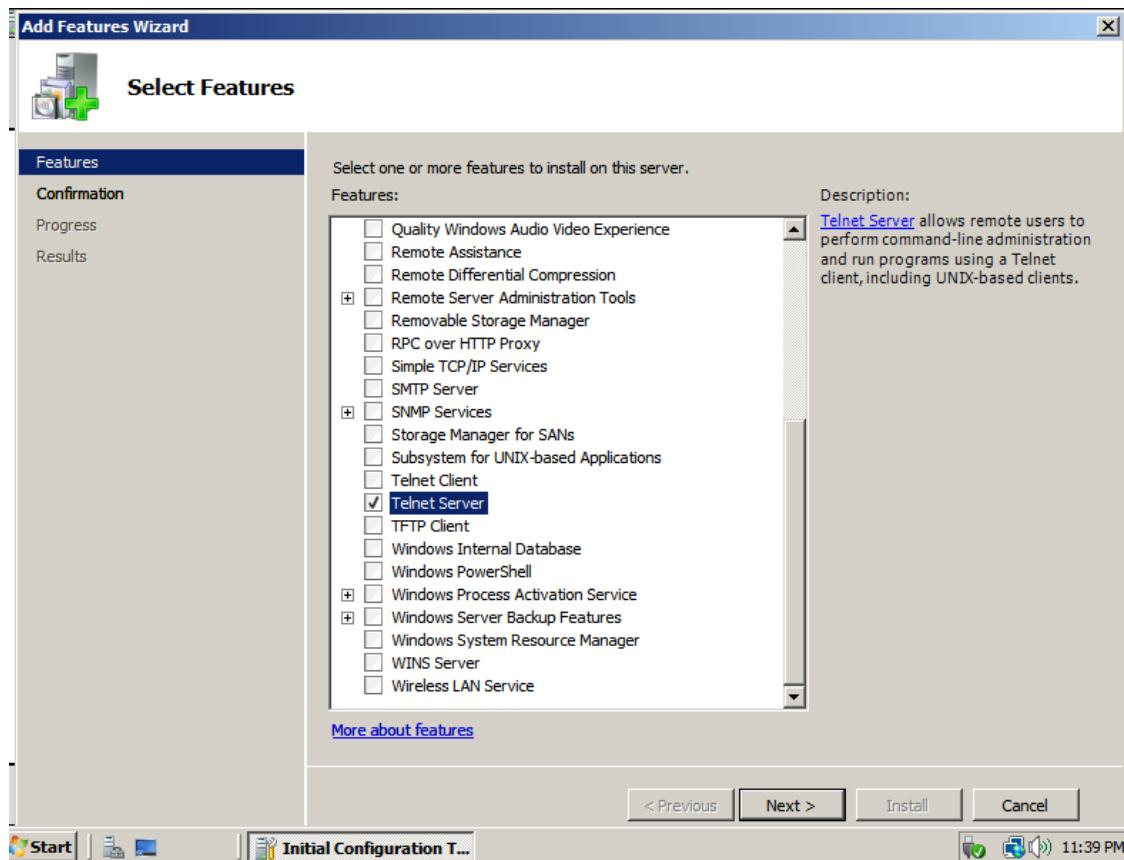
Command Prompt với lệnh: net user huyen 0850080024 /add



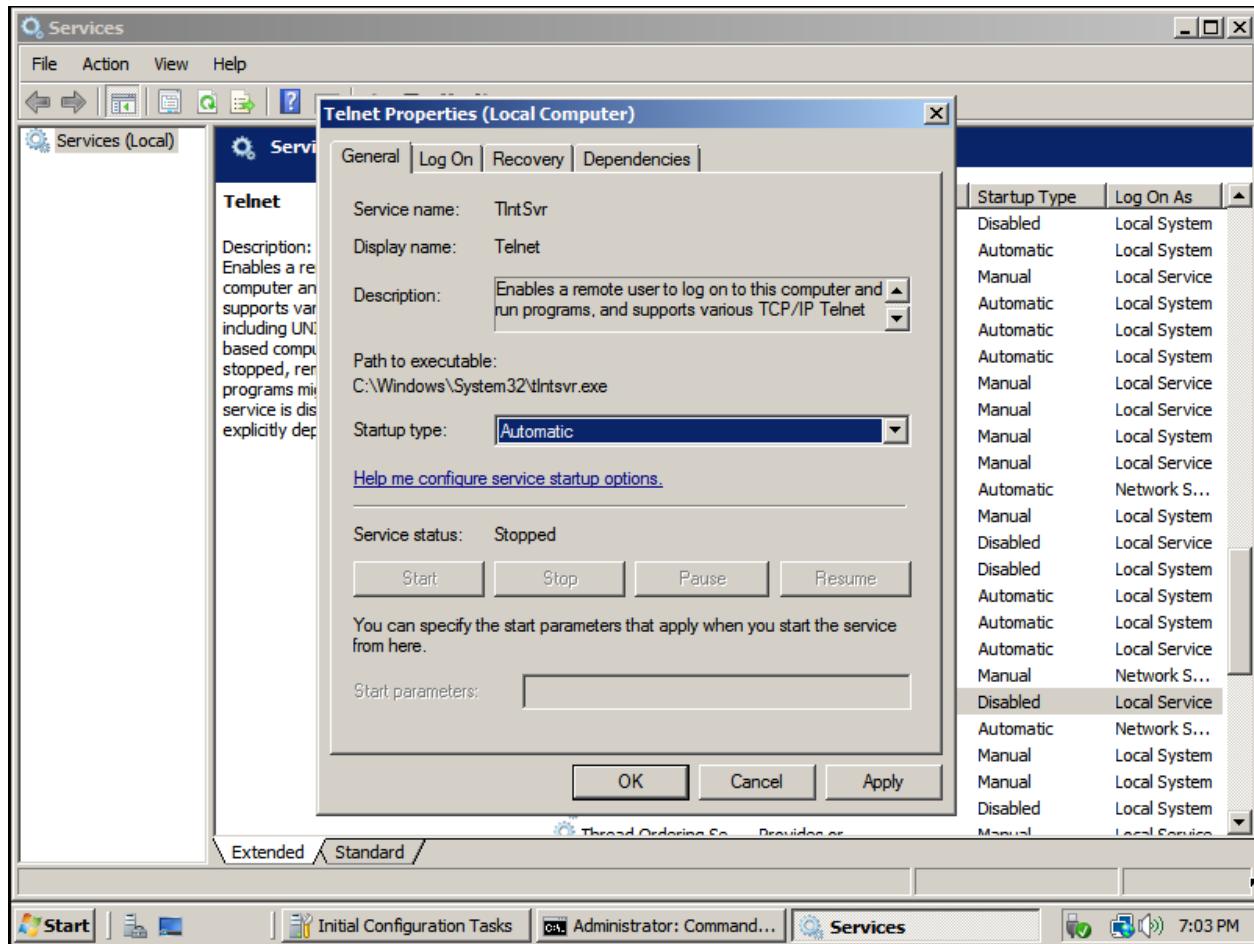
## 2. Bắt gói tin khi sử dụng Telnet

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

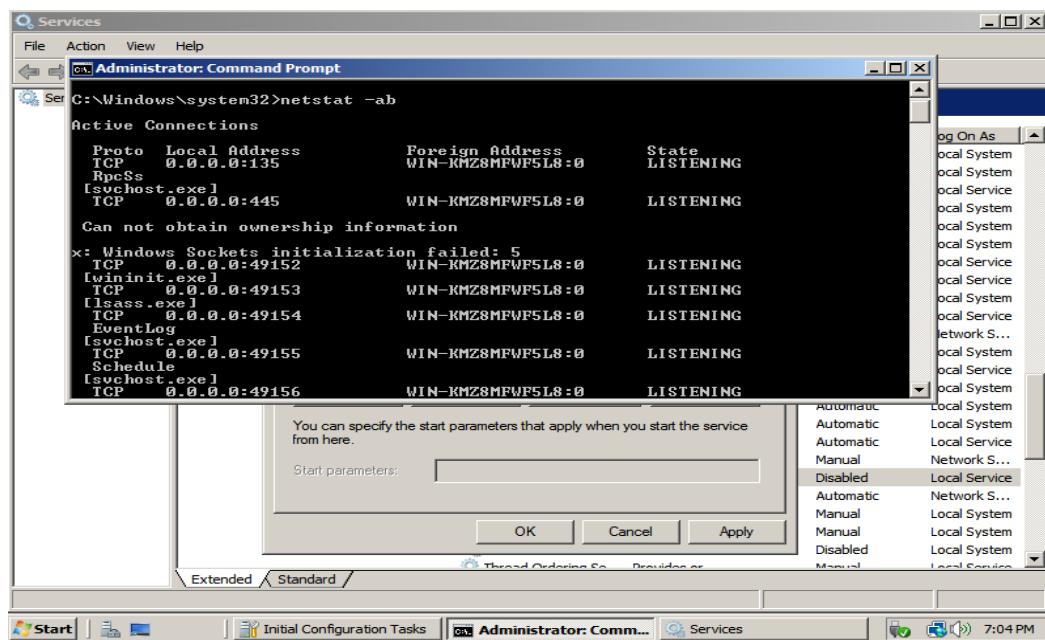
- Nếu máy chủ chưa có feature Telnet, ta vào Server Manager > Features > Chọn Add Feature > Chọn Telnet Server và tiến hành Install.



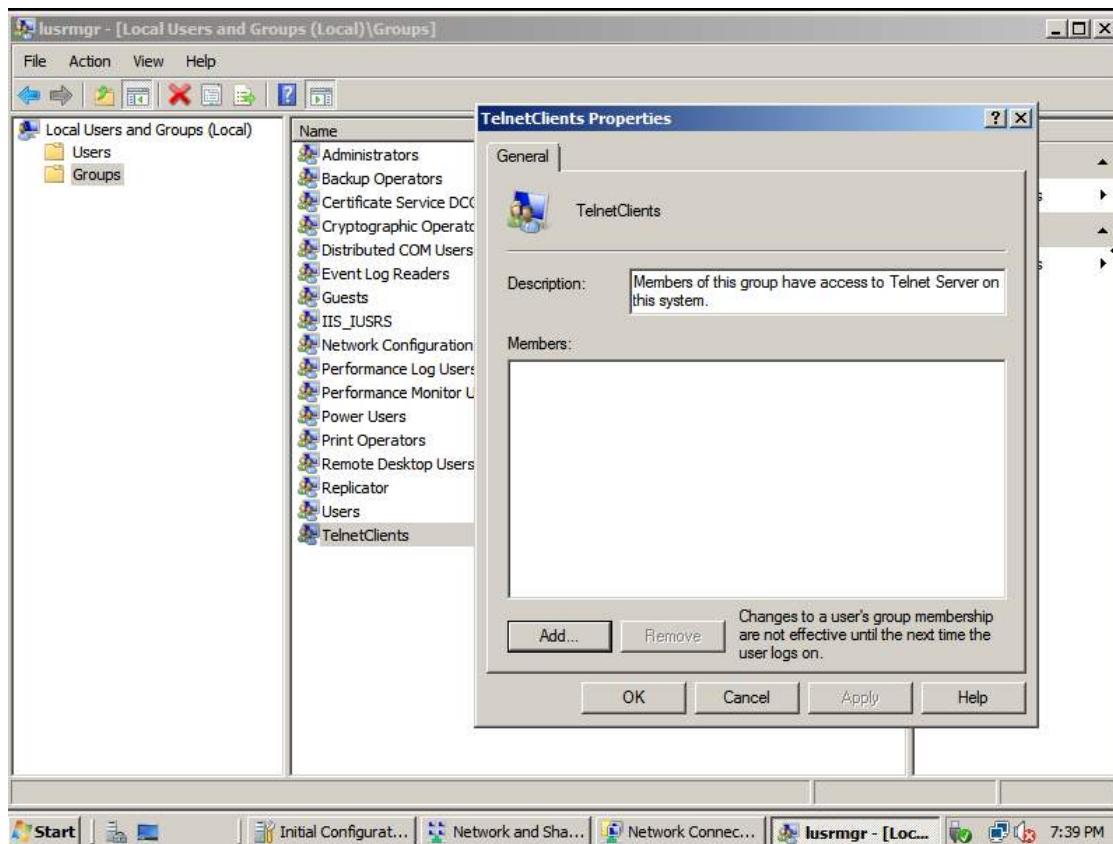
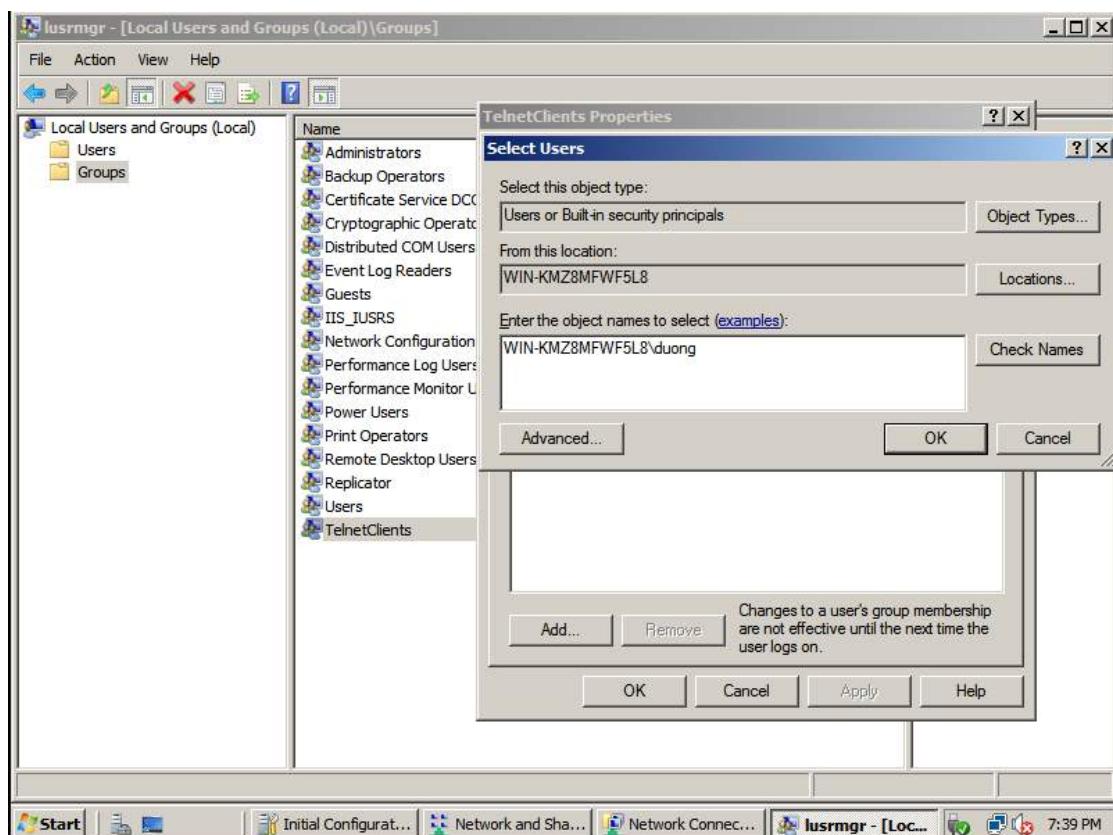
- Vào Start > Run > Gõ services.msc > Bật dịch vụ Telnet



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

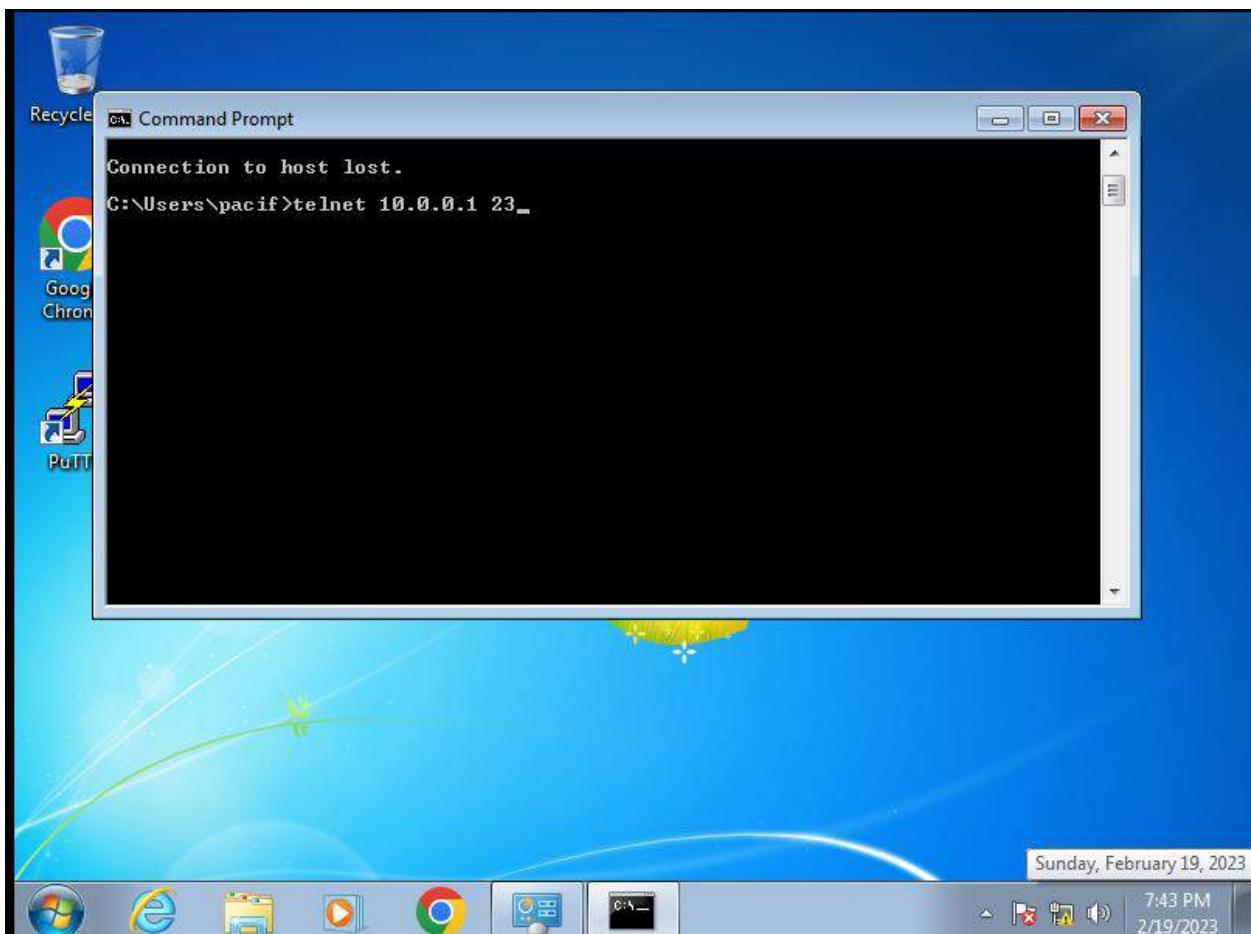


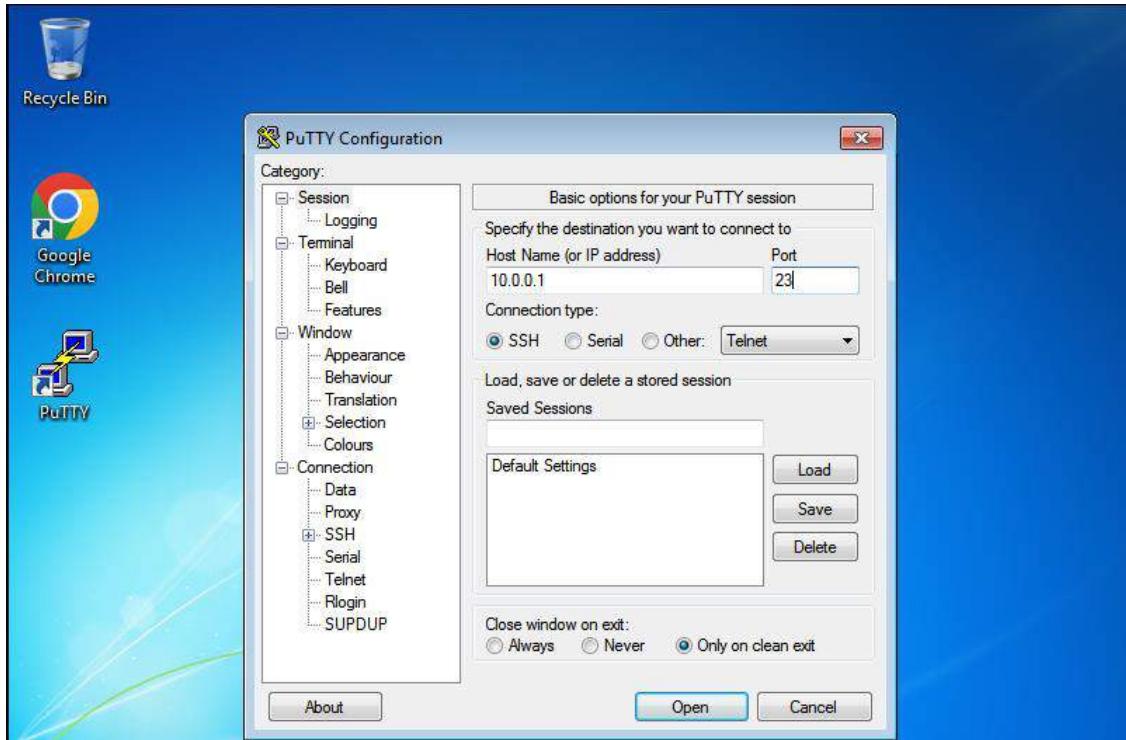
## Bước 2: Thêm user Telnet vào TelnetClient Group tại server



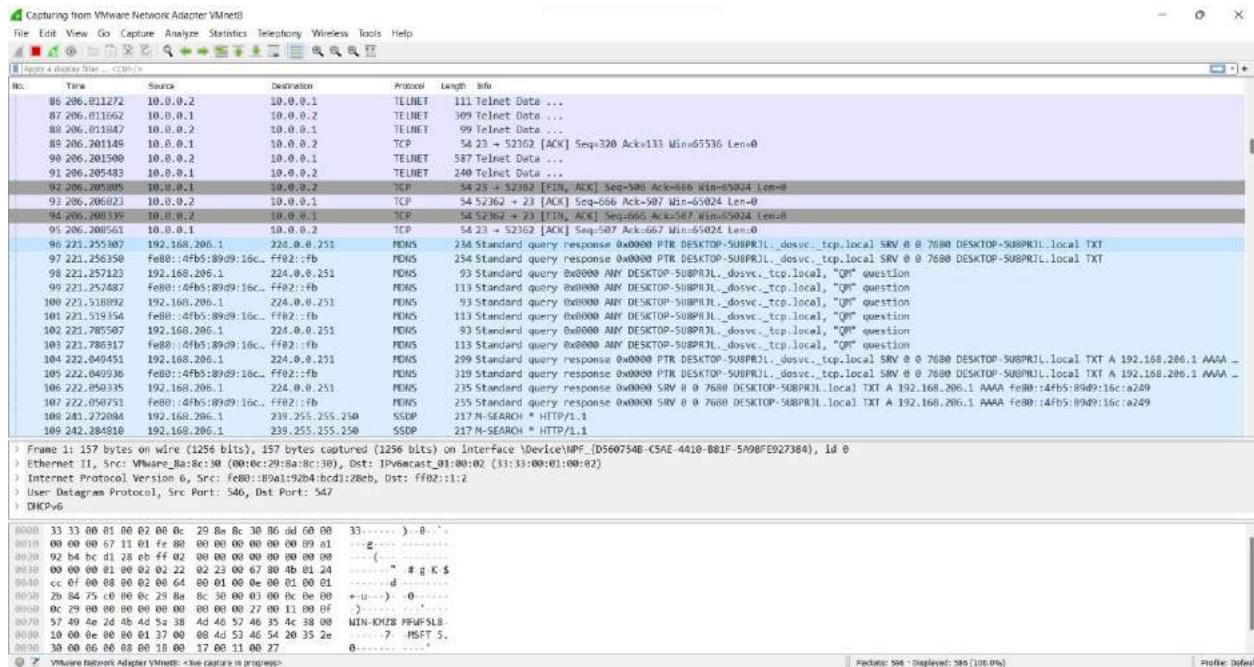
**Bước 3:** Tại máy Attacker, bật Wireshark để theo dõi và bắt gói tin.

**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).





Bước 5: Dùng 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.



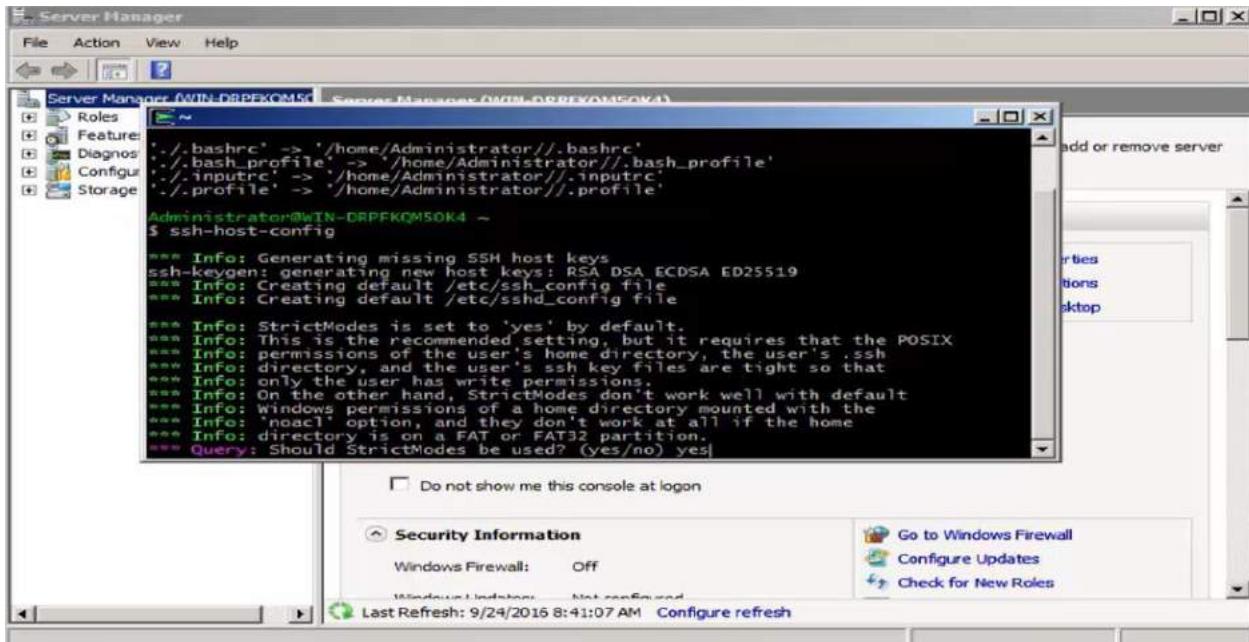
Bước 6: Thay đổi mật khẩu tài khoản đã tạo ở bước 3 thành mật khẩu phức tạp hơn (>10 ký tự, gồm chữ, số và ký tự đặc biệt). Lặp lại quá trình từ bước 3 đến bước 5 với mật khẩu vừa thay đổi.

### 3. Bắt gói tin khi sử dụng SSH

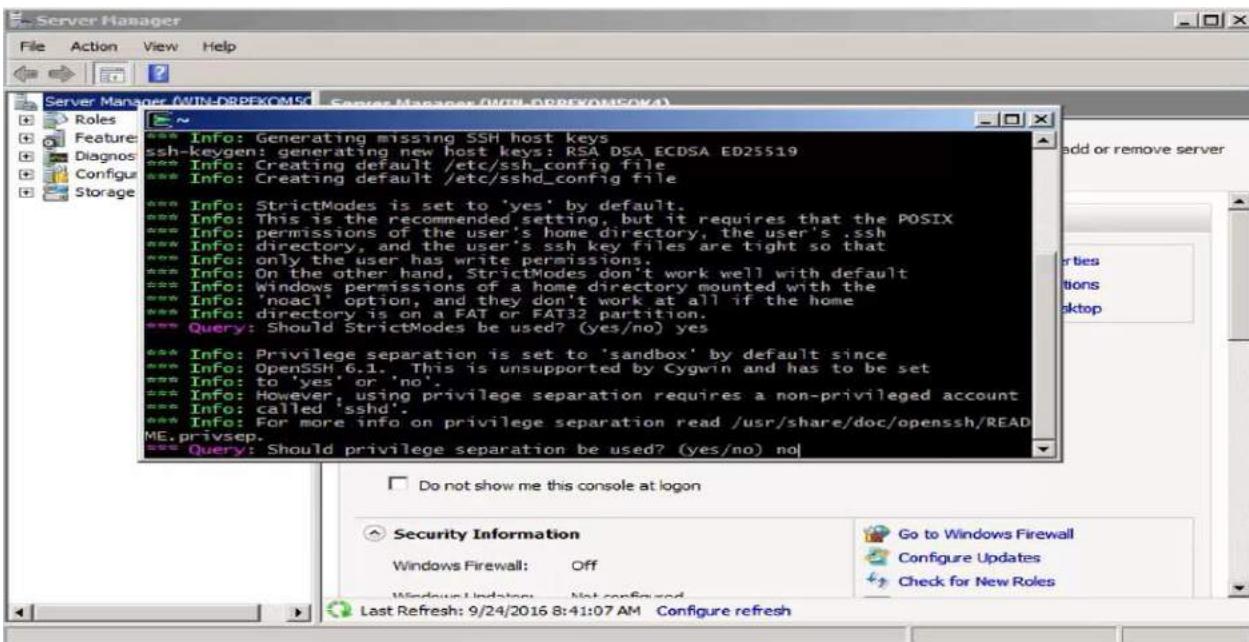
Cài đặt Cygwin để thiết lập SSH server tại máy chủ

Cấu hình và khởi động SSH server

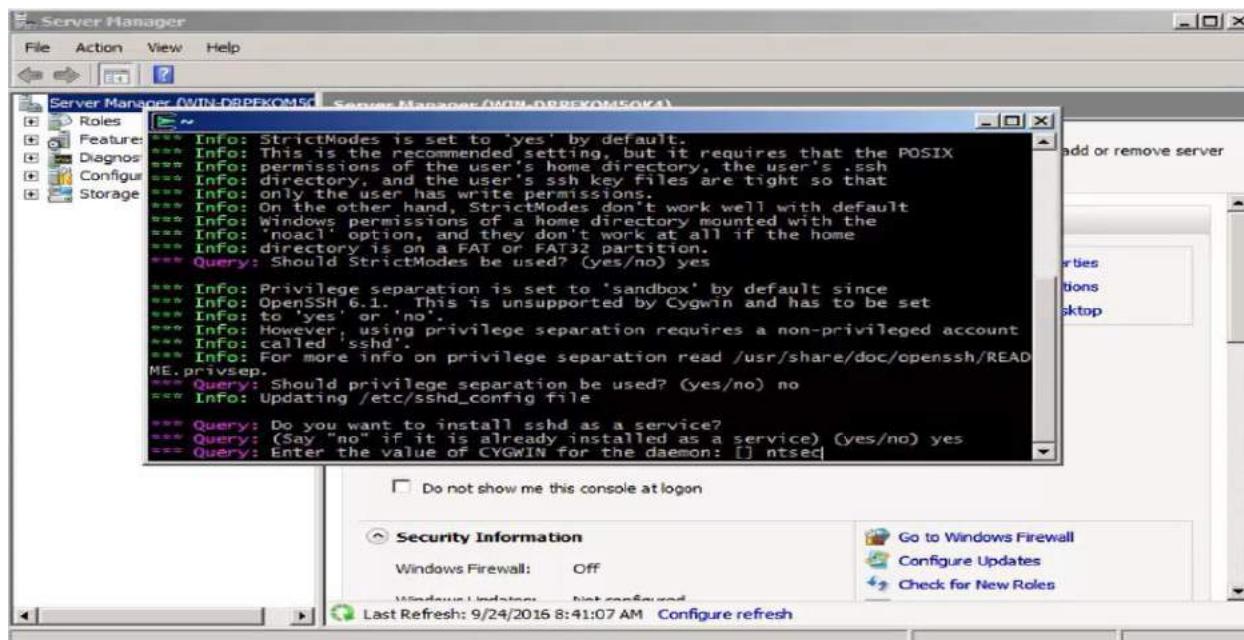
Mở Cygwin Terminal > Cấu hình SSH server bằng lệnh “ssh-host-config” sau đó chọn yes



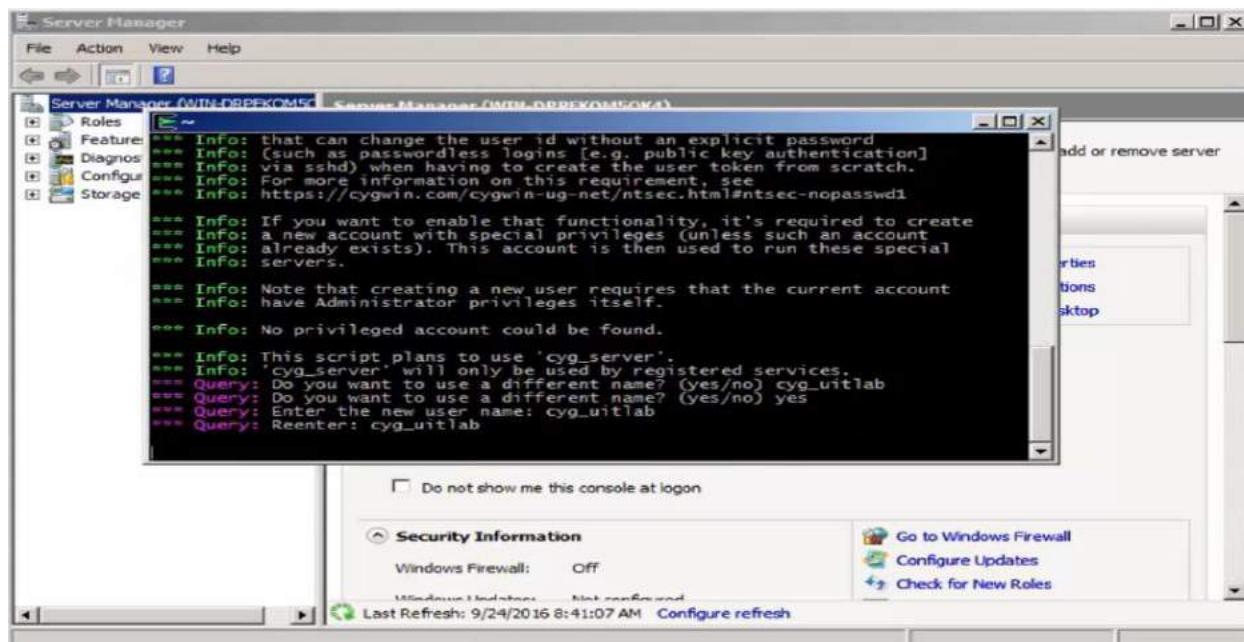
Nhập “no”



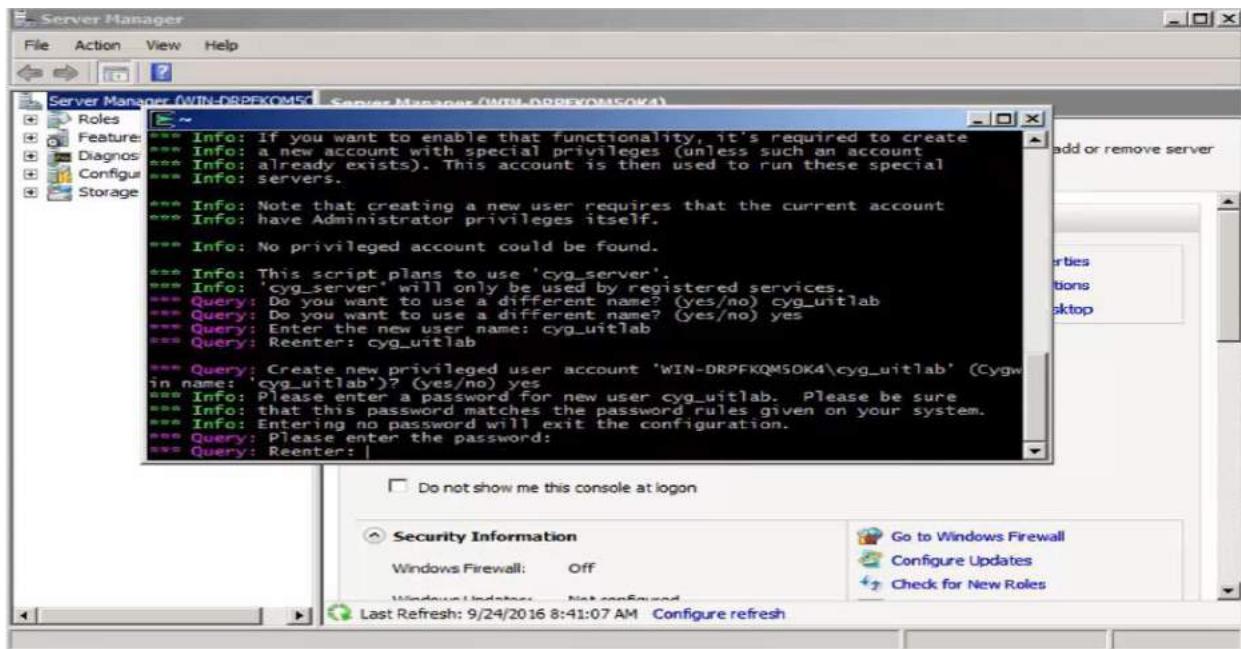
Nhập “yes” sau đó nhập “ntsec”



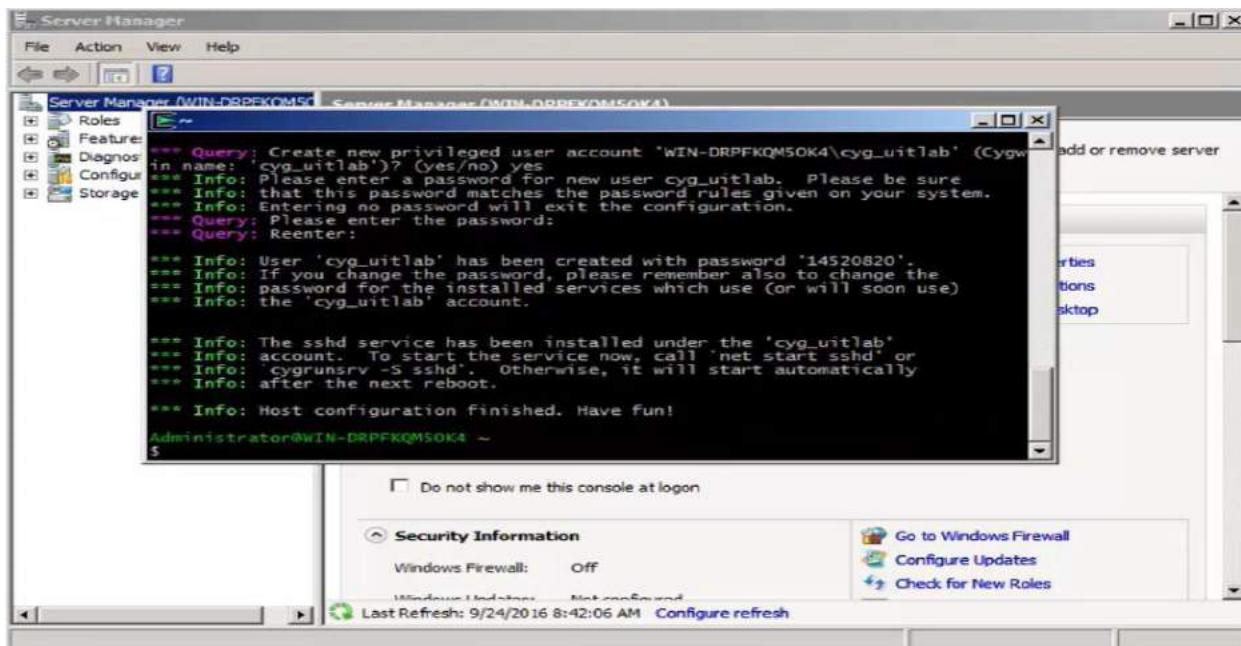
Nhập “cyg\_uitlab” sau đó nhập “yes”. Nhập username mới “cyg\_uitlab” và nhập lại



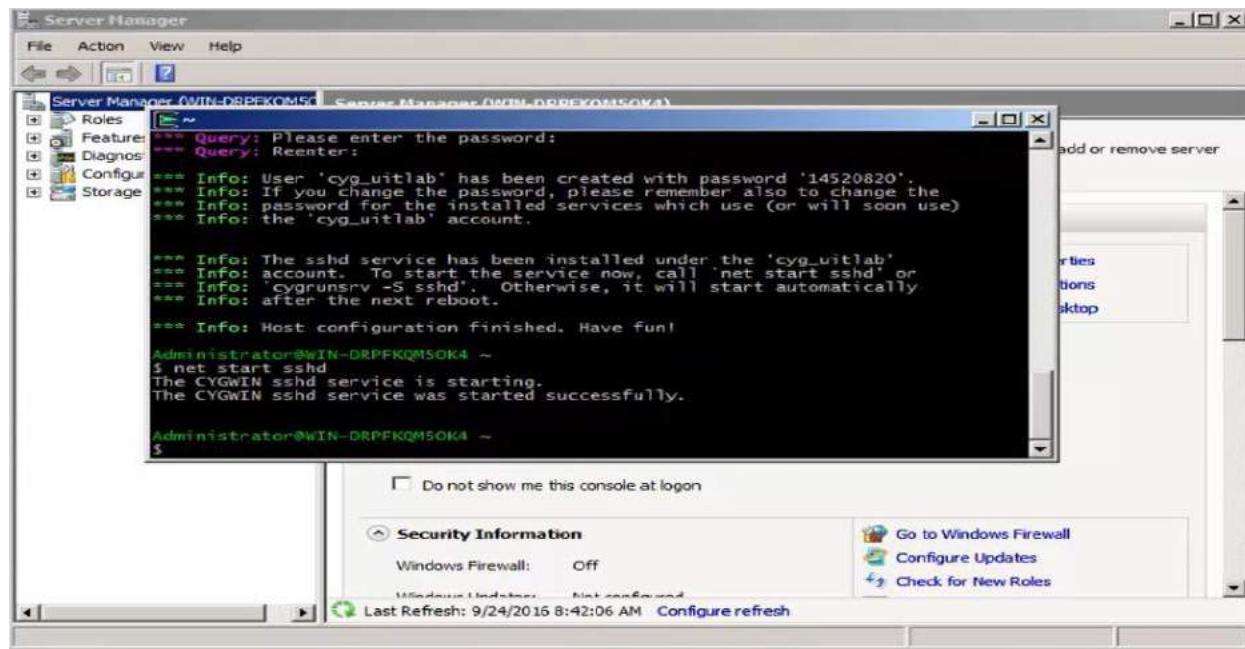
Nhập “yes”. Sau đó nhập mật khẩu rồi nhập lại



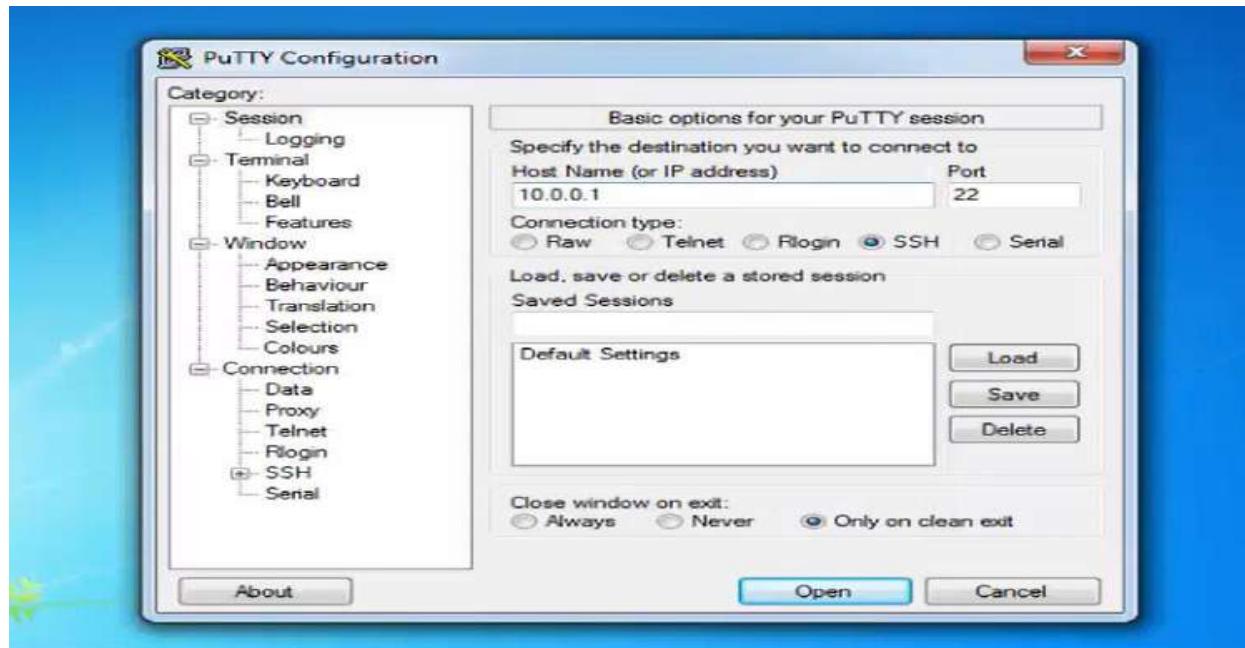
### Thiết lập hoàn tất



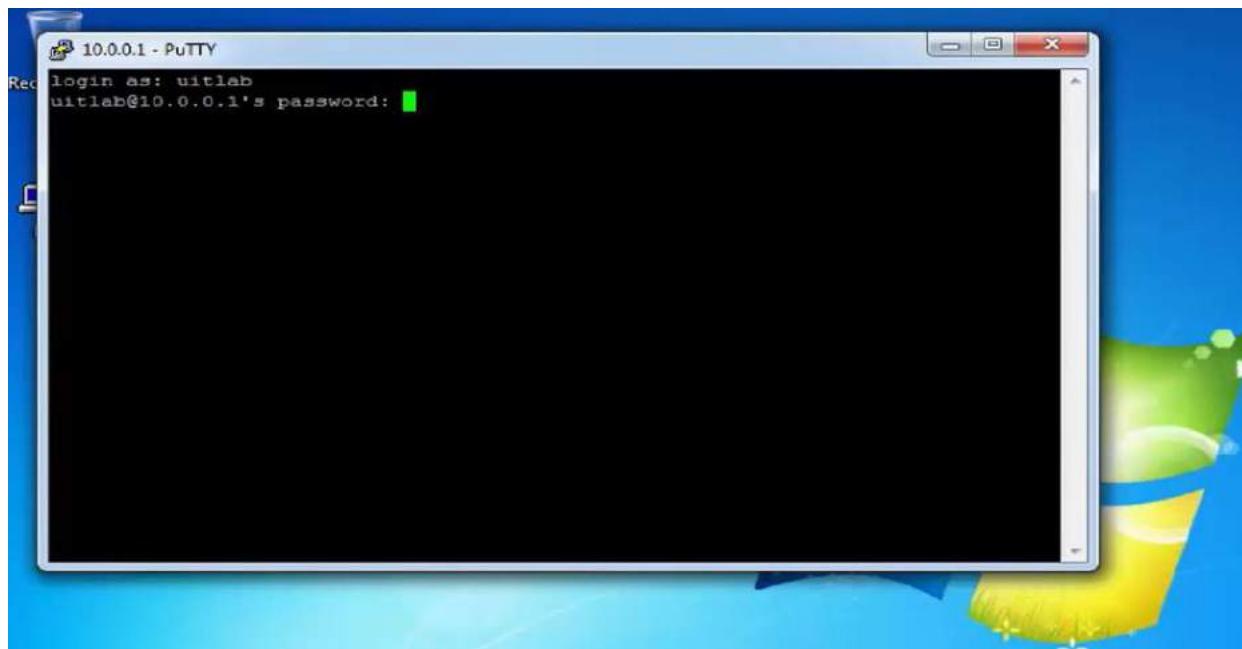
Nhập “net start sshd” để khởi động



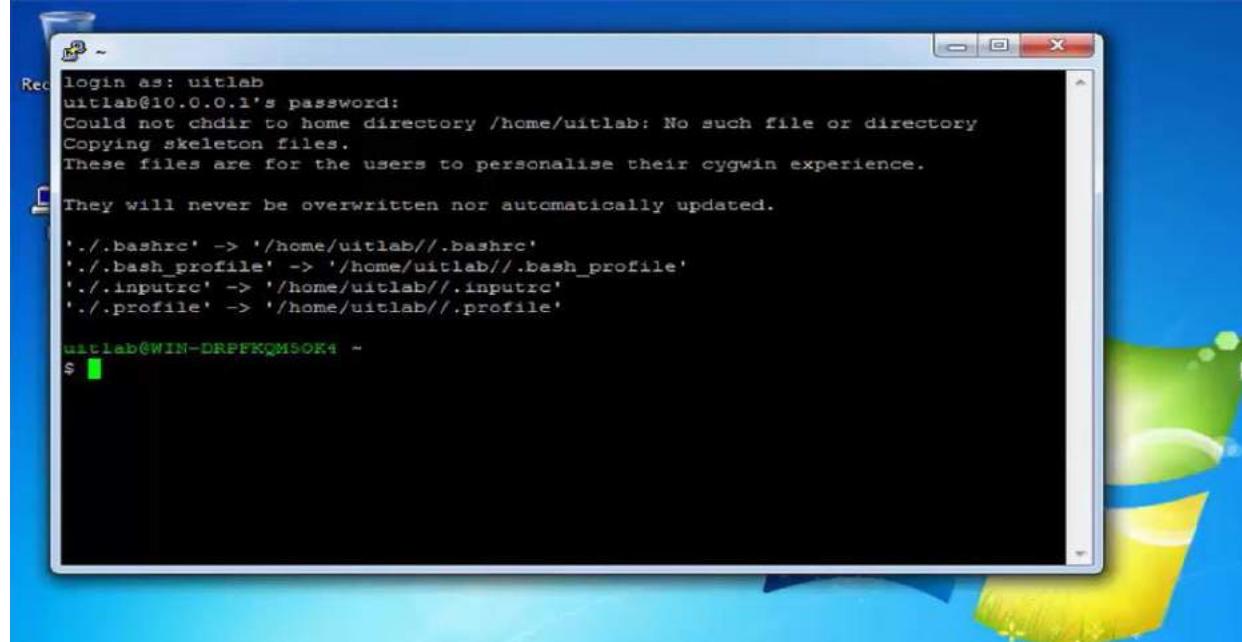
Khởi động putty trên win7 nhập host 10.0.0.1, chọn loại kết nối SSH sau đó nhấn Open



Nhập tài khoản uitlab và mật khẩu đã đổi



10.0.0.1 - PuTTY  
login as: uitlab  
uitlab@10.0.0.1's password: █

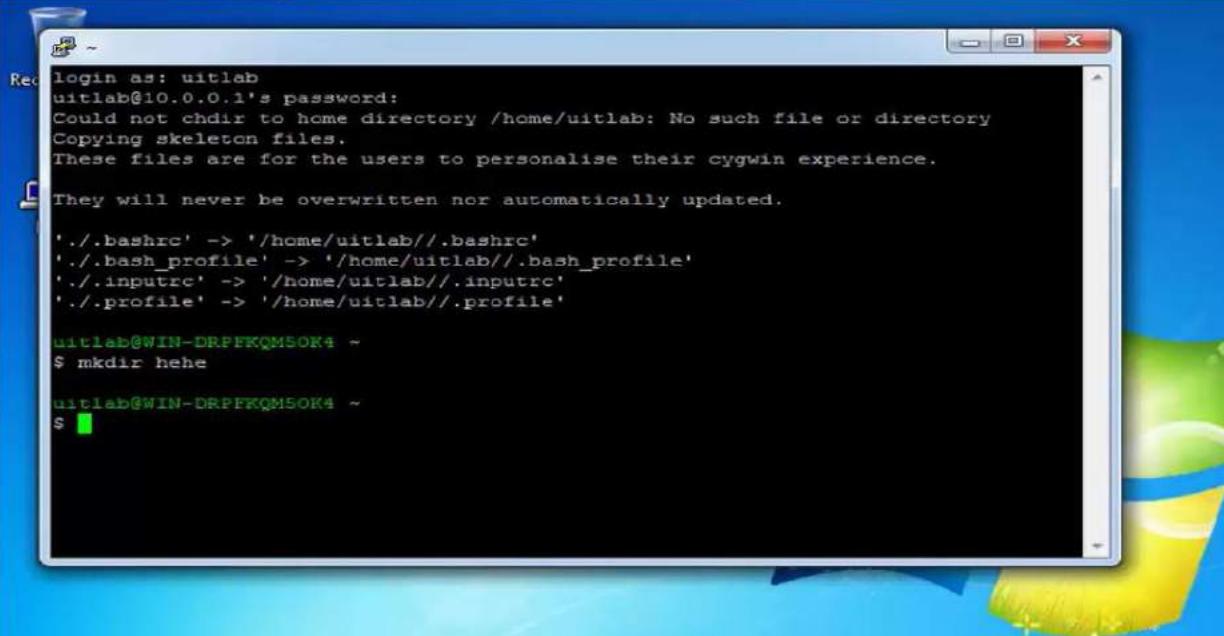
```
Rec 10.0.0.1 - PuTTY
login as: uitlab
uitlab@10.0.0.1's password:
Could not chdir to home directory /home/uitlab: No such file or directory
Copying skeleton files.
These files are for the users to personalise their cygwin experience.

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@WIN-DRPFKQMSOK4 ~
$ █
```

Nhập “mkdir hehe”



```
Recover password: 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.

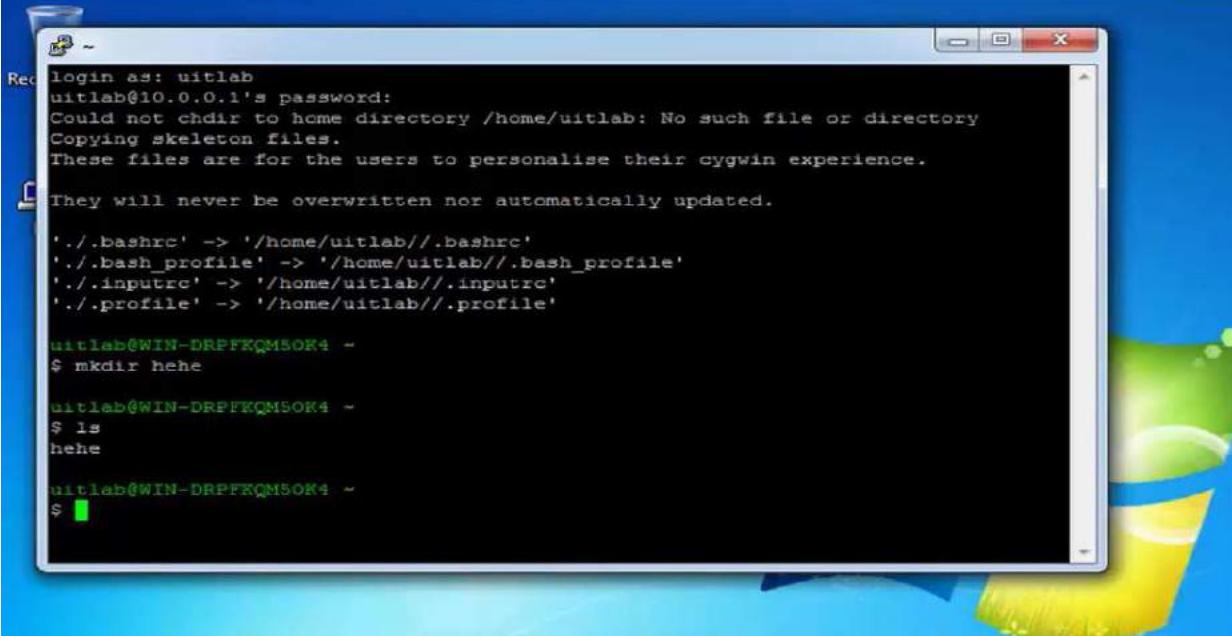
They will never be overwritten nor automatically updated.

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

uitlab@WIN-DRPFKQM5OK4 ~
$ mkdir hehe

uitlab@WIN-DRPFKQM5OK4 ~
$
```

Nhập “ls”



```
Recover password: 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.

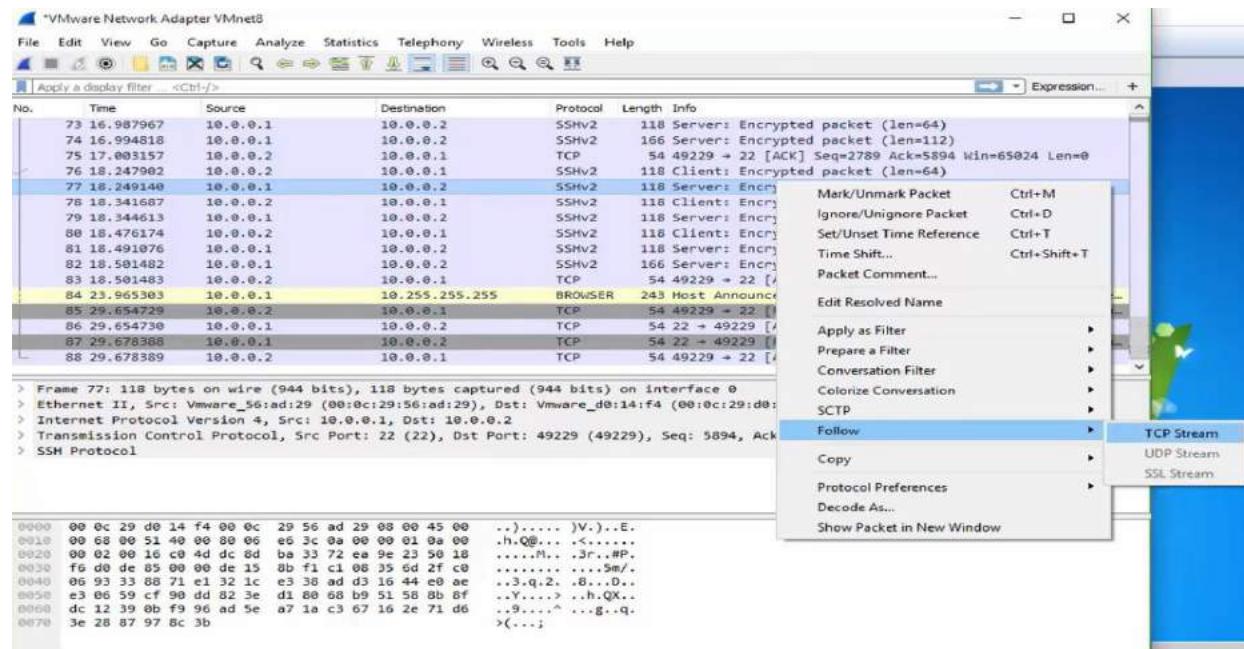
'./.bashrc' -> '/home/uitlab//.bashrc'
'./.bash_profile' -> '/home/uitlab//.bash_profile'
'./.inputrc' -> '/home/uitlab//.inputrc'
'./.profile' -> '/home/uitlab//.profile'

uitlab@WIN-DRPFKQM5OK4 ~
$ mkdir hehe

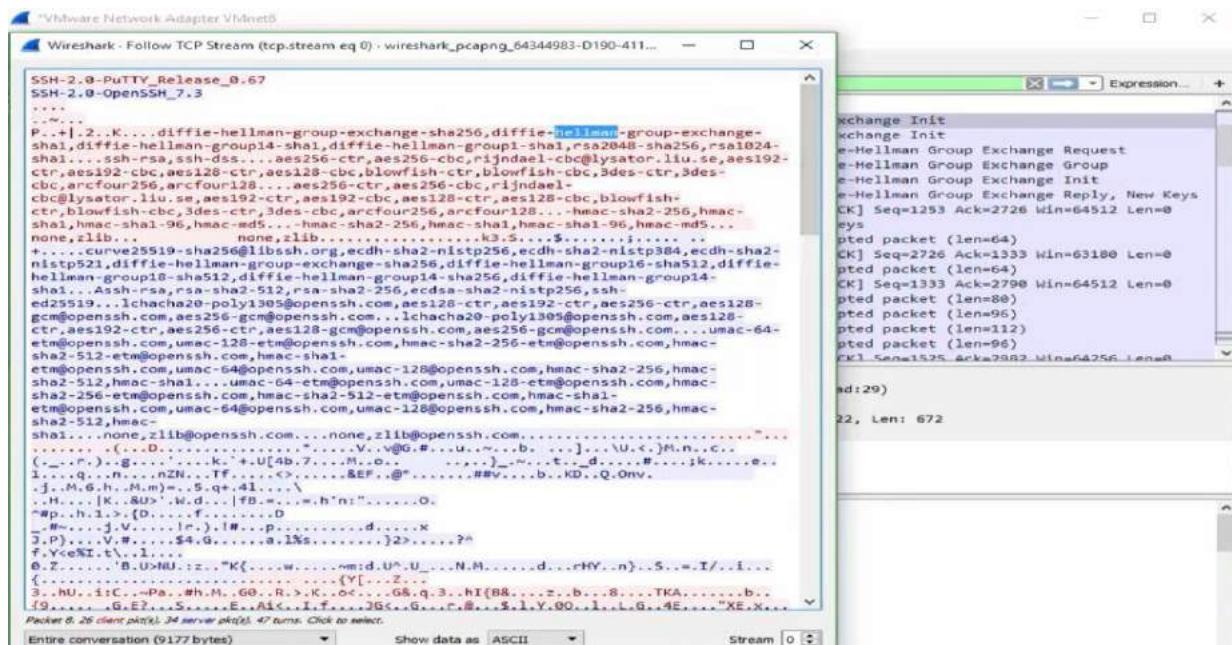
uitlab@WIN-DRPFKQM5OK4 ~
$ ls
hehe

uitlab@WIN-DRPFKQM5OK4 ~
$
```

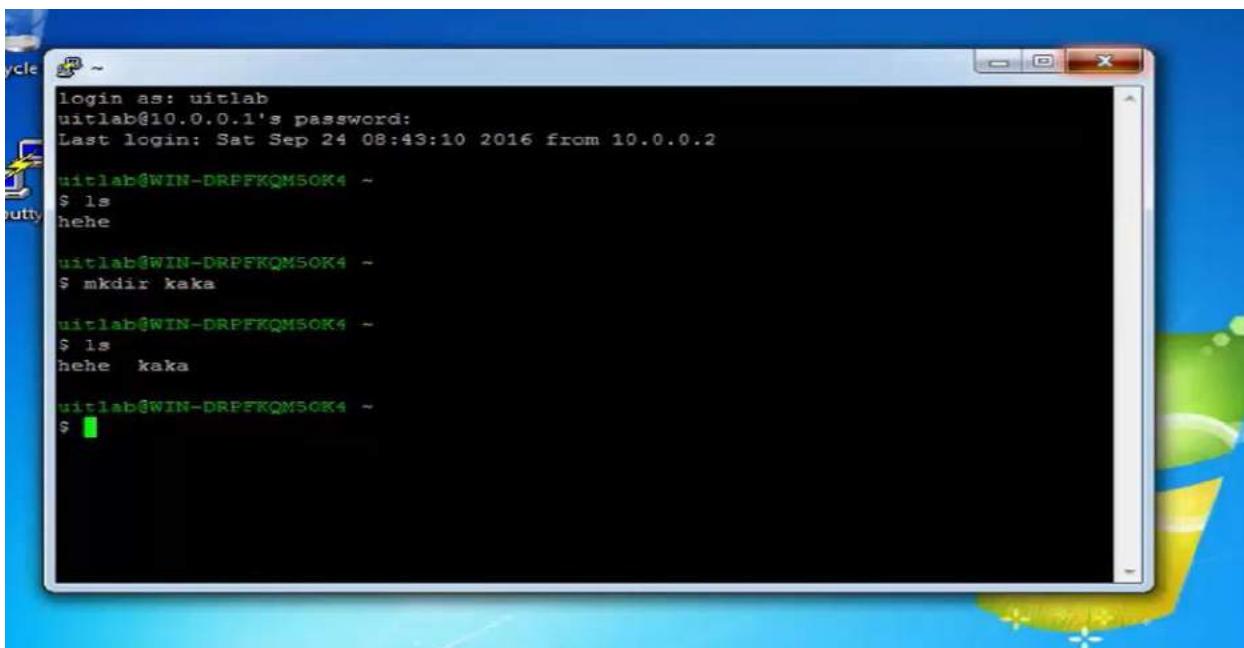
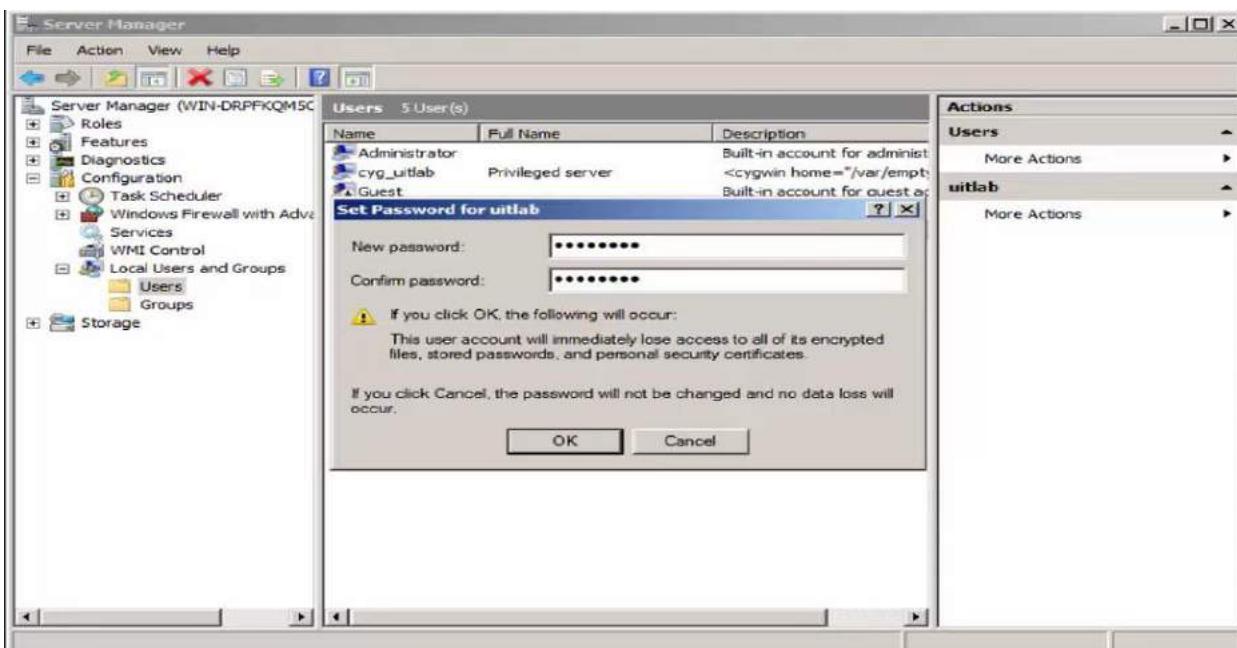
Truy cập wireshark bắt gói tin trên máy attacker

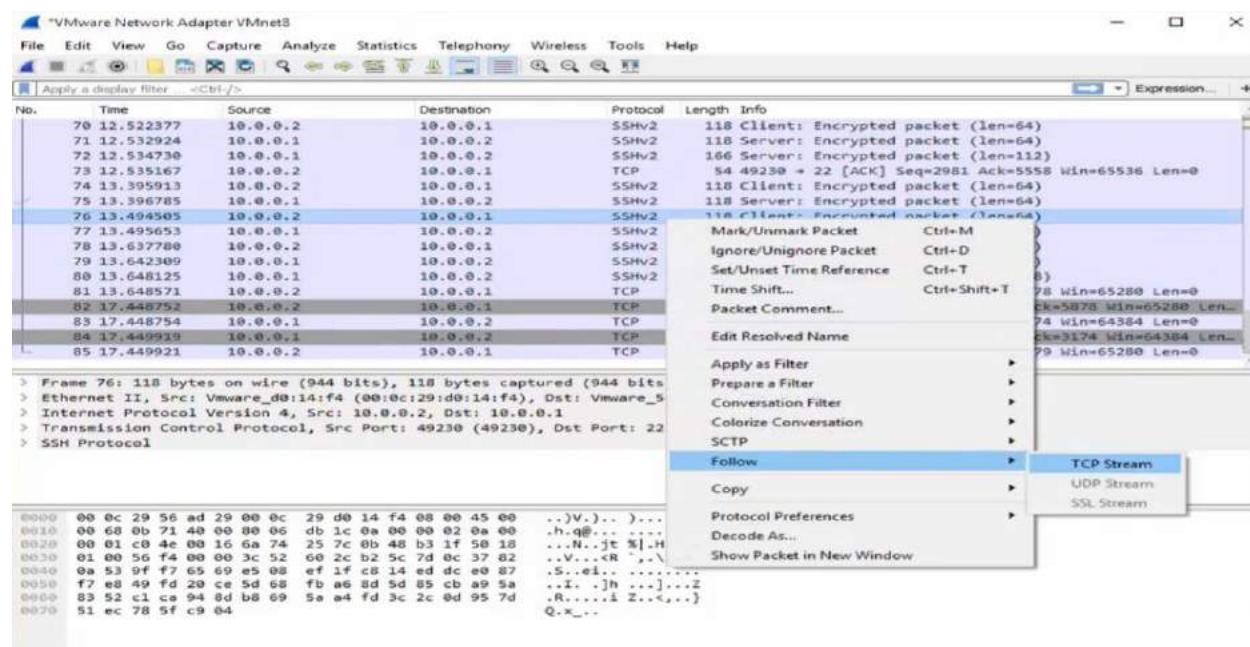
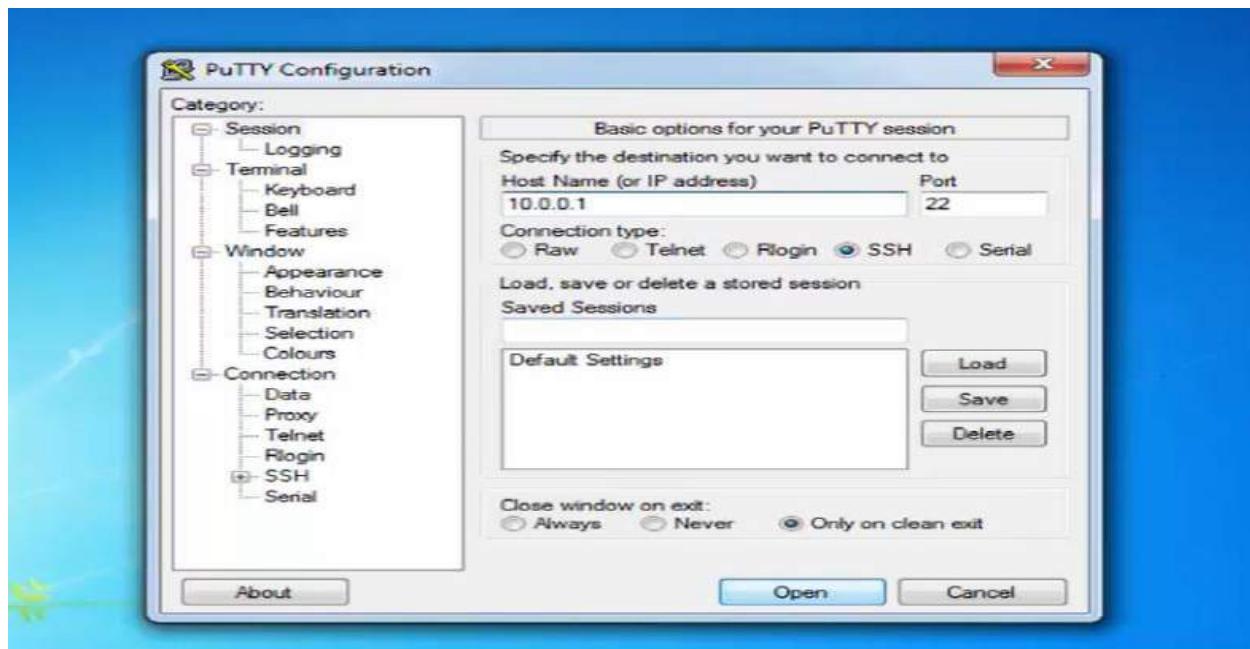


Với loại SSH mật khẩu đã được mã hoá, attacker phải tìm cách mã hoá mới tìm được mật khẩu

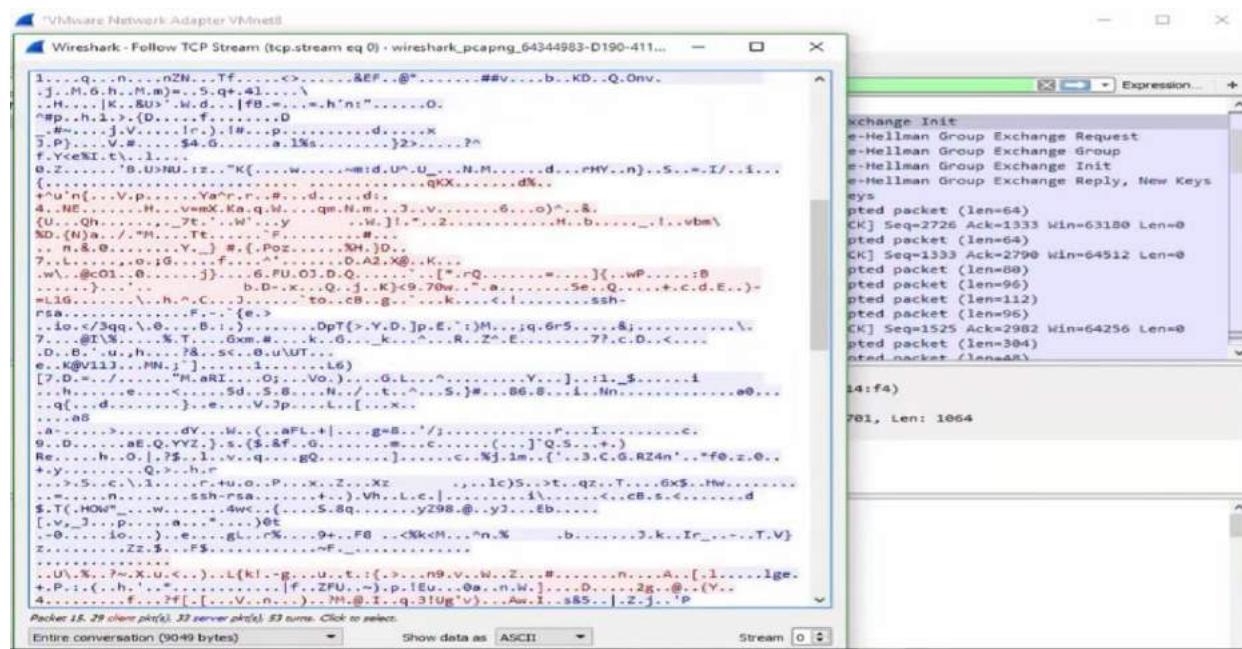


Đổi mật khẩu và lặp lại các bước





Mật khẩu vẫn bị mã hoá



→ SSH an toàn hơn Telnet

## B. Trả lời câu hỏi

### 1. Telnet và SSH là gì và được ứng dụng trong trường hợp nào?

- **Telnet** là một từ viết tắt ghép từ “teletype network”, “terminal network” hay “telecommunications network”. Telnet là một giao thức dòng lệnh được sử dụng để quản lý các thiết bị khác nhau như máy chủ, PC, IoT, Router, Switch, Linux, Tường lửa,... Nó có nhiệm vụ kết nối từ xa, gửi các lệnh hoặc dữ liệu từ các hệ thống mạng để điều chỉnh, thay đổi,... các thiết bị này theo ý muốn.
  - **Telnet** được ứng dụng trong các trường hợp như: Telnet tương thích với nhiều loại thiết bị khác nhau và khách hàng có thể dễ dàng quản lý từ xa. Các thiết bị sử dụng Telnet có thể kể đến là: máy tính, điện thoại thông minh, Router, Switch, camera,...
- **SSH** là giao thức đăng nhập vào server từ xa, cho phép người dùng kiểm soát, chỉnh sửa và quản trị dữ liệu của server thông qua nền tảng Internet. SSH là viết tắt của Secure Socket Shell. SSH cũng giúp việc kết nối của mạng lưới máy chủ và máy khách an toàn, hiệu quả và bảo mật thông tin tốt hơn.
  - **SSH** được ứng dụng trong các trường hợp sau:
    - Sử dụng trong mọi datacenter.
    - Kết nối hệ thống server.
    - Ứng dụng cho hệ thống đăng nhập một lần.
    - Mã hóa dữ liệu.
    - Xác thực thông tin.

### 2. So sánh Telnet và SSH.

**Giống nhau:** Cả SSH và Telnet đều sở hữu một số điểm tương đồng về tính năng nhất định. Tuy nhiên điểm khác biệt lớn nhất của 2 giao thức này chính là cơ chế bảo mật. Theo đó, SSH luôn dùng Public Key khi cần xác thực Terminal Session, mã hóa lệnh đầu ra của từng phiên. SSH và Telnet đều là giao thức mạng cho phép người dùng đăng nhập vào các hệ thống từ xa, và thực hiện các lệnh trên chúng.

**Khác nhau:**

- Quyền truy cập vào dòng lệnh của máy chủ từ xa là tương tự trong cả hai giao thức, nhưng sự khác biệt chính của các giao thức này phụ thuộc vào biện pháp bảo mật của từng giao thức. SSH được bảo mật cao hơn Telnet
- Theo mặc định, SSH sử dụng cổng 22 và Telnet sử dụng cổng 23 cho giao tiếp và cả hai đều sử dụng chuẩn TCP.
- SSH gửi tất cả dữ liệu ở định dạng được mã hóa, nhưng Telnet gửi dữ liệu ở dạng văn bản thuần túy. Do đó, SSH sử dụng một kênh an toàn để truyền dữ liệu qua mạng, nhưng Telnet sử dụng cách thông thường để kết nối với mạng và để giao tiếp.
- Hơn nữa, SSH sử dụng mã hóa khóa công khai để xác thực người dùng từ xa, nhưng Telnet không sử dụng cơ chế xác thực.
- Xem xét tính bảo mật có sẵn trong mỗi giao thức, SSH phù hợp để sử dụng trong các mạng công cộng, mặc dù chúng có đáng tin cậy hay không, nhưng Telnet chỉ thích hợp cho các mạng riêng.
- Cuối cùng, giao thức Telnet có một số hạn chế lớn ở góc độ bảo mật và giao thức SSH đã khắc phục được hầu hết các vấn đề bảo mật đó. Vì vậy SSH có thể được coi là sự thay thế cho giao thức Telnet.

Bảng so sánh:

Tiêu chí so sánh	Giao thức Telnet	Giao thức SSH
Vị trí Port chạy	Port 22	Port 23
Tính an toàn	Rất an toàn	Kém an toàn
Cơ chế mã hóa	Bằng Public Key	Truyền văn bản thuần
Hệ thống phù hợp	Public Network	Private Network
Hệ điều hành tương thích	Tất cả hệ điều hành	Linux và Windows

**3. Khi sử dụng SSH, còn có cách nào để đăng nhập ngoài cách dùng username và mật khẩu truyền thống?**

Có thể sử dụng phương thức xác thực bằng public key để đăng nhập SSH. Để sử dụng phương thức này, ta cần tạo cặp khóa (public key và private key) trên máy tính local của mình và truyền public key đến máy chủ SSH để thực hiện xác thực.

## LAB 02: KEYLOGGER TRÊN PC VÀ ĐIỆN THOẠI

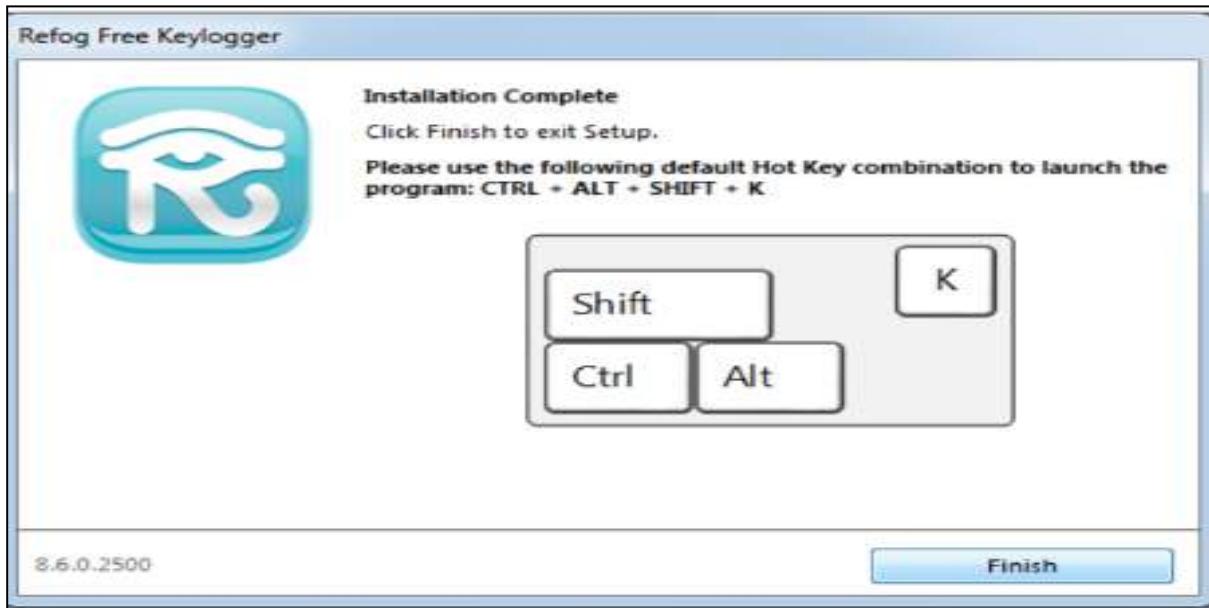
### A. Thực hành

- 1 Máy tính Windows 7 /8 /10 có kết nối Internet để cài Keylogger.

#### 1. Thử nghiệm Keylogger đơn giản với REFOG Free Keylogger



**Bước 1:** Tải và cài đặt RFK trên Windows.



Khởi động RFK.

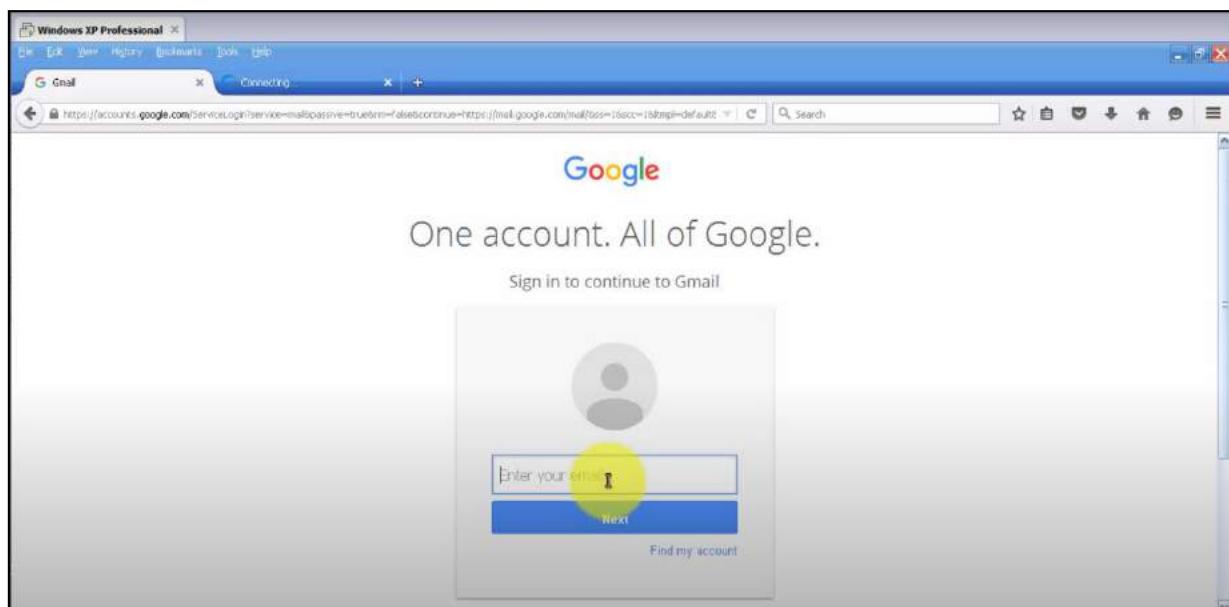
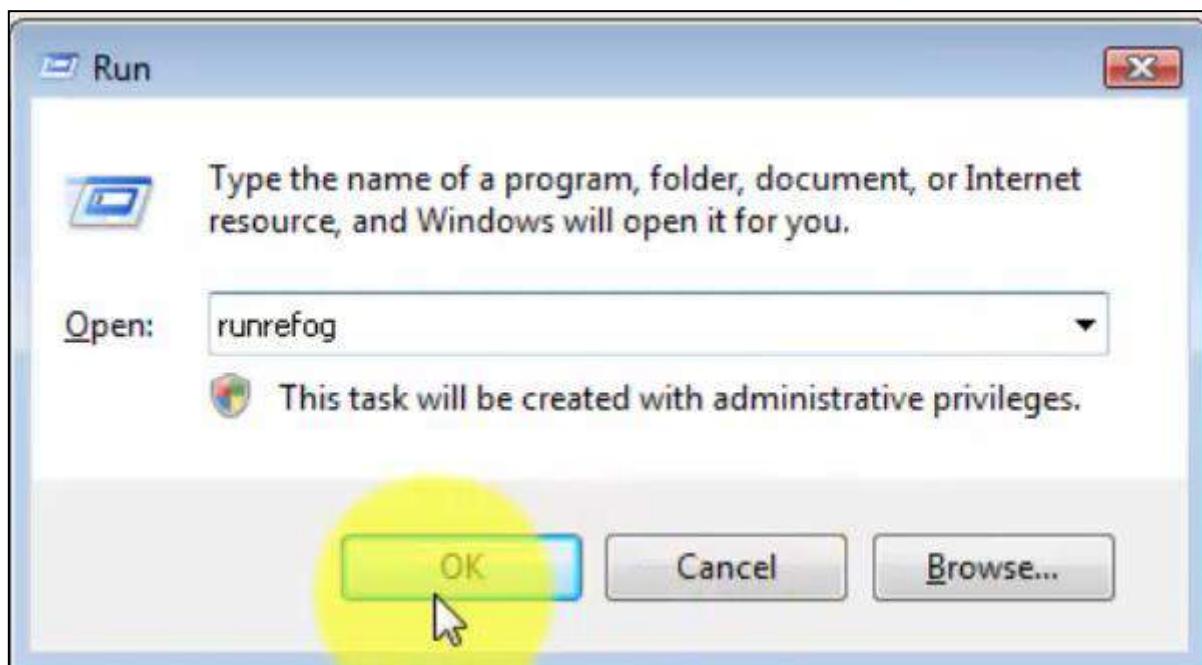


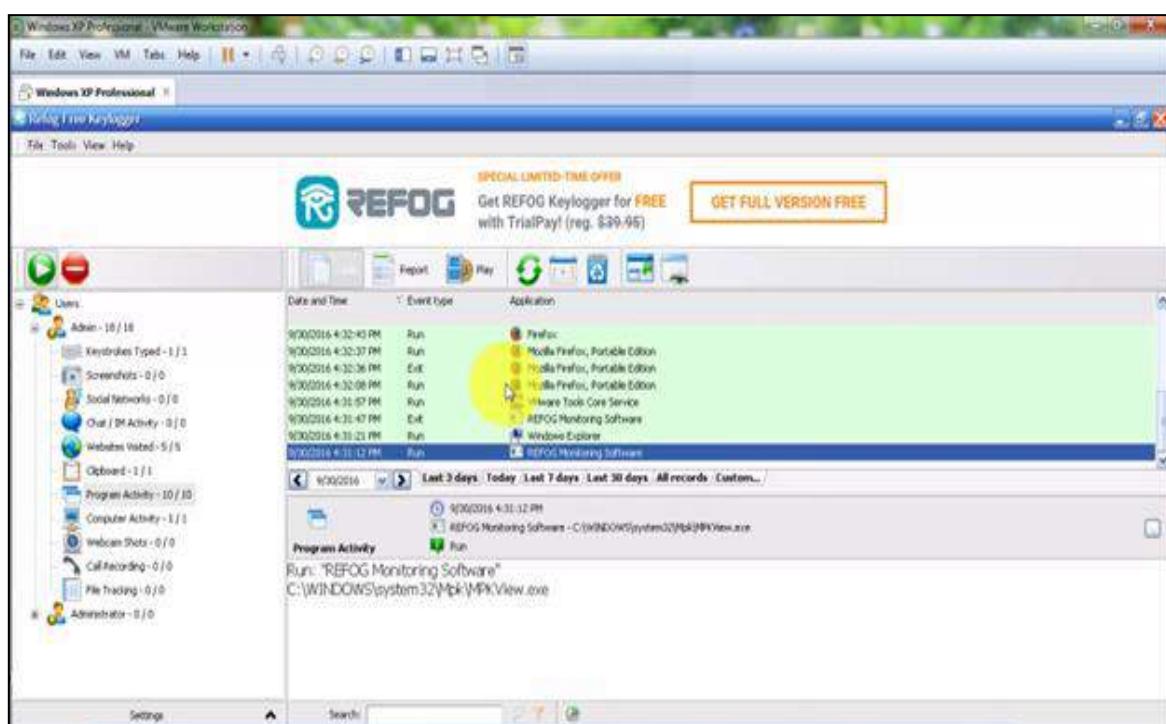
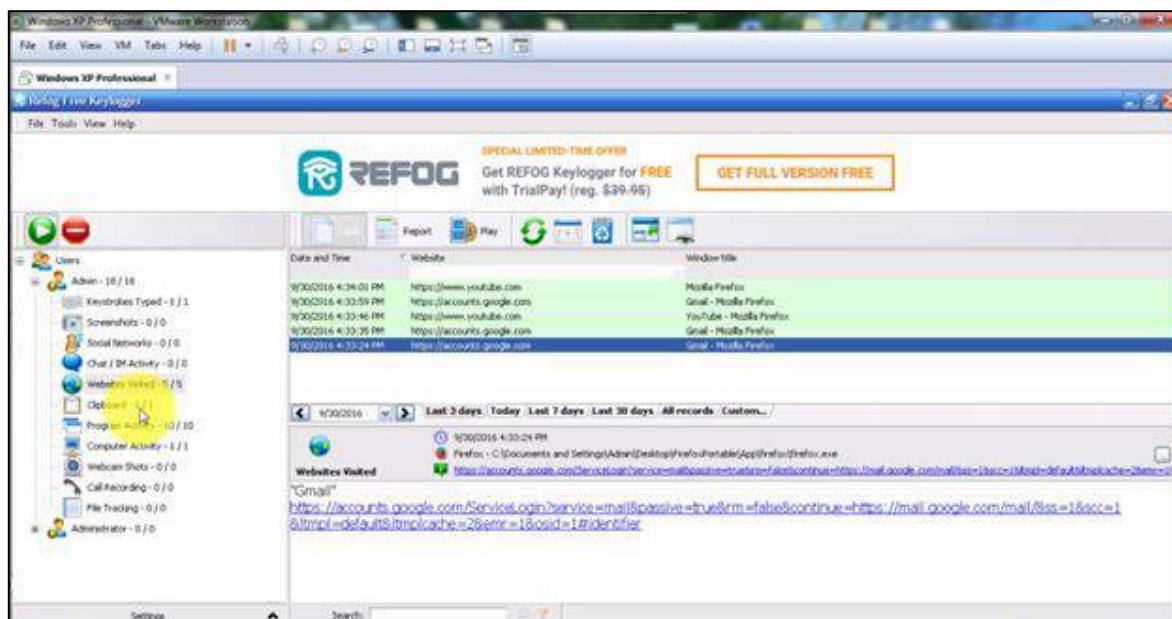
**Bước 2:** Dùng trình duyệt web, đăng nhập thành công vào một tài khoản Gmail tại <https://gmail.com>

**Bước 3:** Truy cập vào Youtube.com và chọn xem một video bất kỳ.

**Bước 4:** Truy cập Google.com và tìm kiếm với từ khóa là tên sinh viên, chọn xem một kết quả bất kỳ.

**Bước 5:** Mở RFK và xem kết quả thu thập được.





## B. Trả lời câu hỏi

### 1. Nêu biện pháp phòng tránh, cách phát hiện Keylogger trên máy tính - điện thoại.

- Cách tránh keylogger:

#### 1. Sử dụng các công cụ bảo mật

Một cái gì đó cơ bản là sử dụng **công cụ bảo mật**. Chúng tôi có nhiều thứ theo ý của chúng tôi. Nhiều phần mềm chống vi-rút có sẵn cho mọi loại hệ điều hành và thiết bị.

Có các chương trình bảo vệ chúng ta là rất quan trọng để ngăn chặn sự xâm nhập của phần mềm độc hại, nhưng cũng để phát hiện và loại bỏ nó. Do đó, lời khuyên của chúng tôi là luôn có loại phần mềm này trong hệ thống của chúng tôi.

## 2. Luôn cập nhật thiết bị

Một vấn đề rất quan trọng khác là bảo quản thiết bị đúng cách **cập nhật**. Trong nhiều trường hợp, các lỗ hổng bảo mật xuất hiện bị tin tặc lợi dụng để khai thác chúng và thực hiện các cuộc tấn công của chúng.

Điều cần thiết là chúng tôi luôn cài đặt các phiên bản mới nhất. Bằng cách này, chúng tôi có thể tránh được các vấn đề không chỉ ảnh hưởng đến hiệu suất mà còn cả bảo mật. Một cách nữa để tránh keylogger trong Windows.

## 3. Cài đặt phần mềm chính thức

Như chúng tôi đã đề cập, trong nhiều trường hợp, keylogger đến thông qua các chương trình mà chúng tôi đã cài đặt. Để ngăn điều này xảy ra, chúng tôi chỉ phải cài đặt phần mềm từ **các trang web chính thức**.

Đúng là đôi khi chúng ta có thể truy cập nhiều loại phần mềm trên các trang web của bên thứ ba, nhưng chúng không phải lúc nào cũng được đảm bảo. Điều quan trọng là đảm bảo rằng những gì chúng tôi đang tải xuống là hợp pháp.

- **Cách phát hiện keylogger trong Windows**

1. **Sử dụng trình quản lý tác vụ**

Một trong những tùy chọn là sử dụng **nhiệm vụ quản lý**. Ở đó, nó cho chúng ta thấy tất cả các chương trình và quy trình đang chạy. Các công cụ như trình duyệt hoặc bất kỳ ứng dụng

nào mà chúng tôi đang sử dụng sẽ xuất hiện. Nhưng nó cũng có thể cho chúng ta thấy các quy trình khác với chúng ta.

Có cái gì đó đang chạy mà nó không nên? Một manh mối rất phổ biến là khi chúng tôi thấy quá trình ứng dụng Khởi động Windows bị trùng lặp. Nó nằm trong Windows Processes. Trong trường hợp chúng tôi thấy một quy trình được gọi là Úng dụng Khởi động Windows hoặc tương tự, điều đó có nghĩa là ai đó có thể nằm trong nhóm của chúng tôi. Nó có thể là một keylogger.

Nombre	Estado	3% CPU	52% Memoria	1% Disco	0% Red
<b>Procesos de Windows (92)</b>					
Administrador de sesión de Win...		0%	0,1 MB	0 MB/s	0 Mbps
Administrador de ventanas del ...		0%	56,3 MB	0 MB/s	0 Mbps
Aplicación de inicio de sesión d...		0%	0,8 MB	0 MB/s	0 Mbps
<b>Aplicación de inicio de Windows</b>		0%	0,1 MB	0 MB/s	0 Mbps
Aplicación de servicios y control...		0%	3,3 MB	0 MB/s	0 Mbps
> Host de servicio: Adquisición de...		0%	0,5 MB	0 MB/s	0 Mbps
> Host de servicio: Iniciador de pr...		0%	7,6 MB	0 MB/s	0 Mbps
> Host de servicio: Llamada a pro...		0,1%	6,5 MB	0 MB/s	0 Mbps
> Host de servicio: Servicio de red		0%	2,9 MB	0 MB/s	0 Mbps
> Host de servicio: Servicio local		0%	0,5 MB	0 MB/s	0 Mbps
> Host de servicio: Servicio local (...)		0%	0,7 MB	0 MB/s	0 Mbps
> Host de servicio: Servicio local (...)		0%	0,8 MB	0 MB/s	0 Mbps
< >					
<b>Menos detalles</b>					<b>Finalizar tarea</b>

## 2. Phát hiện các mối đe dọa bằng phần mềm chống vi-rút

Một tùy chọn cổ điển khác là sử dụng **antivirus** để phát hiện các mối đe dọa. Chúng tôi đã biết rằng có rất nhiều công cụ bảo mật mà chúng tôi có thể sử dụng. Có cả miễn phí và trả phí và cho Windows có một số lượng lớn các lựa chọn thay thế.

Ý tưởng ở đây là chạy một **quét toàn bộ** của máy tính của bạn để phát hiện các mối đe dọa tiềm ẩn, phần mềm độc hại và các sự cố có thể tồn tại. Thêm một cách nữa để phát hiện kịp thời keylogger có thể có trong hệ thống.

## 3. Sử dụng dòng lệnh

Chúng tôi cũng có khả năng sử dụng Windows **dòng lệnh** để phát hiện các kết nối Internet đáng ngờ. Đối với điều này, chúng tôi vào Start, chúng tôi viết CMD và chúng tôi thực hiện Command Prompt.

Chúng ta phải chạy lệnh **netstat b**. Sẽ xuất hiện tất cả các trang web và ứng dụng Internet được kết nối với máy tính của chúng ta. Chúng tôi có thể xem các địa chỉ IP để phát hiện một số vị trí từ xa không xác định và đáng ngờ.

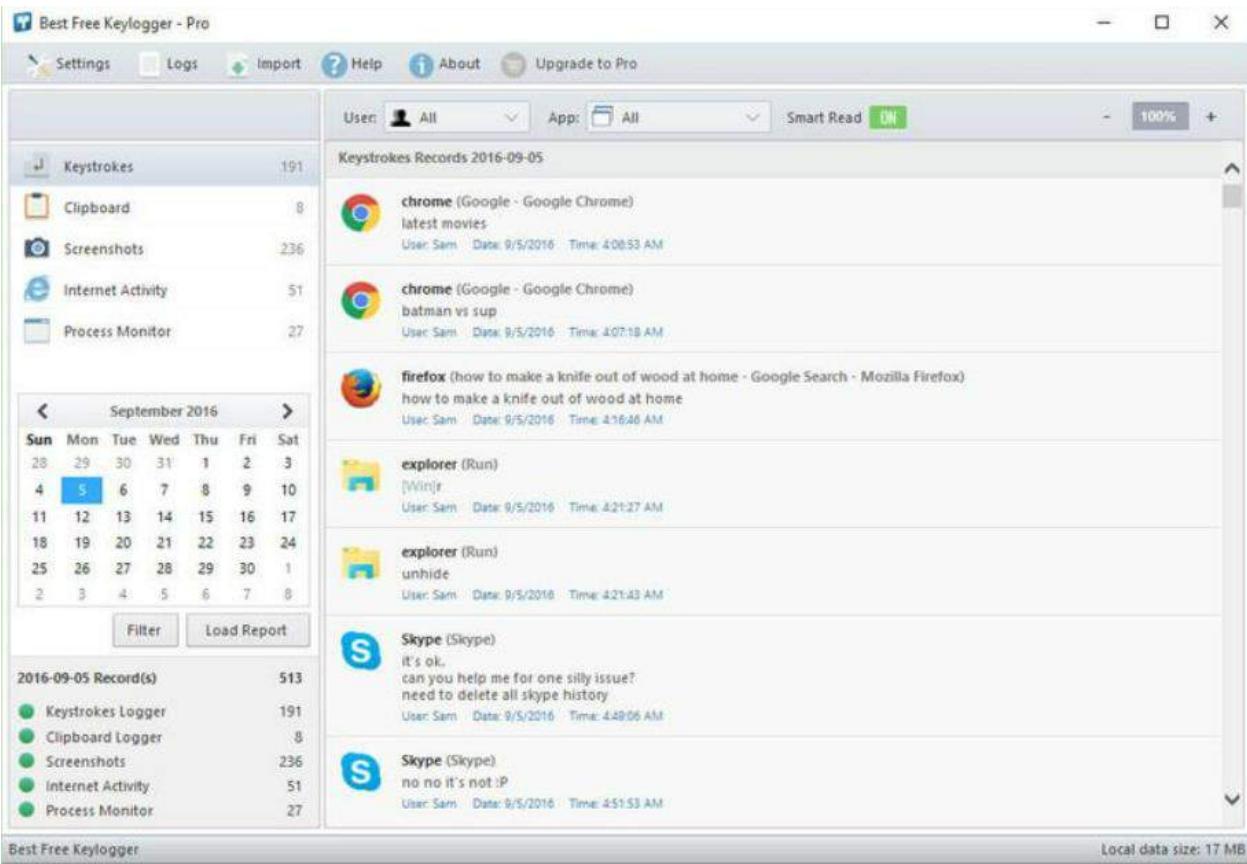
## 4. Xem các ứng dụng đáng ngờ đã cài đặt

Có thể khi cài đặt chương trình một số **ứng dụng bổ sung** là ẩn. Chúng ta đã thấy điều gì đáng ngờ chưa? Keylogger có thể bị ẩn trong một ứng dụng mà chúng tôi đã cài đặt và chúng tôi thực sự không biết tại sao.

Vì vậy, luôn thuận tiện để xem lại tất cả các chương trình mà chúng tôi đã cài đặt. Một cách kiểm soát mọi lúc mọi nơi mà không có gì lạ.

## 2. Tìm thêm và giới thiệu một số loại Keylogger trên máy tính - điện thoại khác.

### 01 – Best Free Keylogger

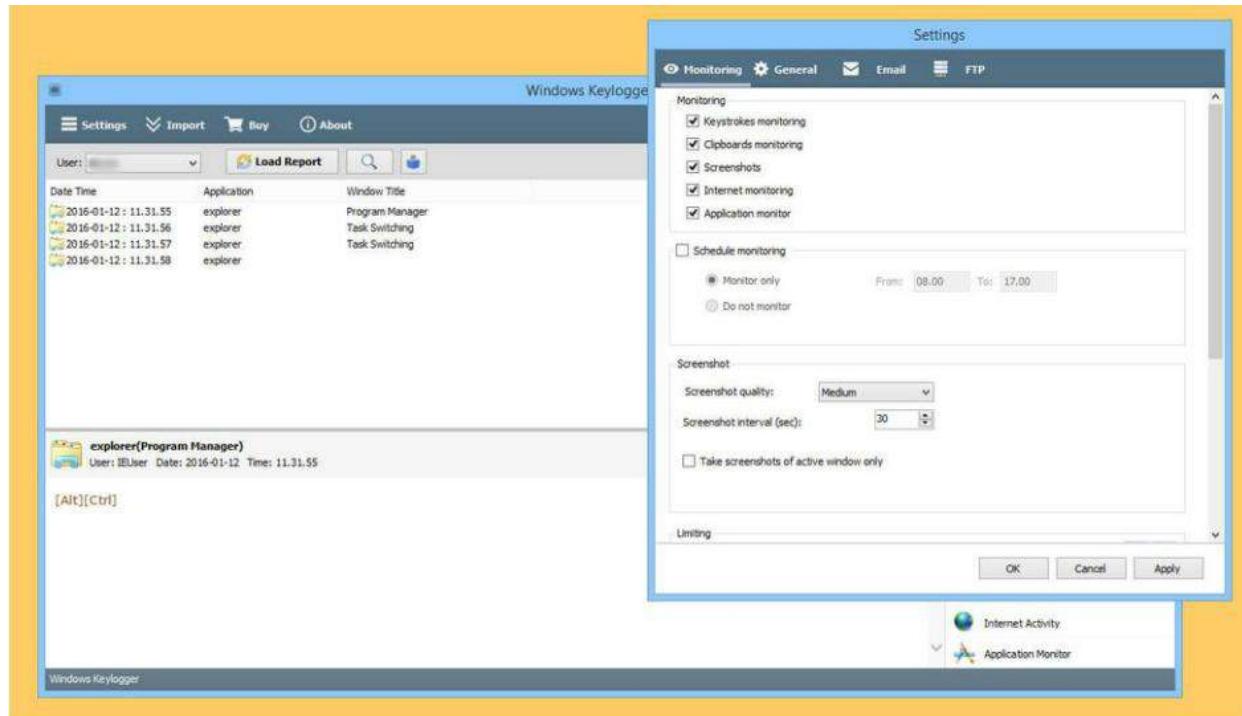


Best Free Keylogger là một tiện ích giám sát PC hoạt động **hoàn toàn bí mật** trong máy tính của bạn. Phần mềm này có thể giám sát tổ hợp phím; Trò chuyện, hoạt động trên Internet, URL đã truy cập, bản sao văn bản Clipboard, Bản sao file và ảnh chụp màn hình. Phần mềm này là giải pháp tốt nhất để theo dõi những gì con cái đang làm với máy tính khi cha mẹ không có ở nhà.

- Ghi âm phím tắt
- Ghi lại hoạt động Internet
- Trò chuyện và đăng nhập mật khẩu
- Theo dõi clipboard
- Giám sát ứng dụng
- Chụp ảnh màn hình
- Email, FTP, LAN, giao hàng qua USB
- Chế độ ẩn và bảo vệ mật khẩu

- 100% không thể phát hiện
- Theo dõi lịch biểu
- Tự động đăng nhập

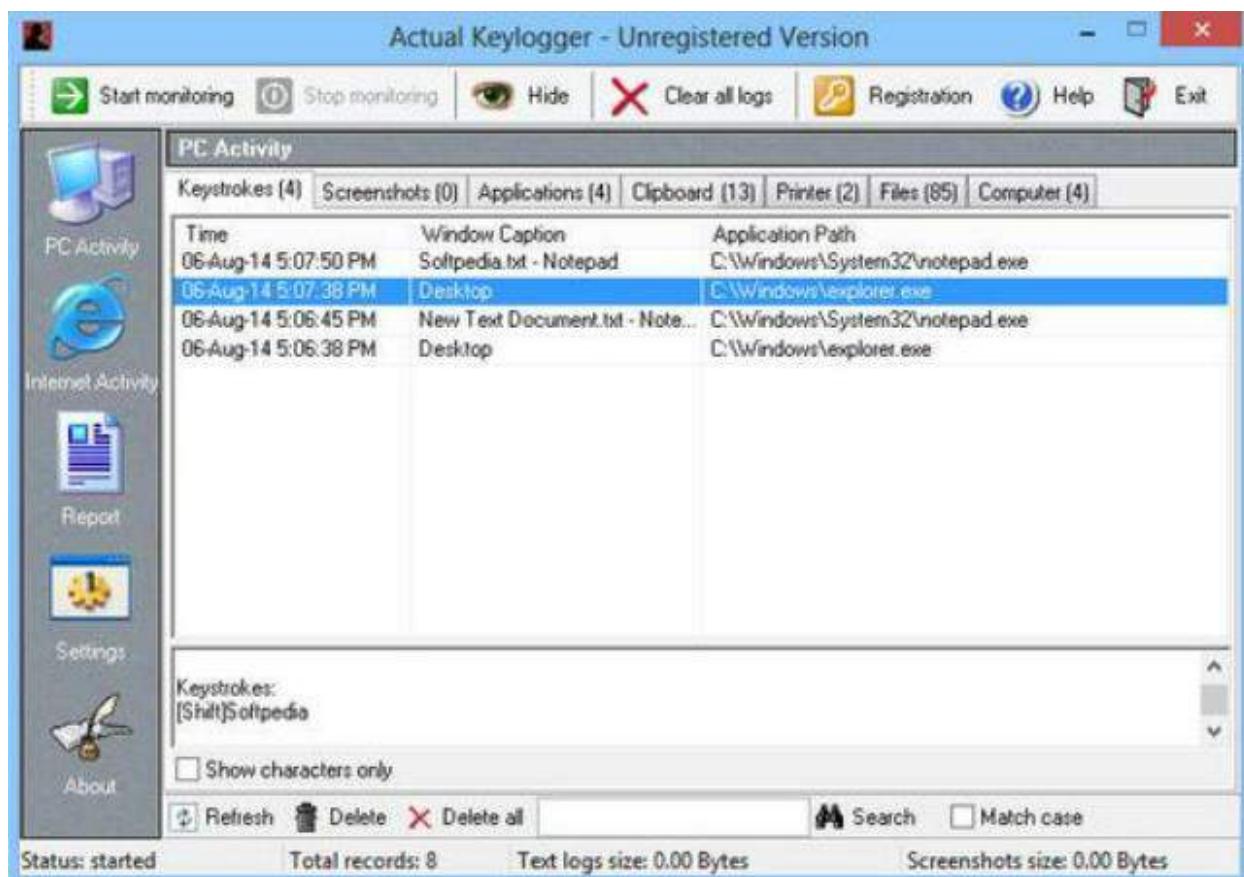
## 02 – Windows Keylogger



Windows Keylogger là phần mềm giám sát hàng đầu trên Windows. Hàng ngàn người dùng trên toàn thế giới sử dụng Windows Keylogger để bí mật theo dõi con cái sử dụng máy tính.

- Bạn có thể dễ dàng đọc các thao tác gõ phím với tính năng “Easy Read” được cung cấp bởi Windows Keylogger.
- Nó có thể được cấu hình để theo dõi người dùng được chọn và chỉ giám sát trong các ứng dụng được chọn.
- Bạn có thể lọc nhật ký bạn cần, bằng tìm kiếm nâng cao.
- Có thể được cấu hình để gỡ bỏ cài đặt tự động, vào một ngày đã chọn trước đó.

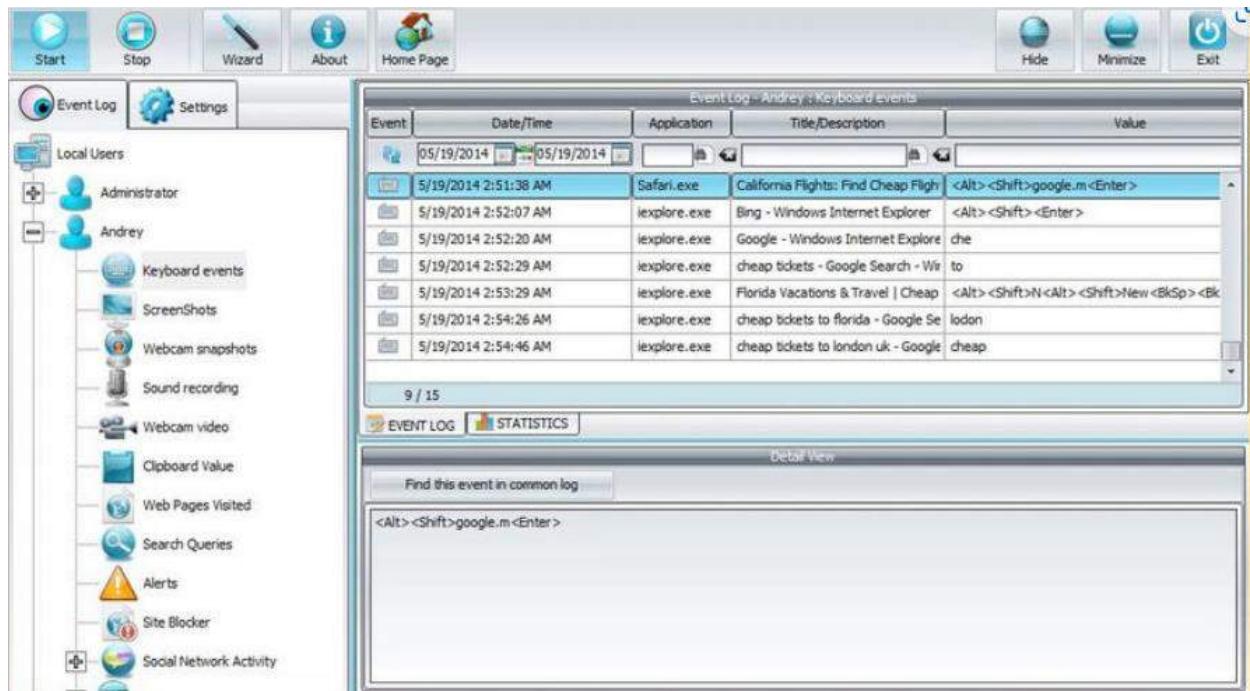
### 03 – Actual Keylogger



Actual Keylogger là một chương trình giám sát hoạt động trên máy tính. Bạn có thể khám phá những gì người dùng khác đang làm trên máy tính của bạn khi bạn không có mặt. Phần mềm keylogger theo dõi các chương trình chạy hoặc đóng, các trang web đã truy cập và nhấn phím bất kỳ, và cũng có thể ghi lại ảnh chụp màn hình và nội dung được sao chép vào bộ nhớ tạm. Tính năng, đặc điểm:

- Ứng dụng nào đang chạy và đóng
- Đã nhấn tất cả các lần nhấn phím (trình ghi phím tắt)
- Tất cả hoạt động in
- Tất cả các trang web đã truy cập
- Ảnh chụp màn hình trong một khoảng thời gian đã đặt
- File nhật ký được mã hóa cho tất cả hoạt động

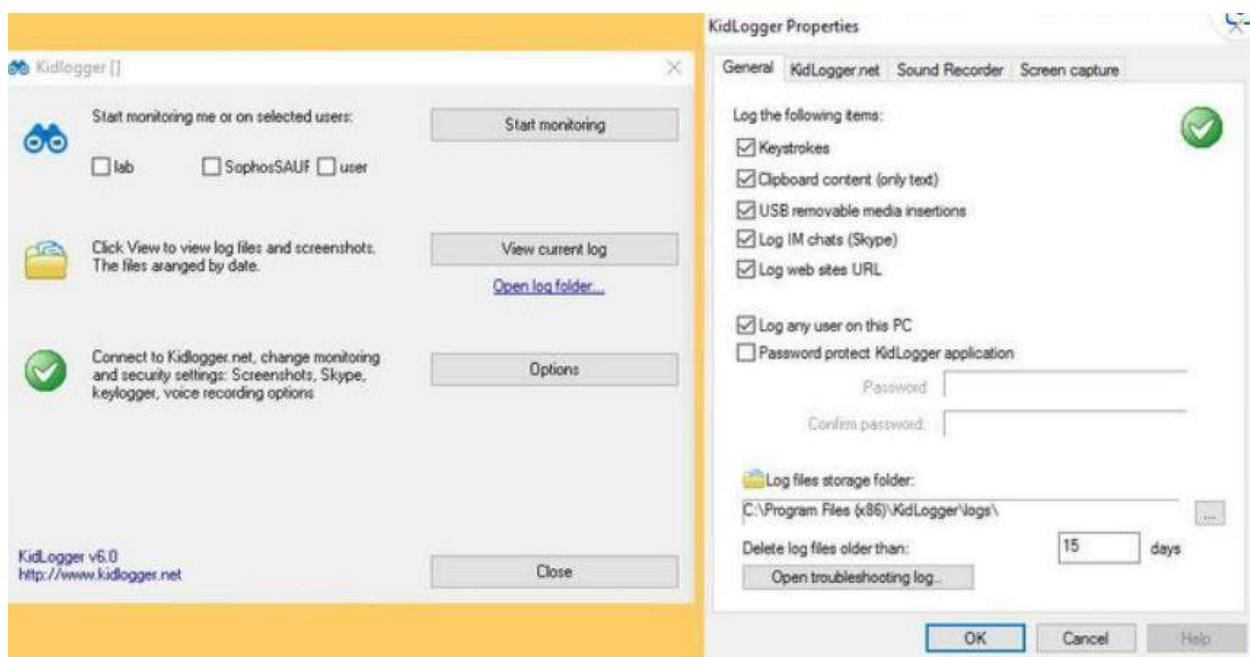
## **04 – Spyrix Keylogger Free**



Spyrix Keylogger là một phần mềm cho phép ghi lại và theo dõi tất cả các phím tắt. Phần mềm miễn phí này cũng có thể chụp ảnh chụp màn hình của các chương trình hoạt động tại các khoảng thời gian được chỉ định để bạn có thể theo dõi tất cả các hoạt động đang diễn ra trên PC của mình. Nó cũng có thể tạo báo cáo về các chương trình đang chạy.

- Giám sát từ xa thông qua tài khoản web bảo mật
- Ghi nhật ký bàn phím
- Chụp ảnh màn hình
- Không thể phát hiện được với phần mềm chống vi-rút
- Giám sát bằng giọng nói Microphone (80\$)
- WEB Camera Surveillance (80\$)

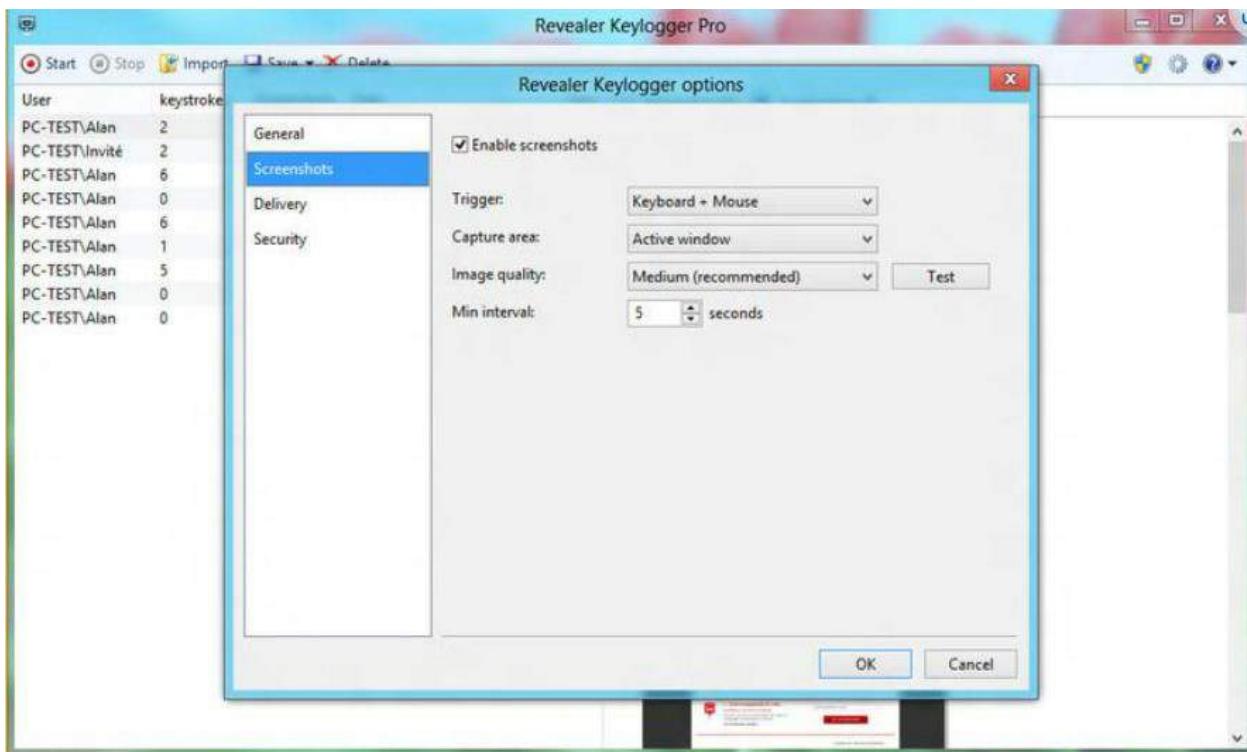
## 05 – Kidlogger Free



**Parental Control** – Giữ con bạn an toàn trong không gian mạng. Tìm hiểu xem con của bạn đang nói chuyện qua điện thoại hoặc khi nào trong không gian mạng. Theo dõi và theo dõi thời gian của nhân viên. Cải thiện kỷ luật nhân viên. Nhật ký tự động cá nhân của bạn. Theo dõi số ghi chép hoặc vị trí điện thoại bằng GPS.

- Ghi lại tổ hợp phím
- Tạo ảnh chụp màn hình
- Giám sát lịch sử web
- Ghi âm giọng nói (cho Windows)
- Theo dõi thời gian
- Giám sát trò chuyện (Windows và MAC)
- Theo dõi vị trí điện thoại (Android, iOS, BlackBerry, MAC OS X) ghi lại điều hướng điểm đến điểm trong ngày, theo tọa độ GPS hoặc WiFi
- SMS (Android, Nokia, BlackBerry) Ghi lại tất cả tin nhắn SMS đến/đi với số điện thoại và tên người nhận.

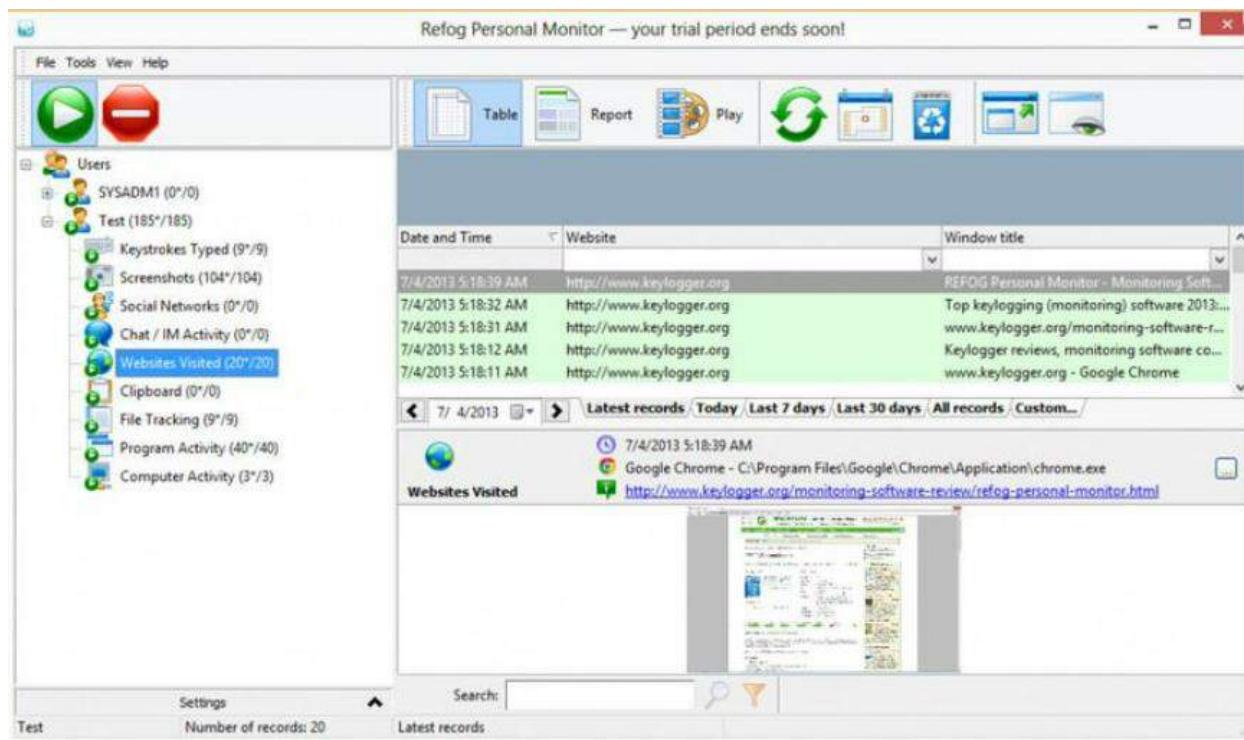
## 06 – Revealer Keylogger Free



Revealer Keylogger Free là một keylogger đơn giản. Nó có thể chạy lúc khởi động, ẩn chính nó khỏi người dùng và bảo vệ quyền truy cập bằng mật khẩu. Nhưng các tính năng cơ bản như ảnh chụp màn hình và thông báo qua email không có sẵn trong phiên bản miễn phí và chương trình không ghi lại địa chỉ IP.

- Theo dõi cuộc hội thoại cho Skype, Facebook, MSN, AOL, ICQ, AIM, GTalk, v.v.
- Keystroke Recorder Ghi lại văn bản, mật khẩu và cuộc hội thoại
- Bảo vệ mật khẩu Ngăn người khác mở chương trình
- Chụp ảnh màn hình (bản Pro 50\$)

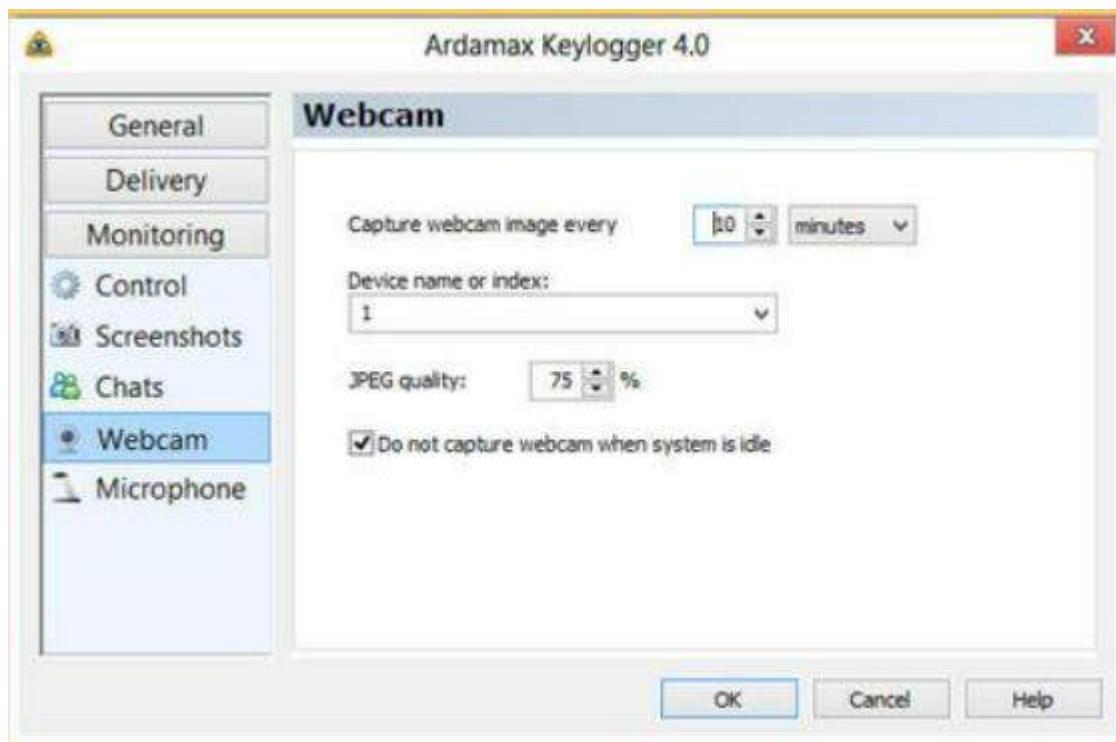
## **07 – Refog Personal Monitor**



efog Free Keylogger đánh bại tất cả các đối thủ khác vì: nó đơn giản để sử dụng và nó hoàn toàn miễn phí. AnonyViet đã nhìn thấy quá nhiều sản phẩm gián điệp đang cồng kềnh với chuông và còi không cần thiết và không thể được sử dụng bởi các bà mẹ và ông bố. Không phải cái này. Thật dễ dàng để cài đặt và sử dụng, và nó không tốn kém gì cả. Danh sách những thứ được ghi lại, ghi lại và ghi lại quá lâu nó gần như không có ý nghĩa gì cả. Đây chỉ là một rất nhiều tính năng của Refog Free Keylogger

- Tất cả các lần gõ phím được nhập vào tất cả các cửa sổ, bao gồm cả mật khẩu
- Đã gửi và nhận tin nhắn trò chuyện
- Các trang web đã truy cập
- Sự kiện đăng xuất và đăng xuất
- Cuộc trò chuyện qua Skype và cuộc trò chuyện thoại
- Ra mắt các chương trình và trò chơi
- Ảnh chụp màn hình của nội dung trên màn hình

## 08 – Ardamax Keylogger



AnonyViet đã từng có bài giới thiệu về Ardamax Keylogger 4.x Full Version. Một KeyLogger mạnh mẽ với đầy đủ các tính năng của các Keylogger được giới thiệu ở trên. Ardamax Keylogger là một keylogger nhỏ, dễ sử dụng để ghi lại hoạt động của người dùng và lưu nó vào một logfile. Các logfile có thể được xem như là một văn bản hoặc trang web. Sử dụng công cụ này để tìm hiểu những gì đang xảy ra trên máy tính của bạn trong khi bạn đi.

- Ghi nhật ký bàn phím – Ghi lại tất cả các lần gõ phím, mật khẩu và các ký tự bị ẩn.
- Trình duyệt chụp – Ghi nhật ký của tất cả các trang web được truy cập cho tất cả các trình duyệt.
- Webcam ghi âm – Định kỳ làm cho hình ảnh webcam và lưu trữ chúng để đăng nhập.
- Gửi nhật ký email – Keylogger có thể gửi cho bạn các bản ghi được ghi lại thông qua việc gửi e-mail vào những thời điểm nhất định – hoàn hảo cho việc giám sát từ xa!
- Ghi âm micrô – Ghi âm giọng nói từ micrô với néo thời gian thực.

- Giám sát trực quan – Định kỳ làm cho ảnh chụp màn hình và lưu trữ các hình ảnh nén để đăng nhập.

Giám sát trò chuyện – Ardamax Keylogger được thiết kế để ghi lại và giám sát cả hai mặt của cuộc hội thoại trong các cuộc trò chuyện sau: AIM, Windows Live Messenger, ICQ, Skype, Yahoo Messenger, Google Talk, Miranda, QiP.

## LAB 03: THIẾT LẬP MÔ HÌNH TƯỜNG LỬA SOPHOS UTM

### A. Thực hành

#### 1. Thiết lập máy chủ Domain Controller

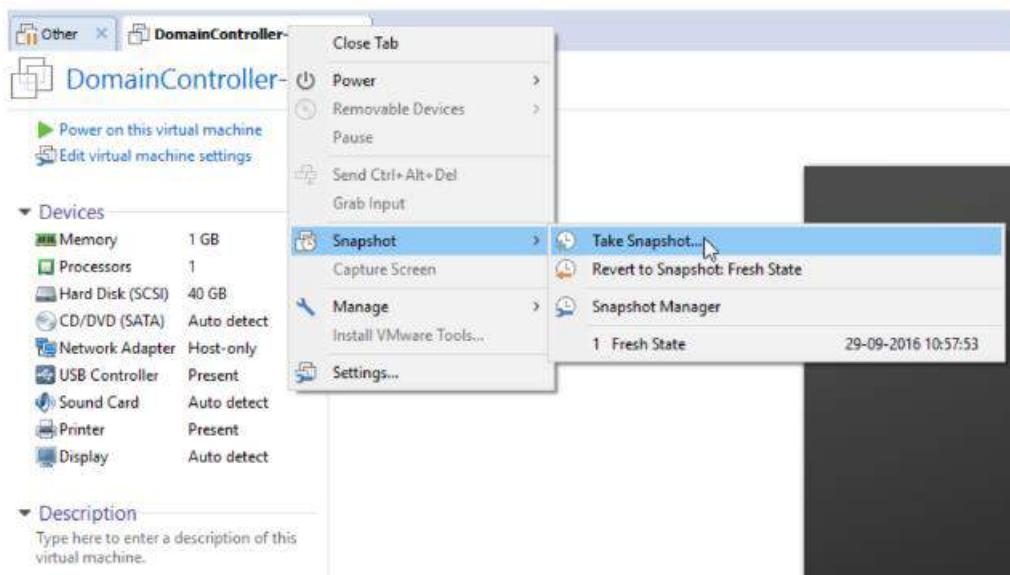
Bước 1: Chuẩn bị máy ảo làm Domain Controller:

+ RAM: 512MB – 1GB

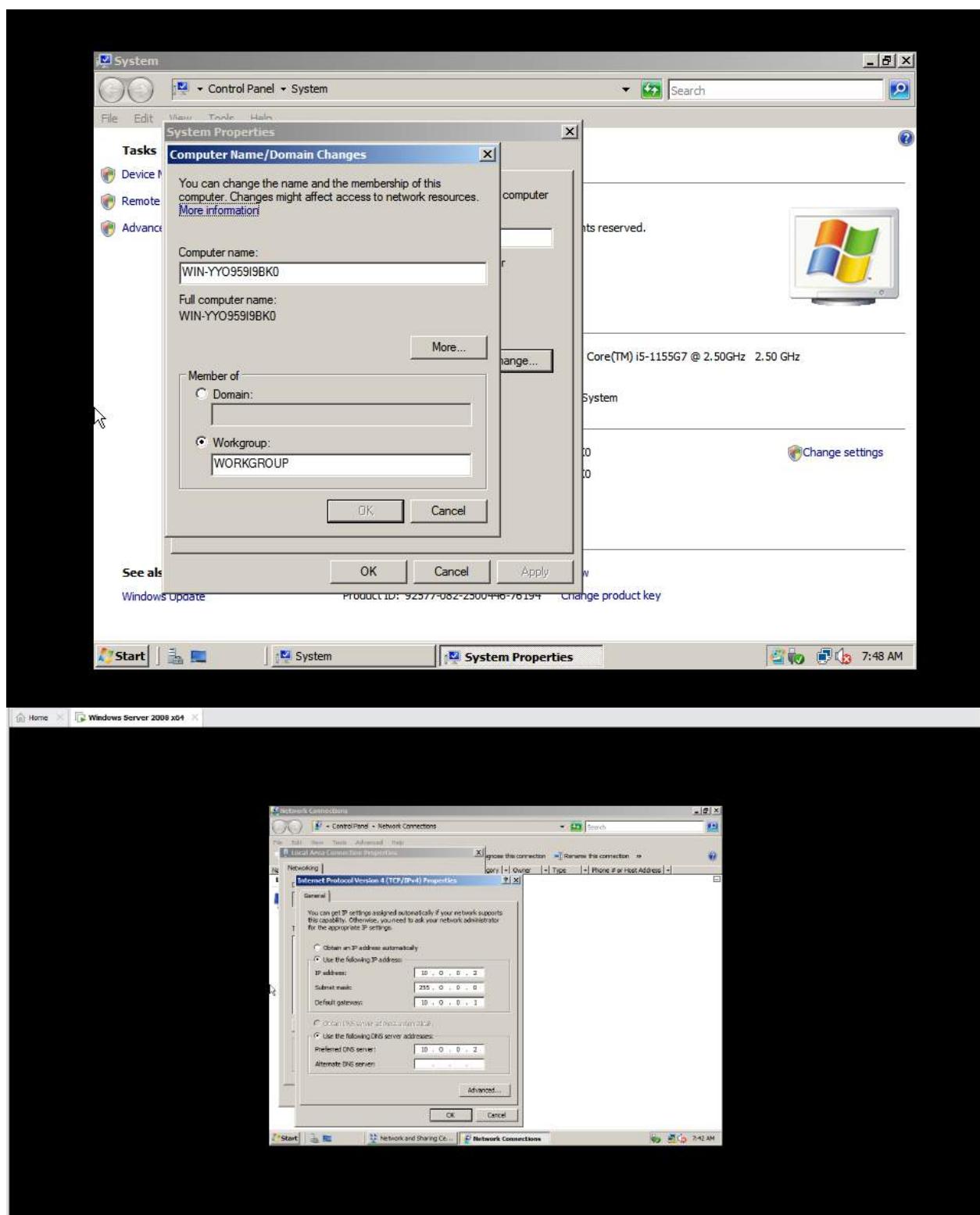
+ 1 Network Adapter Host-Only

+ OS: Windows Server 2008. Trong hướng dẫn này sử dụng Windows Server 2008.

Sau khi cài đặt xong máy ảo Windows Server 2008, nên Snapshot (sao lưu) lại máy ảo để có thể khôi phục lại trạng thái ban đầu nếu quá trình nâng cấp bị lỗi.

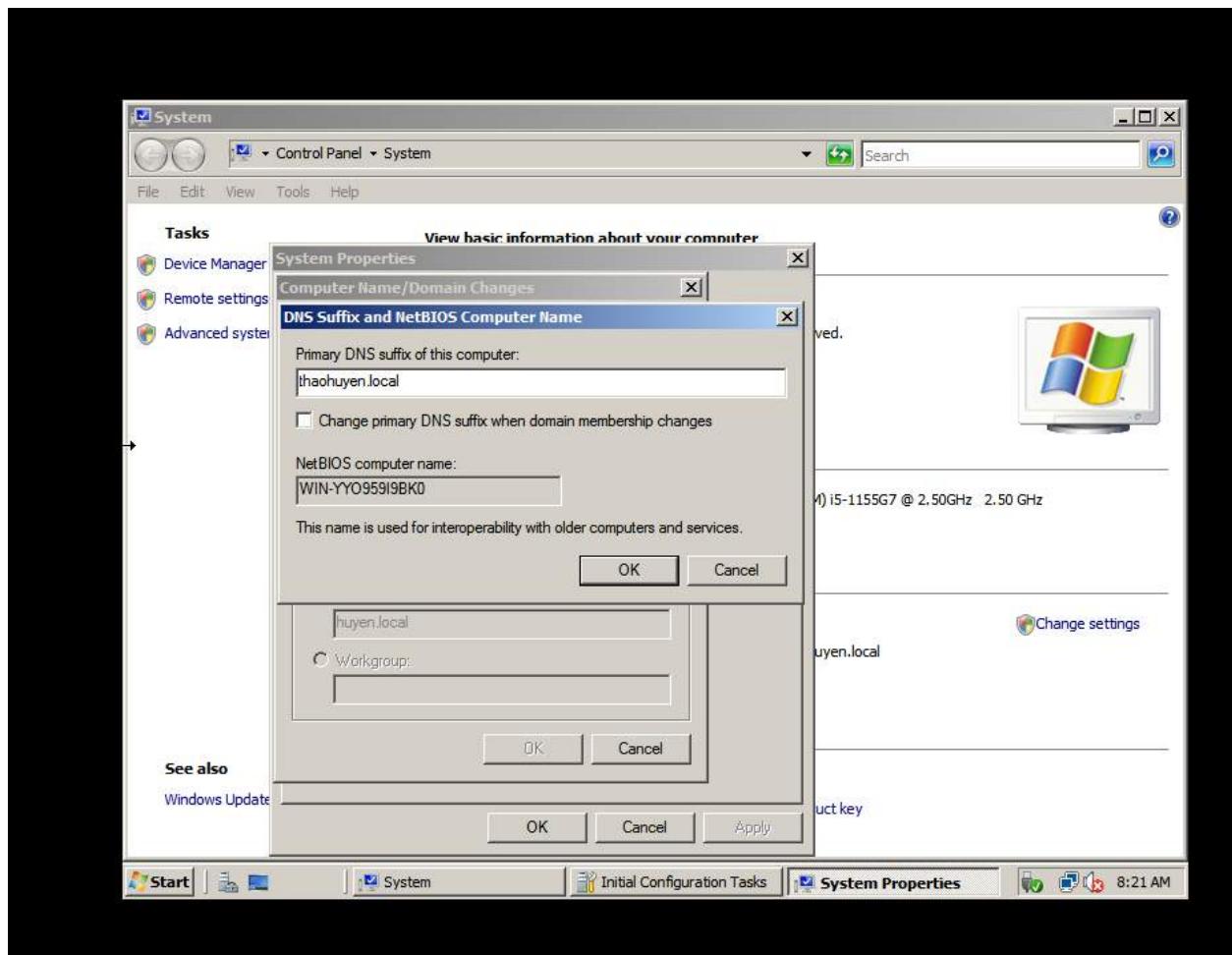


## Bước 2: Đặt IP cho máy Domain Controller là 10.0.0.2/8



**Bước 3: Đặt DNS Suffix bằng cách click phải lên My Computer > Properties >**

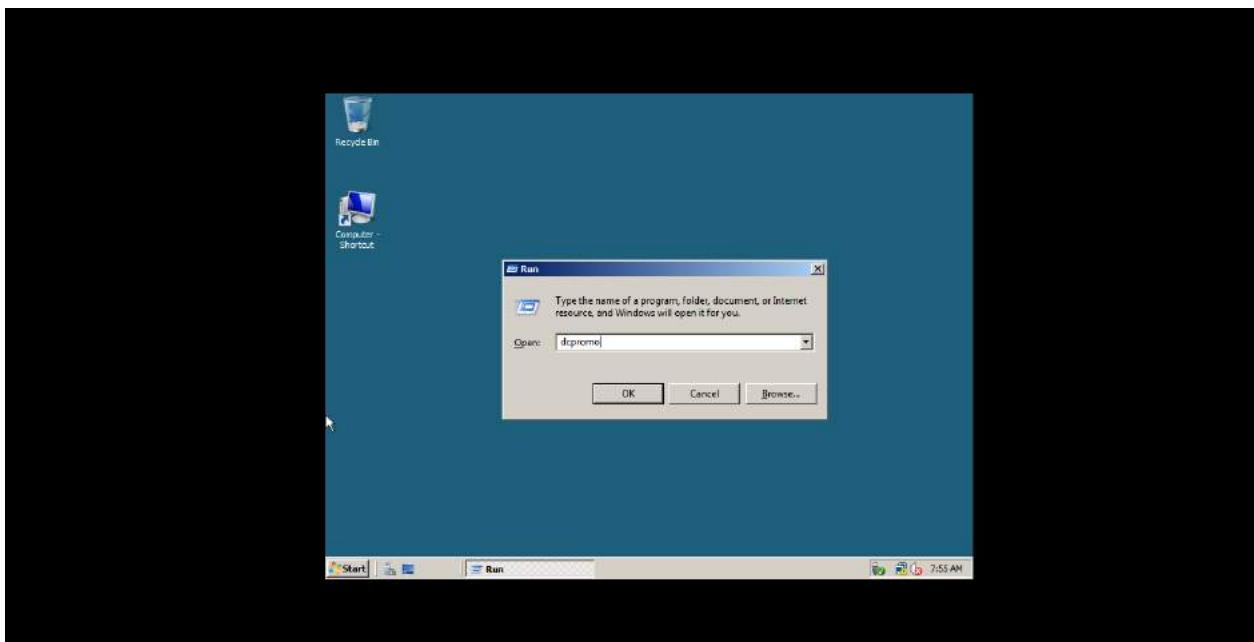
**Change Setting > Change > chọn More.**



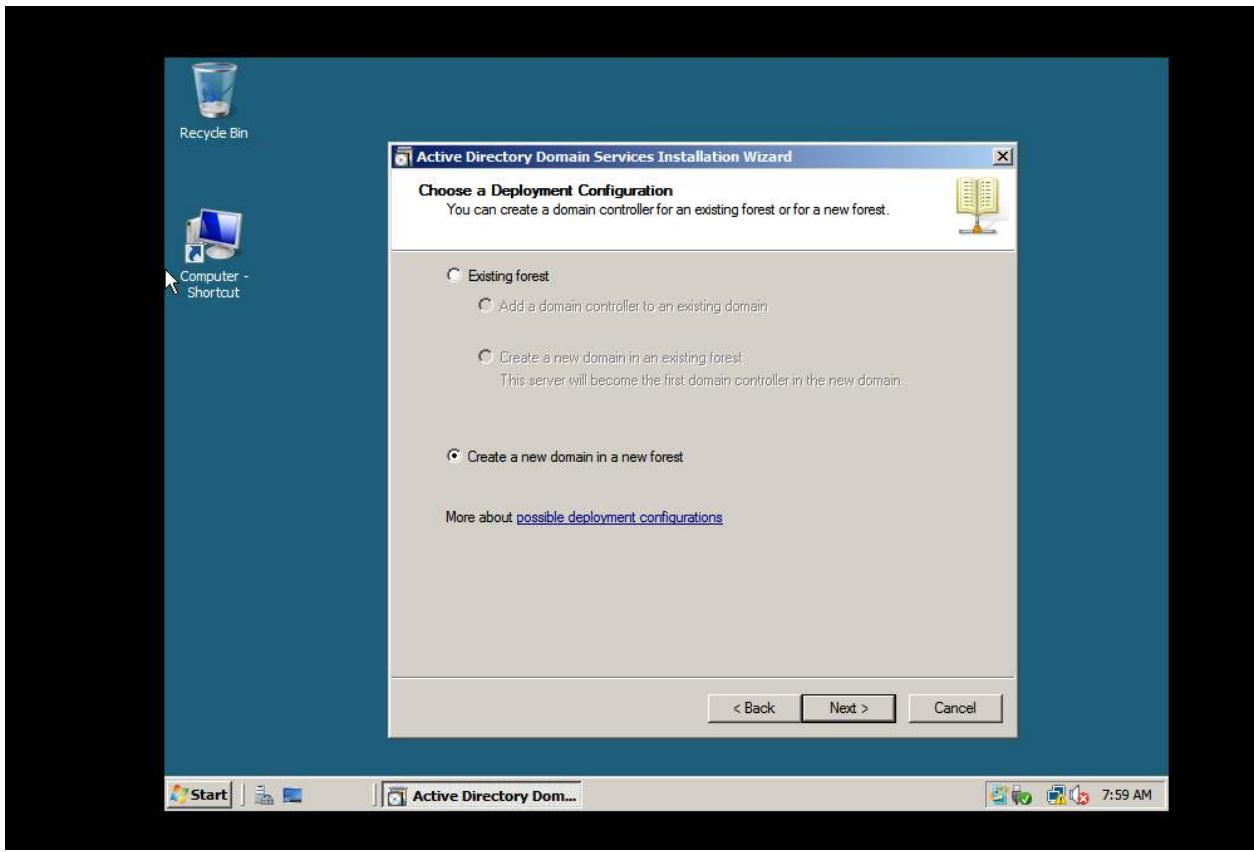
Sau đó Restart lại máy tính để áp dụng các thay đổi.

#### Bước 4: Nâng cấp máy chủ thành Domain Controller

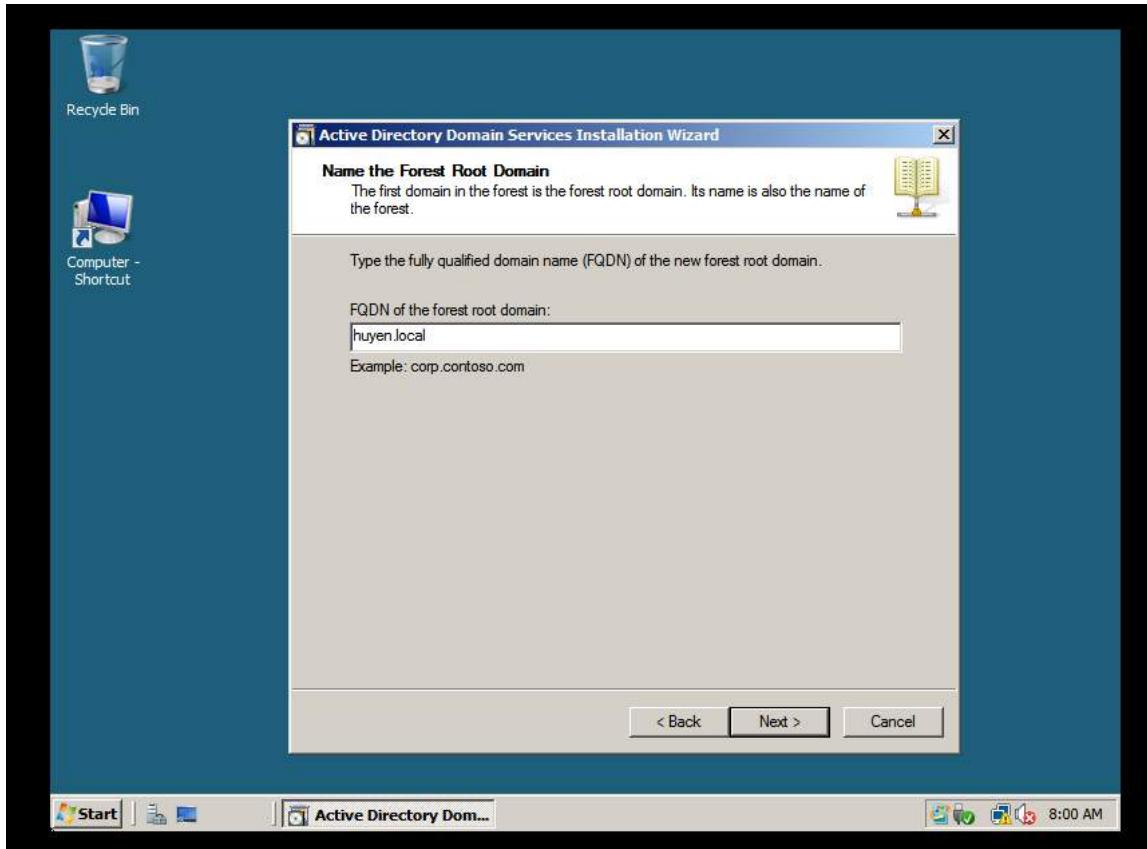
Hướng dẫn này thực hiện trên Windows Server 2008, nếu sử dụng phiên bản khác có thể có một số thay đổi trong quá trình nâng cấp.



Vào Start > run > nhập dcromo



Chọn Create a new domain in a new forest

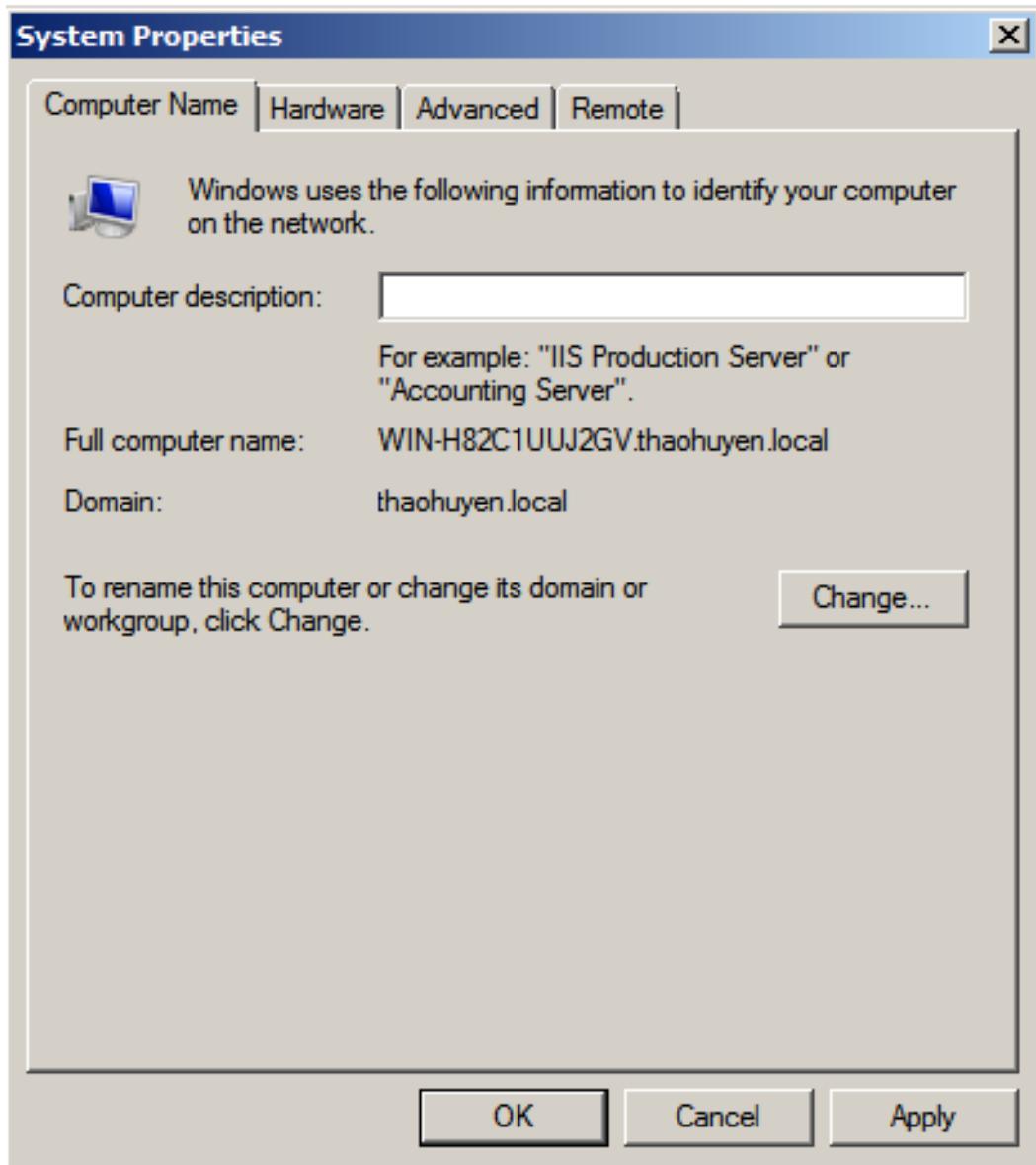


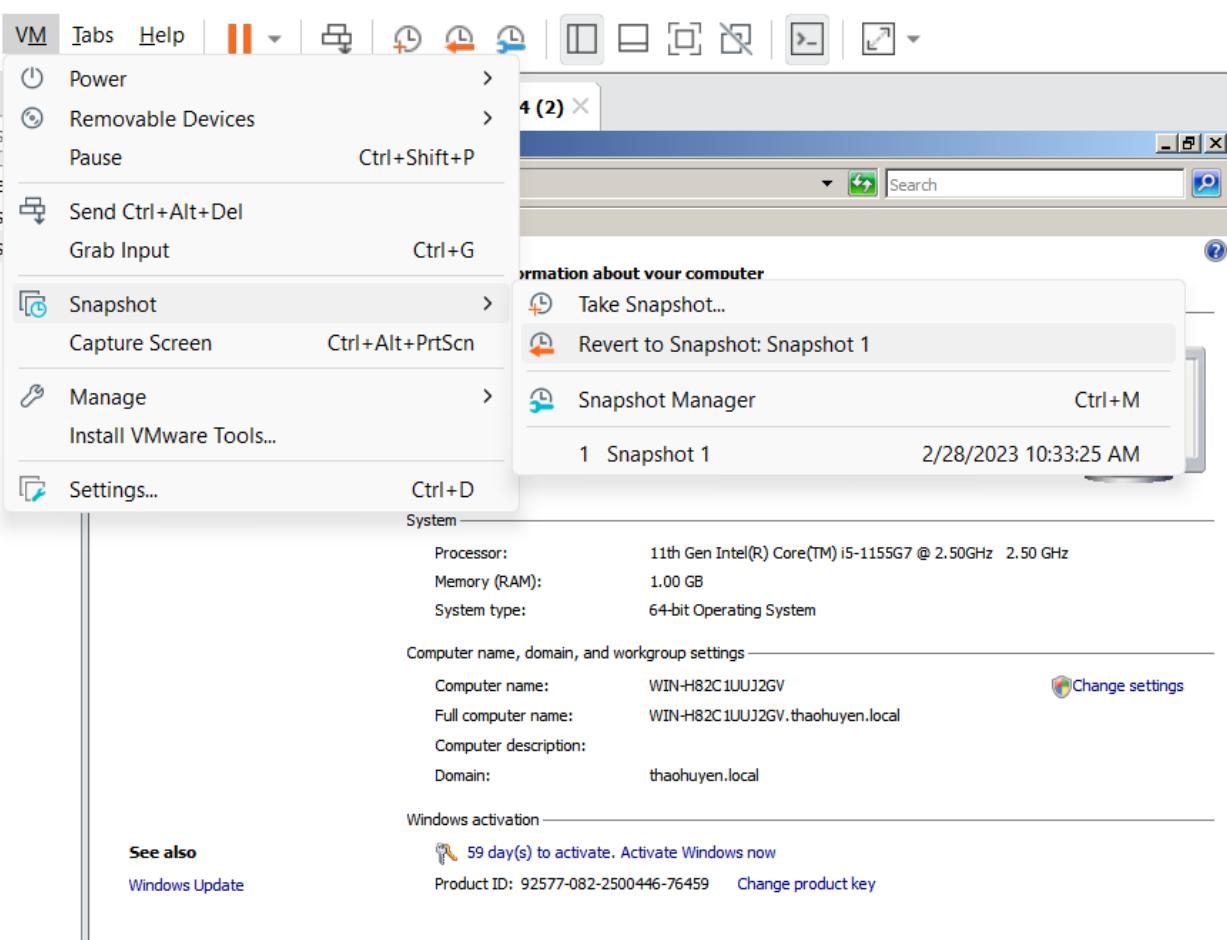
Nhập domain (thaohuyen.local) cho Forest Root Domain.



Quá trình nâng cấp hoàn tất.

Sau khi nâng cấp thành công, khởi động lại server và vào Properties của Computer để kiểm tra:

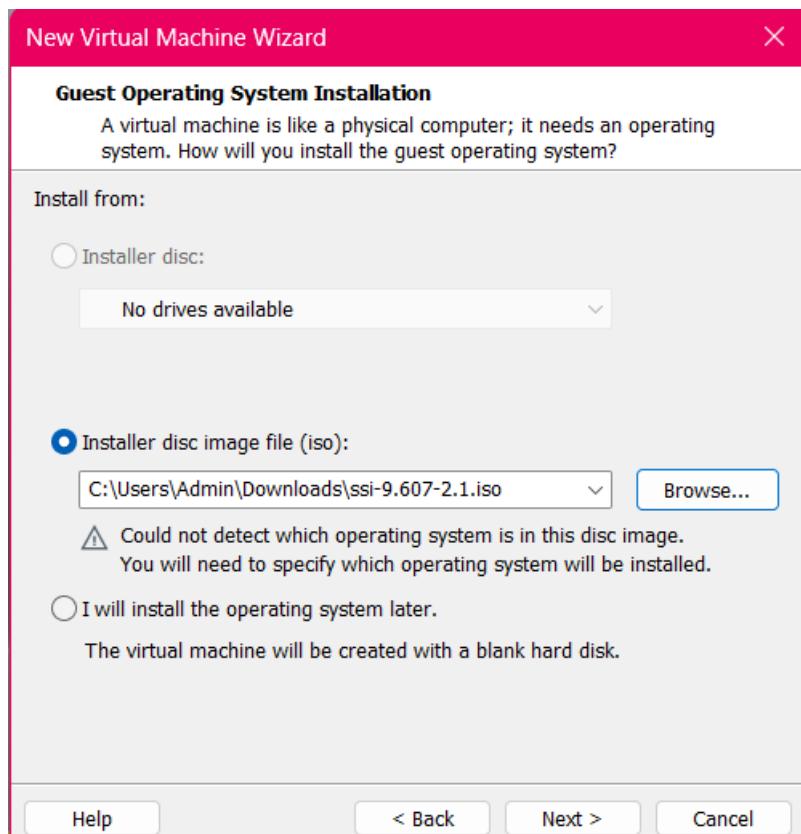


**Bước 5:** Tiến hành Snapshot lại để lưu lại trạng thái máy ảo lúc này.

## 2. Cài đặt và cấu hình máy Firewall Sophos UTM

Bước 1: Tải Sophos UTM 9.5, ta được file ISO cài đặt asg-9.511-2.1.iso

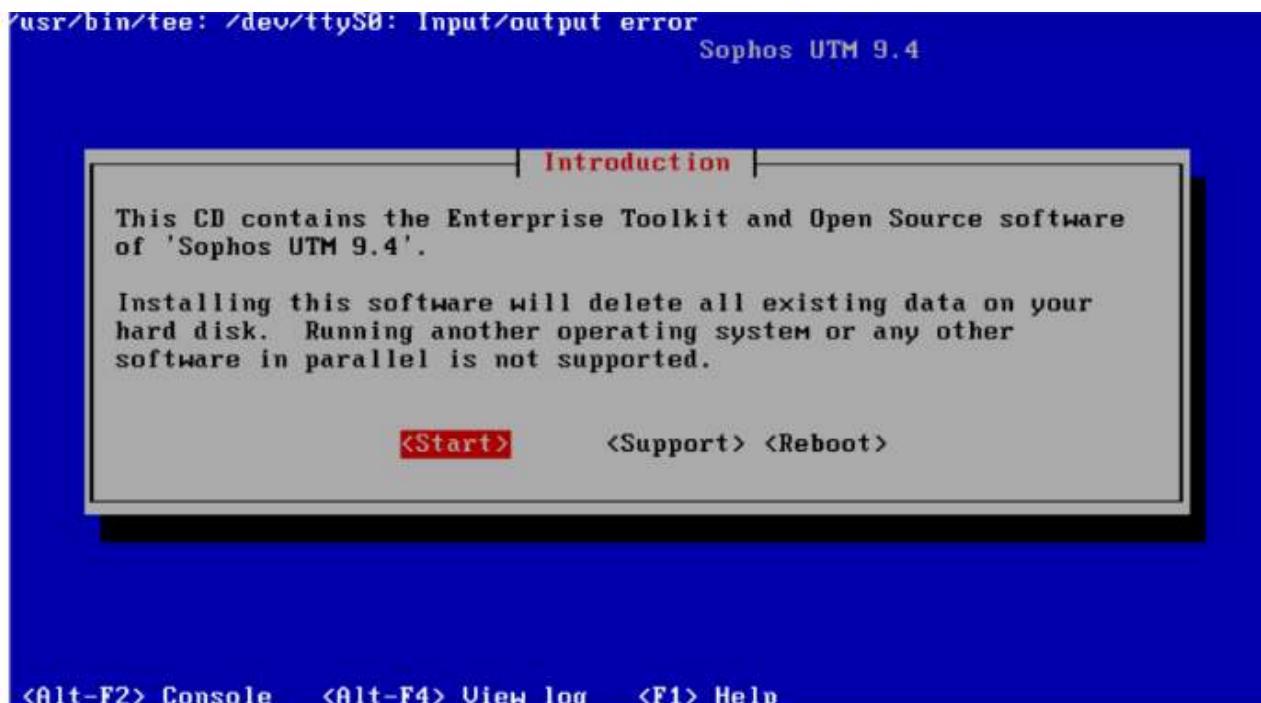
Bước 2: Tạo máy ảo mới bằng VMware và load file iso của Sophos UTM 9 để cài đặt tường lửa Sophos UTM.



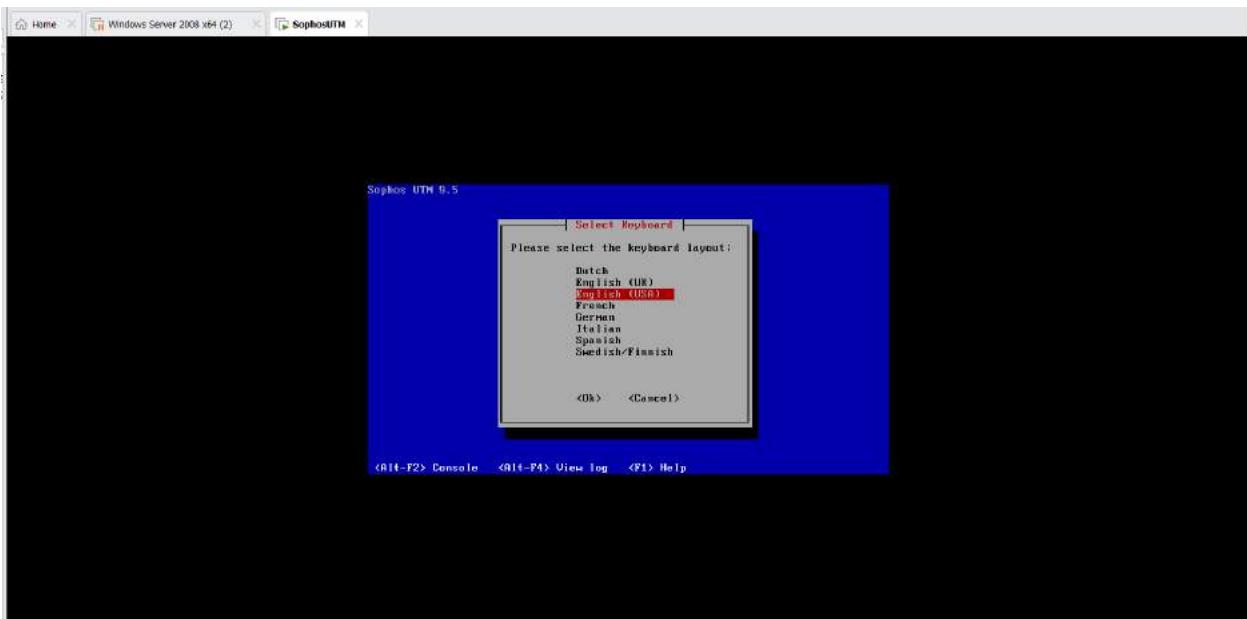
Bước 3: Khởi động máy ảo và nhấn Enter để bắt đầu cài đặt



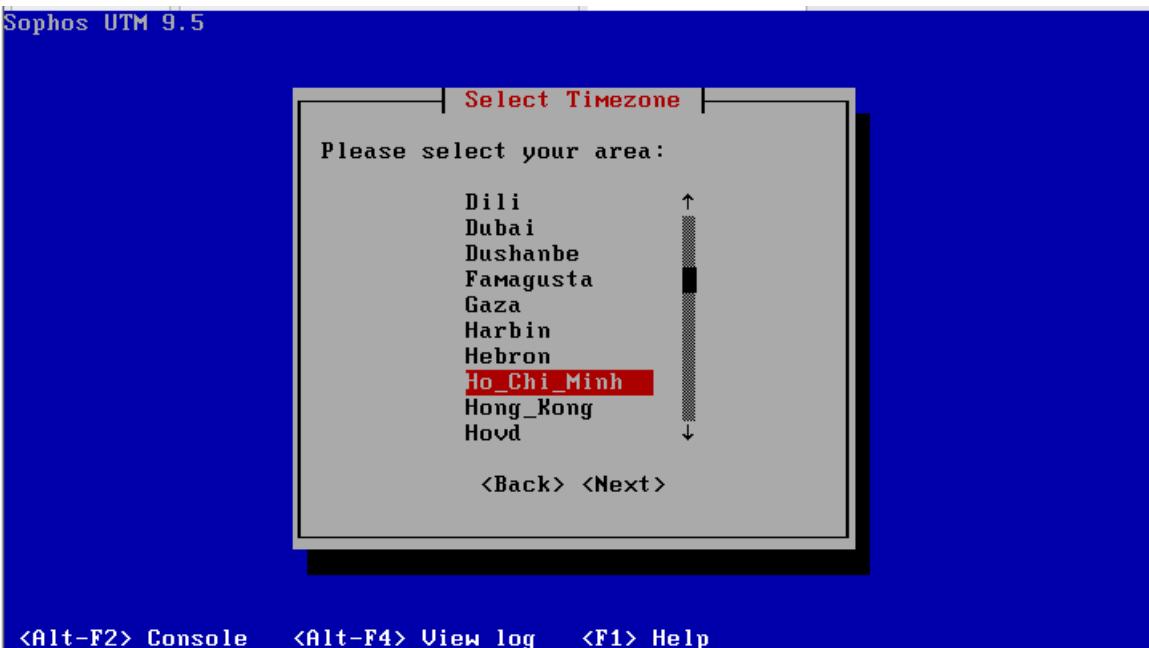
Sau đó, chọn Start để bắt đầu:



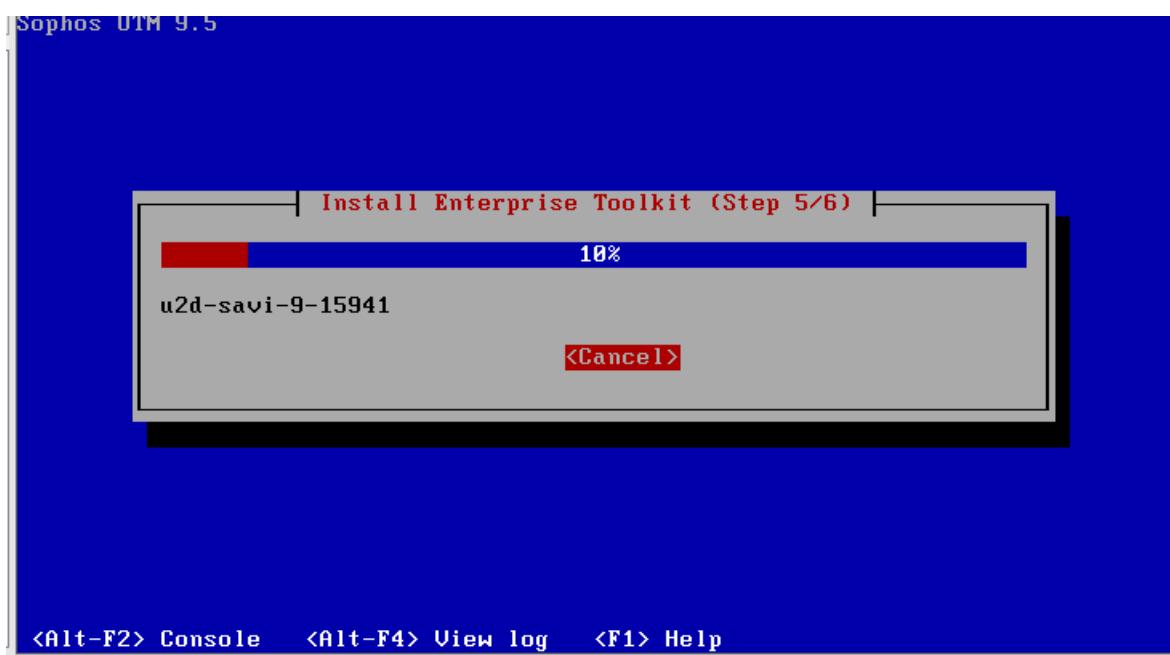
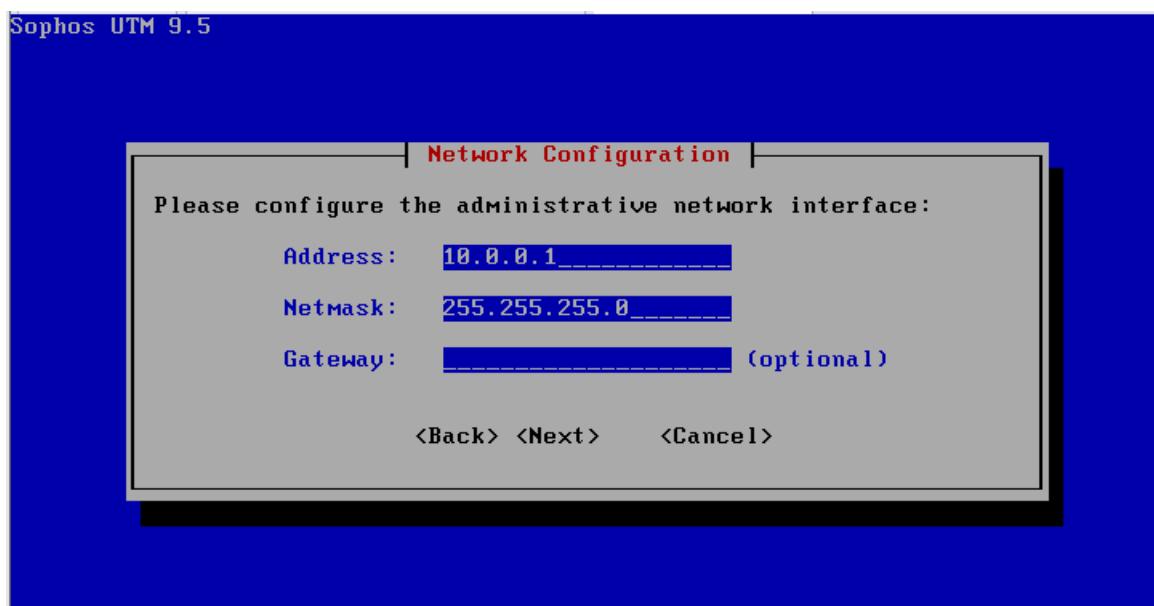
## Bước 4: Thiết lập ngôn ngữ:



Chọn ngôn ngữ English và múi giờ HCM:

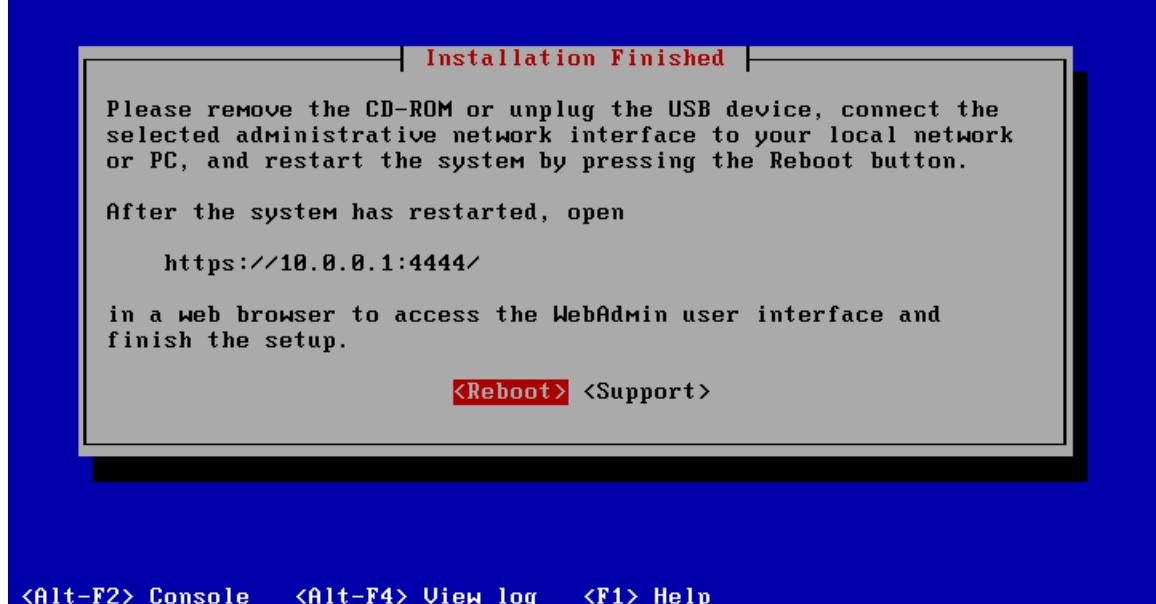


Bước 5: Chọn card mạng eth0 và thiết lập IP mặc định cho trang quản trị



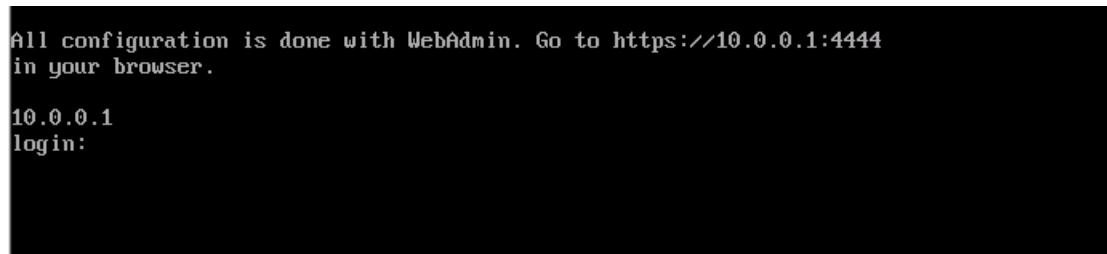
Sau khi cài đặt thành công, hệ thống sẽ thông báo địa chỉ IP đăng nhập vào trang quản trị  
WenAdmin <http://10.0.0.1:4444>

Sophos UTM 9.5



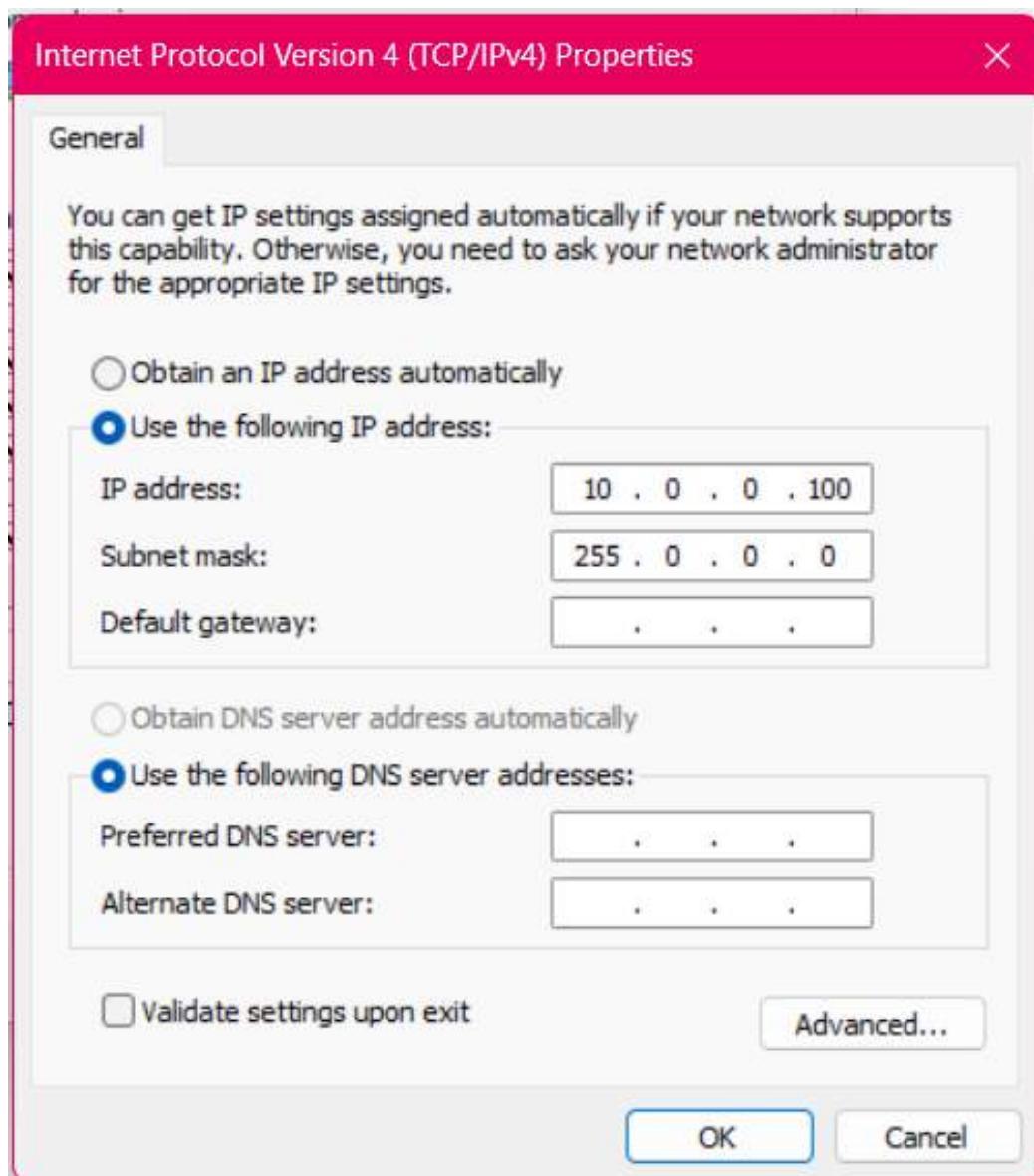
#### Bước 6: Khởi động lại Firewall Sophos UTM.

Sau khi khởi động thành công, chúng ta sẽ thấy IP được dùng để kết nối vào trang quản trị Firewall 10.0.0.1 (Tài khoản mặc định để đăng nhập là root và đặt mật khẩu ở lần đầu tiên, tuy nhiên chúng ta thực hiện các thiết lập cho Firewall qua WebAdmin)



#### Bước 7: Đặt IP cho card VMNet 1 để kết nối vào Firewall để quản lý

Thiết lập lớp mạng cho VMnet1 là 10.0.0.0/8 tại VMware (Chọn Edit > Virtual Network Editor...). Sau đó đặt IP cho card VMnet1 tại máy thật thành IP khác 10.0.0.1, ví dụ 10.0.0.100/8.



Bước 8: Từ máy thật, thực hiện lệnh ping 10.0.0.1 để kiểm tra máy thật đã thấy máy firewall chưa. Nếu chưa thấy thì cần kiểm tra lại IP và card mạng.

```
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time<1ms TTL=64
Reply from 10.0.0.1: bytes=32 time<1ms TTL=64
Reply from 10.0.0.1: bytes=32 time<1ms TTL=64
Reply from 10.0.0.1: bytes=32 time=1ms TTL=64

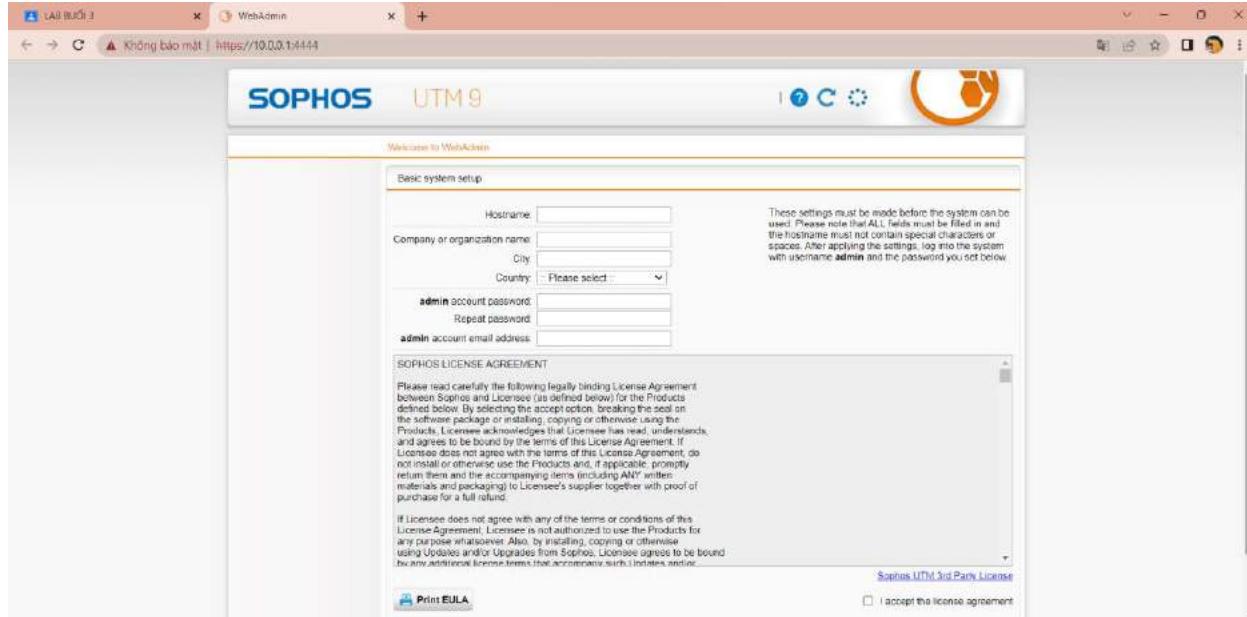
Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Admin>
```

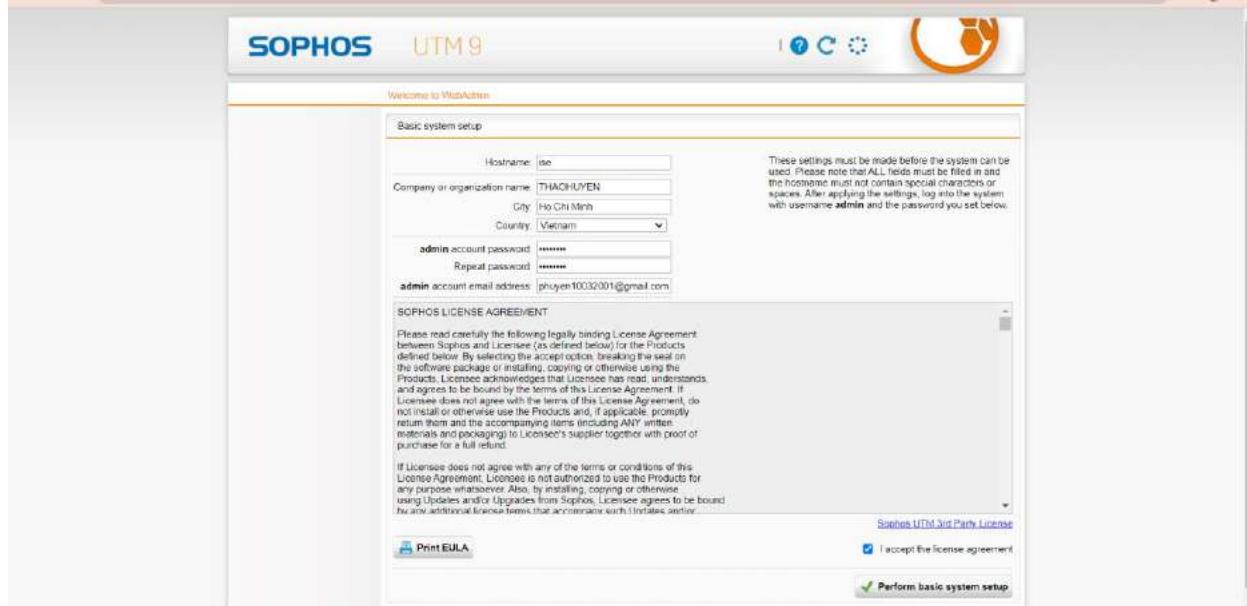
### Bước 9: Từ máy thật, kết nối vào WebAdmin của Firewall bằng địa chỉ

<https://10.0.0.1:4444>

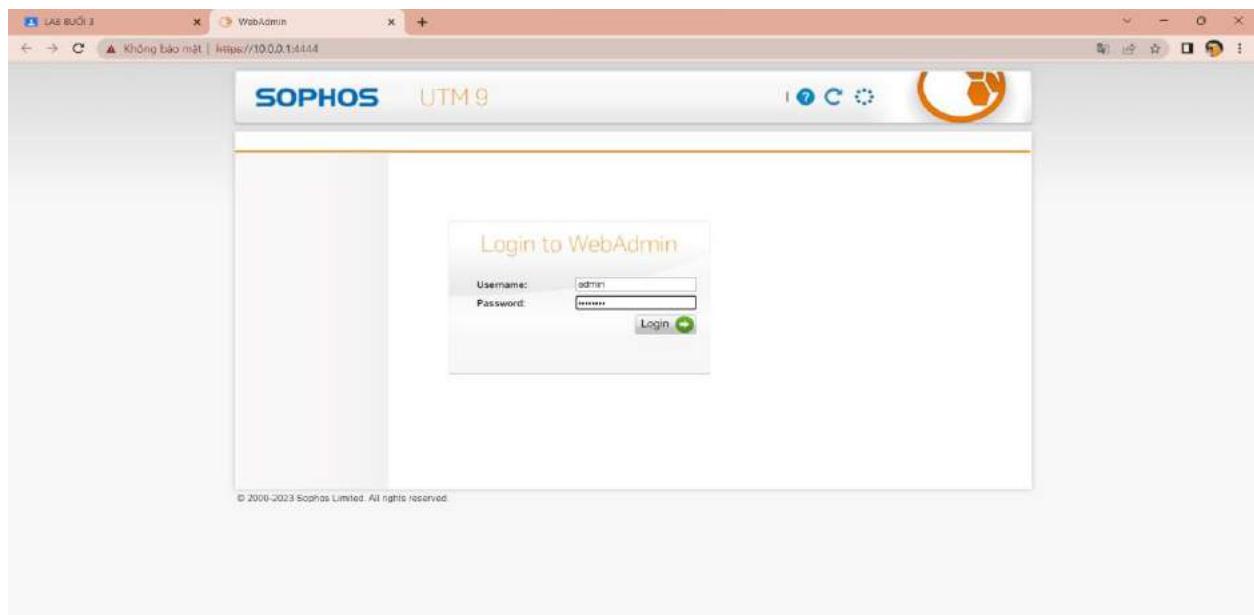
Nếu gặp cảnh báo bảo mật của trình duyệt, bỏ qua và tiếp tục truy cập WebAdmin



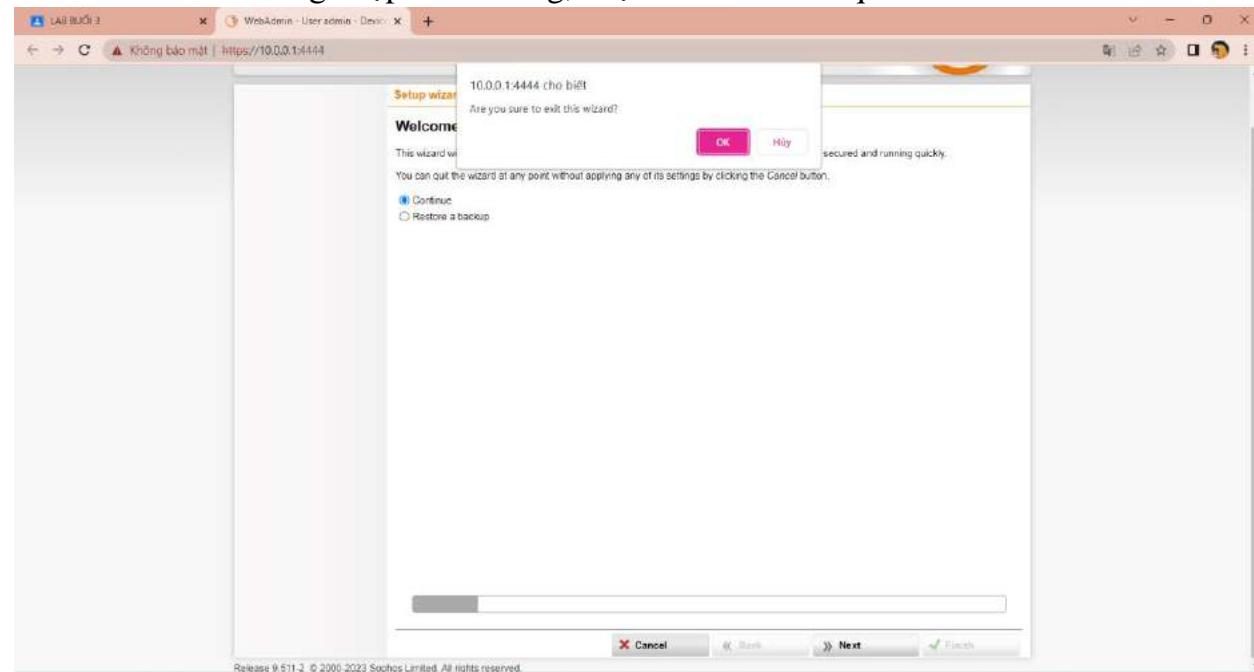
### Bước 10: Thiết lập các thông tin cơ bản cho Firewall Sophos và đặt mật khẩu cho tài khoản admin



Bước 11: Đăng nhập vào:



Bước 12: Sau khi đăng nhập thành công, chọn Cancel để bỏ qua trình Wizard.



## Giao diện trang quản lý firewall

The screenshot shows the Sophos UTM 9 dashboard. On the left, there's a sidebar with various management and protection modules like Management, Definitions & Users, Interfaces & Routing, Network Services, Network Protection, Web Protection, Email Protection, Advanced Protection, Endpoint Protection, Wireless Protection, Webserver Protection, RED Management, Site-to-Site VPN, Remote Access, Logging & Reporting, Support, and Log off. The main area has several cards: 'Info' (Model: ASG Software, License ID: 000000, Subscriptions: Basic Functionality, Uptime: 0d 0h 5m), 'Advanced Threat Protection' (Botnet/Command-and-control traffic detection is disabled), 'Current System Configuration' (listing various services like Firewall, Intrusion Prevention, Web Filtering, etc., many of which are inactive), 'Resource Usage' (CPU at 7%, RAM at 11% of 4.0 GB, Log Disk at 8% of 25.8 GB, Data Disk at 4% of 19.7 GB), and 'Today's Threat Status' (Firewall: 0 packets filtered, IPS: 0 attacks blocked, Antivirus: 0 items blocked, Antispam: 0 emails blocked, Antispyware: 0 items blocked, Web Filter: 0 URLs filtered, WAF: 0 attacks blocked, Sandstorm: 0 malicious items detected).

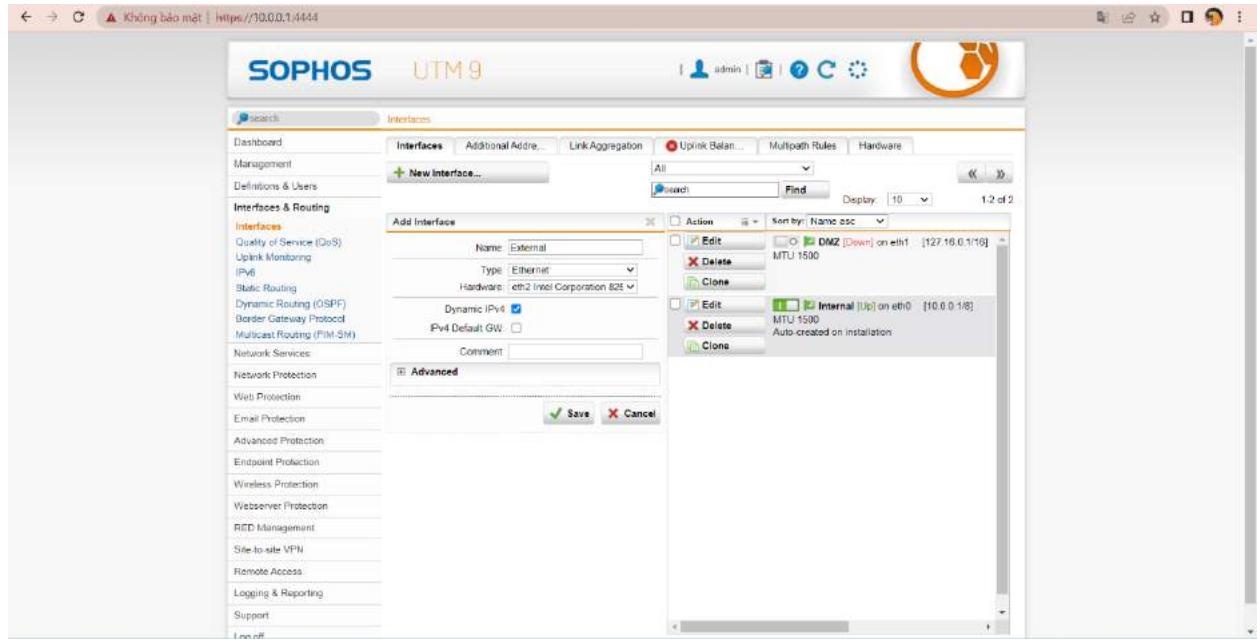
Bước 13: Cấu hình IP cho interface của Firewall theo đúng mô hình triển khai

Vào Interface & Routing để thiết lập các interface

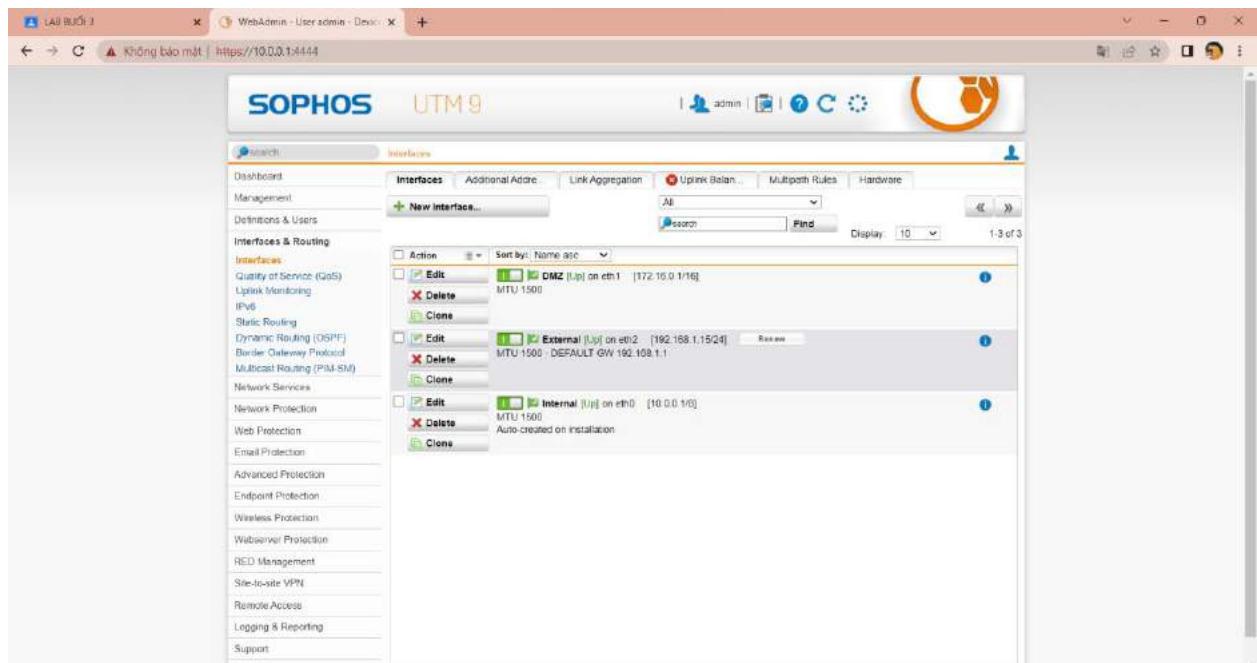
Tạo interface cho vùng DMZ

The screenshot shows the 'Interfaces' configuration screen. The sidebar includes Management, Definitions & Users, Interfaces & Routing (selected), Quality of Service (QoS), Uplink Monitoring, IPv4, Static Routing, Dynamic Routing (OSPF), Border Gateway Protocol, Multicast Routing (PIM-SM), Network Services, Network Protection, Web Protection, Email Protection, Advanced Protection, Endpoint Protection, Wireless Protection, Webserver Protection, RED Management, Site-to-site VPN, Remote Access, Logging & Reporting, Support, and Log off. The main area has tabs for Interfaces, Additional Address, Link Aggregation, Uplink Balancing, Multipath Rules, and Hardware. A 'New Interface...' button is visible. The 'Edit Interface' dialog is open for a 'DMZ' interface, showing settings for Type (Ethernet), Hardware (eth1 Intel Corporation 825), Dynamic IPv4 (IPv4 address: 172.16.0.1, IPv4 Netmask: 255.255.0.0, IPv4 Default GW: 0), and Comment. To the right, a list of existing interfaces is shown: 'DMZ [Up] on eth1 [172.16.0.1/16]' (MTU 1500), 'External [Up] on eth2 [192.168.209.1/24]' (MTU 1500), and 'Internal [Up] on eth0 [10.0.0.1/8]' (MTU 1500, Auto-created on installation). Buttons for Edit, Delete, and Clone are available for each entry.

## Tạo Interface External để kết nối internet



Bước 14: Bật cả 3 interface và đặc biệt External đã nhận được IP từ DHCP Server hay chưa.



Kiểm tra xem máy Firewall có kết nối được internet hay không bằng cách vào

Support > Tool > dùng tool Ping check để ping google.com dùng interface

The screenshot shows the Sophos UTM 9 WebAdmin interface. In the top navigation bar, there is a message 'Không bảo mật | https://10.0.0.1:4444'. The main title is 'SOPHOS UTM 9'. On the left sidebar under 'Tools', the 'Ping Check' tab is selected. The main panel shows a 'Ping Check' form with the following fields: 'Ping host' dropdown set to 'Custom hostname/IP add.', 'Hostname/IP address' input field containing 'google.com', and 'Ping over interface' dropdown set to 'External'. A green 'Apply' button is at the bottom right of the form.

Firewall đã kết nối thành công đến Internet

The screenshot shows the Sophos UTM 9 WebAdmin interface. The 'Ping Check Result' section displays the output of a ping command to google.com. The output shows the following details:

```

PING google.com (142.250.199.78) From 192.168.1.15 ttl=256(64) bytes of data.
64 bytes from hkg07s37-in-f14.1e100.net (142.250.199.78): icmp_seq=1 ttl=57 time=43.7 ms
64 bytes from hkg07s37-in-f14.1e100.net (142.250.199.78): icmp_seq=2 ttl=57 time=44.3 ms
64 bytes from hkg07s37-in-f14.1e100.net (142.250.199.78): icmp_seq=3 ttl=57 time=44.8 ms
64 bytes from hkg07s37-in-f14.1e100.net (142.250.199.78): icmp_seq=4 ttl=57 time=44.4 ms
64 bytes from hkg07s37-in-f14.1e100.net (142.250.199.78): icmp_seq=5 ttl=57 time=44.8 ms

```

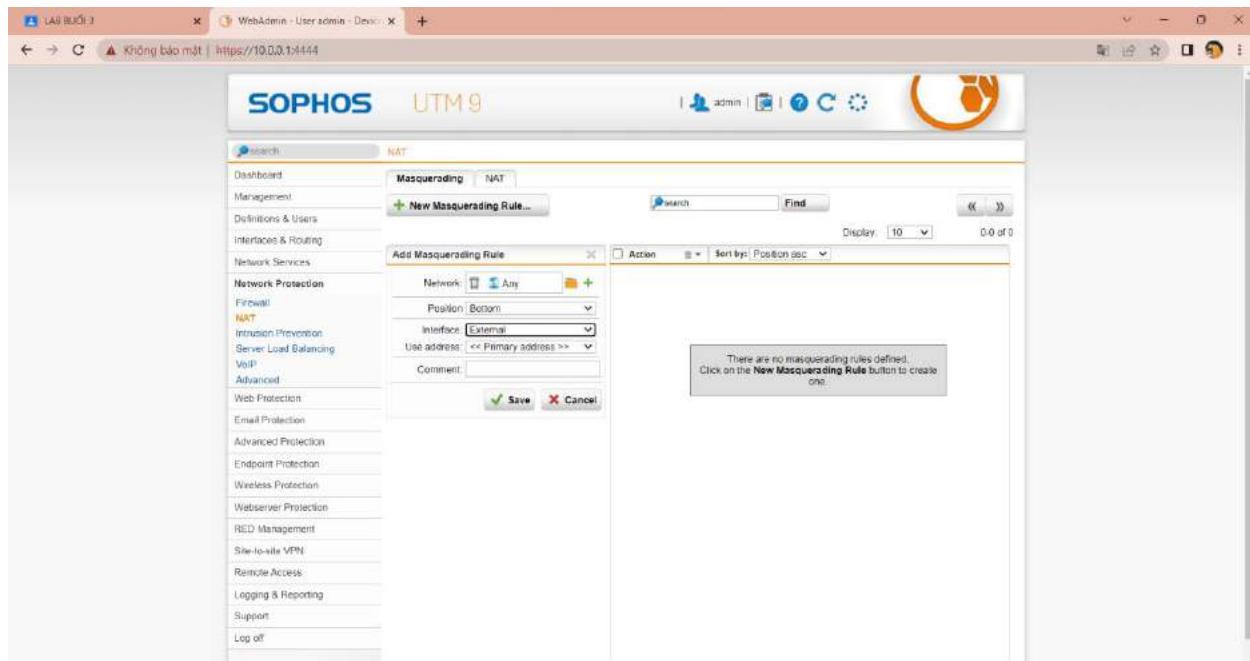
Below the ping results, it says '--- google.com ping statistics ---' and shows '5 packets transmitted, 5 received, 0% packet loss, time 400ms'. At the bottom, it shows 'rtt min/avg/max/mdev = 43.757/44.434/44.855/0.462 ms'.

Lưu ý: Nếu không kết nối được hay interface External không nhận được IP thì chúng ta sẽ không làm gì được nữa và cần kiểm tra kỹ lại quá trình cấu hình theo các bước đã hướng dẫn hoặc khởi động lại Firewall để kiểm tra lại.

Bước 15: Cấu hình NAT Outbound. Cơ chế Nat sẽ xác định mạng nào sẽ NAT mạng ra ngoài Internet

Vào Network Protection > NAT > New Masquerading Rule và cấu hình như sau

Chọn interface External



Sau đó kích hoạt rule này. Kết quả sau khi cấu hình:

The screenshot shows a 'Masquerading' tab selected under 'NAT'. A single rule is listed: 'Any' (Internal) to 'External'. The interface includes buttons for 'Edit', 'Delete', and 'Clone', and a search bar.

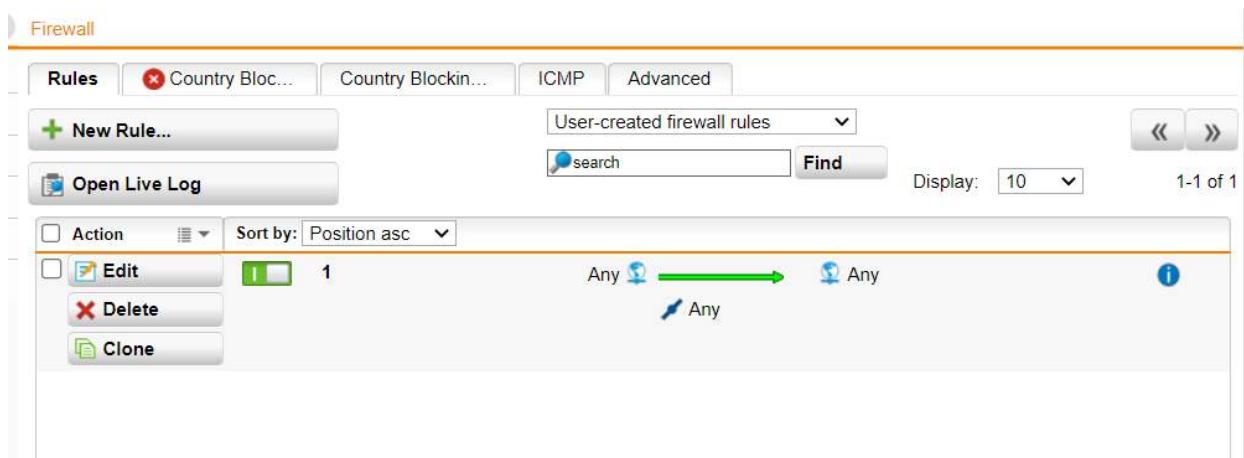
Kết quả sau khi thêm rule NAT

Bước 16: Cấu hình Rule để máy chủ Domain Controller kết nối được với internet bình thường.

Vào Network Protection > Firewall > Rule > New Rule

The screenshot shows the 'Add Rule' dialog in the Sophos UTM 9 interface. The 'Sources' section has 'Any' selected. The 'Services' and 'Destinations' sections also have 'Any' selected. The 'Action' is set to 'Allow'. The message 'There are no such firewall rules defined.' is displayed.

Chọn Any ở Source, Service và Destinations



Kết quả sau khi thiết lập Rule

Bước 17: Kiểm tra kết nối Internet của máy Domain Controller

```
C:\WINDOWS\system32\cmd. + ▾
Microsoft Windows [Version 10.0.22621.1265]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping google.com

Pinging google.com [2404:6800:4005:804::200e] with 32 bytes of data:
Reply from 2404:6800:4005:804::200e: time=69ms
Reply from 2404:6800:4005:804::200e: time=69ms
Reply from 2404:6800:4005:804::200e: time=69ms
Reply from 2404:6800:4005:804::200e: time=70ms

Ping statistics for 2404:6800:4005:804::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 69ms, Maximum = 70ms, Average = 69ms

C:\Users\Admin>
```

Ping thành công đến Google.com



Dùng trình duyệt để truy cập web và kiểm tra.

Nếu Domain Controller kết nối được Internet tức quá trình thiết lập tường lửa cơ bản đã thành công.

Bước 18: Quay lại trang WebAdmin của Firewall thử tắt Rule Firewall và một vài Rule vừa thiết lập và quay lại máy Domain Controller để truy cập Internet và rút ra kết luận.

## B. Trả lời câu hỏi

### 1. Nêu nguyên tắc hoạt động của Firewall Sophos UTM và Domain Controller trong mô hình mạng đã thiết lập trong bài lab.

- Nguyên tắc hoạt động của Firewall Sophos UTM

#### *Đại lý xác thực Sophos*

Đây là một tác nhân nhẹ với mục đích duy nhất là xác thực người dùng bằng UTM. Có thể tải xuống và cấu hình Sophos Authentication Agent (SAA) từ **Definitions & Users > Client Authentication**.

Đây là tùy chọn ưu tiên để xác thực người dùng trên mạng cục bộ.

#### VPN truy cập từ xa

Phần mềm VPN máy khách cho phép người dùng từ xa kết nối với UTM thông qua một đường hầm an toàn. Để truy cập VPN, người dùng phải xác thực, do đó người dùng VPN cũng phải tuân theo các quy tắc tường lửa dựa trên người dùng.

UTM hỗ trợ một số giao thức VPN bao gồm SSL, IPsec, PPTP và L2TP. Chúng có thể được cấu hình trong phần VPN truy cập từ xa.

#### Quy tắc tường lửa dựa trên người dùng

Sau khi người dùng đã được xác thực, một đối tượng Mạng người dùng cho người dùng đó có thể được sử dụng làm nguồn hoặc đích trong các quy tắc tường lửa.

#### Quy tắc tường lửa dựa trên nhóm

Ngoài ra, các nhóm được tạo trong **Định nghĩa & Người dùng > Người dùng & Nhóm > Nhóm** có thể được sử dụng trong quy tắc tường lửa. Các nhóm này cũng có thể được liên kết với các nhóm dịch vụ thư mục (ví dụ: Active Directory).

- Nguyên tắc hoạt động của DC

**Domain Controller** sẽ đóng vai trò như một người gác cổng. Các yêu cầu của dùng dùng sẽ được thông qua bởi Domain Controller để xác thực danh tính và ủy quyền đăng nhập. Cách xác thực thường là dùng username và mật khẩu người dùng. Sau khi thực hiện các thao tác xác thực trên, người dùng có thể sử dụng tài nguyên website như bình thường.

Một mô hình Domain Controller không tự có sẵn mà người quản trị hệ thống cần cài đặt để tích hợp các tính năng vào hệ thống. Các bước để cài đặt như sau:

- **Bước 1:** Thực hiện thao tác đặt IP tĩnh cho thiết bị máy chủ được lựa chọn làm Domain Controller.
- **Bước 2:** Ở bước này việc xây dựng Domain Controller dựa trên máy server đã được lựa chọn để làm Domain Controller.
- **Bước 3:** Tiến hành quá trình tạo User ngay trong Domain Controller cho những máy Client.
- **Bước 4:** Thực hiện thao tác đặt địa chỉ IP cũng như Join cho các Client vào vị trí Domain.
- **Bước 5:** Ở bước cuối cùng này chúng ta đăng nhập vào máy Client sau đó thực hiện việc kiểm tra lại toàn bộ Domain Controller để hoàn thành quá trình.

## LAB 04: THIẾT LẬP RULES TƯỜNG LƯẨA SOPHOS UTM

### A. Thực hành

#### 1. Tích hợp Domain vào Sophos UTM

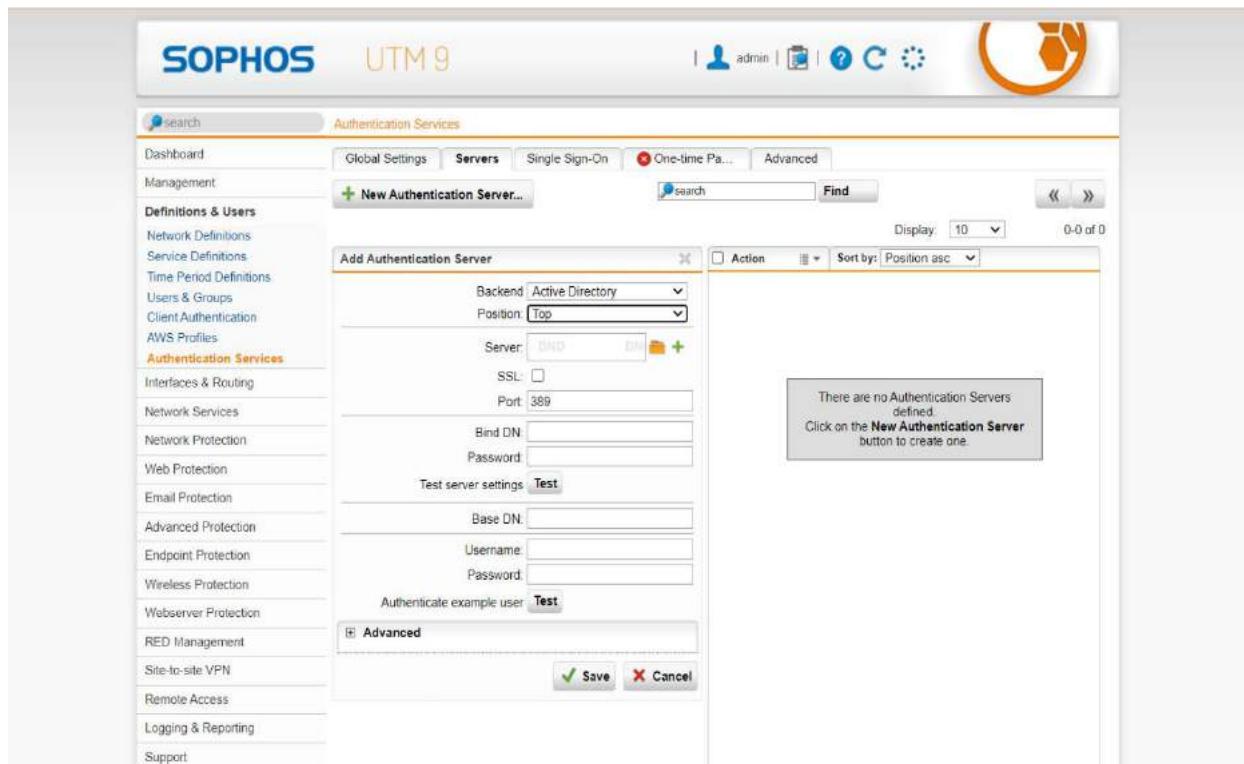
Bước 1: Khởi động và kiểm tra các máy Domain Controller và Firewall Sophos UTM đã hoạt động ổn định chưa. Kiểm tra và đặt mật khẩu cho tài khoản Administrator trên máy Domain Controller nếu chưa thiết lập mật khẩu.

Bước 2: Kết nối vào WebAdmin của Firewall Sophos UTM.

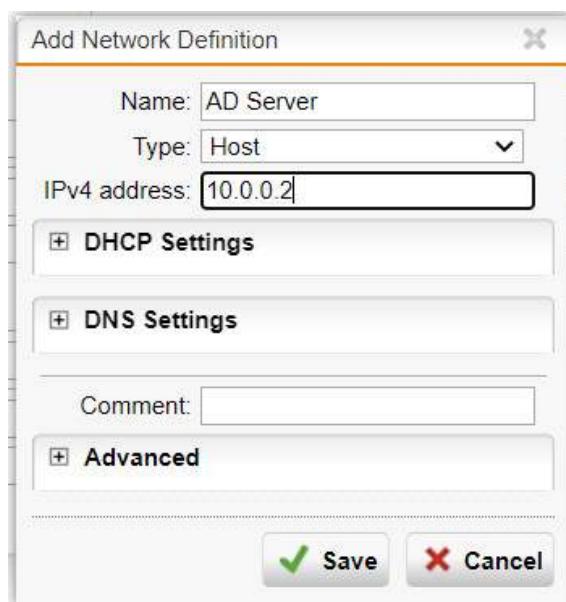
Vào Definitions & Users > Authentication Services > Chọn Server > Chọn New

Authentication Server...

Bước 3: Tại mục Backend, chọn Active Directory



Bước 4: Tại phần Server, chọn dấu cộng và nhập thông tin Domain Controller



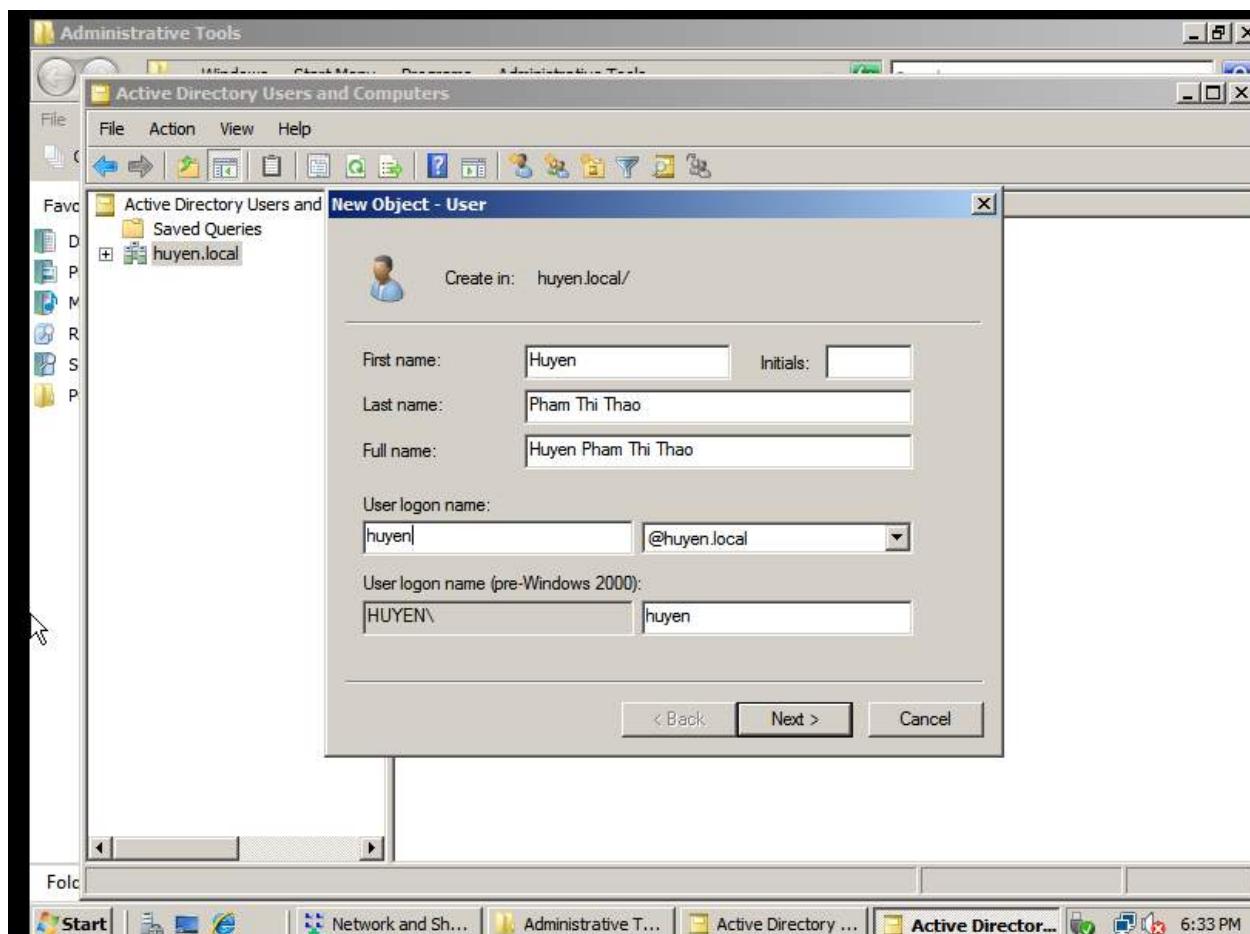
- Bước 5: Tại trường Bind DN, nhập thông số cấu hình như sau ứng với domain huyen.local đã thiết lập.

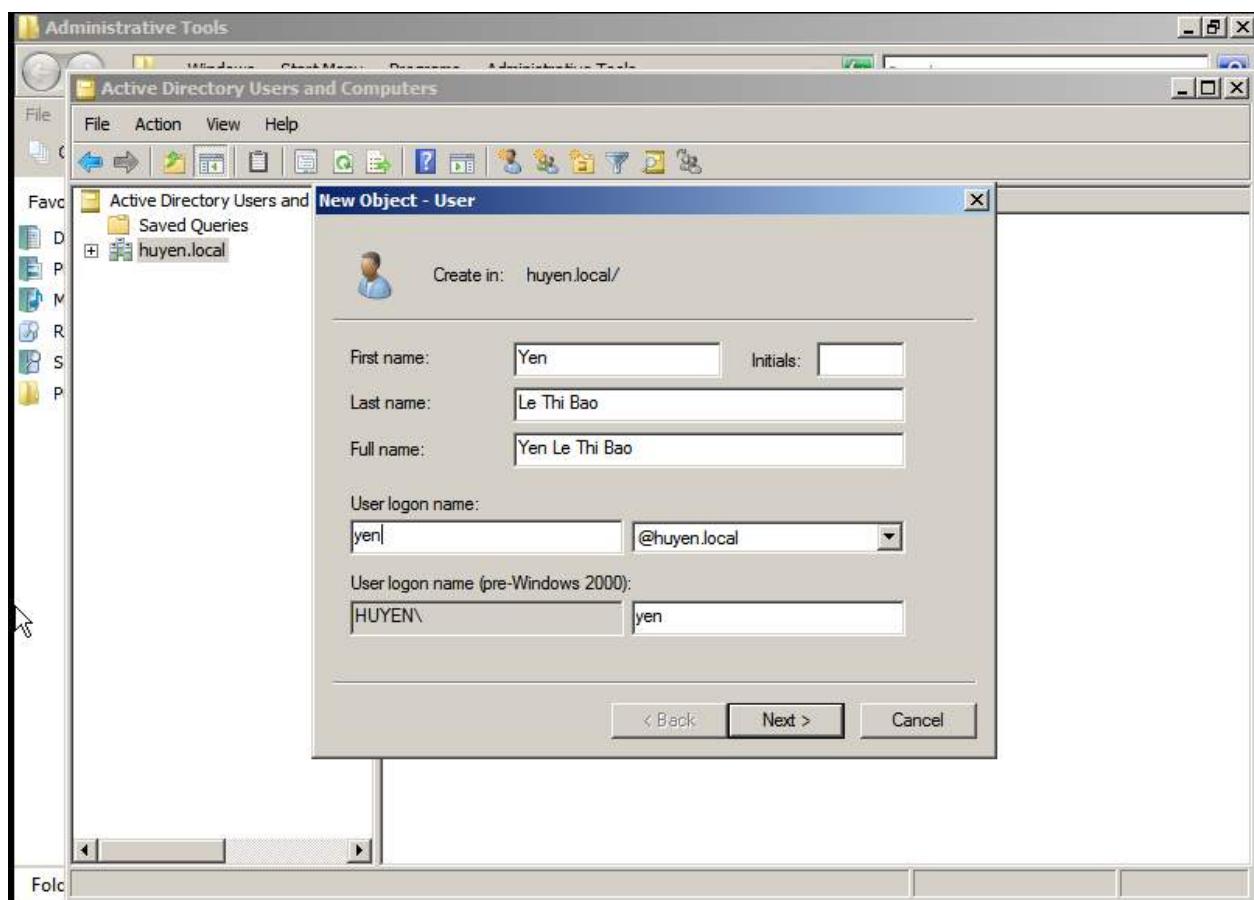
CN=administrator,CN=Users,DC=huyen,DC=local

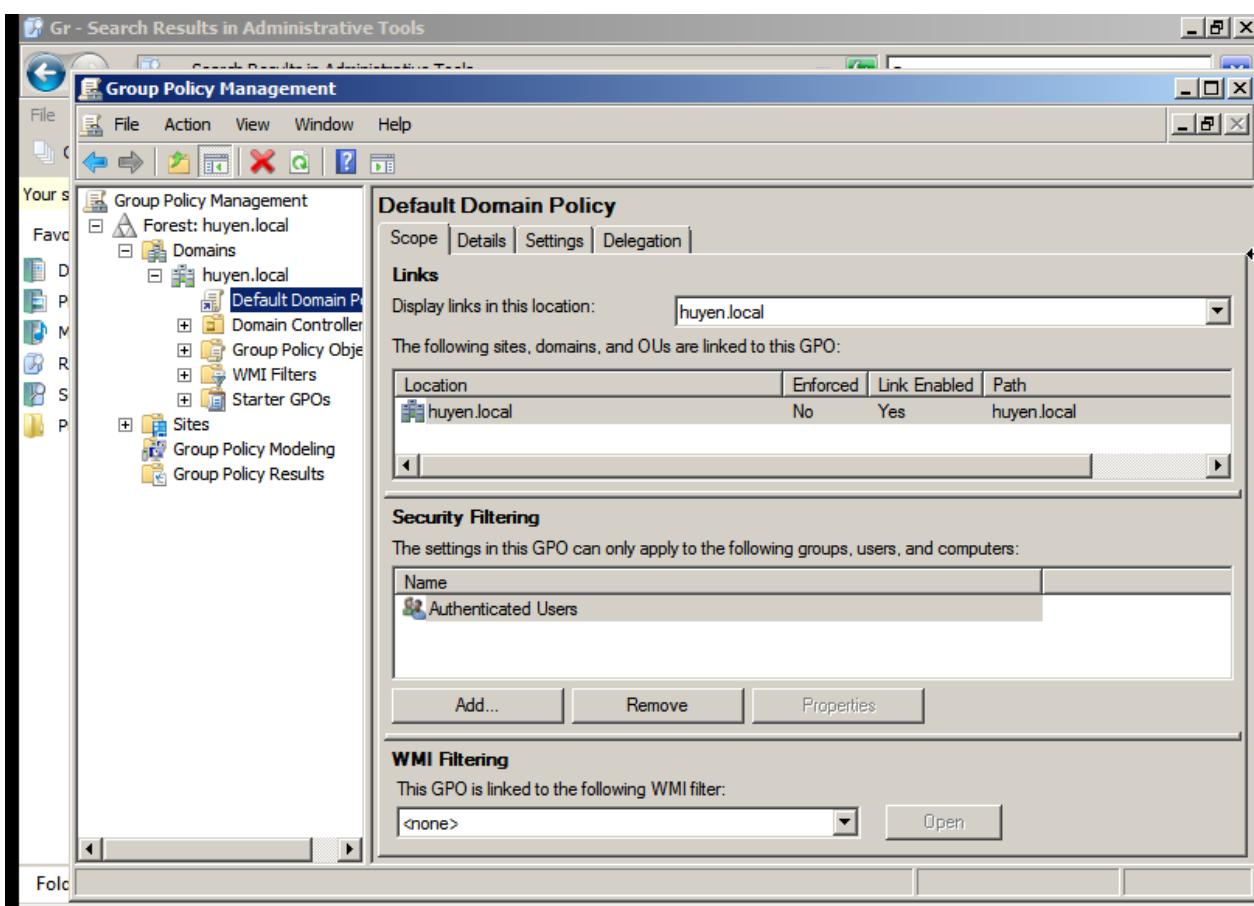
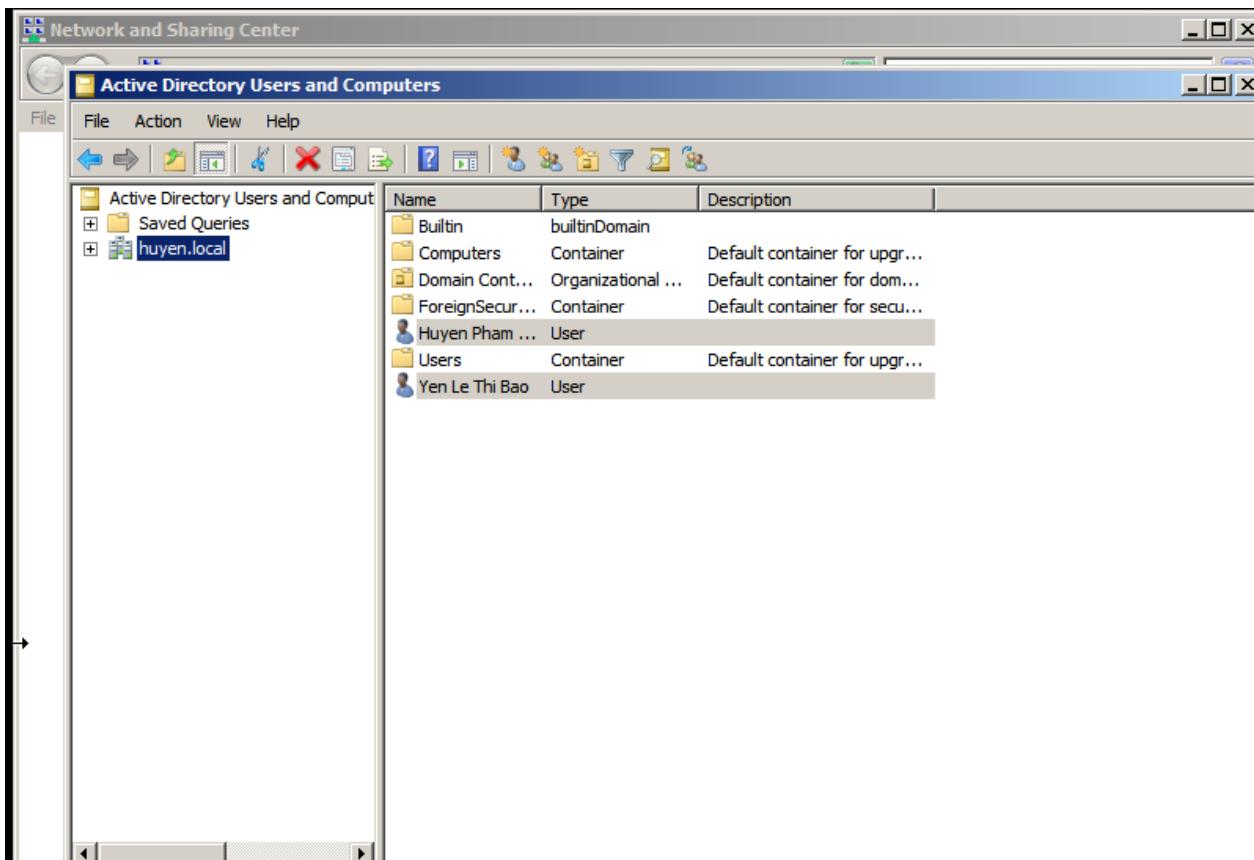
Bước 6: Nhập mật khẩu tài khoản Administrator trên máy DC và nhấn Test để kiểm tra.  
Nếu kết quả Server test passed là thành công.

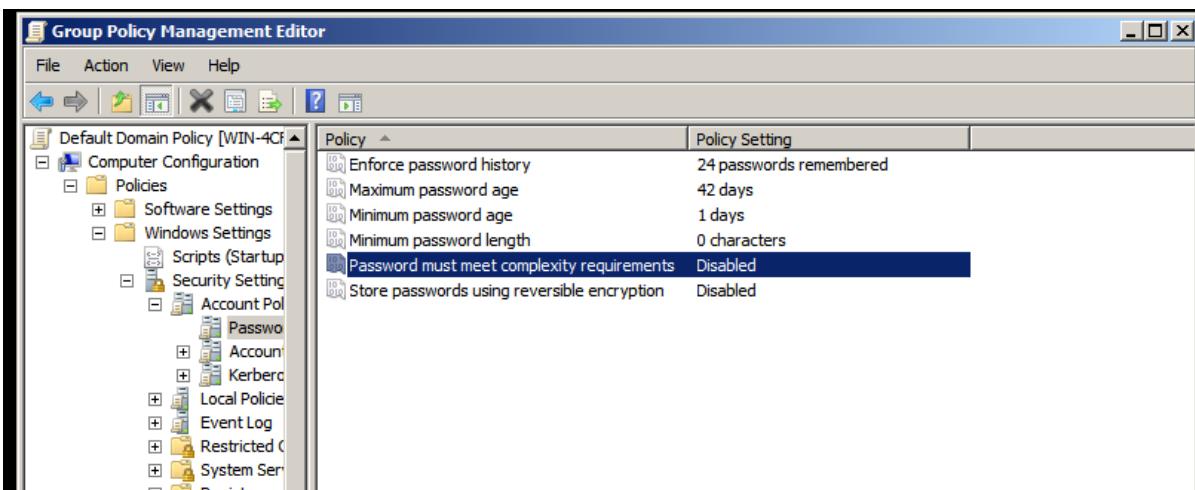
Bước 7: Chọn Save để lưu lại cấu hình.

Bước 8: Tạo 2 user mới trên Domain tại máy Domain Controller. Vào Start > Administrative Tools > Active Directory Users and Computers

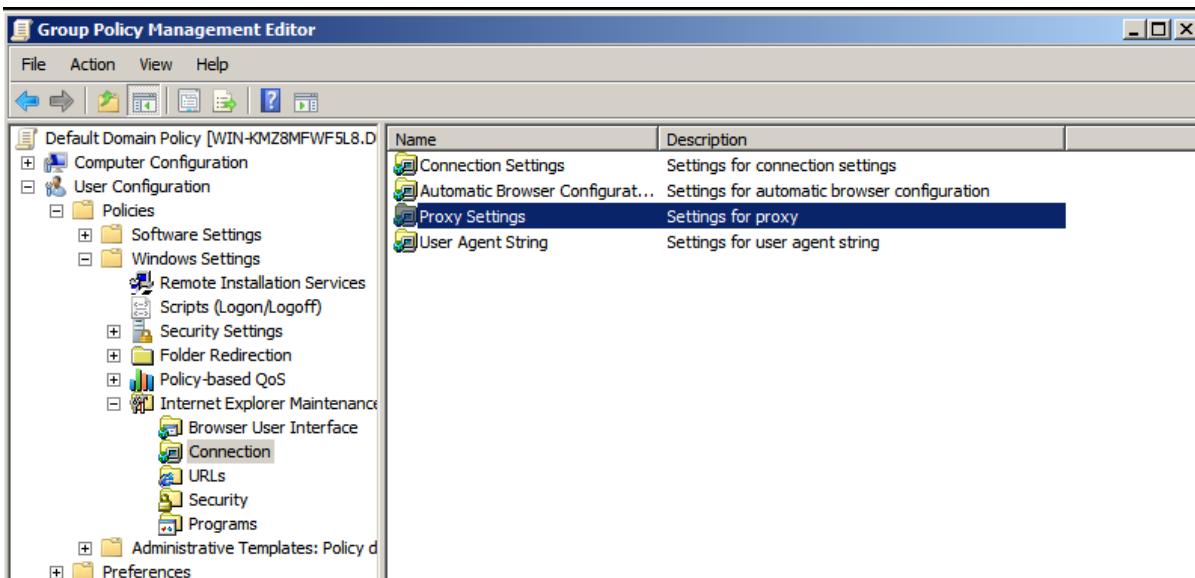


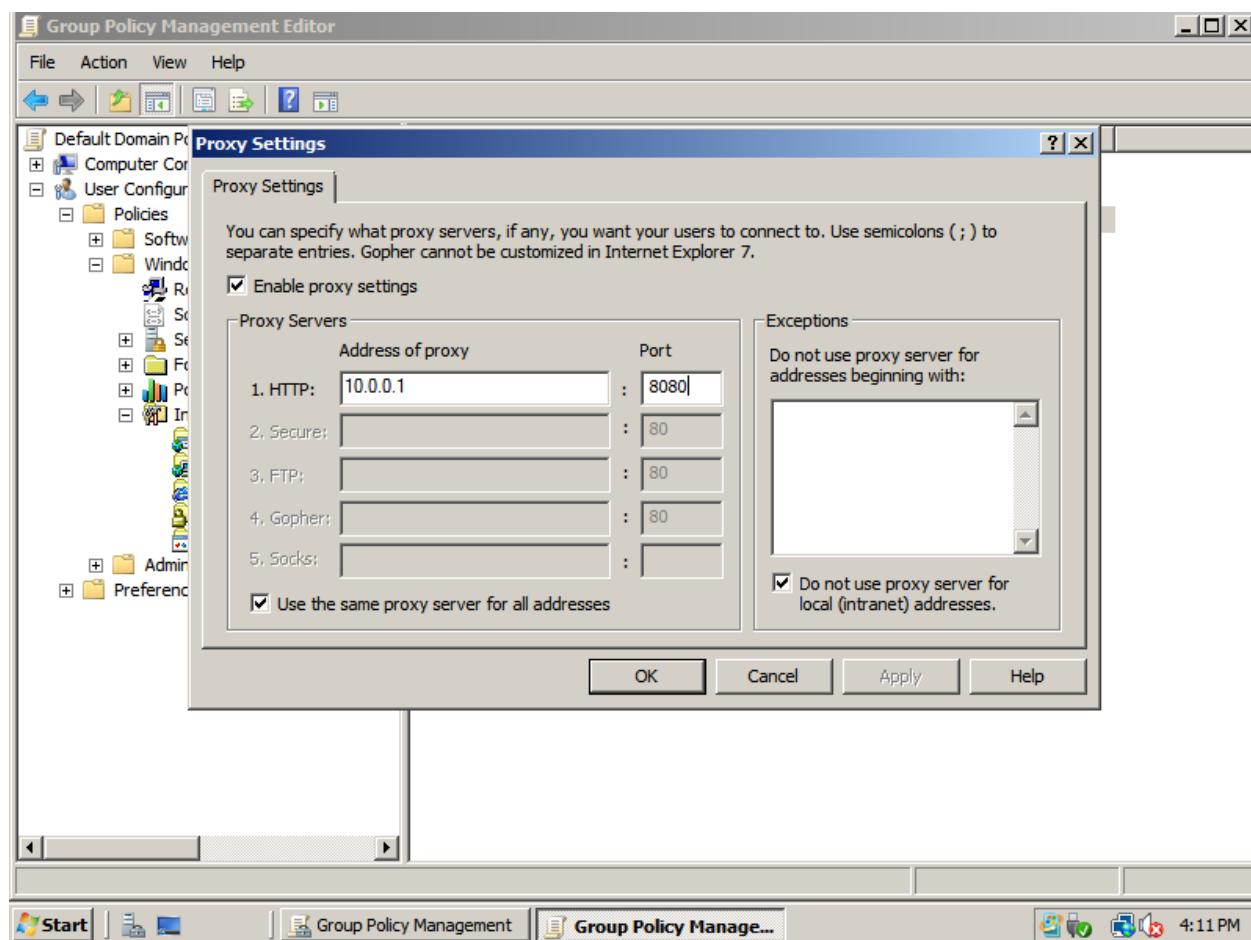




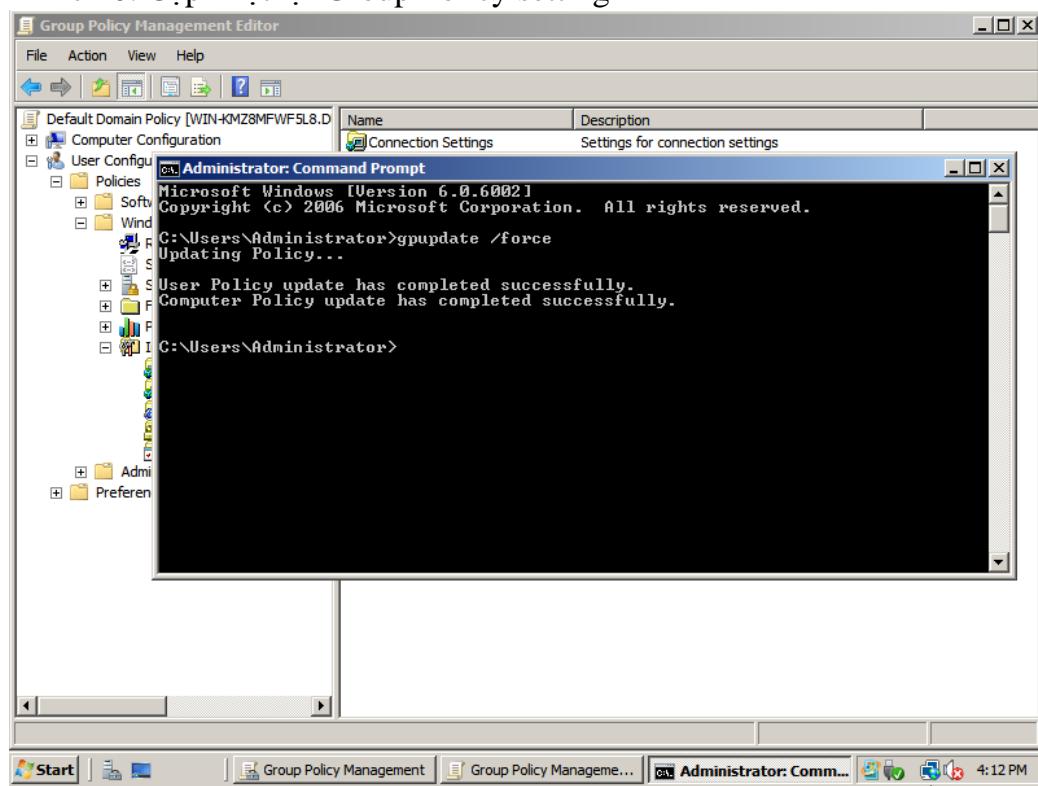


Bước 9: Thiết lập Proxy Server cho domain. Tại Domain Controller: Vào User Configuration > Windows Settings > Internet Explorer Maintenance > Connection





### Bước 10: Cập nhật lại Group Policy setting



Bước 11: Tại WebAdmin của Firewall Sophos UTM, chọn Authentication Services > chọn Tab Global Settings.

Chọn Create users automatically và End-User Portal và Apply như sau

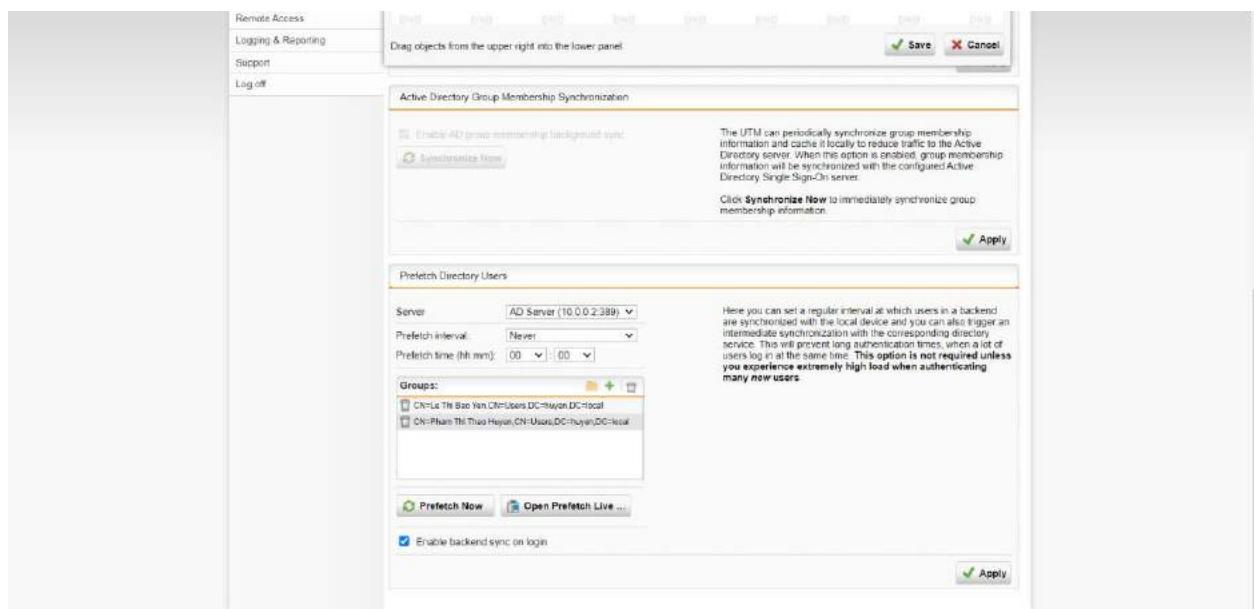
The screenshot shows the Sophos UTM WebAdmin interface. On the left, there's a sidebar with various service definitions and management options. The main area is titled 'Global Settings' under 'Authentication Services'. It contains several tabs: 'Global Settings' (selected), 'Servers', 'Single Sign-On', 'One-time Pa...', and 'Advanced'. Under 'Global Settings', there are two main sections: 'Automatic User Creation' and 'Automatic User Creation for Facilities'. In 'Automatic User Creation', the checkbox for 'Create users automatically' is checked. A note explains that this will automatically create user objects whenever an unknown user successfully authenticates to a backend mechanism. There is an 'Apply' button. In 'Automatic User Creation for Facilities', the checkbox for 'End-User Portal' is checked. A note says you can specify which facilities will automatically create user objects whenever an unknown user successfully authenticates to a backend mechanism. There is also an 'Apply' button. Below these sections, a message says 'Settings saved successfully'. Further down, there are sections for 'Authentication Cache' (with a 'Flush Authentication Cache' button) and 'Live Log' (with an 'Open Live Log' button). Each of these sections also has an 'Apply' button.

Bước 12: Chọn Authentication Services > chọn Tab Advanced. Tại phần Prefetch Directory Users > chọn icon thư mục.

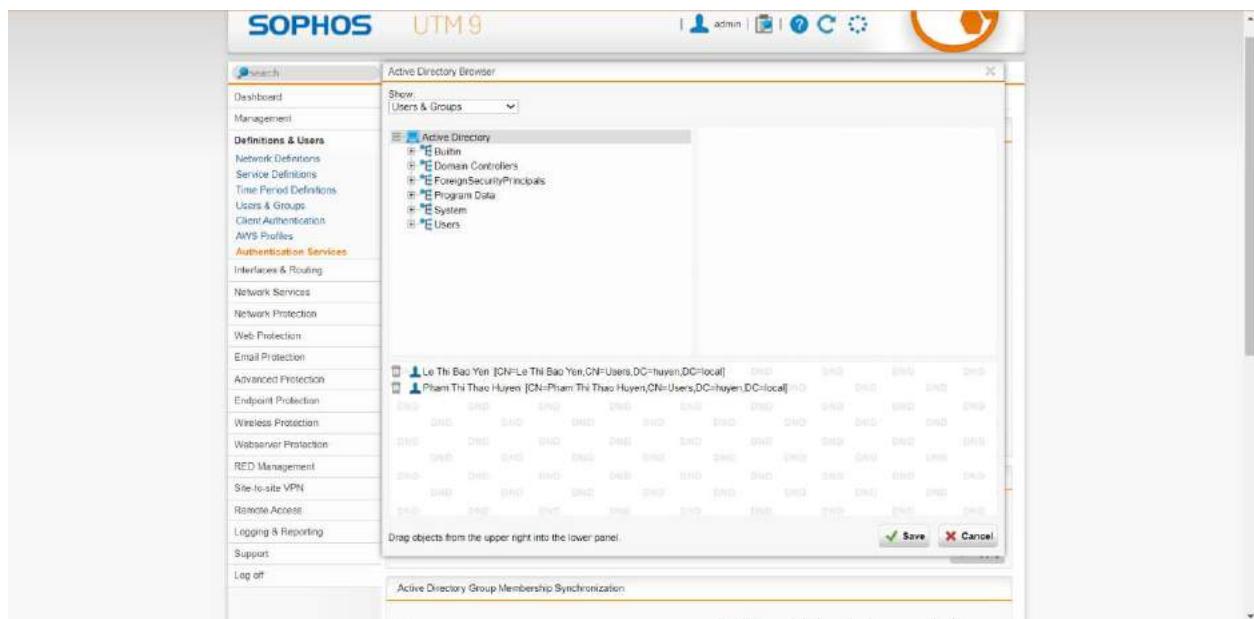
Tiếp theo chọn Users và kéo 2 user đã tạo ở bước 9 vào phần DND bên dưới.

Chọn Save để lưu lại.

Bước 13: Chọn Enable backend sync on login và nhấn Apply để áp dụng.



Kiểm tra lại tại Definitions & Users > Users & Groups

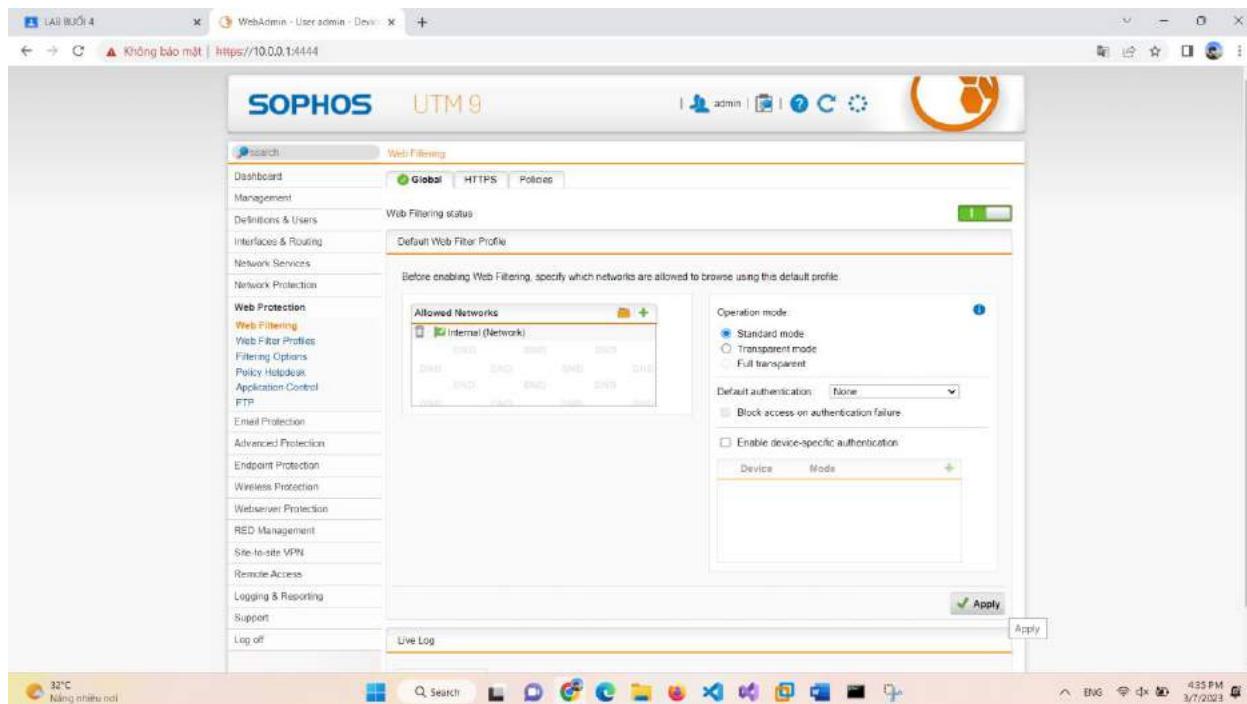


## 2. Thiết lập một số kịch bản quy định về chính sách với tài khoản tại Domain

a) Kịch bản 1: Quản trị muốn cấm tài khoản nhân viên Nguyễn Thanh Tùng truy cập các trang web tìm kiếm việc làm (Job Search) khi sử dụng tài khoản được cấp trong domain.

Bước 1: Tại WebAdmin Firewall Sophos UTM, vào Web Protection > chọn Web

Filtering và bật bộ lọc này. Chọn Standard mode và nhấn Apply.



Bước 2: Để tạo quy tắc lọc web mới, vào Web Protection > Web Filter Profiles > Chọn New Filter Action...

The screenshot shows the Sophos UTM 9 interface under the 'Web Protection' section. On the left, a sidebar lists various protection categories. In the center, the 'Web Filter Profiles' section is active, displaying two filter actions:

- Default content filter action**: Mode: Blacklist; Action: Uncategorized sites are allowed.
- Default content filter block action**: Mode: Whitelist; Action: Uncategorized sites are blocked.

### Bước 3: Thiết lập chính sách cấm truy cập các website tìm việc (Job Search)

The screenshot shows the 'Add Filter Action' dialog box. The 'Categories' tab is selected. The 'Name' field contains 'Block job search for huyen'. Under 'Action', the 'Block all content, except as specified below' option is selected. The 'Category' section lists various website types, and the 'Action' column shows 'Allow' for most categories except 'Job Search', which is set to 'Block'. At the bottom, there is a checkbox for 'Block websites with a reputation below a threshold of'.

Category	Action
Community / Education / Religion	Allow
Criminal Activities	Allow
Drugs	Allow
Entertainment / Culture	Allow
Extremistic Sites	Allow
Finance / Investing	Allow
Games / Gambles	Allow
IT	Allow
Information and Communication	Allow
Job Search	Block
Lifestyle	Allow
Locomotion	Allow
Medicine	Allow
Nudity	Allow
Ordering	Allow
Private Homepages	Allow
Suspicious	Allow
Weapons	Allow
Uncategorized websites	Allow

Chọn

Save

để

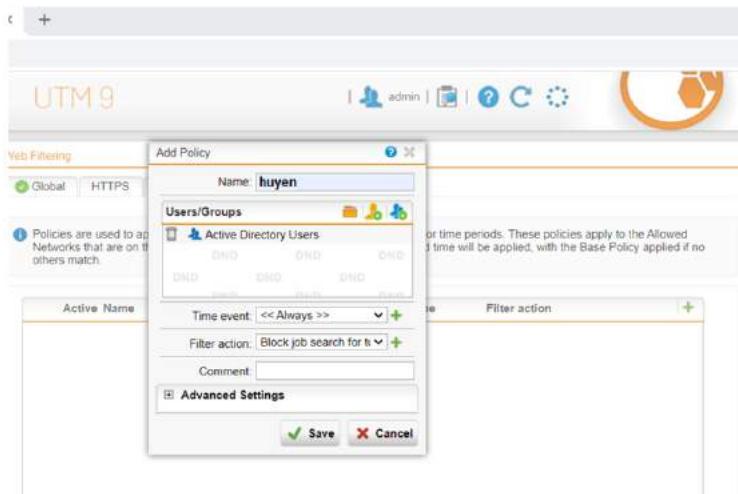
lưu

lại.

The screenshot shows the Sophos UTM 9 interface with the 'Web Protection' section selected. Under 'Web Filter Profiles', there are three entries listed:

- Block job search for huynh** (Mode: Blacklist)
  - Blocked Categories: JobSearch
  - Uncategorized sites are: allowed
  - Spyware is: blocked
  - Antivirus scanning: deactivated
- Default content filter action** (Mode: Blacklist)
  - Uncategorized sites are: allowed
  - Spyware is: blocked
  - Blocked file extensions: exe, msi, com, bat, vbs, hta, int, jar, wsf, vba, vbe, ink, chm, pdf, reg, scr, cmd
  - Antivirus scanning: Single Scan
  - PUA detection: deactivated
- Default content filter block action** (Mode: Whitelist)
  - Uncategorized sites are: blocked
  - Antivirus scanning: deactivated

Bước 4: Vào Web Protection > chọn Web Filtering > Tại Tab Policies: Tạo 1 Policy mới và áp dụng cho user Huyen

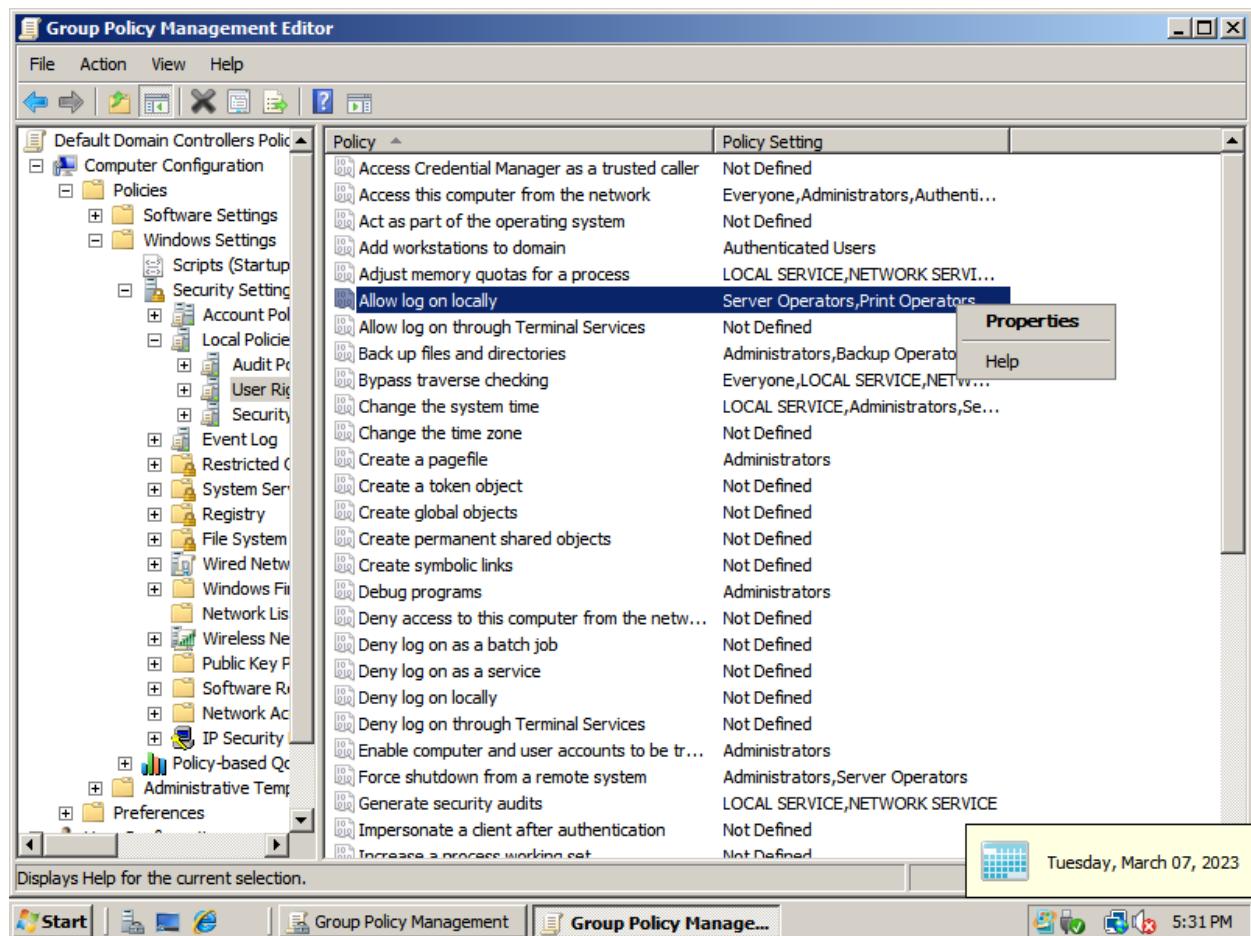


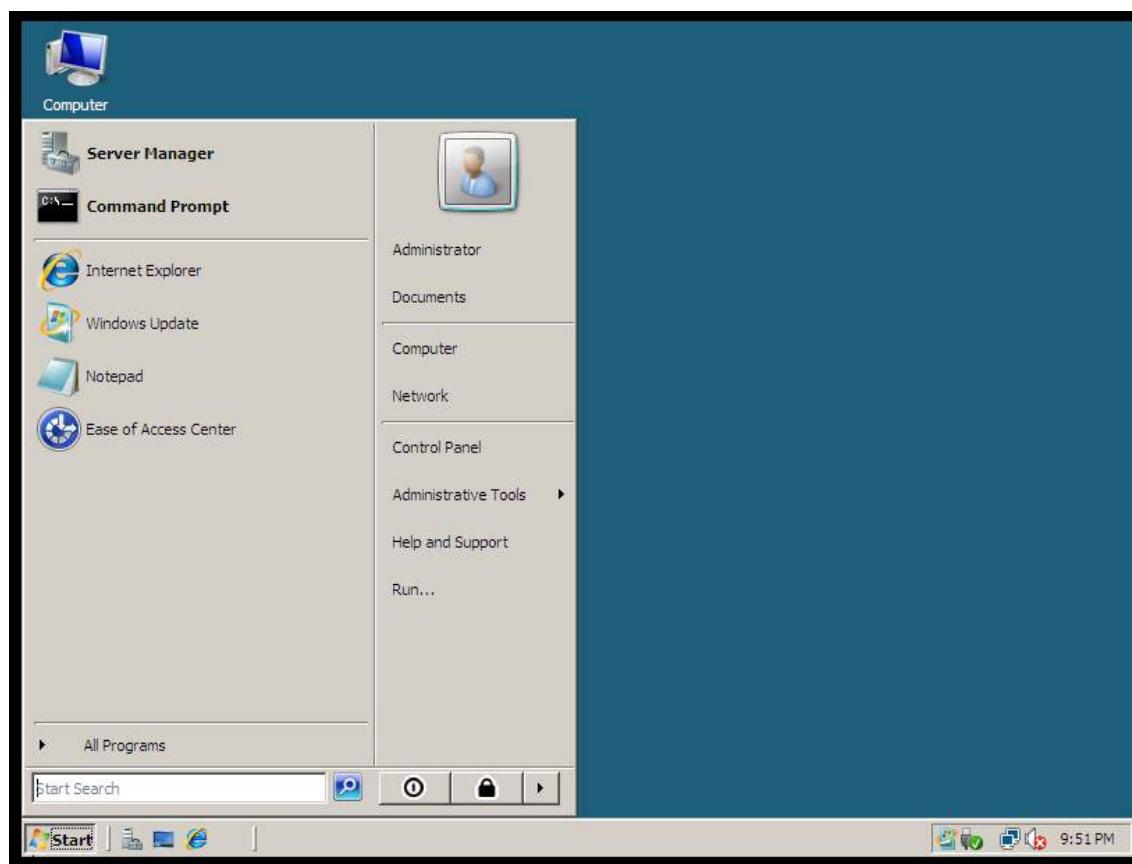
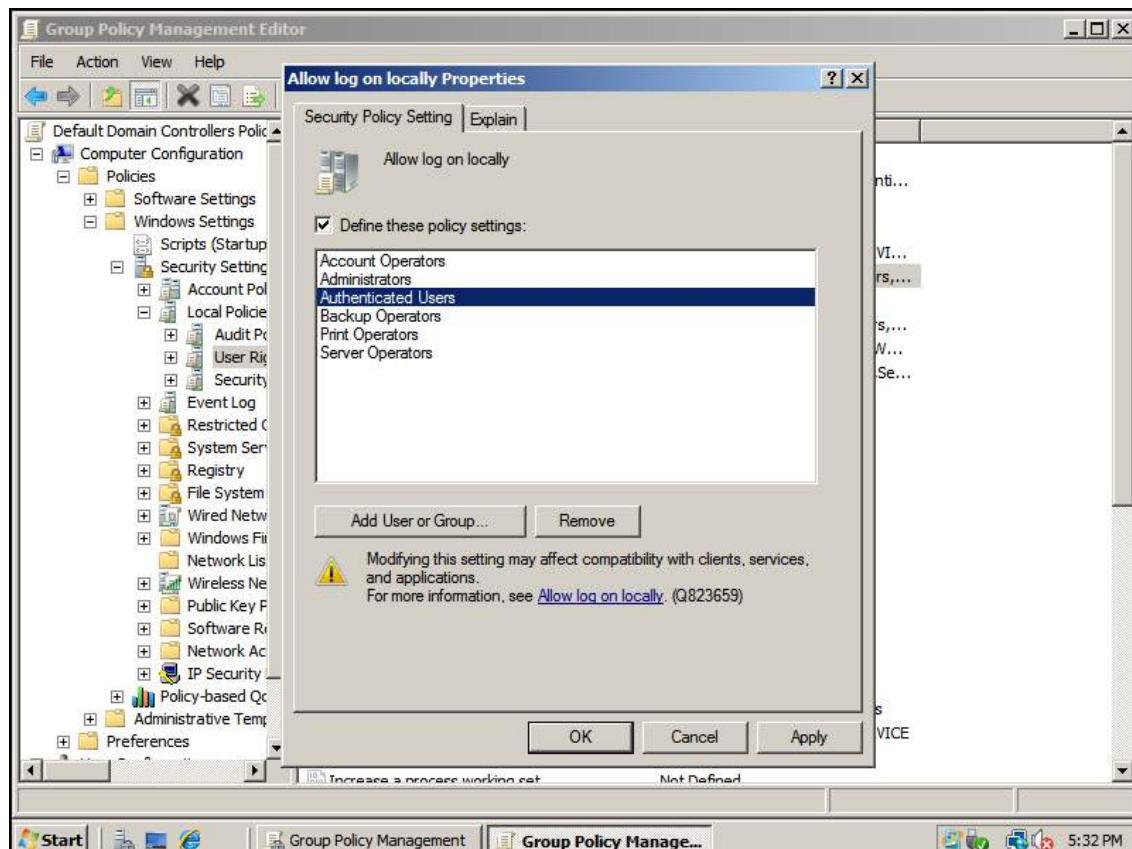
Bước 5: Tại máy Domain Controller, đăng nhập vào user a để kiểm tra (không đăng nhập được do chưa cấp quyền)



Lưu ý: Nếu không thể đăng nhập khi đã cung cấp đúng mật khẩu thì do máy Domain Controller chưa cấp quyền cho user chúng thực đăng nhập vào, ta thay đổi lại chính sách này trong Group Policy Management như sau.

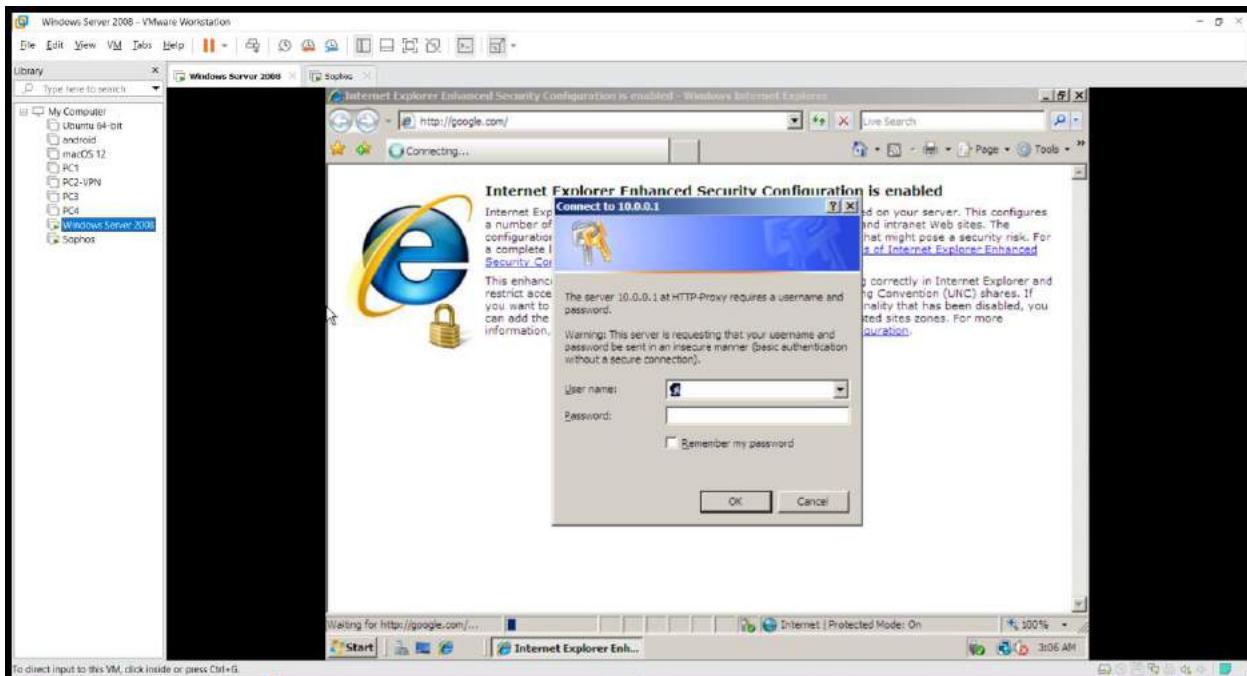
Tại Group Policy Management > chỉnh sửa Default Domain Controller Policy và vào Computer Configuration > Windows Settings > Local Policies > User Rights Assignment > Thay đổi chính sách Allow log on locally





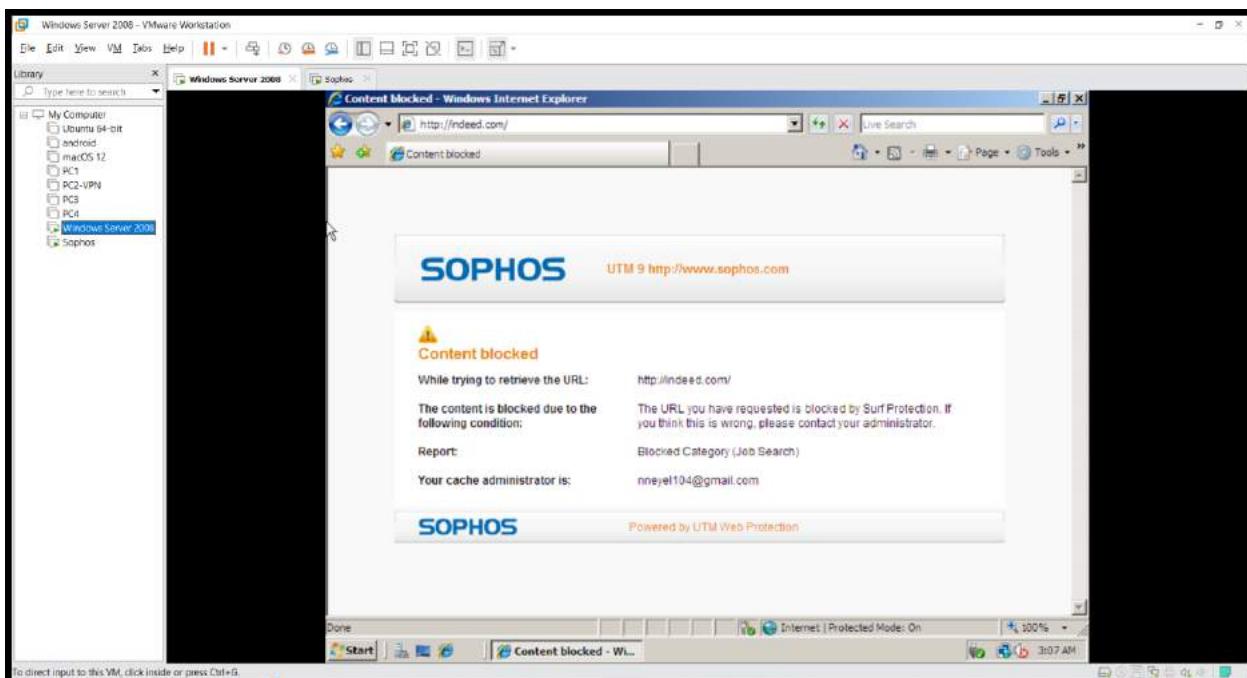
Sau đó thực hiện lệnh gpupdate /force để cập nhật lại chính sách.

Bước 6: Sau khi đã đăng nhập thành công vào user a, mở trình duyệt để kiểm tra kết quả.  
Khi truy cập Internet, trình duyệt sẽ yêu cầu nhập username và password ở lần đầu tiên:



Bước 7: Thử truy cập một số website thông thường

Bước 8: Tìm kiếm một vài website thuộc thể loại đã cấm ở bước 3 và thử truy cập



# LAB 05: TƯỜNG LỬA SOPHOS UTM: XÂY DỰNG CHÍNH SÁCH WEB

## A. Tổng quan

Sử dụng mô hình mạng đã xây dựng từ Lab 03.

- Mạng nội bộ: 10.0.0.0/8 với 1 Domain Controller để quản lý tập trung các máy tính theo domain.
- Vùng DMZ: 172.16.0.0/16 bao gồm các Server Web, Mail, FTP.

Thực chất trong mô hình trên, sinh viên chỉ cần chuẩn bị 2 máy tính. Trong đó:

- Máy 1: Windows Server 2008 làm Domain Server (1 card mạng Host-only)
- Máy 2: Firewall Sophos UTM 9.6

## B. Thực hành

### 1. Tổng quan về xây dựng chính sách bảo vệ truy cập web

Action	User Name	Description
<input type="checkbox"/> Edit	admin	Locally authenticated Default Super-Admin user
<input type="checkbox"/> Delete		
<input type="checkbox"/> Edit	huyen	Remotely authenticated [User data updated from backend automatically] sync'd from adirectory
<input type="checkbox"/> Delete		
<input type="checkbox"/> Edit	yenn	Remotely authenticated [User data updated from backend automatically] sync'd from adirectory
<input type="checkbox"/> Delete		

## 1.1. Xây dựng bộ lọc tại Web Filter Profile > Tab Filter Actions > New Filter Action...

## 1.2. Tạo và áp dụng chính sách tại Web Filter Profiles > Filter Profiles

The screenshot shows the Sophos UTM 9 interface under the 'Web Protection' section. The 'Filter Actions' tab is selected. Three filter actions are listed:

- Block Job search for Yen**: Mode: Blacklist, Blocked Categories: jobsearch, Uncategorized sites are: allowed, Spyware is: blocked, Antivirus scanning: deactivated.
- Default content filter action** [This is the default content filter action profile]: Mode: Blacklist, Uncategorized sites are: allowed, Spyware is: blocked, Blocked file extensions: exe, msi, com, bat, vbs, msi, pdf, wmv, vbe, ink, doc, pif, reg, scr, cpl, Antivirus scanning: single scan, PUA detection: deactivated.
- Default content filter block action** [This is the default content filter block action profile]: Mode: Whitelist, Uncategorized sites are: blocked, Antivirus scanning: deactivated.

The screenshot shows a Windows Server 2008 desktop environment. A 'Windows Internet Explorer' window is open, displaying a 'Content blocked' message. The message states:

**SOPHOS** UTM 9 http://www.sophos.com

**Content blocked**

While trying to retrieve the URL: http://indeed.com/

The content is blocked due to the following condition:

Report: Blocked Category (Job Search)

Your cache administrator is: nneyel104@gmail.com

**SOPHOS** Powered by UTM Web Protection

The taskbar shows the URL as 'Content blocked - Wi...'. The status bar at the bottom right indicates 'Protected Mode: On'.

## 2. Xây dựng bộ chính sách bảo vệ truy cập Web

2.1 Chỉ cho phép toàn bộ người dùng sử dụng Internet để truy cập web, sử dụng email qua các giao thức SMTP, IMAP, POP3, chặn tất cả các dịch vụ khác.

The screenshot shows the Sophos UTM 9 Firewall Rules configuration. It displays three rules:

- Rule 1:** Any → Any (Actions: DNS, HTTP, HTTPS)
- Rule 2:** Any → Any (Actions: DNS, HTTP, HTTPS, IMAP, POP3, SMTP)
- Rule 3:** Any → Any (Actions: DNS, HTTP, HTTPS, IMAP, POP3, SMTP, SMTP-SSL)

2.2 Chặn truy cập tất cả website từ Trung Quốc và toàn bộ khu vực Trung Đông (Iran, Iraq, Syria, ...).

The screenshot shows the Sophos WebAdmin interface under the 'Country Blocking' section. It lists countries categorized by continent:

- Europe:** Finland, France, Germany, Gibraltar, Luxembourg, Macedonia, Malta, Moldavia, Norway, Poland, Portugal, Romania, Russia, San Marino, Sweden, Switzerland, Ukraine.
- Middle East:** Bahrain, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine Territory (Occ.), Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen.
- Africa:** Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Congo, Democratic Rep., Djibouti, Equatorial Guinea, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Guinea, Ivory Coast, Kenya, Liberia, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Namibia, Niger, Nigeria, Rwanda, Saint Helena, Saint Tome and Principe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, Sudan, Swaziland, Tanzania, Togo, Tunisia, Uganda, Western Sahara, Zambia, Zimbabwe.
- Asia:** Afghanistan, Armenia, Azerbaijan, Bangladesh, Bhutan, British Indian Ocean Terr., Brunei Darussalam, Cambodia, Kingdom of, China, Christmas Island, Cocos Islands, Cyprus, Georgia, Hong Kong, India, Indonesia, Japan, Kazakhstan, Kyrgyz Republic (Kyrgyzstan), Laos, Macau, Malaysia, Mongolia, Myanmar, Nepal, North Korea, Pakistan, Philippines, Singapore, South Korea, Sri Lanka, Tajikistan, Taiwan, Thailand, Timor-Leste, Turkmenistan, Uzbekistan, Vietnam.

2.3 Cấm truy cập tất cả các website tìm kiếm việc làm, trong đó có một số website tìm kiếm việc làm tại TP.HCM.

The screenshot shows the Sophos UTM 9 Web Filter Profiles configuration interface. A modal window titled "Edit Filter Action" is open, showing the configuration for "Lab05-Rules". The "Categories" tab is selected. The "Action" dropdown is set to "Allow all content, except as specified below". The "Block spyware infection and communication" checkbox is checked. The main table lists various categories and their actions:

Category	Action
Community / Education / Religion	Allow
Criminal Activities	Allow
Drugs	Allow
Entertainment / Culture	Allow
Extremistic Sites	Allow
Finance / Investing	Allow
Games / Gambles	Allow
IT	Allow
Information and Communication	Allow
Job Search	Block
Lifestyle	Allow
Locomotion	Allow
Medicine	Allow
Nudity	Allow
Ordering	Allow
Private Homepages	Allow
Suspicious	Allow
Weapons	Allow
vụ kí, ton giao, chính trị	Warn
Uncategorized websites	Allow

At the bottom of the dialog, there is a checkbox for "Block websites with a reputation below a threshold of:" followed by a dropdown menu set to "Unverified". The dialog has buttons for "Back", "Next", "Save", and "Cancel". Below the dialog, a summary table provides information about blocked categories and uncategorized sites:

Blocked Categories	CriminalActivities ExtremisticSites Nudity
Uncategorized sites are	allowed
Spyware is	blocked
Antivirus scanning	deactivated

2.4 Cảnh báo khi truy cập các website về vũ khí, chính trị - tôn giáo. Không cảnh báo với các website giáo dục.

The screenshot shows the Sophos UTM 9 WebAdmin interface. The top navigation bar includes a warning message "Không bảo mật" and the URL "https://10.0.0.1:4444". The main title is "SOPHOS UTM 9". On the left, there's a sidebar with various protection modules: Dashboard, Management, Definitions & Users, Interfaces & Routing, Network Services, Network Protection, Web Protection (selected), Filtering Options (selected), Policy Helpdesk, Application Control, FTP, Email Protection, Advanced Protection, Endpoint Protection, Wireless Protection, Webserver Protection, RED Management, Site-to-site VPN, Remote Access, Logging & Reporting, Support, and Log off. The main content area is titled "Filtering Options" and shows the "Categories" tab selected. It displays five categories with their respective sub-items:

- Ordering**: Auctions/classifieds, Online shopping, Consumer protection
- Private Homepages**: Personal pages, Personal network storage, Residential IP addresses
- Suspicious**: Spyware/adware, Parked domain, Malicious sites, Spam URLs, Web ads, Phishing
- Weapons**: Weapons
- vũ khí, tôn giáo, chính trị**: Criminal activities, Government/military, Major global religions, Politics/opinion, Religion/ideology, Violence, Weapons

At the bottom, it says "Release 9.511-2 © 2000-2023 Sophos Limited. All rights reserved."

The screenshot shows the Sophos UTM 9 web interface. The top navigation bar includes a search bar, filtering options, and tabs for Exceptions, Websites, Bypass Users, PUAs, Categories, HTTPS CAs, and Misc. A search bar shows the term "game". The main content area displays a list of filter categories:

- Extremistic Sites**:
  - Violence
  - Gruesome content
  - Extreme
  - Game/cartoon violence
- Games / Gambles**:
  - For kids
  - Games
  - Gambling
  - Gambling related
- Giai trí, game**:
  - Chat
  - Entertainment
  - Gambling
  - Gambling related
  - Game/cartoon violence
  - Games
- streaming**:
  - Streaming media

The left sidebar lists various protection profiles: Dashboard, Management, Definitions & Users, Interfaces & Routing, Network Services, Network Protection, Web Protection, Web Filtering, Web Filter Profiles, Filtering Options, Policy Helpdesk, Application Control, FTP, Email Protection, Advanced Protection, Endpoint Protection, Wireless Protection, Webserver Protection, and RED Management.

2.5 Giới hạn truy cập các website Giải trí và Game trong tối đa 60 phút, riêng đối với các website giải trí dạng chia sẻ video như Youtube.com, vimeo.com (Streaming Media) thì chỉ cảnh báo khi truy cập.

Cấm hẳn truy cập website lienminh.garena.vn

The screenshot shows the Sophos UTM 9 interface under the 'Web Filter Profiles' section. A 'Filter Action' is being edited, specifically for 'Websites'. In the 'Block These Websites' list, the URL 'LMHT' is listed with a red 'X' icon. The 'Allow These Websites' list is empty. Below the lists, there's a 'Tags' section with a grid of 'DND' (Do Not Disturb) status for various categories. At the bottom right, there are buttons for 'Back', 'Next', 'Save', and 'Cancel'.

## 2.6 Quét virus khi download tập tin.

The screenshot shows the Sophos UTM 9 web filter profiles configuration. On the left, there's a sidebar with various protection categories like Network Services, Web Protection, and Email Protection. The main area displays the 'Edit Filter Action' dialog for 'Antivirus' settings. Under the 'Antivirus' tab, several options are configured:

- Use antivirus scanning
- Single scan (maximum performance)
- Dual scan (maximum security)
- Refer suspicious items to Sophos Sandstorm
- Block potentially unwanted applications (PUAs)

A note specifies "Do not scan files larger than: 100 Megabytes". Below this, under "Active content removal", there are two unchecked options: "Disable JavaScript" and "Remove embedded objects (ActiveX/Java/Flash)". At the bottom right of the dialog are buttons for "Back", "Next", "Save" (with a checkmark), and "Cancel". A "Blacklist" section lists categories: CriminalActivities, ExtremisticSites, and Nudity. A note states: "Uncategorized sites are allowed", "Spyware is blocked", and "Antivirus scanning deactivated".

## 2.7 Không cho download các file lớn hơn 100MB.

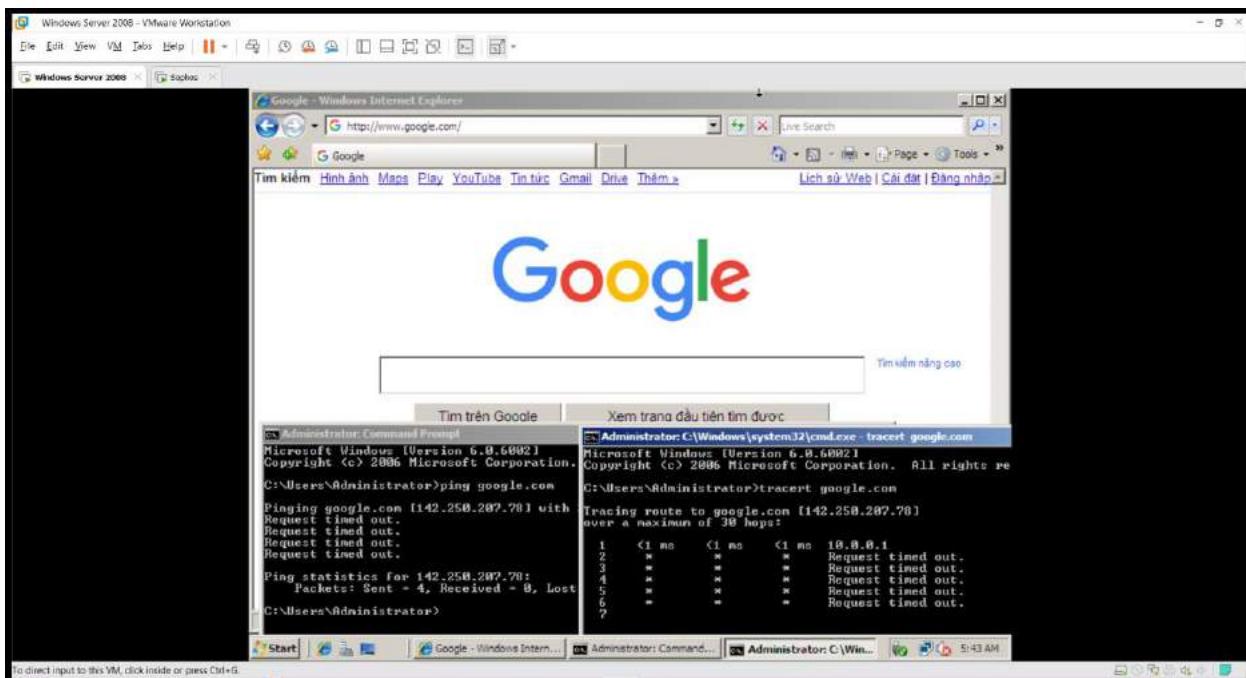
The screenshot shows the Sophos UTM 9 interface for configuring Web Filter Profiles. The left sidebar lists various protection categories. The 'Web Protection' section is expanded, showing 'Web Filtering' and 'Web Filter Profiles'. The 'Web Filter Profiles' page is displayed, with the 'Downloads' tab selected in the top navigation bar. The main area shows sections for 'Warned File Extensions', 'Warned MIME Types', 'Blocked File Extensions', and 'Blocked MIME Types'. A checkbox at the bottom is checked, stating 'Block downloads larger than: 100 Megabytes'. Below this, there are sections for 'Blacklist' and 'Blocked Categories' (listing 'CriminalActivities', 'ExtremisticSites', and 'Nudity'). At the bottom right are 'Back', 'Next', 'Save', and 'Cancel' buttons. The status bar at the bottom indicates 'Release 9.511-2 © 2000-2023 Sophos Limited. All rights reserved.'

2.8 Khi truy cập vào website bị chặn thì có thể mở khóa trực tiếp để bỏ chặn website đó với tài khoản manager / 12345

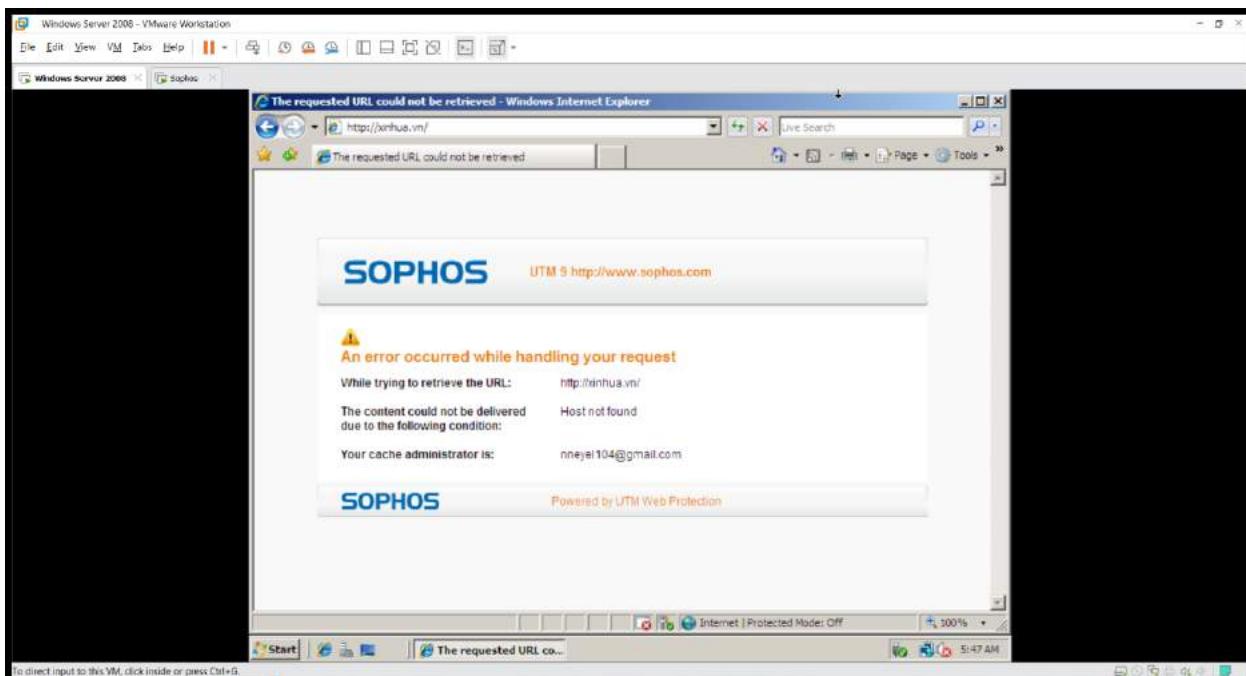
The screenshot shows the Sophos UTM 9 WebAdmin interface. On the left, there's a sidebar with various management options like Dashboard, Management, Definitions & Users, and Network Services. The main area is titled "Bypass Blocking" under "Filtering Options". It asks to specify users allowed to bypass blocking. A modal window titled "Add User" is open, prompting for a Username (manager), Real name (Lalisa), and Email address (nneyle104@gmail.com). It also includes fields for Authentication (Local), Password (\*\*\*\*\*), and Repeat (\*\*\*\*\*). There are checkboxes for "Use static remote access IP" and "Comment". At the bottom of the modal are "Save" and "Cancel" buttons, with "Save" being highlighted.

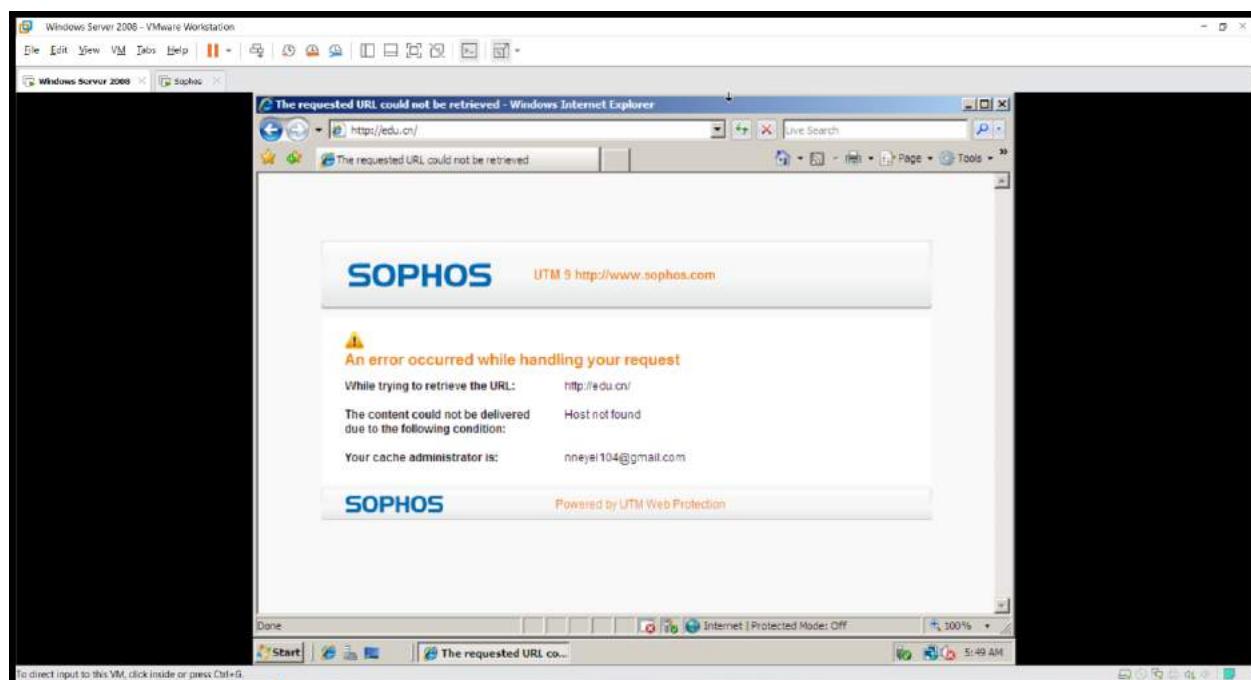
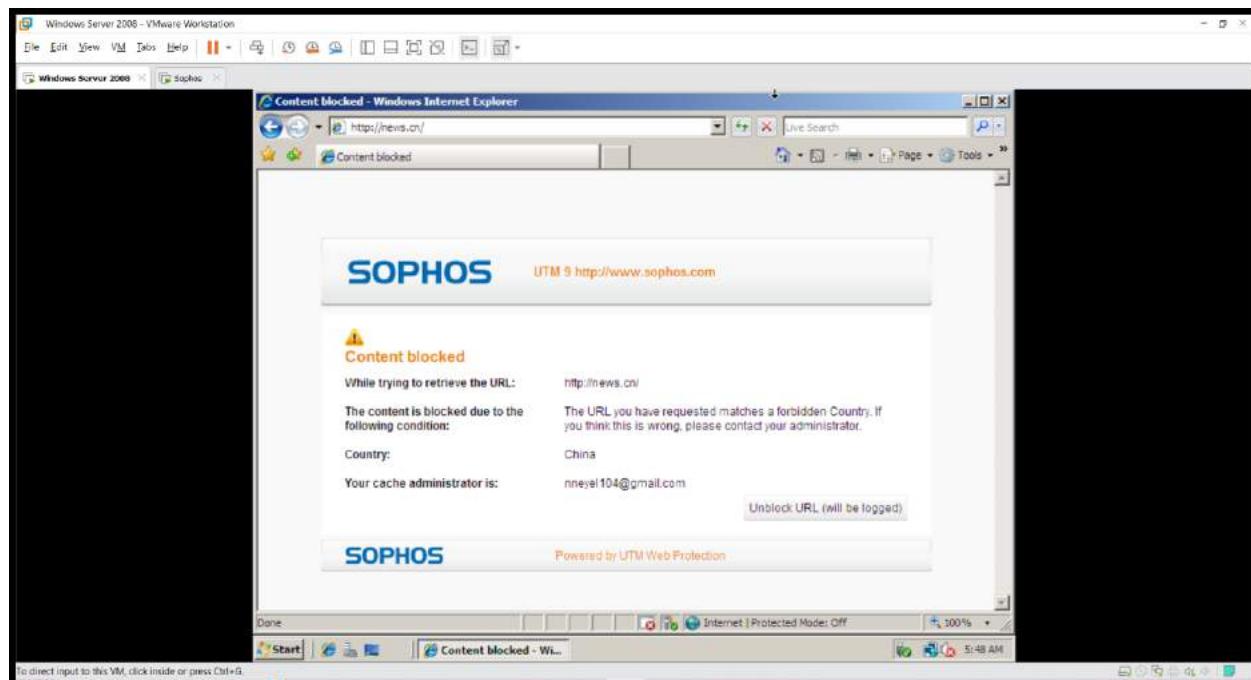
### 3. Kiểm tra kết quả & ứng dụng

3.1 Truy cập 1 website được phép truy cập bình thường, thao tác traceroute và ping đến website đó không thành công.



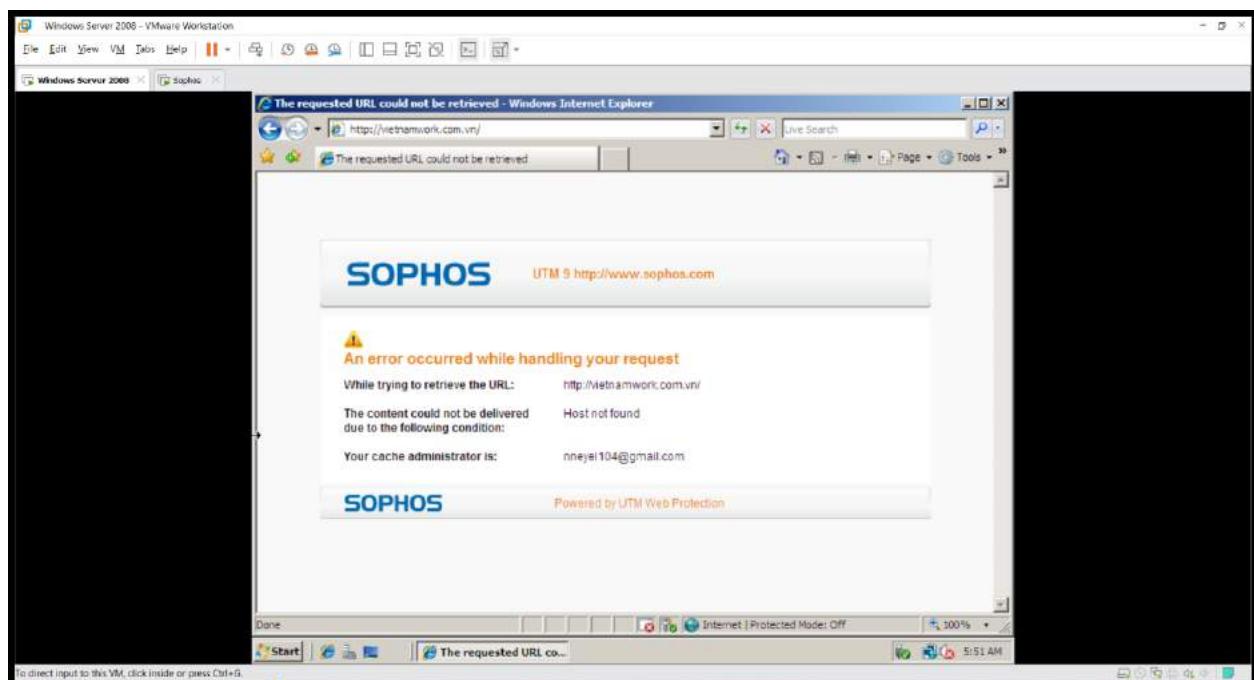
3.2 Không thể truy cập website báo Tân Hoa xã (xinhua.vn – news.cn) và ít nhất 2 website khác từ Trung Quốc và Trung Đông.

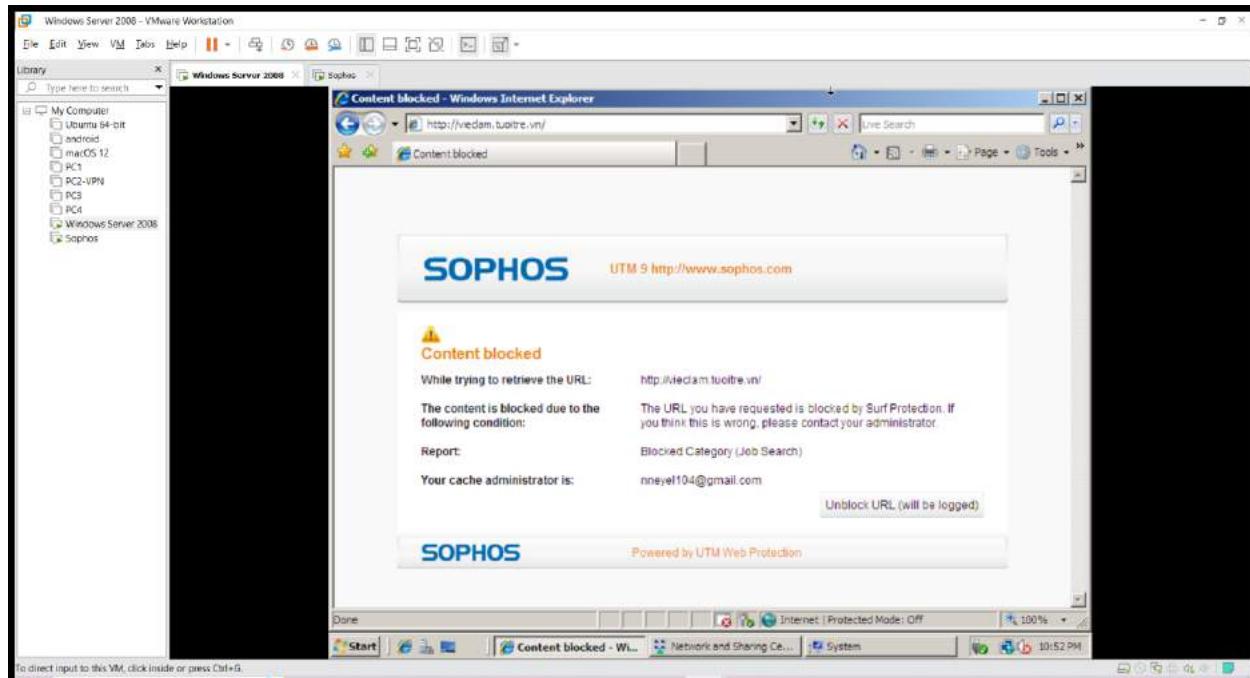
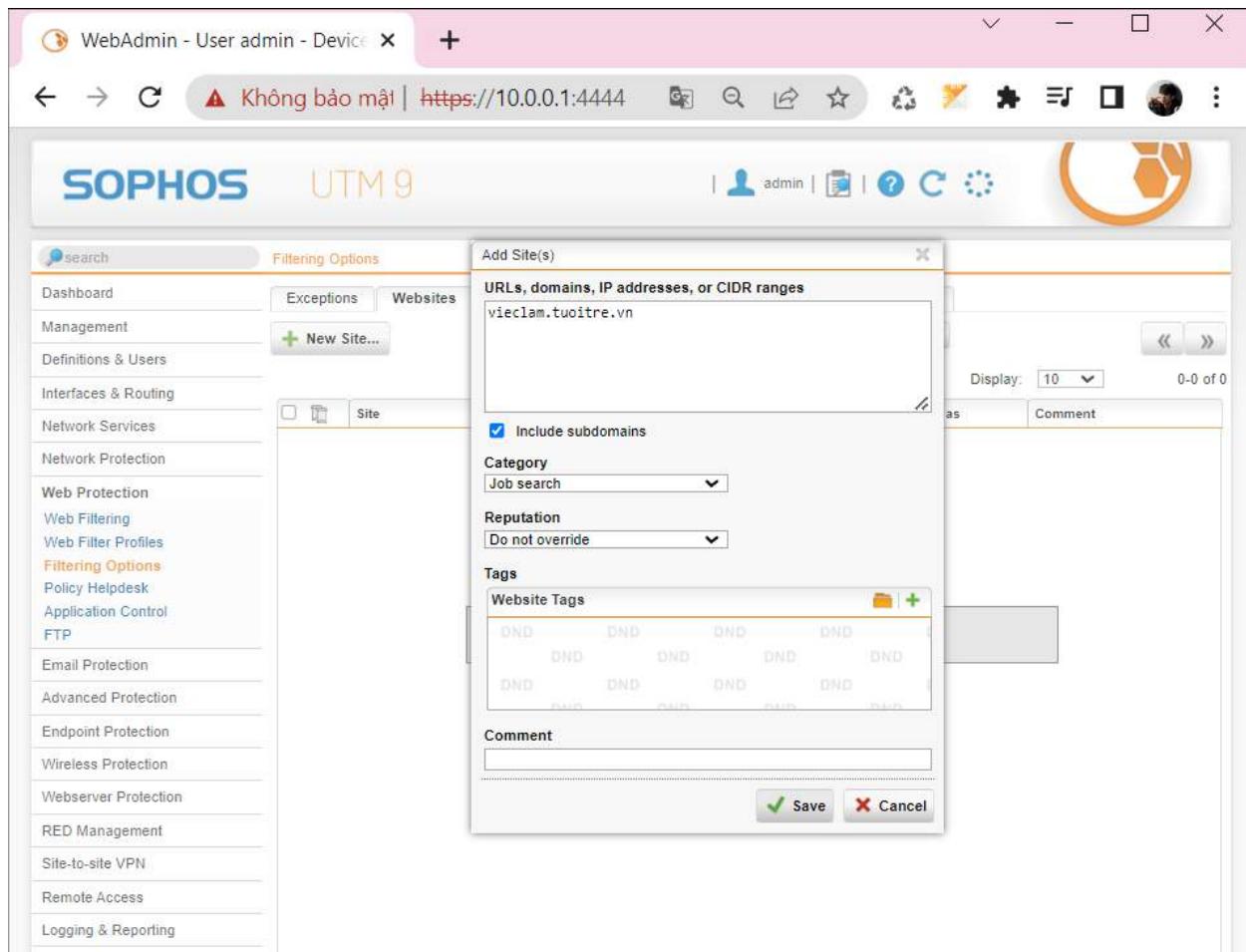


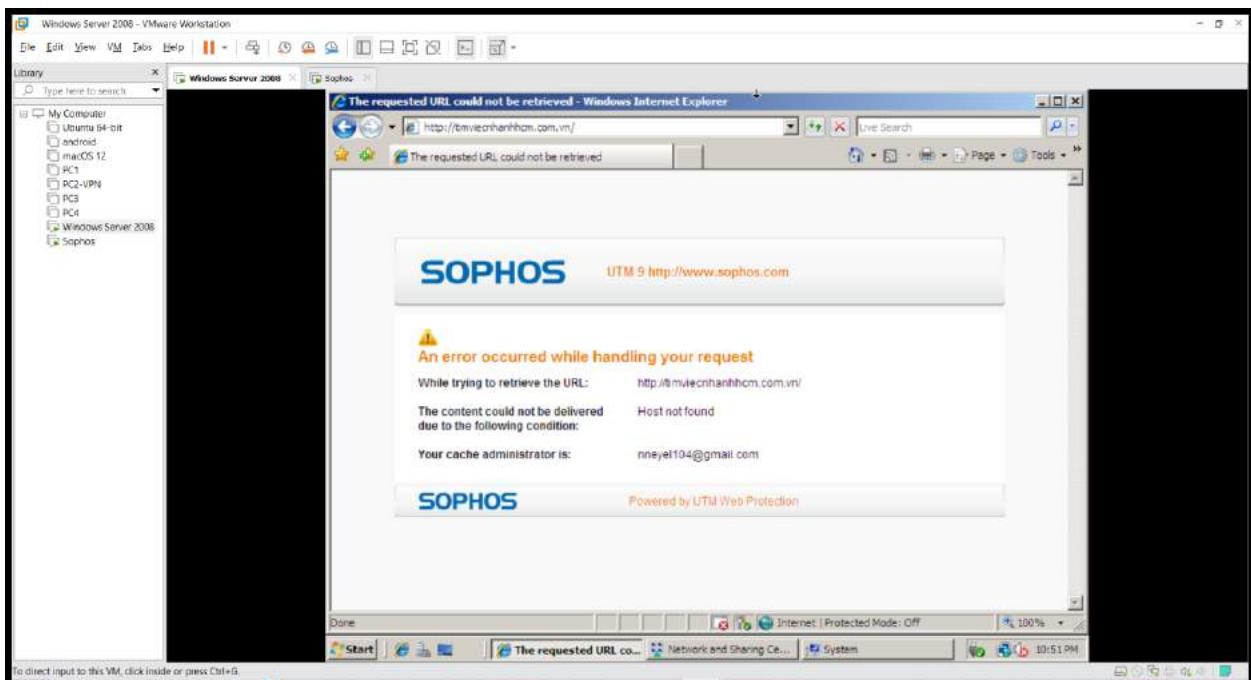




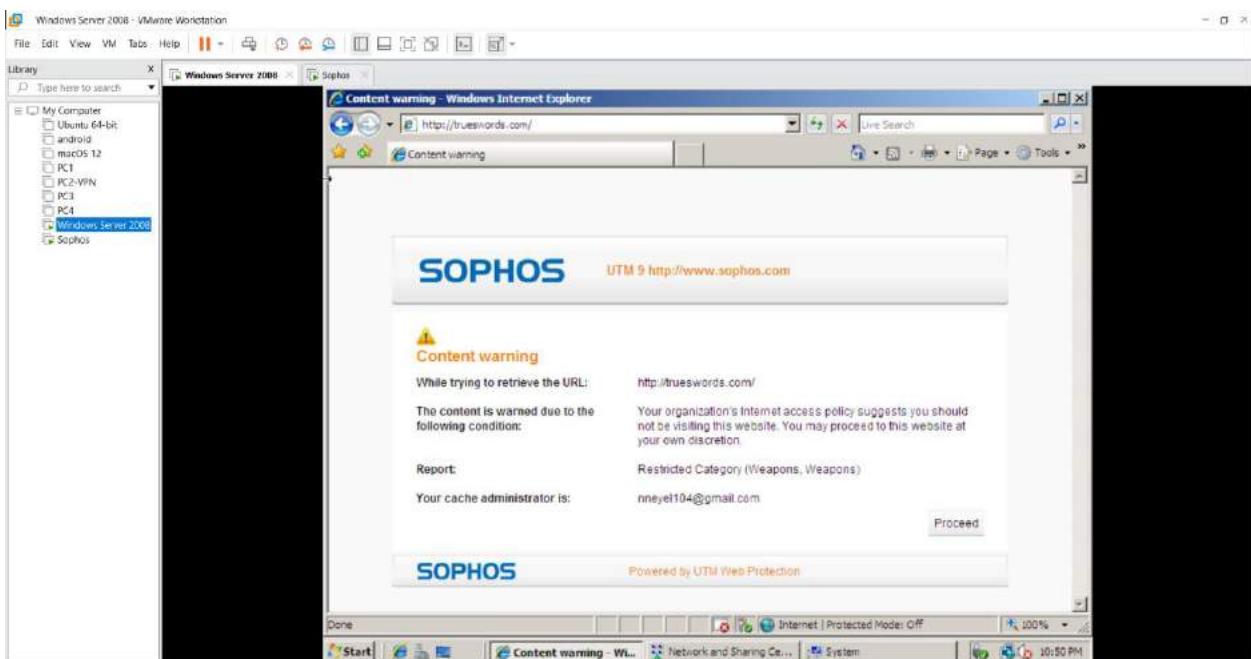
3.3 Không thể vào các website về tìm kiếm việc làm trên thế giới và tại Việt Nam, tại TP.HCM trong đó chặn được 4 website sau: vietnamworks.com.vn, vieclam.tuoitre.vn, timviecnhanhhcm.com, itviec.com.

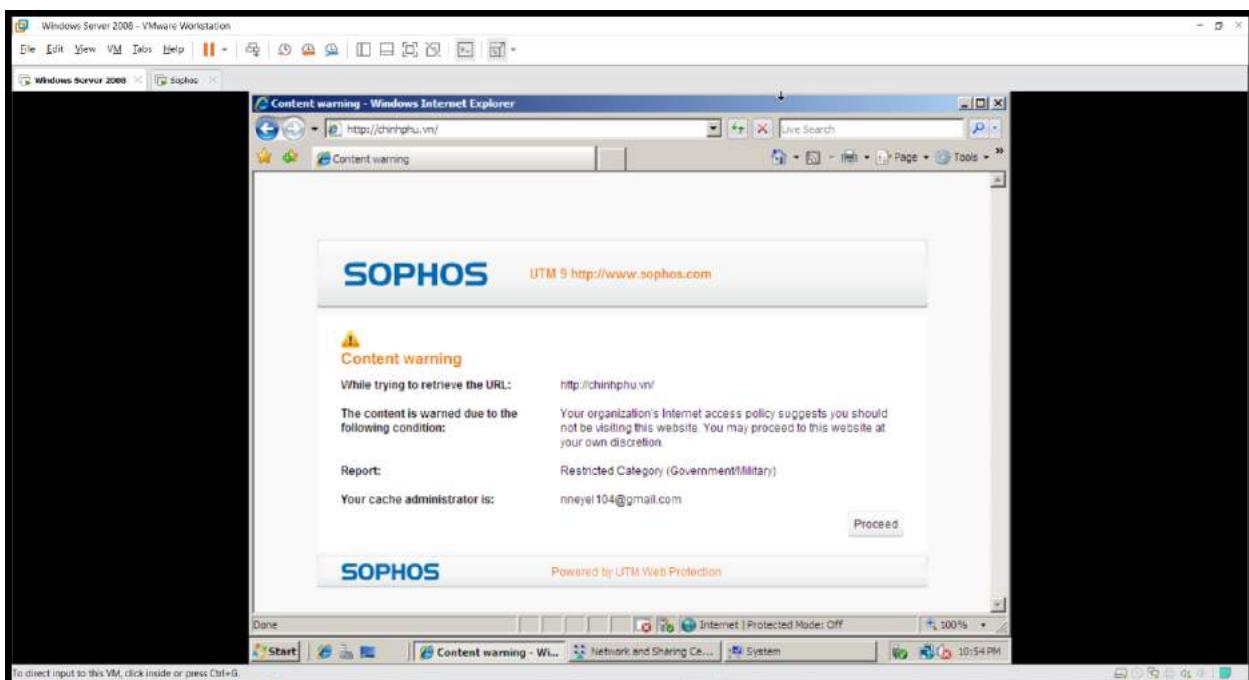
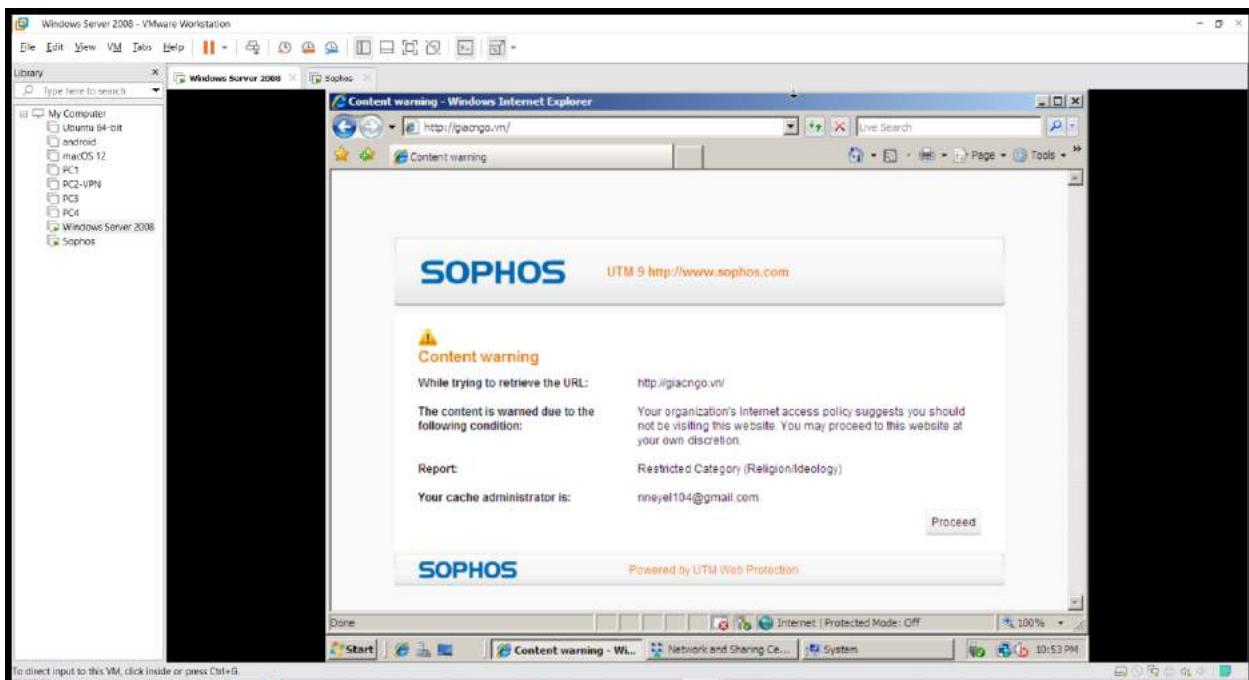






3.4 Hiện cảnh báo đối với một số website thuộc thể loại vũ khí, chính trị - tôn giáo như trueswords.com (vũ khí), giacngo.vn (tôn giáo), chinhphu.vn (chính trị).

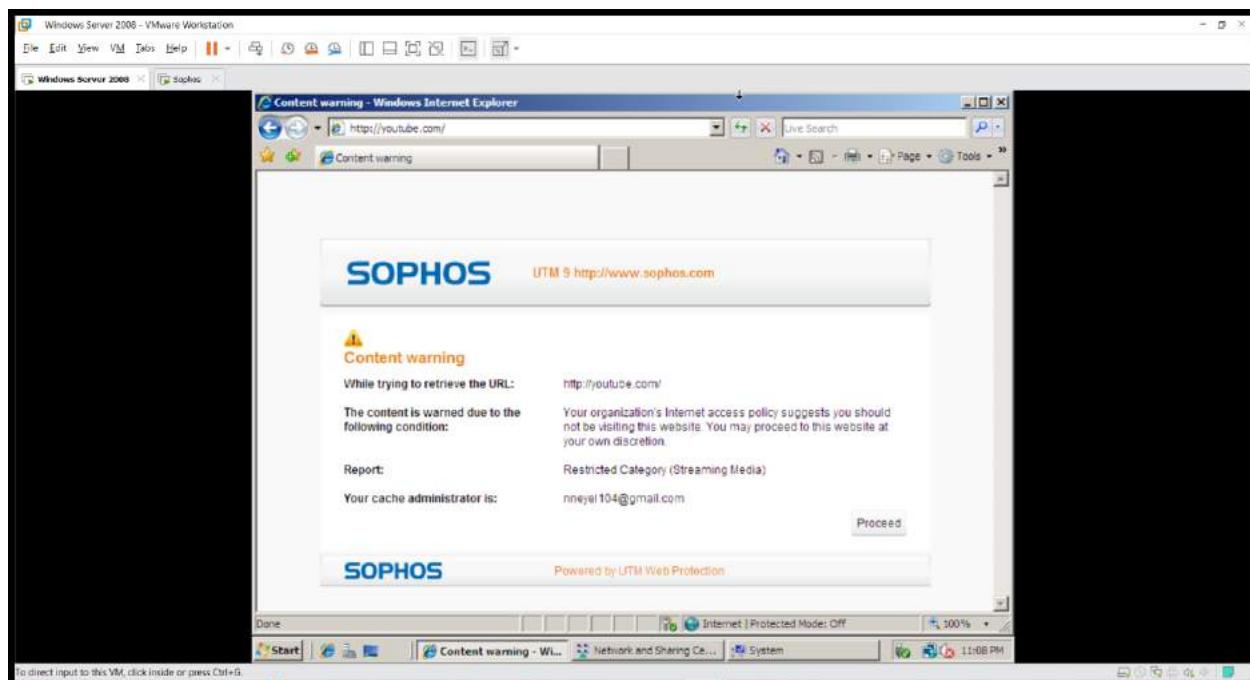




3.5 Kiểm tra khi truy cập một số website giải trí như kenh14.vn, yeah1.com,... và gamevui.vn, pokemongo.com chỉ cho phép truy cập tối đa trong 60 phút

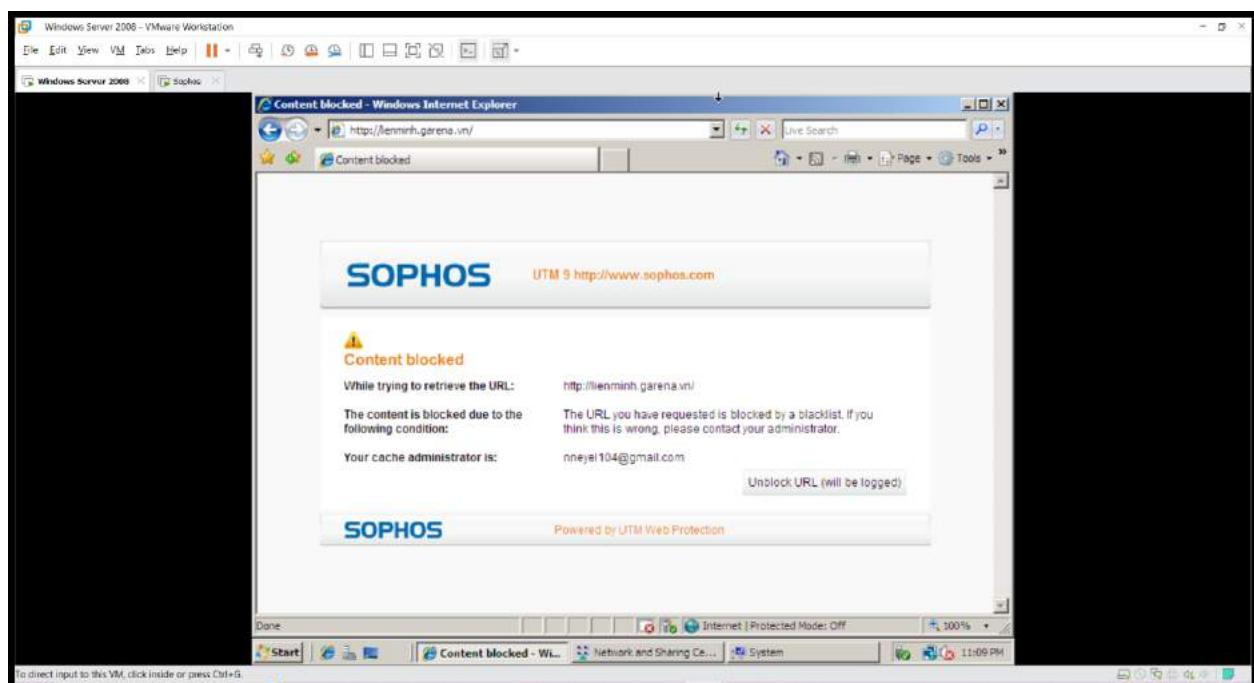


Kiểm tra kết quả khi vào trang Youtube.com và Vimeo.com.

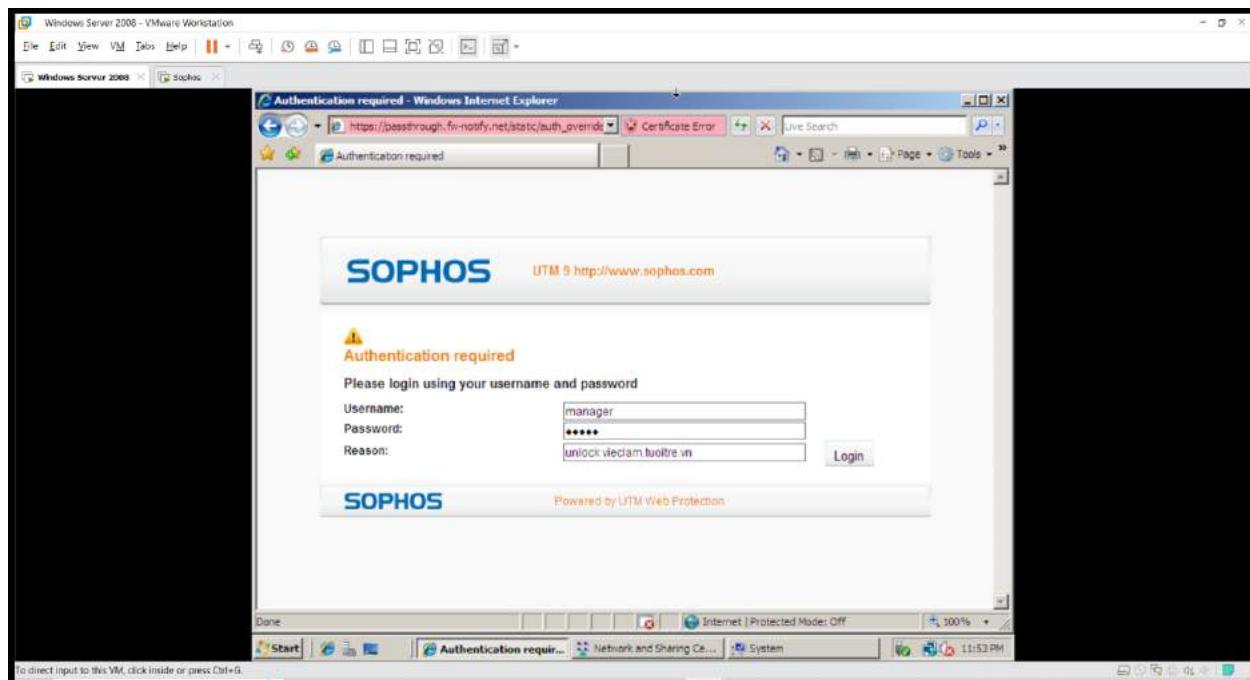


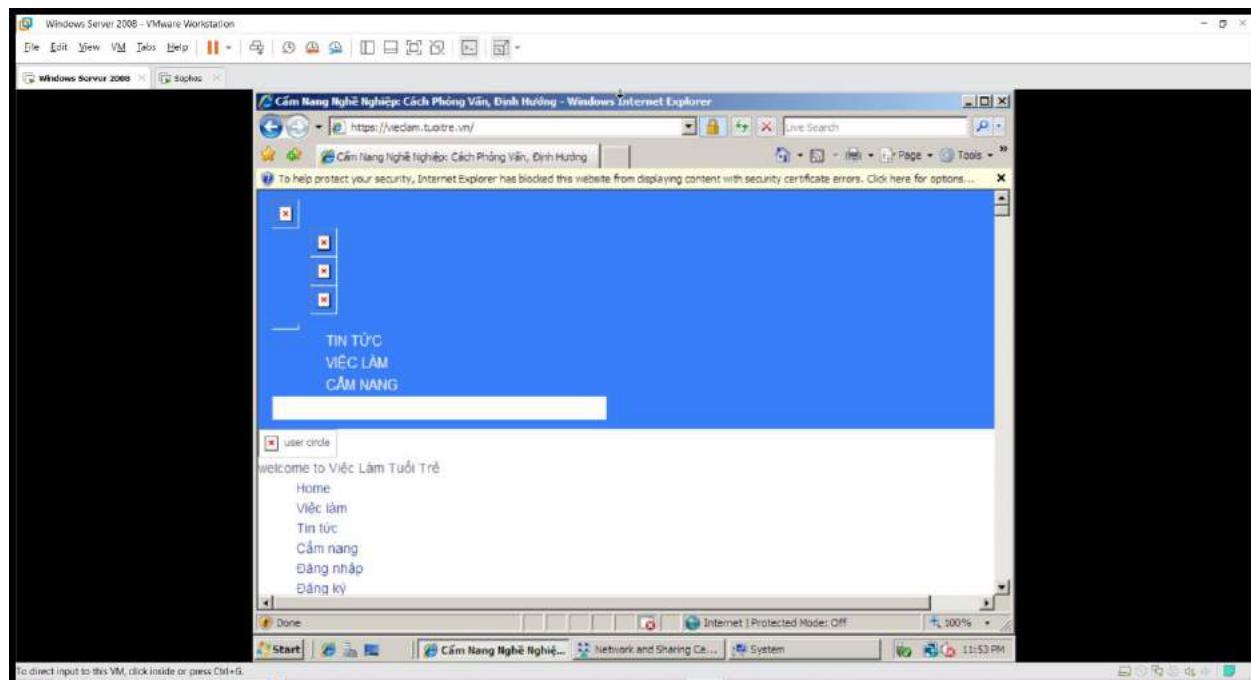


Kiểm tra kết quả khi vào trang lienminh.garena.vn



### 3.8 Với các website bị chặn, khi kiểm tra sẽ xuất hiện tùy chọn Unlock





## LAB 06: TUỜNG LƯẢ SOPHOS UTM: CHÍNH SÁCH ỨNG DỤNG

### A. Tổng quan

Sử dụng mô hình mạng đã xây dựng từ Lab03.

- Mạng nội bộ: 10.0.0.0/8 với 1 Domain Controller để quản lý tập trung các máy tính theo domain.
- Vùng DMZ: 172.16.0.0/16 bao gồm các Server Web, Mail, FTP.

Thực chất trong mô hình trên, sinh viên chỉ cần chuẩn bị 2 máy tính. Trong đó:

- Máy 1: Windows Server 2008 làm Domain Server (1 card mạng Host-only)
- Máy 2: Firewall Sophos UTM 9.6

### B. Thực hành

#### 1. Tổng quan về xây dựng chính sách kiểm soát ứng dụng

Trong Sophos UTM, việc xây dựng các quy tắc kiểm soát các ứng dụng mạng được thực hiện trong Web Protection > Application Control.



Để tiến hành thiết lập các quy tắc, cần bật Network visibility. Tại đây còn cung cấp chức năng Flow Monitor cho phép theo dõi lưu lượng mạng (network traffic) của các ứng dụng thông qua các card mạng theo thời gian thực.

Interface: all						
#	Application	Clients	Bandwidth Usage now	Total Traffic	Actions	
1	unclassified	11	9 KB/s	215 KB		
2	Sophos Webadmin	1	1 KB/s	1 MB	Block  Shape  Throttle	
3	McAfee	1	<1 KB/s	93 KB	Block  Shape  Throttle	
4	Google	1	<1 KB/s	89 KB	Block  Shape  Throttle	
5	NTP	1	<1 KB/s	17 KB	Block  Shape  Throttle	
6	Sophos Content Filter Framework Server	1	<1 KB/s	9 KB	Block  Shape  Throttle	
7	HTTP	1	<1 KB/s	<1 KB	Block  Shape  Throttle	
8	Microsoft OneDrive	2	<1 KB/s	18 KB	Block  Shape  Throttle	
9	Sophos UTM Up2Date	1	<1 KB/s	244 MB	Block  Shape  Throttle	
10	SSL	2	<1 KB/s	44 KB	Block  Shape  Throttle	
11	YouTube	1	<1 KB/s	12 KB	Block  Shape  Throttle	
12	DNS	3	<1 KB/s	41 KB	Block  Shape  Throttle	

Để thiết lập các quy tắc, ta thực hiện ở tab Application Control Rules.

The screenshot shows the Sophos UTM 9 Application Control interface. On the left, there's a sidebar with various navigation links such as Dashboard, Management, Definitions & Users, Interfaces & Routing, Network Services, Network Protection, Web Protection, Web Filtering, Web Filter Profiles, Filtering Options, Policy Helpdesk, Application Control (which is selected), FTP, Email Protection, Advanced Protection, Endpoint Protection, Wireless Protection, Webserver Protection, RED Management, Site-to-site VPN, Remote Access, Logging & Reporting, Support, and Log off. The main panel is titled "Application Control" and shows a list of rules. There are two rules listed: "1 Block FB Post" and "2 Demo 1". Each rule has an "Edit" button, a "Delete" button, and a "Clone" button. To the right of each rule, there are fields for "For" (set to "Source networks Any") and "Risk" (set to "Productivity ≤ 5 Risk ≥ 1"). A search bar and a "Find" button are also present at the top of the main panel.

## 2. Xây dựng bộ chính sách kiểm soát ứng dụng và triển khai CA (HTTPS)

### 2.1. Khắc phục lỗi HTTPS khi truy cập web tại máy DC

Vào Web Protection > Filtering Options > tab HTTPS Cas > Tải Signing CA và cài đặt vào Trusted Root Certification Authorities của máy DC.

The screenshot shows the Sophos UTM 9 web interface. On the left, there is a sidebar with various navigation links. At the top, it says "UTM 9". The main area has tabs for "Exceptions", "Websites", "Bypass Users", "PUAs", "Categories", "HTTPS CAs", and "Misc".

### Signing CA

The Signing CA is used to sign all autogenerated site certificates that are transmitted to end-user browsers. End-Users should import this certificate into their browsers to avoid SSL warning messages.

baoyen baoyen Proxy CA

[Upload](#) [Regenerate](#) [Download](#)

### Verification CAs

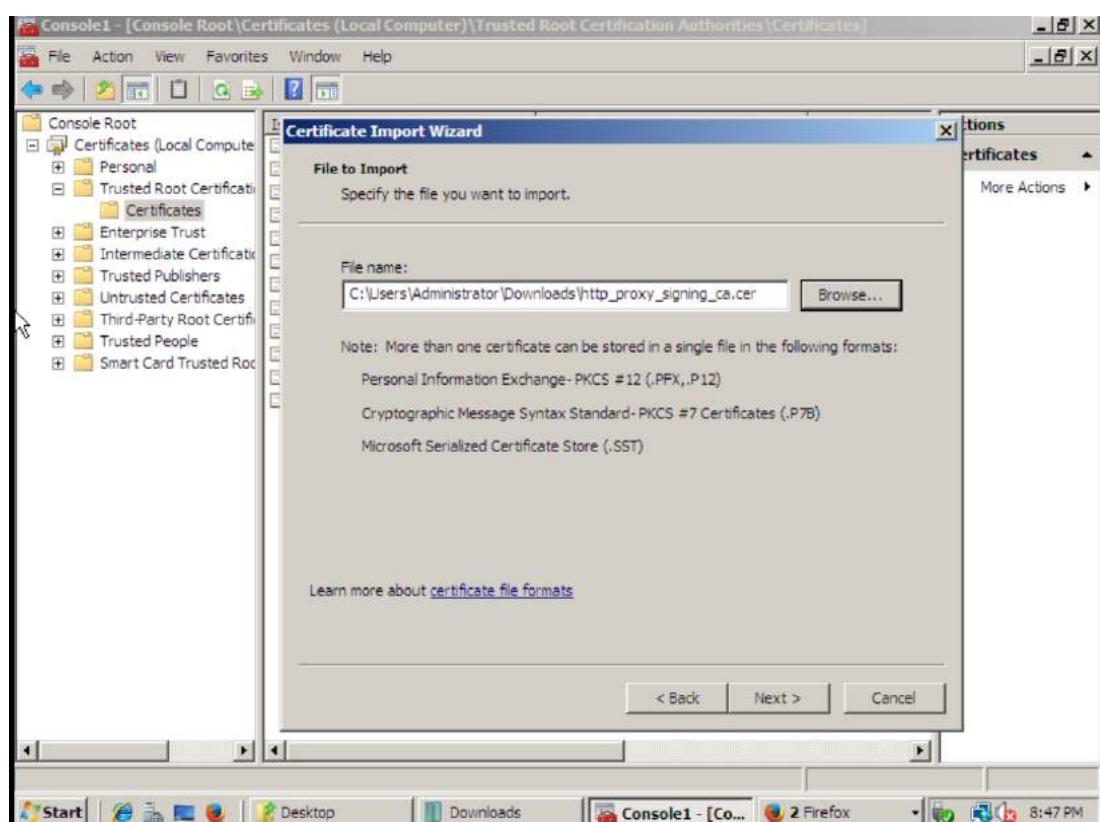
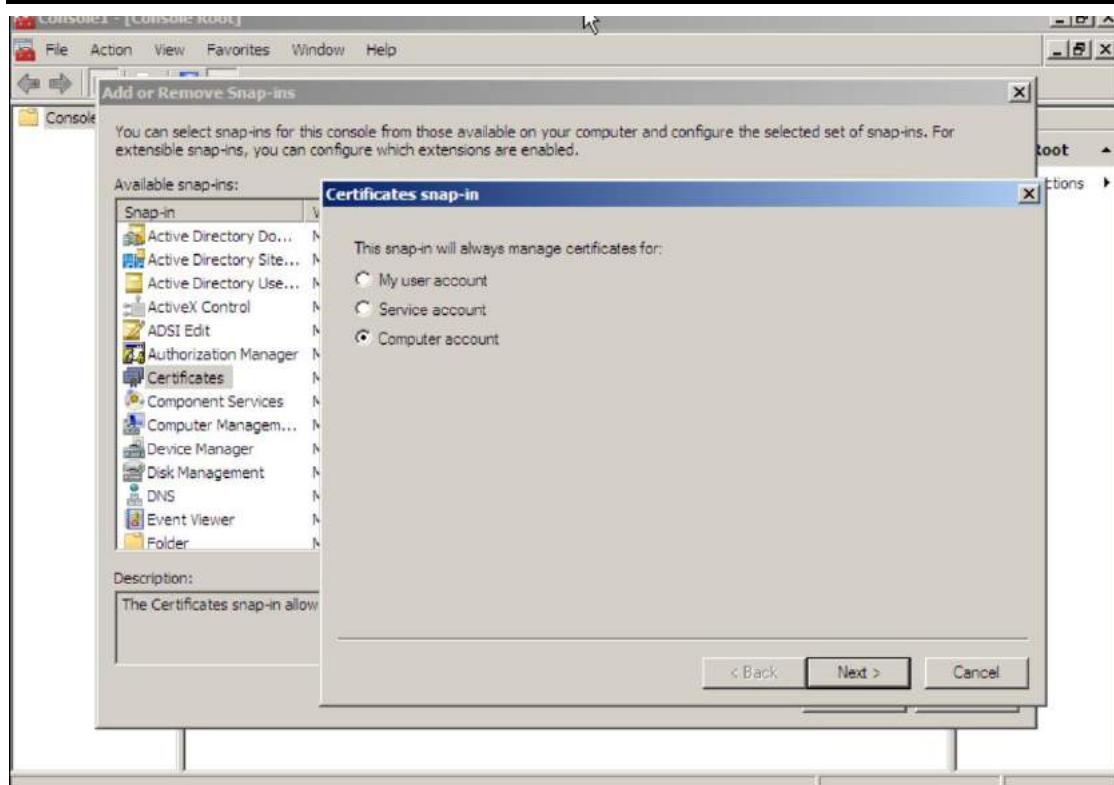
Verification CAs are used by the proxy to establish trust in the authenticity of a remote site. The Global CAs are equivalent to those used in client browsers. In addition, you can upload Local CAs that can verify additional sites, for example on your intranet.

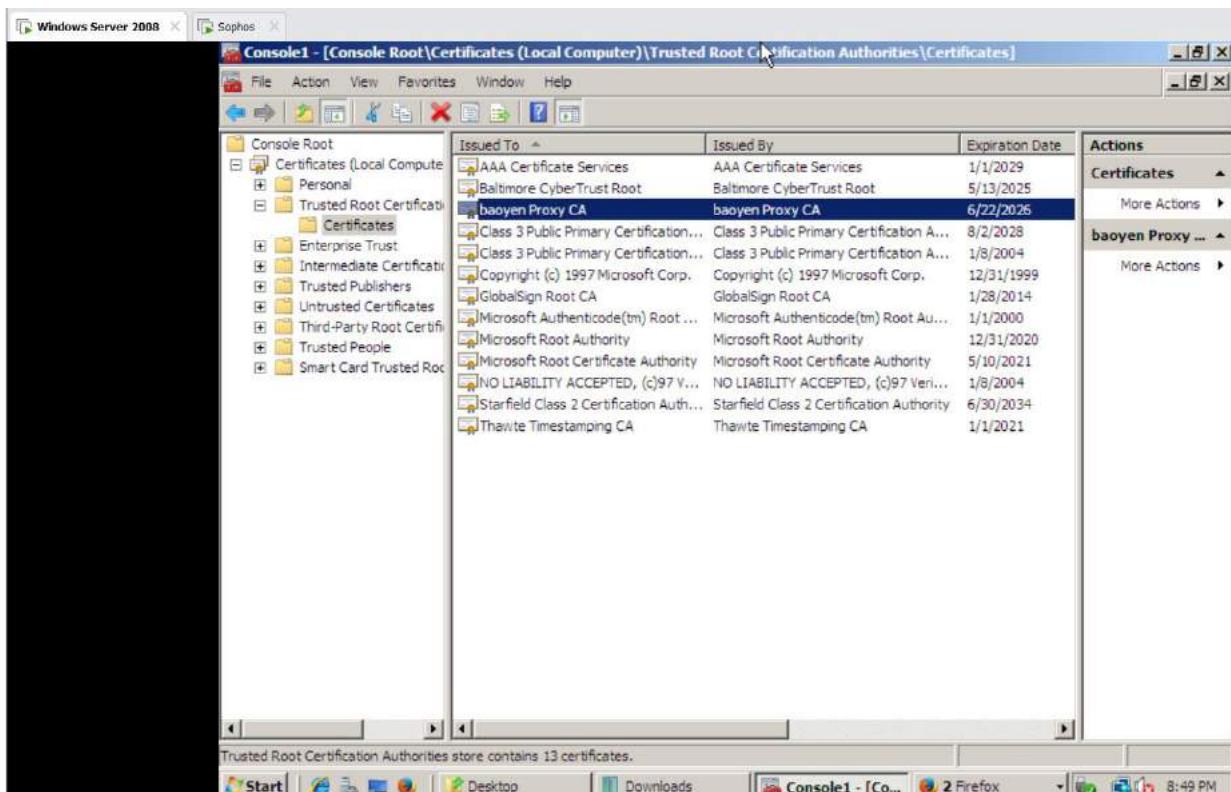
#### Local verification CAs

No local CA Certificates installed [Upload local CA](#) [Upload](#)

#### Global verification CAs

		ACCV ACCVRAIZ1
		Actalis S.p.A./03358520967 Actalis Authentication Root CA
		AffirmTrust AffirmTrust Premium ECC
		AffirmTrust AffirmTrust Networking
		AffirmTrust AffirmTrust Premium
		AffirmTrust AffirmTrust Commercial
		Agence TunTrust Root CA
		Agencia EC-ACC
		Amazon Amazon Root CA 2
		Amazon Amazon Root CA 3
		Amazon Amazon Root CA 1
		Amazon Amazon Root CA 4
		ANF Autoridad de Certificacion ANF Secure Server Root CA
		Asseco Data Systems S.A. Certum Trusted Root CA
		Asseco Data Systems S.A. Certum EC-384 CA

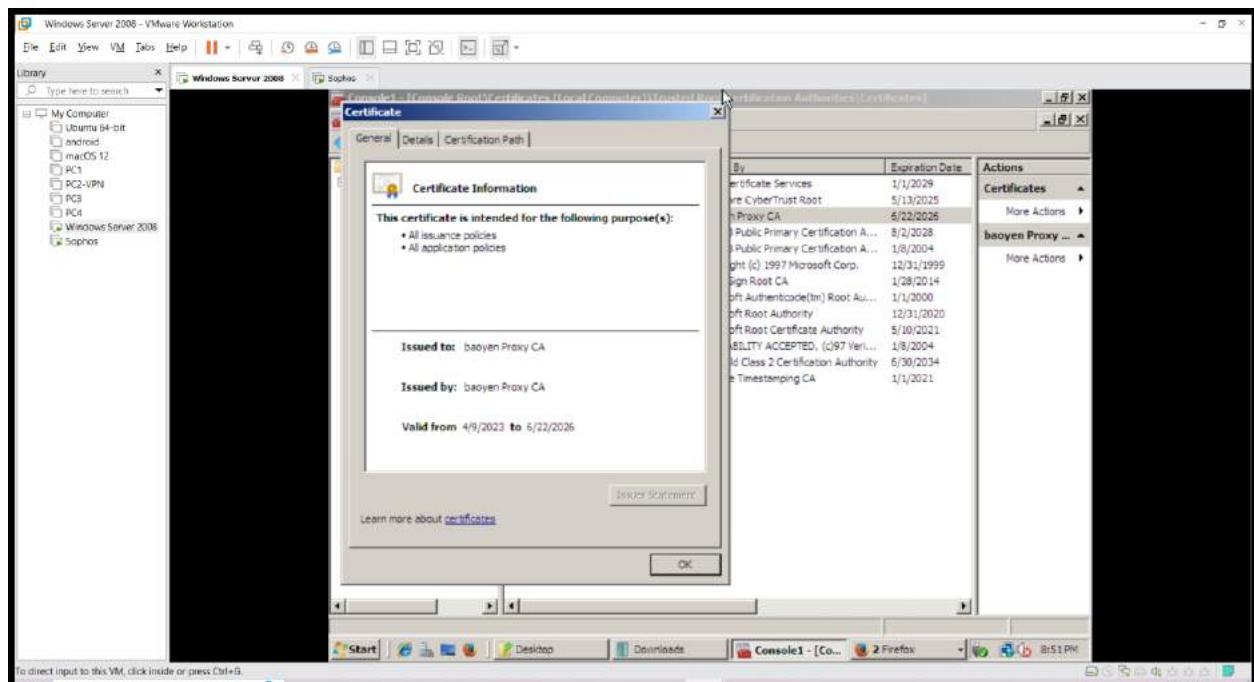




Upload lại.

The screenshot shows the Sophos Firewall interface with the 'HTTPS CAs' tab selected. It includes three main sections: 'Signing CA', 'Verification CAs', and 'Local verification CAs'. Each section has a corresponding icon (a pen nib, a padlock, and a folder), a description, and buttons for 'Upload', 'Regenerate', and 'Download'.

- Signing CA:** Described as used to sign all autogenerated site certificates. It shows a yellow pen nib icon, the name 'baoyen baoyen Proxy CA' with a Vietnamese flag icon, and buttons for 'Upload', 'Regenerate', and 'Download'.
- Verification CAs:** Described as used by the proxy to establish trust in the authenticity of a remote site. It shows a yellow padlock icon and a description: 'Verification CAs are used by the proxy to establish trust in the authenticity of a remote site. The Global CAs are equivalent to those used in client browsers. In addition, you can upload Local CAs that can verify additional sites, for example on your intranet.'
- Local verification CAs:** Shows a list with icons for delete, info, and status, followed by the name 'baoyen baoyen Proxy CA' with a Vietnamese flag icon. It also includes a 'Upload local CA:' input field with a browse button and an 'Upload' button.



## 2.2 Thiết lập các quy tắc

- Cấm tất cả người dùng sử dụng các phương thức truyền tập tin qua Internet bằng các website chia sẻ file (File transfer) như Mediafire.com, box.net
- Cấm tất cả người dùng sử dụng giao thức truyền tập tin FTP, không cho download Torrent.
- Hạn chế người dùng sử dụng mạng xã hội: Cấm sử dụng Twitter, Google+.  
*Đối với Facebook cho truy cập nhưng cấm đăng status trên tường và nhắn tin trên Facebook (nếu không thực hiện được thì cấm hẳn sử dụng Facebook).*
- Cấm sử dụng các chương trình thay đổi Proxy như Tor hay Ultrasuft
- Cấm không cho sử dụng các email server (gmail, yahoo,...), ngoại trừ email server của công ty, ví dụ giả sử cho phép http://ctmail.vnu.edu.vn

The screenshot displays seven separate configuration panels, each consisting of a header, application selection, and a 'For' section.

- Panel 3 Lab6 Cau2:** Applications: MediaFire, Box.net. For: Source networks (Any).
- Panel 4 Lab6 Cau3:** Applications: torrentz.eu, FTPSDATA, FTPS. For: Source networks (Any).
- Panel 5 Lab6 Cau4:** Applications: Facebook Video Chat, Facebook Video, Facebook Search. For: Source networks (Any).
- Panel 6 Lab6 Cau5:** Applications: Ultrasurf, Tor Directory Services, Tor. For: Source networks (Any).
- Panel 7 Lab6 Cau6:** Applications: XNS Mail, Sky Mail, QQ Mail, MC Outlook. For: Source networks (Any).

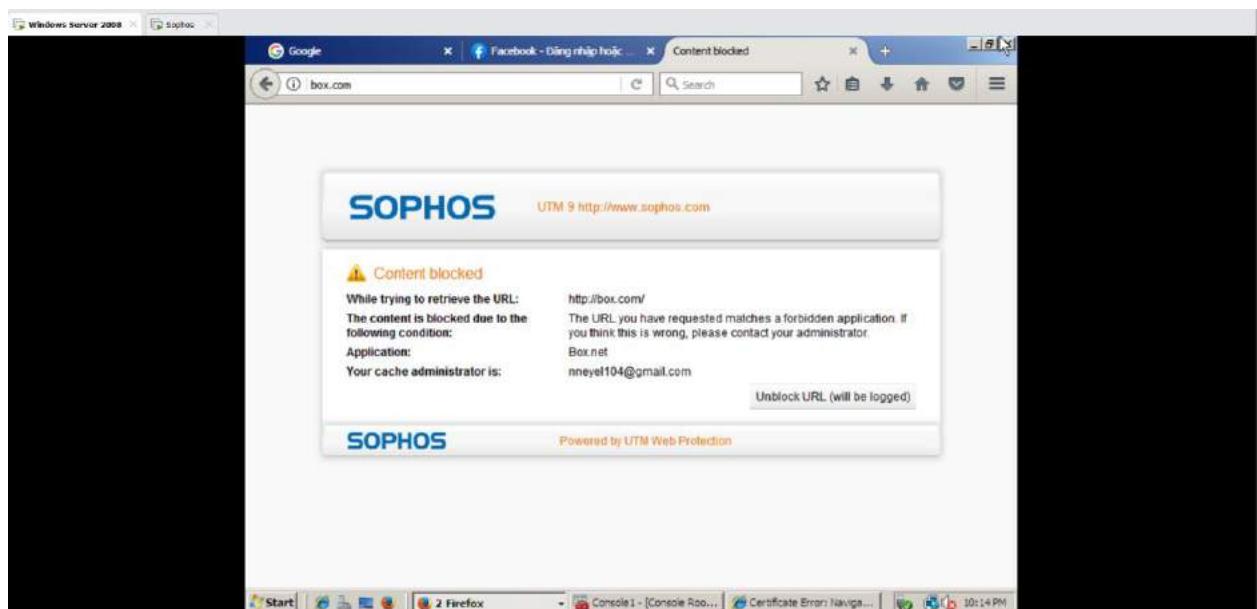
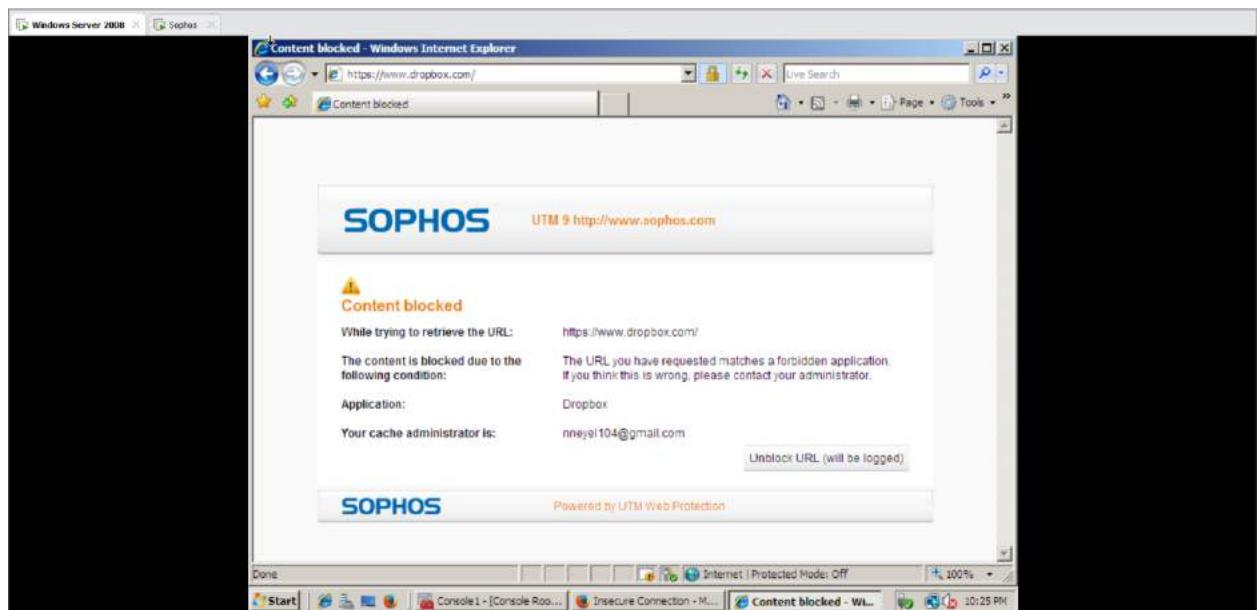
### 3. Kiểm tra kết quả & ứng dụng

3.1. Khi vào các website có https trên Chrome không còn xảy ra tình trạng bị cảnh báo HTTPS



3.2. Không thể truy cập các website chia sẻ file như Mediafire, Dropbox, ...



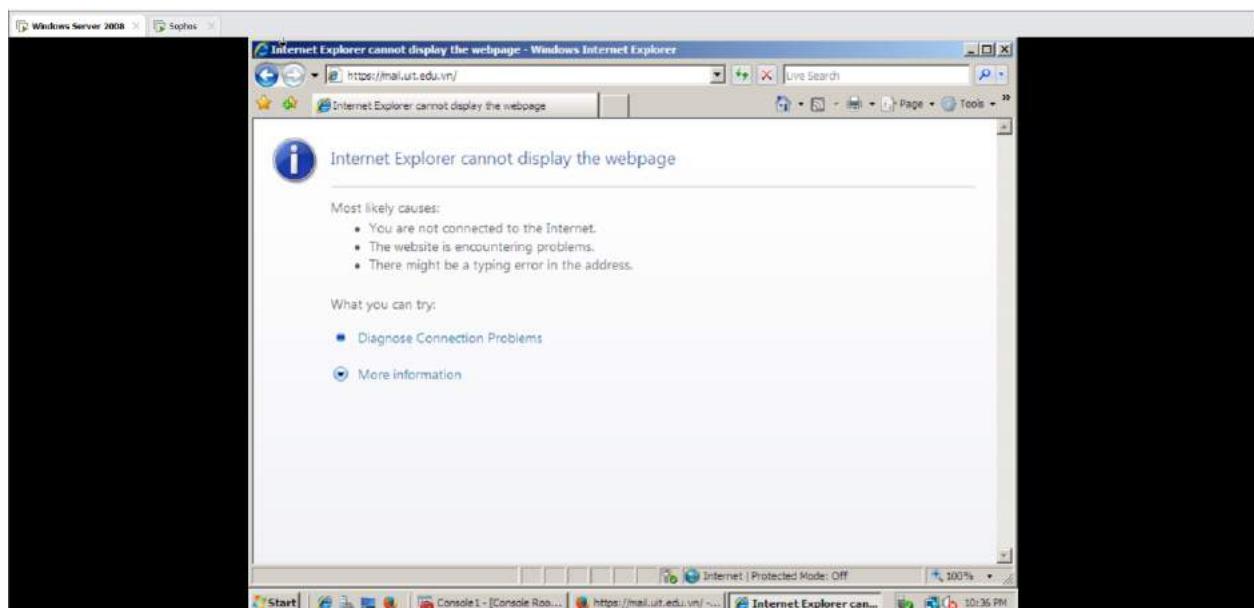


### 3.4. Thử nghiệm khi truy cập và sử dụng với các Mạng xã hội phổ biến.



### 3.6. Kiểm tra kết quả khi truy cập gmail.com; mail.uit.edu.vn; ctmail.vnu.edu.vn





## LAB 07: LOCAL DNS ATTACK

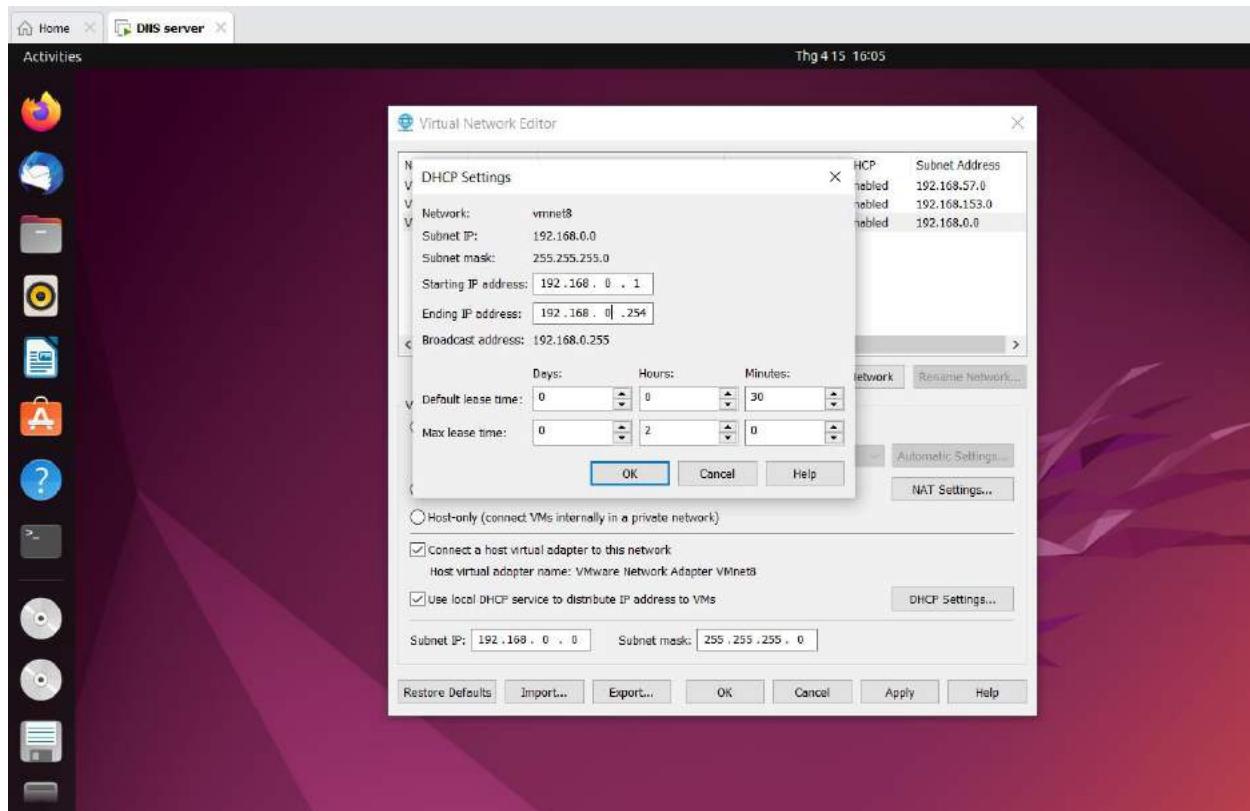
### A. Môi trường

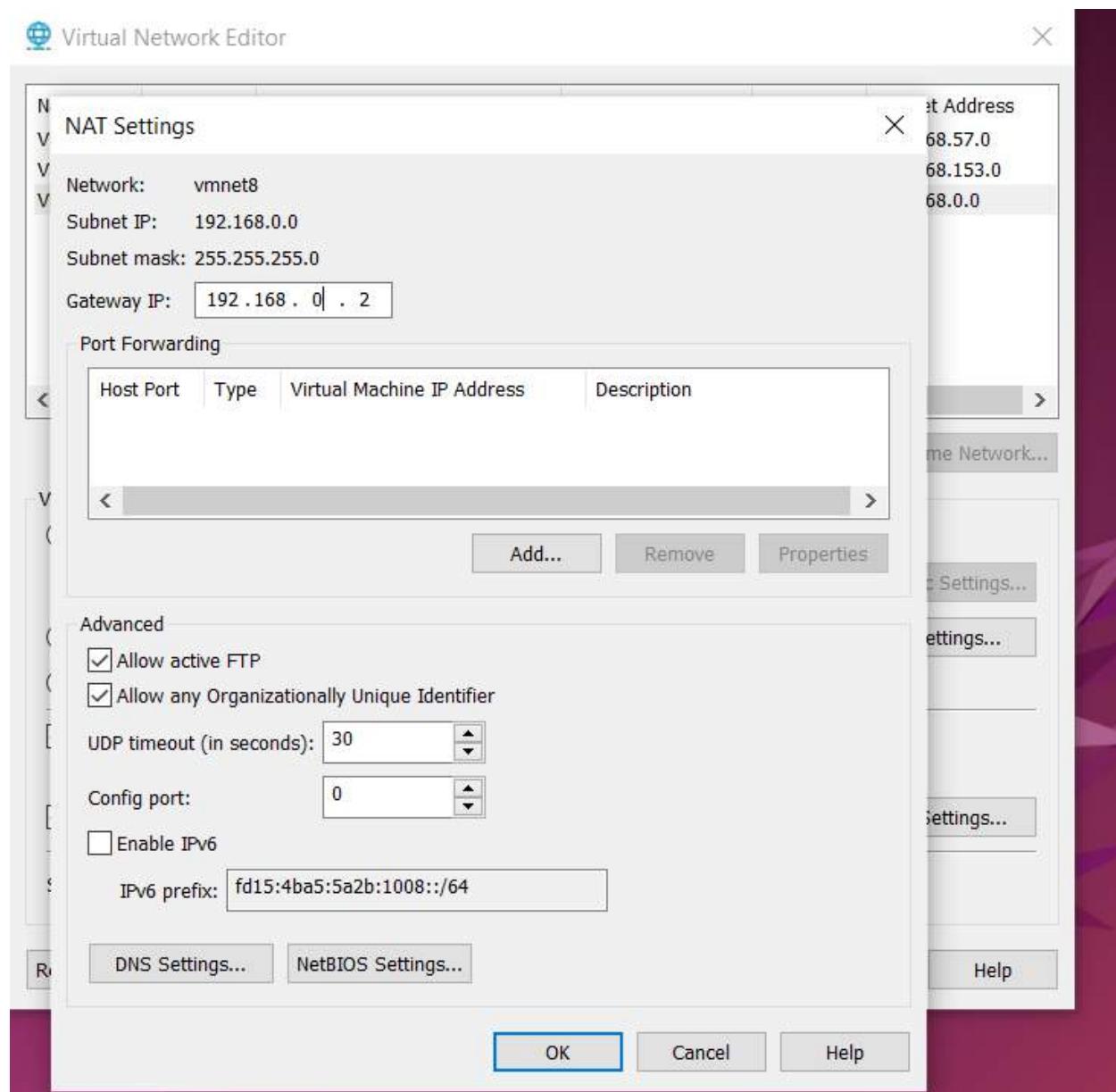
- Máy ảo Vmware Ubuntu 22.04.2 làm DNS server
- Máy ảo Vmware Ubuntu 22.04.2 làm User
- Máy ảo Vmware Ubuntu 22.04.2 làm Attacker

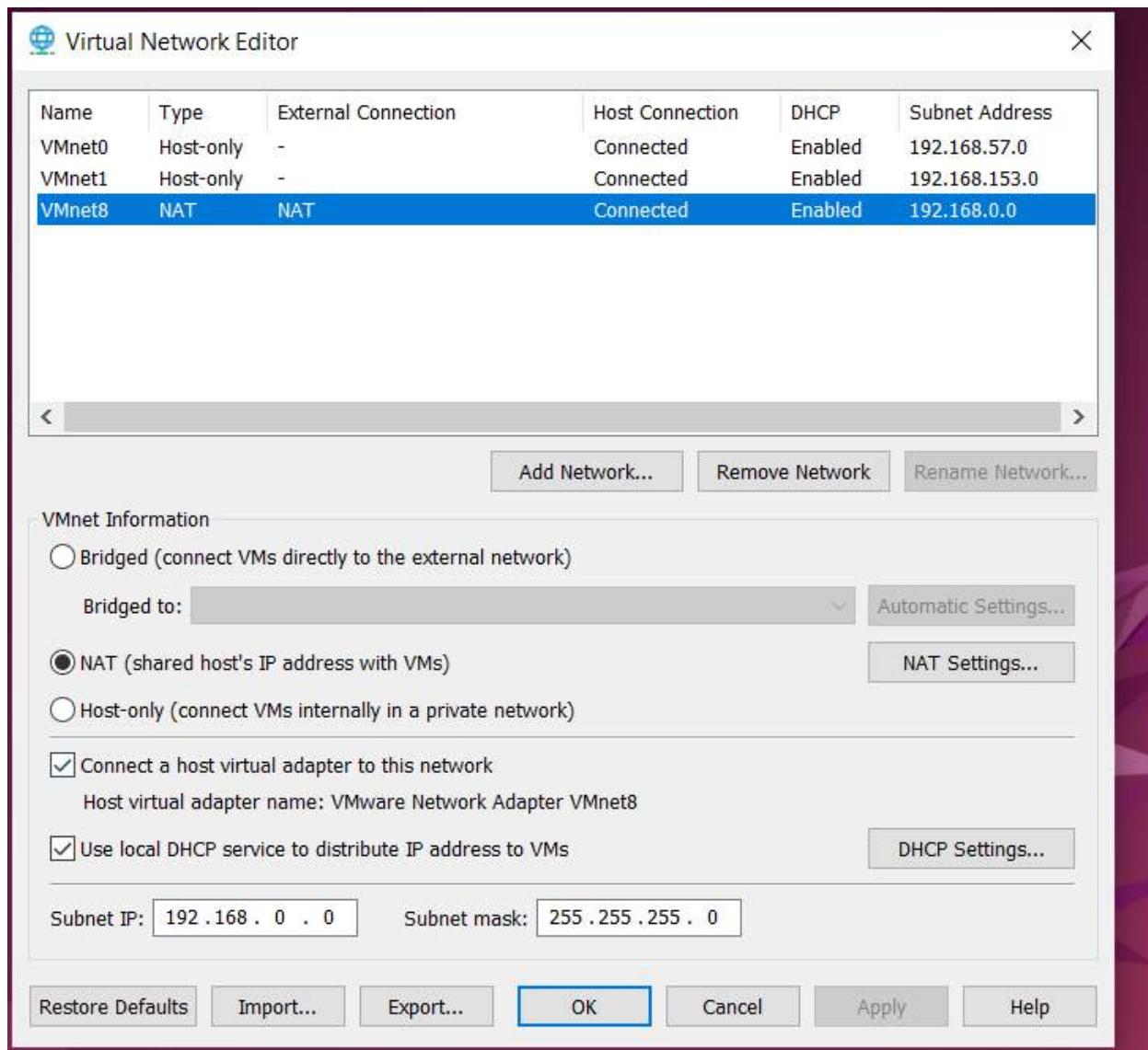
### B. Thiết lập IP tĩnh cho cả 3 máy

- DNS server: 192.168.0.10/24
- User: 192.168.0.100/24
- Attacker: 192.168.0.200/24

Trước tiên, cần thiết lập vùng mạng NAT trước, vì có thể máy ảo không thuộc lớp mạng 192.168.0.0/24.

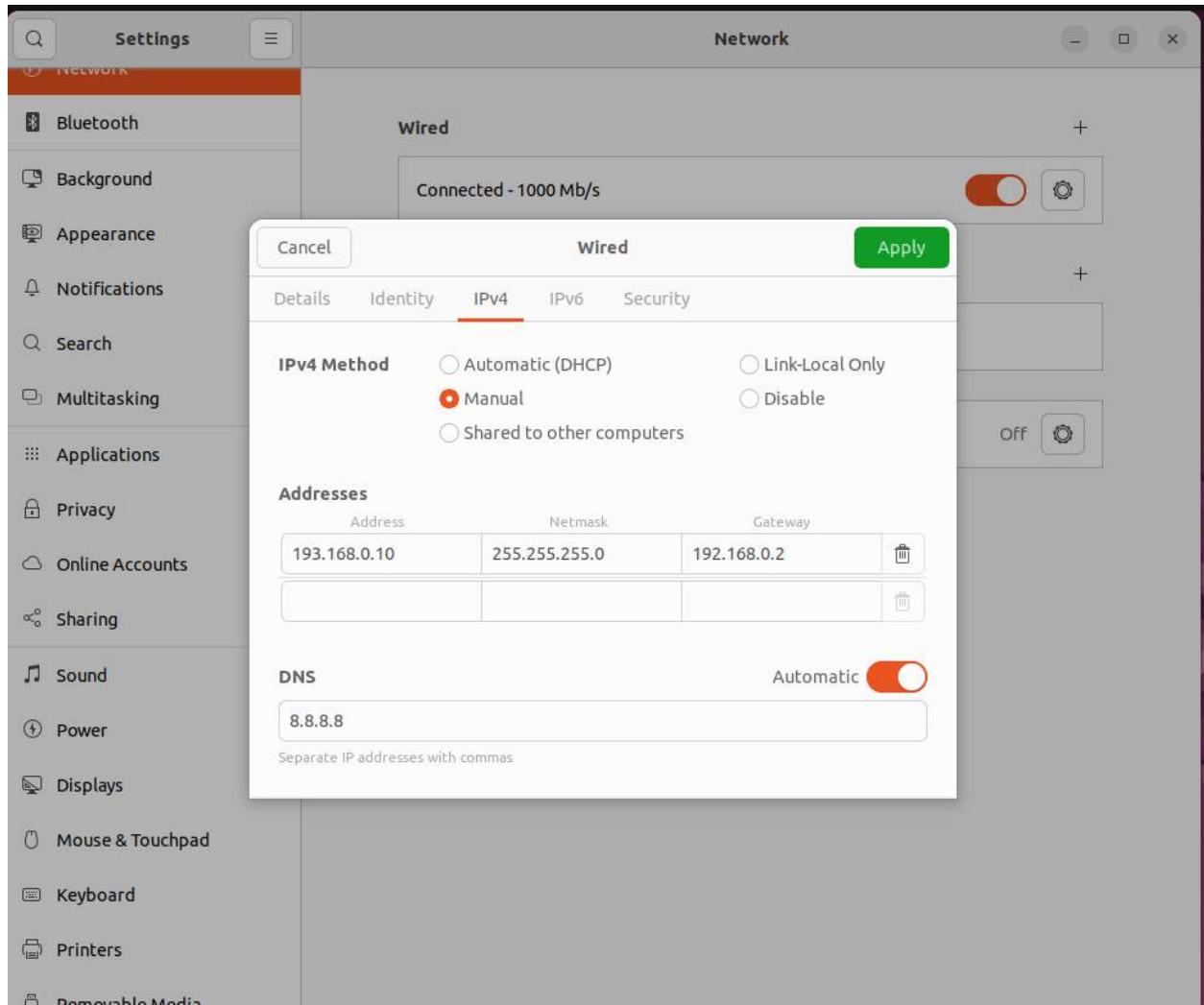


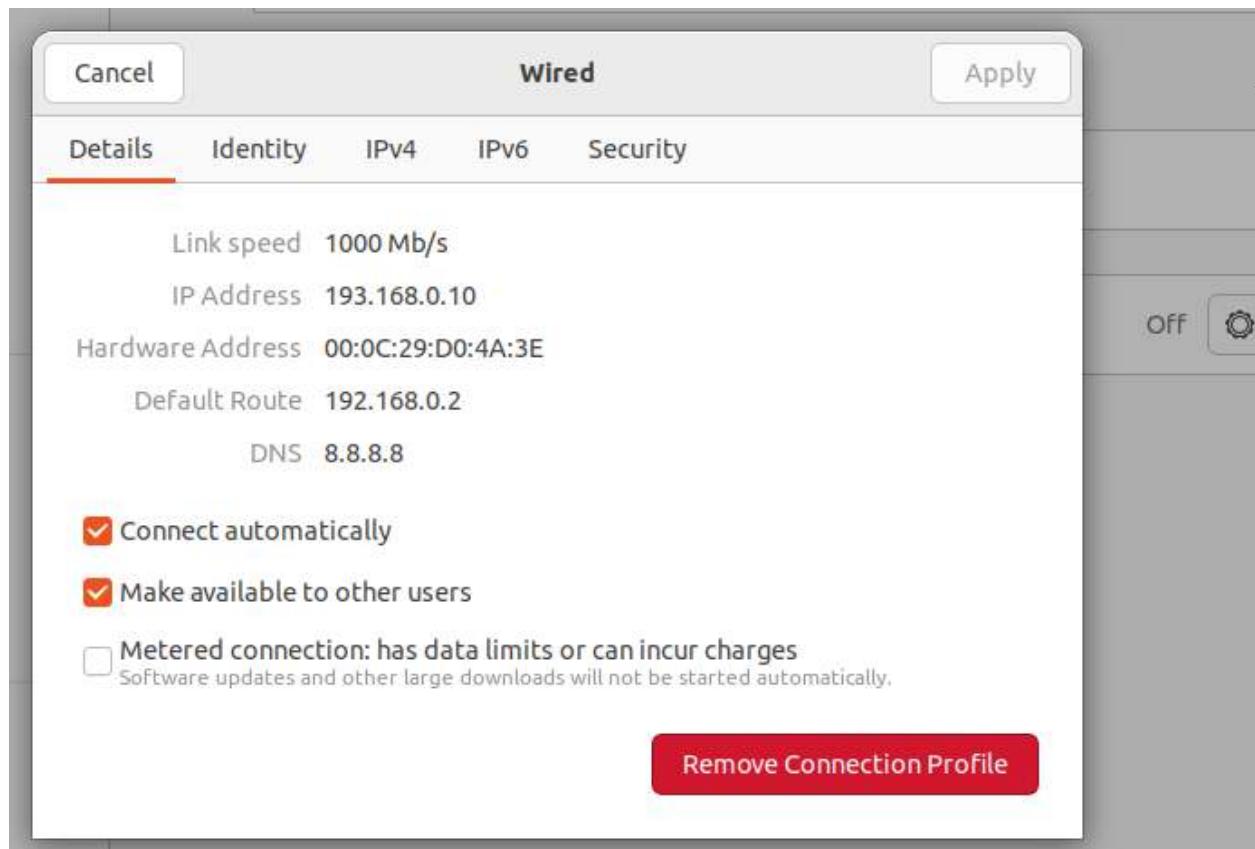




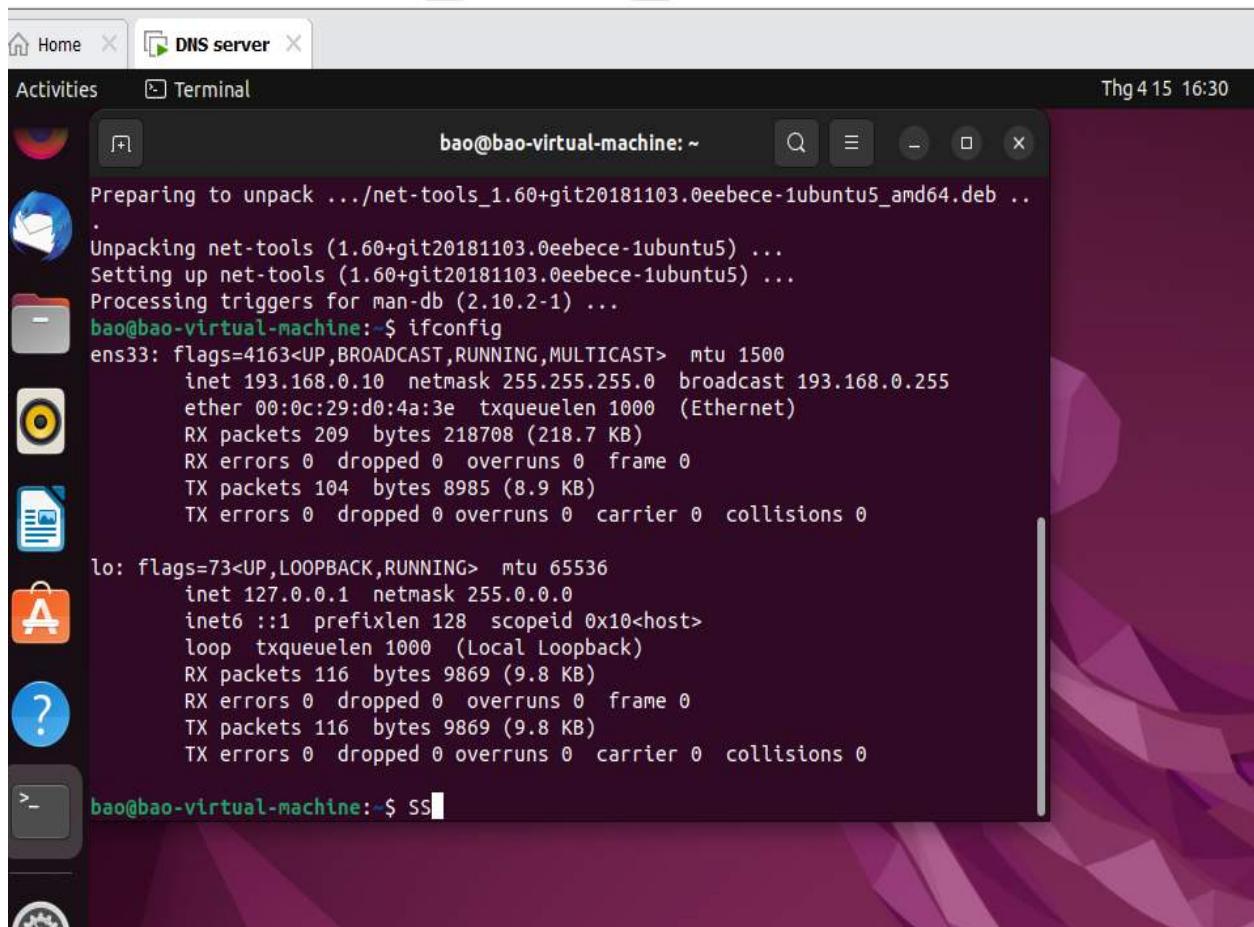
## 2.1. Install and configura the DNS server

Sau đó ta thiết lập IP tĩnh cho DNS server như sau:





Và sau đó restart lại máy để apply vào. Sau đó vào terminal để kiểm tra bằng lệnh: ifconfig.



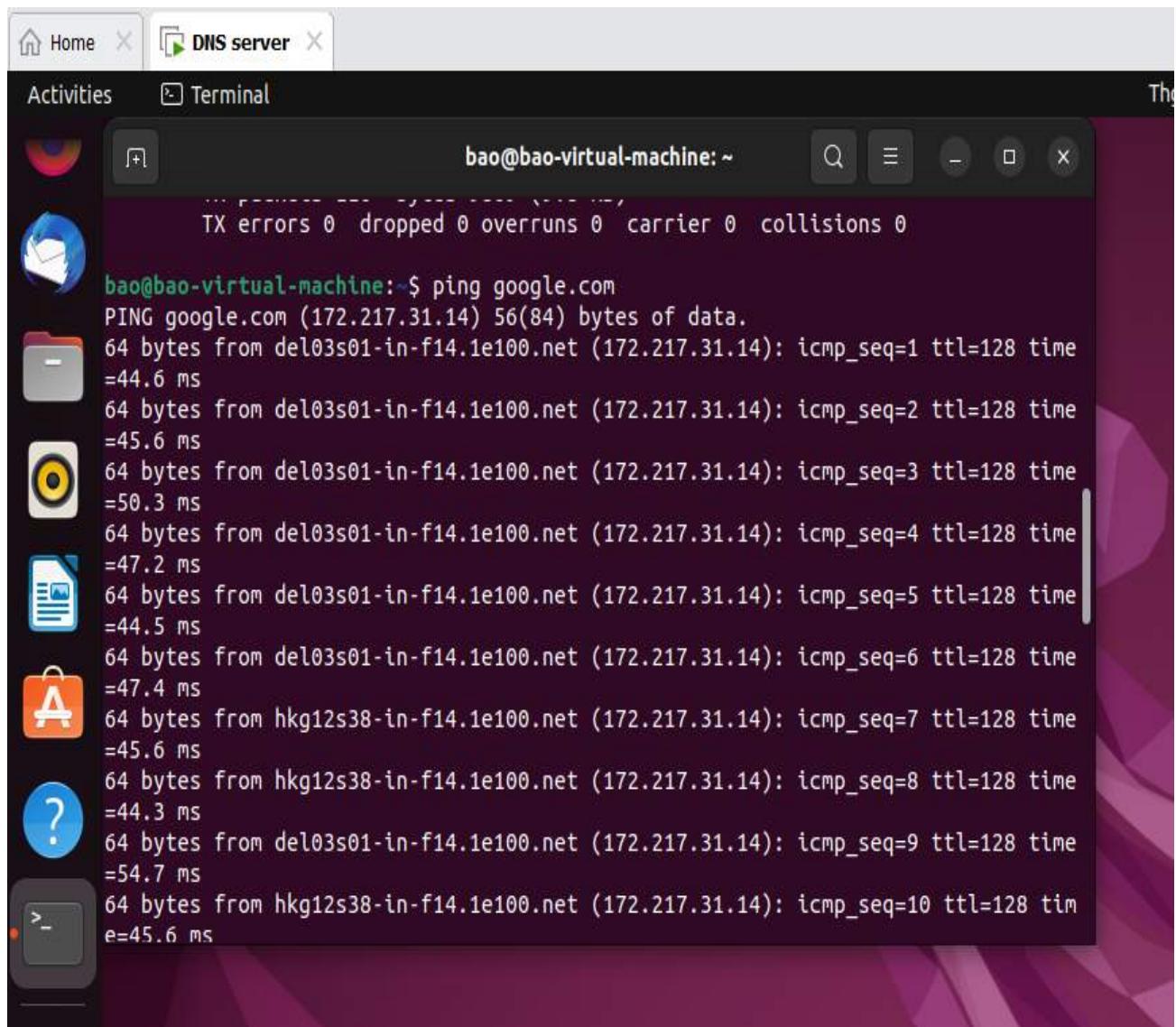
The screenshot shows a Linux desktop environment with a purple and green abstract background. A terminal window titled "bao@bao-virtual-machine: ~" is open, displaying the output of several commands:

```
Preparing to unpack .../net-tools_1.60+git20181103.0eebece-1ubuntu5_amd64.deb ...
.
Unpacking net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Setting up net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Processing triggers for man-db (2.10.2-1) ...
bao@bao-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 193.168.0.10 netmask 255.255.255.0 broadcast 193.168.0.255
        ether 00:0c:29:d0:4a:3e txqueuelen 1000 (Ethernet)
          RX packets 209 bytes 218708 (218.7 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 104 bytes 8985 (8.9 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inetc6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
          RX packets 116 bytes 9869 (9.8 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 116 bytes 9869 (9.8 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

bao@bao-virtual-machine:~$ ss
```

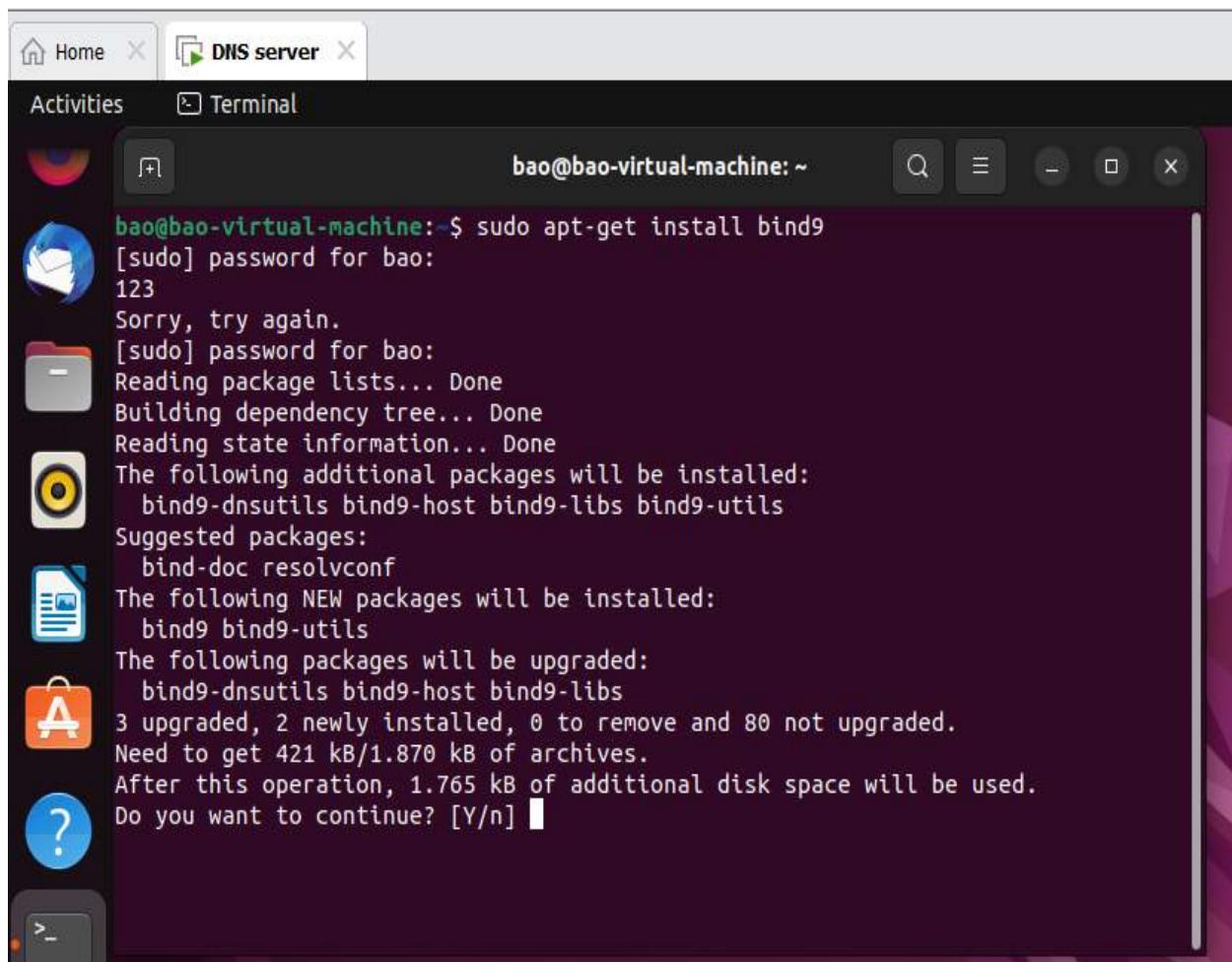
Và kiểm tra tốc độ mạng google: ping google.com



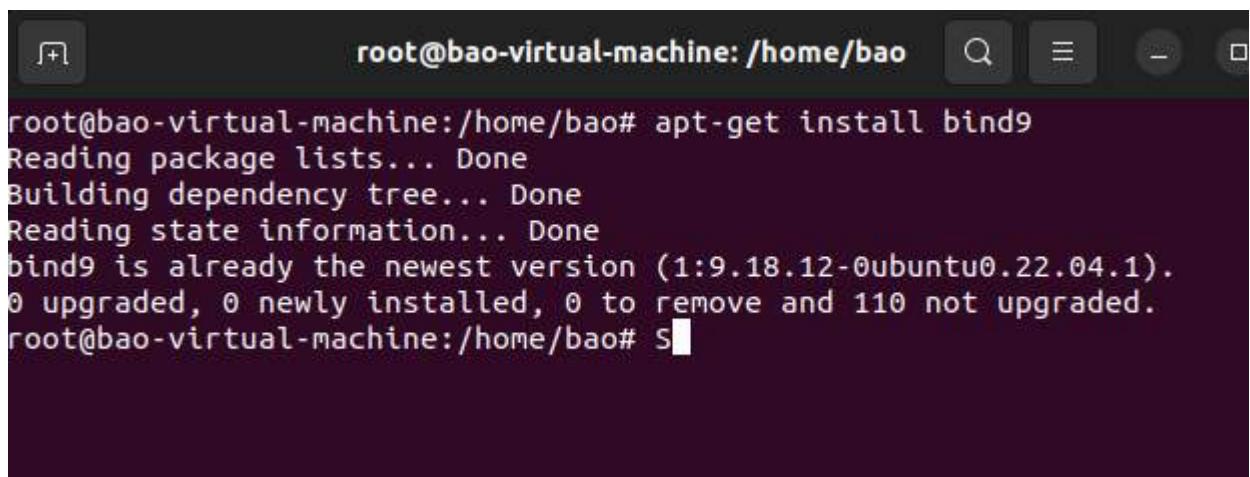
The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "DNS server". The terminal content shows network statistics and the output of a ping command to google.com.

```
bao@bao-virtual-machine:~$ ping google.com
PING google.com (172.217.31.14) 56(84) bytes of data.
64 bytes from del03s01-in-f14.1e100.net (172.217.31.14): icmp_seq=1 ttl=128 time
=44.6 ms
64 bytes from del03s01-in-f14.1e100.net (172.217.31.14): icmp_seq=2 ttl=128 time
=45.6 ms
64 bytes from del03s01-in-f14.1e100.net (172.217.31.14): icmp_seq=3 ttl=128 time
=50.3 ms
64 bytes from del03s01-in-f14.1e100.net (172.217.31.14): icmp_seq=4 ttl=128 time
=47.2 ms
64 bytes from del03s01-in-f14.1e100.net (172.217.31.14): icmp_seq=5 ttl=128 time
=44.5 ms
64 bytes from del03s01-in-f14.1e100.net (172.217.31.14): icmp_seq=6 ttl=128 time
=47.4 ms
64 bytes from hkg12s38-in-f14.1e100.net (172.217.31.14): icmp_seq=7 ttl=128 time
=45.6 ms
64 bytes from hkg12s38-in-f14.1e100.net (172.217.31.14): icmp_seq=8 ttl=128 time
=44.3 ms
64 bytes from del03s01-in-f14.1e100.net (172.217.31.14): icmp_seq=9 ttl=128 time
=54.7 ms
64 bytes from hkg12s38-in-f14.1e100.net (172.217.31.14): icmp_seq=10 ttl=128 tim
e=45.6 ms
```

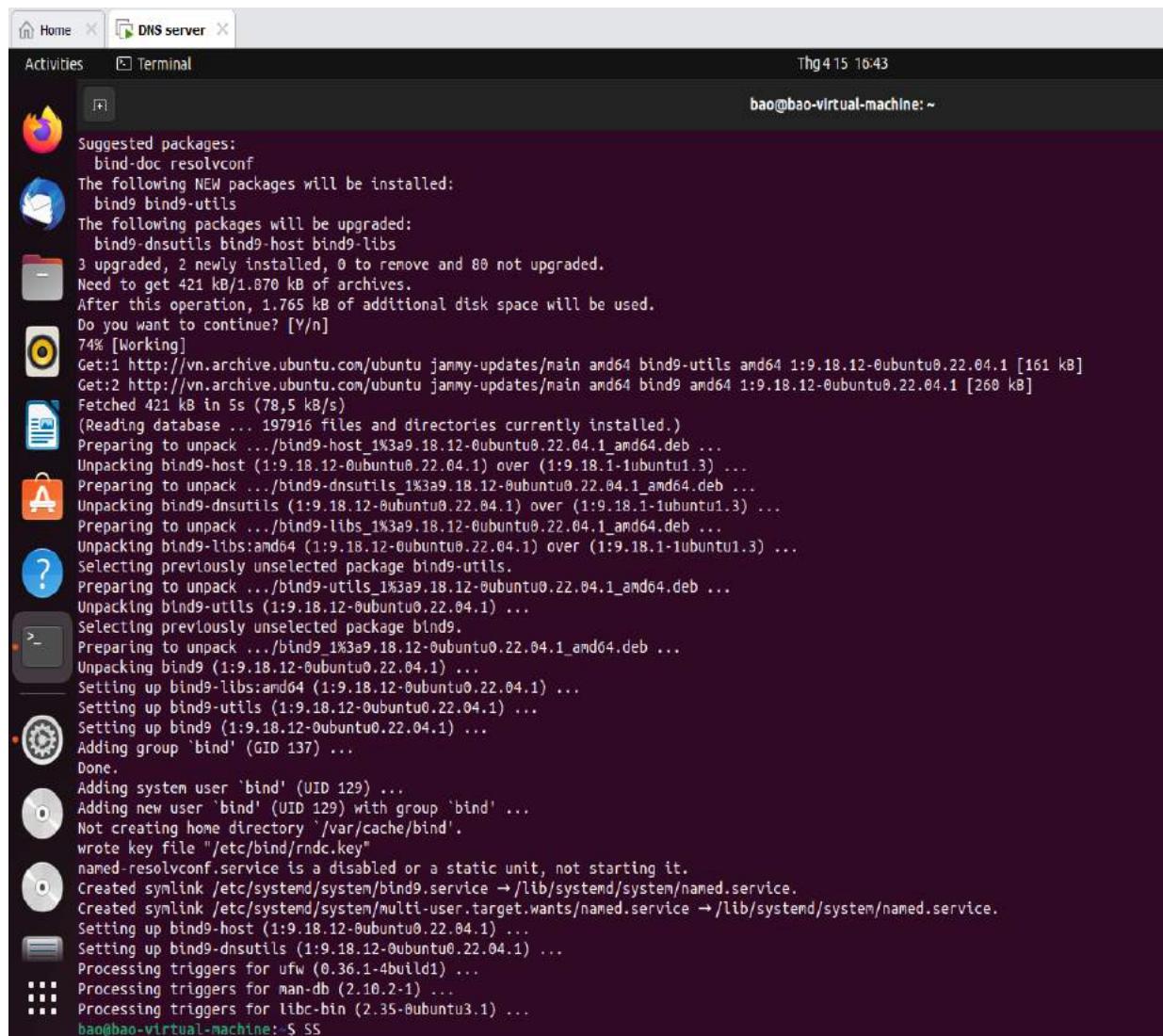
Và cài bind9 vào DNS Server này: sudo apt-get install bind9:



bao@bao-virtual-machine:~\$ sudo apt-get install bind9  
[sudo] password for bao:  
123  
Sorry, try again.  
[sudo] password for bao:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
bind9-dnsutils bind9-host bind9-libs bind9-utils  
Suggested packages:  
bind-doc resolvconf  
The following NEW packages will be installed:  
bind9 bind9-utils  
The following packages will be upgraded:  
bind9-dnsutils bind9-host bind9-libs  
3 upgraded, 2 newly installed, 0 to remove and 80 not upgraded.  
Need to get 421 kB/1.870 kB of archives.  
After this operation, 1.765 kB of additional disk space will be used.  
Do you want to continue? [Y/n] █

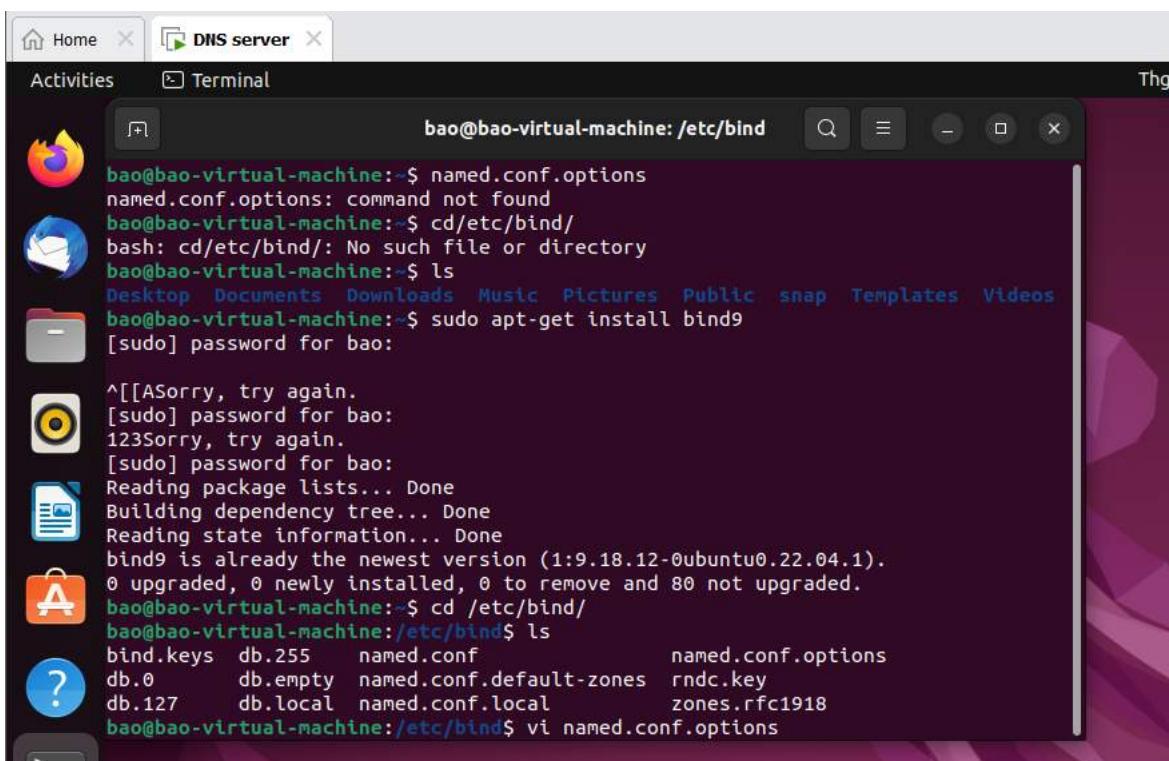


root@bao-virtual-machine:/home/bao# apt-get install bind9  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
bind9 is already the newest version (1:9.18.12-0ubuntu0.22.04.1).  
0 upgraded, 0 newly installed, 0 to remove and 110 not upgraded.  
root@bao-virtual-machine:/home/bao# S █



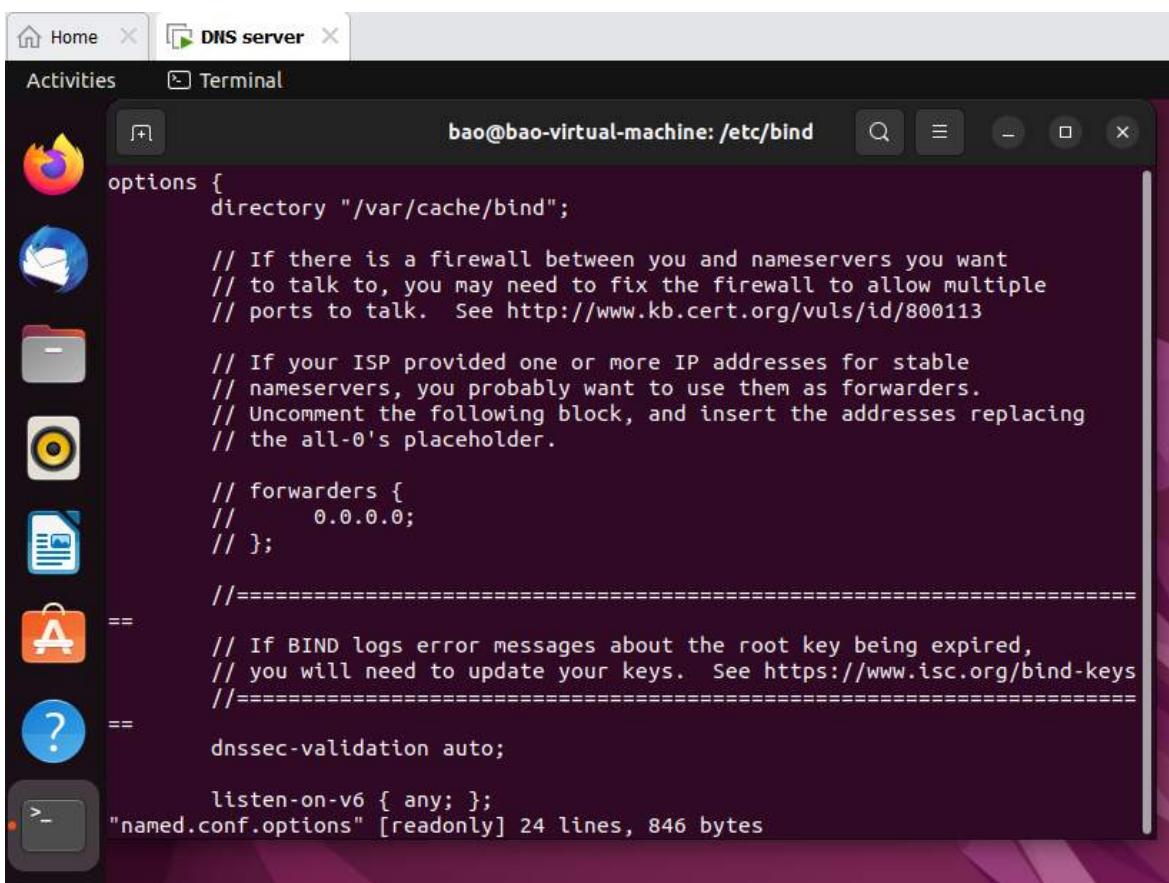
The following NEW packages will be installed:  
bind9 bind9-utils  
The following packages will be upgraded:  
bind9-dnsutils bind9-host bind9-libs  
3 upgraded, 2 newly installed, 0 to remove and 80 not upgraded.  
Need to get 421 kB/1.870 kB of archives.  
After this operation, 1.765 kB of additional disk space will be used.  
Do you want to continue? [Y/n]  
74% [Working]  
Get:1 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 bind9-utils amd64 1:9.18.12-0ubuntu0.22.04.1 [161 kB]  
Get:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 bind9 amd64 1:9.18.12-0ubuntu0.22.04.1 [260 kB]  
Fetched 421 kB in 5s (78.5 kB/s)  
(Reading database ... 197916 files and directories currently installed.)  
Preparing to unpack .../bind9-host\_1%3a9.18.12-0ubuntu0.22.04.1\_amd64.deb ...  
Unpacking bind9-host (1:9.18.12-0ubuntu0.22.04.1) over (1:9.18.1-1ubuntu1.3) ...  
Preparing to unpack .../bind9-dnsutils\_1%3a9.18.12-0ubuntu0.22.04.1\_amd64.deb ...  
Unpacking bind9-dnsutils (1:9.18.12-0ubuntu0.22.04.1) over (1:9.18.1-1ubuntu1.3) ...  
Preparing to unpack .../bind9-utils\_1%3a9.18.12-0ubuntu0.22.04.1\_amd64.deb ...  
Unpacking bind9-utils (1:9.18.12-0ubuntu0.22.04.1) ...  
Selecting previously unselected package bind9-utils.  
Preparing to unpack .../bind9-utils\_1%3a9.18.12-0ubuntu0.22.04.1\_amd64.deb ...  
Unpacking bind9-utils (1:9.18.12-0ubuntu0.22.04.1) ...  
Selecting previously unselected package bind9.  
Preparing to unpack .../bind9\_1%3a9.18.12-0ubuntu0.22.04.1\_amd64.deb ...  
Unpacking bind9 (1:9.18.12-0ubuntu0.22.04.1) ...  
Setting up bind9-dnsutils:amd64 (1:9.18.12-0ubuntu0.22.04.1) ...  
Setting up bind9-utils (1:9.18.12-0ubuntu0.22.04.1) ...  
Setting up bind9 (1:9.18.12-0ubuntu0.22.04.1) ...  
Adding group 'bind' (GID 137) ...  
Done.  
Adding system user 'bind' (UID 129) ...  
Adding new user 'bind' (UID 129) with group 'bind' ...  
Not creating home directory '/var/cache/bind'.  
wrote key file "/etc/bind/rndc.key"  
named-resolvconf.service is a disabled or a static unit, not starting it.  
Created symlink /etc/systemd/system/bind9.service → /lib/systemd/system/named.service.  
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /lib/systemd/system/named.service.  
Setting up bind9-host (1:9.18.12-0ubuntu0.22.04.1) ...  
Setting up bind9-dnsutils (1:9.18.12-0ubuntu0.22.04.1) ...  
Processing triggers for ufw (0.36.1-4build1) ...  
Processing triggers for man-db (2.10.2-1) ...  
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...  
ban@bao-virtual-machine:~\$

## Step 2: Tạo file có tên named.conf.options



```
bao@bao-virtual-machine:~$ named.conf.options
named.conf.options: command not found
bao@bao-virtual-machine:~$ cd/etc/bind/
bash: cd/etc/bind/: No such file or directory
bao@bao-virtual-machine:~$ ls
Desktop Documents Downloads Music Pictures Public snap Templates Videos
bao@bao-virtual-machine:~$ sudo apt-get install bind9
[sudo] password for bao:

^[[ASorry, try again.
[sudo] password for bao:
123Sorry, try again.
[sudo] password for bao:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bind9 is already the newest version (1:9.18.12-0ubuntu0.22.04.1).
0 upgraded, 0 newly installed, 0 to remove and 80 not upgraded.
bao@bao-virtual-machine:~$ cd /etc/bind/
bao@bao-virtual-machine:/etc/bind$ ls
bind.keys  db.255      named.conf          named.conf.options
db.0        db.empty   named.conf.default-zones  rndc.key
db.127     db.local   named.conf.local    zones.rfc1918
bao@bao-virtual-machine:/etc/bind$ vi named.conf.options
```



```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====

    dnssec-validation auto;

    listen-on-v6 { any; };

"named.conf.options" [readonly] 24 lines, 846 bytes
```

```
// If there is a firewall between you and nameservers you want
// to talk to, you may need to fix the firewall to allow multiple
// ports to talk. See http://www.kb.cert.org/vuls/id/800113

// If your ISP provided one or more IP addresses for stable
// nameservers, you probably want to use them as forwarders.
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.

// forwarders {
//   0.0.0.0;
// };

// =====
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-
// =====
dnssec-validation auto;
dump-file "var/cache/bind/dump.db";
auth-nxdomain no;    # conform to RFC1035
listen-on-v6 { any; };
```

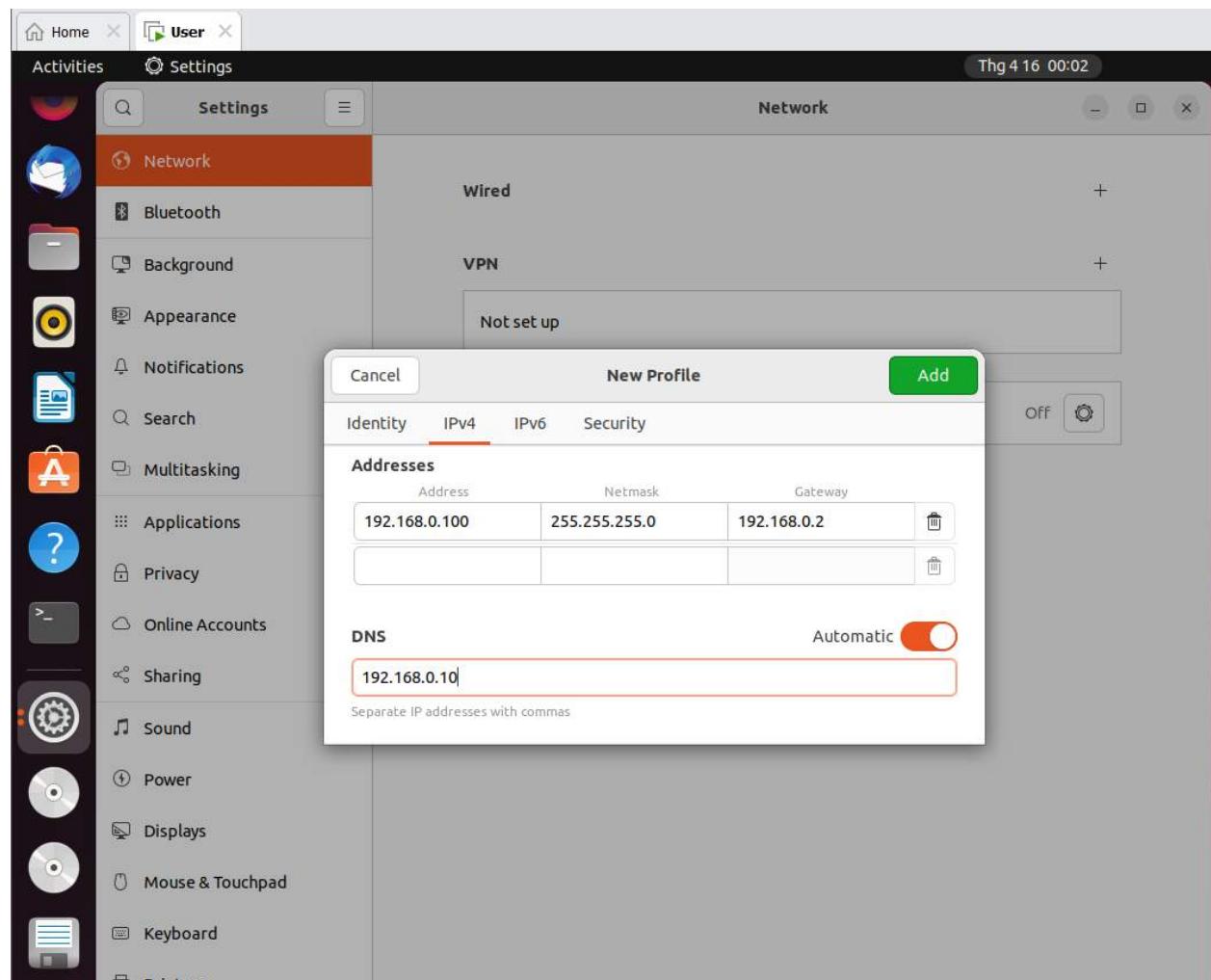
### Step 3: Tạo zone

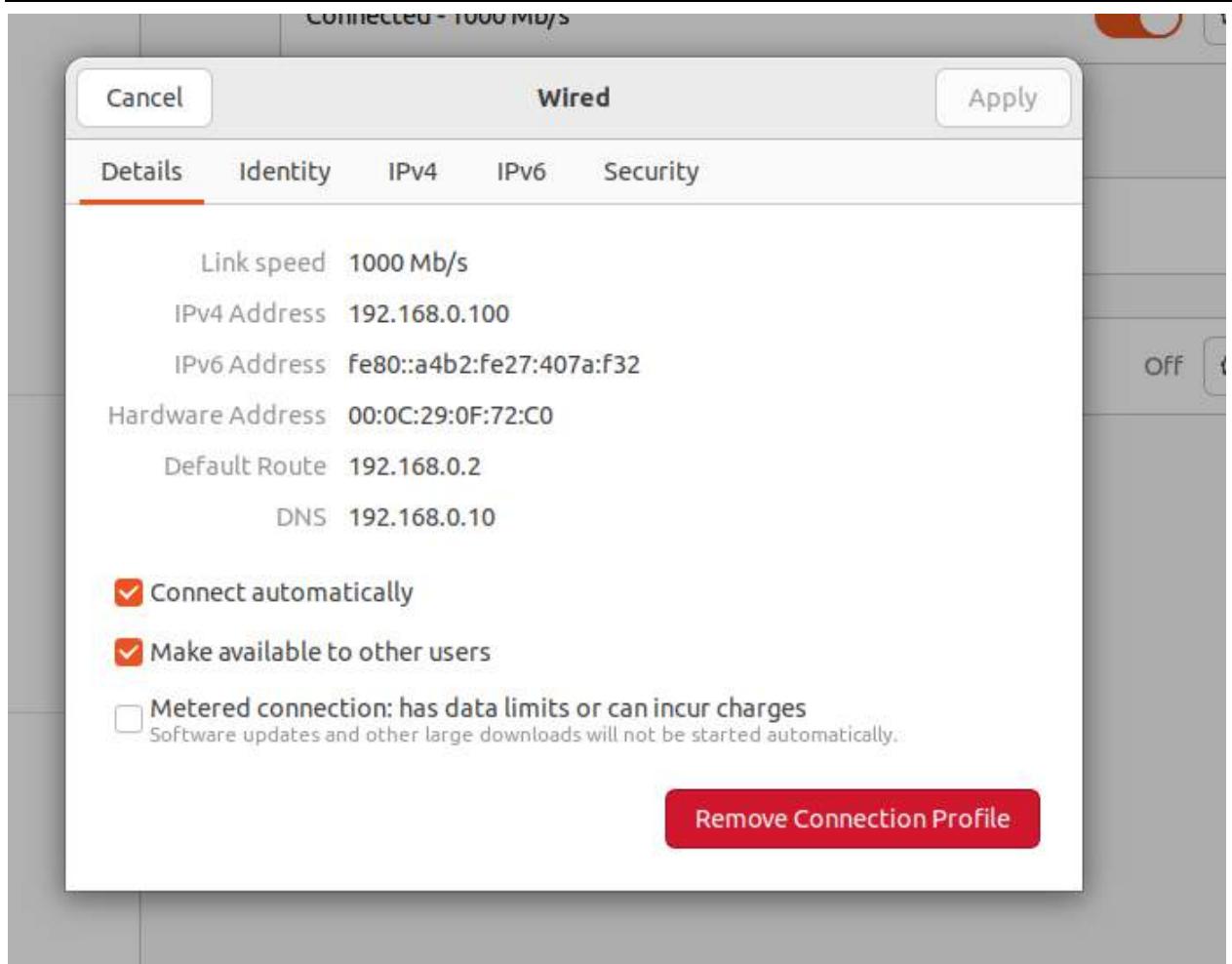
Ta sử dụng một domain là example.com

Và đườn dẫn /etc/bind/ để tạo file named.conf với nội dung như trên

## 2.2. Cấu hình máy User

Bên máy này cũng thiết lập IP tĩnh 192.168.0.100





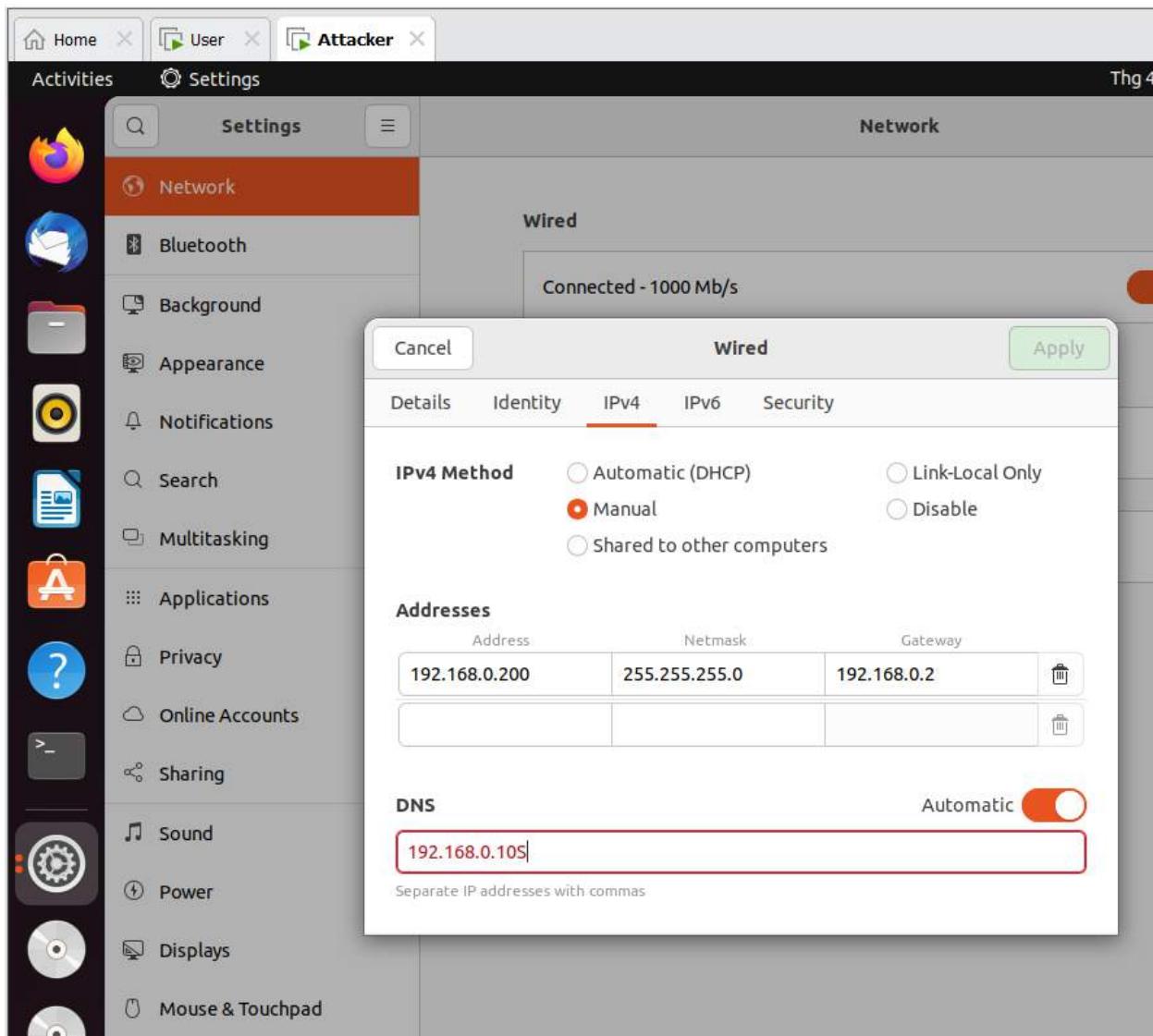
Và ta chỉnh sửa file /etc/resolv.conf để chỉ ra khi cần phân giải tên miền thì phải thông qua máy nào (IP).

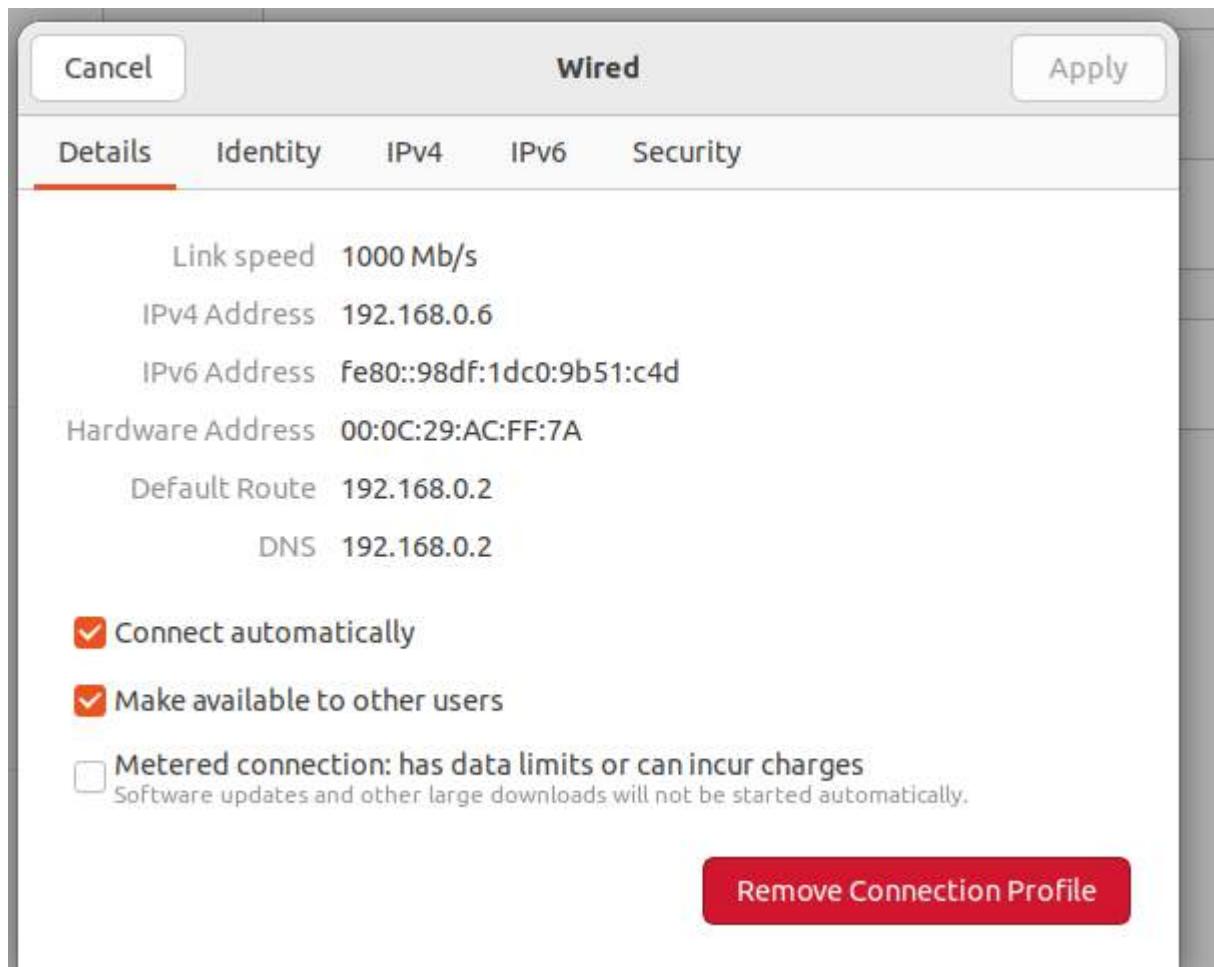
Ở đây ta thiết đặt là nameserver 192.168.0.10

Restart lại để apply nó

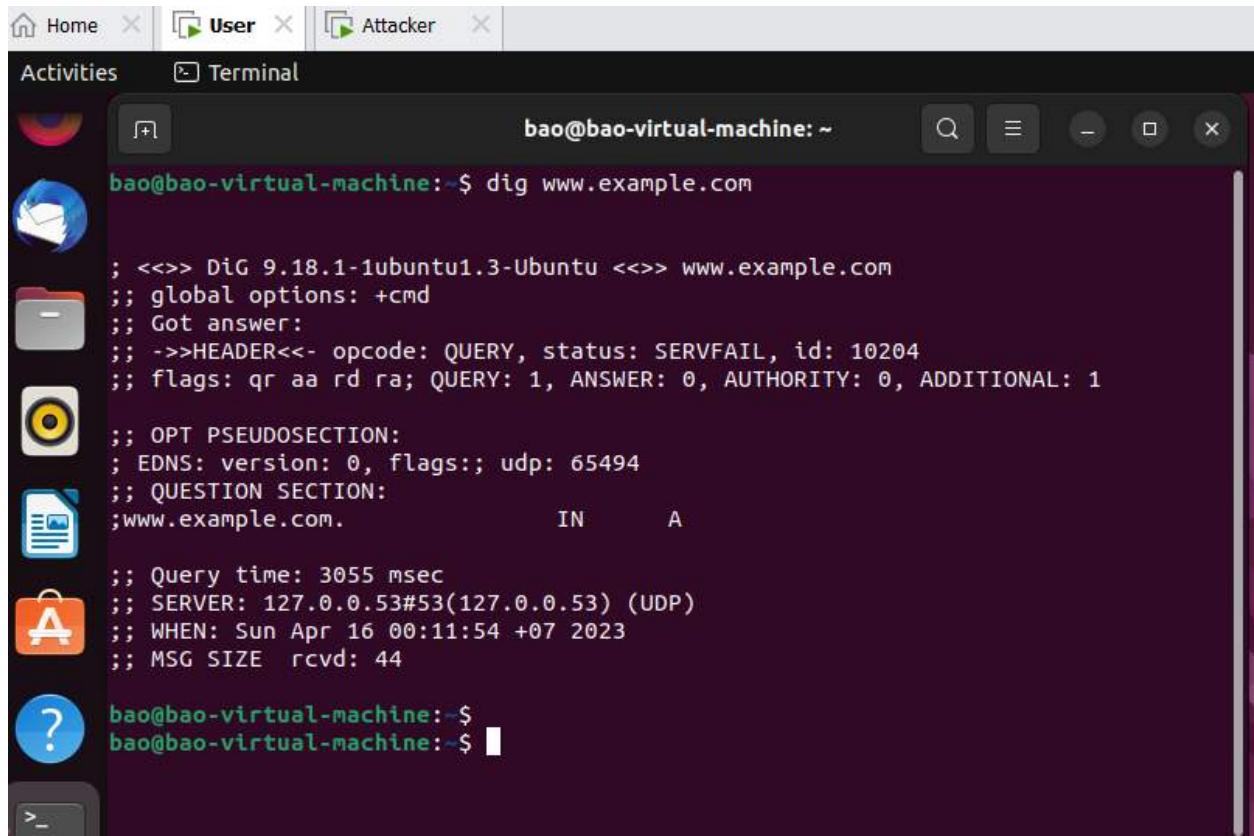
### 2.3. Attacker

Ta không cần cấu hình gì nhiều- chỉ đặt mỗi IP cho nó như mặc định của mô hình: 192.168.0.200





2.4. Ta sử dụng lệnh dig www.example.com trên máy User để xem một vài thông tin về domain www.example.com



The screenshot shows a Linux desktop environment with a terminal window open. The terminal window title is "User" and the command being run is "dig www.example.com". The output of the command is displayed in the terminal window, showing the DNS query process and the lack of an answer section.

```
bao@bao-virtual-machine:~$ dig www.example.com

; <>> DiG 9.18.1-1ubuntu1.3-Ubuntu <>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 10204
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.example.com.           IN      A

;; Query time: 3055 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Apr 16 00:11:54 +07 2023
;; MSG SIZE  rcvd: 44

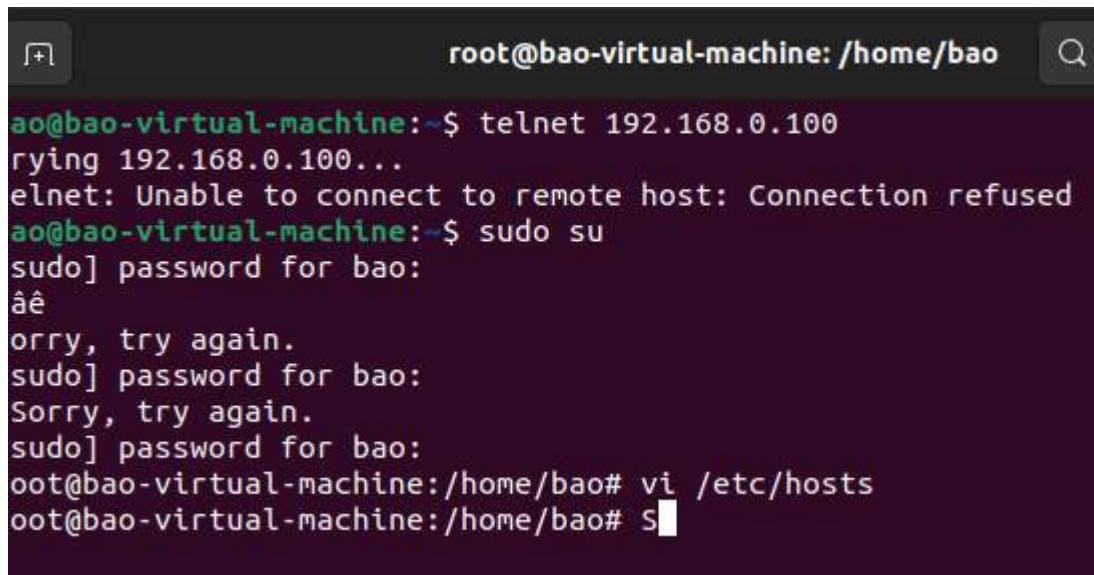
bao@bao-virtual-machine:~$
```

ANSWER SECTION chúa bảng ánh xạ DNS. Ví dụ www.example.com là 192.168.0.101

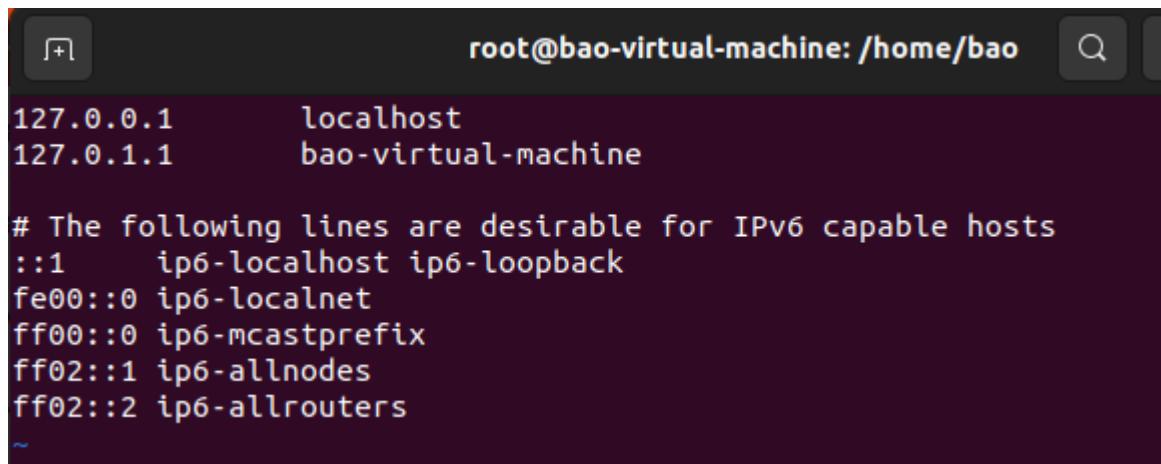
### 3.1. Attacker have already compromised the victim's machine

Trong tấn công này, attacker xâm nhập máy người dùng có quyền chỉnh sửa file/etc/host để chuyển hướng truy cập của người dùng đến địa chỉ độc hại

Ví dụ như trường hợp attacker có thể telnet đến máy user và có quyền chỉnh sửa file host đó.



```
root@bao-virtual-machine: /home/bao
ao@bao-virtual-machine:~$ telnet 192.168.0.100
trying 192.168.0.100...
telnet: Unable to connect to remote host: Connection refused
ao@bao-virtual-machine:~$ sudo su
[sudo] password for bao:
âè
Sorry, try again.
[sudo] password for bao:
Sorry, try again.
[sudo] password for bao:
root@bao-virtual-machine:/home/bao# vi /etc/hosts
root@bao-virtual-machine:/home/bao# S
```



```
root@bao-virtual-machine: /home/bao
127.0.0.1      localhost
127.0.1.1      bao-virtual-machine

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

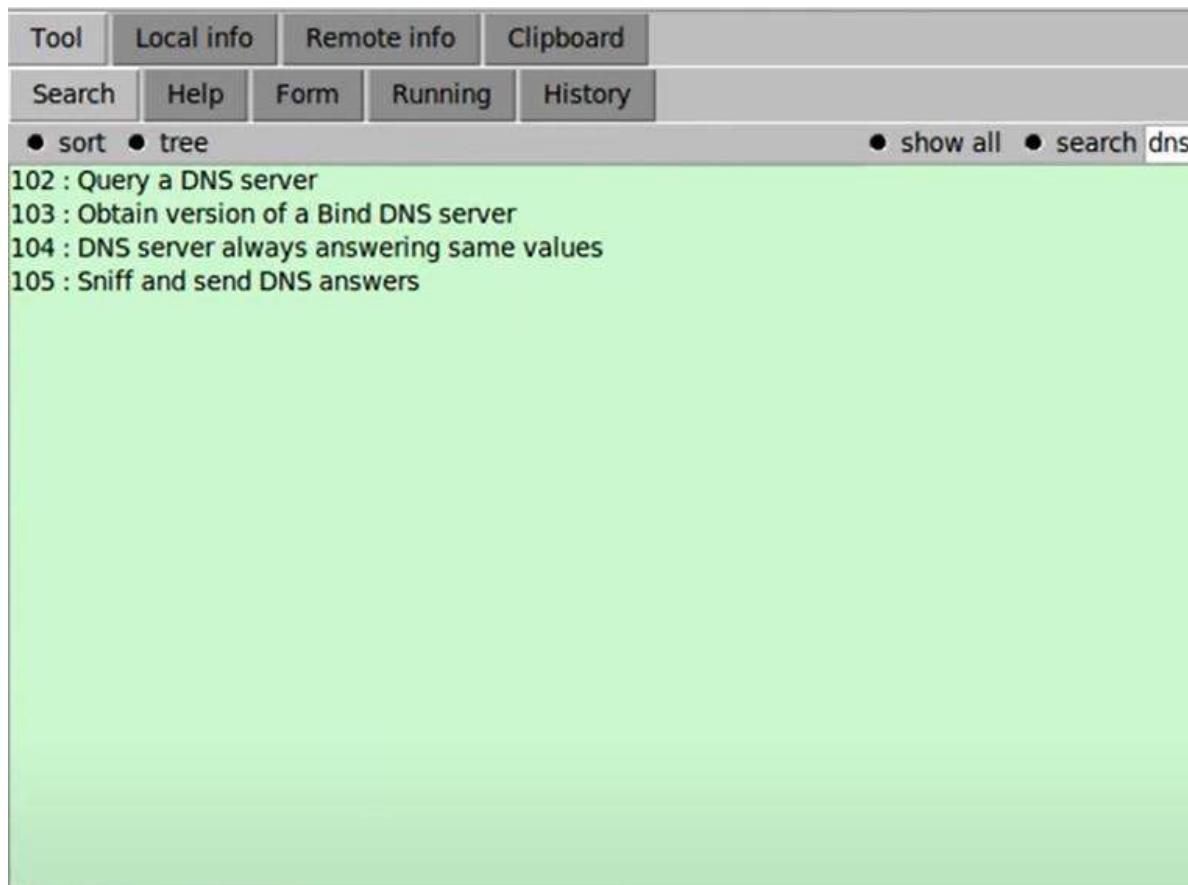
Attacker chuyển hướng tên miền www.example.com vốn được maping đến 192.168.0.101, thì đổi thành 192.168.0.200 www.example.com (địa chỉ Attacker)

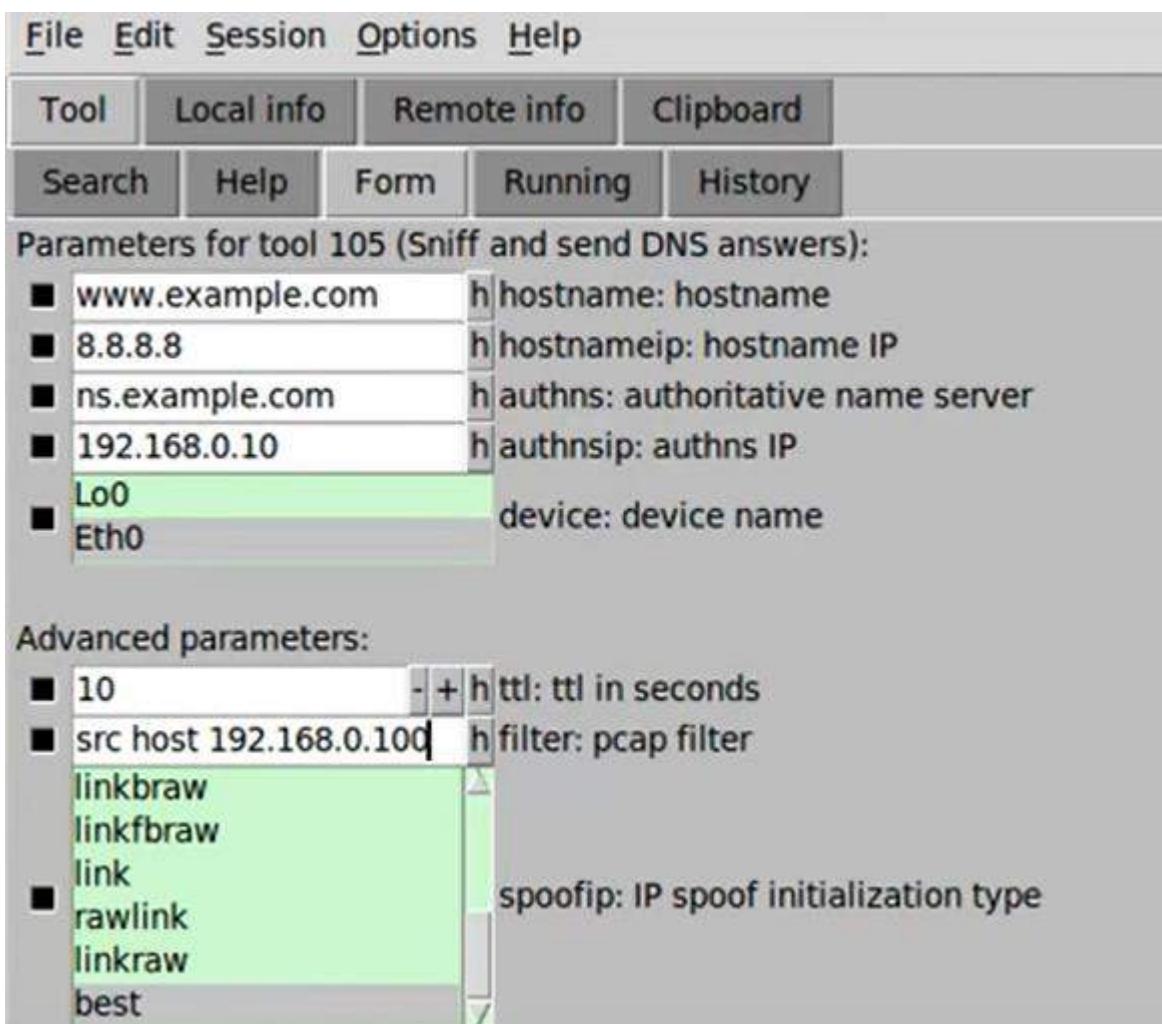
Đối với nslookup thì có vẻ nó không khả quang, như lệnh ping hoặc truy cập bằng web browser thì được

```
bao@bao-virtual-machine:~$  
bao@bao-virtual-machine:~$ nslookup  
> clear  
Server:      127.0.0.53  
Address:     127.0.0.53#53
```

### 3.2 Directly Spoof Response to User

Trong phần này, khi User truy vấn tên miền, thì nó sẽ gửi một gói tin DNS request đến DNS server. Lúc này, Attacker sniff được, lấy thông tin từ gói tin đó và giả mạo một gói tin phản hồi DNS response đáp ứng đầy đủ các yêu cầu của một gói DNS response thật, nhưng trong gói này Attacket đã đổi IP domain cần truy vấn thành IP độc hại của mình mong muốn.





Trong này, Attacker sử dụng công cụ Netwag để thực hiện điều này. Và trong trường hợp filter gõ src host <địa chỉ ip user> để chỉ tấn công mỗi ip user này

```

Command 105 --hostname "www.example.com" --hostnameip 8.8.8....:
DNS_question_____.  

| id=25304 rcode=OK      opcode=QUERY  

| aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=0  

| www.example.com. A  

|_____  

DNS_answer_____.  

| id=25304 rcode=OK      opcode=QUERY  

| aa=1 tr=0 rd=1 ra=1 quest=1 answer=1 auth=1 add=1  

| www.example.com. A  

| www.example.com. A 10 8.8.8.8  

| ns.example.com. NS 10 ns.example.com.  

| ns.example.com. A 10 192.168.0.10  

|_____  

DNS_question_____.  

| id=40708 rcode=OK      opcode=QUERY  

| aa=0 tr=0 rd=1 ra=0 quest=1 answer=0 auth=0 add=0  

| daisy.ubuntu.com. A  

|_____

```

### 3.3 DNS server Cache Poisoning

Trong phần tấn công, Attacker tấn công vào máy server thay vì máy người dùng để đạt hiệu quả. Vì khi user truy vấn 1 tên miền không nằm trong DNS server (Apollo), thì DNS server này sẽ truy vấn một Root DNS server ở a nằm ngoài mạng local. Lợi dụng điểm này, Attacker sẽ gửi một tin giả mạo đến DNS server trước khi gói tin từ Root DNS server phản hồi về sẽ giống như tấn công ở Task 2 nhưng lần này nhắm vào DNS server.

Cuộc tấn công này sẽ lâu dài, vì kết quả của gói tin giả mạo sẽ được lưu trên DNS cache của server. Từ đó, mà nhiều user khi truy cập tên miền đó thông qua DNS server sẽ cũng bị ảnh hưởng.

Trước khi làm phần này nên config một số thứ bên DNS server để các máy mà thiết lập DNS đến server 192.168.0.10 đều có thể truy vấn được

### Cấu hình của forwarding DNS server

Bên máy user và attacker thì trong file /ect/resolv.còn phải chỉ ra nameserver 192.168.1.10 – là địa chỉ của DNS server

Giờ thì truy cập thử bằng nslookup trên máy user. User đã truy xuất thành công và tiếp tục trên attacker sẽ tấn công vào DNS server.

# ĐỘ AN TOÀN CỦA HỆ CHỮ KÝ ELGAMAL

## I. Hệ chữ ký Elgamal là gì?

### 1.1 Tổng quan

- Hệ chữ ký ElGamal được xây dựng trên nền tảng hệ mã khóa công khai ElGamal và sử dụng cùng một bộ khóa công khai và khóa bí mật. Hệ mã khóa công khai ElGamal sử dụng tính toán đường cong Elliptic (ECC) để mã hóa và giải mã thông điệp.
- Hệ chữ ký ElGamal hoạt động bằng cách sử dụng một cặp khóa: khóa riêng (private key) và khóa công khai (public key). Khóa riêng được sử dụng để ký và khóa công khai được sử dụng để xác minh chữ ký. Các bước để tạo và xác minh một chữ ký ElGamal bao gồm:
  - + Tạo khóa: Người dùng tạo cặp khóa ElGamal (khóa riêng và khóa công khai).
  - + Ký thông điệp: Người dùng sử dụng khóa riêng để tạo chữ ký cho thông điệp.
  - + Xác minh chữ ký: Người nhận sử dụng khóa công khai của người ký để xác minh tính hợp lệ của chữ ký.
- Hệ chữ ký ElGamal được sử dụng rộng rãi trong các ứng dụng an ninh mạng để bảo vệ tính toàn vẹn và độ tin cậy của các thông điệp và giao dịch truyền qua mạng.

### 1.2 So sánh với các hệ mã hóa khác

- RSA: là một trong những thuật toán mã hóa khóa công khai được sử dụng phổ biến. RSA có tốc độ xử lý cao hơn hệ ElGamal, tuy nhiên cùng một kích thước khóa, RSA yêu cầu số bit đầu vào lớn hơn làm tăng chi phí lưu trữ khóa.
- Diffie-Hellman: là một thuật toán trao đổi khóa được sử dụng để thiết lập một khóa chung giữa hai bên trong hệ mã hóa khóa công khai, tương tự như hệ ElGamal. Tuy nhiên, hệ ElGamal có khả năng chống lại tấn công theo kiểu sinh tử mạnh hơn hệ Diffie-Hellman.
- ECC: là một hệ mã hóa khóa công khai mới, có thể sử dụng khóa ngắn hơn so với RSA hoặc ElGamal với cùng mức độ bảo mật. Hệ mã hóa này cũng cung cấp khả năng bảo mật cao hơn khi sử dụng khóa ngắn hơn.

## II. Cách tạo chữ ký số trong hệ thống ElGamal

### 2.1 Tạo khóa

- Chọn  $p$  là 1 số nguyên tố rất lớn ( $>1024$  bit) và giá trị khởi tạo  $g$ .
- Chọn một số nguyên  $x$  làm khóa bí mật, sử dụng để kí với  $0 < x < p$
- Tính giá trị  $y = g^x \text{ mod } p$
- Ta sẽ có cặp khóa là: Public key ( $p, g, y$ ) và Private key ( $x$ )

Sau khi có cặp khóa, người dùng có thể sử dụng khóa riêng để ký các thông điệp và khóa công khai để xác minh chữ ký.

### 2.2 Tạo chữ ký

Người dùng muốn ký một thông điệp message sẽ thực hiện các bước sau :

- Nhập thông điệp là message, chuyển đổi message về dạng chuỗi thập lục phân và sử dụng băm.
- Chọn một số ngẫu nhiên  $k$ , với  $0 < k < p - 1$
- Tính  $r = g^k \text{ mod } p$ .
- Tính  $s = (\text{message} - x^k r) * k^{-1} \text{ mod } (p-1)$ .
- ⇒ Chữ ký là cặp  $(r, s)$ .

### 2.3 Xác minh chữ ký

Người nhận thông điệp đã băm là message và chữ ký sẽ thực hiện các bước sau để xác minh chữ ký :

- Tính  $v1 = g^{\text{message}} \text{ mod } p$ .
- Tính  $v2 = (y^r \text{ mod } p) * ((r^s \text{ mod } p) \text{ mod } p)$ .
- ⇒ Nếu  $v1 = v2$ , chữ ký được xác minh là hợp lệ.

### III. Demo

The screenshot shows the Spyder Python 3.9 IDE interface. On the left, there are two code editors: one for `demoelgamal.py` and another for `signature.py`. The `demoelgamal.py` editor contains the ElGamal encryption code. The right side of the interface features a "Usage" help window, a "Console" tab with a command-line interface, and a "Python console" tab where a message was decrypted.

```

# demoelgamal.py
# generate key & signature
# g = 2
# p = random(1,p-1)
# ElGamal
# V = pow(g,A,p)
# public_key = (A,V)
# private_key = A
# K = random(1,p-1)
# K = pow(g,A,K)
# K = (public_key, private_key)
# (public_key, private_key)

# sign(x, private_key, public_key):
#   p, g, A = public_key
#   x, k = private_key
#   r = random(1,p-1)
#   r = pow(g,k,p)
#   return r

# ElGamal is ham tinh nganh doi modulo
# y = (pow(x,r,p) * pow(r,s,p)) % p
# signature = (r, s)
# return signature

# verify(x, signature, public_key):
#   p, g, A = public_key
#   r, s = signature
#   if pow(x,A,p) == (pow(x,r,p) * pow(r,s,p)) % p:
#     return True
#   else:
#     return False

# public_key, private_key = generate_keys()
# message = "Tôi là Lê Thị Bảo Yến"
# print("Thông điệp gốc:", message)
# message = message.encode()
# m = int.from_bytes(message.encode(), 'big')
# m2 = m | 1
# signature = sign(m, private_key, public_key)
# message2 = input("Nhập thông điệp xác minh: ")
# message2 = bytes.fromhex(message2).decode('utf-8').encode()
# h = digest(m2, message2)
# if verify(m2, signature, public_key):
#   print("Thúy Anh hợp lệ")
# else:
#   print("Thúy Anh không hợp lệ")

```

In [6]: `runfile('C:/Users/Yuta/.spyder-py3/demoelgamal.py', wdir='C:/Users/Yuta/.spyder-py3')`  
Thông điệp gốc: Lê Thị Bảo Yến  
Nhập thông điệp xác minh: Lê Thị Bảo Yến  
Chữ ký không hợp lệ

In [7]: `runfile('C:/Users/Yuta/.spyder-py3/demoelgamal.py', wdir='C:/Users/Yuta/.spyder-py3')`  
Thông điệp gốc: Lê Thị Bảo Yến  
Nhập thông điệp xác minh: Lê Thị Bảo Yến  
Chữ ký hợp lệ

In [8]: