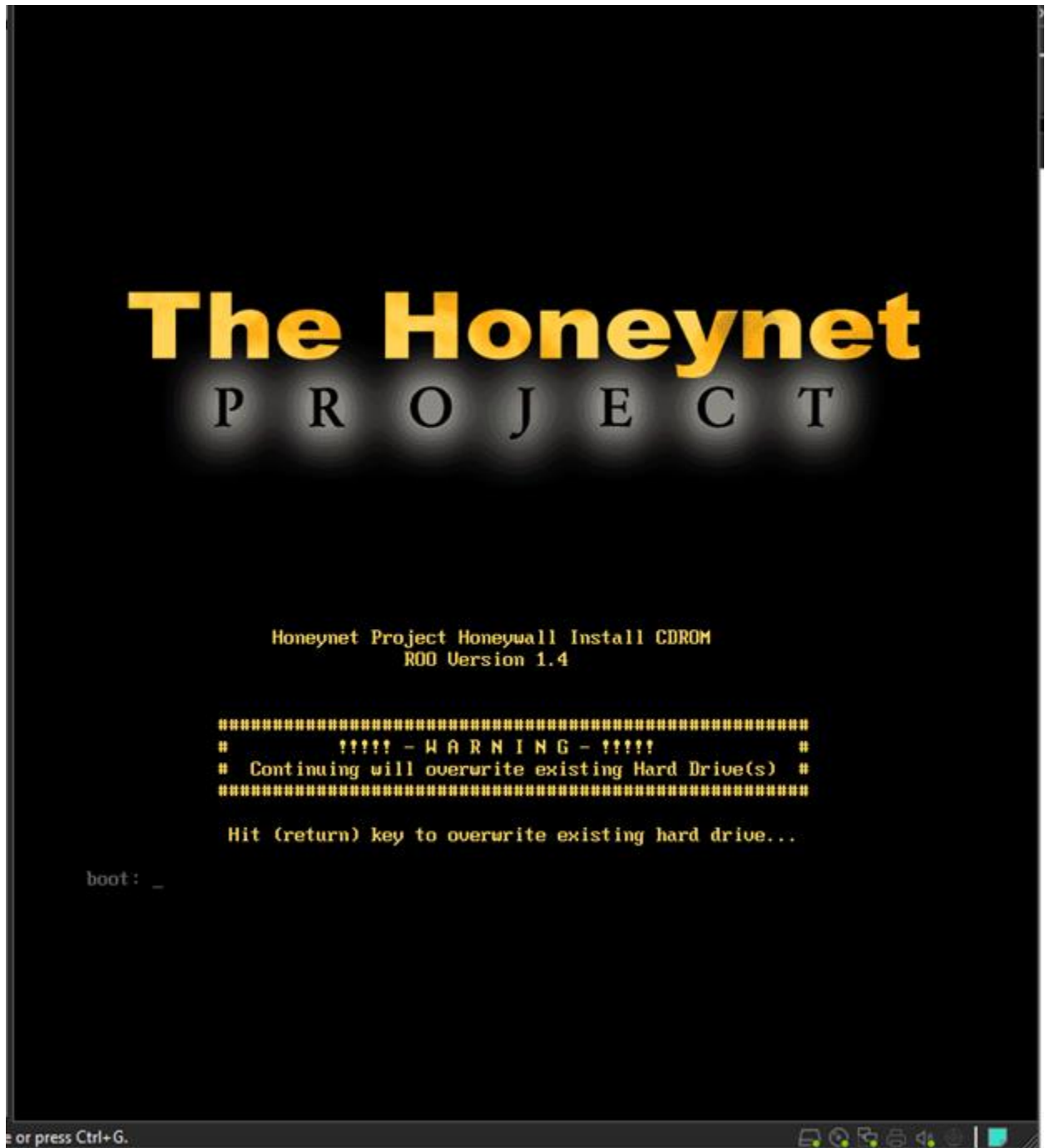


Bài 1: Triển khai honeynet sử dụng honeywall

a) Cài đặt máy ảo honeywall



Welcome to CentOS

Package Installation

Name : ghostscript-fonts-5.50-13.1.1-noarch
Size : 1466k
Summary: Fonts for the Ghostscript PostScript(TM)
interpreter.

100%

	Packages	Bytes	Time
Total :	366	628M	0:00:54
Completed:	192	277M	0:00:24
Remaining:	174	351M	0:00:30

44%

<Tab>/<Alt-Tab> between elements ; <Space> selects ; <F12> next screen

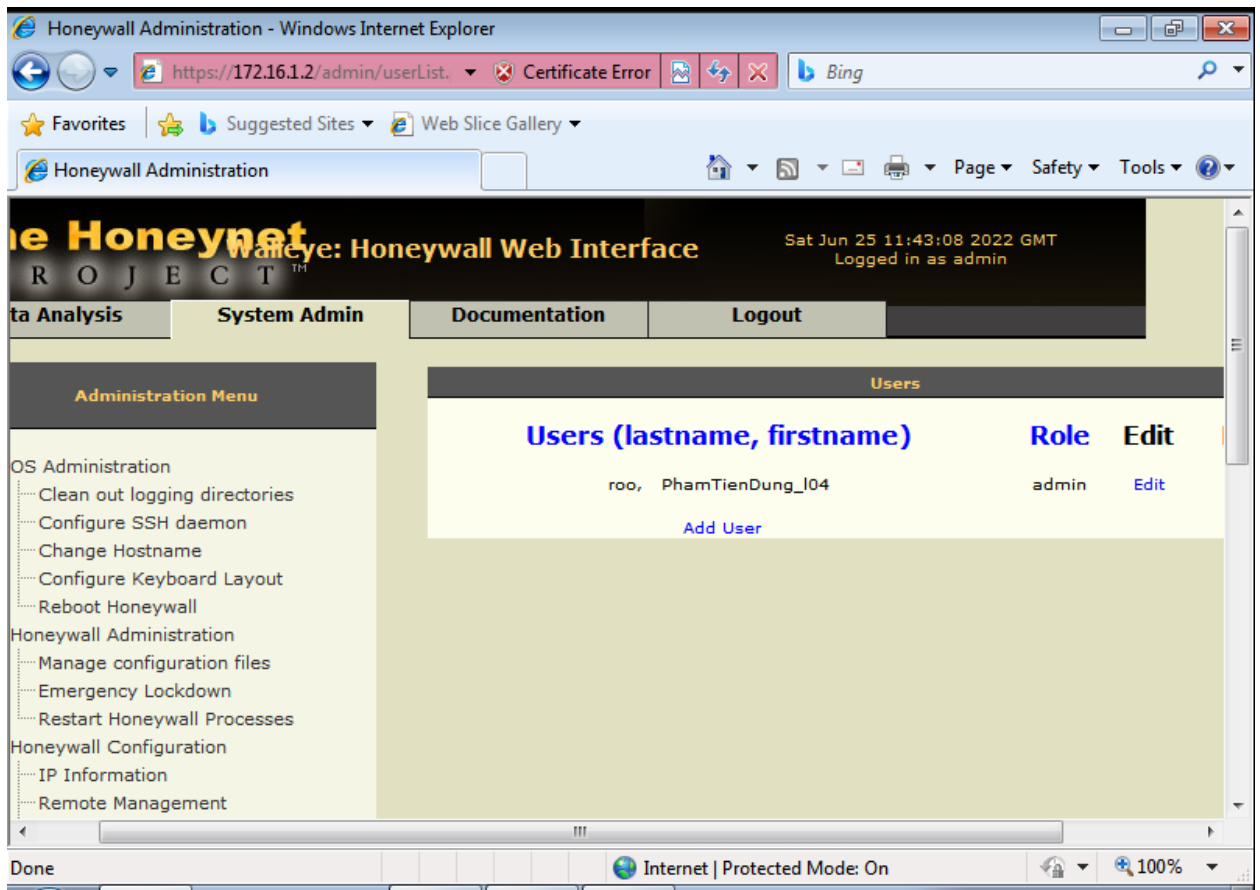
```
UP BROADCAST RUNNING NOARP MULTICAST MTU:1500 Metric:1
RX packets:423 errors:0 dropped:0 overruns:0 frame:0
TX packets:1543 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:57620 (56.2 KiB) TX bytes:204680 (199.8 KiB)
Interrupt:59 Base address:0x2000

eth2    Link encap:Ethernet HWaddr 00:0C:29:70:88:63
        inet addr:172.16.1.2 Bcast:172.16.1.255 Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
        RX packets:1447 errors:0 dropped:0 overruns:0 frame:0
        TX packets:570 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:173715 (169.6 KiB) TX bytes:310425 (303.1 KiB)
        Interrupt:67 Base address:0x2400

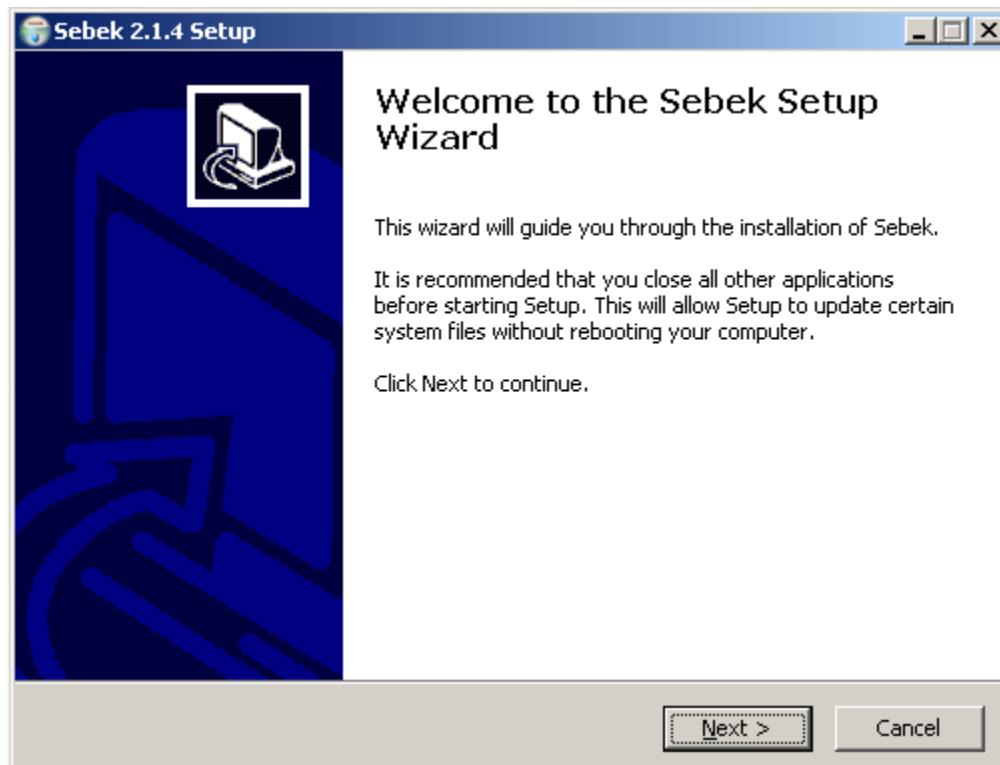
lo      Link encap:Local Loopback
        inet addr:127.0.0.1 Mask:255.0.0.0
        UP LOOPBACK RUNNING MTU:16436 Metric:1
        RX packets:20 errors:0 dropped:0 overruns:0 frame:0
        TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:1512 (1.4 KiB) TX bytes:1512 (1.4 KiB)

[root@ATTT ~]#
```

- b) Quản trị Honeywall với tài khoản quản trị là: “tên sinh viên”_“tên lớp”



c) Cài đặt sebek client



Sebek Configuration Wizard - Welcome [X]



Welcome to the Sebek Configuration Wizard.

This wizard helps you create a configuration for Sebek. With this wizard you will:


- Select a Destination MAC, IP Address, and Port
- Select a magic value used to hide the data sebek generates.
- Select a network interface to send the recorded data on.
- Select the name of the process that will have access to the Sebek driver.

< Back **Next >** Cancel Help

Sebek Configuration Wizard - Server Configuration [X]

Server Configuration

Sebek logs all data it collects to a central server. Please specify the information sebek will use to generate packets the server can collect.



This field specifies the MAC address to use for all outgoing packets. If the logging server is more than one hop away from the honeypot, then the Destination MAC should be set to the MAC of the default gateway for this network.

Destination MAC: 00 : 20 : ED : 70 : 35 : 68

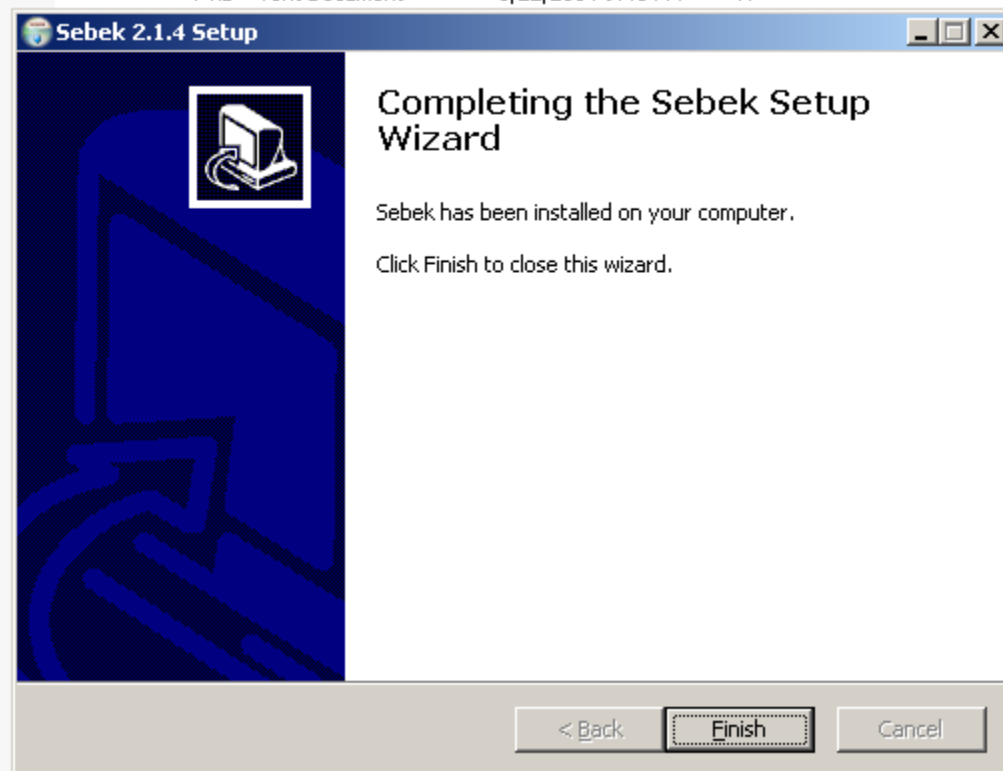
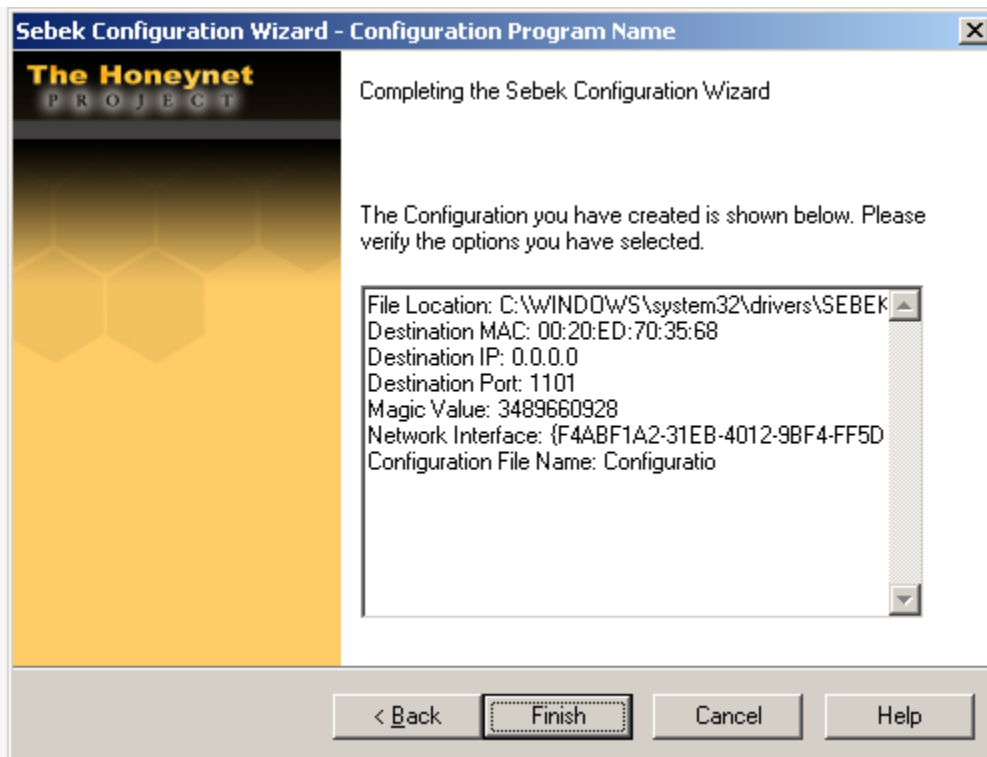
This field defines the IP address used in all the packets generated by Sebek. Since the Sebek server does not look at the Destination IP address when it collects packets, it is not required nor recommended to set this to IP of the Sebek server.

Destination IP: 0 . 0 . 0 . 0

This field defines the UDP destination port to be configured in the Sebek packets. This value is used by the Server to identify packets of interest.

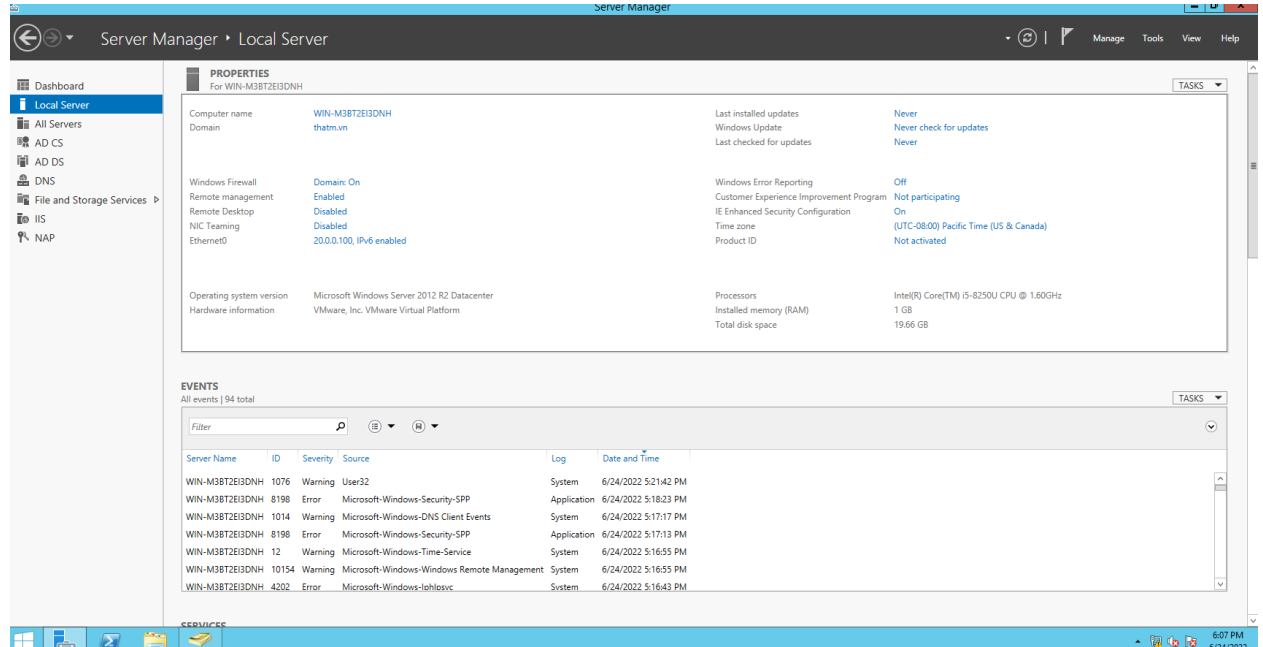
Destination Port: 1101

< Back **Next >** Cancel Help

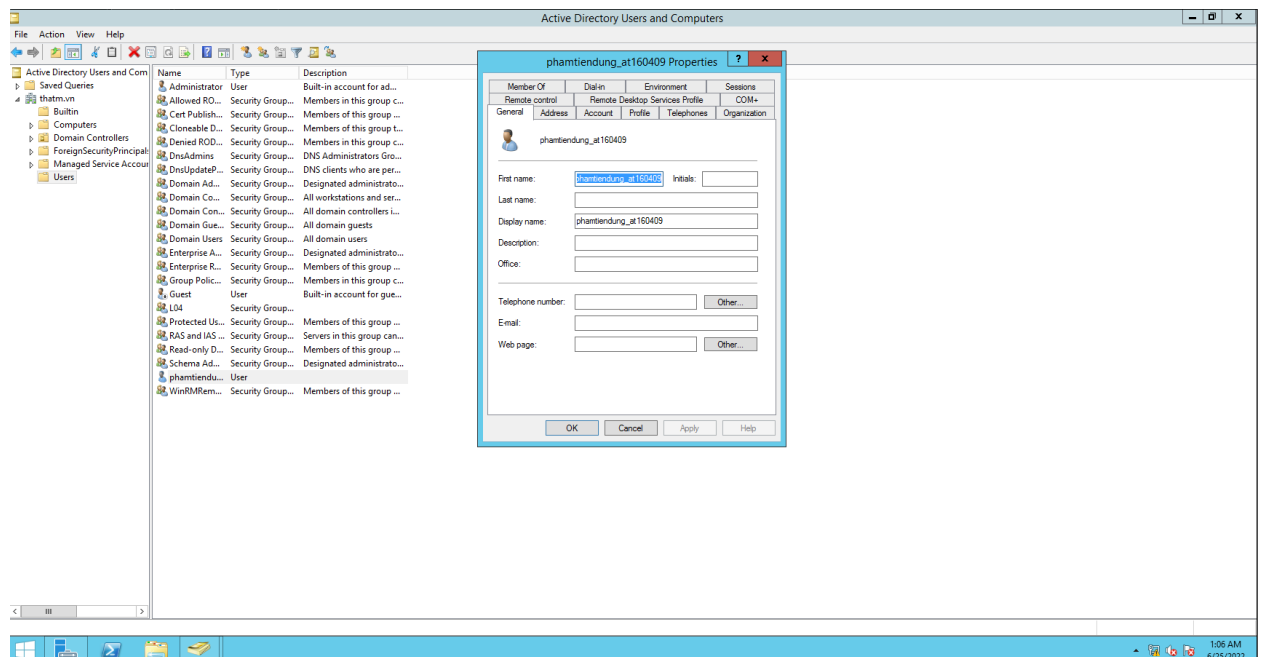


Bài 2: Triển khai mạng riêng ảo VPN SSTP

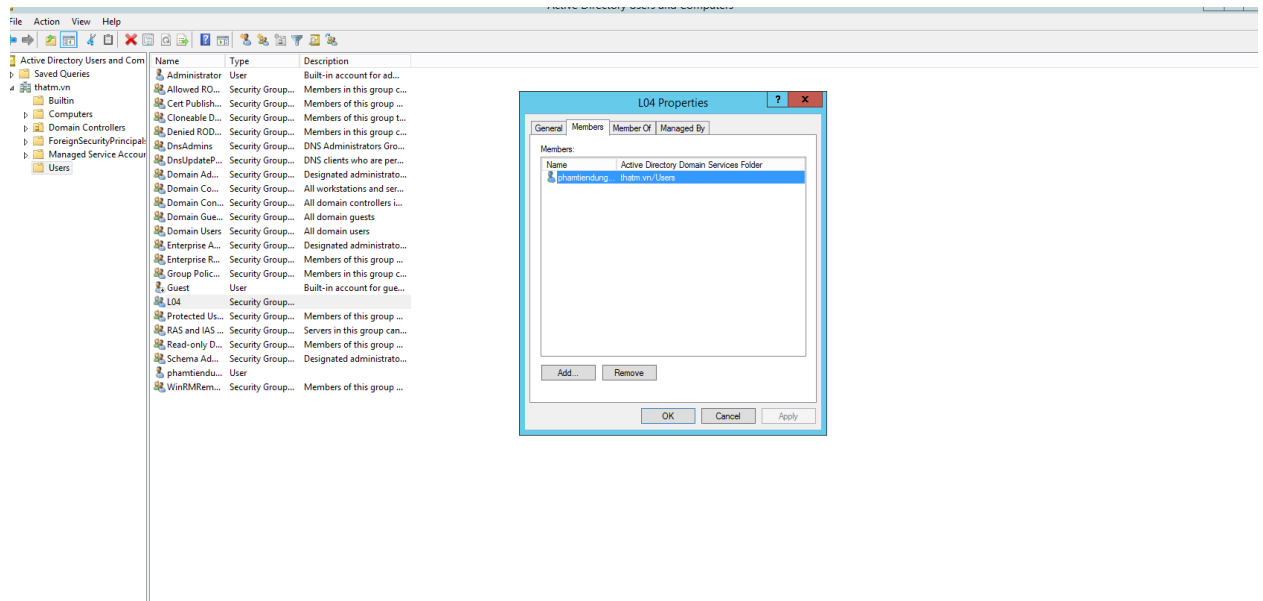
Nâng cấp domain



Tạo Tài khoản VPN:



Tạo nhóm L04:

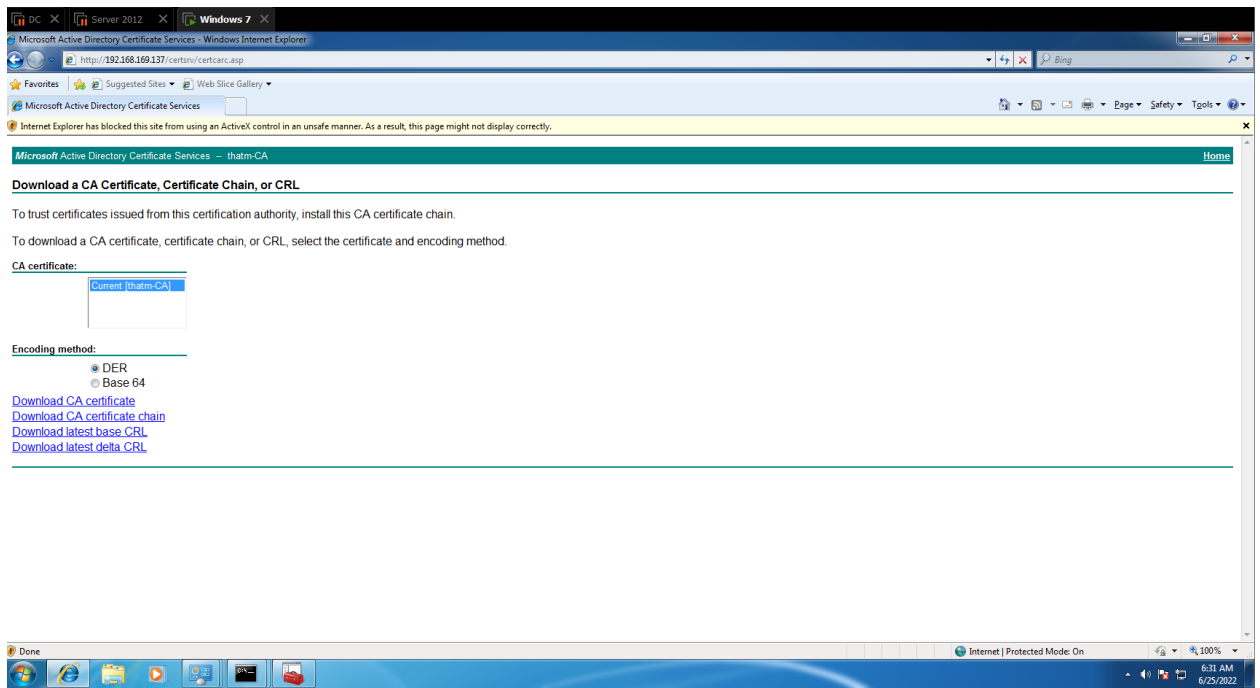


User và Group trong tham.vn

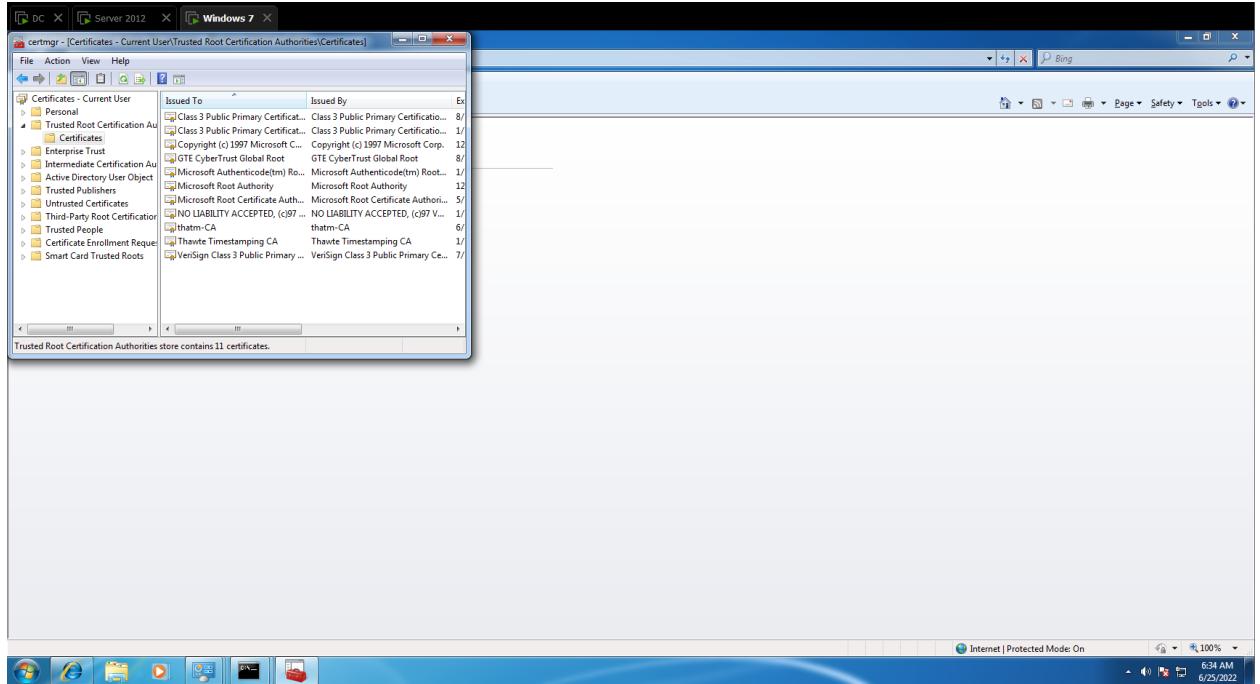
	Name	Type	Description
Active Directory Users and Computers	Administrator	User	Built-in account for ad...
Saved Queries	Allowed RO...	Security Group...	Members in this group c...
thatm.vn	Cert Publish...	Security Group...	Members of this group ...
Builtin	Cloneable D...	Security Group...	Members of this group t...
Computers	Denied ROD...	Security Group...	Members in this group c...
Domain Controllers	DnsAdmins	Security Group...	DNS Administrators Gro...
ForeignSecurityPrincipal	DnsUpdateP...	Security Group...	DNS clients who are per...
Managed Service Accounts	Domain Ad...	Security Group...	Designated administrato...
Users	Domain Co...	Security Group...	All workstations and ser...
	Domain Con...	Security Group...	All domain controllers i...
	Domain Gue...	Security Group...	All domain guests
	Domain Users	Security Group...	All domain users
	Enterprise A...	Security Group...	Designated administrato...
	Enterprise R...	Security Group...	Members of this group ...
	Group Polic...	Security Group...	Members in this group c...
	Guest	User	Built-in account for gue...
	L04	Security Group...	
	nguyenvanh...	User	
	Protected Us...	Security Group...	Members of this group ...
	RAS and IAS ...	Security Group...	Servers in this group can...
	Read-only D...	Security Group...	Members of this group ...
	Schema Ad...	Security Group...	Designated administrato...
	WinRMRem...	Security Group...	Members of this group ...

Cấp phát chứng thư CA trong window :

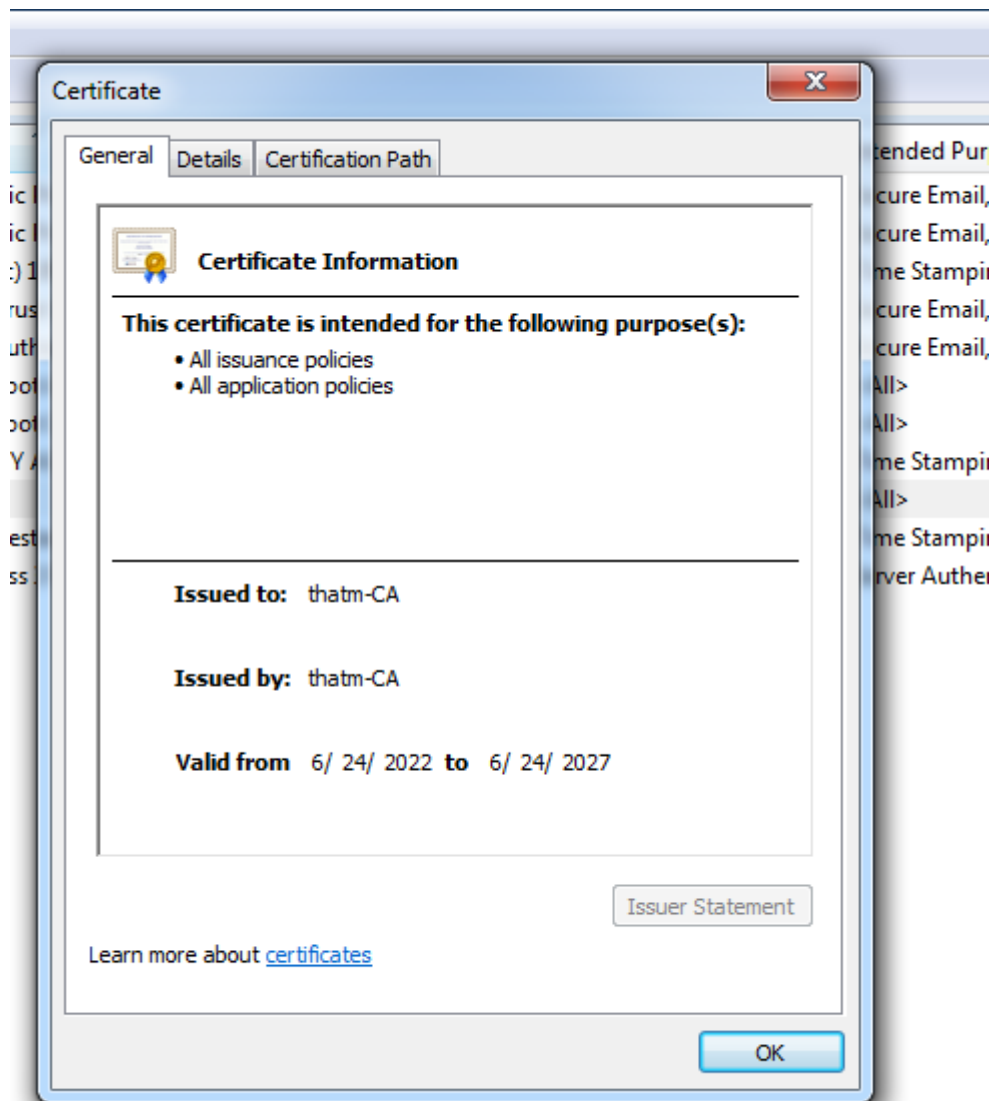
Tải chứng thư trên giao diện web <http://192.168.169.137/certsrv>



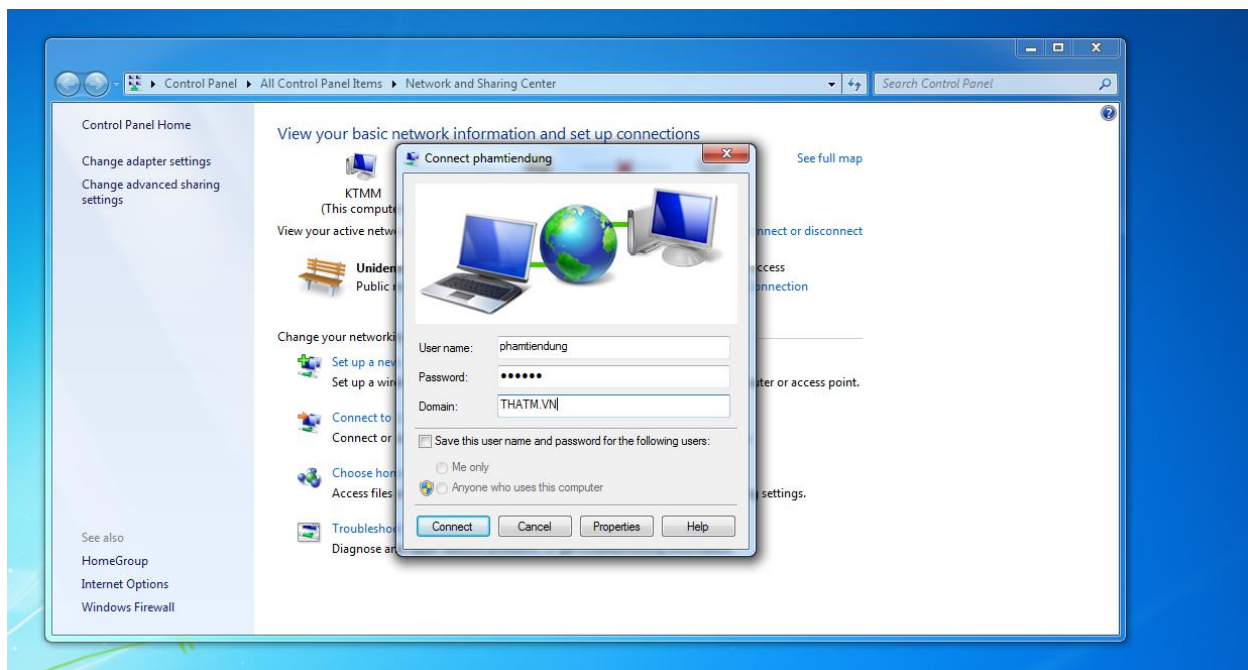
Chứng thi tham CA từ web <http://192.168.169.137/certsrv> đã lưu vào máy



Giới thiệu Chứng thư thatm-CA và năm hết hạn



Kết nối tài khoản vpn đến domain:



Kết nối thành công

– Tại máy Windows 7 thực hiện Ping tới máy chủ DC

```
C:\Users\admin>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time=2ms TTL=127
Reply from 172.16.1.2: bytes=32 time=2ms TTL=127
Reply from 172.16.1.2: bytes=32 time=2ms TTL=127
Reply from 172.16.1.2: bytes=32 time=2ms TTL=127
```

Truy cập vào tài nguyên chia sẻ của máy chủ DC

