??:OSSLab thx

??EPS ?? ?Windows 2000 ,2003 Sever , XP ,7 ,Vista ??? (????? ,2008??)

Windows ????????????? SAM HKEY_LOCAL_MACHINE\SAM ??????????
????Ntfs ?????os ???,?? Offline nt ??windows sam????
??????AD? ,????.

???????????????SAM ??????????????.

??????? ?????? VHD image file +??? ????????

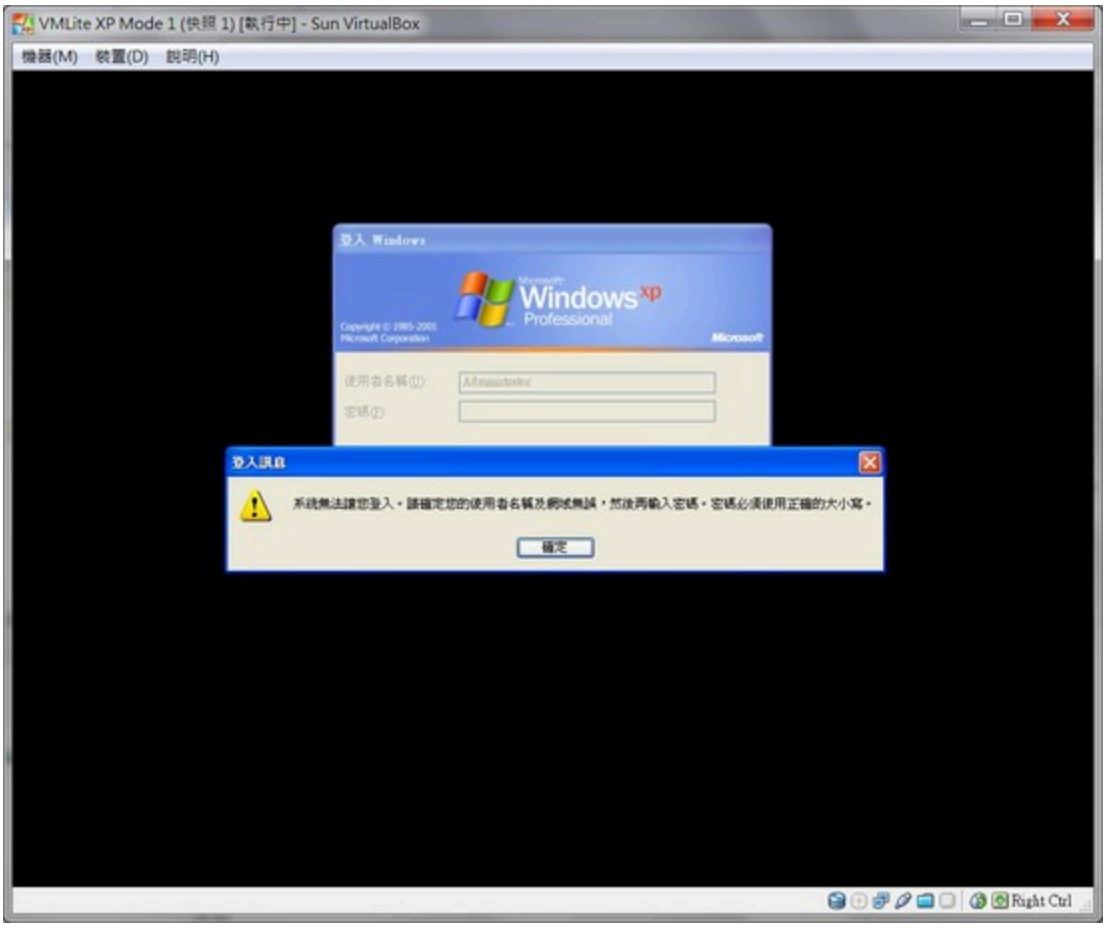
????.

1.http://ophcrack.sourceforge.net/
2.http://jay-fva.blogspot.com/2009/12/...nistrator.html

??:
??? ultimate CD ISO 5.0rc 1 ?

??????? ?? XP mode ??,??? VHD file ,

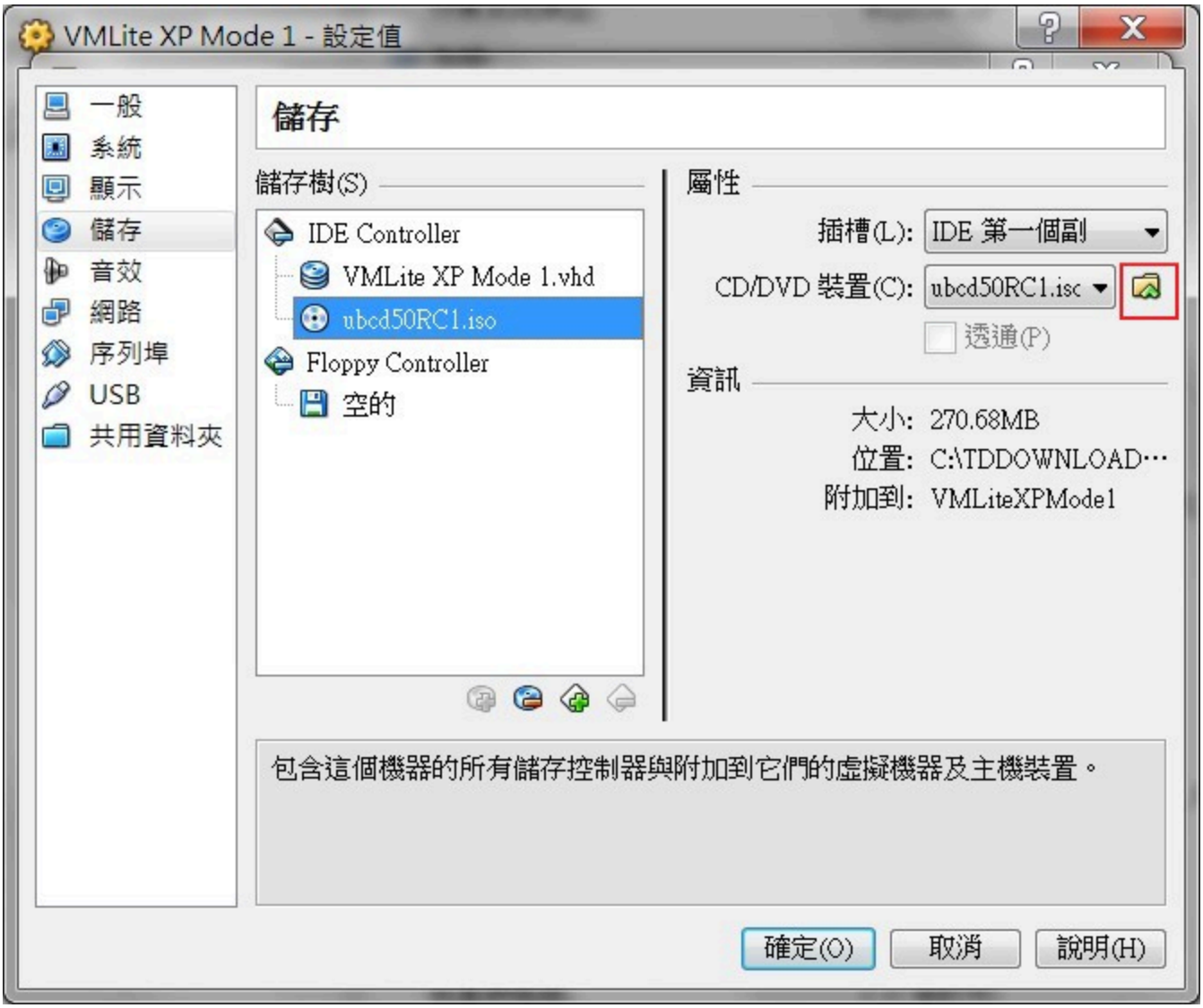
??? XP VM VHD in Virtualbox
??XP mode ?VM ??administrator ???????



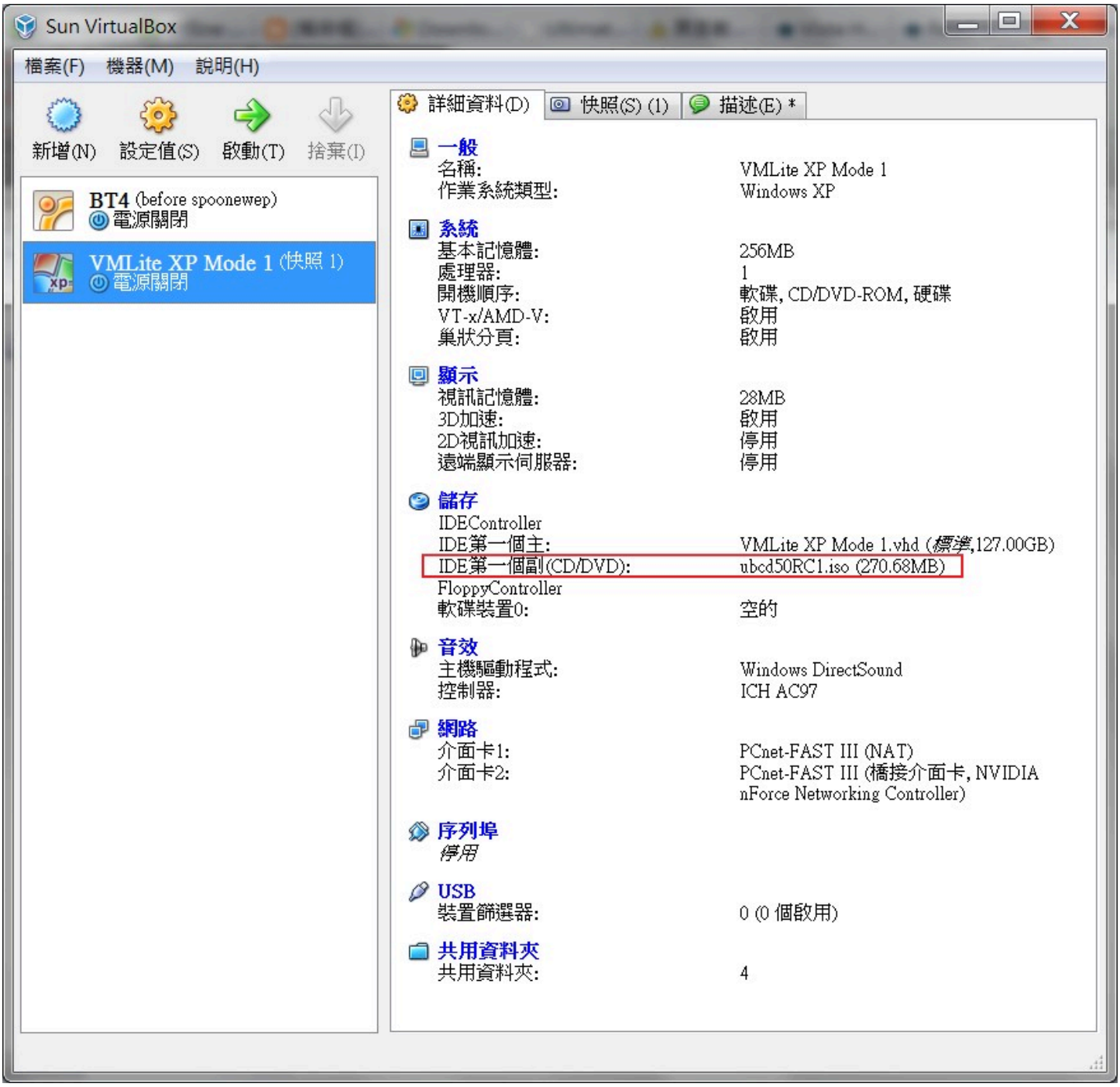
????????

?virtualbox?????? ?????

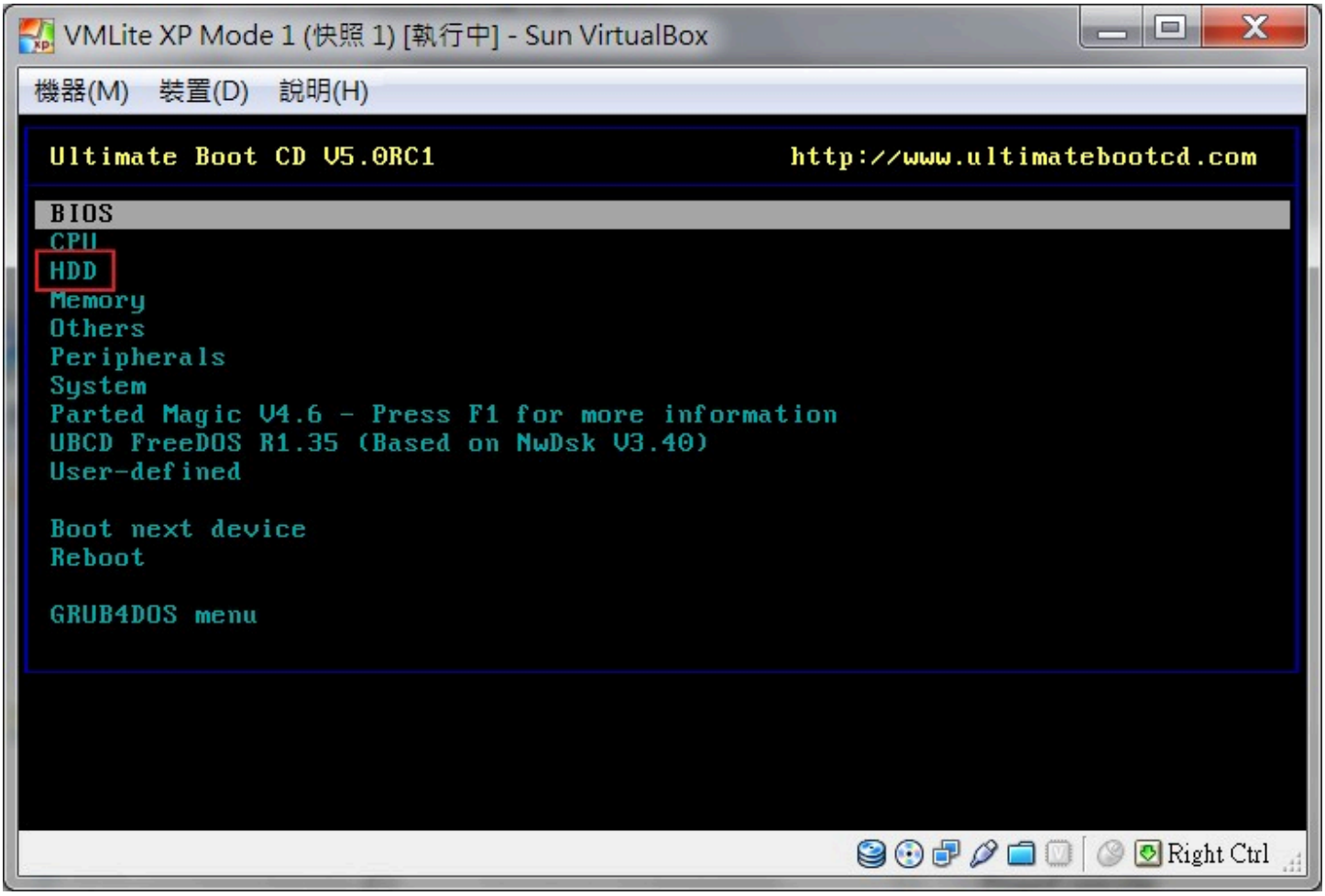
1.??????? ubcd5rc1?iso?.


VMLite XP Mode 1 - 設定值
一般
系統
顯示
儲存
音效
網路
序列埠
USB
共用資料夾
儲存
儲存樹(S)
IDE Controller
VMLite XP Mode 1.vhd
ubcd50RC1.iso
Floppy Controller
空的
屬性
插槽(L): IDE 第一個副
CD/DVD 裝置(C): ubcd50RC1.isc
透通(P)
資訊
大小: 270.68MB
位置: C:\TDDOWNLOAD…
附加到: VMLiteXPMode1
包含這個機器的所有儲存控制器與附加到它們的虛擬機器及主機裝置。
確定(O)
取消
說明(H)

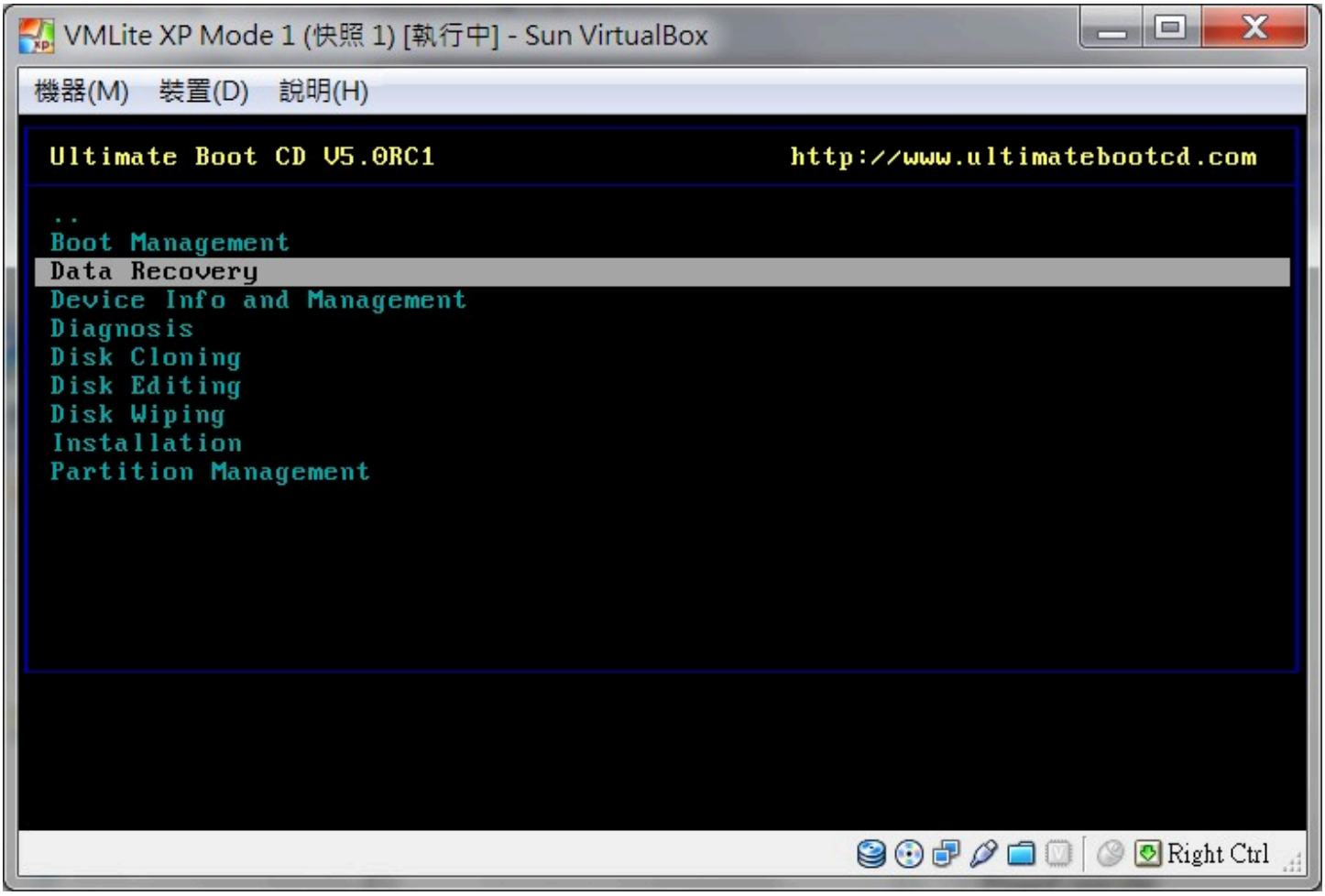
??????????iso????


Sun VirtualBox
檔案(F) 機器(M) 說明(H)
新增(N) 設定值(S) 啟動(T) 捨棄(I)
BT4 (before spoonewep)
電源關閉
VMLite XP Mode 1 (快照 1)
電源關閉
詳細資料(D) 快照(S) (1) 描述(E) *
一般
名稱: VMLite XP Mode 1
作業系統類型: Windows XP
系統
基本記憶體: 256MB
處理器: 1
開機順序: 軟碟, CD/DVD-ROM, 硬碟
VT-x/AMD-V: 啟用
巢狀分頁: 啟用
顯示
視訊記憶體: 28MB
3D加速: 啟用
2D視訊加速: 停用
遠端顯示伺服器: 停用
儲存
IDEController
IDE第一個主: VMLite XP Mode 1.vhd (標準,127.00GB)
IDE第一個副(CD/DVD): ubcd50RC1.iso (270.68MB)
FloppyController
軟碟裝置0: 空的
音效
主機驅動程式: Windows DirectSound
控制器: ICH AC97
網路
介面卡1: PCnet-FAST III (NAT)
介面卡2: PCnet-FAST III (橋接介面卡, NVIDIA nForce Networking Controller)
序列埠
停用
USB
裝置篩選器: 0 (0 個啟用)
共用資料夾
共用資料夾: 4

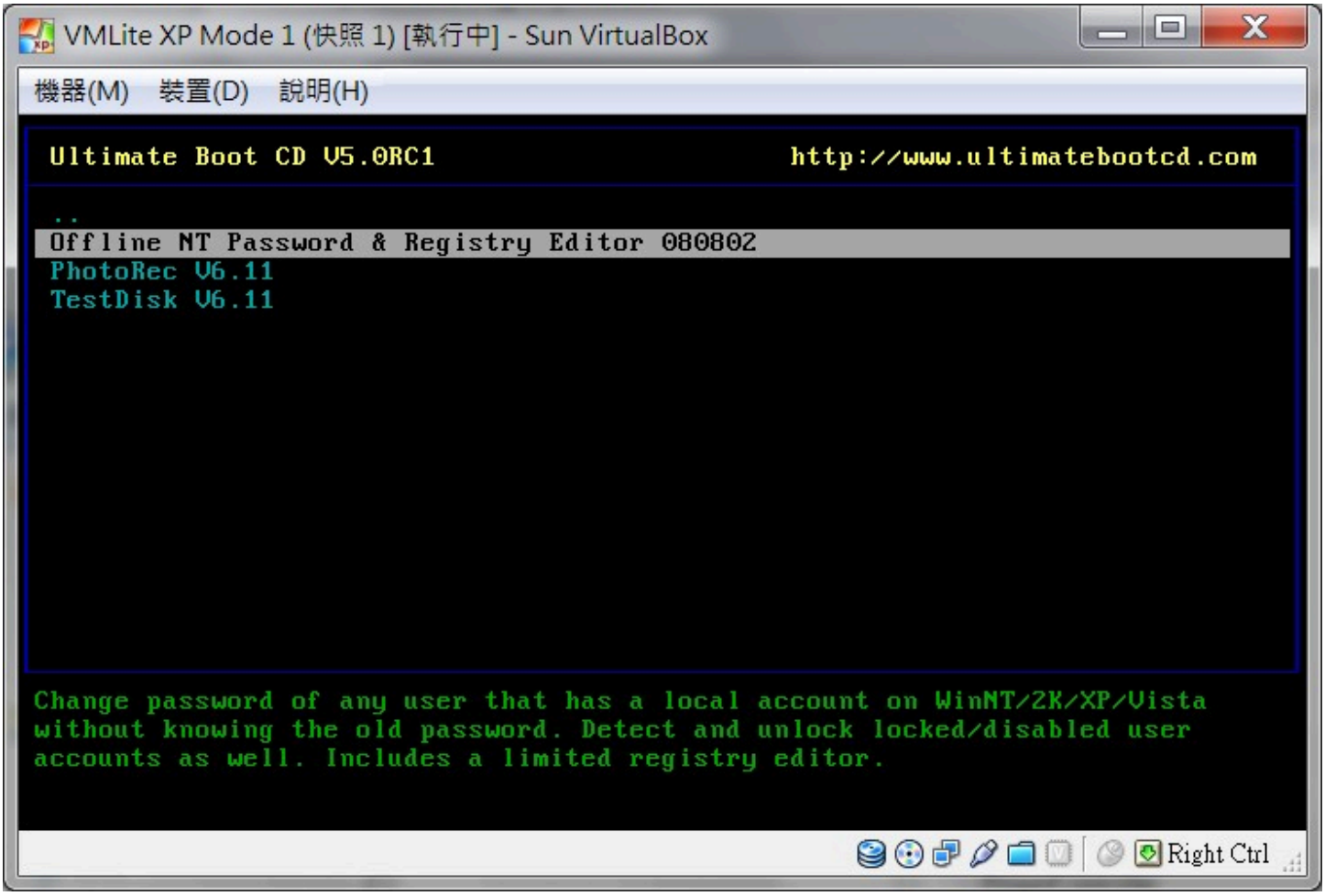
?????ISO????????????iso???????????????F12???


VMLite XP Mode 1 (快照 1) [執行中] - Sun VirtualBox
機器(M) 裝置(D) 說明(H)
Ultimate Boot CD V5.0RC1 http://www.ultimatebootcd.com
BIOS
CPU
HDD
Memory
Others
Peripherals
System
Parted Magic V4.6 - Press F1 for more information
UBCD FreeDOS R1.35 (Based on NwDsk V3.40)
User-defined
Boot next device
Reboot
GRUB4DOS menu
Right Ctrl

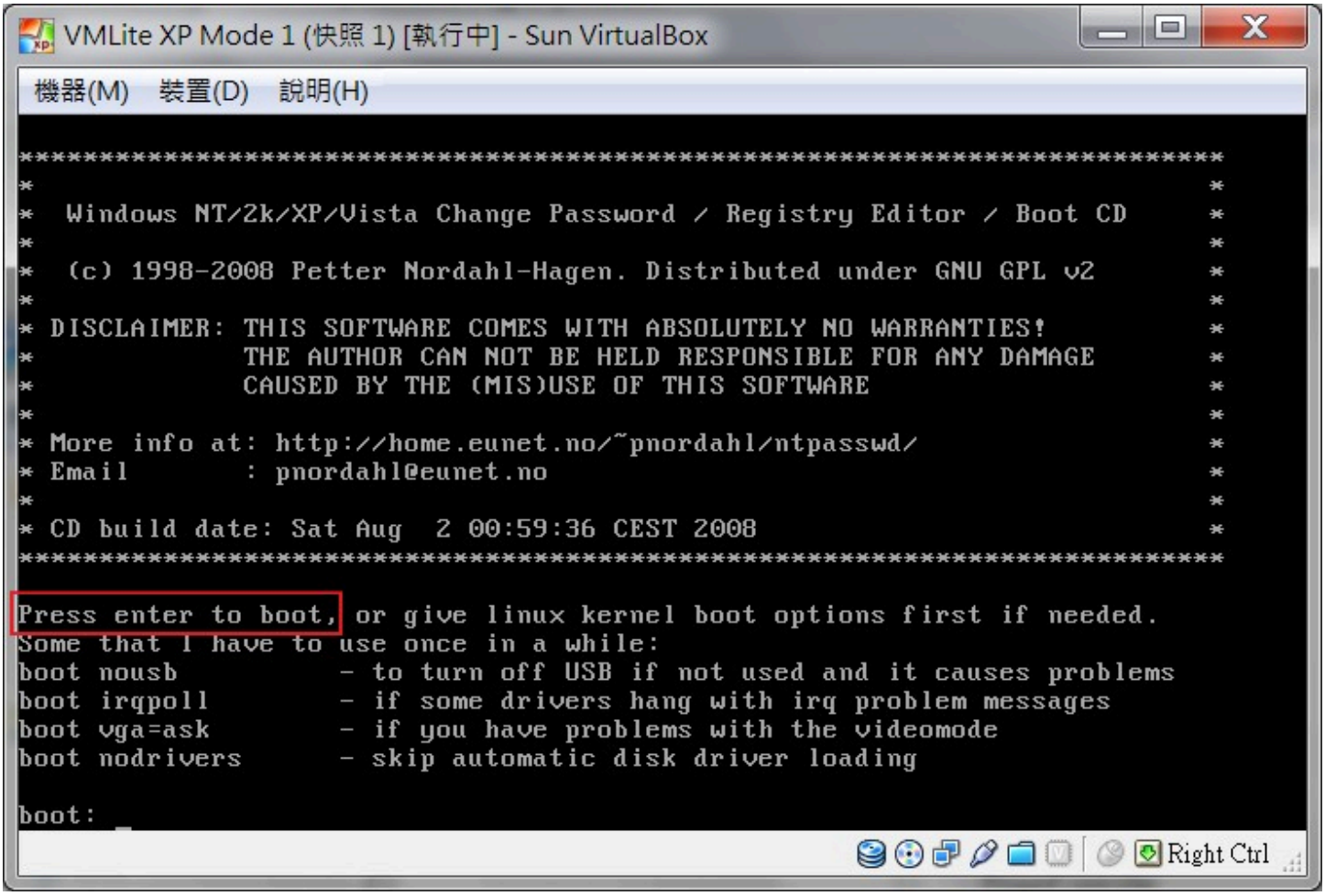
????????ubcd?????HDD?



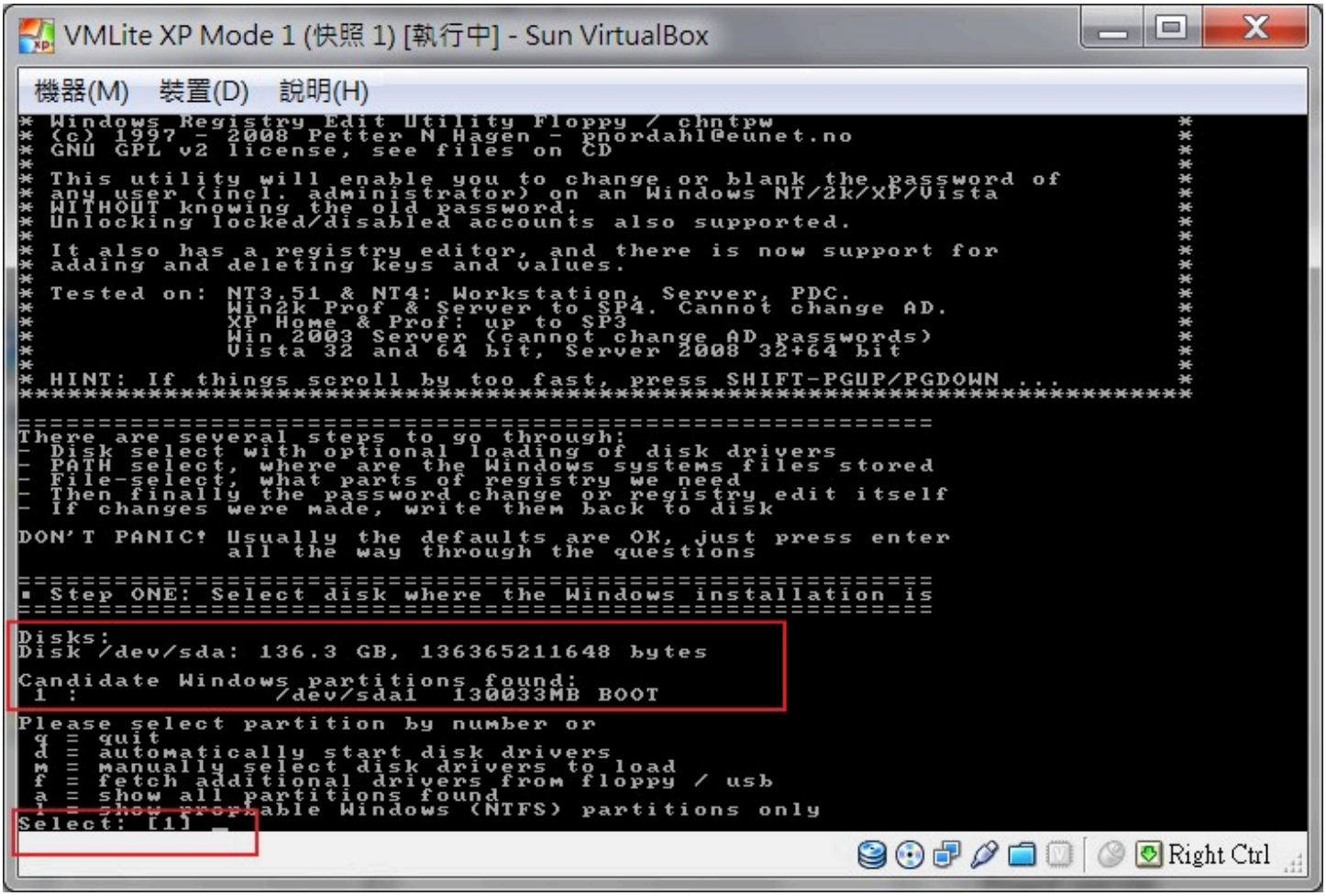
??data recovery?



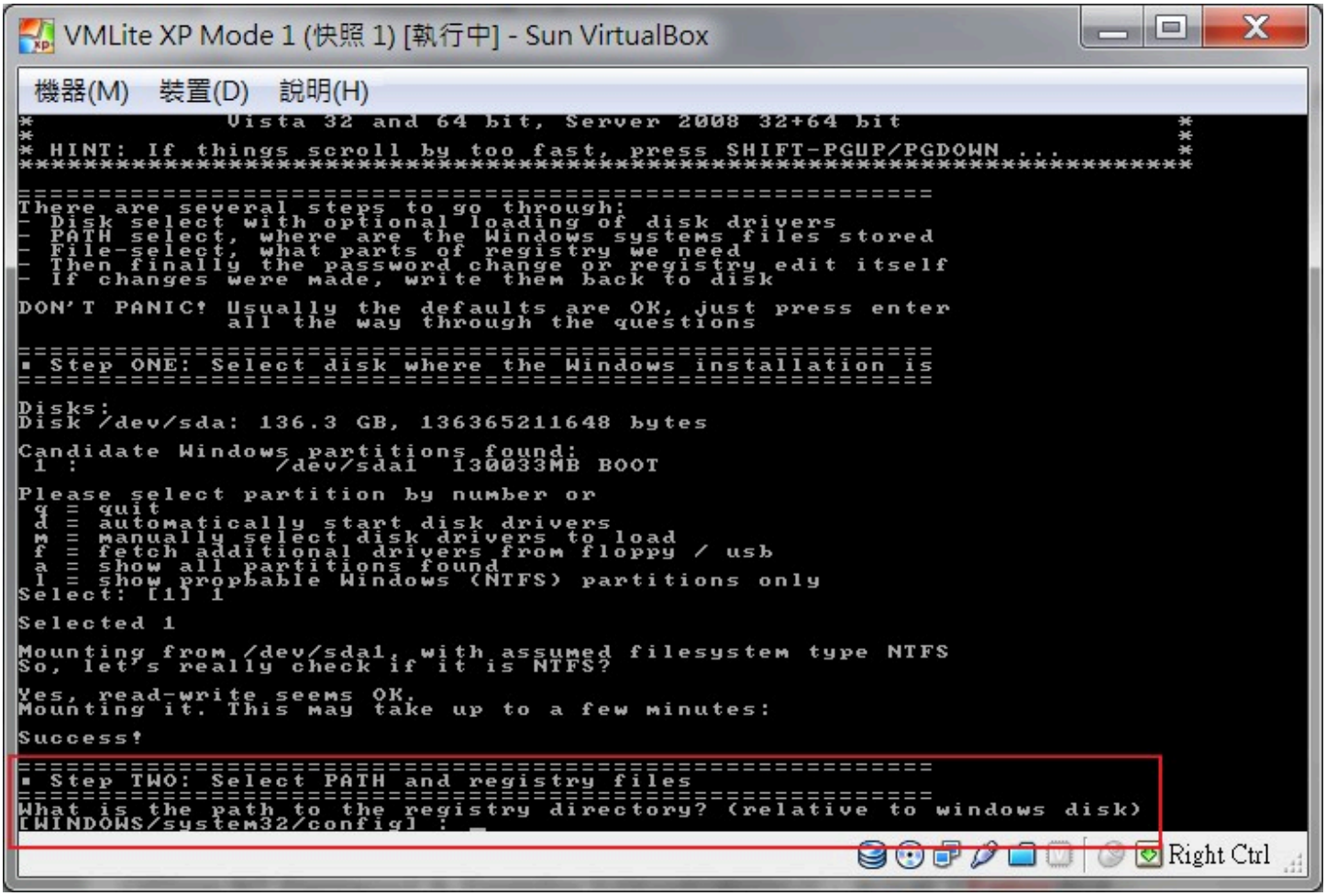
??Offline NT Password & Registry Editor?



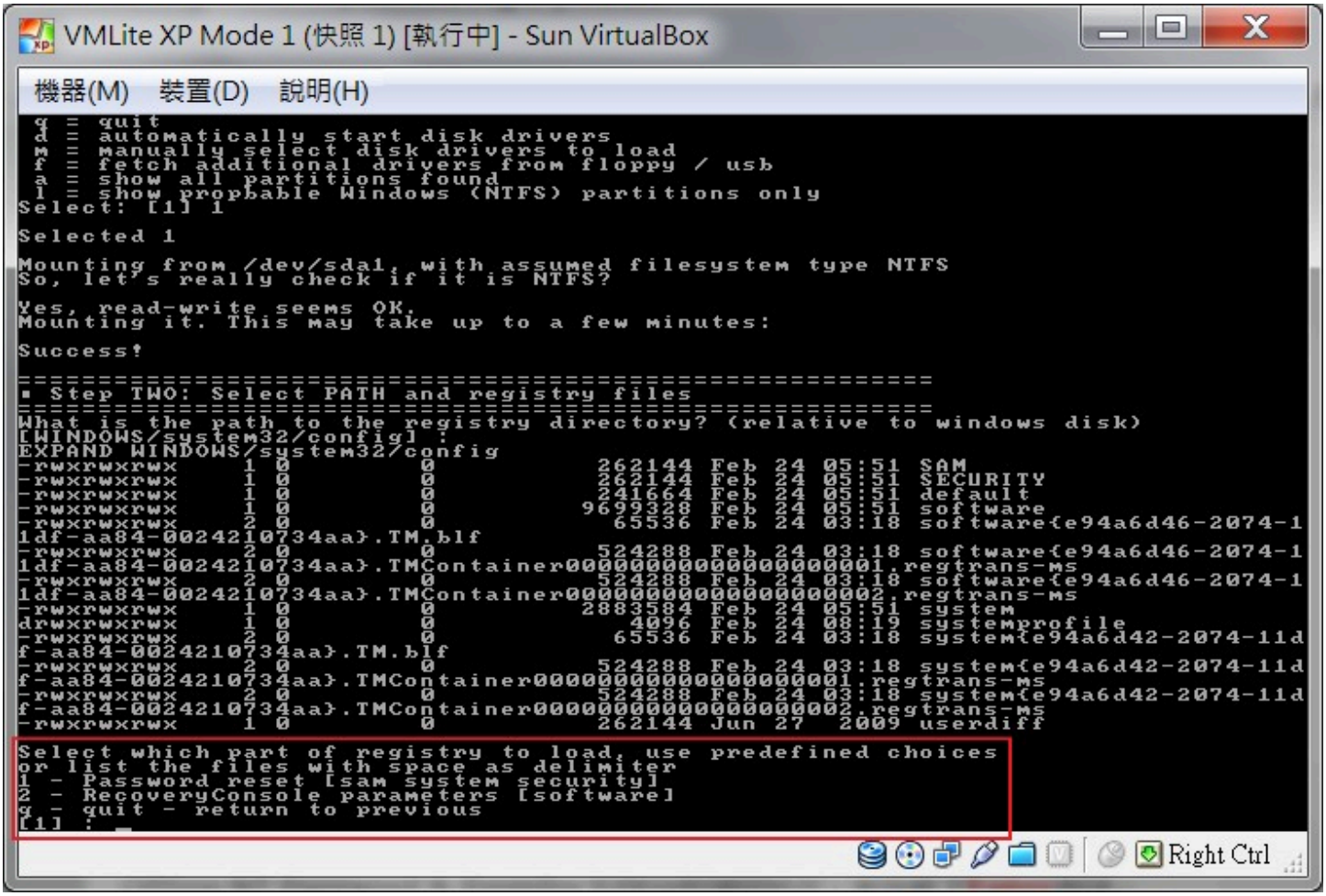
??Offline NT Password & Registry Editor???enter to boot ??????


VMLite XP Mode 1 (快照 1) [執行中] - Sun VirtualBox
機器(M) 裝置(D) 說明(H)
* Windows Registry Edit Utility Floppy / chntpw *
* (c) 1997 - 2008 Petter N Hagen - pnordahl@eunet.no *
* GNU GPL v2 license, see files on CD *
* This utility will enable you to change or blank the password of *
* any user (incl. administrator) on an Windows NT/2k/XP/Vista *
* WITHOUT knowing the old password. *
* Unlocking locked/disabled accounts also supported. *
* It also has a registry editor, and there is now support for *
* adding and deleting keys and values. *
* Tested on: NT3.51 & NT4: Workstation, Server, PDC. *
* Win2k Prof & Server to SP4. Cannot change AD. *
* XP Home & Prof: up to SP3 *
* Win 2003 Server (cannot change AD passwords) *
* Vista 32 and 64 bit, Server 2008 32+64 bit *
* HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN ... *
There are several steps to go through:
- Disk select with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File-select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk
DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions
* Step ONE: Select disk where the Windows installation is
Disks:
Disk /dev/sda: 136.3 GB, 136365211648 bytes
Candidate Windows partitions found:
1 : /dev/sda1 130033MB BOOT
Please select partition by number or
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show probable Windows (NTFS) partitions only
Select: [1]
Right Ctrl

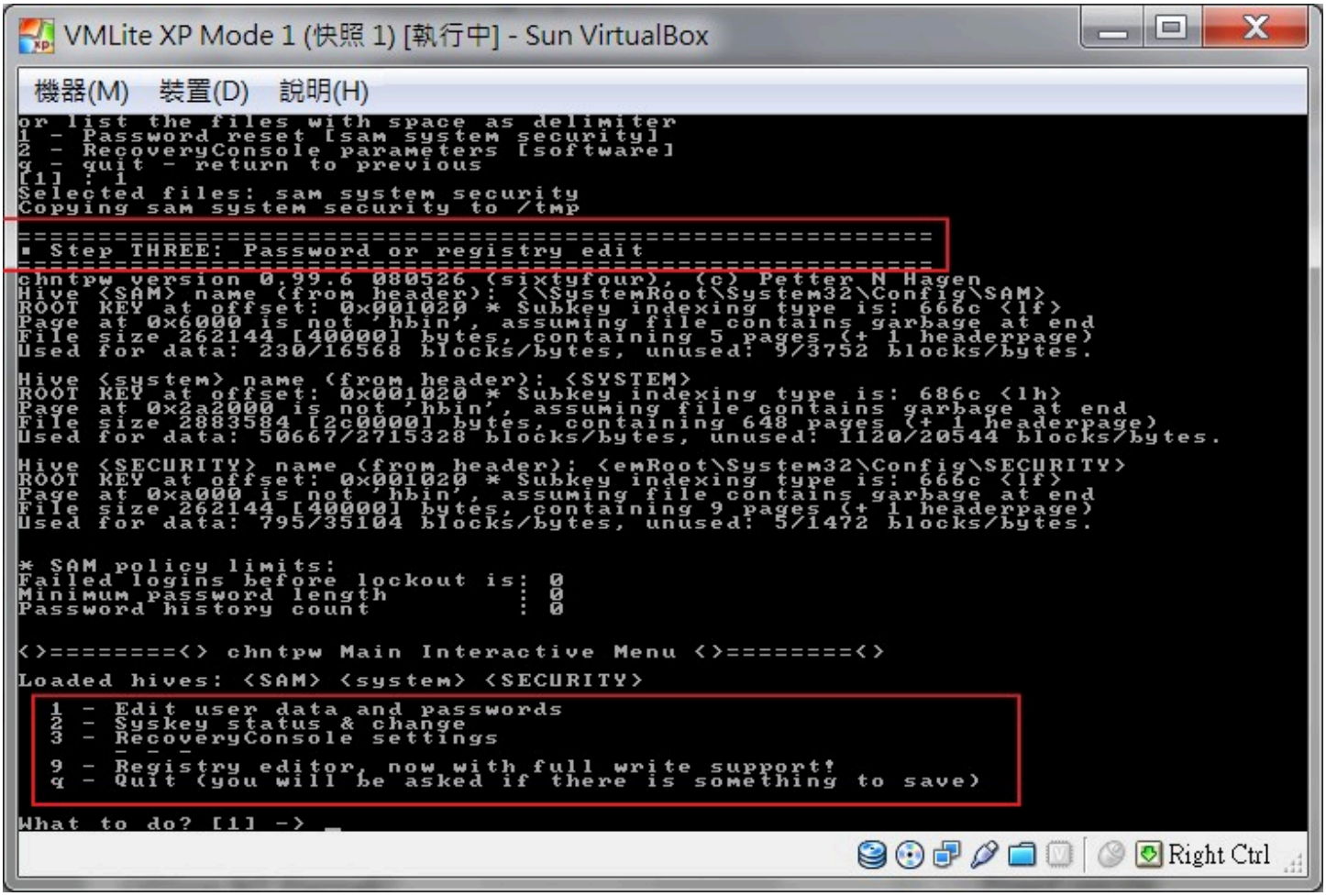
??XP?????:
????1????????"1"?? "??1"



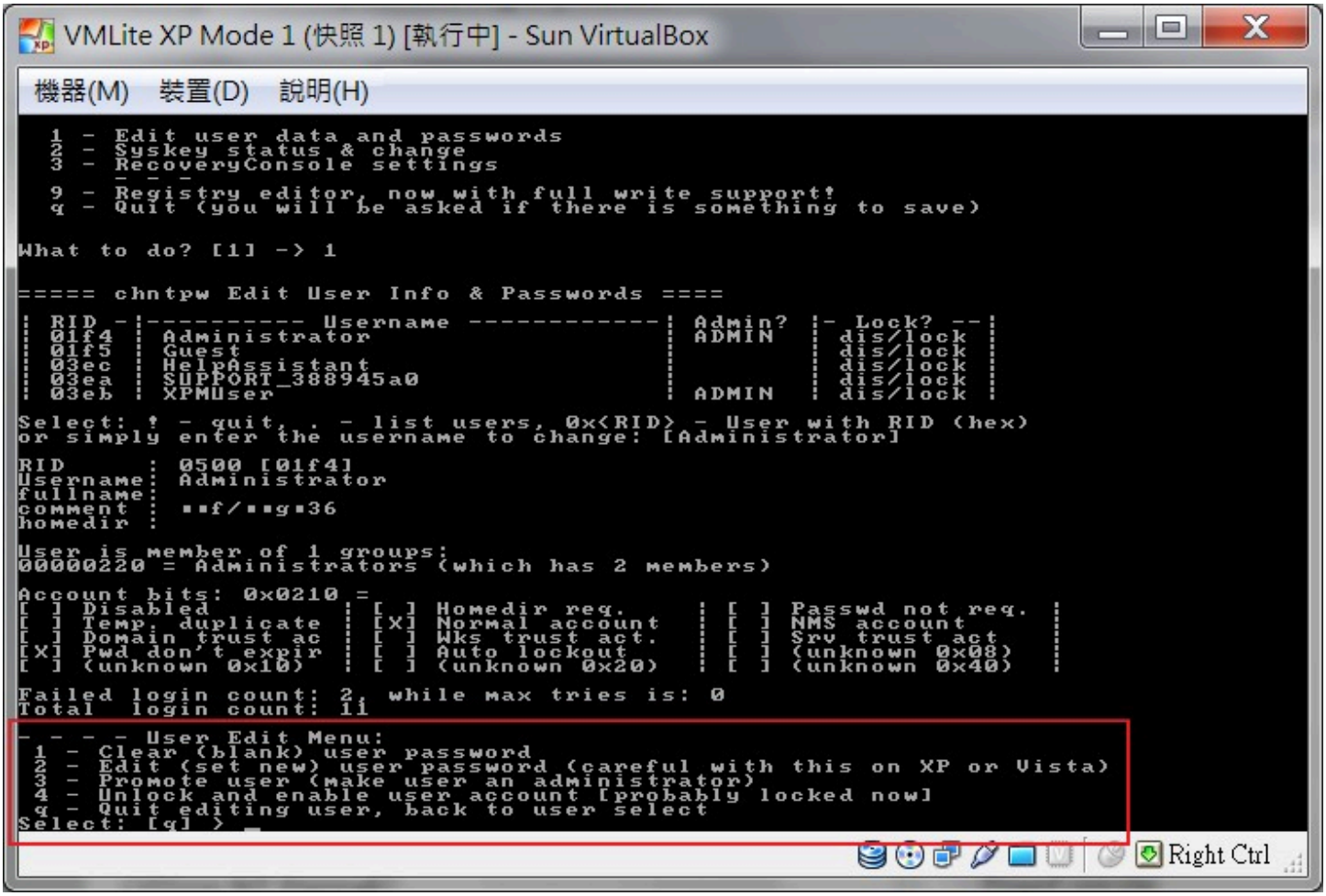
??XP?????:
??registry???????????\windows\system32\config???enter?????


VMLite XP Mode 1 (快照 1) [執行中] - Sun VirtualBox
機器(M) 裝置(D) 說明(H)
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show probable Windows (NTFS) partitions only
Select: [1] 1
Selected 1
Mounting from /dev/sda1, with assumed filesystem type NTFS
So, let's really check if it is NTFS?
Yes, read-write seems OK.
Mounting it. This may take up to a few minutes:
Success!
Step TWO: Select PATH and registry files
What is the path to the registry directory? (relative to windows disk)
[WINDOWS/system32/config] :
EXPAND WINDOWS/system32/config
-rwxrwxrwx 1 0 0 262144 Feb 24 05:51 SAM
-rwxrwxrwx 1 0 0 262144 Feb 24 05:51 SECURITY
-rwxrwxrwx 1 0 0 241664 Feb 24 05:51 default
-rwxrwxrwx 1 0 0 9699328 Feb 24 05:51 software
-rwxrwxrwx 2 0 0 65536 Feb 24 03:18 software{e94a6d46-2074-11d
1df-aa84-002421 0734aa}.TM.blf
-rwxrwxrwx 2 0 0 524288 Feb 24 03:18 software{e94a6d46-2074-11
1df-aa84-002421 0734aa}.TMContainer00000000000000000001.regtrans-ms
-rwxrwxrwx 2 0 0 524288 Feb 24 03:18 software{e94a6d46-2074-11
1df-aa84-002421 0734aa}.TMContainer00000000000000000002.regtrans-ms
-rwxrwxrwx 1 0 0 28835 84 Feb 24 05:51 system
drwxrwxrwx 1 0 0 4096 Feb 24 08:19 systemprofile
-rwxrwxrwx 2 0 0 65536 Feb 24 03:18 system{e94a6d42-2074-11d
f-aa84-002421 0734aa}.TM.blf
-rwxrwxrwx 2 0 0 524288 Feb 24 03:18 system{e94a6d42-2074-11d
f-aa84-002421 0734aa}.TMContainer00000000000000000001.regtrans-ms
-rwxrwxrwx 2 0 0 524288 Feb 24 03:18 system{e94a6d42-2074-11d
f-aa84-002421 0734aa}.TMContainer00000000000000000002.regtrans-ms
-rwxrwxrwx 1 0 0 262144 Jun 27 2009 userdiff
Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] :
Right Ctrl

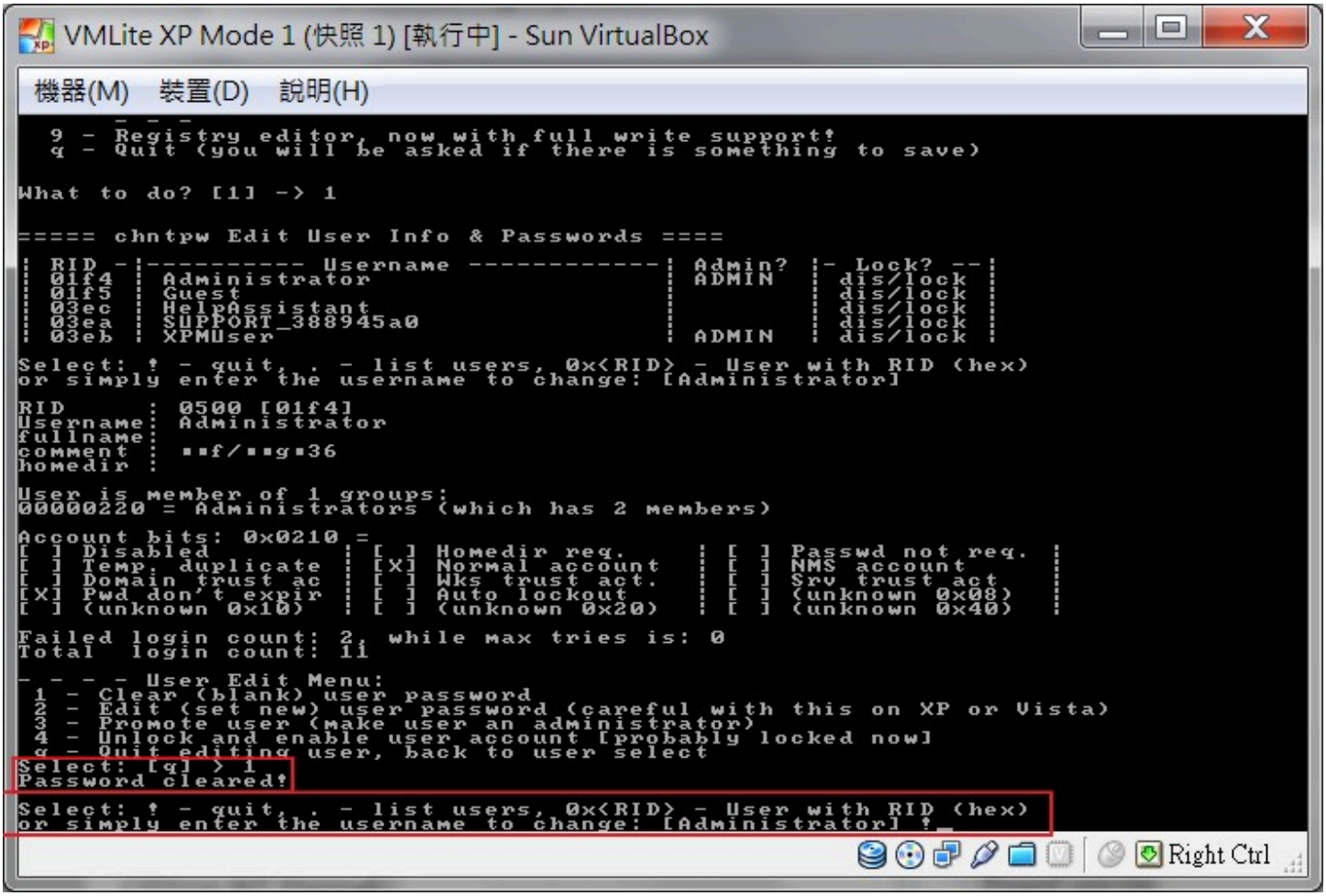
???????1?????


VMLite XP Mode 1 (快照 1) [執行中] - Sun VirtualBox
機器(M) 裝置(D) 說明(H)
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] : 1
Selected files: sam system security
Copying sam system security to /tmp
* Step THREE: Password or registry edit
chntpw version 0.99.6 080526 (sixtyfour), (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0x6000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 230/16568 blocks/bytes, unused: 9/3752 blocks/bytes.
Hive <system> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
Page at 0x2a2000 is not 'hbin', assuming file contains garbage at end
File size 2883584 [2c0000] bytes, containing 648 pages (+ 1 headerpage)
Used for data: 50667/2715328 blocks/bytes, unused: 1120/20544 blocks/bytes.
Hive <SECURITY> name (from header): <emRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
Page at 0xa000 is not 'hbin', assuming file contains garbage at end
File size 262144 [40000] bytes, containing 9 pages (+ 1 headerpage)
Used for data: 795/35104 blocks/bytes, unused: 5/1472 blocks/bytes.
* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length : 0
Password history count : 0
<>========<> chntpw Main Interactive Menu <>========<>
Loaded hives: <SAM> <system> <SECURITY>
1 - Edit user data and passwords
2 - Syskey status & change
3 - RecoveryConsole settings
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)
What to do? [1] -> _
Right Ctrl

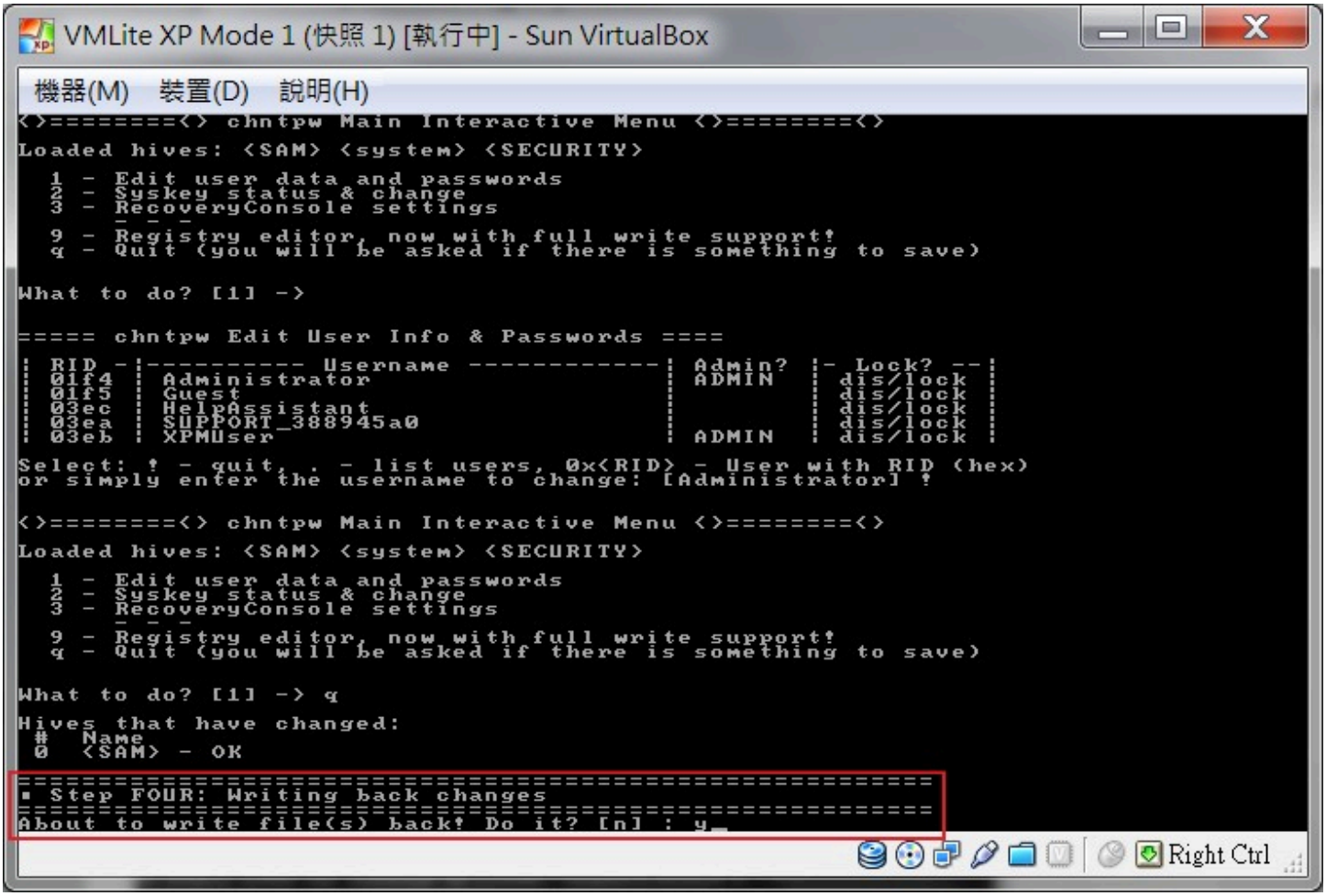
??XP?????:
???????1?????


VMLite XP Mode 1 (快照 1) [執行中] - Sun VirtualBox
機器(M) 裝置(D) 說明(H)
1 - Edit user data and passwords
2 - Syskey status & change
3 - RecoveryConsole settings
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)
What to do? [1] -> 1
===== chntpw Edit User Info & Passwords ====
RID | Username | Admin? | Lock?
01f4 | Administrator | ADMIN | dis/lock
01f5 | Guest | | dis/lock
03ec | HelpAssistant | | dis/lock
03ea | SUPPORT_388945a0 | | dis/lock
03eb | XPMUser | ADMIN | dis/lock
Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator]
RID : 0500 [01f4]
Username: Administrator
fullname:
comment :
homedir :
User is member of 1 groups:
00000220 = Administrators (which has 2 members)
Account bits: 0x0210 =
[ ] Disabled | [ ] Homedir req. | [ ] Passwd not req.
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account
[ ] Domain trust ac | [ ] Wks trust act. | [ ] Srv trust act
[X] Pwd don't expir | [ ] Auto lockout | [ ] (unknown 0x08)
[ ] (unknown 0x10) | [ ] (unknown 0x20) | [ ] (unknown 0x40)
Failed login count: 2, while max tries is: 0
Total login count: 11
- - - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
q - Quit editing user, back to user select
Select: [q] >
Right Ctrl

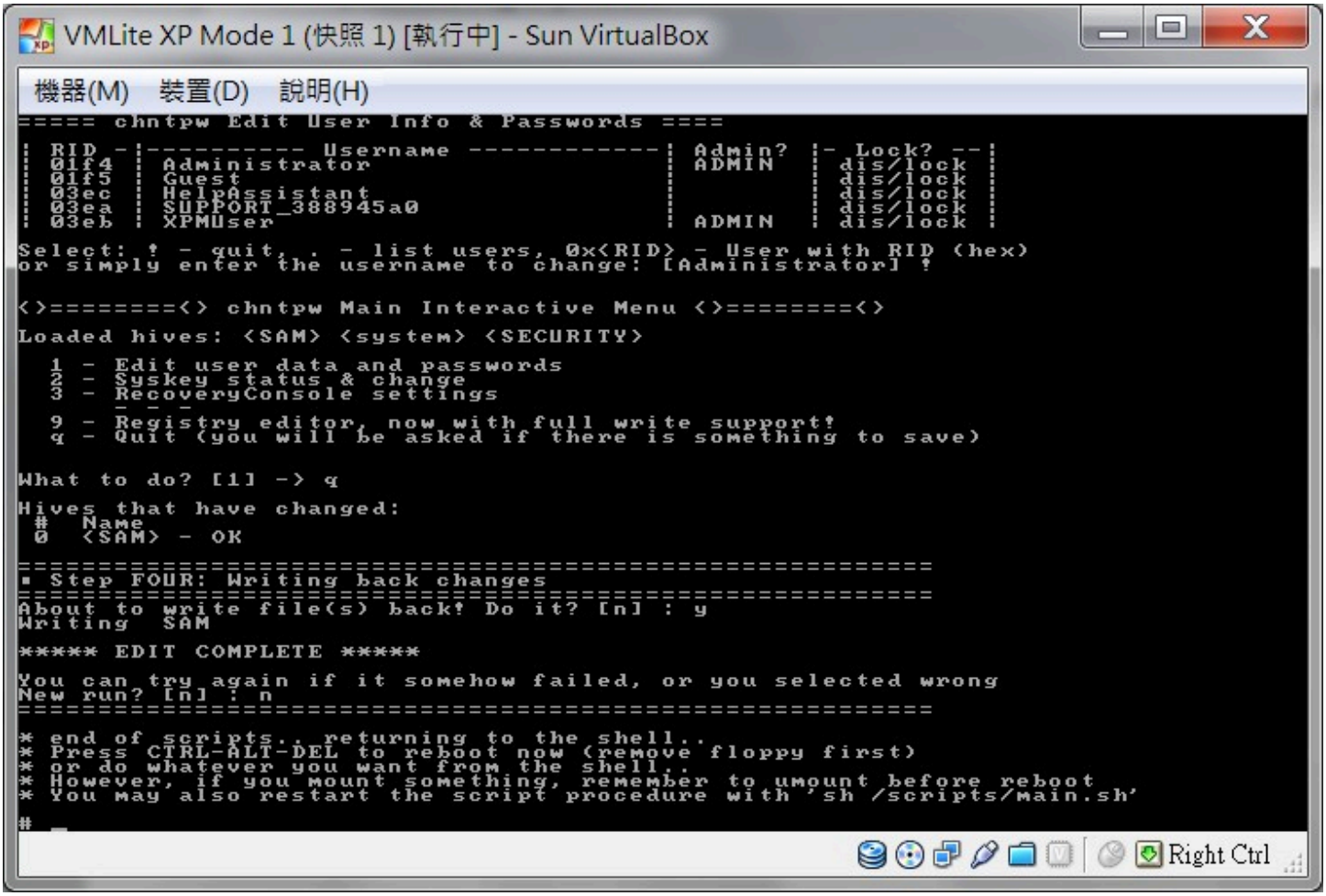
????1?????(????????)?



??????????????Offline NT Password & Registry Editor?????username????administrator????enter???????

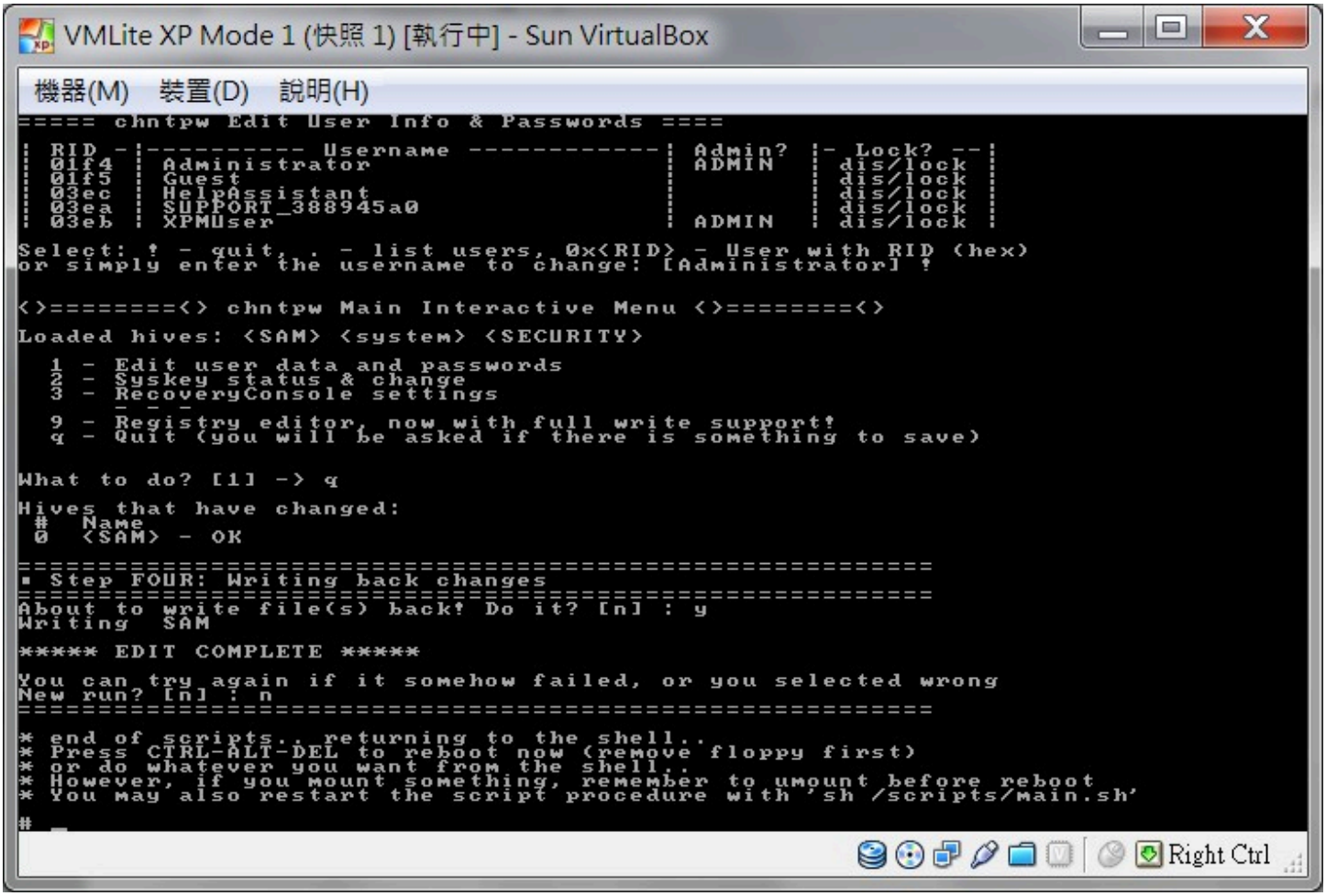

VMLite XP Mode 1 (快照 1) [執行中] - Sun VirtualBox
機器(M) 裝置(D) 說明(H)
<>========<> chntpw Main Interactive Menu <>========<>
Loaded hives: <SAM> <system> <SECURITY>
1 - Edit user data and passwords
2 - Syskey status & change
3 - RecoveryConsole settings
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)
What to do? [1] ->
===== chntpw Edit User Info & Passwords ====
RID | Username | Admin? | Lock?
01f4 | Administrator | ADMIN | dis/lock
01f5 | Guest | | dis/lock
03ec | HelpAssistant | | dis/lock
03ea | SUPPORT_388945a0 | | dis/lock
03eb | XPMUser | ADMIN | dis/lock
Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] !
<>========<> chntpw Main Interactive Menu <>========<>
Loaded hives: <SAM> <system> <SECURITY>
1 - Edit user data and passwords
2 - Syskey status & change
3 - RecoveryConsole settings
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)
What to do? [1] -> q
Hives that have changed:
Name
0 <SAM> - OK
* Step FOUR: Writing back changes
About to write file(s) back! Do it? [n] : y
Right Ctrl

??XP?????:
offline???????????"Y"???



EDIT COMPLETE!

??????????????????????????????????????**??n???Enter**???Offline NT Password & Registry Editor?



???????virtual machine??????
??? ??F12 ? IDE Primary ??

Administrator????,??????
???Raid card ?????Driver.????Win PE CD

??NT offline ??SAM password?? ???????