27th January

Reset Active Directory Administrator Password

Imagine the scenario. You arrive at a client's site to be informed they have "lost" the password to the default built-in Active Directory Administrator user account. Your first thought may be: "No Problem. I will just log on with another user account with domain-level admin privileges." Panic slowly creeps in when you're eventually told it happens to be the *only* Active Directory user account with those privileges. So, you're now confronted with the situation where you essentially have no control over Active Directory. What do you do at this point?

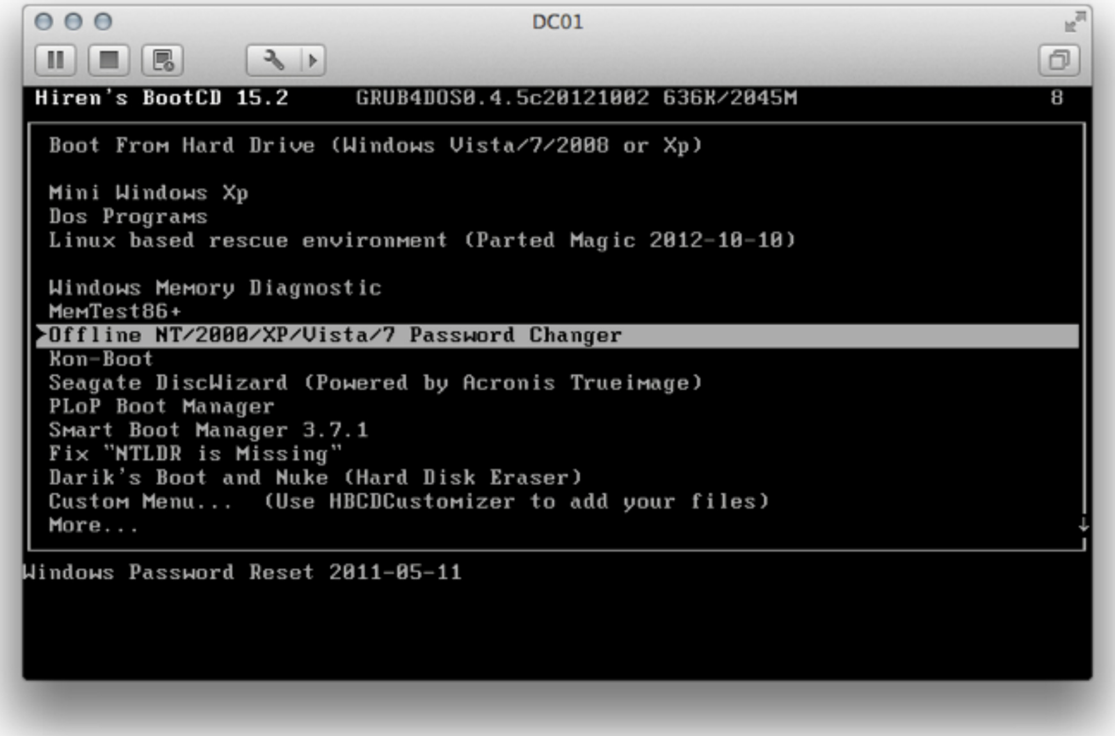
This procedure was tested on Windows Server 2003 R2, 2008 R2 and also Windows Server 2012 (which I will be using for examples in this post). I highly recommend the procedure to be performed on the AD domain controller that hosts the primary domain controller (PDC) emulator operations master role.

Clear Local Admin Password

Before we can modify the password for the AD Administrator user account, we need to modify the password for the local Administrator account stored in the SAM database on the domain controller computer.

A few utilities are available that will perform this function, but we will be using the excellent Offline NT Password Editor [http://pogostick.net/~pnh/ntpasswd] tool by Petter Nordahl-Hagen. The tool is included on Hiren's BootCD [http://www.hiren.info/pages/bootcd] , so it will be required for our tutorial. You have the option to either burn the ISO image to CD or copy the data to a USB flash (or hard) drive.

- Start the computer with Hiren's BootCD (CD or USB) as the first boot device. Refer to your hardware vendor documentation for information on changing boot order in the firmware.
- Upon boot, you should be presented with Hiren's BootCD main menu. Select the `Offline NT/2000/XP/Vista/7 Password Changer` option.



```
Hiren's BootCD 15.2     GRUB4DOS0.4.5c20121002 636K/2045M                8

 Boot From Hard Drive (Windows Vista/7/2008 or Xp)

 Mini Windows Xp
 Dos Programs
 Linux based rescue environment (Parted Magic 2012-10-10)

 Windows Memory Diagnostic
 MemTest86+
>Offline NT/2000/XP/Vista/7 Password Changer
 Kon-Boot
 Seagate DiscWizard (Powered by Acronis Trueimage)
 PLoP Boot Manager
 Smart Boot Manager 3.7.1
 Fix "NTLDR is Missing"
 Darik's Boot and Nuke (Hard Disk Eraser)
 Custom Menu...  (Use HBCDCustomizer to add your files)
 More...

Windows Password Reset 2011-05-11
```

[https://dl.dropbox.com/u/1030586/blog/img/hiren720.png]

- Press the `enter` key at the Linux `boot:` prompt.

We will now need to choose the disk and partition where our Windows registry is located. My Windows Server 2012 configuration has a single disk with two partitions. Partition 1 is the hidden system reserved partition, so I will select partition 2 which is represented as the C:

drive in Windows.

```
=========================================================
 Step ONE: Select disk where the Windows installation is
=========================================================

Disks:
Disk /dev/sda: 64.4 GB, 64424509440 bytes

Candidate Windows partitions found:
 1 :            /dev/sda1     350MB BOOT
 2 :            /dev/sda2   61088MB

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] 2
```

The tool will now go thru its operations to verify it can successfully access and mount the NTFS file system. You can just press the `enter` key to accept the default `Windows/System32/config` path for step two.

```
Selected 2

Mounting from /dev/sda2, 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] : <enter>
```

Press the `enter` key to select the default `1 - Password reset [sam system security]` option.

```
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] : <enter>
```

Press the `enter` key to select the default `1 - Edit user data and passwords` option.

```
=========================================================
 Step THREE: Password or registry edit
=========================================================
...

<>========<> chntpw Main Interactive Menu <>========<>
```

```
Loaded hives:

  1 - Edit user data and passwords
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] -> <enter>
```

Our Administrator user should be the default option selected, so just press the enter key.

```
===== chntpw Edit User Info & Passwords ====
: RID -:---------- Username ------------: Admin? :- Lock? --:
: 01f4 : Administrator                  :        :          :
: 01f5 : Guest                          :        : dis/lock :

Select: ! - quit, . - list users, 0x - User with RID (hex)
or simply enter the username to change: [Administrator] <enter>

RID     : 0500 [01f4]
Username: Administrator
fullname:
comment : Built-in account for administering the computer/domain
homedir :
```

You may be tempted to select option 2 to edit the Administrator password, but this operation has never worked in my experience. This leaves us with option 1 to clear the local Administrator user account password.

```
...

- - - - 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) [seems unlocked already]
 q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!
```

Our task of "blanking" the local Administrator user account password is now complete. Our change will not be set until we write (save) our configuration. Enter ! to quit.

```
Select: ! - quit, . - list users, 0x - User with RID (hex)
or simply enter the username to change: [Administrator] !
```

And enter q to take us to step four.

```
<>========<> chntpw Main Interactive Menu <>========<>

Loaded hives:

  1 - Edit user data and passwords
      - - -
  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
```

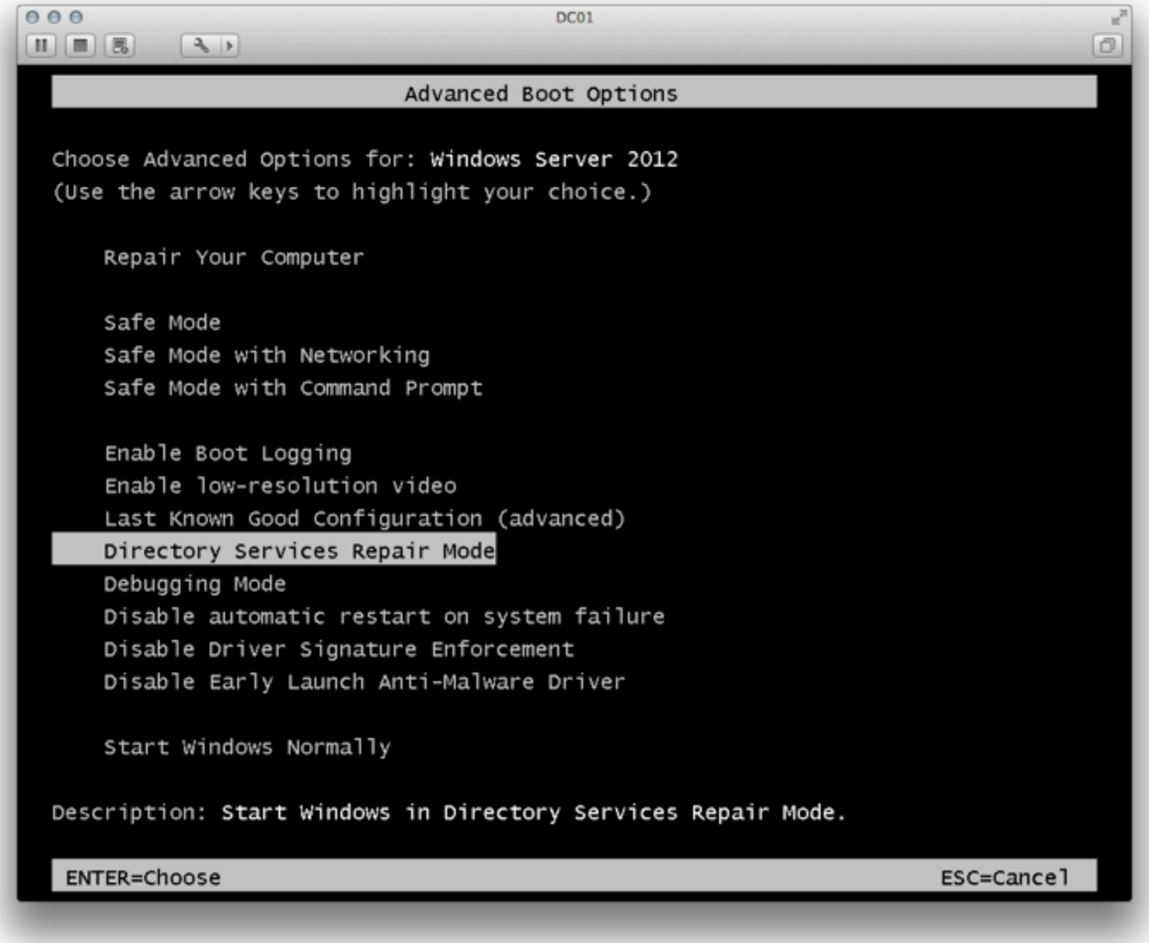
Let's now save our configuration. Enter y to save our work, then enter n to decline the option to perform another run. Finally, enter reboot or halt depending on whether you want to restart or shutdown the computer before we move on to the next major phase. Don't forget to eject the media before you restart or shutdown.

```
=========================================================
 Step FOUR: Writing back changes
=========================================================
About to write file(s) back! Do it? [n] : y
Writing  SAM

***** EDIT COMPLETE *****

You can try again if it somehow failed, or you selected wrong
New run? [n] : n
=========================================================

* end of scripts.. returning to the shell..
* Press CTRL-ALT-DEL to reboot now (remove floppy first)
* or do whatever you want from the shell..
* However, if you mount something, remember to umount before reboot
* You may also restart the script procedure with 'sh /scripts/main.sh'

# reboot
```

Directory Services Repair Mode (DSRM)

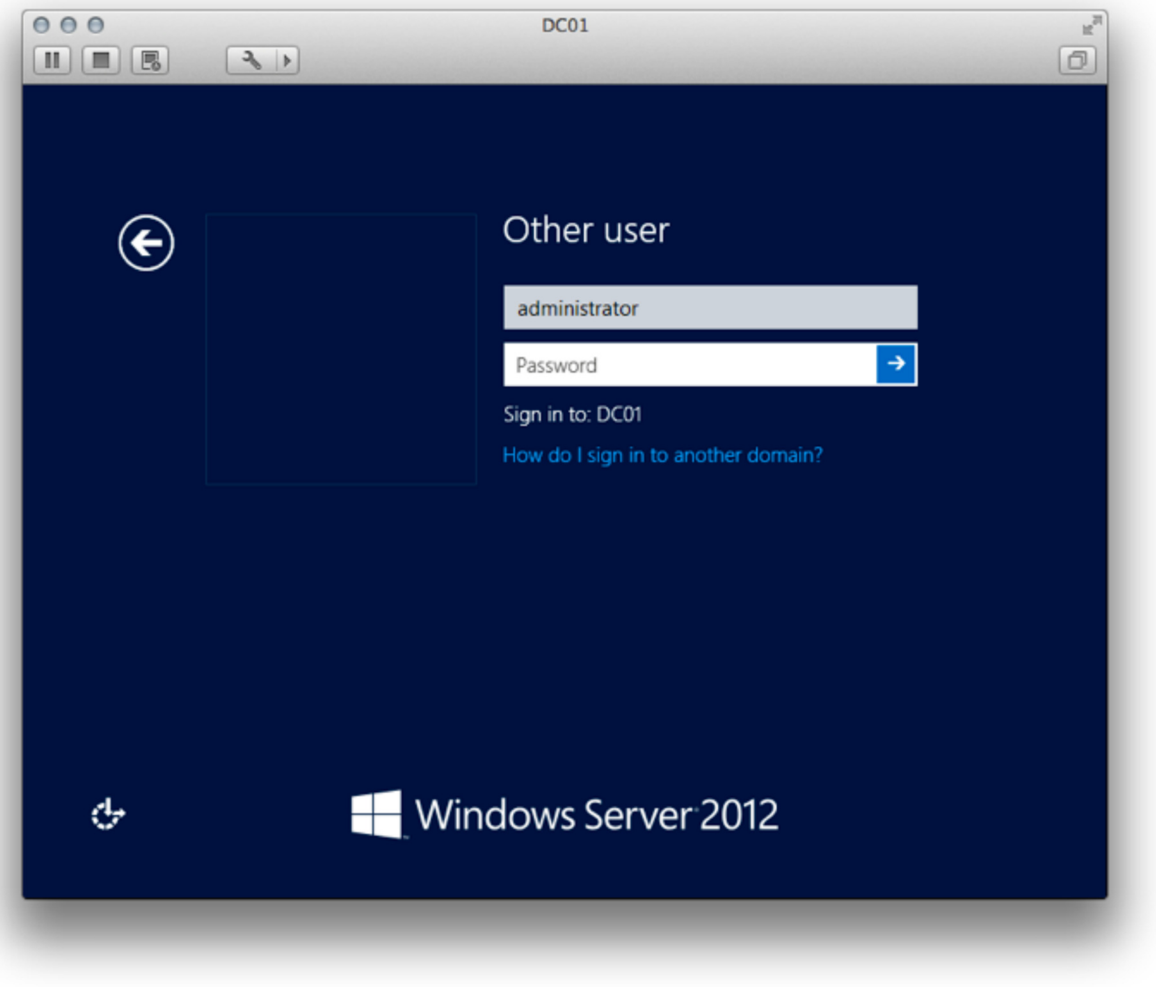
We will now need to boot into Directory Services Repair Mode as this will allow us to log on to the computer with the local Administrator user account (which is now blank). If we booted in normal mode, it would require us to log on with a privileged domain user account. Starting in DSRM takes the domain controller offline, meaning it functions as a member server, not as a domain controller.

We can start a domain controller in Directory Services Repair Mode manually by pressing the F8 key during the domain controller startup. At the Advanced Boot Options menu, select the Directory Services Repair Mode option.



```
                          Advanced Boot Options

Choose Advanced Options for: Windows Server 2012
(Use the arrow keys to highlight your choice.)

    Repair Your Computer

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Enable Boot Logging
    Enable low-resolution video
    Last Known Good Configuration (advanced)
    Directory Services Repair Mode
    Debugging Mode
    Disable automatic restart on system failure
    Disable Driver Signature Enforcement
    Disable Early Launch Anti-Malware Driver

    Start Windows Normally

Description: Start Windows in Directory Services Repair Mode.

 ENTER=Choose                                                   ESC=Cancel
```

[https://dl.dropbox.com/u/1030586/blog/img/dsrmselect720.png]
At the Logon Screen, sign in as the administrator with no password. Note how I'm signing in to the local machine and not the domain (because Active Directory Domain Services is in a stopped state). My computer's hostname is dc01 and the Active Directory NETBIOS name is example.



[https://dl.dropbox.com/u/1030586/blog/img/dsrmlogon720.png]
After a successful log on, open a command prompt window.

We can verify information for our current user by running the following command:

```
C:\> whoami /user

USER INFORMATION
----------------

User Name          SID
================== ============================================
dc01\administrator S-1-5-21-3243332244-383894547-2364936909-500
```

Before we forget, let's change our local Administrator user account password from the very insecure non-existent password to something complex. Run the following command:

```
C:\> net user administrator *
```

Our current task is now to change the default built-in Active Directory Administrator user account password. We can accomplish this by creating a custom service that executes a command. This command will set the default built-in Active Directory Administrator user account password to whatever we choose. It should also be noted the password will need to comply with the domain's password minimum length and complexity rules. Run the following command, but pay special attention to the unique syntax with the space between the '=' symbol and parameter value:

```
C:\> sc create ResetPW binPath= "%ComSpec% /k net user administrator PA$$w0rd94" start= auto
[SC] CreateService SUCCESS
```

The preceding command essentially creates a Windows service named ResetPW that executes the net user command that changes the default built-in Active Directory Administrator user account password. The service is created with the behavior to autostart at boot and also run in the context of the LocalSystem user account.

Note: Check out my follow-up post [http://binarynature.blogspot.com/2013/02/find-active-directory-administrator-users-in-dsrm.html] if the default built-in Active Directory Administrator user account is not an option for use with the custom service.

We can verify the service configuration by running the following command:

```
C:\> sc qc ResetPW
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: ResetPW
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\Windows\system32\cmd.exe /k net user administrator PA$$w0rd94
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : ResetPW
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

Let's now reboot to have Windows start normally and allow our custom service do its job. Run the following command:

```
C:\> shutdown -r -t 0
```

Sign In and Cleanup

At the Logon Screen, sign in as the default built-in Active Directory Administrator user with the password we assigned with our custom service. My example used PA$$w0rd94 as the password.

You should now be successfully signed in as the default built-in Active Directory Administrator user. Open a command prompt window, so we can verify information for our current user by running the following command:

```
C:\> whoami /user

USER INFORMATION
----------------

User Name             SID
===================== ============================================
example\administrator S-1-5-21-1717405439-783545762-1294388781-500
```

Our custom service has served its purpose, so we now need to delete it. Before we delete it, we need to verify it's in the stopped state. Run the following command:

```
C:\> sc query ResetPW

SERVICE_NAME: ResetPW
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Delete the service. Run the following command:

```
C:\> sc delete ResetPW
[SC] DeleteService SUCCESS
```

Verify the service has been deleted. Run the following command:

```
C:\> sc qc ResetPW
[SC] OpenService FAILED 1060:

The specified service does not exist as an installed service.
```

Now that we have total control over Active Directory, I would highly recommend you change the default built-in Active Directory Administrator user account password at this point. Run the following command:

```
C:\> net user administrator *
```

We can optionally logoff and sign back in with the updated default built-in Active Directory Administrator user account to verify our configuration. Run the following command:

```
C:\> logoff
```

Summary

I had two primary objectives for this post. The first is to provide a solution for technical professionals to overcome "lost" or "missing" administrator-level user account password issues, and the second is to point out how trivial it is for someone to "pwn t3h" AD network when you lack physical security for your IT infrastructure.

Posted 27th January by Marc Weisel

Labels: AD, Security, Windows

2 View comments

1 comment

Add a comment as Adam Leinss

Top comments

Nathan Wielenga shared this via Google+ 4 months ago - Shared publicly

1 · Reply