GNU/Linux Administration - Support #935

Reset Windows Password Offline Using Arch Linux

04/21/2018 01:10 PM - Daniel Curtis

Status:	Closed	**Start date:**	04/22/2018
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Workstation	**Estimated time:**	1.00 hour
Target version:	Arch Linux	**Spent time:**	1.50 hour

Description

This is a guide on resetting a forgotten Windows 7 password using an Arch Linux install media.

Prepare the Environment

- Make sure the package repo databases are updated:

```
pacman -Sy
```

- Install chntpw:

```
pacman -S chntpw
```

Reset Windows Password

- Use fdisk to list out the drive partitions:

```
fdisk -l
```

  - *Example output*

```
Disk /dev/sda: 232.9 GiB, 1000204886016 bytes, 1953525168 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disklabel type: dos
Disk identifier: 0xc05a68a1

Device     Boot Start       End   Sectors   Size Id Type
/dev/sda1  *     2048 488394751 488392704 232.9G  7 HPFS/NTFS/exFAT
```

- Mount the Windows partition:

```
mount /dev/sda1 /mnt
```

- Change into the Windows System32 directory:

```
cd /mnt/Windows/System32/config/
```

- Get a list of users in the SAM:

```
chntpw -l sam
```

- Run chntpw for the Bob user:

```
chntpw -u Bob sam
```

- Enter **1** to clear Bobs password:

```
1
```

- Enter **2** to unlock Bobs account:

```
2
```

- Quit chntpw and write the hive file:

```
q
y
```

- Unmount the Windows partition and reboot:

```
umount /mnt
reboot
```

Resources

- https://www.techrepublic.com/blog/tr-dojo/reset-windows-passwords-with-the-help-of-linux/

History

#1 - 04/21/2018 01:33 PM - Daniel Curtis

- % Done changed from 0 to 100

- Status changed from New to Resolved

- Description updated

#2 - 04/21/2018 01:33 PM - Daniel Curtis

- Start date changed from 04/21/2018 to 04/22/2018

#3 - 06/10/2019 02:34 PM - Daniel Curtis

- Status changed from Resolved to Closed