Erledigt Adminpasswort für Windows vergessen? Kein Problem.

Beitrag von „Sascha_77“ vom 2. März 2018, 09:37

Um in Windows (7/8/10) sein vergessenes Adminpasswort zu "recovern" bedarf es nur ein paar Schritten.

Kauft bloß nicht irgendwelche teuren Passwort-Recover-Programme. Alles rausgeworfenes Geld.

1) Win Rescue. bzw Installationsmedium booten
2) Beim Fenster mit der Sprachauswahl "Shift + F10" drücken (es geht eine Commandline auf)
3) auf die Platte wechseln wo sich die Win-Partition befindet (dürfte bei den meisten D: sein wenn man von einen USB-Stick Rescue bzw. Install gebootet hat)
4)

Code

1. D:
2. cd Windows/System32
3. ren sethc.exe sethc.exe.bak
4. copy cmd.exe sethc.exe

7) Reset und von Platte ganz regulär booten
8) Im Anmeldefenster 5 mal Shift drücken
9) Es geht eine Commandline auf (bereits im Adminmodus)
10) **lusrmgr.msc** aufrufen
11) Hier dann das Passwort zurücksetzen welches man vergessen hat.
12) Fertig!

Wenn man will kann man die alte sethc.exe wieder herstellen. Muss aber nicht zwingend wenn man diese Shift "Blockier" Funktion von WIndows nicht benötigt.

Beitrag von „Doctor Plagiat“ vom 2. März 2018, 13:05

Ich kenne noch das Prozedere mit dem Austausch der osk.exe durch cmd.exe. Das war in Windows 7, weiß gar nicht ob es in Windows 10 so noch funktioniert.
Anschließend am Anmeldebildschirm die Bildschirmtastatur aufrufen und es öffnet sich die Commandline.
Jetzt mit "net user Administrator /active:yes" den vorhandenen Administrator aktivieren oder mit "net user BENUTZERNAME /add" einen neuen Benutzer anlegen.

Beitrag von „Sascha_77“ vom 2. März 2018, 13:22

So oder so ist es irgendwie erschreckend wie einfach man das aushebeln kann. Aber OSX ist ja ähnlich. Von einem Installer Booten und dort dann das Passwort zurücksetzen (steht sogar dick im Menu oben drin) . Zumindest war es damals so. Keine Ahnung ob die das geändert haben.

Beitrag von „Doctor Plagiat“ vom 2. März 2018, 13:30

Ja, geht noch. In die Recovery booten, Terminal öffnen und `resetpassword` eingeben.

Beitrag von „DataV“ vom 2. März 2018, 13:36

Ich würde mal sagen, dass absolut kein Betriebssystem sicher ist, solange man Zugriff auf die Hardware hat.
Sicherheitslücken gibts überall, selbst wenn sie so dämlich sind.
Mir als Admin rettet sowas allerdings häufig mal den Tag, wenn Neukunden keine Kennwörter haben.

BTW. Das funktioniert so sogar mit dem Domänenadmin. Über den weg setzt man sein Passwort für die AD Recovery im Abgesicherten Modus zurück und kann danach im Active

Directory machen was man will.

P.s. und ja das geht mindestens von Server 2003-2016 durchgehend

---

Beitrag von „Sascha_77“ vom 2. März 2018, 13:57

Das es keine 100%ige SIcherheit gibt ist klar. Aber das es so einfach ist ist ja auch schon fast fahrlässig. Zumal das ja nichtmal im entferntesten mit "Hacken" zu tun hat. Das kriegt im Grunde jeder hin der weiss was eine CMD ist.

Aber mir solls recht sein. Brauche ich wenigstens nicht für jeden Mist nen Ticket aufmachen. 

Beitrag von „al6042“ vom 2. März 2018, 22:17

Ich kannte das noch unter NT4 SP3 mit dem Umbenennen des "login.scr" nach "cmd.exe"...
Anstatt Bildschirmschoner kam dann der DOS-Prompt im System-Profil... das war auch witzig... 

Beitrag von „Sahui89“ vom 14. August 2020, 09:42

Ich hatte ein ähnliches Problem auf einem alten Windows 10-Computer. Ich erinnere mich,dass ich Offine NT Password & Registry Editor verwendet habe,um mein Passwort zurückzusetzen. Das war das erste Mal, dass ich das tat. Es wurde mir von meinem Kollegen empfohlen.

https://pogostick.net/~pnh/ntpasswd/

https://www.iseepassword.de/wi...0-passwort-vergessen.html

Beitrag von „Sascha_77“ vom 14. August 2020, 09:50

Leider sind die Rechner die wir jetzt haben TPM verschlüsselt. Da ist definitiv kein Rankommen mehr. Bzw. Rankommen schon ... kann man im BIOS abschalten. Dann verfällt allerdings das Zertifikat um mich im Firmennetzwerk anzumelden und die Hardware muss komplett ausgetauscht werden. Schlecht. Den Adminzugang kann ich somit knicken. Aber damit kann ich leben. Viel wichtiger ist, das ich mich im Netz frei bewegen kann, da das NDIS Device über USB zu meinem Samsung (USB-Tethering) funktioniert. Muss nur noch auf dem Handy einen Proxyserver starten und den Traffic von z.B. FireFox (mittels Proxy-PlugIn) oder MobaXTerm auf die IP des Handys umleiten und schwupps gibts keinerlei Restriktionen mehr.

Mich wundert ehrlich gesagt, warum sie die autom. Einrichtung eines NDIS Devices nicht unterbunden haben. Dafür das die Kiste sonst jetzt ziemlich wasserdicht ist etwas verwunderlich.

Beitrag von „itisme“ vom 14. August 2020, 14:07

Danke Sascha_77 für Deine wertvollen Tipps!