Три способа сбросить пароль в Windows 7: простой, сложный и неправильн

Автор: Игорь Осколков Дата: 26.01.2012

Пароли, а особенно безопасные (читай сложные) имеют неприятное свойство — они легко забываются. Ну или чаще всего просто теряется бумажка с этим самым паролем. Ситуация, в общем, типичная. Поэтому неплохо бы подготовиться к ней заранее и знать, как быстро сбросить или сменить пароль

Напоминаем, что попытки повторить действия автора могут привести к потере гарантии на оборудование и даже к выходу его строя. Материал приведен исключительно в ознакомительных целях. Если же вы собираетесь воспроизводить действи описанные ниже, настоятельно советуем внимательно прочитать статью до конца хотя бы один раз. Редакция 3DNews не нес никакой ответственности за любые возможные последствия.

В Windows уже давно для хранения паролей всех пользователей и управления ими используется система SAM. Вся информация ней хорошо защищена, поэтому для того чтобы узнать пароль, придётся затратить кучу времени и ресурсов, особенно если с достаточно сложный. Чаще всего, однако, вовсе не требуется именно узнать пароль — достаточно сбросить его или поменяя Для этого разработано несколько утилит, одной из которых мы воспользуемся. Ещё один важный момент — очевидно, что, ког, ОС запущена, она не позволит просто так влезать в хранилище паролей. Поэтому надо убедиться, что компьютер поддержива загрузку с CD/DVD- или USB-носителя, чтобы запустить нужные утилиты.

Самая известная из них — это Offline NT Password and Registry editor, которая умеет работать с паролями и реестром Windov XP/Vista/7. Скачайте USB- или CD-версию утилиты, запишите загруженный образ на диск или воспользуйтесь нашими советая по созданию мультизагрузочной флешки. Утилита не имеет графического интерфейса, но пугаться этого не стоит — всё в ни довольно просто и понятно. К тому же часто нужная опция предлагается по умолчанию, так что от вас потребуется толь нажать клавишу Enter.

		M GNU GPL v2 license, see files on CD
**************************************	-	This utility will enable you to change or black the password of any user find. Administratory on an Windows NFZK/XP/Dista HEINOR knywhy how of a second seco
 Windows Reset Fassword / Registry Laitor / Boot CD 	2	* It also has a registry editor, and there is now support for * * * * * * * * * * * * * * * * * * *
 (c) 1998-2011 Petter Nordahl-Hagen, Distributed under GNU GPL v2 	5	* Tested on: NI3.51 & NT4: Workstation, Server, PDC. Hingk Prof. & Server to SP4. Cannot change AD.
DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES! THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE CAUSED BY THE (HIS)SUSE OF THIS SOFTWARE	-	XF MORES & FFOI: UP to TJAnnge AD Passabo 5253 A st Ulte 14 bits 53 Ad 25 Ab Store Program State 5253 A st HINT: If things soroll by too fast, press SHIFT-POUP/PODOWN
More info at: http://pogostick.net/~pnh/ntpasswd/ Email : pnh0pogostick.net	-	There are set of a supplication of a structure with a set of the structure of the set of
* CD build date: Wed May 11 20:16:09 CEST 2011	-	DON'T PANICY Usually the defaults are OK, just press enter all the way through the questions
Press enter to boot, or give linux kernel boot options first if needed. Some that I have to use once in a while: hoot nousb - to turn off USB if not used and it causes problems boot irgpoll - if some drivers hang with irg problem messages boot uga=ask - if you have problems with the videomode boot nodrivers - skip automatic disk driver loading boot:		Step ONE: Select disk where the Mindows installation is Bisks Jdev/sda: 21.4 GB, 21474036488 bytes Candidate Hindows partitions found ::

Загрузитесь со съёмного носителя Offline NT Password and Registry editor. Вам вряд ли понадобятся дополнительные опци загрузки, но в некоторых случаях придётся опытным путём подобрать те, которые помогут утилите запуститься. На следующе этапе надо выбрать номер раздела, на котором установлена Windows. Ориентироваться придётся в первую очередь по е размеру. В принципе, до самого последнего момента программа не вносит никаких изменений в Windows, поэтому в случ ошибки можно просто начать процедуру сброса пароля заново.

ingrow and souroodi, styrkong un strengen disk Arivers – Parking souro, when any the Mindows systems files stoned – File-select, when any the Mindows systems files stoned – File-select, when any the parts of peristry we result itself – If constances when and any work or other sources and you file	Gelected 2 Mountiny from /dev/sdp2, with assympt filesystem type NTFS 20, lett poally check if it is NTFS
DON'T PANIC! Usually the defaults are OK, just press enter all the way through the questions	Yes, poad-write seeмs OK. Mounting it, This may take up to a few minutes: Successt
Step ONE: Select disk where the Hindows installation is	Step THO: Select PATH and registry files
Disks: Disk ∕dev/sda: 21.4 GD, 21474036400 hytes Candidate Hindows warittions found:	DEBUG path: windows found as Windows DEBUG path: surtows? found as Sustem32 DEBUG path: sonf/g found as config DEBUG path: sonf/g found as config DEBUG path: found sover coser is b. /
	What is the path to the registry directory? (relative to windows disk) (Hindows System 2/000119)
Please steet partition by number or a survey is tart disk drivers m = manually select disk drivers to load f = fetch, additional drivers from floppy / usb	BERNES PATRI Dindows frann as stindows Dennes at the second secon
T = Enow prophable Windows (NTFS) partitions only Select: (1)	-Purrus a se
Selected 2 Manatan Canada Claudala, with annual Cilconnean tura NTEC	- 가내가 내기 다니, - 001 g 05c 0.102 4), [HContainer 관중 중 영향 영화 학교 학교 학교 학교 학교 영상 (COPPONENTS (6 6 6 e e d 2 e d - 6 e - 11 d e - 15 he d - 001 g 05c 0.102 4), [HContainer 관중 한 한 한 한 한 한 한 한 한 한 한 한 한 한 한 한 한 한
So, lety really obeck if it is wills?	1130 U 60 U
Yes, read-write seems OK, Mounting it. This may take up to a few minutes:	drukrukruk I 0 0 0 0 Jul 14 2009 Journal drukrukruk I 0 0 9 220140 Jan 12 11 15 BegBack
Successt	
Step TWO: Select PATH and registry files	-huxhuxhux I 0 0 79699300 7961 80 11 10 10 10 10 10 10 10 10 10 10 10 10
Sebuc path: system32 found as System32 Pebuc path: yonfy found as conig Sebuc path: found correct case to be: Windows/System32/config	Select which part of registry to load, use predefined choices or list the files with space as delimiter 4 - tassmorn,recet, sam, system peoprisyl,
What is the path to the registry directory? (relative to windows disk)	g _ guit = peturn to previous

Затем утилита попросит указать путь до папки, где находятся файлы SAM (фактически это куст реестра). По умолчанию э *X:/Windows/System32/config*, его же и предлагает вначале программа. Потом надо выбрать первый пункт (Password reset), т как мы собрались сбросить пароль.

Justicipando i B B 2024 2025 Jai 25 Ling Just Hundrautor i B B 2024 2025 Jai 25 Ling Just Select which part of prysistry to lark use predefined choices T Ist the flow and the space as deliniter T - Statut of a construction security - Suite spectrum i spectrum term (1) F od files; sam system security (1) F od files; f	Cupying tak system touping to find Stop THREE Password on peristru edit Stop THREE Password on peristru edit Stop Your Stop Stop Stop Stop Stop Stop Stop Stop
Step HANRE: Password or provising edit That we convert an digg of Hanne State and State and State and State Hanne Convert and the state and State and State and State and State Hanne Convert and State and State and State and State and State Hanne State and State and State and State and State and State Hanne State and State and State And State and State and State Hanne State and State and State And State and State and State Hanne State and State and State and State and State and State State and State and State and State and State and State and State State and State and State and State and State and State and State State and State and State and State and State and State and State and State State and State and	BOOT KRV -4,0655381,0858840898 + Subsey indexing type 1: 6866 [16] Nied Flow Asia: 15324979813381 Klosks/Asia: "Manusal" 4043/149888 STORENS/Lutes. Hive (SRCURITY, name (from header); cenRoetSusten2>Config% SECURITY Boot Rov : for a for a logistic best in under a logistic best store (fr Store Rov : for a logistic best in under a logistic best store (fr State for a data: 3269888 kylicks/Soverinunder at Marketa best store (fr)
Blog (SUSTRM) pares (Spogn Beader); (SUSTRM) Pile pize Sied for data: 152472/945153K filosker/sustants data/table bioderpage/sustant Sied for data: 152472/945153K filosker/sustant, data/table bioderpage/sustant Alve (SECURITY) name (Econ.beader); (embody/sustant22/config/SECURITY)	n Sahn spilou links: United San
BOOT NEV algoficari, BubBallaza = Subbey indexiany type is; 6666 (if) Used for alt: 32619572 byock/Sover "unus-d""TG74648 blocks/Sover. = SOM policy ijm(is:	<pre>Q=======(> ontpw Main Interactive Menu (>======(> Loaded hives: (SAN ≤ SUSTEN < SECURITY> 1 - Edit user data and passwords</pre>
paried Logins Extrem Incloud is Paried Logins Extrem Social () Social States Count () C)=======() Chntpm Main Interactive Menu ()=======()	2 − Queistry entropy now with rull write support to save) 4 − Rull (you will on asked if there is something to save) What to do? [13 ->
Loaded hives: (SAM) (SYSTEM) (SECURITY) 1 - Editusee data and passwords 7 - Registry editor, now with full write support! 9 - Registry editor, now with full write support! 9 - Registry editor, now with full write support!	ESSES SANEYE KAİL ÜSEF INFO & PASSWORDS SSES BID
Hhat to do? fil -> _	or simply enter the username to change: () 3DTH?

Дальше всё просто. Выбираем первый пункт (Edit user data and password) и вписываем имя пользователя или его идентификат в формате *0xabcd*, где *abcd* — это RID, указанный в первом столбце. RID пригодится, если имя пользователя некоррект отображается или его не получается ввести. Например, при использовании кириллицы.



Осталось указать пункт 1 (сброс пароля) или 2 (смена пароля) для выбранного пользователя. Выходим из режи редактирования пароля, введя восклицательный знак и нажав Enter.



Всё, почти готово. Вводим *q*, нажимаем Enter, а затем соглашаемся с внесением изменений, введя *y* и ещё раз нажав Enter Отказываемся от дальнейшей работы в Offline NT Password and Registry editor (*n*), извлекаем флешку или CD-диск и нажимае заветную комбинацию Alt+Ctrl+Del для перезагрузки. Готово — пароль сброшен!

<pre>Number of the second seco</pre>	<pre></pre>
u (SARA) - OR Step Polk: Weiting back changes About fourpite file(s) hackt bo it? [n] : y Weiting SAR warms EDIT COMPLETE memory War on try again if it somehow failed, or you selected wrong Men rung [n] :	You can try again if it somehow failed, or you selected wrong Hen rung.Tol: * end of coriging.preturning to the shell. * press CFRI-MIT-SET to reboot now (remove floppy first) * Obwersen it you would be action of the pression of the second * Obwersen it you would be action of the pression of the second * You may also restart the script procedure with 'sh /scripts/main.sh' = _

Это был простой способ сброса пароля Windows 7. Сложностей с ним быть не должно. Надо всего лишь быть внимательным аккуратным. Проблемы могут возникнуть только при отсутствии необходимых драйверов для работы с жёстким диском. Тог, придётся закинуть их на дискету (если вы, конечно, найдёте живого представителя этого почти вымершего вида и рабочи привод для него) или на USB-флешку и на первом этапе выбрать пункт fetch additional drivers.

Для второго и третьего способов понадобится только установочный диск Windows 7 и больше ничего. Более сложный вариа подразумевает включение изначально скрытой учётной записи «Администратор» путём правки реестра из установочной сред Windows 7. В дальнейшем можно будет войти в систему под этой учёткой и отредактировать любой другой аккаунт в ОС. І умолчанию «Администратор» не имеет пароля, что только играет нам на руку.

	a numera a Manfrana		6	Редактор рестра Правка Вид Избра	ное Справка				
				Инпорт Экспорт		По утолчанию)	Twn REG_SZ	Значение (значение не присвоено	
	диннистратор Xi\windows\system32\cmd.exe ensoft Vindows [Version 6.1.758]11			Выгрузить куст					
X : \	Sources>regedit			Падключить сетевой реек Отключить сетевой реек					
				Печаты	CTRL +P				
				Buotog					
		Y	3	агрузка файла куста реестр	a s peecrp.			¥	
•		Далее		Ф Корпорация К					Dance

Итак, загружаемся с установочного диска и нажимаем Shift+F10 для вызова командной строки, где вбиваем *regedit* и жмём Ent для запуска редактора реестра.



Выделяем раздел *HKEY_LOCAL_MACHINE*, а в меню выбираем «Файл» → «Загрузить куст...» (File → Load hive...). Нам на, открыть файл SAM, который находится в папке |*Windows*|*System32*|*config* на том разделе, где установлена Windows 7. П_I открытии будет предложено ввести имя загружаемого куста — вбивайте любое.



Теперь надо выбрать раздел *HKEY_LOCAL_MACHINE|имя_куста|SAM|Domains|Account|Users0001F4* и дважды кликнуть по клю *F*. Откроется редактор, в котором надо перейти к первому числу в строке 038 — это 11. Его надо изменить на 10. Будь аккуратны и не ошибитесь — поменять надо только его, не добавляя и не удаляя другие числа!



Теперь надо выделить наш куст *HKEY_LOCAL_MACHINE* и*мя_куста* и в меню выбрать «Файл» → «Выгрузить куст...» (File Unload hive...), а затем подтвердить выгрузку куста.



Всё, можно перезагрузиться, вытащив предварительно установочный диск, и войти в систему под администраторским аккаунто В панели управления Windows в разделе управления пользователями можно изменить настройки другой учётной записи. В то числе поменять пароль.



Остался последний способ, неправильный. Почему неправильный? Потому что мы займёмся подменой системных файлов, а э дело неблагородное. В чём заключается основная идея? Всё просто — в ОС по умолчанию включена функция детектирован залипающих клавиш. Вы с ней наверняка сталкивались хотя бы раз, а если нет — то просто быстро нажмите Shift не менее 5 ра и вы увидите вот такое замечательное окошко:

Sticky Keys
Do you want to turn on Sticky Keys?
Sticky Keys lets you use the SHIFT, CTRL, ALT, or Windows Logo keys by pressing one key at a time. The keyboard shortcut to turn on Sticky Keys is to press the SHIFT key 5 times.
Go to the Ease of Access Center to disable the keyboard shortcut
Yes No

Окошко это принадлежит маленькой вспомогательной программке *sethc.exe*, которая лежит в системной директории Window Более того, она запускается даже на экране приветствия, когда вам предлагают выбрать пользователя и ввести пароль. Но ве, её можно заменить чем-нибудь полезным. К примеру, *cmd.exe*. Естественно, не прямо в запущенной OC, а загрузившись установочного диска Windows 7 и нажав Shift+F10.

Aдминистратор: X:\windows\system32	\cmd.exe	
\X:\sources>dir c:\ Том в устройстве С имеет метку Серийный номер тома: 74С9-9806	ј Зарезервировано систем)	ой
Содержимое папки с:\		
Файл не найден		
X:\sources>dir d:\ Том в устройстве D не имеет ме Серийный номер тома: A0CB-177F	атки. 7	
Содержимое папки d:\		
11.06.2009 00:42 11.06.2009 00:42	24 autoexec.bat 10 config.sys	
14.07.2009 05:37 (DIR) 21.11.2010 05:39 (DIR)	PerfLogs Program Files	
19.01.2012 14:34 (DIR) 19.01.2012 14:34 (DIR)	Windows 24 casis	
4 папок 13 440	774 144 байт свободно	
X:\sources>_		
Koonopause Mažkpocoér (Microsoft Corp.) 200	9. Все права защищены.	

Начать надо с определения буквы диска, на котором установлена Windows. Самое легкое — просто просмотреть содержим корня раздела командой *dir*. С:, скорее всего, будет виден как D:, но необязательно.

y scranobka willu	luws		
🔜 Администрато	op: X:\windows\system32\/	cmd.exe	
Файл не найде	н		
X:\sources)di Том в устрой Серийный ном Содержимое п 11.06.2009 б 14.07.2009 б 21.11.2010 б 19.01.2012 1	ir d:\ iстве D не инест не: нер тона: AOCB-177F Naпки d:\)0:42)0:42)5:37 <dir>)5:37 <dir>)5:39 <dir>)5:39 <dir></dir></dir></dir></dir>	гки. 24 autoexec.bat 10 config.sys PerfLogs Program Files Users	
X:\sources>co Ckonupomano ¢	2 файлов 4 папок 13 440 ору d:\Windows\Systematizet	34 байт 34 байт 274 144 байт свободн em32\sethc.exe d:\	D
Х:\sources)co Заменить d:\\ Скопировано ф	рру d:\Windows\Syste Vindows\System32\se райлов: 1.	em32\cmd.exe d:\Wind thc.exe [Yes (ga)/No	ows\System32\sethc.exe (нет)/All (все)]: у
X:\sources>_			
🖲 Корпорация Ма	айкрософт (Microsoft Corp.), 2009		Далее

Определившись с буквой тома, выполняем две простые команды — одной копируем на всякий случай оригинальный фаi *sethc.exe* в корень диска или куда душе угодно, а второй меняем его на *cmd.exe*.

1 copy d:\windows\system32\sethc.exe d:\
2 copy d:\windows\system32\cmd.exe
d:\windows\system32\sethc.exe

Перезагружаемся, быстро нажимаем несколько раз клавишу Shift (или Ctrl, или Alt) и наблюдаем окно с командной строкой. нём надо ввести ещё одну команду, подставив соответственно имя нужного пользователя и новый пароль. С други параметрами этой команды можно ознакомиться в официальной справке.

1 net user имя_пользователя новый_пароль

EN	🔤 Адлиниктратор: sethc.exe					
	Microsoft Windows [Version 6.1.?601] (с) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.					
	C:\Windows\system32>net user 3DTW7 newpassword Команда выполнена успешно.					
	C:\Windows\system32>					
	3DTW7					
	Пароль					
C	🖲 🥵 Windows 7 Максимальная 🔤	D -				

Если вы захотите вернуть всё на круги своя, то надо снова загрузиться с установочного диска, открыть консоль и выполни команду:

1 copy d:\sethc.exe d:\windows\system32\sethc.exe

Впрочем, можно ничего не восстанавливать, а оставить такой маленький трюк в системе на всякий случай. Помиг перечисленных выше способов, есть множество других методик сброса или восстановления пароля в Windows, но сейчас мы рассматривать не будем. Ещё раз призываем наших читателей быть внимательными и аккуратными при работе с внутренностяг ОС, а ещё лучше не доводить ситуацию до «хирургического» вмешательства в SAM. Удачного вам восстановления доступа учётным