زکات علم آموزش و انتقال آن به دیگران است

مقدمه ای از خودم

متاسفانه کسی حوصله ی خواندن مقدمه ی کتاب ها و مقالات را ندارد ولی شما این بار را طاقت بیارید اصلا کامل کتاب رو مطالعه کنید اگر مفید بود زحمت خواندن مقدمه و مخصوصا در خاتمه به نکته ای اشاره کرده ام که از شما خوانندگان گرامی خواهش دارم که حتما آن را مطالعه نمایید .

در میان فناوری های عصر جدید جایگاه علوم کامپیوتر و نقش آفرین آن در تمام زمینه ها بر همگان معلوم است و این در حالیست که هر روز عمق و گستردگی بیشتری پیدا می کند و البته این علم همچون سایر علوم می تواند در مواردی استفاده های منفی هم داشته باشد که بیمار دلان در این عرصه خباثت درون خود را به نمایش می گذارند و با کسب تخصص و مهارت های نفوذ در حریم شخصی دیگران و مخدوش کردن امنیت جامعه در قالب علم هک به انواع سرقت ها و تجاوز به حقوق دیگران و کار های غیر اخلاقی می پردازند و لذا ارائه اطلاعاتی در زمینه هک و روش مقابله با آن افراد غیر مسئول که حرمت های اخلاقی و انسانی را نادیده می گیرند و حفاظت از حریم شخصی افراد حقیقی و حقوقی کاری است که هرچند بضاعت علمی اینجانب بسیار اندک است ولی شاید سهم خود را با این مقاله و اگر خدا بخواهد با مقالات بعدی توانسته باشم ادا نمایم و باز هم شاید این کار بسیار کوچک مقبول درگاه ایزد منان قرار گیرد آنچه را خدا بپذیرد هرچند بسیار کوچک و حقیر باشد چون مقبول حق افتد در واقع بزرگ خواهد شد .

Windows Hacking and Security Book

Only Physical Access

Lesson 2

Author : Moslem Haghighian

L4tr0d3ctism

Location : Sanandaj

L4tr0d3ctism(47)Y4h00•com , L4tr0d3ctism(47)H0tm4il•com , L4tr0d3ctism(47)Gm4il•com

Spider Security Team

Greeting to :

SHabgard Digital Security Groups Members

Black Hat Group Security Center members

هک و امنیت در سیستم عامل ویندوز فقط در دسترسی های فیزیکی

درس دوم

مولف : مسلم حقیقیان

L4tr0d3ctisn@yahoo.com , l4tr0d3ctism@gmail.com , L4tr0d3ctism@hotmail.com

تیم امنیتی SpideR

سنندج

هشدار **1** :

کلیه ی مطالب گفته شده در این کتاب فقط و فقط جنبه آموزشی دارد استفاده ی نادرست از آن به عهده ی خود کاربر است و نویسنده ی کتاب هیچ مسئولیتی در قبال استفاده نادرست از مطالب گفته شده را نمی پزیرد .

هشدار **2** :

این کتاب برای تمامی خوانندگان و کاربران به صورت کاملا رایگان می باشد و تنها هدف برای نوشتن این کتاب بالا بردن سطح علمی دانشجویان و کاربران کامپیوتر و مدیران امنیتی و ... می باشد تمامی حقوق معنوی کتاب متعلق به مؤلف کتاب یعنی مسلم حقیقیان می باشد .

فقط به خواندن این کتاب اکتفا نکنید بعد از خواندن تمامی درس های این مجموعه به سراغ مفاهیم پیشرفته در زمنیه ی سیستم عامل بروید . در صورتی که کل کتاب را هم خوب درک کرده اید خود می توانید مفاهیم پیشرفته را ادامه دهید .برای این کار هم بنده خودم گوگل را به شما پیش نهاد میکنم . در صورتی که در این راه به مشکلی بر خوردید می توانید به من میل بزنید تا شما را راهنمایی کنم .در ضمن در این مقاله بیشتر سطح علمی مقاله مد نظر بنده بوده تا مشکلات نگارشی و املایی آن .

فهرست مطالب

پسورد برنامه Winrar

نحوه ی دور زدن پسورد برنامه های قفل کننده فایل و فولدر

- نحوه ی حذف پسورد برنامهAccess Administrator
- نحوه ی حذف پسورد برنامه Click And Lock1
- نحوه ی حذف پسورد برنامه Program Protector
- نحوه ی حذف پسورد برنامه Ashampoo Magical Security
- نحوه ی حذف پسورد برنامه Anfibia Deskman
- نحوه ی حذف پسورد برنامه Access lock
- نحوه ی حذف پسورد برنامه Private Encryption
- نحوه ی حذف پسورد برنامه XP Smoker
- نحوه ی حذف پسورد برنامه Lock My Pc
- نحوه ی حذف پسورد برنامه PC Security Tweaker
- نحوه ی حذف پسورد برنامه PC Security
- نحوه ی حذف کردن پسورد برنامه Securr Browser
- نحوه ی حذف کردن پسورد برنامه Securr Browser
- نحوه ی حذف پسورد برنامه Password Door
- نحوه ی حذف کردن پسورد برنامه FolderMage Pro
- نحوه ی حذف پسورد برنامه Stealth Encrypto
- نحوه ی حذف پسورد برنامه Private Desktop
- نحوه ی حذف پسورد آنتی ویروس nod32
- نحوه ی حذف پسورد برنامه USB Disk Security
- نحوه ی حذف پسورد برنامه Hide My Folders
- نحوه ی حذف پسورد برنامه Private Pix
- نحوه ی حذف پسورد برنامه Clear Lock
- نحوه ی حذف پسورد برنامه Security Administrator
- نحوه ی حذف کردن پسورد برنامه Anti porn
- نحوه ی حذف پسورد برنامه FolderGuard

استخراج و کرک رمز های عبور

کلمات عبور یکی از معمولی ترین و متداول ترین ابزار و در عین حال مهمترین روش در تامین امنیت در دنیای کامپیوتری می باشد ، کلمه ی عبور در دنیای مجازی به منزله ی کلید قفل یک خانه در یک آپارتم می ماند در صورتی که کلید گم شود و در اختیار یک فرد گذاشته شود می تواند با ورود به خانه ی شما کلیه ی اطلاعات محرمانه و شخصی شما را به سرقت ببرد .کلمه ی عبور یا به اصطلاح پسورد هم همین گونه است در صورت لو رفتن این کلمات افرادی می توانند با ورود به سیستم ها کلیه ی اطلاعات محرمانه را بردارند.

در بسیاری از سازمان های مهم یک کلمه ی عبور از بسیاری از اطلاعات محرمانه ی آن سازمان در برابر افراد ناشناس محافظت می کند و می شود گفت که مهمترین اطلاعات یک کشور بسته به یک یا چند کلمه ی عبور می باشد

حساب های کاربری و کلمات عبور

حساب های کاربری راهی برای شناساندن کاربران در سیستم عامل می باشد . به طور کل یک حساب کاربری در ویندوز مخصوص یک کاربر و یا چند کاربر خاص بوده و برای اینکه از ورود افراد ناشناس به حساب های کاربری جلوگیری شود ویندوز کلمات عبور را برای هر حساب کاربری مشخص کرده و یشه گفت که حساب های کاربری برای حفظ امنیت در سیست هستند.

در اکثر سیستم ها زمانی که یک درخواست جهت تشخیص هویت دریافت میکنند ، به منظور تکمیل چرخه ی احزار هویت دو معیار کلی یعنی حساب کاربی و کلمه ی عبور (در صورت وجود) از کاربر در خواست می کنند .حساب های کاربری و کلمه ی عبور هر دو در یک راستا وجود دارند حساب کاربری و کلمه ی عبور هر دو مکم یکدیگرند .برای حساب های کاربری می توان کلماتی را مانند User name,

Login , Id , User Idو ... را به کار ببریم .حساب های کاربری معمولا بر اساس نام کاربر مثلا Moslem یا نوع کار و وظیفه ی آن مثلا Admin و یا Member یا بر اساس نوع کاری که انجام می دهد و یا کد مخصوص کاربری و در ایران بر اساس اسم عزیزان خودشان انتخاب می شود ☺

سیستم عامل ویندوز به صورت پیش فرض دارای یک سری حساب های کاربری بوده که مهمترین آنها Admisnitrator , Guest بوده حساب کاربری Guest مخصوص مهمان بوده و دارای کمترین سطح دسترسی می باشد و به صورت پیشفرض غیر فعال بوده ولی حساب administrator همیشه فعال بوده این حساب مخصوص مدیر اصلی و دارای بیشترین سطح دسترسی می باشد و یک سطح دسترسی با نام System هم هست که مخصوص خود سیستم عامل می باشد .

گروه های کاربری

سیستم عامل ویندوز برای جلوگیری از سو استفاده های کاربران برای هر کاربری وضعیتی مشخص و محدودیت هایی مشخص اعمال کرده است . گروه های کاربری به دو دسته تقسیم می شوند

- گروه های موجود در یک سیستم محلی (مستقل)
- گروه های موجود در یک شبکه
- گروه های موجود در یک سیستم محلی (مستقل)

نوع اول کاربرانی هستند ما می توانیم آنها را به کاربر و یا حساب کاربری خواص نسبت دهیم . در یک سیستم محلی کاربران هم به طو کلی به 3 گروه تقسیم می شوند

1 - گروه مدیران سیستم

2 - گروه کاربران محدود شده

3 - گروه کاربران مهمان

گروه اول که کاربران ویژه و اصلی هستند. آنها دارای بالاترین سطح دسترسی می باشند. کاربرانی جزء این گروه هستند جز مدیران سیستم به حساب می آیند.

گروه کاربران محدود شده هم گروهی از کاربران هستند که به صورت غیر دائم بر روی سیستم مشغو به فعالیت هستند این گروه از کاربران زیر مجموعه ی مدیران سیستم هستند.

گروه سوم هم که مخصوص مهمان هایی هستند که به صورت ره گذر با سیستم کار میکنند . این گروه محدود ترین گروه در سیستم عامل است .

فرق این 3 گروه را می توانید در جدول زیر مشاهده کنید

	مدیر اصلی	محدود شده	مهمان
نصب برنامه و سخت افزار جدید	☺	☹	☹
اعمال تغییرات اساسی در سیستم	☺	☹	☹
دسترسی به فایل های غیر محرمانه و خواندن آنها	☺	☹	☹
ایجاد و حذف حساب های کاربری	☺	☹	☹
تغییر حساب های کاربری سایر کاربران	☺	☹	☹
تغییر نام و نوع حساب های کاربری خود	☺	☹	☹
تغییر تصویر نمایشی خود هنگام ورود	☺	☺	☹
ایجاد ، تغییر و یا حذف گذر واژه	☺	☺	☹

این گروه هم خود دارای انواع مختلف هست که طبق نیاز کاربر باید هر کاربری را عضو یکی از گروه ها کنیم .در اینجا به چند مورد از گروه های کاربری اشاره می کنم

Administrator	کاربران عضو این گروه دارای بالاترین سطح دسترسی و مدیران اصلی سیستم محسوب می شوند
power users	کاربران این گروه هممعاونین مدیر حساب می شوند و ما بقیه ی گروه ها را می توانند تغییر یا حذف و اضافه کنند نکته : اصلی ترین کار این گروه Sharingاست .
Guests	کاربران این گروه محدود ترین کاربران هستند که در بالا شرح دادیم .
backup operators	اعضای این گروه امکان گرفتن نسخه ی پشتیبان و اجرای آن و همچنین ریستور کردن سیستم هستند .
network configuration operators	اعضای این گروه می توانند کلیه ی خط فرمان های وینوز و شبکه را اجرا کنند .
remote desktop users	اجزای این گروه امکان دسترسی رموت به یک سیستم واقع در شبکه را دارند .
replicator group	اعضای این گروه در شبکه می توانند عملیات replication و مدیریت بر روی فایل را به صورت کامل انجام دهند . کار اصلی آنها همسان سازی **DC** ها در شبکه می باشد .
users group	اعضای این گروه همان کاربران محدود شده ای هستند که در بالا شرح دادیم . این کاربران بر اساس مجوز های تعیین شده به منابع دسترسی دارند .
debugger users	همان طور که از نام آنها پیداست اعضای کاربران عضو این گروه می توانند کارهای اشکال یابی را در سیستم های شبکه ای و محلی انجام دهند
help service groups	کاربران این گروه دارای امکاناتی برای کمک به کاربران دیگر در شبکه و یا سیستم های محلی هستند . کاربران دیگر در هنگام برخورد با مشکل به این گروه ها مراجعه می کنند .

گروه های موجود در یک شبکه

اعضای موجود در این گروه هنگامی کاربرد دارند که ما عضو یک شبکه یا دامنه ی کار و یا اینکه سیستم عضو یک گروه کاری باشد . ما نمی توانیم حساب کاربری خاصی ا عضو این گروه قرار دهیم بلکه اعضای این گروه بنابر کار و یا وظیفه ای که انجام می شوند عضو یکی از این گروه ها می شود

هنگام ایجاد محدودیت ها و دادن مجوز ها بر روی یک منبع به اشتراک گذاشته شده در شبکه این گروه ارزش زیادی دارند.

در اینجا به ذکر چند ورد از این گروه ها می پردازم .

every one	**تمامی کاربرانی ه به کامپیوتر دسترسی پیدا میکنند عضو این گروه می شوند**
authenticated users	کاربرانی که با حساب های معتبر وارد سیستم می شوند عضو این گروه می شوند
anonymous log on	کاربرانی که به صورت ناشناس (مهمان)، بدون استفاده از یک حساب کاربری معتبر وارد سیستم می شوند عضو این گروه محسوب می شوند
creator owner	هر کاربری که در سیستم یک فایل ویا ... ایجاد کند عضو این گروه می شود
dial up	کلیه ی کاربرانی که با استفاده از شماره گیری به شبکه و یا سیستم شما متصل شوند عضو این گروه می شوند .
intractive group	کلیه ی کاربرانی که دسترسی محلی به سیستم دارند عضو این گروه می شوند
Network group	کلیه ی کاربران متصل به شبکه و کاربرانی که از طریق شبکه وار سیستم می شوند عضو این گروه می شوند .

هدف اصلی نفوذگر

حال که شما با گروه های کاربری و حساب های کاربری آشنا شدید به سادگی راحل زیر را هم درک می کنید و می فهمید که حساب Adminsitrator چه اهمیتی دارد.

یکی از مهمترین موضوع برای یک هکر ورود به یک حساب کاربری با دسترسی Power Users یا administrator به منظور سوء استفاده بیشتر از سیستم جهت بدست آوردن اطلاعات مهم مانند پسورد های حساب های کاربری که با داشتن آن هکر مالک سیستم خواهد شد .در این مقاله قصد دارم به روش های مختلف این کار و نحوه ی مقابله با آن را شرح دهم .

اطلاعات کلی

تا حالا شاید فکر کرده باشید وقتی که هر بار که ما با وارد کردن User , Password وارد سیستم می شویم .چگونه سیستم از صحت و سقم پسورد با خبر می شود .مثلما این نشانگر آن است که حساب های کاربری و پسورد های سیستم در داخل یک فایل یا DataBase ذخیره می شود و سیستم در هر بار تلاش کاربر برای ورود به سیستم ، پسورد وارد شده توسط کاربر با را پسورد درون DB مقایسه می کند در صورت درستی کاربر به سیستم وارد می کند و در غیر این صورت کاربر را با پیغام خطا متوقف می کند .

درسیستم عامل ویندوز فرآیند بالا با استفاده از زیرسیستم Security یا همان LSA (**L**ocal **S**ecurity **A**uthority) انجام می شود.بدین گونه که در هر بار که کاربر قصد ورود به سیستم را دارد پسورد وارد شده، توسط LSA به پایگاه داده ای به اسم SAM که کلیه ی پسورد های حساب های کاربری را در خود دارد (در همین مقاله با SAM DB هم آشنا می شوید) فرساده می شود و مقایسه ای انجام می شود و در صورت درستی کاربر به صفحه ی Desktop راهنمایی می شود و در صورت نادرستی ا کاربر درخواست می شود که دوباره پسورد را وارد نماید . برای بالا برن دسترسی هکر از روش های زیادی استفاده می کند که بعضی از روش ها را برای دسترسی به حساب های کاربری Administratorرا شرح می دهیم .

ورود به حساب کاربریadministrator

اولین روش در عبور از پسوردی که کاربران در ویندوز XP برای یوزر های خود انتخاب میکنند قبل از ورود ویندوز در Welcom Screen وارد شدن به حساب مدیر کل یعنی administrator هست (این حساب کاربری به صورت پیش فرض در کلیه ی ویندوز ها وجود دارد) که برای این کار باید Alt + Ctrl + Duble Delete را بزنید و ر پنجره ی زیر ظاهر می شود

ما باید در قسمت User name : کلمه ی administrator رو تایپ کنید و کادر پسورد را هم خالی بگذارید . در صورتی که بر روی administrator پسورد نداشته باشند وارد آن میشوید و شما می توانید پسورد را تغییر دهید.

اما این روش در ویندوز 7 و ویستا عملی نیست چونکه پیش فرض حساب کاربری administrator غیر فعال می باشد و برای فعال کردن آن باید از فرمان Net User Administrator password /active:yes استفاده کنیم .

روش مقابله :

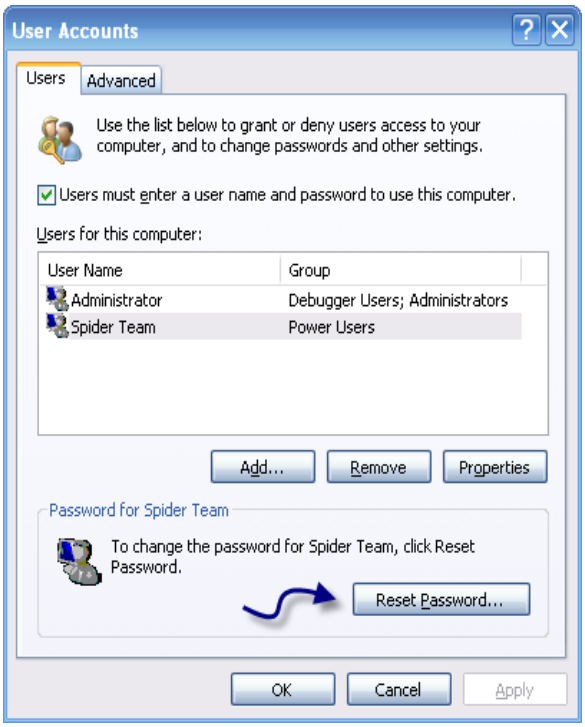
گزاشتن پسورد بر روی این حساب کاربری Administrator از ورود افرادی که دسترسی لوکال یا رموت دارند و می خواهند بدون مجوز وارد سیستم شوند جلوگیری می کند . این بحث فقط مربوط به حساب اصلی نیست بلکه مربوط به کلیه ی حساب های کاربی در ویندوز است بهتر است هیچ حساب کاربری را بدون پسورد نگذاریم.

استفاده از فرامین و ابزار های خود ویندوز

خود ویندوز هم یک سری ابزار ها و فرامین را در اختیار ما گذاشته که حتی بدون دانستن پسورد قبلی ، پسورد های جدید را برای حساب های کاربری انتخاب کنیم . این فرامین و ابزار ها فقط در محیط های که از نوع administrator ، Power Userو یا حسابی که این اجازه به آنها داده شده اند قابل استفاده است .مثلا حساب های کاربری که در هنگام نصب ویندوز ساخته می شوند اجازه انجام این کار ها را دارند . شما در صورتی که وارد ویندوز شده باشید می توانید از این امکانات استفاده کنید .البته این ابزار ها در اصل برای کاربران حرفه ای ویندوز و مدیران شبکه ساخته شد ولی دیده می شود که استفاده های اشتباه هم از آن می شود

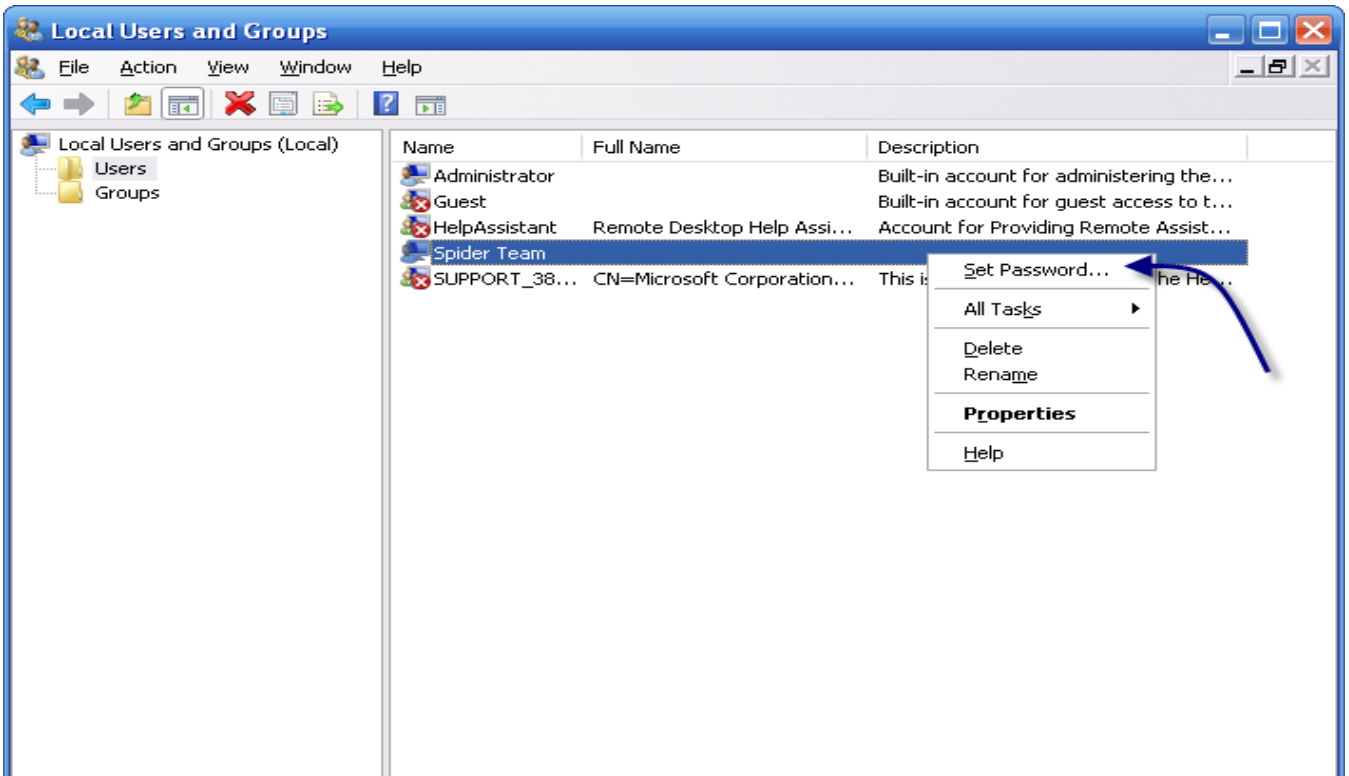
User Accounts (Control Userpasswords2)

وارد Run شوید و سپس کلمه ی Control Userpasswords2 را وارد کنید اینتر را زده . پنجره زیر ظاهر می شود . در پنجره ظاهر شده حساب کاربری مورد نظر را انتخاب کنید و سپس بر روی دکمه ی Reset Password... کلیک کنید و در کادر ظاهر شده پسورد جدید را بنویسید .(نیازی به پسورد قبلی نیست)



(lusrmgr.msc) Local Users And Groups

وارد Run شوید و تایپ کنید lusrmgr.msc تا پنجره ی زیر ظاهر شود .



بر روی پوشه ی UserS رفته و بر روی حساب کاربری مورد نظرمون کلیک راست کرده و سپس گزینه ی ... Set Password را می زنیم و اگر پیغامی هم ظاهر گزینه ی Proceed را بزنید . سپس پسورد های جدید را وارد کنید (نیازی به دانستن پسورد قبلی نیست)

Net User Command

وارد Run یا Ms-Dos شوید و سپس تایپ کنید

Net User AccountName Passoword

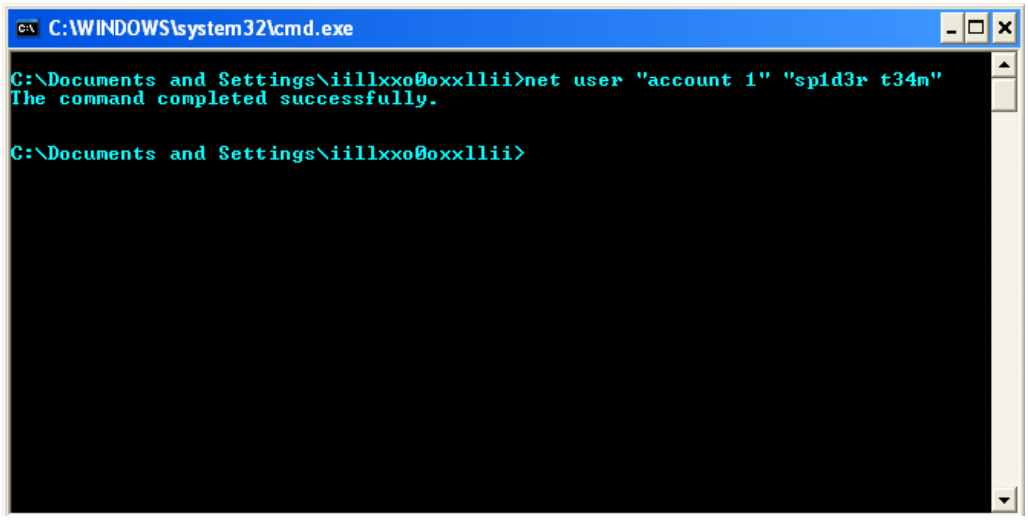
به جای AccountsName نام حساب کاربری مورد نظر را بنویسید و به جای Password کلمه ی عبور جدید را وارد نمایید.

به عنوان مثال در صورتی که نام حساب کاربر شماspider بوده شما می توانید به شکل زیر عمل کنید.

Net User Spider p4ssw0rd

این فرمان پسورد حساب کاربری Spider را به p4ssw0rd تغییر میدهند.

مثال 2:



در این مثال پسورد حساب کاربری Account 1 بهsp1d3r t34mتغییر پیدا کرده.

نکته 1 : فاصله رعایت شود

نکته 2 : بزرگی و کوچک بودن حروف نقشی در فرمان ندارد اما در پسوردی که برای حساب کاربریمان انتخاب می کنیم نقش دارد

نکته 3 : در صورتی که می خواهید در پسورد و یا نام حساب کاربری فاصله بگذارید باید از "" استفاده کنید مثلا

Net user "U S E R" "P a S s W o R d"

در این صورت پسورد به Spider Team تغییر میکند (به کوچکی و بزرگی حروف در پسورد دقت کنید(

نکته 4 : اگر می خواهید پسورد را حذف کنید می توانید از علامت "" استفاده کنید به شکل زیر

Net User User “”

این فرمان پسورد را حذف می کند.

روش مقابله در جلوگیری از استفاده از این فرامین و ابزار ها

برای جلوگیری از این امر باید به هر کاربر بر اساس نیاز کاری به حساب کاربریشان مجوز داده شود. حدالمقدور از دادن مجوز مدیر سیستم به کاربر جلوگیری شود اگر حساب کاربری Guests داده شود به کاربر اجازه ی این کار داده نمی شود .

برای ایجاد مجوز ها و مشخص کردن مجوز ها برای یک حساب خواص می توانید از روش های زیر استفاده کنید .

در Local And Users Groups بر روی پوشه ی Users رفته و بر روی حساب کاربری مورد نظر کیک راست می کنیم و سپس گزینه Properties را انتخاب می کنیم و در سربرگ دوم آن (Member Of) روی گزینه

ی Add کلیک می کنیم و در پنجره ی Select Groups بر روی دکمه ی Advanced... کیک میکنیم و سپس لیستی از مجوز را برایمان ظاهر می گردد و ما می توانیم یکی از گروه ها را برای کاربر مورد نظر انتخاب کنیم

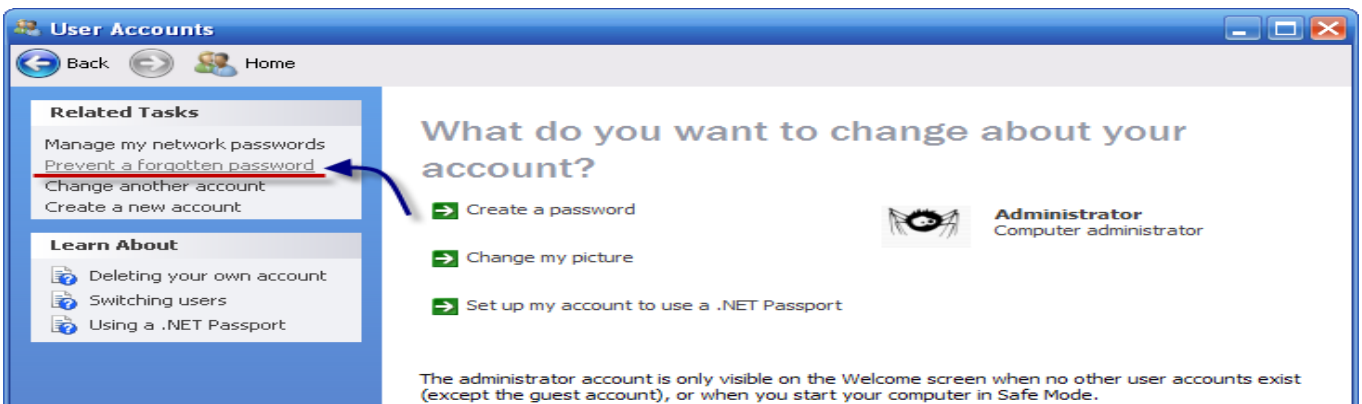
ایجاد دیسکت حذف کننده ی پسورد

یکی دیگر از امکاناتی که در ویندوزهای مایکروسافت وجود دارد استفاده از امکان ایجاد یک دیسک برای ریست کردن پسورد می باشد .این دیسکت در هنگامی که ما در صفحه ی لوگین هستیم و پسورد هیچکدام ار حساب ها را نداریم کاربرد دارد و از طریق آن می توانیم پسورد حساب کاربری Administrator را تغییر بدهیم .

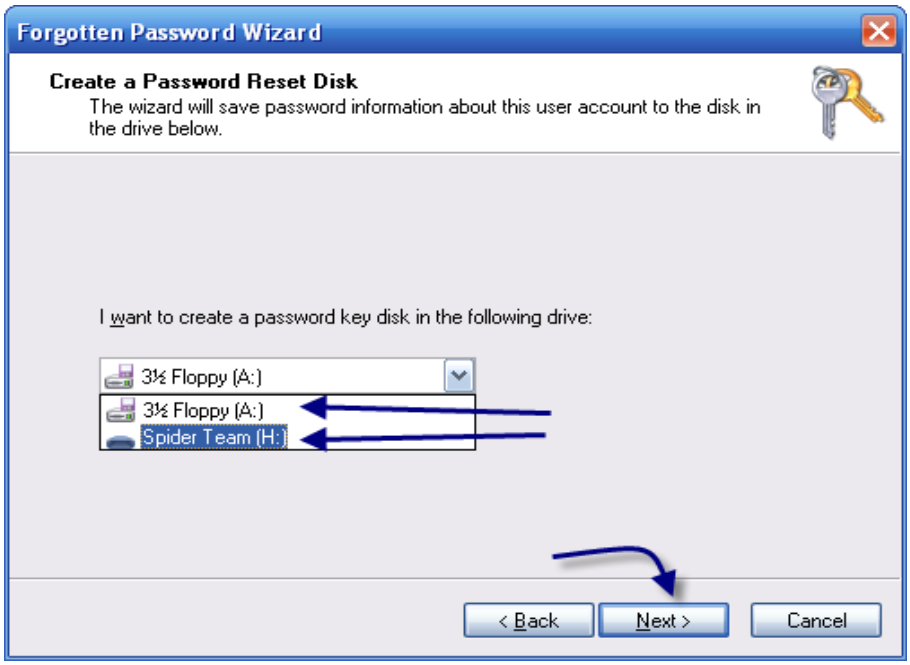
یک نفوذ گر می تواند در صورتی که فرصتی 20 ثانیه ای پیدا کند بر روی سیستم شما بیاید و فورا یک دیسکت ایجاد کند و سپس بعدا و یا هروقتی که بخواهد از آن دیسکت برای ریست کردن پسورد استفاده کند .و یا اینکه در سیستم به دنبال فایل با پسوند PSW باشد که بتواند از طریقق آن به ریست کردن پسورد بپردازد .

برای ایجاد این دیسکت ها وارد User Account می شویم و درقسمت چپ پنجره بر روی گزینه یPrevent a Forgotten password کلیک می کنیم به شکل زیر (این مراحل تمامی ویندوز ها به همین شکل می باشد .)

بعد از کلیک بر روی این گزینه پنجره ی زیر ظاهر می شود در پنجره ی ظاهر شده بر رویNext کلیک می کنیم .



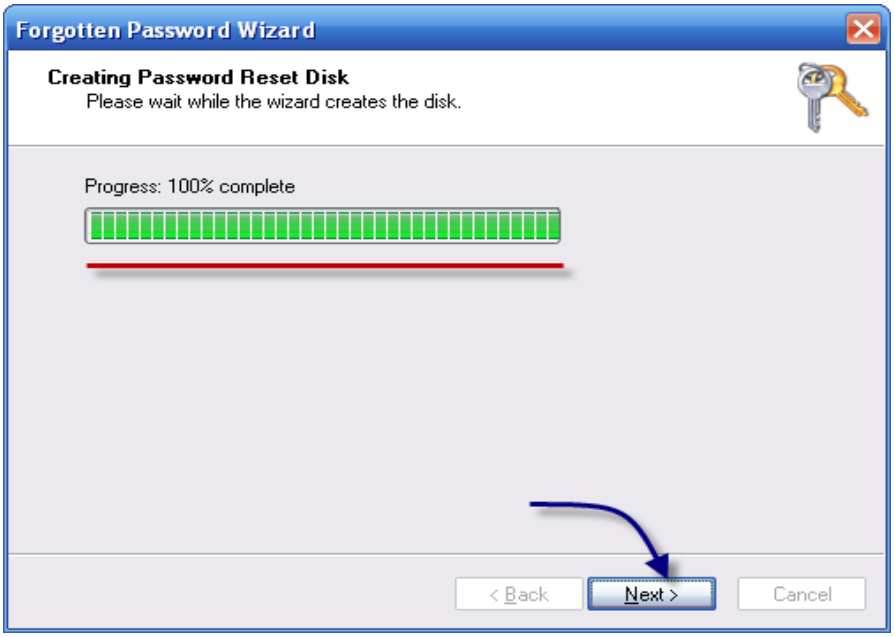
بعد از کلیک بر روی گزینه Next در مرحله ی بعدی باید دیسکتی که می خواهیم فایل دیسک ریست بر روی آن قرار گیرد را انتخواب میکنیم . توجه کنید که در این قسمت فقط فلاپی دیسک و یا UsB ما می آید و انتخاب آنها باعث Format شدن آنها نمی شود .



بعد از زدن Next در مرحله ی بعدی هم باید پسورد فعلی خودمان را وارد کنیم .

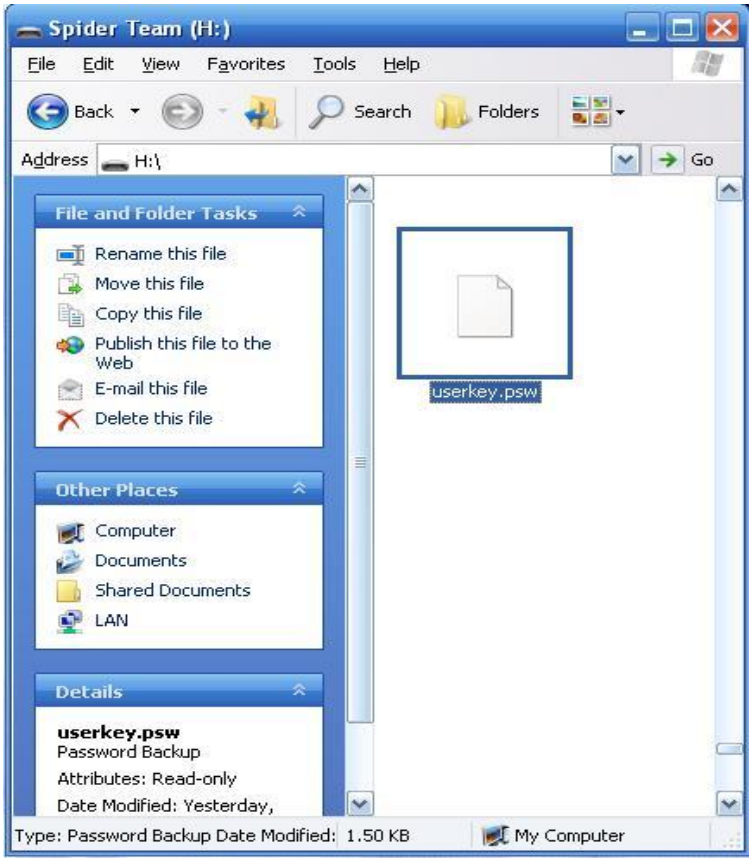
در صورتی که پسوردی بر روی حساب کاربری نداشته باشیم کادر را خالی گذاشته و بر روی گزینه ی Nextکلیک می کنیم .

با زدن Next سیستم شروع به ایجاد این دیسکت می کند و بعد از کامل شدن شما ی توانید بر روی Next کلیک کنید و سپس Finish را بزنید .



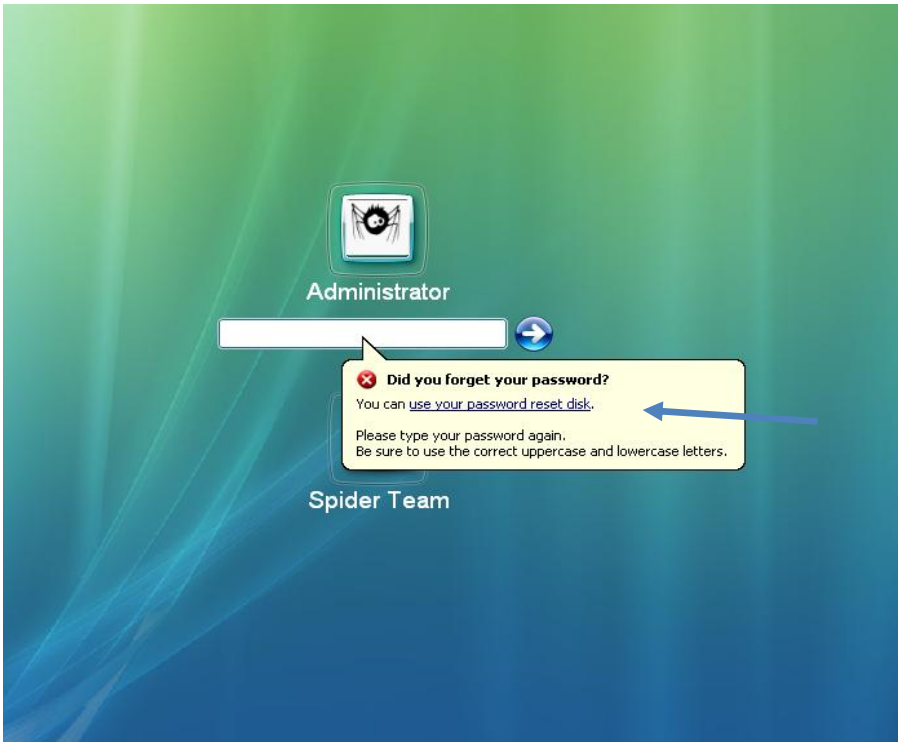
به شکل زیر

در اینجا دیگر فایل شما آماده شده و شا می توانید از آن استفاده کنید .



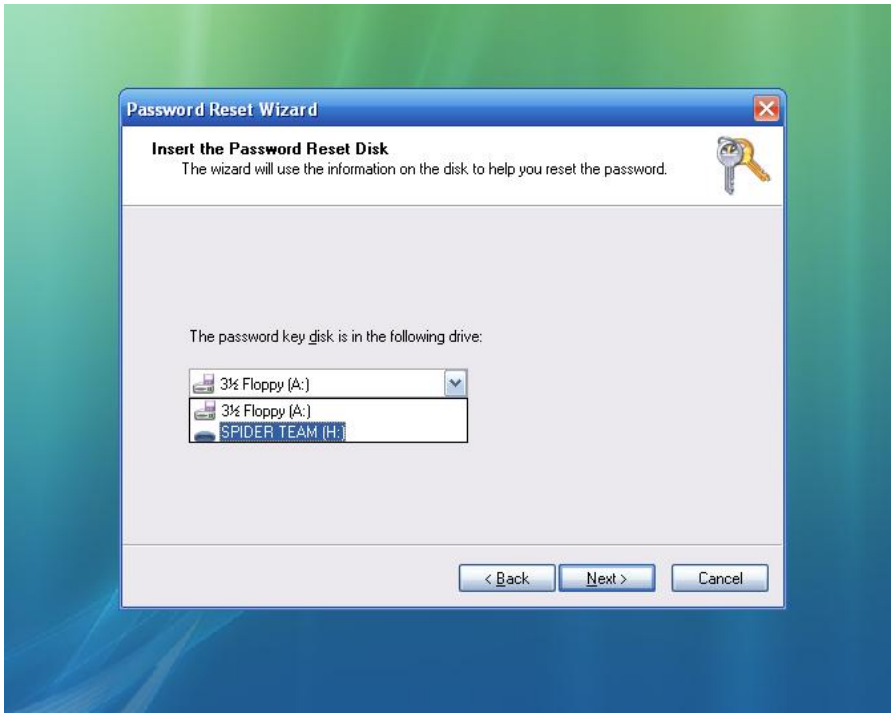
ولی چگونه از این دیسکت استفاده می کنید ؟

به عنوان مثال شما بعد از ایجاد این دیسکت می توانید Switch User کنید و سپس روی حساب Adminsitrator کلیک کنید و پسورد را اشتباه وارد کنید در این هنگام پیغای می آید و در آن می گوید آیا می خواهید که از دیسکت ریست کننده استفاده کنید ؟ شما بر روی آن کلیک کنید .



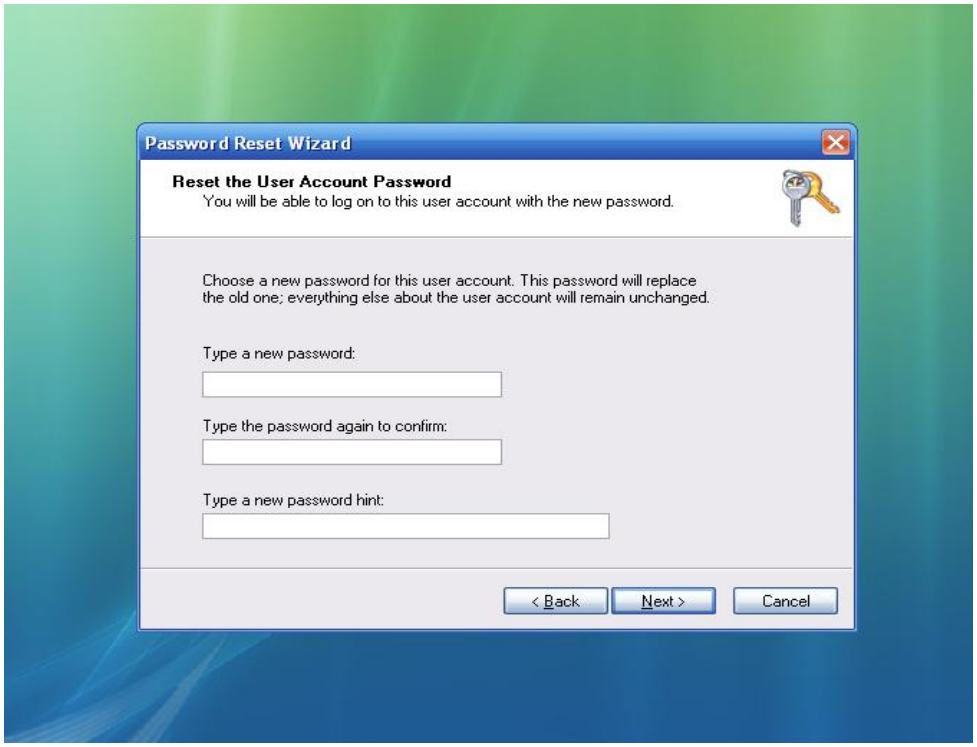
یا به شکل زیر

بعد از انتخاب هم که مراحلی که آنها را در زیر می بینید به ترتیب می آید فقط توجه داشته باشید که این دیسکت فقط بر روی سیستم شما کار می کند و شا نمی توانید آنرا بر روی یک سیستم دیگر اجرا کنید .



در این قسمت پسورد ها را می نویسید فقط قسمت Password Hint نبای خود پسورد را بنویسید .
آن قسمت را یا خالی بزارید و یا اینکه در صورتی که آدم فراموش کاری هستید یک کلمه به عنوان

کمک برای به یاد آوردن پسورد بنویسید که این کار اصا توصیه نمی شود و بهتر است آن را یا خالی بگذارید و یا اینکه یک کلمه ی بی ربط بنویسید که فرد نفوذ گر را سرد گم کند .



پسورد گذاری کامل syskey و حساب های کاربری

اما در صورتی که دسترسی هکر به یک حساب کاربری Limit مانند Guestباشد و یا اینکه بر روی سیستم Syskey نصب باشد آن وقت چیکار هایی انجام می دهند ؟ به هر حال هکر باید بتواند که پسورد ها را یا ریست کند یا حذف کند و یا آنها را بدست بیاورد . روش های مختلفی را هکر ها با استفاده از خلاقیت های خود انجام می دهند در زیر به چند نونه از روش های آن می پردازیم .

حذف SYskey و پسورد حساب Administrator

روش زیر یکی از روش های جالب بوده که بدون استفاده از هیچ ابزاری می توان همه ی پسورد های نام برده را حذف کرد . فقط کافیست یک فلاپی یا یو اس بی فلش و یا هر نوع سیدی bootable را داشته باشیم و یا به نحوی با استفاده از یک سیستم عامل دیگر وارد سیستم شویم .

روش کار

بعد از بالا آمدن با استفاده از سیستم عامل دیگر وارد مسیر %winddir%\repair می شویم در این مسیر تمام فایل های داخل آن را به جای فایل های موجود در %winddir%:\WINDOWS\system32\config کپی می کنیم و سیستم رو ریستارت می کنیم .
با بالا اومدن ویندوز کلیه پسورد ها مانند Syskey و Administrator برداشته شده و هکر به راحتی وارد سیستم می شود . در سیستم عامل 7 این پوشه با نام Regback در همان پوشه Config قرار دارد

روش مقابله

فقط کافیست پوشه ی Repir را حذف کنید این پوشه برای عملیات بازسازی در ویندوز ایجاد شده است که پاک شدن آن هیچ تاثیر منفی در عمل کرد ویندوز ندارد .

حساب کاربری guest را به حد admiistrators ببرید

این کار رو ما با استفاده از ابزاری با نام sysshell انجام می دهیم که باید آن را به جای فایلی با اسم Spoolsv در مسیر System32 کپی کنیم .نام فایل را بهSpoolsv تغییر می دهیم .

در صورتی که فایل درایو سیستم fat یا Fat32 می باشد مراحل زیر را طی نمایید .

اول فلاپی راه انداز سیستم عامل ویندوز رو در داخل درایو قرار دهی د و فایل Spoolsv رو داخل آن کپی نمایید بعد سیستم رو راه اندازی کنید و ابتدا با استفاده از فرمان زیر از فایل spoolsv اصلی یک کپی برداری کنید و ان را در یک محل دیگر قرار دهید .

A:\copy c:windows\system32\spoolsv.exe c:\ spoolsv.exe

حالا فایل spoolsv اصلی در داخل درایو C:\ کپی میشه

سپس با فرمان زیر فایل spoolsv تقلبی را داخل System32 کپی نمایید .

A:\ copy spoolsv.exe c:\windows\system32\spoolsv.exe

حال اگر سیستم را راه اندازی نمایید و با حساب کاربری Guest وارد شوید سطح دسترسی Administrator را دارا می باشد و شما می تونید با فرمان Net user administrator l4tr0d3ctism پسورد حساب کاربری administrator را به L4tr0d3ctism تغییر دهید .

و سپس سیستم رو دوباره با فلاپی راه ادای کنید و فایل Spoolsv اصلی را به جای Spoolsv تقلبی کپی نمایید .

copy c:\spoolsv.exe c:\windows\system32\spoolsv.exe

Del C:\spoolsv.exe

اما در صورتی که سیستم درایو شما به فرم ntfs باشد

از فلاپی بوت سیستم عامل لینوکس برای این کار استفاده می کنیم

برای این کار فلاپی بوت لینوکس را Boot کنید و بعد برای کپی از spoolsv از فرمان زیر استفاده کنید .

$mnt/nt1/spoolsv.exef/ cp /mnt/windows/system32/spoolsv.exe

خوب منظور از nt1 اولین پارتیشن ویندوز هست این فرمان فایل spoolsv که در system32 قرار دارد را به ریشه درایو C:\ کپی خواهد کرد .

و حالا باید با استفاده از فرمان زیر فایل Spoolsv تقلبی رو جایگزین کنیم

$mnt/nt1/windows/system32/spoolsv.exe/ sc /mnt/nt1/spoolsv.exe

و سپس سیستم رو رستارت کنید و بعد وارد حساب کاربری guest بشید

روش مقابله

حساب کاربری Guest را غیر فعال کنید یا حذف نمایید و بر روی Syskey و مادر بورد پسورد بگذارید .

حذف پسورد در Welcom Screen

باید این را بدانید که در صفحه ی Welcom Screen هر نوع فایلی که با پسوند Exe اجرا شود امنیت آن را به خطر مواجهه می کند .کلیه ی محدودیت ها در سیستم عامل های ویندوز بعد از ورود به حساب های کاربری اتفاق می افتد پس کلیه ی فایل هایی که در welcom screen به آن دسترسی داریم در سطح System اجرا می شود یعنی بالاترین سطح دسترسی که مخصوص خود ویندوز می باشد . حال نتیجه گیری این می شود که اگر ما بتوانیم نرم افزاری را به جای آن فایل ها و با اسم آن فایل ها جا بزنیم می توانیم آن نرم افزار را با سطح دسترسی System به اجرا درآوریم .

خوب حال باید بدانیم که چه فایل هایی در محیط Welcom screen قابل اجرا شدن می باشد .

لیست فایل هایی که قابل اجرا هستند به شرح زیر می باشد .

در Seven

Displayswitch.exe – sethc.exe – narrattor.exe – magnify.exe – OSK.exe - utilman.exe

در XP

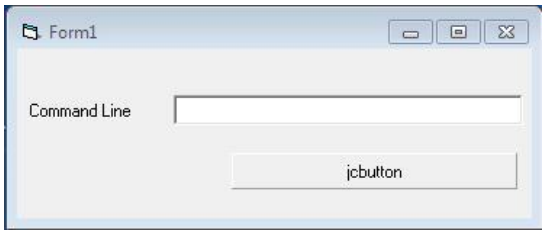
sethc.exe ،msswchx.exe ، osk.exe ، Magnify.exe ، narrator.exe، utilman.exe

حال با موارد بالا چه کار ها و سو استفاده هایی میشه انجام داد .

اینجا دو نمونه از سو استفاده ها رو میگم

1 – ساختن یک فایل exe و جابجا کردن آن با یکی از فایل های Exe

به عنوان مثال بنده در اینجا با استفاده از ویژوال بیسیک یک فایل میسازم یعنی یک فایل متنی و یک دکمه که در داخل دکمه فرمان زیر را نوشته باشیم (”Shell(“text1.text به شکل زیر

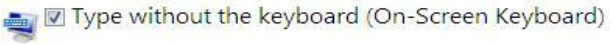


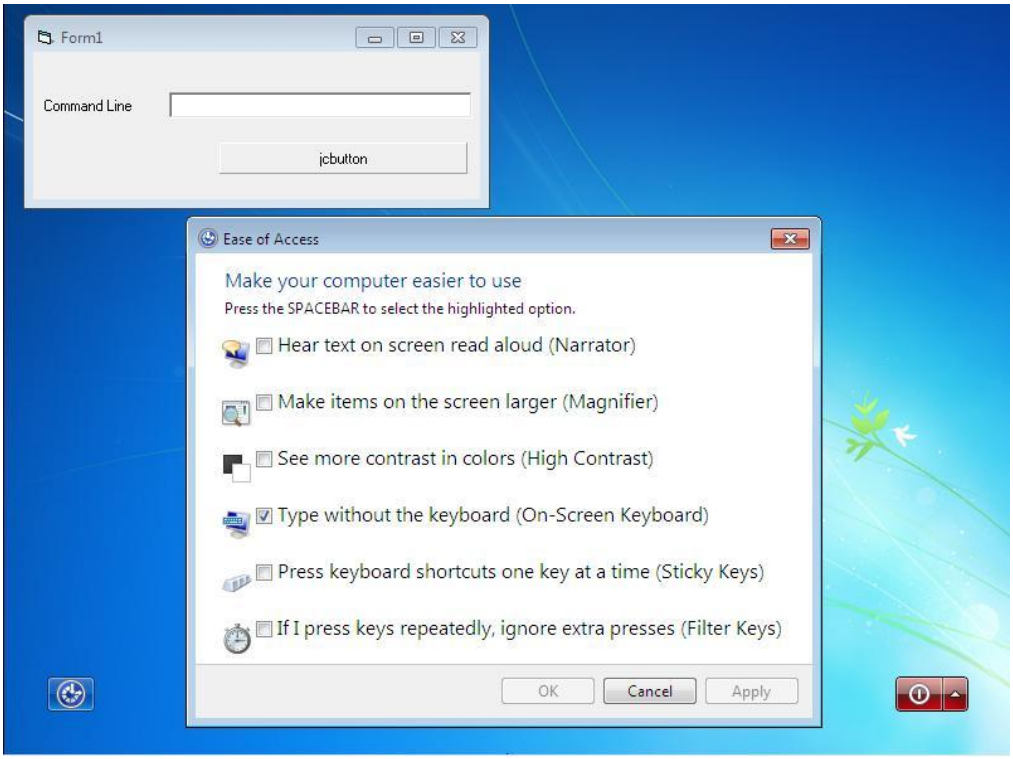
و حالا فایل بالا را با نام OSK.exe ذخیره نمایید و با استفاده از یک سیستم عامل یا یک دیسک bootable سیستم را BOOT کنید و آن را به جای فایلOSK.EXE که در SYSTE32 می باشد کپی کنید البته قبل از آن فایل OSK را در یک قسمت دیگر کپی کنید که از بین نرود . اگر از سیستم تحت داس Boot شده اید با استفاده از فرمان زیر این کار را انجام دهید

Copy C:\windows\system32\OSK.exe C:\osk.exe

Copy Drive:\osk.exe C:\windows\system32\osk.exe

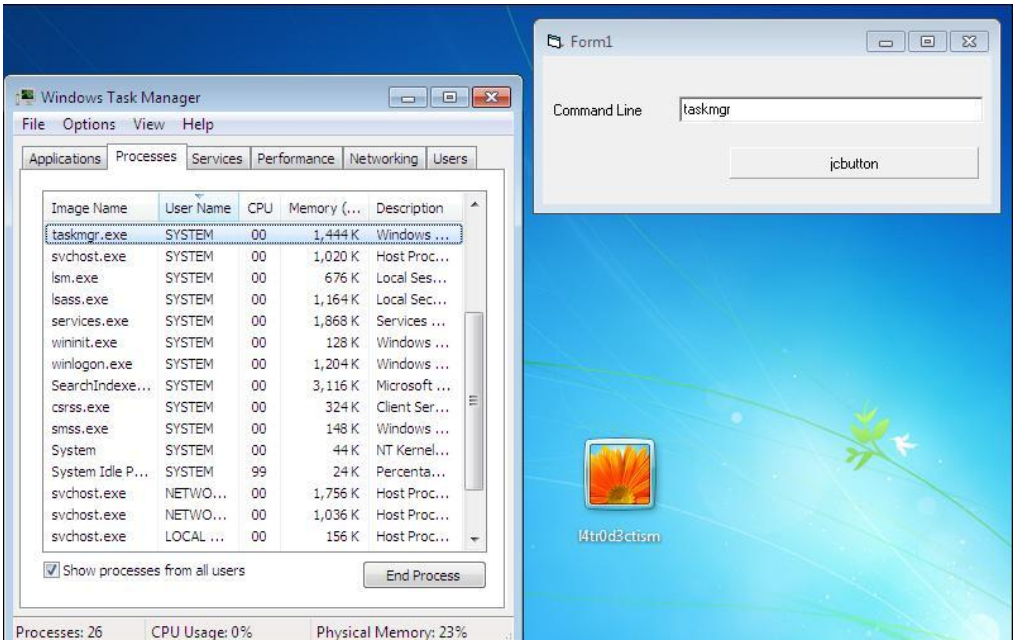
خط اول یک کپی از فایل OSK.exe را در داخل درایو C:\ قرار میدهد و خط دوم فایل ساخته شده را به جای فایل اصلی کپی می کند .

حال سیستم عامل را دوباره راه اندازی کنید و با آمدن به صفحه ی Welcom Screen و زدن دکمه های Win + U گزینه ی  را کلیک نمایید . تا به جای برنامه on Screen keyboard برنامه خودمان اجرا شود .به شکل زیر

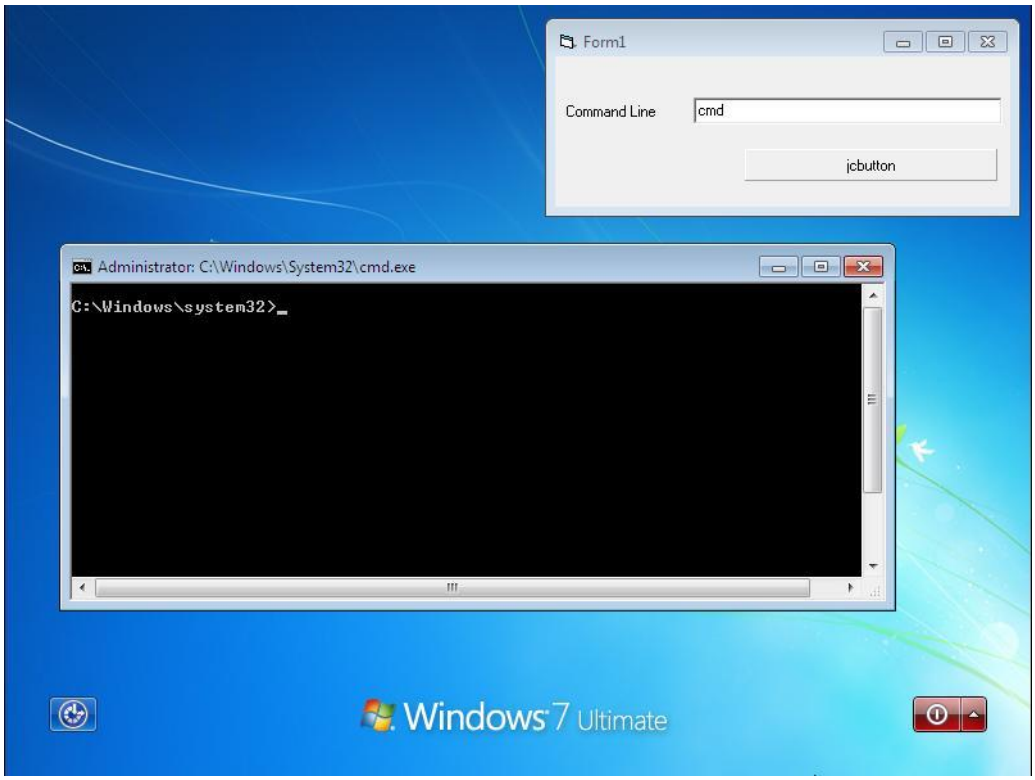


حال می توانیم مانند Run هر فرمان یا قسمتی از ویندوز را که بخواهیم اجرا کنیم مثلا – cmd – regedit -Taskmgr explorer و ... به شکل های زیر توجه کنید .

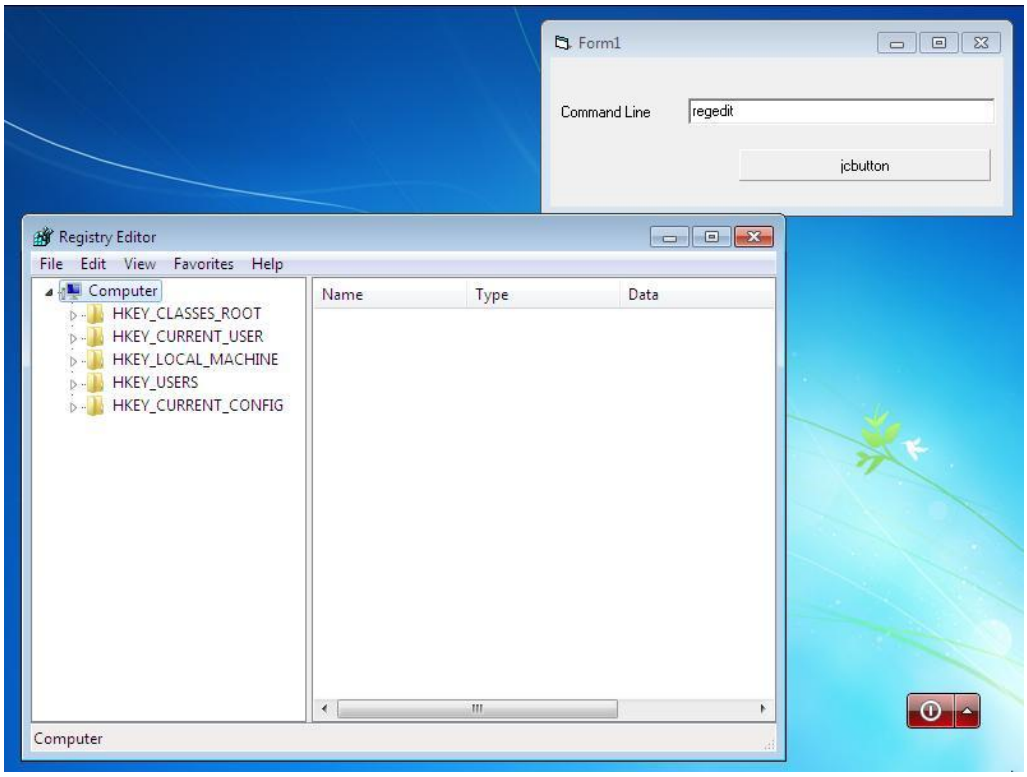
Taskmgr



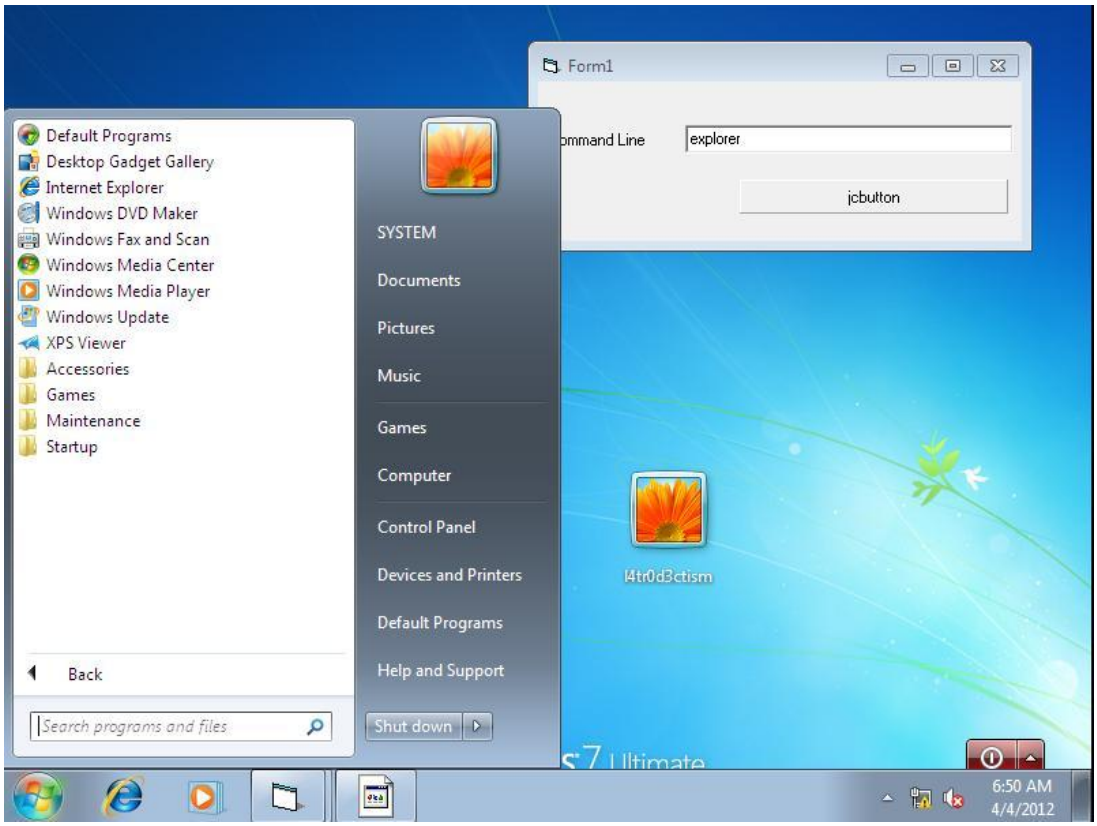
Cmd


Form1
Command Line
cmd
jcbutton
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>_
Windows 7 Ultimate

Regedit


Form1
Command Line
regedit
jcbutton
Registry Editor
File Edit View Favorites Help
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
Name
Type
Data
Computer

و اجرای فرمان explorer که خود مانند ورود به حساب کاربری System در ویندوز Seven می باشد .

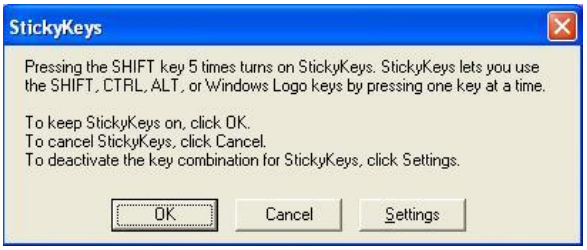


خوب دیدید که چقدر هم مهیج می باشد .

2 – بدون ساخت ابزار با استفاده از برنامه های ویندوز

اما اگر بخواهید بدون استفاده از هیچ برنامه ای این کار را انجام دهید می توانید فایل CMD.exe را جایگزین این فایل ها کنید .برای این کر در اینجا فایل CMD.exe را به جای فایل Sethc.exe جایگزین میکنیم .

Sethc.exe یکی از ابزار های ویندوز می باشد که در صورت فشرده شدن دکمه Shift به تعداد زیاد به شکل زیر فورا ظاهر می شود .



این برنامه در صفحه خوش آمد گویی هم به همین شکل با فشرده شدن 5 یا 6 بار دکمه Shift ظاهر شده اما یک هکر چگونه می تواند از این برنامه سو استفاده کند و از آن برای حذف پسورد استفاده کند .

کافیست با یک فلاپی یا یک سیستم عامل دیگه وارد سیستم شویم سپس فایل Sethc.exe که در مسیر C:\Windows\System32\Sethc.exe می باشد را تییر نام داده و ا به یک محل دیگر کپی شود و یک کپی از فایل CMD.exe که در همان مسیر می باشد با نام Sethc.exe در System32 ایجاد شود .

این کار را می توانید با فرمان زیر انجام دهید .

copy c:\windows\system32\sethc.exe c:\sethc.exe

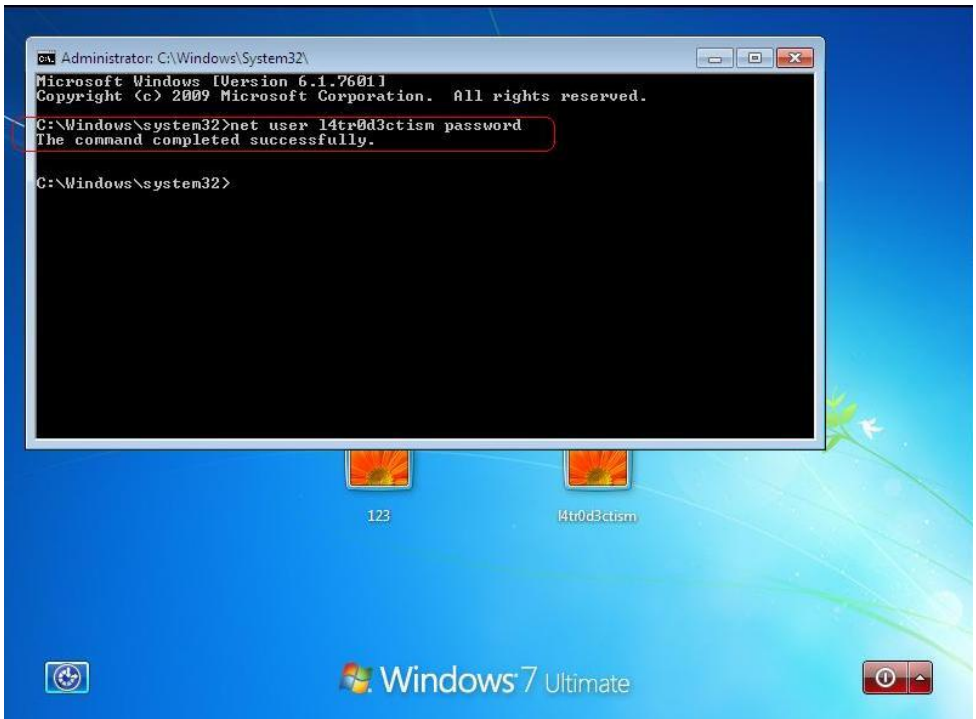
copy c:\windows\system32\cmd.exe c:\windows\syetm32\sethc.exe

یا

Ren c:\windows\system32\sethc.exe c:\windows\syetm32\sethc1.exe

Ren c:\windows\system32\cmd.exe c:\windows\syetm32\sethc.exe

و سپس سیستم را ریستارت کرده و در صفحه ی خوش آمد گویی با فشردن 5 بار دکمه Shift می بینیم که برنامه ی CMD که جایگزین برنامه sethc.exe شده بود باز می شود و می توان با فرمان Net User administrator 123 پسورد حساب کاربری administrator و یا ... را تغییر داد .



وسپس برای بازگرداند فایل به حالت اولیه در Safemod و یا یک سیستم عامل دیگری آن را با فرمان زیر به حالت اولیه بازگرداند

copy c:\windows\syetm32\sethc.exe c:\windows\system32\cmd.exe

copy c:\sethc.exe c:\windows\system32\sethc.exe

یا

Ren c:\windows\syetm32\sethc.exe c:\windows\system32\cmd.exe

Ren c:\windows\syetm32\sethc1.exe c:\windows\system32\sethc.exe

و در نهایت سیستم را دوباره راه اندازی کنید و با پسورد جدید وارد سیستم شوید .

روش مقابله

کافیست بر روی Syskey پسورد بگذارید تا فرد هکر نتواند موارد بالا را به اجرا درآورد .

نحوه ی ریست کردن پسورد با استفاده از ابزار های مختلف موجود در اینترنت

برنامه های بسیار فراوانی برای ریست کردن پسورد حساب های کاربری ساخته شده اند . این ابزار ها با یک سیستم عامل دیگری وارد سیستم می شوند و دسترسی خود را به فایل SAM بدون هیچ محدودیت یا زحمتی می رسانند و سپس لیست حساب های کاربری را که در آن بوده میاورند و از ما می خواهند که یا آن را ریست کنیم یا آن را عوض کنیم برای ریست کردن فقط کافیست برنامه کلمه ی عبور هش شده را پاک کند و این کار باعث ریست شدن پسورد حساب کاربری مربوطه می شود و در صورتی که قادر به ساختن فایل هش MD4 هم باشد می توانند که پسورد را عوض کنند یعنی پسورد وارد شده تسط کاربر به صورت هش شده و الگوریتم مخصوص (MD4) درآمده و جایگزین هش داخل فایل SAM می شود . معمولا این ابزار ها باید از سیستم فایل لینوکس و یا ابزاری که با سیستم فایل NTFS سازگاری

داشته باشد مانند ابزار NTFS4Dos دلیل آن هم این است که در حال حاضر کم سیستمی پیدا می شود که از سیستم فایل Fat32 استفاده کند .

طرز کار برنامه ها هم تقریبا مثل هم بوده

1 - سیستم را با سیدی ، USB Flash و یا فلاپی که نرم افزار مربوطه داخل آن بوده بوت می کنیم (به شرطی که بوتابل باشد)
2 - برنامه را Run میکنیم و سپس برنامه از ما آدرس درایو ویندوز و یا مستقیما فایل SAM را می خواهد
3 - سپس برنامه فایل Sam را باز می کند و لیست حساب های کاربری را برایمان می آورد
4 - از ما می پرسد که پسورد کدام از حساب ها کاربری را ریست می کنید و ...

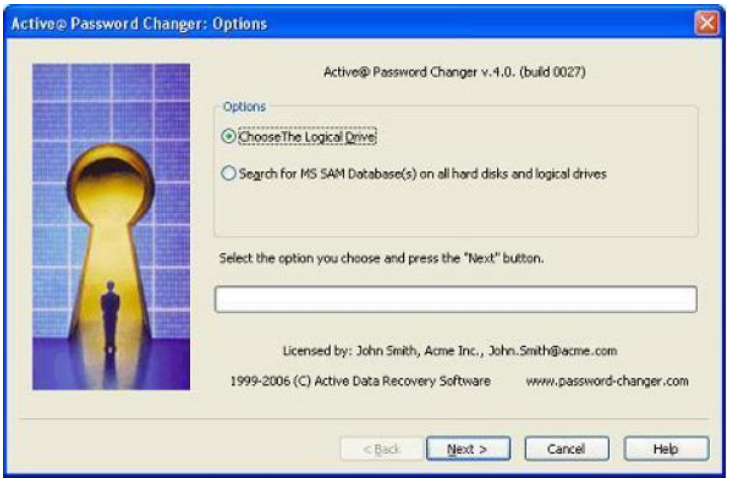
خوب با توجه به مراحل بالا ما در اینجا به ذکر و آموزش وی ترین ابزار ها برای ریست کردن پسورد ویندوز می پردازیم .

ابزار Active@ Password Changer

این برنامه از ساده ترین ابزار ها برای این کار محسوب می شود به دلیل محیط گرافیکی و مراحل ساده ای که در خود دارد که از سیستم فایل های FAT16 / FAT32 / NTFS / NTFS5 و سیستم عامل های NT / 2000 / XP / 2003 / 2008 / VISTA و ویندوز های 64 بیتی پشتیبانی می کند .

طرز کار برنامه

فایل PasswordChanger.exe را اجرا کنیدتا پنجره زیر نمایان شود

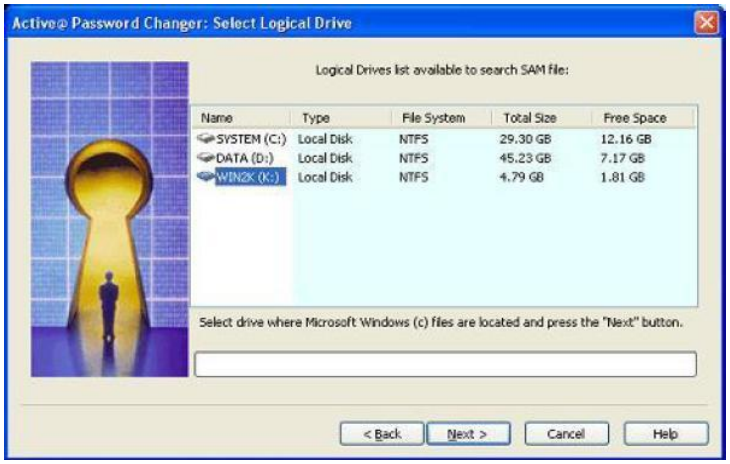


در این قسمت از ما آدرس درایو ویندوز جهت پیدا کردن پایگاه داده SAM را از ما می خواهد .

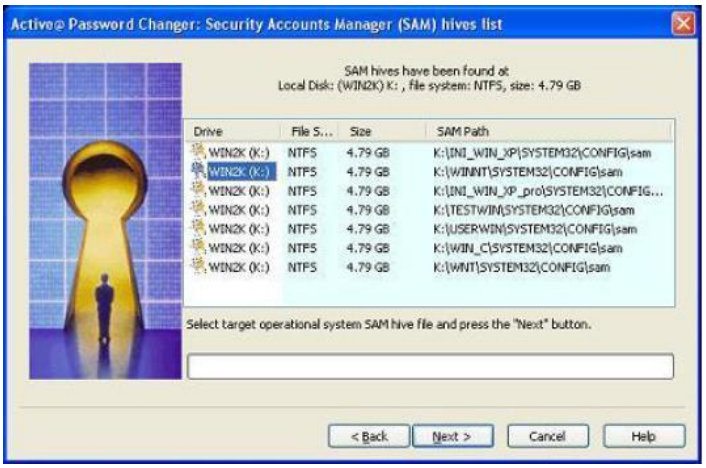
Chose The Logical Drive : اگر درایوی که ویندوز در آن نصب می باشد را می دانیم این گزینه را انتخاب می کنیم .

Search For MS SAM database(S) On All Hard Disks And logical drive : در صورتی که نام درایوی که ویندوز بر روی آن نصب می باشد را نمی دانیم این گزینه ار انتخاب می کنیم تا خود به جستجوی فایل SAM در تمامی درایو ها نماید .

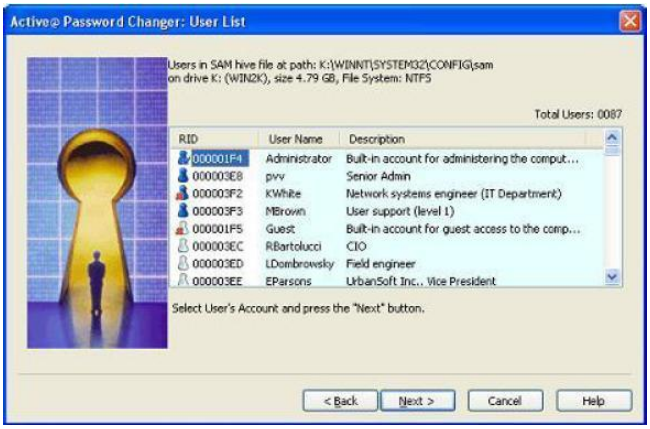
گزینه ی اول را انتخاب می کنیم و به مرحله ی بعد می رویم .



در این مرحله درایوی که ویندوز بر روی آن نصب بوده را انتخاب می نماییم . و بر روی Nextکلیک می نماییم .



در این قسمت برنامه تمامی فایل هایی که با اسمSAM می باشند را برای ما جستجو ی کن و آن را یست می کند و از ما می خواهد نام فایل Samکه مد نظر ماست را انتخاب کنیم .که به صورت پیش فرض در ویندوز XP و Vista در پوشه WINDOWS\SYSTEM32\CONFIGقرار دارد . آن را انتخاب می نماییم و بر روی Nextکلیک می کنیم .



در این قسمت باید حساب کاربری مورد نظر که معمولا خود administrator می باشد را برای حذف کردن پسورد آن انتخاب کنیم .

در نهایت در این قسمت با تیک دار کردن گزینه Clear This User's Password می توان پسورد را حذف کرد

نحوه ی عوض کردن و یا حذف کردن پسورد های ویندوز با استفاده از Ubuntu Live CD

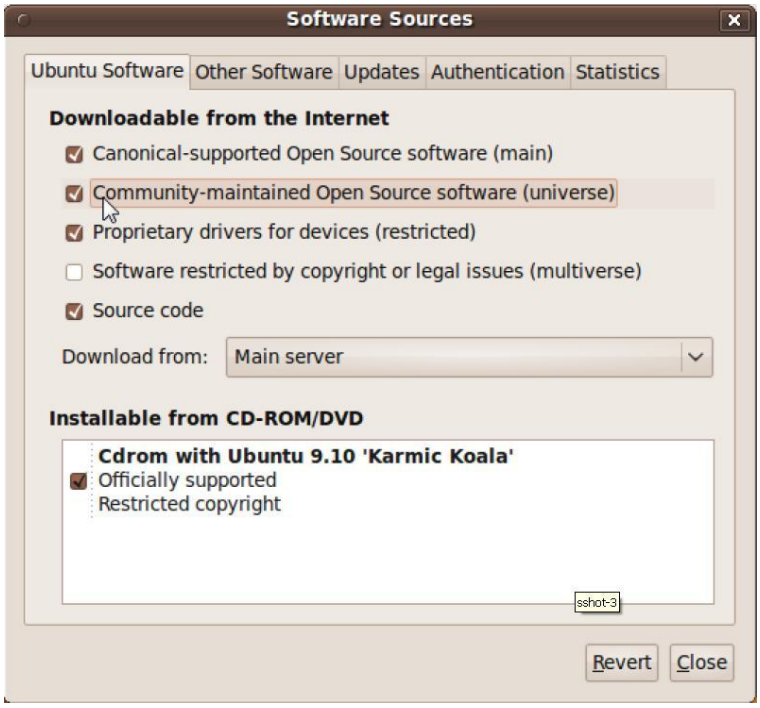
یکی دیگر از روش ها استفاده از سیدی بوتایبل سیستم عامل Ubuntu برای حذف پسورد در ویندوز است فقط کافیت با سیدی live سیستم عامل Ubuntu بالا بیایم این سیستم عامل در Hiren boots 12 به بعد وجود دارد .

با استفاده از این ترفند شما قادر به ریست کردن پسورد سیستم عامل های , Xp (SP1,2,3) , Vista , Seven (Windows server (2003 , 2008خواهید بود .این کار را با استفاده از فراخوانی ابزار chntpw صورت می کیرد .

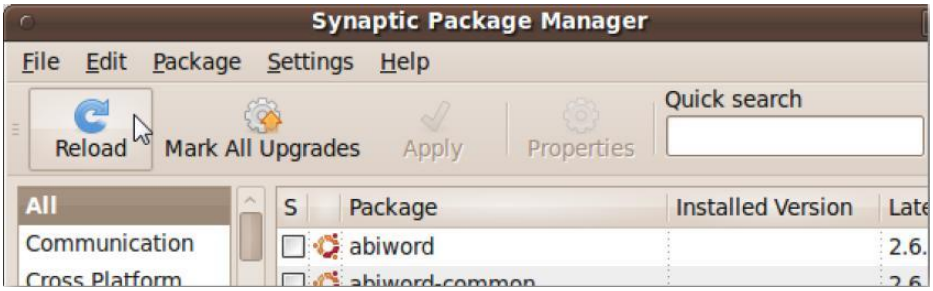
بر روی Tab بالای Os گزینه ی STSTEM را کلیک کنید و در منوی باز شو گزینه ی Synaptic Package Manager را انتخاب نمایید .

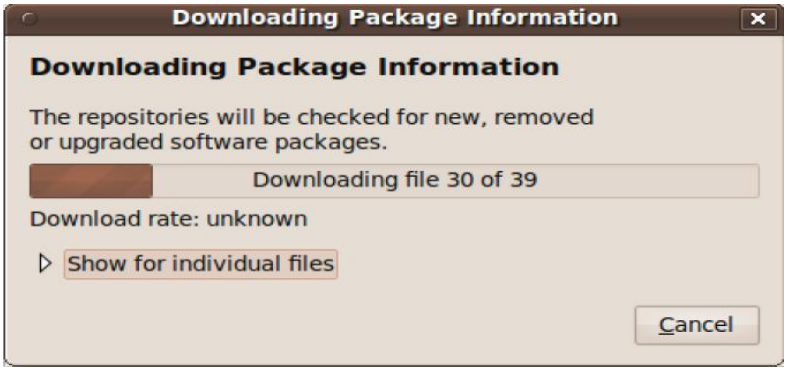
در این مرحله ما باید نرم افزار chntpw را فعال کنیم در صورتی این نرم افزار را نداشتید می توانید آن را دانود نمایید که این کار را با استفاده از universe repository,انجام می دهیم . برای این کار در پنجره Synaptic Package Manage از منوی Settings گزینه یRepositories را انتخاب می نماییم .

در پنجره ی باز شده بر روی گزینه ی "Community-maintained Open Source software (universe)" کلیک می نماییم تا ✓ دار شود .

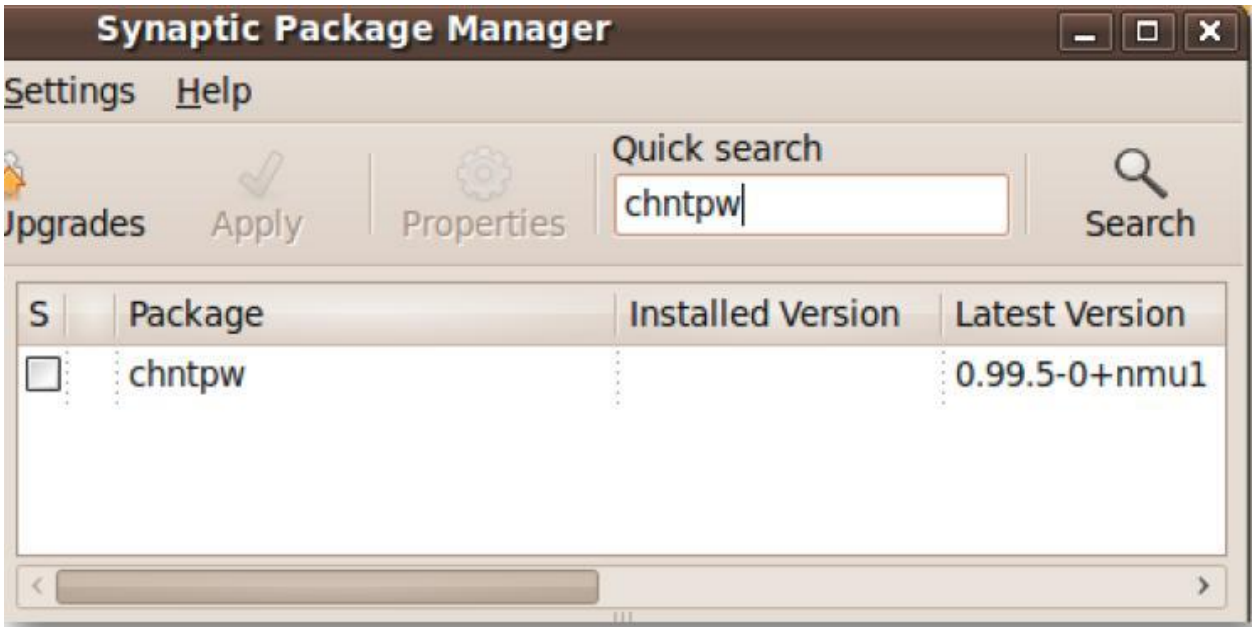


وسپس برای بروز رسانی تنظیمات بر روی گزینه ی ReLoad کلیک می نماییم تا سیستم عامل شروع به دانلود لیسیتی از برنامه های Open source مخصوص به خود کند .

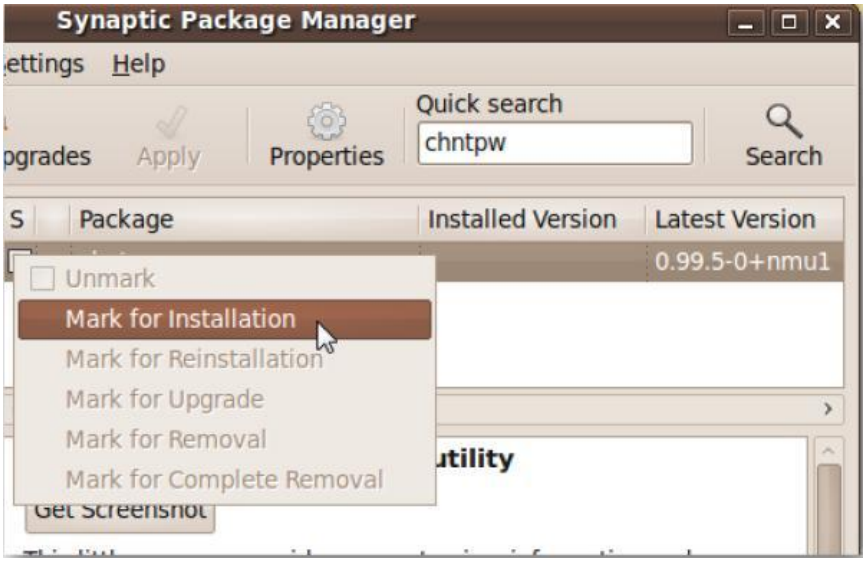




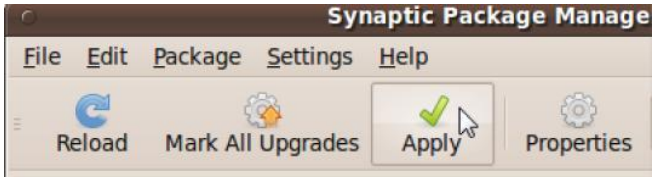
سپس در این مرحله بعد از دانلود برنامه ها در قسمت Qick Search گزینه ی chntpw را سرچ می نماییم .



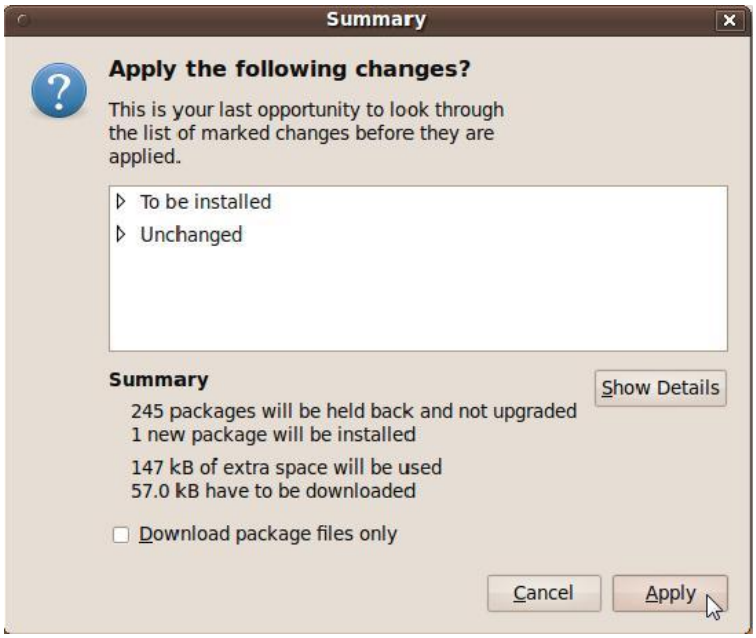
و برنامه را برای نصب آن مارک دار می نماییم .و گزینه Mark For Installation را کلیک می کنیم .



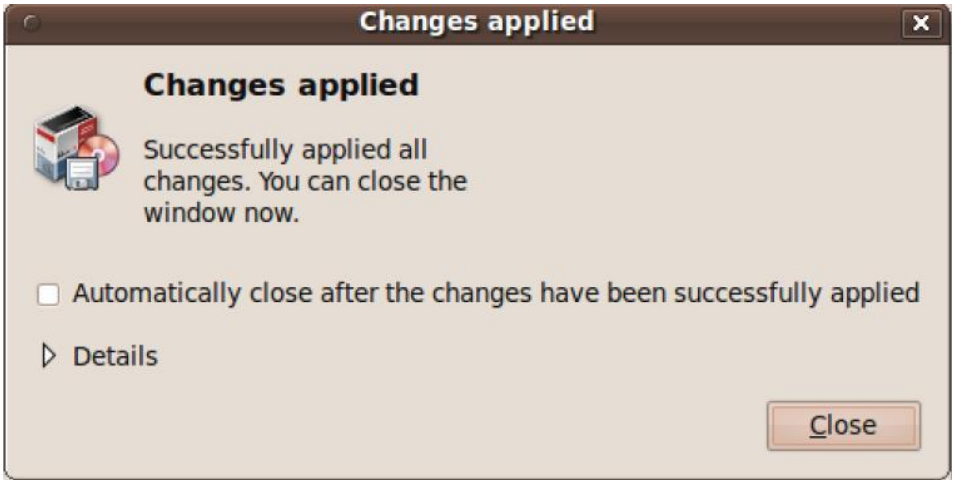
و دکمه ی Applay فعال می شود و بر روی آن کلیک می نماییم .



در این مرحله جهت نصب برنامه باید بر روی APPLY کلیک نماییم .

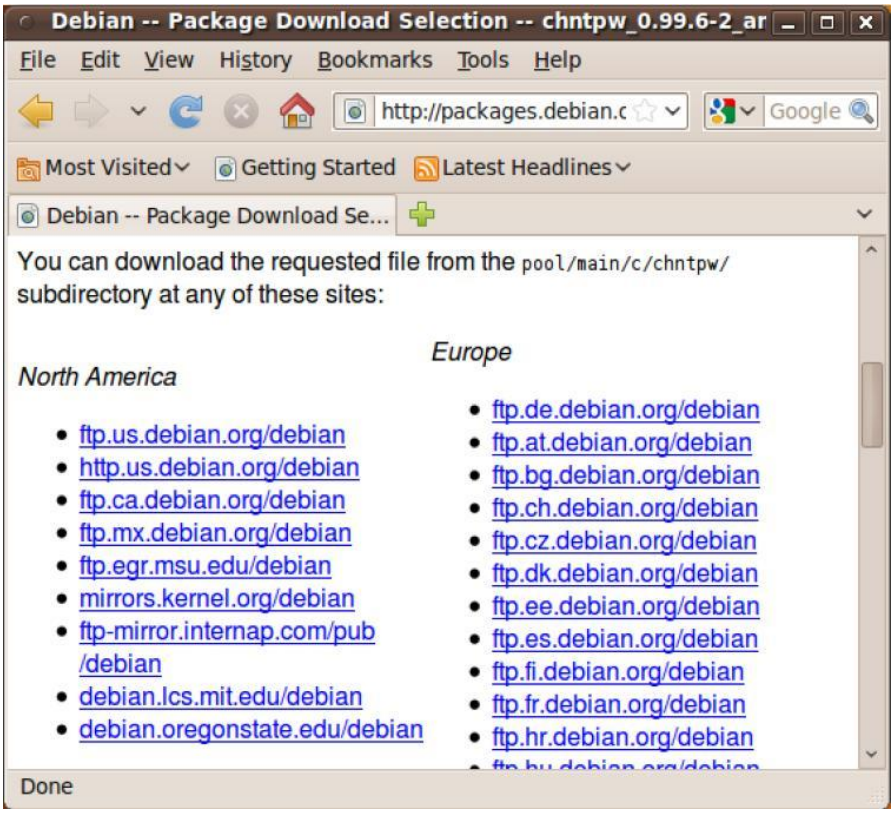


در نهایت برنامه نصب می شود .



در صورتی که از سیستم عامل های 64 بیتی استفاده می کنید باید نسخه ی 64 BIT برنامه chntpw را بر روی Ubuntu نصب نمایید . که برای دانلود آخرین نسخه از برنامه DEB به سایت زیر مراجعه کنید .

http://packages.debian.org/sid/amd64/chntpw/download



سپس برنامه را در مسیر پیش فرض خود ذخیره نمایید .

سپس با استفاده از برنامه Terminal واقع در نوار APPlication > Accessories برنامه را با فرمان زیر نصب می کنیم .

cd Downloads

sudo dpkg –i chntpw*

به شکل زیر

و برنامه به صورت کامل نصب می شود .

حذف یا تغییر پسورد های ویندوز با استفاده از برنامه Chntpw در Ubuntu

حال در این مرحله باید پسورد را ریست کنیم که برای این کار باید از طریق برنامه chntpw وارد قایل SAM شویم و از طریق فرامین برنامه به تغییر یا حذف پسورد بپردازیم .مراحل به شکل زیر می باشد .

اول از همه باید برچسب درایوی که ویندوز در داخل آن نصب می باشد را بدت بیاوریم که به شکل زیر عمل می کنیم .

از منوی Places باید Filesystem خود را انتخاب کنیم .

و وارد آن شویم .

برچسب آن که در قسمتTitle bar پنجره می باشد را می نویسیم .

پنجره Terminal را در مسیر .Applications > Accessories > Terminal باز می کنیم

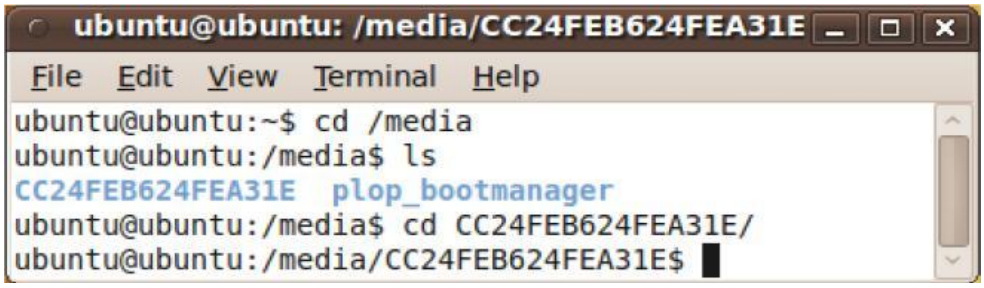
سپس برای تغیر ایرکتوری و فهرست آن از فرمان زیر استفاده می کنیم

cd /media

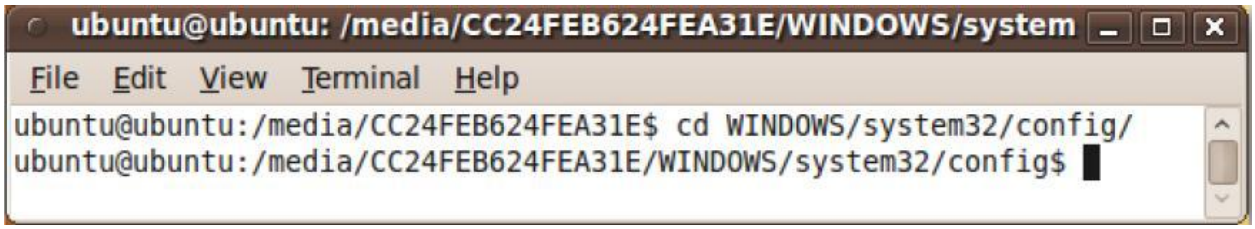
Ls

با وارد کردن فرمان بالا یک یا چند متن ظاهر می شود که باید برچسب موجود در متن با برچسب درایو ویندوز در مرورگر فایل یکی باشد .در صورتی که برچسب ها با هم مغایرت داشته باشد می توانید جهت تغییر آن و رفتم به درایو مربوطه از فرمان زیر استفاده نایید

CD < برچسب درایو>



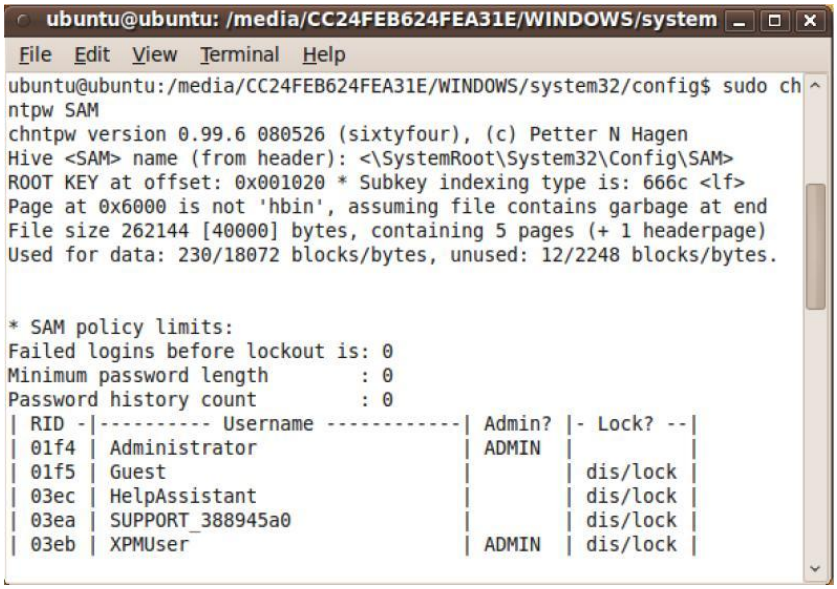
با استفاده از فرمان cd WINDOWS/system32/config/ وارد پوشه Config می شویم .



جهت خواندن محتویات فایل SAM و اتصال به فایل از طریق برنامه دستور زیر را می نویسیم

sudo chntpw SAM

بعد ار ورود به فایل نام حساب های کاربری هم برای ما ظاهر مش و در زیر تر برای ما 4 گزینه در رابطه با تغییر و حذف حساب کاربری را می آورد



گزینه ها موارد زیر می باشند

1 –Clear (Blank) user password : انتخاب این گزینه باعث حذفپورد حساب کاربری می شود .

2 – Edit (Set new) userpassword : برای ایجاد یک حساب کاربری

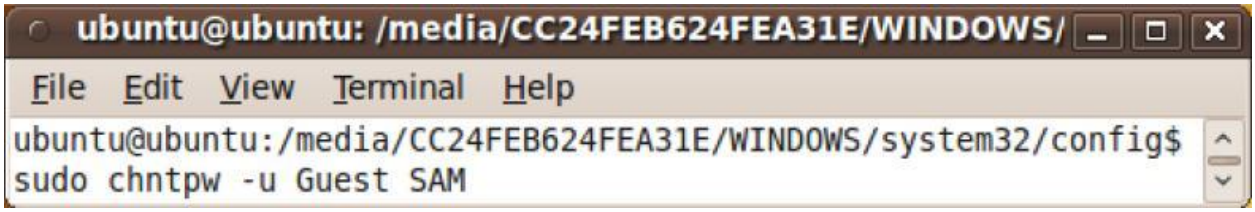
3 - Promote User (Make user an administrator) : برای تغییر نوع حساب کاربری

4 –Unlock and enable user accounts: برای فعال یا غیر فعال کردن حساب کاربری

گزینه ی 1 را انتخاب میکنیم و Y را می نویسیم تا پسورد ریست شود .

شما می توانید با استفاده از فرمان زیر هم مراحل را برای دیگر کاربران انجام دهید .

sudo chntpw –u <username> SAM



و مراحل بالا را برای حذف و یا تغییر پسورد دوباره انجام دهید .

در نهایت با انجام تمامی مراحل فوق می توانید به راحتی وارد ویندوز شوید

روش مقابله

فقط کافیست بر روی Syskey پسورد بگذارید .

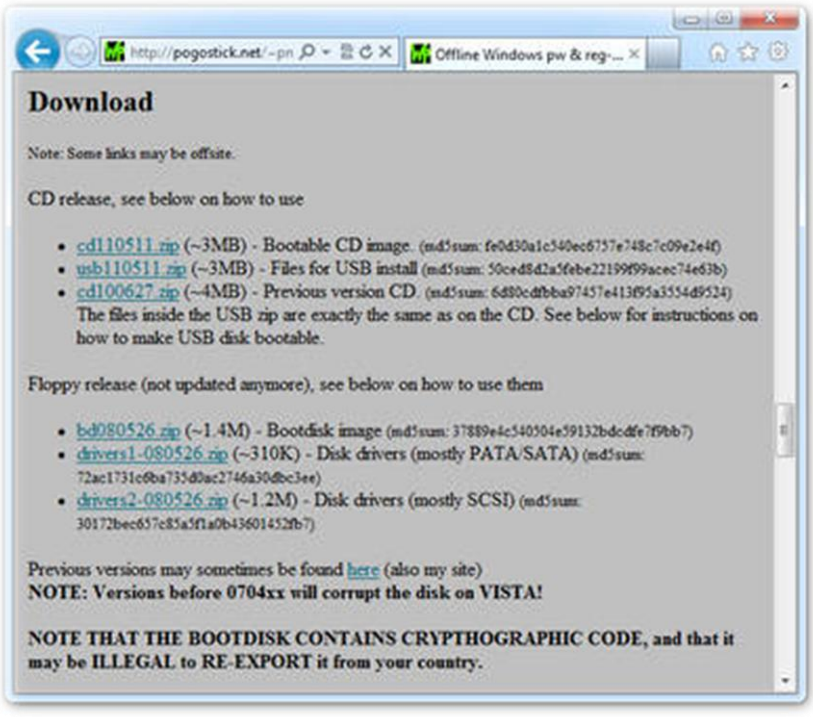
با استفاده از ابزار NTPswd

ابزار ntpswd یکی از قدرتمند ترین و معروفترین ابزار در بین ابزار های حذف کننده پسورد ویندوز می باشد

این ابزار به دلیل استفاده از کرنل سیستم عامل لینوکس برای بوت کردن خود قابلییت سازگاری با سیستم فایل های NTFS و Fat32 را دارد و قادر به حذف پسورد سیستم عامل های windows 2000 , Xp (sp2-sp3),vista , Seven می باشد .

در اینجا نحوه ی حذف پسورد را با استفاده از این ابزار یاد می گیرید .

در مرحله ی اول باید نرم افزار را در وب سایت اصلی خود به صورت رایگان دانلود نمایید .

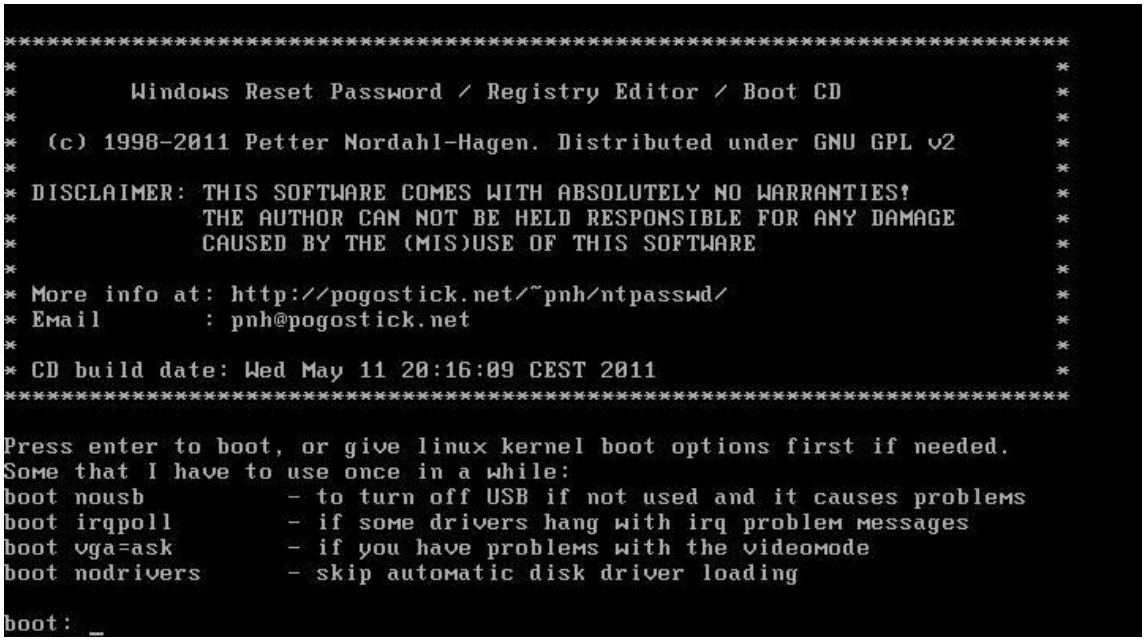


http://pogostick.net/~pnh/ntpasswd/bootdisk.html

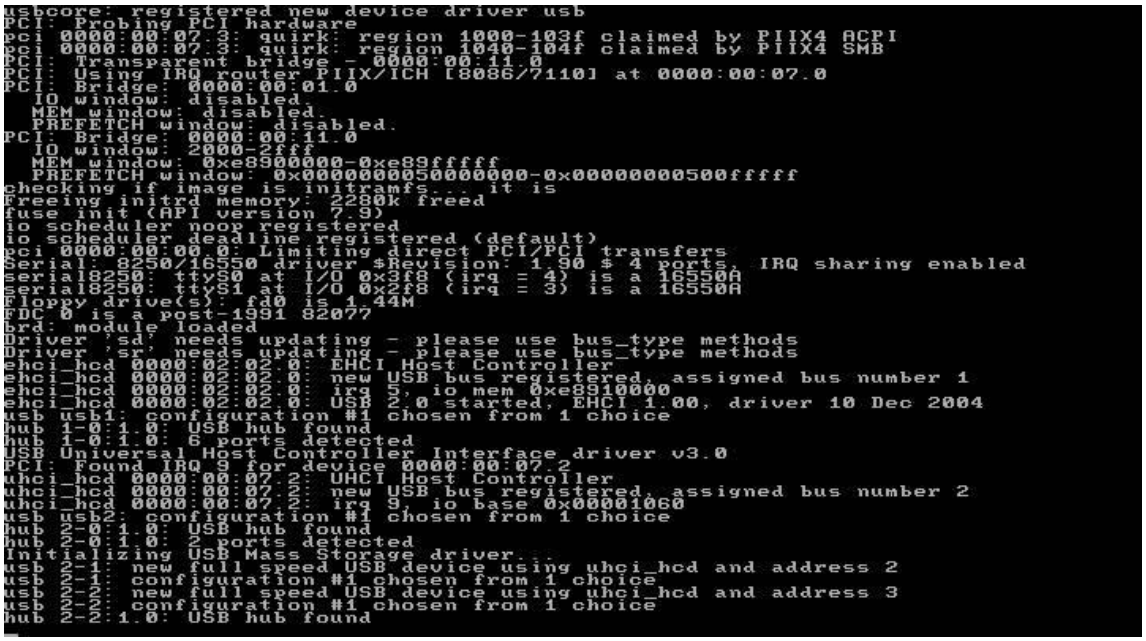
بعد از دانلود نسخه ی مورد نظر خود آن را روی سیدی یا فلاش رایت می نماییم و سیستم عامل را با آن بوت می کنیم .فایل به صورت ISO می باشد .

بعد از بوت کردن سیستم باید متن زیر را نمایش دهد

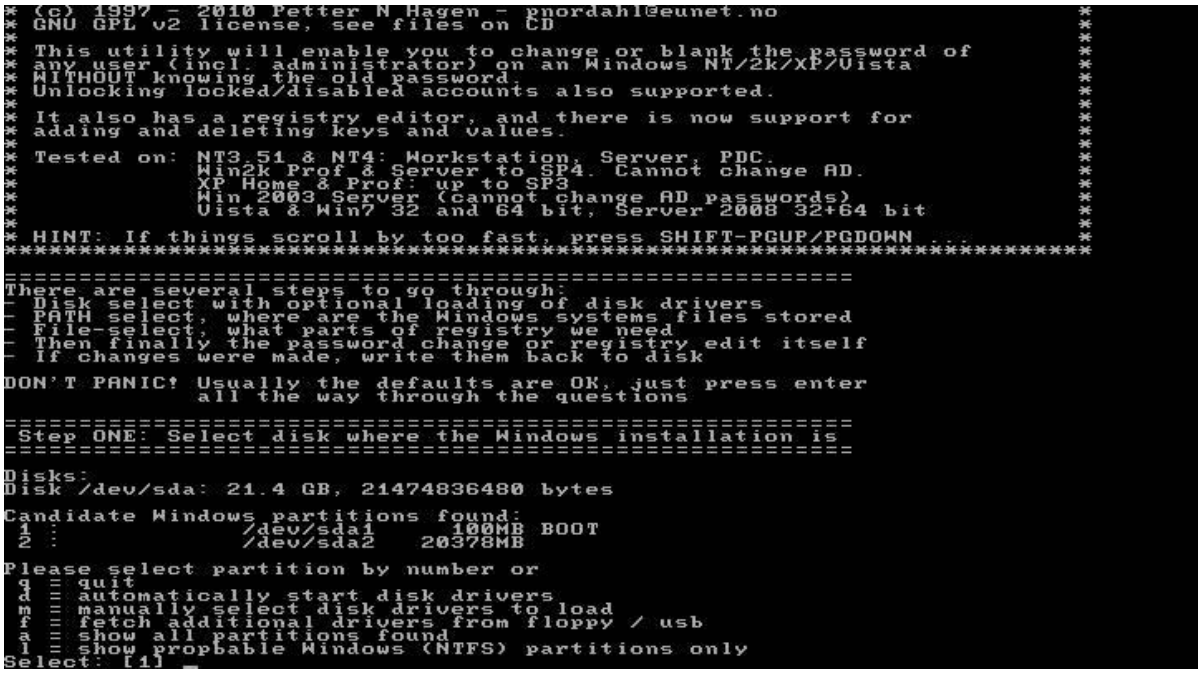
Press ENTER at the boot: prompt, shown above



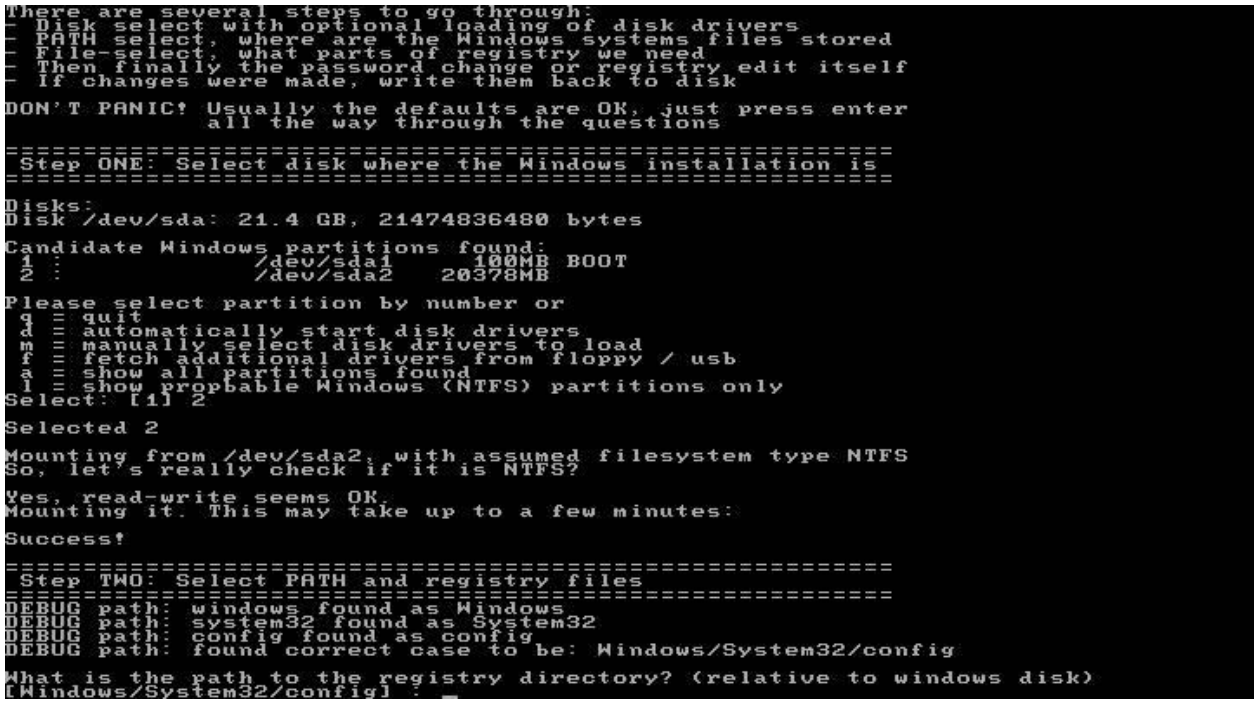
در مرحله بعد برنامه شروع به Load کردن فایل های مورد نیاز خود در رابطه با وظیفه خود می کند



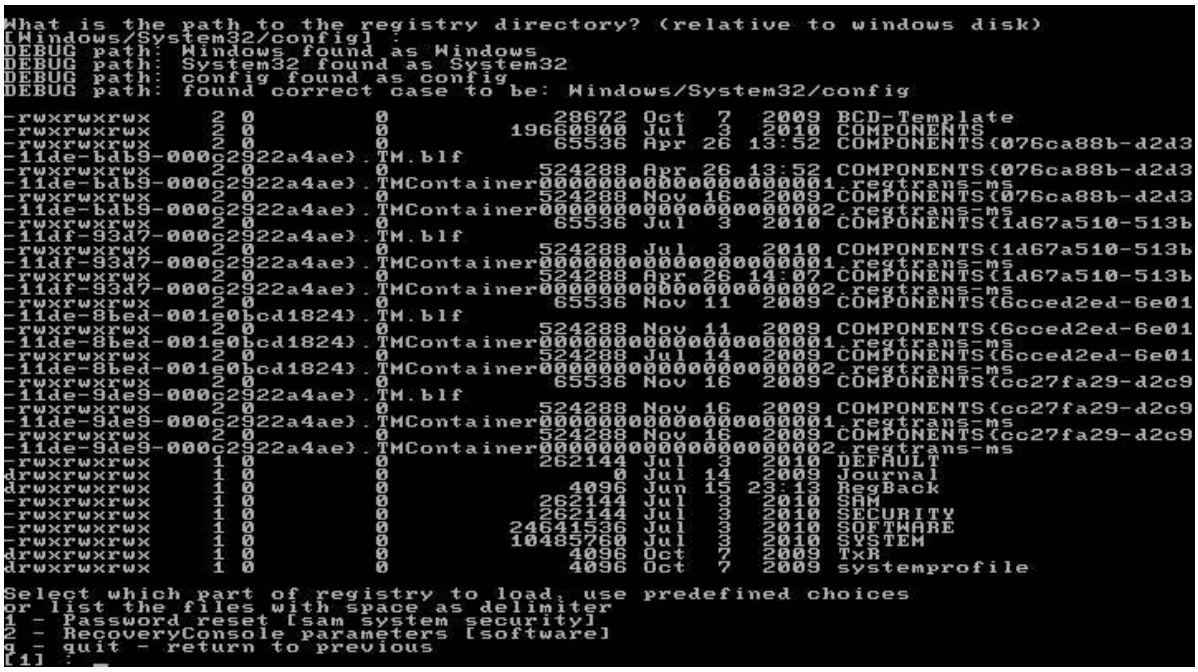
در مرحله بعد جهت حذف پسورد باید پارتیشن سیستم عامل را انتخاب کنیم که با گذاشتن شماره گزینه ی ورد نظر و Enter این کار انجام می شود .



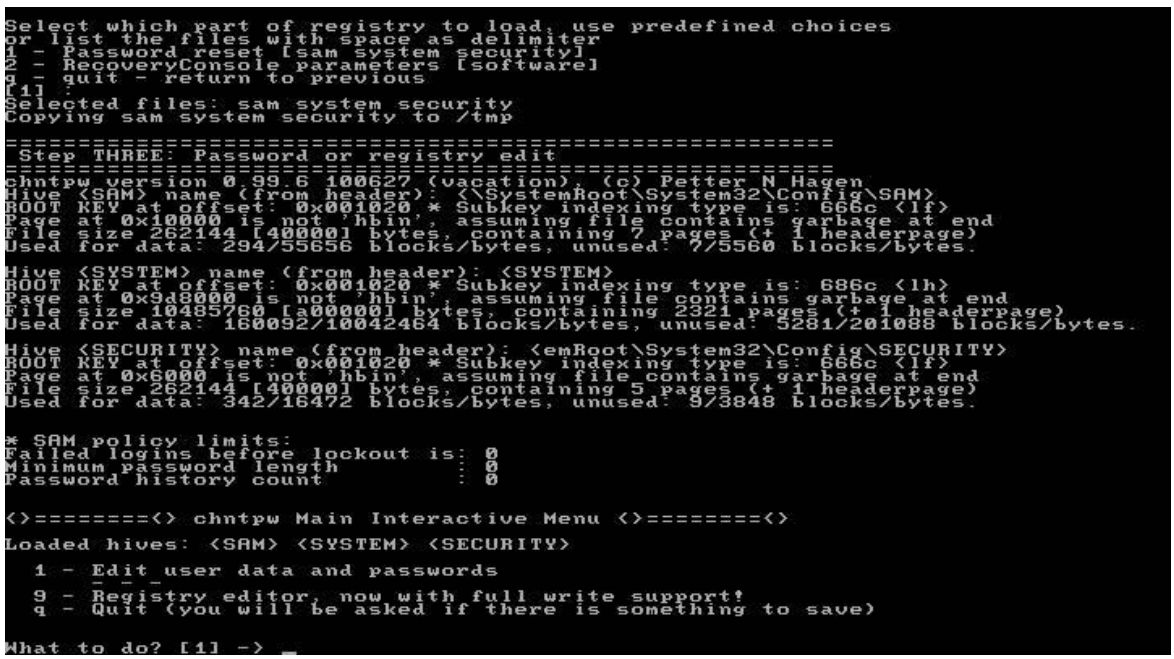
در این مرحله برنامه از ما محل فایل های Hive که به صورت پیش فرض همان فایل های مووجد در پوشه Config می باشد به منظور دستیابی به فایل SAM را از ما می خواهد . این فایل که به صورت پیش فزض در Windows\System32\Config وجود دارد در نتیجه با زدن Enter برنامه به آن مسیر راهنمایی می شود



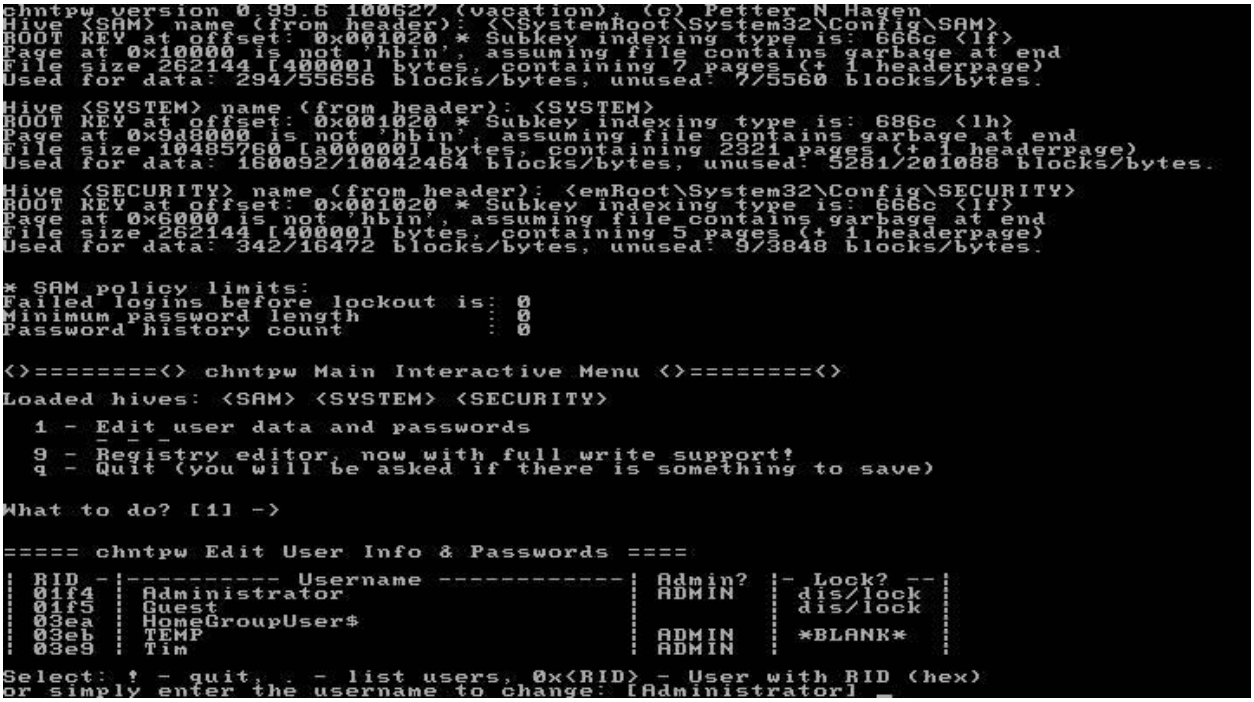
برنامه در اینجا فایل Sam را پیدا کرده و از ا می خواهد که جهت حذف پسورد و ورود به فایل Sam 1 را انتخاب کنیم و Enter را بزنیم .



در اینجا 1 را دوباره انتخاب می کنیم تا به ویرایش USER و Password حساب های کاربری بردازیم .



در این مرحله لیست کلیه ی حساب های کاربری و سطح مدیریتی آنها را به شما نشان می دهد .برنامه به صورت پیش فرض حساب Administrator را جهت عملیات انتخاب کرده است که شما می توانید با نوشتن نام حساب کاربری مورد نظر به مرحله ی بعد بروید .



در این قسمت به ما چند امکان کدیریتی داده می ود .

1 – با زدن این گزینه پسورد حذف می شود .

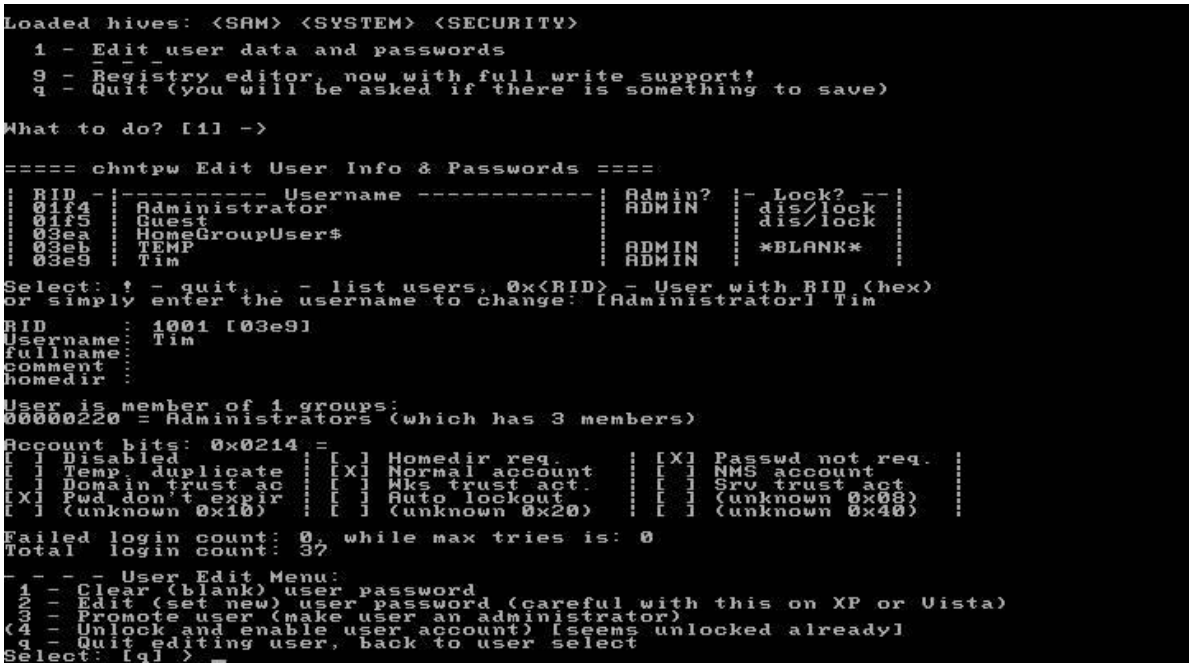
2 – این گزینه می تواند پسوردی جدید برای حساب کاربری انتخاب کند

3 – این گزینه می تواند سطح دسترسی یک حساب کاربری را از Limited به administrator افایش دهد .

5 - این گزینه هم قابلیت فعال یا غیر فال کردن حساب کاربری را به ما می دهد .

6 - با زدن q هم که برنامه به صورت پیش فرض آن را انتخاب نموده از برنامه خارج می شویم.

بعد از انتخاب گزینه مورد نظر به مرحله ی بعد می رویم (ما 1 را انتخاب میکنیم)



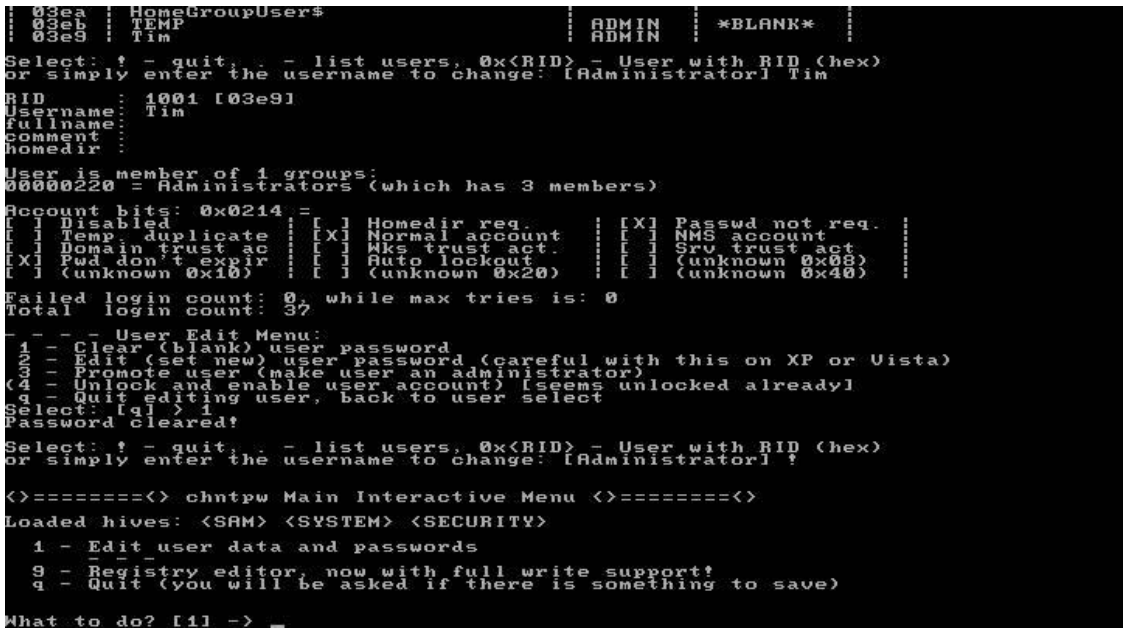
در این مرحله دوباره می توان به مراحل بعد برگشت

- جهت خروج از این مرحله و رفتن به مرحله ی بعد "!" را می زنیم
- جهت دیدن لیست تمامی حساب های کاربری "." را میزنیم
- جهت ویرایش دیگر حساب های کاربری یا اسم آن را مینویسیم و یا کد هگز آنها وارد حساب کاربری مربوطه میشویم RID(Hex)

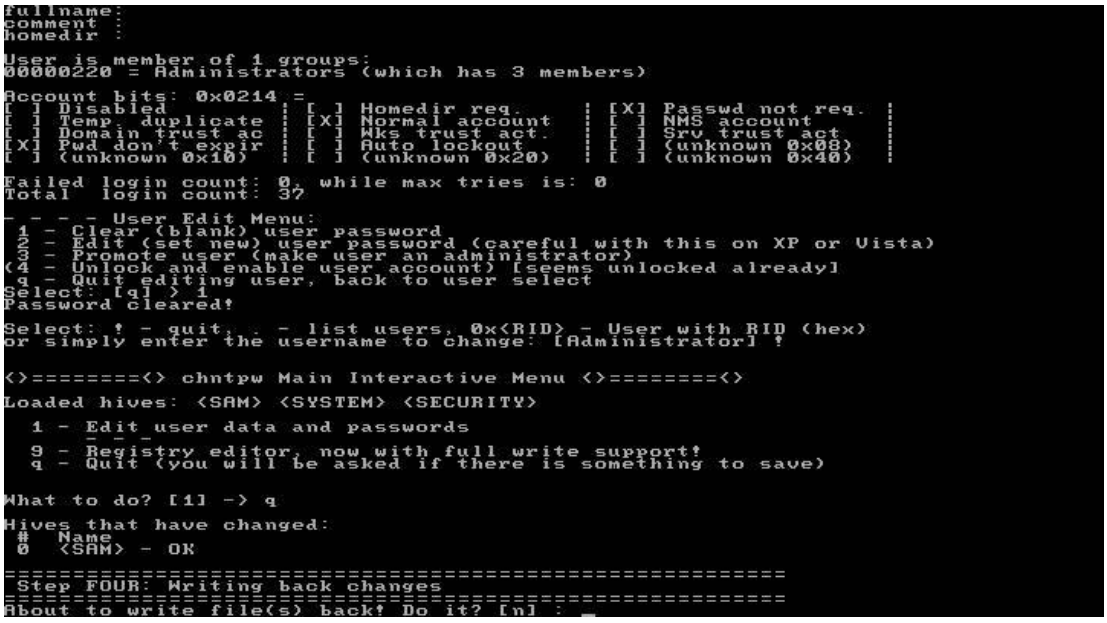
! را جهت رفتن به مرحله ی بعد می زنیم .

با زدن ! از ما سوال می پرسد که آیا قصد انجام کار دیگری بر روی حساب کاربری مورد نظر را دارید یا خیر تغییرات ایجاد شده در فایل Sam را ذخیره کنم

در این قسمت q را زده تا تغییرات ایجاد شده در فایل Sam ذخیره شود .



با زدن کلید qتغییرات ذخیره شده و پسورد حاب کاربری مورد نظر حذف می شود .و در صورتی که می خواهید عملیات جدیدی انجام دهید و به عقب برگردید Y را زده در غیر این صورت N را بزنید



و دوباره از ما پرسیده می شود که در صورتی که به هر نحوی خطایی پیش آمده و یا دچار اشتباه شده اید با زدن Y به عب برگردید و در غیر این صورت n را بزنید

```
Account bits: 0x0214 =
[ ] Disabled        | [ ] Homedir req.      | [X] Passwd not req.   |
[ ] Temp. duplicate | [X] Normal account    | [ ] NMS account       |
[ ] Domain trust ac | [ ] Wks trust act.    | [ ] Srv trust act     |
[X] Pwd don't expir | [ ] Auto lockout      | [ ] (unknown 0x08)    |
[ ] (unknown 0x10)  | [ ] (unknown 0x20)    | [ ] (unknown 0x40)    |

Failed login count: 0, while max tries is: 0
Total  login count: 37

- - - - 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!

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

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

Loaded hives: <SAM> <SYSTEM> <SECURITY>

  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

================================================================
 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] : _
```

و در نهایت برنامه به مکانیزم خود پایان میدهد .

```
Total  login count: 37

- - - - 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!

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

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

Loaded hives: <SAM> <SYSTEM> <SECURITY>

  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

================================================================
 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] :
================================================================

* 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'

# _
```

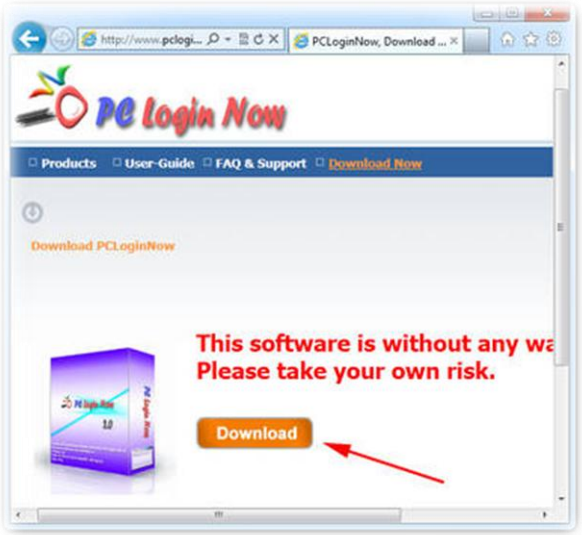
و با راه اندازی دوباره سیستم عامل دیگر پسوردی بر روی حساب کاربری شما وجود ندارد و می توانید راحت وارد ویندوز شوید .

روش مقابله

فقط کافیست بر روی Syskey پسورد بگذارید .

PC Login Now

PC Loginیکی دیگر از برنامه های حذف کننده ی پسورد می باشد که کار با آن بسیار ساده بوده .این برنامه ی تحت داس قادر به حذف پسورد در تمام نسخه های ویندوز مانند NT ، ویندوز Xp ، Vista و Seven می باشد.برای کار با برنامه اول از همه باید آن را بر روی CD رایت کنید و با آن Boot کنید

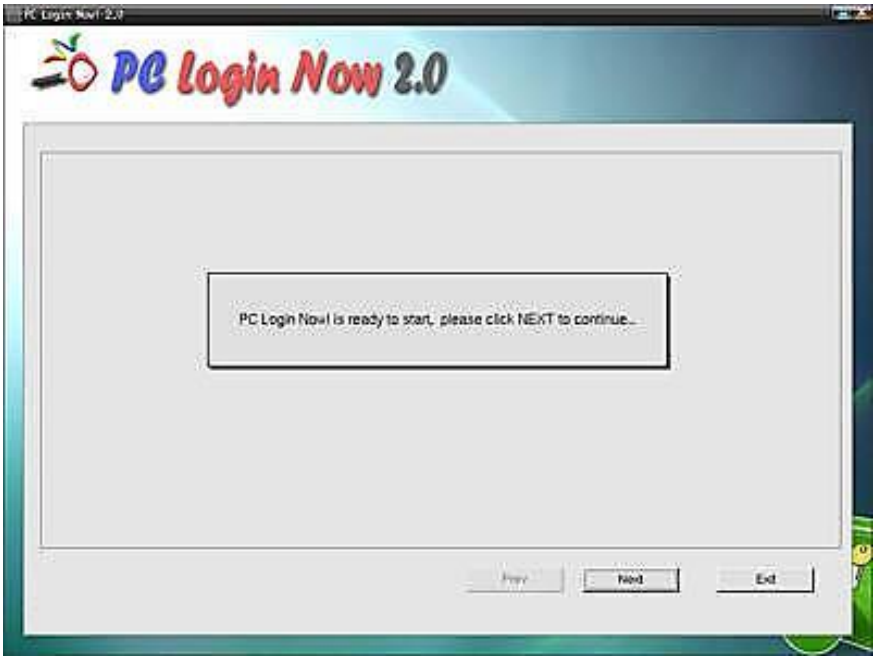


بعد از بوت شدن CD برنامه و بالا آمدن کامل برنامه از ما می خواهد که نوع Boot شدن برنامه را تعیین کنیم که در صورتی که می خواهیم به صورت معمولی بوت شود کلید 1 و در صورتی که می خوهیم که

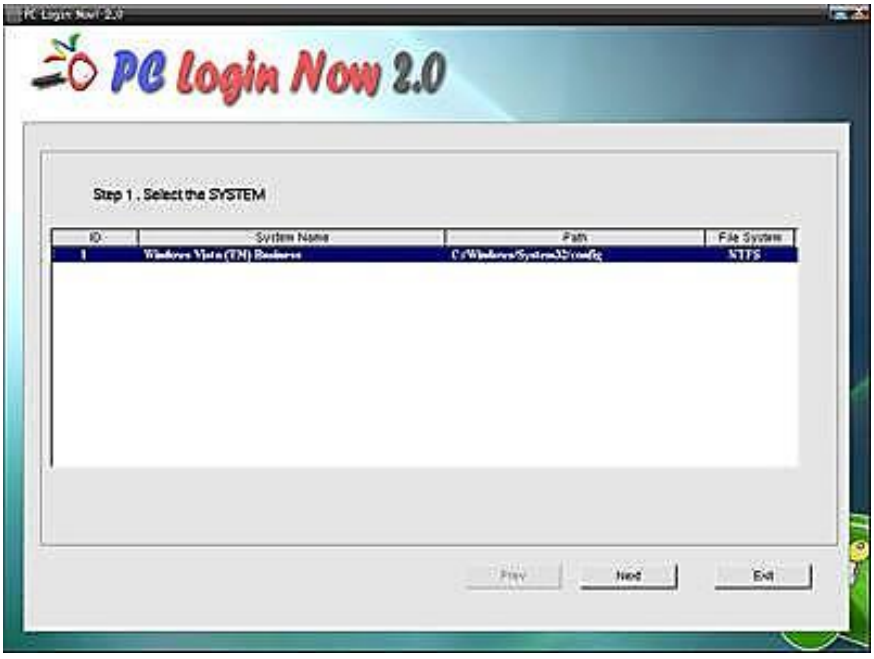
اندازه تصویر را تعیین کنیم گزینه ی 2 را میزنیم .گزینهNormal Boot را انتخاب می کنیم و به مرحله ی بعد می رویم .

برنامه خود شروع به آماده کردن و load کردن خود در حافظه برای حذف پسورد می کند

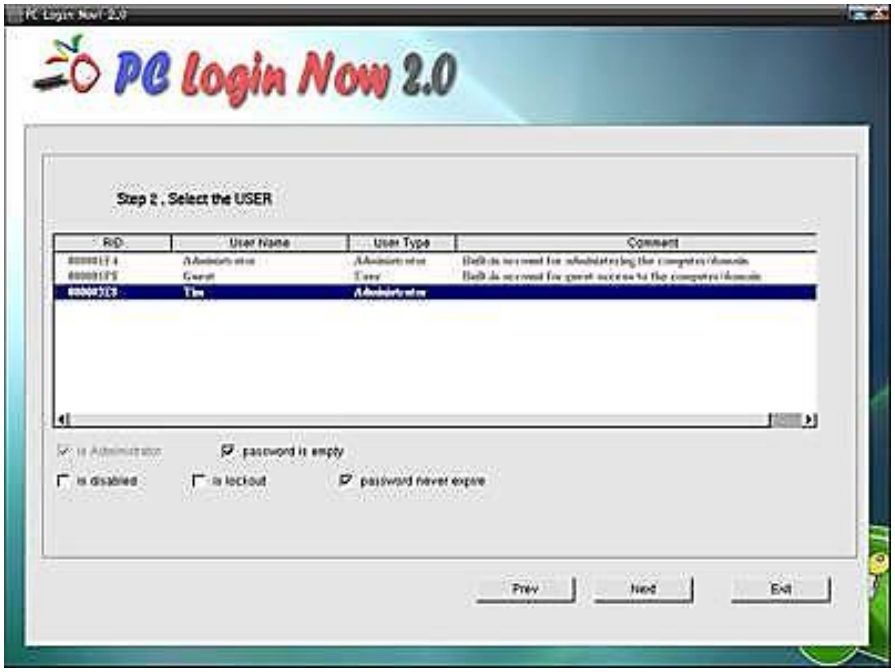
برنامه آماده انجام فرایند حذف پسورد می شود و کاربر را با صفحه ی زیر روبرو می سازد .در این مرحله کاربر باید Next را بزند تا به مرحله بعد برود.



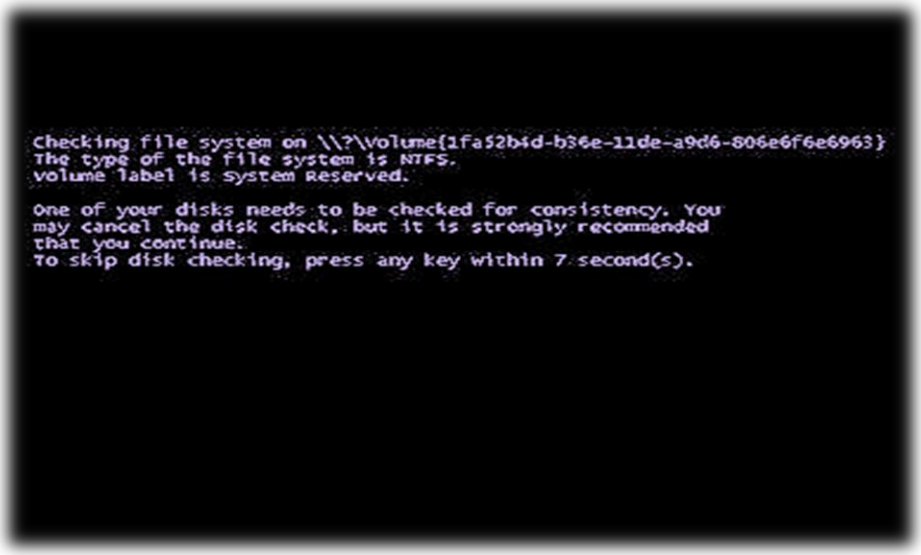
ئ در مرحله ی بعد برنامه خود فایل Sam را شناسایی میکند و وارد آن می شود .



و در مرحله ینهایی لیست حساب های کاربری را برایمان مشخص میکند و از ما می خواهید با تیگ دار کردن موارد و گزینه های خود تغییرات مورد نیاز را بر روی حساب کاربری انتخاب شده انجام دهیم و در نهایت Next را زده .



و برنامه به کار خود پایان می دهد . با راه اندازی دوباره می توانید وارد ویندوز شوید .

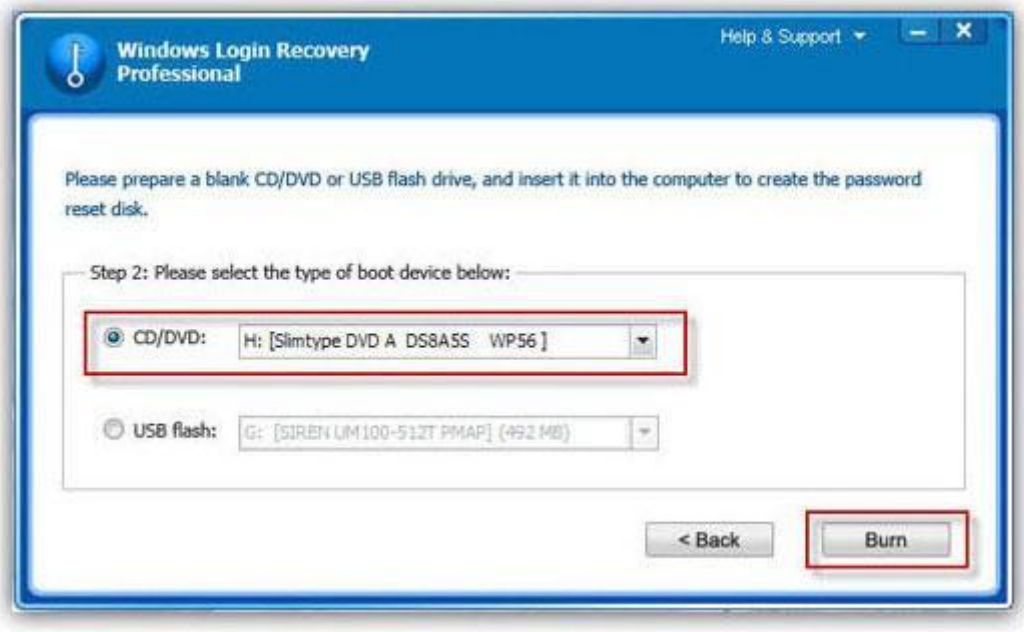


Windows Login Password Professional

برنامهWindows Login Password Professionalساده ترین ابزار برای حذف پسورد در سیستم عامل های مایکروسافت می باشد . که با داشتن محیط گرافیکی و محیط بسیار ساده امکان حذف پسورد را برای کاربران بسیار مبتدی را هم فرآهم می آورد و دارای سرت کاری زیادی می باشد . این برنامه قادر حذف کردن پسورد ویندوز های Windows 7/Vista/XP/2008/2003/2000 و حتی پسورد دامین در ویندوز Server 2008/2003/2000 می باشد .

بعد از دانلود برنامه آن را اجرا کنید تا با پنجره زیر ظاهر گردد و در این پنجره باید مشخص کنید که می خواهید پسورد کدام یک از نسخه های ویندوز را می خواهید حذف کنید .یکی از دسته ها را انتخاب کنید و Next را کلیک کنید .

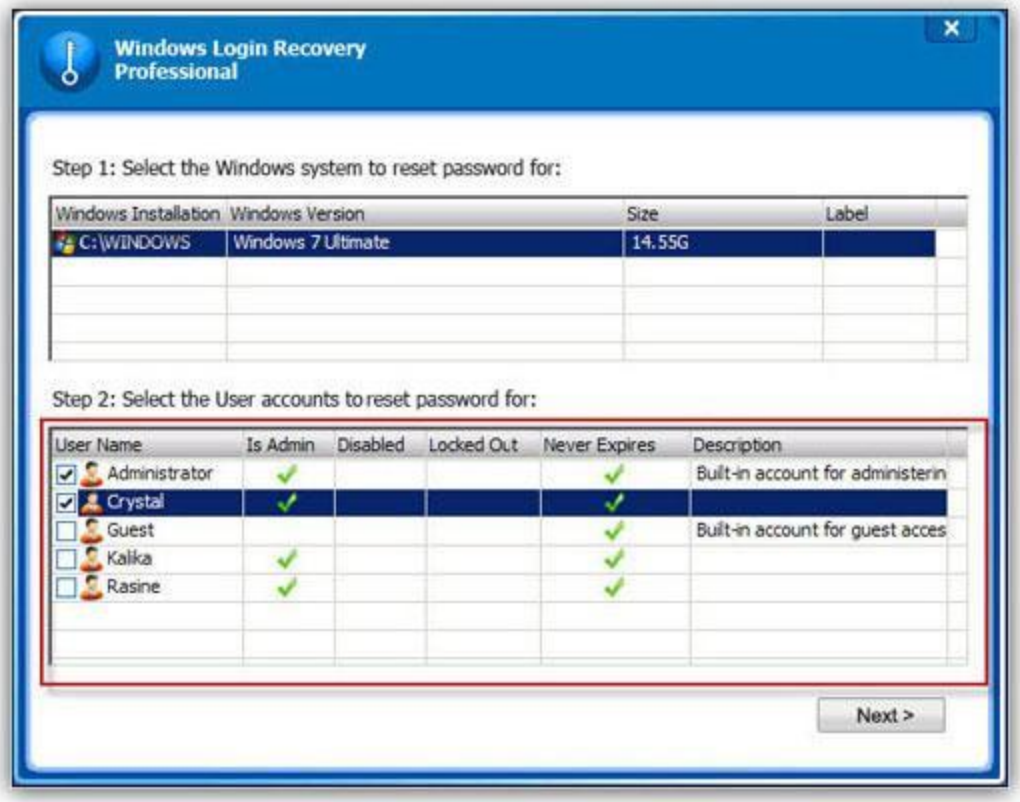
در مرحله بعد برنامه ار ما می خواهد که یک دیسکت حذف کننده پسورد را ایجاد کنیم این و ما می توانیم یا یک CD راه انداز ایجاد کنیم یا خیر گزینه ی دوم را انتخاب کنیم که یک USB فلش بوتایبل داشته باششیم که طب نیاز کاربر یکی را باید انتخاب کنیم .و بر روی Burn کیک می کنیم تا سیدی آماده کار شود .



در صورتی که بر روی گزینه دوم USB Flash کلیک کنیم باید بر روی Start کلیک نماییم تا برنامه مراحلی را برای آماده سازی USBفلش انجام نماید .

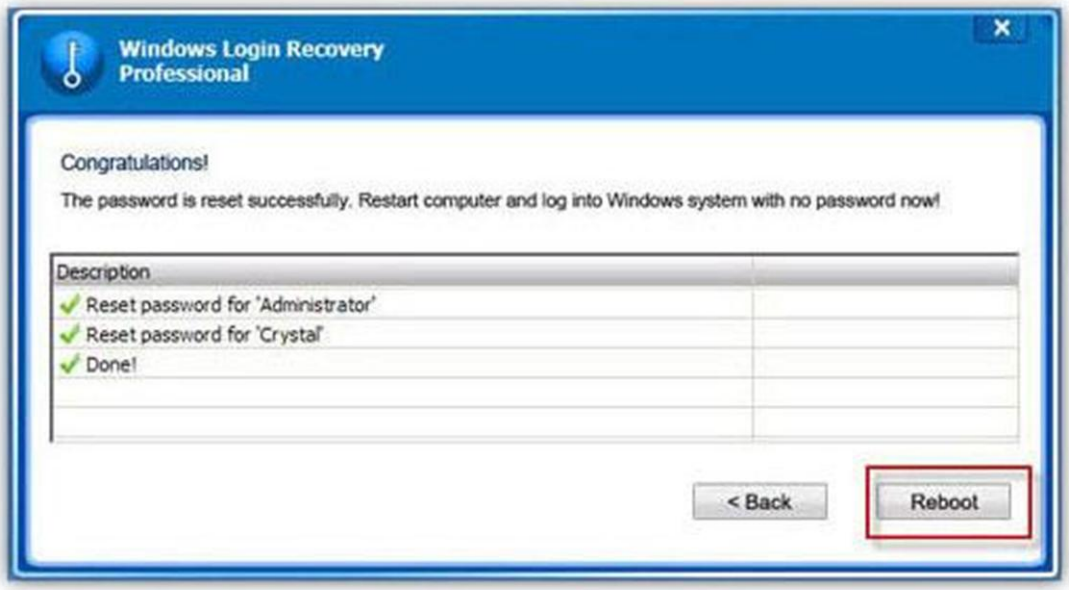
و بعد از اتمام و آماده شدن فلش بر روی Close کلیک نمایید

سپس باید با USB Flash و یا CD بوت کنید و آنها ا بالا بیاورید تا برنامه شروع به کار کند و مراحل جهت تشخیص درایو ویندوز و محل فایل Sam انجام شود و صفحه ی زیر ظاهر شود .که لیست کلیه حساب های کاربری را در خود دارد و شما می توانید با تیک دار کردن هر یک از حساب های کاربری پسورد آن را با زدن دکمه Next حذف کنید



در صورتی که از سیستم عامل های ویندوز Server 2008 , 2003 استفاده می کنید و گزینه Reset Domain administrator password for Server 2008/2003/2000 را انخاب کرده اید با زدن Next به صفحه ی زیر میروید و می توانید گزینه خود را جهت حذف پسورد تیک دار کنید .

با زن Next صفحه زیر به منظور انجام موفقیت آمیز عملیات نشان داده می شود و جهت رفتن به ویندوز و راه اندازی دوباره سیستم بر روی گزینه ی Reboot کلیک می نماییم .



پسورد برنامه ی Winrar

روش های گفته شده ی زیر تنها روش برای پیدا کردن پسورد این برنامه است و هیچ راه دیگری به غیر از موارد گفته شده در این مقاله را ندارید پس بی خود وقت خودتان را در مورد شکستن پسورد برنامه ی وینرار تلف نکنید چون به هیچ نتیجه ای نمی رسید .البته بماند حال شاید فردا که از خواب بلند شدیم یک الگوریتم ریاضی برای این الگوریتم رمز نگاری کشف شد ☺

در بسیاری از سایت های حرفه ای و غیر حرفه ای بحث های زیادی در این رابطه شده و متاسفانه و یا خوشبختانه به دلیل الگوریتم پیچیده ای که در پسورد برنامه winrar به کار برده شده کسی به هیچ نتیجه ای نرسیده است .

در Winrar پسورد به صورت کد شده است و الگوریتم آن هم یک الگوریتم غیر قابل بازگشت می باشد این برنامه از الگوریتم رمزنگاری AES 128 بیتی استفاده می کند شاید بگم نه تنها در سایت های ایرانی حتی در سایت های معروف خارجی هم نتوانسته اند زیاد به نتیجه ای مطلوبی در این رابطه برسند به همین دلیل بهتر است چند توصیه در این رابطه را بگویم که در خیلی از موارد هم جواب داده است .

فرض کنید شما یک فایل Rar را دانلود میکنید و بر روی آن پسورد وجود دارد .در این گونه مواقع شاید بگم روش های زیر 40%جواب داده اند .

- امکان دارد نام فایل Rar خود کلمه ی پسورد باشد و یا اینکه نام یک سایت باشد و یا ... شما می توانید با کمی آزمایش و خطا و اضافه کردن پسوند های com. و ... به آخر نام فایل Rar و یا www. به اول آن پسورد را پیدا کنید .

- در بعضی از موارد با باز کردن فایل در قسمت comment یا پسورد فایل می باشد و یا نام سایت سازنده ی این فایل و یا ...شما با کمی آزمایش و خطا امکان دارد پسورد را بدست

آورید .

- در بعضی از موارد یک فایل Txt و یا Inf و ...در درون این فایل ها وجود دارد که یا پسوردی بر روی آنها نیست و در درون آن یا پسورد و یا نام سایت و یا شاید نام خود آن فایل کلمه ی پسورد و یا نام سایت سازنده باشد که باز بحث به آزمایش و خطا بر می گردد

به عنوان مثال فرض می کنیم که در قسمت comment و یا نام فایل و ... نام یک سایت باشد (مثلا نوشته باشد Sanandaj) خوب ما در این حالت باید گزینه های زیر را امتحان کنیم

shabgard

shabgard.org

www.shabgard.org

Shabgard

Shabgard.org

www.Shabgard.org

WWW.SHABGARD.ORG

- در صورتی که موارد بالا کار نکرد باید به اینترنت متصل شوید و با زدن نام فایل مورد نظر در گوگل (فارسی یا انگلیسی) پسورد فایل در سایتی که اولین بار این فایل را پخش کرده است نوشته شده است (و یا شاید در هر سایت دیگری پسورد باشد)این روش بسیار جواب داده چون اکثرا مشاهده شده که یک فایل Rar که در آن یک کتاب و یا یک نرم افزار و ... می باشد قبلا توسط فرد دیگری گذاشته شده است و چون دست به دست (فلش به فلش ☺) گردیده پسورد را فراموش کرده اند و می شود با یه سرچ در گوگل آن را دوباره بدست آورد .حال در اینجا گوگل هکینگ هم بسیار به کار ما می آید به عنوان مثال اگر فایل Rar با نام SST را دارید می توانید از فرمان زیر در گوگل استفاده کنید (یک نمونه ی بسیار ساده)

"پسورد :" + "SST.rar"

"Password :" + "SST.rar"

فارسی یا انگلیسی بزنید زیاد وقتتون رو نمی گیره .

- بسیاری از کاربران به دلیل بی حوصلگی و یا فراموش کاری بیش از اندازه پسورد هایی که برای فایل های خود می گذارند با پسوردی که برای ایمیل خود و یا سایت خود انتخاب می کنند دقیق یکی بوده و شما می توانید با بدست آوردن پسورد های دیگر این کاربران به کلمه ی عبور دست یابید .که البته این کار نیازمند یادگیری علوم هکینگ بوده و افراد مبتدی بهتر است به این روش فکر نکنند .
- در بسیاری از موارد هم می شود که سورد را حدس زد چون بسیاری از کاربران مبتدی و فراوش کار پسود های خود را کلماتی مانند 123456 ، 123123،55555، اسم خود ، شماره تلفن خود ، شماره شناسنامه ، نام فک و فامی خود و از همه مهمتر شرح حال خود و آن چیزی که علاقه دارند باشند مانند zerangtarinam و... را برای پسورد خود انتخاب مکنند . باید این مطلب را به شما بگم که بیش از 90% افراد مبتدی که با آنها رابطه داشتم پسورد های خود را اینگونه انتخاب کرده اند .که واقعا جای تعجب داره :دی

و اما ...

در صورت پیدا نشدن پسورد دیگر باید به سراغ نرم افزار ها برویم . نرم افزار های زیادی در این رابطه وجود دارد که با نام های winrar password recovery یا winrar password remover یا Winrar Password Cracker و ... که در اینترنت فراوان است و در یک سرچ جزئی در گوگل می توانید آنها را پیدا کنید این نرم افزار ها از 2 روش استفاده می کنند .

1 – دیکشنری (Dictionary)

2 – بروتیفورس (Brute Force)

روش اول :

- در روش Dictionary برنامه از یک DB که انواع و اقسام نام ها (حیوانات تا نام انسان و خلاصه همه چیز) وجود دارد استفاده می کند و دنبال کلمه ی پسورد در میان آن دیکشنری می گردد در صورتی که پسورد در فهرست باشد که پسورد را تشخیص می دهد بهتر است برای استفاده از این کار از یک دیکشنری کامل استفاده کنید . البته دیکشنری های زیادی هم وجود دارد که بسیار کامل هستند ولی این دیکشنری ها بیشتر اسامی افراد خارجی را در خود دارند و در کل امکان پیدا شدن پسورد از طریق روش دیکشنری بسیار کم هست . شما هم خود می توانید که کلمه هایی که به ذهنتان می خورد خود در فای دیکشنری که یک فایل متنی با پسوند TXT بوده را اضافه کنید تا درصد به دست آوردن پسورد بالا رود .

روش دوم :

- در روش brute force هم ،به چک کردن حروف ها که ترکیبی از اعداد،حروف کوچک و بزرگ و سیمبل ها است می پردازد در این روش که مدت زمان آن هم معلوم نیست یعنی امکان دارد 1 ساعت و تا 20 سال طول بکشد پس این روش یک روش 100% عملی در بدست آوردن پسورد Winrarاست ولی برای بدست آوردن کلمه ای مثل s04(#P5?< R|{ که یک پسورد 13رقمی هست باید 3- 4 سال یک کامپیوتر را روشن بگذاریم .البته بگم به سرعت کامپیوتر هم بستگی داره مثلا سوپر کامپیوتر ها زود تر پسورد رو گیر میاورند تا کامپیوتر های خانگی : D ☺.

- نوع Brute force کردن هم شرط هست مثلا شما می توانید با استفاده از یک شبکه این کار را

انجام دهید برای این کار اول نیاز هست که یک نرم افزار مدیریت برای تقسیم رنج کلمات عبور برای هر کامپیوتر طراحی کنید و عملا به هر کامپیوتر محدوده کوچکی از پسوردها را برای چک کردن بدهید . اون برنامه به عنوان مدیر تصمیم گیرنده رنج کاری را به هر کلاینت اعلام میکنه و اون کلاینت هم لیست پسورد را براساس دستور دریافتی جنریت و سپس روی فایل رمز دار اجرا میکنه .

برای ساده تر کردن موضوع فکر کنید که پسورد فقط از اعداد تشکیل شده ...

```
Client1   0000   1000
Client2   1001   2000
Client3   2001   3000
Client4   3001   4000
Client5   4001
Client6
Client7
...
```

هر کامپیوتری پسورد را به روش بروتیفورس پیدا کرد به سرور مادر اطلاع می دهد.

در این روش زمان پیدا کردن پسورد به تعداد کامپیوتر ها نصف شده و پسورد زودتر پیدا می شود .

ولی به طور کل شما برای بدست آوردن این پسورد ها نیاز به جمع آوری اطلاعات بیشتری دارید که سرعت کار را بالا ببرید و برای این کار اول سرچ در گوگل و بعد مهندسی اجتماعی (که در این ضمینه زیاد

بحث شده) را توصیه می کنم .این رو بگم که شما می توانید در بحث مهندسی اجتماعی حتی کل پسورد را یا مقداری از آن را حدس بزنید فقط نیازمند یک هوش خلاق و ..... d: است .

نحوه ی حذف پسورد برنامه Access Administrator

به مسیر زیر از رجیستری برید .

HKEY_LOCAL_MACHINE\SOFTWARE\Access Administrator

و مقدار f94b2aa 281744411را به حذف نمایید .

نحوه ی حذف پسورد برنامهClick And Lock1

به مسیر زیر از رجیستری برید .

HKEY_CURRENT_USER\Software\Microsoft\Secsys\pm

و مقدار PWD را به "" یعنی Null تغییر بدید .

نحوه ی حذف پسورد برنامهProgram Protector

به مسیر زیر از رجیستری برید .

HKEY_LOCAL_MACHINE\SOFTWARE\Karlis Blumentals\Program Protector\3.0\

و مقدار password را حذف نمایید .

نحوه ی حذف پسورد برنامه Ashampoo Magical Security

به مسیر زیر از رجیستری برید .

HKEY_CURRENT_USER\Software\Ashampoo\Ashampoo Magical Security 2

و مقدار prevPasswordHash را حذف نمایید .

نحوه ی حذف پسورد برنامه Anfibia Deskman

به مسیر زیر از ویندوز برید

C:\users\ All Users\Application Data\Deskman9\

و فایل deskman.dat را حذف نمایید .

نحوه ی حذف پسورد برنامه Access lock

به مسیر زیر از ویندوز برید

C:\users\ All Users\Application Data\Access Lock

و فایل f2c01301.dat را حذف نمایید .

نحوه ی حذف پسورد برنامه Private Encryption

به My Documents خودتون برید و فایل های Hidden و سیستمی رو Show کنید و فایل dwphtlts.dvr را حذف نمایید.

سپس به مسیر زیر از رجیستری برید

HKEY_CURRENT_USER\Software\Microsoft\trsys\copp\

و مقدار u را حذف نمایید

و دوباره به مسیر زیر برید

HKEY_CURRENT_USER\Software\Microsoft\trsys\copp\

و مقدار t را حذف نمایید .

نحوه ی حذف پسورد برنامه XP Smoker

به مسیر زیر از رجیستری برید

HKEY_LOCAL_MACHINE\SOFTWARE\WareSoft Software\XP Smoker

و مقدار Password Set را حذف نمایید .

نحوه ی حذف پسورد برنامه Lock My Pc

به مسیر زیر از رجیستری برید

HKEY_LOCAL_MACHINE\SOFTWARE\FSPro Labs\Lock My PC 4

و مقدار hkSmرا حذف نمایید .

نحوه ی حذف پسورد برنامهPC Security Tweaker

به مسیر زیر از رجیستری برید

HKEY_LOCAL_MACHINE\SOFTWARE\PC Security Tweaker

و مقدار DEFAOPTIONS را حذف نمایید

نحوه ی حذف پسورد برنامه st Security Agent1

به مسیر زیر از رجیستری برید

HKEY_LOCAL_MACHINE\SOFTWARE\1st Security Agent

و مقدار DEFAOPTIONS را حذف نمایید .

نحوه ی حذف پسورد برنامهPC Security

فایل زیر رو حذف کنید که در شاخه X:\windows هستند

gercescp.dvr
dwpces23.dru

و بعد به مسیر زیر برید در رجیستری

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\trsys\copp\

و مقدار S رو حذف کنید

نحوه ی حذف کردن پسورد برنامهSecurr Browser

فایل زیر رو در X:\windows حذف نمایید

gerwrbes.dvr

و مقدار b را در مسیر زیر از رجیستری حذف کنید

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Secsys\copp

نحوه ی حذف کردن پسورد برنامهSecurr Browser

فایل زیر رو در X:\windows حذف نمایید

gerwrbes.dvr

و مقدار b را در مسیر زیر از رجیستری حذف کنید

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Secsys\copp

نحوه ی حذف پسورد برنامهPassword Door

اول از هر کاری پروسه TLPD.exe را End نمایید.

و سپس وارد مسیر زیر شوید

X:\User\All Users\Application Data\TopLang\Password Door

و فایل PDoor.dat را حذف نمایید .

نحوه ی حذف کردن پسورد برنامهFolderMage Pro

فایل زیر رو پاک کنید و تمام

X:\windows\deff1.dat

نحوه ی حذف پسورد برنامهStealth Encrypto

وارد مسیر زیر بشید در ویندوز

X:\windows

و دو فایل زیر را حذف نمایید.

GERHTS61.DRU
DWPHTS61.DRU

نحوه ی حذف پسورد برنامهPrivate Desktop

وارد مسیر زیر بشید از رجیستری

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\trsys\pd

و مقدار p رو حذف کنید

و بعد وارد مسیر زیر بشید در ویندوز

X:\windows

در اینجام فایل gerkseds.dvrرا حذف نمایید .

نحوه ی حذف پسورد آنتی ویروسnod32

در Safemode وارد مسیر زیر بشید.

HKEY_LOCAL_MACHINE\SOFTWARE\ESET\ESET Security\CurrentVersion\Info

و مقدار PackageID را حذف می کنیم.

نحوه ی حذف پسورد برنامهUSB Disk Security

در رجیستری به مسیر زیر برید

HKEY_LOCAL_MACHINE\SOFTWARE\ZbshaLab\USBGuard

و مقدار pwd را حذف کنید .

نحوه ی حذف پسورد برنامهHide My Folders

وارد مسیر زیر بشید از رجیستری

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\H FCore

و مقدار Password را حذف کنید .

نحوه ی حذف پسورد برنامهPrivate Pix

وارد مسیر زیر بشید از رجیستری

HKEY_CURRENT_USER\Software\Microsoft\Secsys\pm

و مقدار pwd را حذف کنید .

نحوه ی حذف پسورد برنامهClear Lock

وارد مسیر زیر بشید از رجیستری

HKEY_LOCAL_MACHINE\SOFTWARE\1st Security Agent

و مقدار DEFAOPTIONS را حذف کنید

نحوه ی حذف پسورد برنامهSecurity Administrator

به مسیر زیر میریم تو رجیستری

HKEY_LOCAL_MACHINE\SOFTWARE\Security Administrator

و مقدار DEFAOPTIONS رو حذف می کنیم و تمام

نحوه ی حذف کردن پسورد برنامه Anti porn

اینو میزارم برا بچه هایی که پدر مادراشون اونارو محدود کردن D: و با خیال راحت برید هرچی میخوایید

نگاه کنید d:البته عبور از فیلترینگ هم خودش یک مرحله دیگست اونش عهده ی خودتون

وارد Safe mode شید و فایل زیر را پاک میکنیم

X:\windows\Eleathe.bmp

نحوه ی حذف پسورد برنامهFolderGuard

وارد رجیستری بشید و به کلید زیر برید

HKEY_LOCAL_MACHINE\SOFTWARE\WinAbility\FGD

و تو این قسمت مقدار FGP را حذف کنید و بعد به مسیر زیر برید

X:\Users\All Users\Application Data\Folder Guard

و در اینجام فایل FGp را حذف کنید و تموم خوش پسورد برنامه حذف میشه

در خاتمه دوست دارم به مطلبی اشاره کنم . دنیای اینترنت که حاوی تمام علوم بشریت و تمرکز تمام داشته های انسان است سرشار از علوم و یافته ها و آگاهی های مفید و سرنوشت ساز است که ایام بیکاری را غنا می بخشد . موجب رشد و ارتقا انسان میگردد ولی متاسفانه برخی از کاربران از این گنجینه های با ارزش آن بابی تفاوتی می گذرند و به فضای های مسموم و بی ارزش می پردازند یکی از این موارد عمر بر باد ده همانا فضای چت روم و هم نشینی و مصاحبت با مشتی افراد عقده ای و مریض احوال است البته نه همه شاید بعضی از کنجکاوی سرکی بکشند ولی براستی آن فضا در شأن انسانهای سالم و با شخصیت نیست خوش ندارم که چندین ماه وقت با ارزش شخصی در آنجا تلف شود و بعد متوجه این حقیقت تلخ گردد بی تردید یکبار زندگی خواهیم کرد . عمر دوباره ای به ما داده نخواهد شد پس آن را پاسداریم و بیهوده نگردانیم .

Spider Security Team

From sanandaj

Author : Moslem Haghighian (l4tr0d3ctism)

3mail : l4tr0d3ctism@yahoo@gmail@hotmail.com

Special Thanks To :

All SHabgard Digital Security Groups Members

All Black Hat Group Security Center members

☹|=453 914I-; 914I-;3 ☹