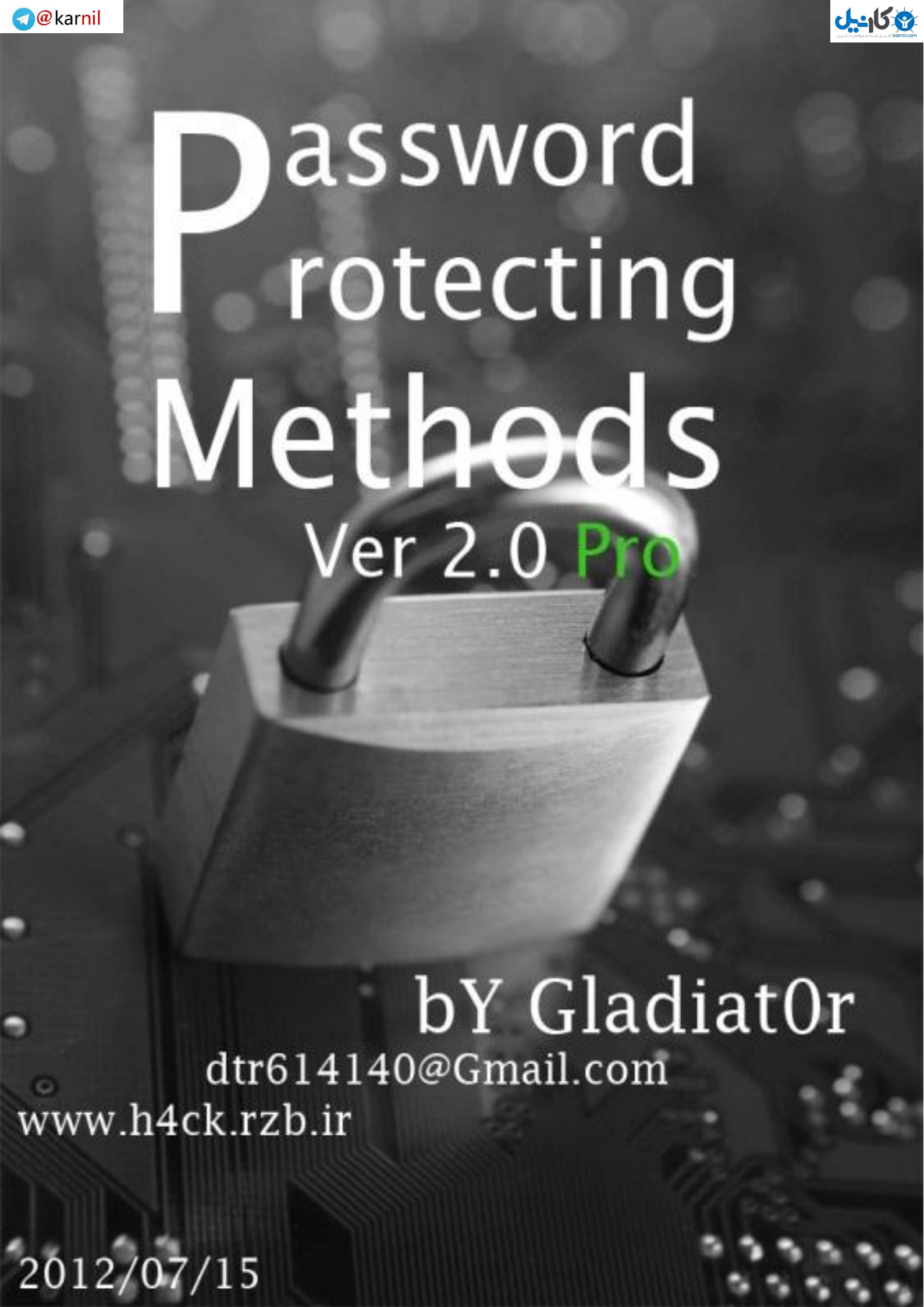
✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و..... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

www.karnil.com

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

https://telegram.me/karnil



Password Protecting Methods

Ver 2.0 Pro

bY Gladiat0r

dtr614140@Gmail.com

www.h4ck.rzb.ir

2012/07/15

Book Information:

Name: Password Protecting Methods Ver 2.0 Pro

Writer: Hassan Lotfi [Gladiat0r] ----- ----- ----- Age: 19 Years

Date & time of write: 02/05/1391 - 3:31 PM

E-Mail: dtr614140@Gmail.Com

Website: http://h4ck.rzb.ir

Tell: +989373153178

v^v^v^v^v^v^v^ v^v^v^v^v^v^v^ v^v^v^v^v^v^v^v^v^v^v^v^v^v^v^v^v^v^

نام کتاب : روشهای محافظت از پسورد ویرایش 2 Pro

نام نویسنده : Hassan Lotfi [Gladiat0r]

تاریخ نگارش: ۲ مرداد ۱۳۹۱ هجری خورشیدی

تشکر و قدردانی:

از کلیه دوستانی که در نگارش این مقاله به بنده راهنمایی و کمک رساندند بخصوص **ارباب مجازی** تشکر صمیمانه و آرزوی موفقیت روزافزون برای تک تک ایشان را خواستارم.این مقاله باید ۸ روز پیش نوشته می شد که بدلیل مشغله کاری امروز نوشته شد.

مقدمه:

امروزه امنیت به یکی از مهمترین مشخصه های یک سیستم یا یک شبکه یا یک وبسایت و یا ... می باشد و بدون داشتن امنیت هیچ یک از موارد فوق کارایی و اطلاع رسانی مناسبی را نخواهند داشت. از این رو بسیاری از مدیران شبکه ها و وبسایت ها بیشتر به امنیت بالای خود اهمیت می دهند. اینجانب نیز در پی کمکی کوچک به این افراد مهم و پر مشغله اقدام به نگارش مقالاتی کوچک با موضوع حفاظت از پسورد نمودم تا کمکی شایان و هرچند کوچک به این افراد را داشته باشم. اولین مقاله از این موضوع اواخر اردیبهشت ماه سال جاری منتشر شد و در پی آن انتقادات و پیشنهادات و راهنمایی های بیشتری به من از سوی شما خوانندگان محترم ارسال شد. بنده نیز برآن شدم تا نگارش دوم و البته حرفه ای این مقاله را منتشر سازم تا از تعداد انتقادات و سوالات مبنی بر مطالب مقاله بکاهم و نیز روشهای جدیدتری از حفاظت را به اطلاع شما برسانم.

امیدوارم تا این مقاله توانایی پاسخگویی به سوالات شما عزیزان در زمینه امنیت را داشته باشد.ازتمامی دوستان و خوانندگان که به من در نوشتن این مقاله انرژی و نشاط دادند صمیمانه سپاسگزارم.

ببخشید سرتون درد اومد!

من در این مقاله ابتدا گوشه چشمی به روشهای هک و نفوذ به پسورد و در پایان شرح هرکدام نیز راههای مقابله با این روش را بیان خواهم کرد.

الف) مهندسی اجتماعی: این روش روشی قدیمی ولی بسیار پرقدرت تر از روشهای دیگر است زیرا بر هوش و ذکاوت هدف بستگی دارد و هرچه فرد مورد حمله از طریق این روش ساده لوح تر و نسبت به موارد مهم امنیتی بی اهمیت تر باشد زودتر در این حمله شکست خواهد خورد. هکرها در نفوذ به موارد مهم تر و دستیابی به اطلاعات محرمانه و حیاتی از این روش استفاده می کنند. مثالهایی در اینترنت دیده شده است که از این روش برای گرفتن رمزهای عبور اکانت های نامه های الکترونیکی یا شارژهای سیم کارتهای اعتباری یا مواردی مشابه استفاده شده است.

روش مقابله با این حمله:

اکثریت هکرها روشها یا مواردی را مطرح می کنند که لابه لای آنها از شما درخواست رمز عبور یا هرچیز مهم دیگری را می کنند. که دریافت این اطلاعات از طرف شما بسیار عادی به نظر برسد.مثلا یک هکر خود را در نقش یک فرد بسیار قابل اطمینان جا زده یا روشهایی را بیان می کند که در آنها دسترسی رایگان و سریع تر به اطلاعات دیگران یا روشی برای دریافت دوبرابر مقدار مجاز از یک مورد باارزش مانند شارژ سیم کارت و یا ... از طریق دوستان یا اوپراتورهای تلفن همراه را بیان می کنند. شما باید بدانید که هیچ یک از این روشها قابل اجرا نیست و مسئولین اصلی از قبل برای این حمله چاره ای را اندیشیده و دسترسی به این

موارد را ممنوع کرده اند.قبل از اینکه به این موارد پاسخ دهید ابتدا با مسئول اصلی آن تماس حاصل کرده و از صحت این روش اطلاع یابید.

مواضب ایمیل های دروغین باشید.برخی از هکرها با ارسال ایمیل دروغین از طرف سرور ارائه دهنده اکانت (مانند یاهو یا بلاگفا و ...) از شما درخواست تغییر رمز عبور و ارسال به ایمیل خود یا اعلام پسورد به خودشان را می کنند.

ب) روش حدس زدن:در این روش هکرها با حدس زدن پسورد شما که یک عبارت ساده (مانند شماره تلفن ، تاریخ تولد ، نام دوست یا بازی یا شخص مورد علاقه و یا مواردی مشابه است) به اطلاعات شما دسترسی پیدا می کند.در این روش پسورد هدف از ضعف امنیتی برخوردار است.

روش مقابله با این حمله:

برای اینکه مورد حمله از طریق این روش قرار نگیرید هرگز پسورد خود را مواردی ساده و قابل یادآوری توسط دیگران انتخاب نکنید.و آن را طوری انتخاب کنید که یادآوری آن توسط خودتان آسان و توسط دیگران دشوار باشدو بصورت یک راز آنرا نزد خود نگه دارید.هرگز پسورد خود را به افراد غیر قابل اعتماد ندهید.

اگر در سایت های اینترنتی عضویت دارید یا از چند اکانت استفاده می کنید هیچ گاه پسودی یکسان برای تمامی ان ها استفاده نکنید(از یک پسورد برای چند اکانت اسفاده نکنید.) چون در این صورت اگر یک هکر به یک اکانت شما نفوذ کند به راحتی می تواند به اکانت های دیگر شما نیز نفوذ کند. برای افرادی که توانایی به خاطر سپردن چندین پسورد را ندارند توصیه می کنم تا برای اکانت های مهم تر خود (مانند ایمیل و کارت اعتباری) پسوردهای قویتری را انتخاب کنند.

پ)روش فرهنگ لغت:در این روش هکرها با استفاده از نرم افزارهای مربوط به این روش پسوردهای قابل حدس زدن یا کلمات رایج مانند نامهای انسانها یا اشیاء را به نرم افزار می دهند و نرم افزار با تست کردن این پسوردهای نمونه (که تست این پسوردها در سرعتی بسیار بالا انجام می گیرد) پسورد نهایی و اصلی را تشخیص می دهند.این روش قادر به تشخیص پسوردهای ترکیبی (amirali→4m1r@li) نیز می باشد.

روش مقابله با این حمله:

برای مقابله با این حمله نمی گویم از روش پسورد ترکیبی استفاده کنید! در استفاده از این روش اسامی خاص و رایج را ترکیب نکنید. اسامی را حداقل به هم بریزید و سپس ترکیب کنید یا اینکه جملات بی ربطی بسازید سپس آنها را ترکیب کنید.همچنین پسورد خود را تا می توانید طولانی انتخاب کنید تا دیر تر تشخیص داده شود.در اینجا من کلمات رو به صورت طنز در آوردم طوری که قابل تشخیص نیست سپس به هم ریختم و جابجایی و ... مثلا:

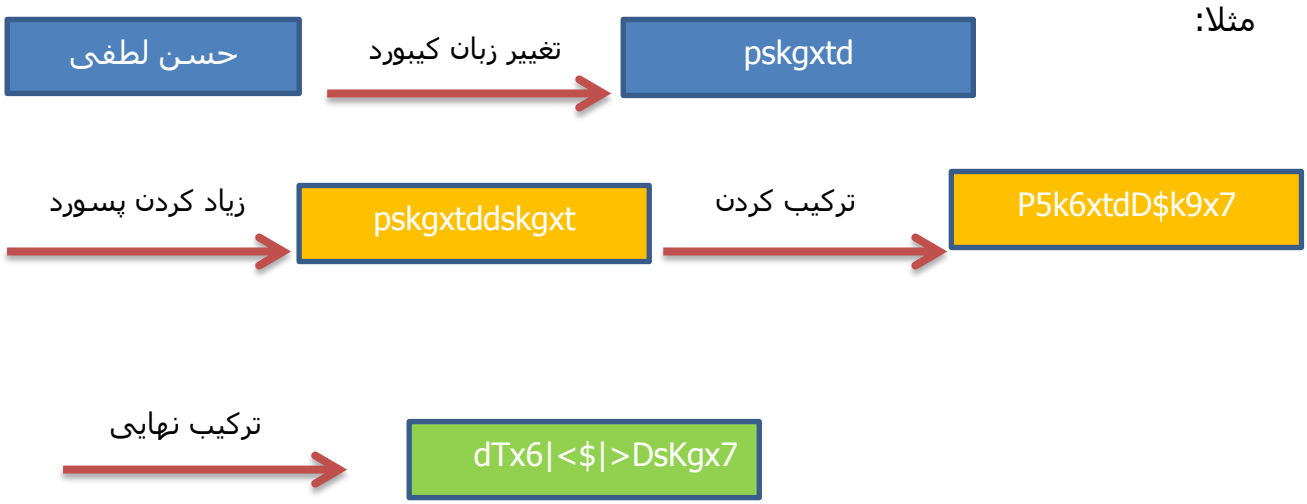
Kilimanjaro ---> karimounjaro ---> K4@rim0uN64ro ---> 4K@R10ouNgAr0M --->

--->4K@R1o0Uog6RoNM

این عبارت می تواند پسورد شما باشد.

یا اینکه پسورد خود را با تغییر زبان وارد کنید. مثلا اگر کلمه یا عبارتی را می خواهید به عنوان پسورد انتخاب کنید به زبان لاتین است آنرا با زبان فارسی وارد کنید و برعکس.

مثلا:



عبارت کادر سبز رنگ می تواند پسورد شما باشد.

یا اینکه از این روش استفاده کنید بدین صورت که کلمه عبور خود را که انتخاب کردید حروف آنرا حروف کناری حروف اصلی در کیبورد قرار دهید.مثلا:

Hassan ---> gsaasn ---> 65@4AS5$N

بدین ترتیب می توانید با استفاده از این روش یک پسورد قوی برای خود ایجاد کنید تا از خطر این حمله مصون بمانید☺

ت) روش ورود به اجبار:این روش که زمان زیادی برای کشف پسورد لازم دارد، قادر به شکستن و هک هر نوع پسوردی می باشد.در این روش هکر با آمیختن اعداد (1,2,3,...) ، کاراکترها(@,$,*,...) و حروف (a,b,c,...) می تواند پسورد صحیح را بدست آورد.لازم به ذکر است سرعت کشف پسورد توسط این نرم افزار به سرعت سیستم هکر بستگی دارد.

روش مقابله با این حمله:

روش حمله به صورت اجبار ، می تواند از امنیت پسوردهای ایجاد شده توسط کاراکترهای متفرقه و کلمات به هم ریخته بکاهد.در این حالت باید پسورد شما از تمامی روشهای مصون ماندن پیروی کرده باشد . اگر اینطور باشد هکر پس از چند روز عملیات ناموفق بالاخره خسته خواهد شد و دست از کرک کردن پسورد شما خواهد برداشت.(انشاءالله)!

ث) روش جدول رنگین کمان: این روش یک لیست قدرتمند از پیش طراحی شده از مقادیر Hash در هر صورت ترکیب شدن از کاراکترهاست.لازم است بگویم که Hash یک کلمه عبور است که به صورت غیر قابل برگست بوده و از هیچ الگوریتمی برای برگشت پذیری پیروی نمی کند(یعنی به هیچ روشی نمی توان آنرا به متن اصلی پسورد تبدیل کرد) .

در این لیست پسورد ها برای تست شدن از میان یک الگوریتم عبور می کنند و به صورت یک Hash در می آیند سپس با Hash اصلی مقایسه می شوند و در صورت یکی بودن پسورد کشف خواهد شد.

روش مقابله با این حمله:

برای مقابله با این حمله باید پسورد شما بیش از اندازه سخت و طولانی باشد. اما خوشبختانه این لیست ها به آسانی در دسترس نیستند.(آخییش!)

ج)حمله به روش فیک پیج:این روش رو دوست خوبم ارباب مجازی در کتابی با همین عنوان منتشر کرده است اما من اینجا برای راحتی کار شما آنرا توضیح می دهم.توصیه می کنم برای اطلاع بیشتر از نحوه این حمله این کتاب را حتما مطالعه بفرمائید.

این روش همان طور که از نامش پیداست با ایجاد صفحات وب دروغین لاگین می توان به پسورد هدف دست پیدا کرد. مثلا برخی از این فیک پیج ها به عنوان صفحه لاگین سرورهای وبلاگ یا ایمیل ساخته می شوند و طوری طراحی می شوند که فرد قربانی با کلیک کردن برروی گزینه لاگین، پسورد خود را برای هکر یا سازنده فیک پیج بدون اینکه اطلاع داشته باشد ارسال می کند.

روش مقابله با این حمله:

برای اینکه در دام فیک پیج نیفتید حتما دقت کنید هنگامی که قصد ورود به وبلاگ یا ایمیل یا هر اکانت دیگری را دارید حتما به آدرس صفحه لاگین دقت کنید که آدرس اصلی باشد.برخی از فیک پیج ها آدرس هایی بسیار مشابه با آدرس اصلی دارند مثلا:

Blogfa.com ---> Bl0gfa.com

یا

Gmail.com ---> Gamil.com

و یا

4shared.com ---> 4sherad.com

و یا ...

کتاب آموزش فیک پیج را از این وبسایت دانلود نمایید:

http://www.hacklib.sabablog.com

چ)حمله از طریق نرم افزارهای جاسوسی (تروجان ها ، جاسوس افزارها و ...):

در این روش هکرها با استفاده از نرم افزارهای جاسوسی (مانند کی لاگرها(Key loggers)) و تروجان ها (مانند تروجان های Magic-Ps و Sub 7) اقدام به کشف رمز عبور شما می کنند.

کی لاگرها نرم افزارهایی هستند که اقدام به ثبت کلیدهای فشرده شده کیبورد کرده و گزارش نهایی را به آدرس هکر ارسال می کنند. این نرم افزارها ممکن است در کافی نت ها نصب گردیده شده باشند و در هنگامی که شما نام کاربری یا رمز عبور یک حساب کاربری خود را وارد می کنید این کی لاگرها نام کاربری و رمز عبور شما را ذخیره کرده و در سیستم مدیر کافی نت ذخیره می کنند و یا هنگامی که شما از کافی نت برای انتقال وجه از حساب بانکی خود به حسابی دیگر یا انجام یک خرید اینترنتی استفاده می کنید کی لاگرها اقدام به ثبت رمز حساب شما کرده و امنیت حساب بانکی شما به خطر می اندازند.

اکثریت قریب به اتفاق کی لاگرها قابل شناسایی توسط آنتی ویروس ها و آنتی اسپای ویرها نیستند.

تروجان ها نیز یک برنامه مخرب هستند که توسط برخی از برنامه نویسان طراحی شده و انواع مختلفی دارند ولی هدف همگی آنها سرقت اطلاعات مهم هدف است. به عنوان مثال تروجان ☻☻☻☻ که یک تروجان ایرانی است جهت سرقت اطلاعات حسابهای کاربری یاهو در برنامه Yahoo Messenger طراحی شده است و یا تروجان ☺☺☺ که امکانات پیشرفته تری نسبت به Magic-PS دارد قابلیت ارسال یمیل های جعلی(Fake E-mails) را داراست و برنامه های دیگر که شرح امکانات آنها در این مقاله دور از انتظار است.تروجان ها رو بدون نام ذکر کردم تا از مطالب این مقاله سوء استفاده نشه!

تمامی تروجان ها توسط آنتی ویروس ها قابل شناسایی هستند.

روش مقابله با این حمله:

برای در امان ماندن از این حمله به نکات زیر توجه کنید:

A. در مورد کی لاگرها و دیگر برنامه های جاسوسی:

I. همیشه برای ورود به حسابهای کاربری مهم خود (مانند ایمیل و ...) و استفاده از امکانات حساب بانکی خود از رایانه خودتان استفاده کنید و اگر این امکان برای شما موجود نیست (مثلا اینترنت شما قطع شده و ...) از رایانه یک شخص قابل اعتماد استفاده کنید.

II. اگر از کافی نت ها برای ورود به حسابهای کابری یا استفاده از حساب بانکی خود استفاده می کنید حتما رمز عبور خود را با صفحه کلید مجازی ویندوز وارد کنید. این صفحه کلید از مسیرهای زیر در دسترس است:

1 – Start → Run → osk → ok

2 – (Windows 7): Start → All Programs → Accessories → Ease of Access → On Screen Keyboard

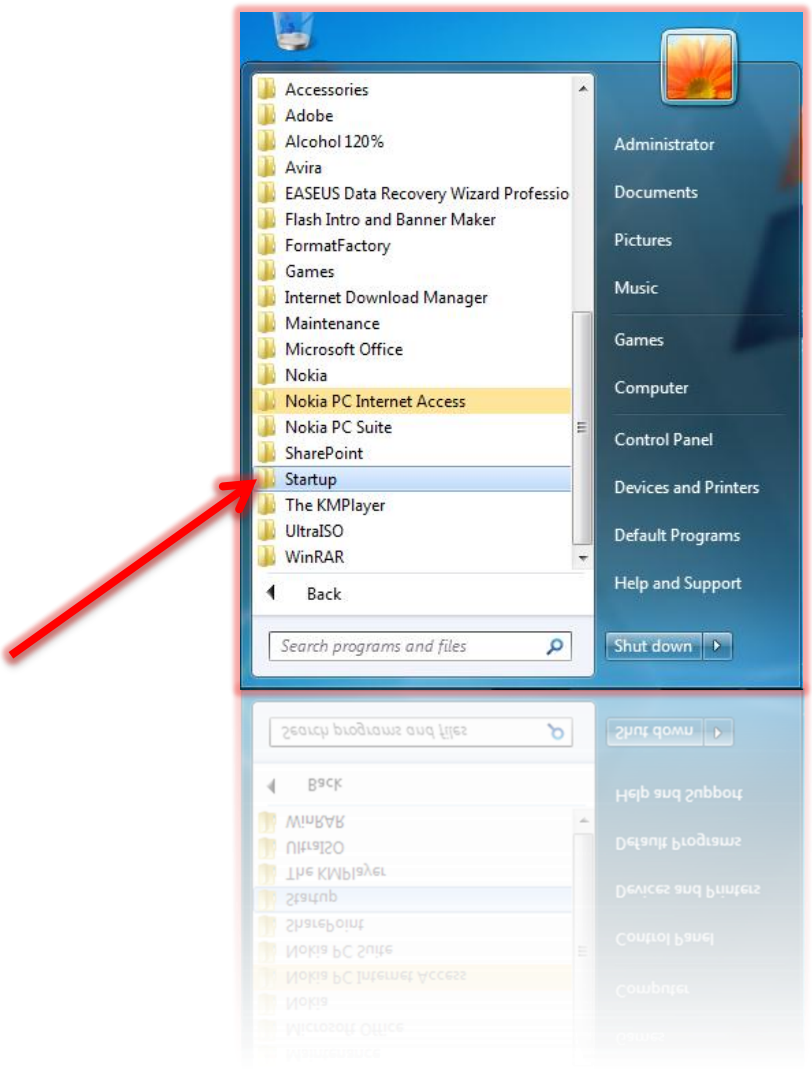
3 – (Windows XP): Start → All Programs → Accessories → On Screen Keyboard

III. از کاراکتر & و در ادامه تعدادی فاصله در پایان پسورد خود استفاده کنید. با این کار رمز عبور ارسالی توسط کی لاگرها غیر قابل خواندن خواهد شد.

IV. از آنتی ویروس هایی استفاده کنید که قابلیت Anti-Spyware را نیز داشته باشند. مانند Kaspersky Internet Security یا ESET Internet Security و یا ...

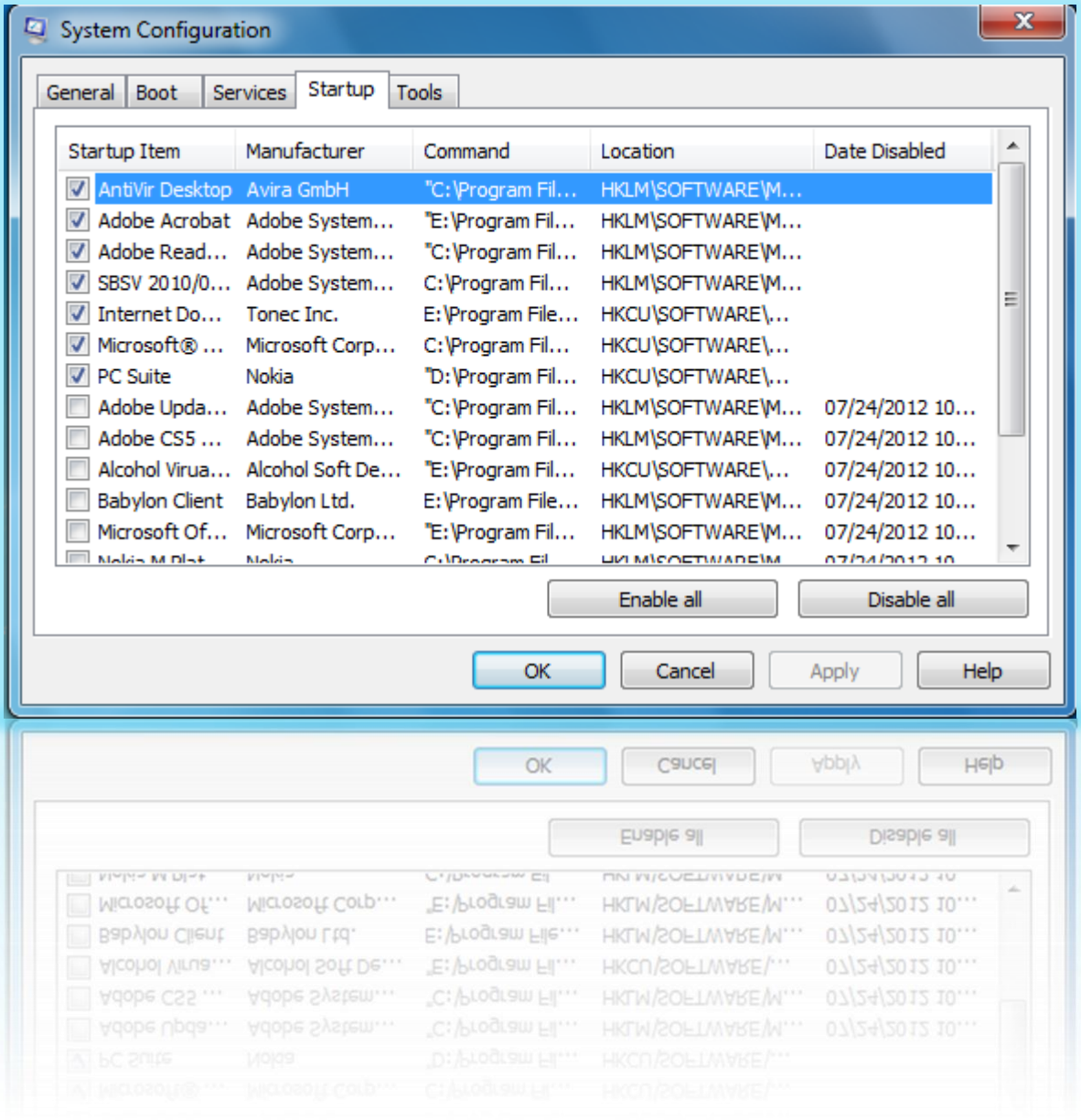
V. هر چند وقت یکبار فولدر Start upو بخش Msconfig را برای مشاهده نرم افزارهای اجرا شونده در هنگام شروع ویندوز را بررسی کنید تا برنامه های متفرقه قابل اجرا نباشند. فولدر Start Up در مسیر Start → All Programs و قسمت Msconfig از بخش Run قابل دسترسی هستند.

مسیر Start up:



START UP FOLDER

و قسمت Msconfig:



MSCONFIG

B. و در مورد تروجان ها:

تروجان ها موارد زیادی دارند که آنها را در مقاله بعدی اعلام می کنم!

حفاظت از پسورد برای مدیران شبکه

نکته:

من در اینجا برای آموزش این بخش از برنامه Local Security Policy استفاده خواهم کرد.

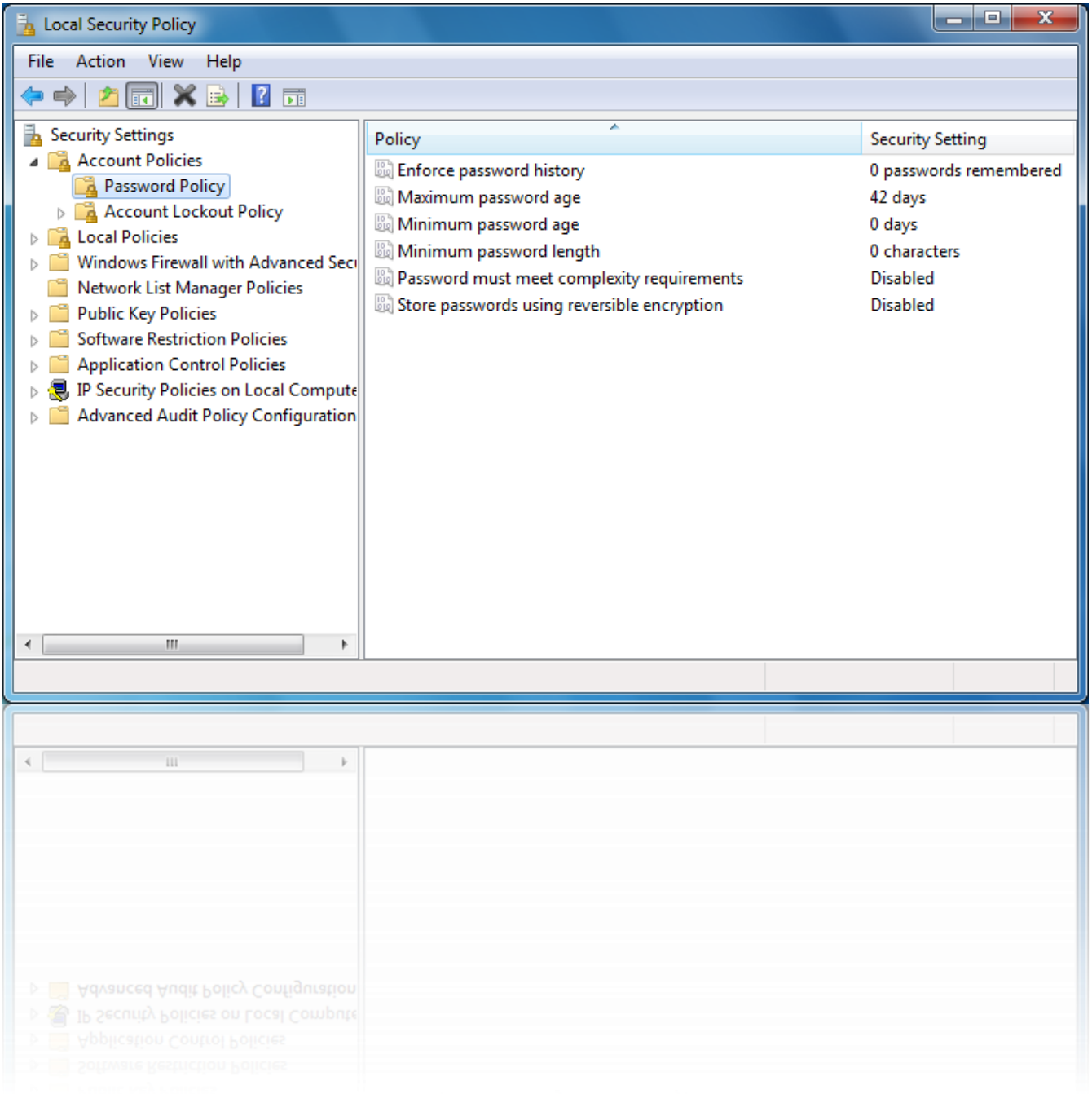
برای دسترسی به این برنامه و قسمت مربوط به حفاظت از پسورد می توانید از روش های زیر استفاده کنید:

الف) ویندوزهای XP، Server 2003-2008 و 2000:

Start → Control Panel → Administrative Tools → Local Security Policy → Account Policies → Password Policy

ب) ویندوز 7:

مشابه قسمت بالا ☺



حال من به شرح و بررسی هریک از گزینه های موجود در این بخش می پردازم:

- گزینه Password must meet complexity requirements:

با فعال کردن این گزینه ، پسوردها باید از موارد استاندارد رمزنگاری پیروی کنند. این موارد عبارتند از:

A. مشابه نبودن پسورد با نام کاربری
B. داشتن حداقل ۸ کاراکتر
C. شامل بودن پسورد از حروف لاتین (A,B,C,...)(a,b,c,...) ، اعداد (1,2,3,...) و کاراکترهای متفرقه(*,&,%,!,...)

- گزینه Enforce password history (Range:0-24) :

با توجه به این که کلمات عبور زمان انقضای مشخصی دارند ، برخی از کاربران پس از تاریخ انقضا همان پسورد قبلی را انتخاب می کنند. این گزینه بیانگر ان است که پس از گذشت چه مدت زمان و بعد از چندین بار اسفاده از پسورد جدید ، مجاز به استفاده از پسورد اول هستند.به منظور نگه داری موثر از پسورد ، نباید امکان تغییر پسوردها پس از پیکربندی گزینه Minimum password age وجود داشته باشد.

- گزینه(Maximum password age (range:0-999 days :

این گزینه مربوط به اعتبار و عمر پسورد می شود و اعتبار آنرا برحسب روز تعیین می کند که با در نظر گرفتن مقدار صفر عمر پسورد شما جاودان خواهد بود☺

- گزینه Minimum password age (Range:0-999 days) :

این گزینه حداقل عمر و اعتبار پسورد را تعیین می کند که با تعیین مقدار صفر برای این گزینه به کاربران اجازه داده خواهد شد تا بلافاصله پسورد خود را تغییر دهند.

نکته مهم: Minimum password ageباید از Maximum password age کمتر باشد. همچنین پیکربندی Minimum password ageباید طوری تعیین گردد که دارای یک مقدار بیشتر از صفر باشد تا گزینه password history نیز اعمال گردیده شده باشد.

بدون وجود یک Minimum password age کاربران قادر به تغییر دوره ای و زمان بندی نشده پسورد شده و امکان استفاده مجدد از پسوردهای قدیمی در یک محدوده زمانی کمتر برای آنها فراهم می شود.مقادیر پیش فرض تامین کننده اهداف و درخواست های امنیتی در یک شرکت نبوده و لازم است مدیران سیستم در ابتدا یک پسورد قوی را برای کاربر خود تعریف کنند و پس از گذشت زمان معینی کاربر را ملزم به تغییر پسورد تعیین شده از سوی مدیر سرور نمایند. زمانی که کاربران عمل Log on را انجام می دهند و در صورتی که password historyمقدار صفر را دارا باشد لزومی در تغییر پسورد جدید برای کاربران وجود نخواهد داشت. به همین دلیل مقدار تعیین شده برای این گزینه عدد یک می باشد.

- گزینه(Minimum password length (range: 0-14 :

این گزینه حداقل تعداد کاراکترهای تشکیل دهنده پسورد را تعیین می کند.با تعیین مقدار صفر برای این گزینه ضرورت وجود پسورد حذف خواهد شد. حداقل تعداد کاراکترهای پسورد را می توان ۸ کاراکتر در نظر گرفت .ولی برخی از شرکت ها مقدار ۱۲ را تعیین کرده اند.

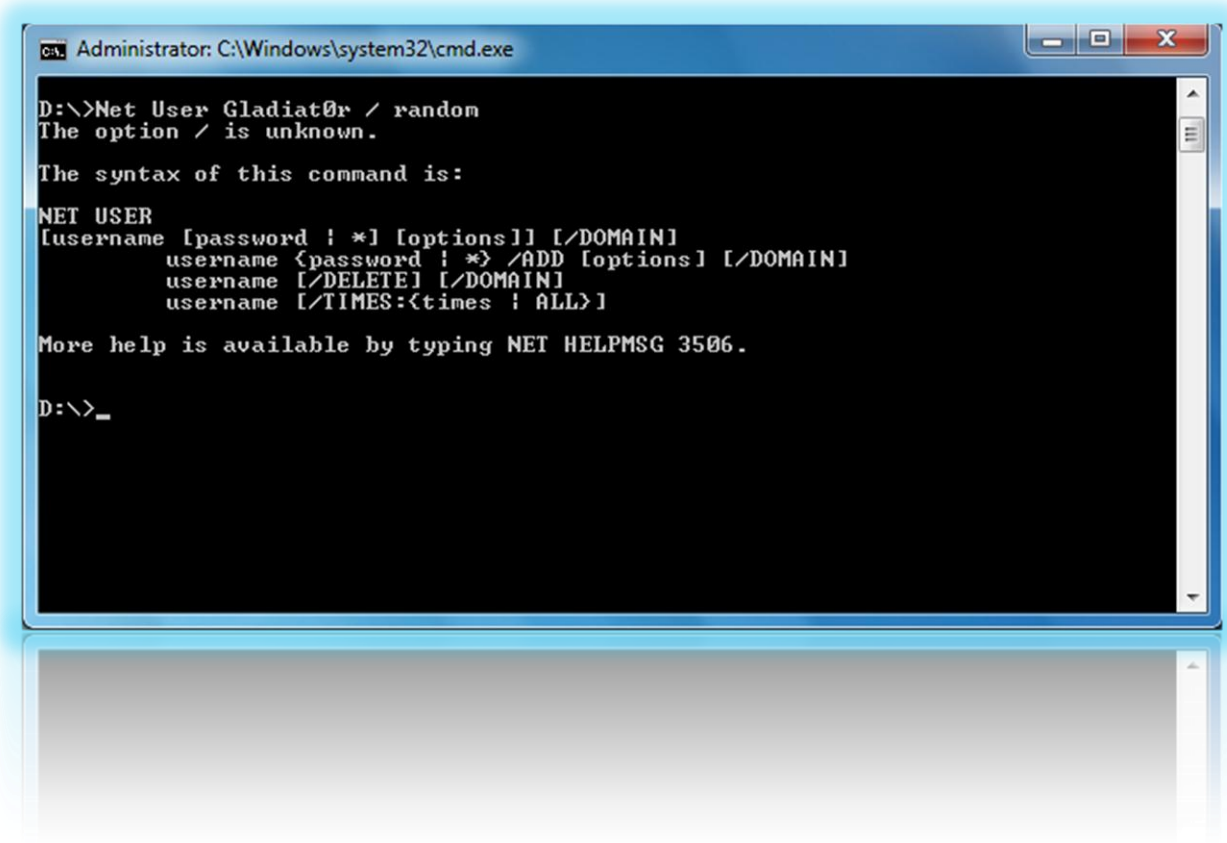
- گزینه (Store password using reversible encryption(for all user in the domain:

این گزینه تعیین کننده ذخیره سازی پسورد با استفاده از روش رمز نگاری وارونه می باشد.فعال کردن این گزینه باید با لحاظ کردن پارامترهای متعددی نظیر لزوم یک برنامه به منظور استفاده از یک پسورد محافظت شده صورت گیرد.

یکی از روشهایی که می توان از آن به منظور ایجاد خودکار و نسبت دهی پسوردهای سنگین و پیچیده به هریک از اکانت ها استفاده کرد اجرای دستور کلی زیر در محیط داس است:

Net User Username / random

در اینجا Username اکانت یا حساب کاربری مدنظرمی باشد:



در مثال فوق که نام کاربری Gladiat0r انتخاب گردیده است ، پسوردهای تصادفی و پیچیده به حساب کاربری نسبت داده شده و در ادامه پسورد مورد نظر روی صفحه نمایش داده می شود. روش مذکور امکان مناسبی به منظور نسبت دهی پسورد در ارتباط با سروسی های حساب کاربری بوده و کمتر در ارتباط با کاربران واقعی استفاده می شود.

در ضمن برای افرادی که با روش جانشینی کاراکترها آشنا نیستند ، من این چند تا جانشینی رو اینجا آوردم شاید به درد بخوره:

1 <---> L , I , |

2 <---> Z , 7

3 <---> E

4 <---> a , A

5 <---> $, S

6 <---> G

7 <---> Z , 2

8 <---> B

9 <---> g

0 <---> o , O

این مقاله در اینجا به پایان رسید.

برای دریافت برنامه حذف کننده SYSKEY می توانید به وب سایت بنده مراجعه نمایید:

http://h4ck.rzb.ir

و اگر سوالی داشتید:

Dtr614140@Gmail.com

و اگر مایل به ارتباط مستقیم بودید:

+989373153178

متشکرم!

و اگر کمی و کاستی بود به بزرگواری خودتون ببخشید!

♣♣

معرفی سایت:

صفحه اصلی وبسایت هکرهای کلاه مشکی:

http://www.blackhat.com

کتابخانه مجازی هک و امنیت اطلاعات:

http://hacklib.sabablog.com

آژانس خبری هک و امنیت اطلاعات:

http://www.persianhack.com

گروه هکرهای لافت:

http://www.l0pht.com

▪▪

The End!