مدیریت پسورد (Password Management)

نویسنده : مهندس شهاب طرقیان (tareghian@parmisgs.com)

مقدمه :

در این مقاله با یکی از مباحث مدیریتی در شبکه به نام مدیریت پسورد آشنا می شویم ، که در ابتدا توضیحی در رابطه با بدست آوردن یک پسورد قوی را به شما آموزش می دهم و بعد از آن شما را با نحوه مدیریت نمودن پسورد خود و کاربران در شبکه آشنا می کنم .

همه ی ما تا به حال بارها اسم پسورد یا رمز عبور را در سایتهای مختلف شنیده ایم؛ و بارها نیز پسوردی را در این سایتها وارد کرده ایم . اما آیا از قدرت پسورد انتخابی خود خبر داشته ایم ؟

پسورد را می توان یک وسیله امنیتی دانست . برای مثال وقتی شما به سایت یاهو وارد مس شوید بعد از وارد کردن نام کاربری خود ، رمز عبور یا پسورد خود را وارد می کنید . اما آیا دوست دارید هرکسی بتواند پیام های شخصی شما را بخواند و به اطلاعات شما سری بزند به اصطلاح پسورد شما را به سادگی هک نماید ؟

مسلماً جواب شما به سوال منفی است . پس آیا تا به حال به این موضوع فکر کرده اید که قدرت پسورد شما چقدر است ؟

در اینجا روش ایجاد و پیدا کردن یک پسورد امن رو به شما می گویم .

ابتدا در یک دید کلی حروف ، اعداد و اشکال موجود در صفحه کلید خود را تقسیم بندی می کنیم :

۱. حروف بزرگ (Upper Case) : شامل تمام حروف بزرگ در صفحه کلید شما می شود . که می توانید برای استفاده از حروف بزرگ از حالت Caps Lock در صفحه کلید خود و یا با گرفتن Shift و زدن هر یک از حروف این کار را انجام دهید. مانند : A , H , Z , E

۲. حروف کوچک (Lower Case) : شامل تمام حروف کوچک در صفحه کلید شما می شود . در حالت عادی با زدن هر حرف در صفحه کلید می توانید حروف کوچک را مشاهده نمایید . مانند : a , h , z ,e

۴. اعداد (Digital) : شامل اعداد ۰ تا ۹ می شود .

۵. نمادها (Symbol) : شامل نمادها و سمبول ها می شود که مکان آن در صفحه کلید اعداد بالا به همراه گرفتن Shift می باشد . مانند : @ , # , & , * , $

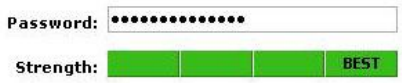
چگونه می توانیم یک پسورد قوی داشته باشیم ؟

اگر جزء دسته افرادی مبتدی باشیم برای انتخاب پسوردهای خود از اعداد یا حروف رایج استفاده خواهیم نمود تا به سادگی در ذهن خود آنها را حفظ کنیم (password,admin,1388,123,123456,0915) از جمله پسوردهایی هستند که معمولاً کاربران مبتدی از آنها استفاده می کنند که من به هیچ عنوان انتخاب اینگونه پسوردها را مناسب نمی دانم ، چون برای یک هکر اولین کار تست چنین پسوردهایی است و هیچ کدام از ما دوست ندارم اطلاعات خود را در دستان هکرها ببینیم و جلوگیری از اینکار تنها با انتخاب یک پسورد قوی صورت می گرد.
موارد مورد نیاز برای داشتن یک پسورد قوی را در زیر برای شما لیست کرده ام که توصیه من به شما رعایت تمام موارد زیر است :

۱. هیچگاه برای پسوردهای خود همان طور که در بالا نیز ذکر شد از تاریخ تولد، شماره موبایل و ... استفاده نکنیم .
۲. باید حتماً پسورد ما از ۱۰ کاراکتر بیشتر باشد .
۳. باید پسورد خود طبق قاعده ترکیب انتخاب نماییم .

قاعده ترکیب (Password Complex) : باید از ۵ مورد دسته بندی انجام شده در بالا حداقل ۳ مورد آن را در پسورد خود رعایت کنیم .
مانند : Gw1A*&4۱$۵
۴. سعی کنیم در پسورد انتخابی خود حداقل یکبار از Space استفاده نماییم .
۵. حتماً قدرت پسورد را در سایتهای مختلف که قدرت پسورد را به ما میدهند؛ تست کنیم .
مانند : www.microsoft.com/protect/yourself/password/checker.mspx
۶. هر ۳ ماه یکبار بنا به دفعات استفاده از پسورد خود آن را تغییر دهید .
۷. از نهگداری پسورد به صورت فایلهای متنی و Excel در کامپیوتر خود جداً خوداری کنید .
۸. به عنوان یک مدیر شبکه حتماً به کاربران خود امکان تغییر پسورد را بعد از ۳۰ روز بدهید و آنان را وادار به تغییر پسوردشان نمایید .

با رعایت موارد بالا شما یک پسورد فوق العاده قوی خواهید یافت که باید قدر آن را بدانید و آن را در اختیار هیچ کسی قرار ندهید.



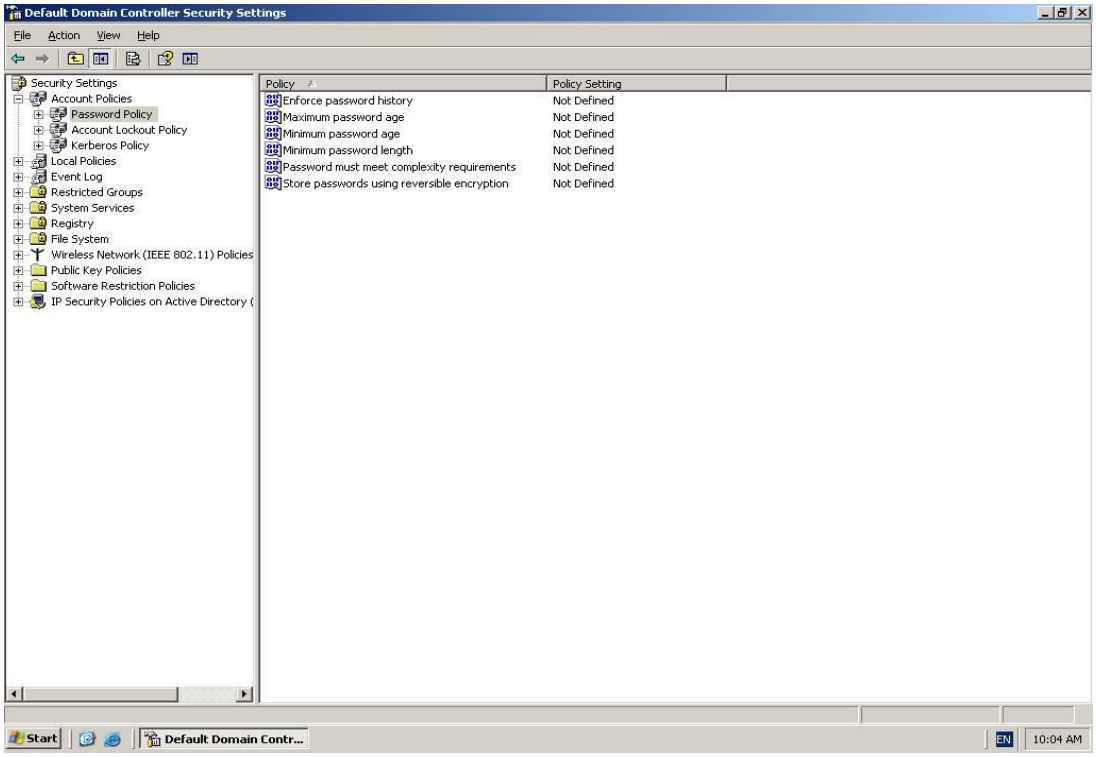
مدیریت پسورد در شبکه

مدیران شبکه های موفق کسانی هستند که با انجام و اعمال Policy (سیاست) های مناسب بتوانند شبکه خود را از لحاظ امنیت و نفوذ هکرها به آن ایمن نمایند . در این قسمت شما را با تنظیمات صحیح در Password Policy آشنا می کنم .

برای اعمال تنظیمات بر روی Password Policy مسیر زیر را دنبال نمایید تا لیست تنظیمات برای شما ظاهر شود :

Start ➔ Administrator Tools ➔ Domain Controller Security Policy ➔ Account Policies ➔ Password Policy

در صفحه باز شده مواردی برای اعمال Policy موجود است که هر یک را بررسی می نماییم .



۱- Enforce Password History : این قسمت یک تاریخچه ای از پسوردهای کاربران را در خود نگهداری می کند . این گزینه را فعال نماییم و در قسمت Password Remember عدد ۳ را وارد می کنیم ؛ حال اگر مدیر شبکه شما را مجبور به تغییر پسورد خود نماید آنگاه شما نمی توانید از ۳پسورد قبلی خود که قبلاً استفاده کردید ، مجدداً استفاده نمایید و باید پسورد جدیدی را انتخاب نماید . حال بعد از این ۳ بار شما می توانید از پسوردهای قبلی خود استفاده نمایید . شما می توانید بنا به سیاست خود این عدد را به هر عدد دلخواه تبدیل نمایید .

۲- Maximum Password Age : حداکثر فاصله ی زمانی مجاز که هر کاربر فرصت دارد رمز عبور خود را تغییر دهد چند روز است . اگر این گزینه را فعال نماییم و عدد مثلاً ۳۰ روز را در آن بنویسیم (پیش فرض آن ۴۲ روز است) یعنی کاربر بعد از اتمام ۳۰ روز حتماً باید پسورد خود را تغییر دهد . این Policy حالت باید دارد و اگر مقدار صفر را به آن بدهیم پسورد هیچ وقت Expire نمی شود . (از بین نمی رود)

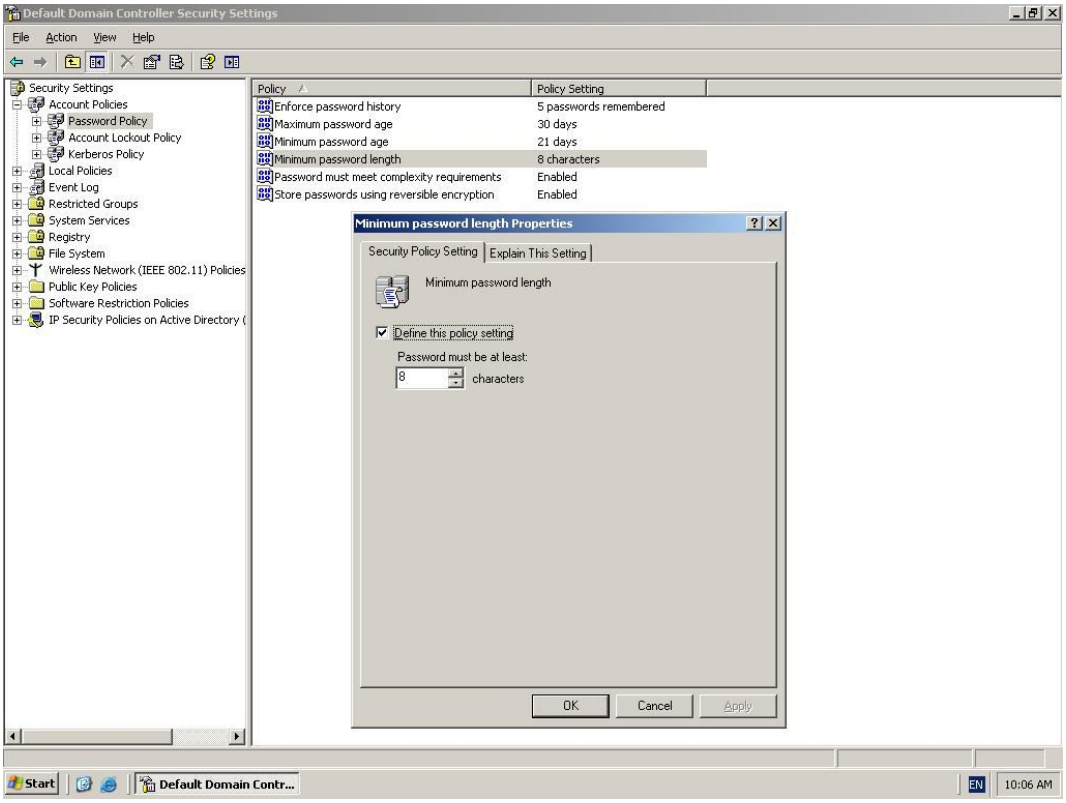
نکته : این Policy تقدم بالایی دارد مثلاً اگر به کاربری گفته شود که پسورد خود را تغییر دهد ، تا مدت زمانی که در این قسمت تعیین شده است ؛ به پایان نرسد نمی تواند پسورد خود را عوض نماید .

۳- Minimum Password Age : حداقل فاصله ی زمانی مجاز که هر کاربر فرصت دارد رمز عبور خود را تغییر دهد چند روز است . اگر این گزینه را فعال نماییم و عدد مثلاً ۲ روز را در آن بنویسیم (پیش فرض آن صفر روز است) زودتر از آن نمی توانیم پسورد را عوض کنیم اما بعد از آن قادر به تغییر پسورد خود هستیم . حالا می توانیم آن را عوض کنیم و می توانیم آن را عوض نکنیم . (حالت باید وجود ندارد)

نکته مهم : Minimum Password Age همیشه باید یکی کمتر از Maximum Password Age باشد .

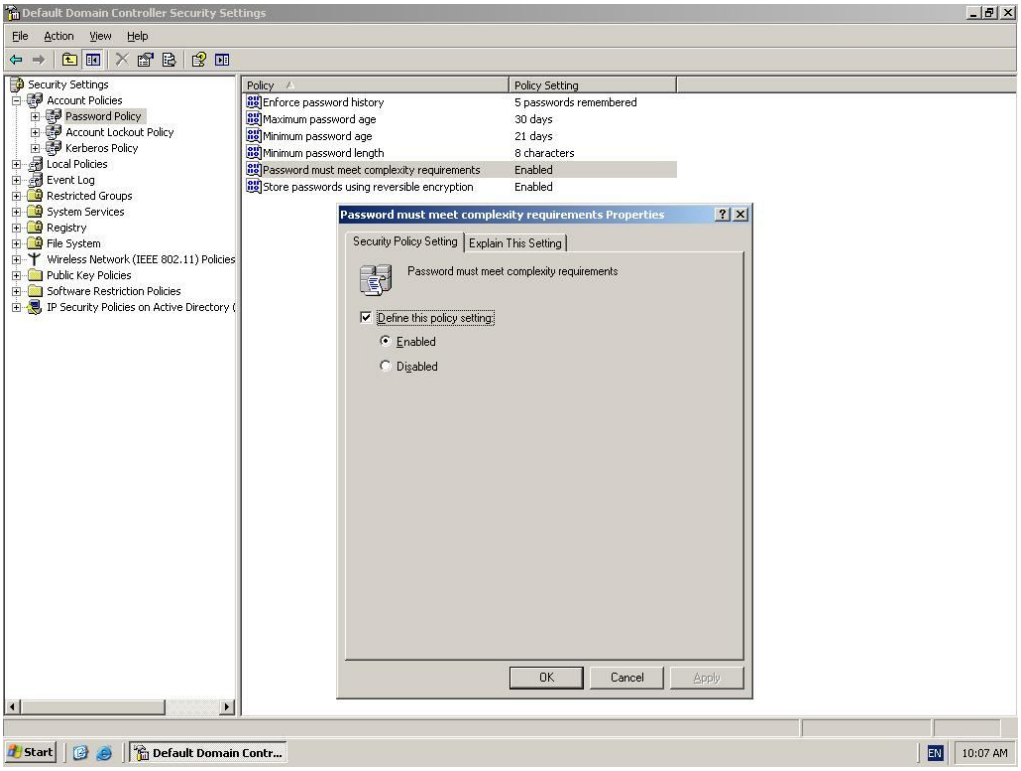
۴- Minimum Password Length : بیانگر این است که حداقل طول پسورد انتخابی چقدر باشد . مثلاً اگر عدد ۴ را در آن قرار دهیم کاربر باید پسوردی با بیشتر از ۴ کاراکتر را برای خود انتخاب نمایید ولی همان طور که در بالا توضیح داده شد سعی نمایید از قوانین بالا در انتخاب سیاست های مناسب استفاده نمایید .

نکته : هر چه طول پسورد بیشتر باشد امنیت بیشتری در شبکه حاکم خواهد بود .



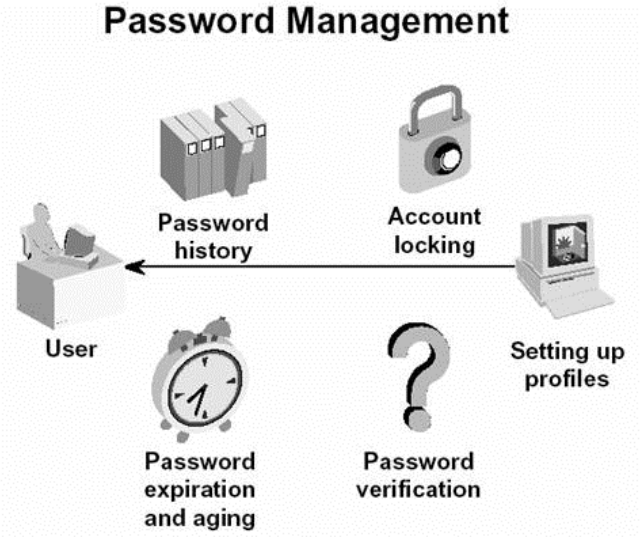
۵- Password Must Meet Complexity : این گزینه فوق العاده مهم است و اشاره به قانون ترکیب که در بالا توضیح داده شده است ، می کند . با فعال کردن آن کاربر باید پسوردی متشکل از ۳ نوع دسته بندی بالا را وارد نماید . توصیه من به شما این است که حتماً این گزینه را فعال نمایید .

نکته : برای فعال نمودن این گزینه توجه نمایید که گزینه طول پسورد عددی کمتر از ۳ نباشد چون آنگاه قانون ترکیب نقض خواهد شد و به شما نیز همچنین اجازه ای داده نمی شود .



۶- Store Password Using Reversible Encryption : اگر این گزینه را فعال نماییم برای تمـام سیسـتم عامل های دیگر غیر از ویندوز در شبکه نیز می توان پسورد انتخاب نمود .

هر یک از مواردی که در بالا اشاره شد بنا به سیاست های مدیر برای اداره شبکه خود قابـل تغییـر اسـت و بایسـتی بهترین حالت ها را انتخاب نمود تا شبکه ای ایمن تر از لحاظ مدیریت پسورد داشته باشیم .



مدیریت پسورد (Password Management)

ارایه شده توسط www.parmisgs.com– بهار ۹۰