

*روشهای حفاظت از کلمات عبور

نویسنده : وحید زارعی

حفاظت از کلمات عبور موجود در شبکه از مهمترین اصول حفظ امنیت یک شبکه میباشد. شما به عنوان یک مسئول حساس و دقیق شبکه باید با اجرای سیاستهای قوی و محکم از کلمات عبور محافظت نموده و مانع از فاش شدن آن شوید. مانند :

- ◀ سیستم عامل را طوری بیکرنیدی نمایید که کلمات عبور کوتاه تر از حد معین را اصلا قبول نکند (مثلا 9 کاراکتر).
- ◀ در صورت امکان قبل از پذیرش کلمه عبور از کاربر ، کلمه انتخابی در یک فرهنگ لغت جستجو شده و در صورت وجود پذیرفته نشود.
- ✓ کاربران مجبور باشند در کلمه عبور خود حداقل از 2 یا 3 کاراکتر غیر الفبایی استفاده نمایند.
- ◀ برای کلمات عبور طول عمر در نظر گرفته شود و سیستم عامل را طوری تنظیم نمایید تا پس از انقضای طول عمر کلمه عبور حساب کاربر قفل نموده و کاربر مجبور به تعویض کلمه عبور باشد و در آینده نیز نتواند به هیچ وجه از آن کلمه عبور استفاده نماید. توصیه میشود کلمات عبور طول عمر حدود 30 تا 90 روز داشته باشند و پس از آن کاربر مجبور به تعویض آن باشد. اگر مدت زمان انقضا بیش از حد کوتاه باشد ، کاربر مجبور به انتخاب کلمات با معنی برای جلوگیری از فراموشی خواهد شد که این به نوبه خود خطرناک میباشد.
- ◀ سیاستهای انتخابی کلمات عبور را بطور آشکار و شفاف در سایت وب خود به همه کاربران اعلام نمایید و حتی کاربران بیرونی سرویس دهنده های شما نیز در صورت وجود مجبور به رعایت این موارد باشند.

آگاهی کاربران:

با توجه به آنکه در محیطهای شلوغ و پرکاربر نمی توان تمام کلمات عبور انتخابی آنان را بررسی نمود و آنها نیز میتوانند به نحوی از قواعد تعیین شده شما به روشهای تصویری بگریزند، لذا سعی کنید با هشدارهای امنیتی و توضیح کافی، ذهن کاربر را با خطراتی که آنها را تهدید میکند، آشنا نمایید. بعنوان مثال ممکن است یک کاربر برای راحتی خود و همچنین برآورده کردن قواعد امنیتی شما کلمه عبور apple1234 را انتخاب نماید که خطرناک خواهد بود.

استفاده از برنامه های مولد کلمه عبور:

در هنگامی که کاربر میخواهد کلمه عبور انتخاب نماید، برای انتخاب یک کلمه عبور خوب و محکم، مردد خواهد ماند زیرا او به این می اندیشد که یک کلمه عبور سخت را چگونه میتوان به خاطر سپرد به گونه ای که نیاز به نوشتن آن روی کاغذ نباشد! آنها را به نحو مناسب راهنمایی کنید. پیدا کردن چنین کلمات عبوری چندان سخت هم نیست. مثلا آیا به نظر شما کلمه عبور "Jsrb,Ayhat7" بقدر کافی طولانی و مناسب نیست؟ به نظر میرسد که این کلمه عبور به اندازه کافی و محکم است و به خاطر سپردن آن هم چندان دشوار نیست چرا که این کلمه عبور حروف نخست جمله "Just sit right back , And you hear a tale" است. کاربر میتواند یک جمله مانند بالا در ذهن خود در نظر بگیرد و کلمه ای از آن بدست آورده و چند علامت و رقم به آن بیافزاید. فقط کاربران شما نباید از یک جمله نمادین مثلاً استفاده نمایند بلکه باید از آنها بخواهید تا متنوع فکر کنند!

میتوانید از برنامه هایی استفاده کنید که کلمه های عبور بی معنی به کاربر پیشنهاد میدهد ولی راه به خاطر سپردن آن را نیز آموزش میدهد.

برای فارسی زبانها این امر ساده است زیرا که اولاً فرهنگ لغت فارسی که به انگلیسی تایپ شده باشد وجود ندارد (فعلاً) ثانياً آنها میتوانند به یک بیت شعر یا ضرب المثل و یا جمله به یاد ماندنی فکر کنند و ابتدای کلمات آنرا به انگلیسی نوشته و کلمه عبور خود قرار دهند.

استفاده از نرم افزارهای غربال کننده کلمات عبور ضعیف:

باید به هر ترتیب مطمئن شوید که کاربران کلمات عبور ضعیف انتخاب نکرده اند. با توجه به اینکه شما قادر نخواهید بود تمام کلمات عبور و تغییراتی که کاربران میتوانند در کلمه عبور خود بدهند بررسی کنید، لذا به یک ابزار خودکار نرم افزاری نیاز خواهید داشت. این ابزار بر روی سرویس دهنده های شما که نیاز به کلمه عبور دارند نصب میشوند. سپس شما قواعد و سیاستهای امنیتی خود را با تنظیم گزینه های آنها تعیین مینمایید. از این به بعد بررسی کلمات عبوری که کاربران انتخاب میکنند به عهده این ابزارها خواهد بود. اینابزارها برای محیط یونیکس و ویندوز به رایگان قابل دسترسی است.

- ابزارهای یونیکس :

Npasswd که از آدرس ftp://ftp.cc.utexas.edu/pub/npasswd قابل تهیه است.
Passwd پلاس که از آدرس ftp://ftp.darthmouth.edu/pub/security قابل تهیه است.

- ابزارهای ویندوز:

PassProp این برنامه توسط مایکروسافت تهیه شده و در بسته قابل خریداری Win NT Server Resource Kit Supplement 4 موجود است.

PassFilt.dll این برنامه هم متعلق به مایکروسافت و در در دیسک فشرده Pack2 Service ویندوز 2000 موجود است.

Password Guardian این برنامه رایگان از آدرس http://www.geogiasoftware.com قابل تهیه است.

Strongpass يك برنامه رایگان قابل تهیه از : http://www.geogiasoftware.com

Fast Lane يك برنامه رایگان موجود در : http://www.fastlanetech.com

در صورت امکان از روشهای احراز هویت بدون استفاده از کلمات عبور استفاده کنید

بدلیل اینکه حتی با رعایت نکات ایمنی ممکن است ابزارهای شکننده کلمات عبور بتوانند يك کلمه عبور را کشف کنند، بهتر است در صورت حساسیت زیاد اطلاعات از مکانیسمهای پیچیده احراز هویت مانند Smart Card و سیستم های بیومتریک استفاده کنید.

ابزارهای شکننده کلمات عبور را گاهی علیه خود بکار ببرید:

برای اطمینان نهایی از عدم آسیب پذیری کلمات عبور، هر از چند گاهی ابزارهای شکننده کلمات عبور را اجرا کرده و بر علیه سیستم خود بکار ببرید. البته باید آنرا در محیطی امن و خارج از شبکه و روی يك سیستم مجزا بکار بگیرید تا شبکه شما دچار اختلال نشود.

ابزار **John** (يك شکننده کلمه عبور) ابزاری رایگان است که کد منبع آن نیز ارائه میشود. اگر به هیچ نرم افزاری از نظر امنیتی اطمینان ندارید میتوانید کدهای منبع آن را دریافت نموده و آنرا کامپایل و اجرا نمایید.

اگر شبکه شما بدلیل سهل انگاری مشتریان از کار بیافتد، آنها را از دست خواهید دادو شما هم به عنوان مسئول شبکه کارتان را! لذا به دقت آسیب پذیری کلمات عبور را بررسی نمایید و اگر پس از استفاده از ابزارهای فوق موفق به کشف يك کلمه عبور شدید، دقت کنید که چه چیزی باعث شده تا کاربر شما با نقض سیاستهای امنیتی کلمه عبور ضعیفی برای خود انتخاب نماید.

از فایل های حاوی کلمات عبور رمز شده بدقت محافظت کنید

آخرین و مهمترین راه حفاظت از کلمات عبور آنست که نگذارید بهیچوجه کسی فایل آنرا در اختیار بگیرد. اگر نفوذگر نتواند فایل محتوی کلمات عبور یا بانک اطلاعاتی SAM را در اختیار بگیرد، کشف کلمات عبور از طریق استراق سمع بسیار مشکل خواهد بود. لذا :

-وقتی در محیط ویندوز دیسک بازیابی (Recovery Disk) میسازید، آنرا در جای مطمئن نگهداری کنید.

-وقتی از سرویس دهنده های مهم خود نسخه پشتیبان میگیرید، مطمئن شوید که فقط در جایی ذخیره میشوند که فقط خودتان به آن دسترسی دارید.

-اگر در محیط یونیکس/لینوکس کار میکنید، مطمئن شوید که گزینه Shadow فعال است.

-اگر در محیط ویندوز کار میکنید از ابزار Syskey استفاده کنید تا قواعد سخت گیرانه تري را برابسیستم شما وضع کند.

-اگر مجبور نیستید در محیط ویندوز از workgroup پشتیبانی کنید و فقط از domain استفاده میکنید، روش احراز هویت LM را غیر فعال کنید چرا که روش ضعیفی محسوب میشود. روش این کار را میتوانید از آدرس

<http://www.microsoft.com/technet/support/kb.asp?id=147706>

◀ وقتی عمل پشتیبان گیری Backup از سیستمتان خاتمه یافت، به خاطر داشته باشید تا مجوز دسترسی به آنرا به گونه ای تنظیم نمایید که هیچ کس حق دسترسی به آنرا (بجز Admin) نداشته باشد.

اگر مطمئن شدید تمام موارد فوق را اجرا نموده اید، احتمال لو رفتن کلمات عبور در شبکه شما به حداقل رسیده است.

<http://www.denaboy.persianblog.ir>

وبلاگ کرانه گمنام

<http://www.et4ir.blogfa.com>

وبلاگ آموزش های کاربردی

<http://denaboy.parsaspace.com>

وبسایت فرزند دنا

مدیر سایت و وبلاگ ها : فرید نیک اقبالی