جمهوری اسلامی ایران
وزارت علوم، تحقیقات و فناوری

مدیریت حراست دانشگاه بیرجند

کلمات عبور

روش ساخت
و
نگهداری

سیدعلی خورشیدی

باسمه تعالی

کلمات عبور

روش ساخت و نگهداری

نگارش،تنظیم و طراحی جلد : سید علی خورشیدی، کارشناس حفاظت فناوری اطلاعات دانشگاه

ویراستاری : حسن زنگوئی، مدیرحراست دانشگاه

تاریخ انتشار : بهمن ماه ۱۳۹۷

سرشناسنامه : حفاظت فناوری اطلاعات .

عنوان و نام پدید آورنده : کلمات عبور- روش ساخت و نگهداری/سیدعلی خورشیدی .

مشخصات نشر : بیرجند، مدیریت حراست دانشگاه بیرجند، توزیع الکترونیکی، ۱۳۹۷ .

فهرست مطالب

مقدمه

پر واضح است که بدون در نظر گرفتن تمهیدات امنیتی در زمینه فناوری اطلاعات قطعا مشکلات جبران ناپذیری پیش خواهد آمد که جز اتلاف وقت و صرف هزینه های گزاف پیامدی نخواهد داشت؛ لذا و با عنایت به اینکه امروزه در مقوله امنیت فناوری اطلاعات، آموزش یک رکن اصلی به شمار آمده که با یاددآوری نکات مهم، منجر به آگاه شدن کاربران و جلوگیری از مشکلات آتی خواهد شد و برهمین اساس به عنوان یک مساله همگانی به بررسی امنیت کلمات عبور خواهیم پرداخت.

با آرزوی سلامتی و بهروزی

سیدعلی خورشیدی

کارشناس حفاظت فناوری اطلاعات دانشگاه

بهمن ماه ۹۷

کلمات عبور و حملات مرتبط با آن ها

ابتدا با یک توضیح بحث را آغاز می‌کنیم و آن این است که در این مختصر هرگاه از کلمه رمز، پسورد و یا کلمه عبور استفاده شود، همگی یک مفهوم دارند و همانی است که متصور هستید.

انتخاب یک کلمه عبور مناسب کار سختی نیست ولی آنچه که در عمل با آن روبرو هستیم کلمات عبور خیلی ساده هستند، شاید علت اصلی استفاده از کلمات عبور ساده همان مساله بخاطرسپاری آن ها باشد، این نقیصه بیشتر خود را در حمله های مهاجمان نشان می‌دهد. یکی از مشهورترین حمله‌هایی که به کاربران می‌شود، brute force attacks نام دارد؛ در این نوع حمله، مهاجمان لیستی از پراستفاده‌ترین پسورها و شناخته‌شده‌ترین آن‌ها را جمع‌آوری و امتحان می‌کنند. هرچه پسورد طولانی‌ترین داشته‌باشید، وقت بیشتری برای پیدا شدن آن نیاز است؛ هکرها نمی‌توانند هزینه زیاد شکستن پسوردهای طولانی را توجیه کنند، برای همین به سراغ اهداف بهتر می‌روند یعنی پسوردهای کوتاه‌تر.

یک پسورد ضعیف پسوردی است که توسط دیگران، چه یک فرد باشد، چه یک کامپیوتر، چه یک شبکه از کامپیوترها، به راحتی قابل حدس‌زدن باشد. حمله هایی که مرتبط با کلمات عبور و امنیت آن ها هستند به طور کلی به دسته های زیر تقسیم می‌شوند:

- حمله **Brute-force:** : امتحان‌کردن همه ترکیبات ممکن با کاراکتر و اعداد مختلف به فرم کلمه می باشد.
- حمله **Dictionary-based:** : استفاده از پسوردهای رایج مانند password123 یا ۱۲۳٤٥٦. هرساله لیستی از بدترین پسوردهای دنیا منتشر می‌شود و شاید تعجب کنید که تعداد آن ها بسیار زیاد است.
- حمله فیشینگ : فیشینگ به معنی فریب کاربر برای فاش‌کردن اطلاعات مهم خود است. این فریب‌ها اغلب در صفحات جعلی قرار داردند که در هنگام ورود، اطلاعات خود را تایپ

می‌کنید. در این صفحات، کاربر با کمال میل پسورد خود را تقدیم می کند؛ برای اجتناب از این نوع فریب، برروی لینک‌های مشکوک کلیک نکرده و به عنوان آدرس ها کاملا دقت کنید.

- مهندسی اجتماعی : ترفندی است که شما راقانع می کند اطلاعاتی را که هکر می خواهد در اختیار او قرار دهید. مثلا از جانب بانک با شما تماس می گیرند و با ارایه اطلاعاتی از شما به خودتان و با بهانه واریز مبلغ جایزه به حساب شما رمز کارت عابر بانک شما را اخذ می‌نمایند.

موازنه بین پیچیدگی و بخاطرسپاری

وقتی بحث از کلمه عبور مناسب می شود باید یک موازنه بین سخت بودن حدس زدن آن و آسان بودن بخاطرسپاری آن برقرار شود ولی ما معمولا کفه سادگی به خاطر سپاری را سنگین تر کرده و یک پسورد ساده خواهیم داشت به طور مثال شماره شناسنامه ام را همواره بخاطر دارم پس رمز برخی حساب هایم است، فرزند اولم را خیلی دوست دارم لذا پسور ویندوزم نام اوست، رمز عابر بانکم همان چهار رقم آخر شماره حسابم است و... . حتما این موارد در مورد شما هم صدق می کند؛ اگر می گویید که چنین نیست مهاجمان فضای سایبری روزی صحت آن را به شما ثابت خواهند کرد. در اینجا لازم است پاسخ به سوالاتی را ارائه دهیم:

سوال اول : امروزه آنقدر هکرها و ابزارهایشان پیشرفت کرده اند که هرگونه پسوردی را شکسته و یا دور می زنند پس چرا خود را برای بکاربردن پسورد سخت به دردسر بیندازیم؟

در پاسخ باید گفت درست است که هکرها و ابزارها پیشرفت کرده اند ولی کلمه عبور مناسب همچنان یکی از لایه های امنیتی است که می تواند هکرها را دچار مشکل و یا کلا مایوس کند؛ همچنین با استفاده از یک کلمه عبور ساده افراد خرابکار بی تجربه و کم سواد را نیز مستعد تبدیل شدن به یک هکر قدرتمند می‌نمایید.

سوال دوم : امروزه ابزارهایی برای مدیریت پسوردها ارایه شده اند که به راحتی می توان از آن ها استفاده کرد پس چرا این زحمت را خودمان متحمل شویم؟

این را از زبان کسی بشنوید که فارغ از شغل و مسئولیت خود شخصا و عقلا مایل نیست پسوردهایش را در اختیار یک نرم افزار (و همچنین به احتمال زیاد توسعه دهندگان آن نرم افزار) قرار دهد حتی اگر از جانب چند موسسه امنیتی بین المللی گواهینامه داشته باشد؛ حالا اختیار با خودتان است.

ابزارهایی برای مدیریت پسوردها وجود دارند مانند LastPass و ۱Password. این ابزارها پسوردهای شمارا در خود ذخیره می‌نمایند و تنها کاری که شما لازم است انجام دهید به خاطر نگه داشتن یک پسورد کلی (Master Password) برای دسترسی به پسوردهای ذخیره شده بر روی این سرویس‌ها است. برخی از این سرویس‌ها، از طریق یک افزونه با مرورگر شما و یا حتی تلفن همراهتان یکپارچه می‌شوند و هر بار که قصد ورود به حساب های کاربری مختلفتان را داشته باشید به صورت خودکار نام کاربری و رمز عبور را برای شما وارد می‌کند. این سرویس ها مانند دادن وکالت تام الاختیار به یک فرد دیگر خطرپذیر هستند.

ساختار مناسب کلمات عبور

برای یک کلمه عبور مناسب ویژگی هایی را بیان می کنند، که برخی از آن ها عبارتند از:

- **طول مناسب: هرچه طول کلمه عبور بیشتر باشد امن تر است. قبلا گفته می شد یک کلمه عبور مناسب حداقل ۸ کاراکتری باشد که به طول کلمه قابل قبول در سیستم عامل یونیکس نیز بستگی داشت ولی امروزه این مقدار کم است و طول کارکتری بیشتر از ۱۲ پیشنهاد می شود؛ به کلمات عبوری که بیش از ۲۰ کاراکتر طول داشته باشند عبارت عبور می‌گویند؛ بخاطر سپاری این عبارات راحت تر و پیدا کردن آن ها سخت تر است.**
- **یک کلمه عبور خوب باید ترکیبی باشد یعنی شامل حروف، اعداد و سایر علایم باشد و از حروف بزرگ و کوچک توام در آن استفاده شود.**
- **یک کلمه عبور خوب نباید در دیکشنری ها و فرهنگ های لغت وجود داشته باشد.**

- **کلمه عبور مناسب نباید همسان یا شبیه نام کاربری باشد. این مساله اغلب در تجهیزات کامپیوتری بطور پیش فرض وجود دارد و برخی کاربران ناآگاه آن را به حال خود رها می کنند مثلا نام کاربری و کلمه عبور مودم اینترنت خانه شما هر دو بطور پیش فرض کلمه admin است. خیلی اوقات نام کاربری شما در سامانه ها کد ملی شماست و پسورد پیش فرض نیز همان انتخاب شده است که بسیار در معرض خطر می باشد.**

ساختارهای نامناسب و در معرض خطر

- **کلمات عبور بسیار ساده مانند ۲٤٦۸،۱۲۳٤٥٦۷۸،۱۲۳،password و...**
- **استفاده از اعداد سری مانند ۰۰۰۰ ، ۱۱۱۱ ، ٤٤٤٤ و ... مخصوصا در مورد کارت های بانکی می‌تواند به صورت دستی نیز کشف گردد.**
- **شماره تلفن یا بخشی از آن، شماره پلاک خودرو، نام خویشاوندان و دوستان و تاریخ های خاص به راحتی قابل حدس و استفاده هستند.**
- **استفاده از کلمه عبور یکسان برای همه حساب های کاربری خطر حدس یا افشای کلمه عبور شما را چند برابر کرده و اشتباه بسیار مهلکی است. حتما شما هم برای انجام فعالیت‌های اینترنتی خود حساب‌های کاربری متفاوتی دارید، مهم‌ترین اشتباهی که بسیاری از کاربران اینترنتی مرتکب آن می‌شوند انتخاب یک رمز عبور یکسان برای تمامی حساب‌های کاربری است.این کار شاید مشکل به خاطر سپردن رمز عبور را برای شما آسان کند، اما تصور کنید که یک هکر در کمین شما باشد و از تمام حساب‌های کاربری شما هم مطلع باشد؛ پس با به دست آوردن اولین رمز عبور آن را روی تمام حساب‌های کاربری شما امتحان کرده و به این ترتیب، مشکلاتی حاد ایجاد می نماید.**

- **استفاده از حروفی که روی صفحه کلید پشت سرهم قرار دارند مانند qwertyui به عنوان پسورد به راحتی قابل کشف است.**

ویژگی‌های دو منظوره

مواردی که ذیلا مطرح می شود شاید در نگاه اول یک ایده خاص و یک تحول بزرگ برای پسوردهای شما به نظر برسد ولی قبلا توسط مهاجمین سایبری شناخته شده است، اگر بدون دقت از آن ها استفاده کنید به ضرر شماست؛ اما به خاطر داشته باشید که با استفاده از تکنیک ترکیب، تصادفی سازی و شخصی سازی می توانید با استفاده از آن ها پسورد مناسبی برای خود ایجاد کنید.

- **استفاده از یک رقم یا کاراکتر خاص در ابتدا و انتهای یک کلمه تقریبا هیچ فایده ای ندارد. مثلا پسورد khorshidi@ بجای khorshidi**
- **استفاده از معکوس کلمات معنی دار برای هکرها قابل حدس است، مثلا اگر نام کاربری شما admin است nimda را به عنوان پسورد انتخاب نکنید.**
- **جایگزین کردن حروف با ارقام یا علایمی که از نظر ظاهر شبیه هم هستند برای هکر ها و ابزارها شناخته شده است مثلا استفاده از ۱ بجای l و @ بجای a در کلمه عبور ali که می شود 1i@ یا استفاده از 0 بجای O در کلمه L0ve**

- **زدن کلید Caps Lock و استفاده از کلید Shift و یا استفاده از حروف ردیف های بالا و یا پایین حروف پسورد شما برای هکر قابل حدس است مثلا پسورد khorshidi را با استفاده از حروف بالای حروف مدنظر به صورت iy94wy8e8 وارد نمودن.**
- **استفاده یکی‌درمیان از دکمه شیفت؛ مثلاً رمزی مانند love می‌تواند تبدیل شود بهLoVe و برای مهاجمان شناخته شده است.**
- **تغییر زبان صفحه کلید و یا در نظر گرفتن حروف دیگر زبان ها نیز توسط هکر با انگیزه آزمایش می شود مثلا کلمه عبور خورشیدی از روی صفحه کلید انگلیسی به صورت o,vadnd می‌باشد؛ البته در این مورد حواستان باشد که ممکن است چیدمان صفحه کلید در همه‌ی کامپیوترها یکسان نباشد.**

بیشتر موارد بالا به این خاطر خطر پذیر هستند که تغییرات را روی عبارات قابل حدس برای مهاجم اعمال کرده ایم. روی نام خانوادگی، روی نام کاربری و... .دقت کنید که اگر روی یک عبارات مناسب این تغییرات را ایجاد کرده بودیم قضیه برعکس بود.

فرآیند خلاقانه ساخت یک کلمه عبورمناسب همراه با قابلیت بخاطرسپاری

در اینجا قصد داریم با استفاده از الگوهای ساده ای که قطعا برای هر نفر متفاوت می باشد یک شالوده پسوردی خوب بسازیم به گونه ای که برای تمامی سامانه ها قابل استفاده باشد و به راحتی بخاطر سپرده شود و یا در صورت فراموشی بتوانید به طریقی یادآوری نمایید.

نکته ای که روی آن تاکید داریم پسورد ها را روی کاغذ یادداشت نکنید فقط یک مورد وجود دارد آن هم پسورد خیلی پیچیده ای که زیاد با آن سروکار ندارید را می توانید در جای امنی مثلا گاوصندوق آن هم بطوری که مشخص نباشد مربوط به چیست، نگهداری نمایید.

نکته دوم اینکه هرگز از ویژگی Remember Password یا حفظ کلمه عبور در کامپیوتر استفاده نکنید. این کار باعث می‌شود که اگر زمانی فردی دیگر به غیر از شما به رایانه تان دسترسی پیدا کرد به راحتی

بتواند به فعالیت‌های اینترنتی شما دسترسی پیدا کند.کلمات عبور را در فایل یا هر سیستم کامپیوتری ذخیره نکنید.

روش زیر را دنبال کنید:

۱- یک عبارت یا بیت شعر که دوست دارید و زمزمه می کنید و ترجیحا خیلی رایج نیست انتخاب کنید: مثلا بیت شیر پسمانده کفتار نخورد با غرور و عظمت جان بسپرد را انتخاب کردیم و حروف اول کلمات را کنار هم می گذاریم shpknbghvajb

۲- در کلمه عبور خوب باید از حروف بزرگ و کوچک استفاده شود پس بطور دلخواه می خواهیم حرف دوم حروفی که در تبدیل فارسی به انگلیسی دو حرفی هستند را بزرگ تایپ کنیم پس خواهیم داشت: sHpknbgHvajb

۳- تاریخ، نام یا عددی را که دوست دارید و در خاطرتان می ماند به عبارت اضافه کنید: sHpknbgHvajb13970707

٤- در کلمه عبور خوب باید از علایم هم استفاده شود پس داریم sHpknbgHvajb!13970707

٥- این شالوده پسورد شماست حالا برای سامانه های مختلف به نحوی که فراموش نشود به اول یا انتهای آن عباراتی را اضافه نمایید. می توانید ویژگی های دو منظوره گفته شده در قبل را به صورت تصادفی و شخصی ترکیب کنید مثلا تصمیم داریم نام سامانه را با حروف فارسی در صفحه کلید انگلیسی به انتهای شالوده اضافه کنیم لذا برای دو مورد ذیل داریم:

- **پسورد سامانه فیش حقوقی:**sHpknbgHvajb!13970707+tda
- **پسورد سامانه احکام:**sHpknbgHvajb!13970707+php;hl

٦- روش های خود را ابداع کنید. سعی کنید از علایم خاص یا عبارات طبق مفهومشان استفاده ننمایید مثلا (my password for gmail=>mp4g) لازم است چند شالوده پسورد داشته باشید و کلمات عبور خود را به صورت دوره ای عوض کنید. بهتر است به کلمات عبور قبلی برنگردید؛ این همه کاری که می توانید انجام بدهید نیست ولی فعلا کفایت می کند، باید خلاقیت به خرج دهید.

تعیین میزان قدرت کلمات عبور

حال که شـــیوه حرفه‌ای رمزگذاری را یاد گرفتید بهتر اســـت تعیین میزان قدرت رمز مورد نظر خود را هم به‌طور حر فه‌ای بســـنجید. ســـا یت های اینترنتی ز یادی برای کار وجود دارد که یکی از آن ها www.passwordmeter.com اســـت. در این ســـایت و با تایپ رمز عبور مورد نظر، اطلاعات زیادی پس از تجزیه و تحلیل رمز عبور مورد نظرتان به شما داده می‌شود.

Test Your Password		Minimum Requirements
Password:	•••••••••••••••••••••••••	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	100%	
Complexity:	Very Strong	

Additions		Type	Rate	Count	Bonus
✪	Number of Characters	Flat	+(n*4)	25	+ 100
✪	Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 46
✪	Lowercase Letters	Cond/Incr	+((len-n)*2)	13	+ 24
✪	Numbers	Cond	+(n*4)	8	+ 32
✪	Symbols	Flat	+(n*6)	2	+ 12
✪	Middle Numbers or Symbols	Flat	+(n*2)	10	+ 20
✪	Requirements	Flat	+(n*2)	5	+ 10
Deductions					


امام سید
علی