Password Security 101

pentestlab.blog/category/external-submissions/page/3

April 1, 2012

We understand that most of our clients are **business-oriented** and not **security-focused**, and so many don't realize the **true implications of a password compromise**. For example, a client recently asked us to reset a password for one of their user's email accounts and provided us with a very weak password to use (in fact, the username was the same as the password). After we explained how that new password would be easy for someone to guess they replied, "*Oh it doesn't really matter if someone breaks into this email account it's not used for anything important*".

A compromise of the email messages themselves is only one aspect. In most cases the reason email accounts are compromised is so that they can be used to **send out spam**. Imagine hundreds of thousands of spam emails being sent out from one of your email addresses. Not only can this affect your company's reputation, but your mail server will likely get blacklisted which means important emails may not get received. Resolving blacklist issues can take time to resolve leaving your entire company's email crippled for days. But the impact of blacklisting doesn't only affect your users and domain, if you're hosted on a shared mail server then all of the domains hosted on the same email server become blacklisted.

Weak passwords can easily lead to a compromise of any service – **ftp, control panel, database, email** – as well as non-hosting related accounts such as **facebook** and your **bank account**, and each can have their own dire consequences.

What is a Weak (bad) Password?

Examples of bad passwords are those that:

- contain a **dictionary word**, your **username**, **company name**, name or other identifying information (such as your **pet or child's name**) – even if you add numbers or other characters after the word.
- are **too short** (under 8 characters)

- are **commonly used passwords** based on statistics of hundreds of thousands of passwords (password is not a good password, 123456 is also not a good password), but here’s 500 horrible passwords that are insanely popular as passwords and thus easily guessed: **please note this image contains foul language, so we do not recommend viewing it if you may be offended.*

(image credits: http://www.forevergeek.com/2010/07/500_worst_passwords)

Most people will find that they have used passwords in the above lists. Note that attackers have lists that contain hundreds of thousands of passwords and use tools to test various combinations of passwords (such as adding numbers at the end of a word)

How do I choose a Strong Password?

There are many methods but here are some recommendations:

- **Use a random password generator** – PC Tools has a really easy to use password generator at http://www.pctools.com/guides/password/
- **Create a password from your favorite song** – create a password from your favorite song lyric such as the first letter of each word, and mix in some other characters to strengthen the password. For example, “***Twinkle, Twinkle Little Star, How I wonder what you are***” could be: **TtL*HIwwya5.**

Finally, **it’s important to not use the exact same password for all your online services**. Even if you have a very strong password – if the password is leaked due to a compromise of a service you use (social networking sites, online forums, etc) – attackers may try your password on other web sites to see if they can access your other accounts using the same password (banks, shopping sites where your password may be stored such as amazon.com, and other sites or services)

HELP! How will I ever remember my new Passwords?

The easiest way to manage your passwords security is by using a password storage application that runs on your computer and ideally also on your mobile devices so you can access your passwords from anywhere.

It’s important to choose a password application that encrypts your passwords so if your PC or phone is stolen they would not be able to see your stored passwords.

With a password application, you typically would **only need to remember one password**, and that master password unlocks the application so you get access to all your saved passwords.

LastPass (https://lastpass.com) is a great option as it can sync your passwords across many computers and even devices (iPad, iPhone, Android), and it also has a built-in password generator. LastPass also has other useful features such as the ability to create secure notes, and securely save personal information so you can easily fill out online forms (including your credit card number if you wish).

We hope this information has been helpful and highly advise all users to review all the passwords you currently have in place and find a password strategy that works best for you and your organization.

Nathalie Vaiser, CEH, MCP, MCTS, Linux+

Nathalie’s personal blog: http://admingal.com

Nathalie is the Virtualization Program Manager for Applied Innovations, a leading Windows web hosting provider at http://appliedi.net