Configuración de sistemas de control de acceso y autenticación de personas (Bastionado de redes y sistemas)

Mecanismos de autenticación. Tipos de factores

Utilizar contraseñas es un método para autenticarse, pero no es el único, hay otros métodos como, por ejemplo, el uso de tarjetas inteligentes que tiene la identidad grabada.

Las contraseñas deben satisfacer unos requisitos de complejidad, con los siguientes ejemplos tenemos algunos requisitos que deberían cumplir:

- La contraseña tiene una longitud correcta.
- La contraseña no aparece en los buscadores.
- La contraseña no debe aparecer en un diccionario.
- La contraseña no tiene un hash que aparece en los buscadores.

Ejercicios

- https://www.jesusninoc.com/01/24/ejercicios-de-powershell-como-hacer-un-login-paso-a-paso-utilizando-hash-en-powershell-utilizando-funciones-avanzadas/
- https://www.jesusninoc.com/02/17/ejercicios-de-seguridad-hacer-un-login-en-el-que-el-password-esta-almacenado-

en-sha512-en-un-fichero-y-el-nombre-del-usuario-tambien-esta-almacenado/

Más información

- https://www.jesusninoc.com/08/28/programacion-de-documentos-web-utilizando-lenguajes-de-script-de-servidor-implantacion-de-aplicaciones-web/#Autenticacion_de_usuarios
- https://www.jesusninoc.com/07/22/administracion-de-servidores-de-aplicaciones-despliegue-de-aplicaciones-web/#Autenticacion_de_usuarios_Dominios_de_seguridad_para_la_autenticacion

---

Aparte de usuario y contraseña, actualmente una gran mayoría de sitios ya ofrecen la llamada «autenticación de doble factor» (textos sacados de INCIBE).

Podríamos definirla como el proceso de seguridad por el cual un usuario debe confirmar su identidad de al menos 2 maneras diferentes. Este método de identificación segura se basa en autenticar a una persona por varios métodos que pueden ser usados simultáneamente:

- Algo que sabes (Contraseña, pin…)
- Algo que tienes (Generador de claves, tarjeta de coordenadas…)
- Algo que seas (huella dactilar, reconocimiento facial, etc…)
- A medida que añadimos capas, mejoramos la seguridad, haciendo que sea más difícil para un atacante hacerse con información sensible. Hablamos de la autenticación de múltiples factores.

Existe una confusión frecuente entre la autenticación de doble

factor y la verificación en dos pasos. La gran diferencia es que, por lo general, en la verificación en 2 pasos se envía un código de seguridad por SMS que puede ser interceptado. El mensaje SMS no cumple los requisitos de seguridad de la autenticación de doble factor, ya que no es ni algo que el usuario sabe, ni algo que tiene, ni algo que es, sino algo que envían.

Más información

- https://www.jesusninoc.com/01/10/curso-de-hacking-con-powershell-contenido/

Autenticación basada en distintas técnicas

Existen diferentes formas de llevar a cabo la autenticación de doble factor, algunas de las más usuales pueden ser:

- Uso de memorias autenticadoras USB, apps generadoras de códigos de seguridad temporales.
- Datos concretos que solo conozcamos nosotros, como el PIN o la respuesta a pregunta de seguridad.
- Medidas biométricas, como el uso de huella dactilar, reconocimiento facial, de voz, etc…