Administración de credenciales de acceso a sistemas informáticos (Bastionado de redes y sistemas)

Gestión de credenciales

La cuenta de usuario consiste en un nombre de usuario y una contraseña (password), en algunos sistemas operativos estos dos elementos forman un conjunto de credenciales y sirven para identificar a una persona.

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.

Ejemplos

- https://www.jesusninoc.com/09/20/almacenar-y-utilizar-credenciales/
- https://www.jesusninoc.com/08/17/utilizar-credenciales-almacenados/
- https://www.jesusninoc.com/03/01/ejercicios-de-powershell-almacenar-varios-credenciales-en-un-fichero-xml-y-utilizarlos-para-arrancar-un-proceso/
- https://www.jesusninoc.com/04/08/almacenar-y-utilizar-credenciales-mediante-json/
- https://www.jesusninoc.com/02/27/validar-credenciales-de-usuario-en-el-propio-ordenador-desde-powershell/

- https://www.jesusninoc.com/02/19/ejercicios-de-powershell-enviar-credenciales-entre-un-cliente-y-un-servidor-por-udp-y-ejecutar-una-aplicacion-en-el-servidor-con-dichos-credenciales/

Ejercicios

- https://www.jesusninoc.com/04/14/enviar-credenciales-get-credential-mediante-el-protocolo-udp-entre-un-cliente-y-un-servidor/

Infraestructuras de Clave Pública (*PKI*)

La criptografía de clave pública fue inventada en 1975 por Whitfield Diffie y Matin Hellman. Se basa en emplear un par de claves distintas, una pública y otra privada. La idea fundamental es que las claves están ligadas matemáticamente pero es computacionalmente imposible obtener una a partir de la otra.

Este tipo de algoritmos tienen dos aplicaciones fundamentales:

1. **Encriptación**. Si un usuario A quiere mandar un mensaje a otro usuario B, lo encripta usando la clave pública de B. Cuando B lo recibe lo desencripta usando su clave privada. Si alguien intercepta el mensaje no puede descifrarlo, ya que no conoce la clave privada de B (de hecho, ni tan siquiera A es capaz de desencriptar el mensaje).
2. **Firmas digitales**. Si B encripta un mensaje usando su clave privada cualquiera que tenga su clave pública podrá obtener el texto en claro correspondiente; si

alguien quiere hacerse pasar por B tendrá que cifrar el mensaje usando la misma clave privada o no se descifrará correctamente con la clave pública de B. Lo que B ha hecho es firmar digitalmente el mensaje. El proceso de desencriptar con una clave pública un mensaje firmado se denomina verificación de firma.

El problema fundamental de este tipo de algoritmos es la distribución de las claves; aunque la clave pública se puede distribuir libremente (A la puede enviar por correo o decírsela a B por teléfono), nos queda el problema de la suplantación (C le puede dar su clave pública a B haciéndose pasar por A). Para solventar estos problemas se emplean autoridades certificadoras y certificados digitales.

Acceso por medio de Firma electrónica

La firma electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

- Identificar al firmante de manera inequívoca.
- Asegurar la integridad del documento firmado. Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación.
- Asegurar el no repudio del documento firmado. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento.

La base legal de la Firma electrónica está recogida en la Ley 59/2003 de Firma Electrónica y se desarrolla en más profundidad en la sección Base legal de las Firmas. La sección también explora, bajo qué circunstancias la ley equipara la firma electrónica a la firma manuscrita, añade notas respecto a la normativa europea y hace distintas

Gestión de accesos. Sistemas NAC (*Network Access Control*, Sistemas de Gestión de Acceso a la Red)

Control de acceso a red es un enfoque de la seguridad en redes de ordenadores que intenta unificar la tecnología de seguridad en los equipos finales, usuario o sistema de autenticación y reforzar la seguridad de acceso a la red.

Gestión de cuentas privilegiadas

Los usuarios tienen distintos privilegios y restricciones, el usuario que más privilegios tiene es el administrador. Hay que tener en cuenta que iniciar sesión con credenciales de administrador puede suponer un riesgo para la seguridad del sistema operativo y de la red (en el caso de que el ordenador forme parte).

El riesgo se debe a que los usuarios administradores pueden realizar cualquier tipo de cambio en el sistema y puede darse el caso de que el administrador ejecute un programa dañino para el sistema como, por ejemplo, un virus, por este motivo, es recomendable iniciar sesión con usuarios no administradores.

Existen grupos para englobar cuentas, la pertenencia a un grupo supone para el usuario tener los permisos y la capacidad de realizar diversas tareas en el equipo local.

Más información

- https://www.jesusninoc.com/07/08/8-gestion-de-usuarios-en-powershell/#Ejecutar_como

Protocolos *RADIUS* y *TACACS*, servicio *KERBEROS*, entre otros

Algunos protocolos de autenticación son:

- **RADIUS** es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.
- **TACACS**. Es un protocolo de autenticación remota privativo de Cisco, comúnmente usado en redes Unix, que se usa para comunicarse con un servidor de autenticación. TACACS permite a un servidor de acceso remoto comunicarse con un servidor de autenticación para determinar si el usuario tiene acceso a la red.
- **Kerberos** es un protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura.

Más información

- https://www.jesusninoc.com/04/20/usuario-actual/
