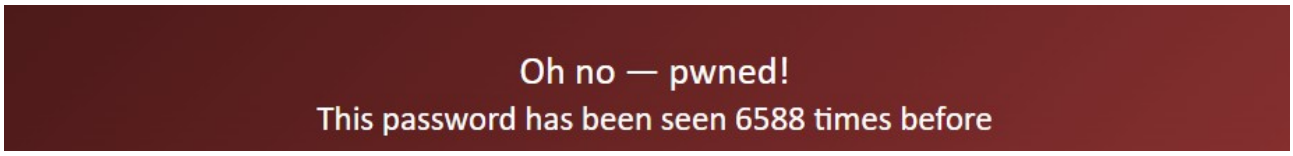
| Unidad didáctica 03. *Introducción a los sistemas en red* | | Módulo*: Sistemas informáticos* |
|---|---|---|
| Tarea 5. *Seguridad básica* | | |
| Nombre: | Apellido1: | Apellido2: |

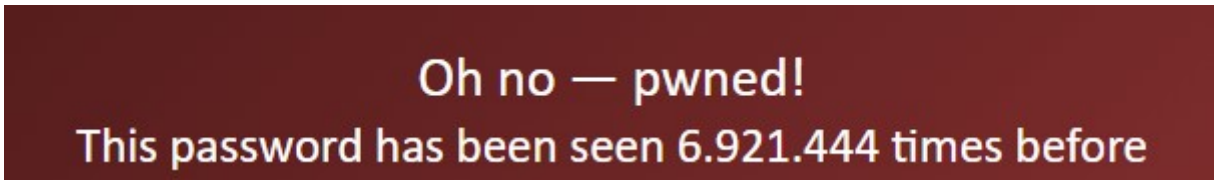
1) Para las siguientes contraseñas indica el número de veces que aparecieron en filtraciones de datos (utiliza https://haveibeenpwned.com/Passwords) y el tiempo estimado en descifrarlas de acuerdo a la web vista en clase (puedes usar otra si prefieres, pero indica cual usaste):

- 15061989




Fuente 1 → 2 milisegundos.
Fuente 2 → 10 milisegundos.

- 12345678




Fuente 1 → Ni aparece tiempo, la respuesta es instantáneamente.
Fuente 2 → Nada, avisa del peligro y recomienda cambio inmediato.

- Admin


Fuente 1 → 9 milisegundos.
Fuente 2 → Para este comprobador tambien es instantanea.

**IES de Teis**
Avda. de Galicia, 101
36216 – Vigo
Tfno: 886 12 04 64
e-mail: ies.teis@edu.xunta.es
http://www.iesteis.es


- ¡W0lfr4M?#Ia


Fuente 1 → 1 millardo de años.
Fuente 2 → 7 billones de años (miles de millones)

Fuentes:
- Seguridad contraseña 1
- Seguridad contraseña 2

2) ¿Qué son Microsoft Authenticator o Google Authenticator? ¿Existen diferencias entre ambos productos?

Tanto *Microsoft Authenticator* como *Google Authenticator* son aplicaciones para verificar tus cuentas en dos pasos. Es decir necesitarás los credenciales de acceso y tener el dispositivo a mano para poder corroborar con él que el inicio de sesión es legítimo.

En la alternativa de *Microsoft* nos permite usar verificaciones biométricas o PIN, mediante un código generado. Siempre que las cuentas admitan verificación en dos pasos.

La solución de *Google* genera códigos para comprobar la veracidad del inicio de sesión y nos pedirá un código temporal de 6 dígitos.

La opción de *Microsoft* parece más completa a primera vista puesto que nos da mas opciones que *Google*, que solo nos permite iniciar sesión con las claves de 6 dígitos alfanumericas.

Fuentes:
- Microsoft Authenticator
- Google Authenticator


XUNTA DE GALICIA
Financiado pola Unión Europea NextGenerationEU | Unión Europea Fondo Social Europeo
GOBIERNO DE ESPAÑA MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
Plan de Recuperación, Transformación y Resiliencia
Xacobeo 21·22

3) Busca información sobre gestores de contraseñas, escoge uno y explica sus ventajas e inconvenientes. ¿Qué pasaría si pierdo la contraseña maestra?

Uno de los gestores de contraseñas más popular y usado, sobre todo en ecosistema Apple, es ***1Password*** . Sus ventajas son que funciona en toda clase de dispositivos y sistemas operativos (PC, móviles, Android, Windows, MACOs, Linux), tiene una clave maestra para su cifrado, verificacion en dos pasos, rellenar contraseñas y cuestionarios, desbloqueo biométrico.

Su mayor desventaja es el precio, bastante más caro que otras alternativas. No tenemos versión gratuita. Tiene planes personales y familiares.

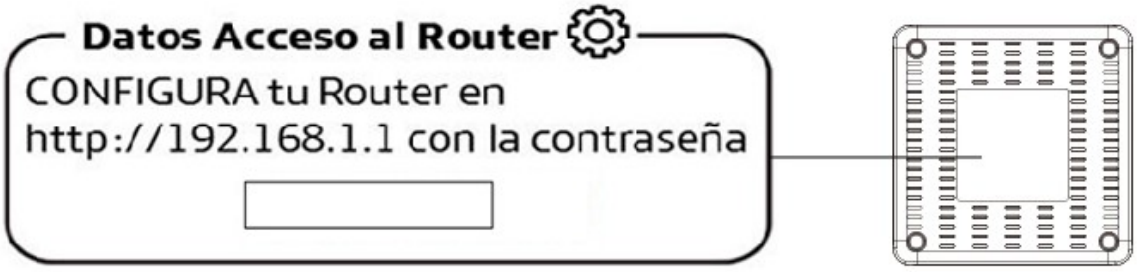
Por poner alguna desventaja a este tipo de software, en última instancia estamos cediendo nuestros credenciales a un tercero. Que es susceptible a hackeos y filtraciones como ya ocurrió en el hackeo a LastPass además si perdemos los credenciales de este gestor de contraseñas perderemos el acceso a todas las sesiones gestionadas por él.

Fuente:

- Comparativa Gestores contraseñas
- Explicaciones rápidas Gestores Contraseña
- 1Password

4) Hemos hablado de que muchos dispositivos utilizan contraseñas por defecto para acceder a su interfaz web de gestión. Busca cual es la contraseña de acceso por defecto al router del proveedor de internet que tengas contratado. Indica qué hiciste y cuánto tiempo tardaste.

Si tenemos acceso a nuestro dispositivo suele tener la IP que debemos escribir en el navegador para acceder y la clave de acceso. Mi router tiene una contraseña por defecto generada de forma aleatoria por el fabricante.




En ocasiones suelen tener claves por defectos como por ejemplo:

Credenciales
Usuario →user
Clave → user
Usuario →admin
Clave → admin
Usuario →Admin

Clave → 1234

Estos son ejemplos de contraseñas usadas por algunos equipos para poder acceder a ellos y configurarlos, siempre es recomendable cambiar la contraseña por defecto que traigan los dispositivos.

Fuentes:

- Recopilatorio de contraseñas por defecto

5) En las actualizaciones de seguridad en los portales de ejemplo vistas en clase, referencian un enlace a algo llamado CVE-YYYY-NNNN (donde YYYY es un año y NNNN cuatro dígitos). ¿Qué es? ¿Cuál es el proceso para crear un CVE?

Estos cuatro digitos hacen referencia al identificador de la vulnerabilidad que es un numero único. Desde 2014 puede contener más de 4 digitos si es necesario.

El proceso de crear una nueva entrada, un nuevo *CVE* consta de 3 partes:

1. Etapa de presentación inicial y tratamiento.
2. Etapa de candidatura, donde se asigna el *CVE-ID*, que puede realizarse de 3 formas.
    1. Una asignación directa por parte del *CVE Content Team.*
    2. Una asignación directa por parte del *CVE Editor* al ser difundida una vulnerabilidad crítica. Si no lo asume el fabricante, es la organización la que asigna directamente un ID a al vulnerabilidad.
    3. Una reserva de un identificador *CVE-ID.* Normalmente los fabricantes reservan un lote de ID para asignar a posibles fallas de sus productos que aparezcan durante su vida útil.
3. Etapa de publicación en la lista si la candidatura es aceptada. Puede prolongarse en el tiempo

Es raro ver que se publiquen vulnerabilidades "*Zero-Day"* por este motivo.

Fuentes:

- Formato Vulnerabilidades

6) Estás trabajando como desarrollador en una empresa que tiene instancias de la versión 8.1.5 de Prestashop, localiza si existe alguna vulnerabilidad para la misma. En caso de ser así, indica el CVE de la misma y su categoría, pon un enlace a la información sobre la vulnerabilidad o vulnerabilidades.

Podemos encontrar la vulnerabilidad con ***CVE-2024-34717*** que fue corregida en la siguiente versión la 8.1.6

En el repositorio de github podemos ver que aparecen dos vulnerabilidades corregidas una de tipo XSS Cross-Site-Scripting. La vulnerabilidad es de tipo *"Revelacion de información".*

Fuentes:

- Vulnerabilidades corregidas en la versión 8.1.6
- Vulnerabilidad CVE-2024-34717
- INCIBE (CVE-2024-34717)
- Ataque tipo XSS
- Ataque cadenas de consulta URL

7) ¿Qué fue Stuxnet? ¿Qué fue LogoFAIL? (Explícalos de manera resumida)

***Stuxnet*** es un virus informático que puede cambiar programaciones de controladores lógicos programables y pasar desapercibido. A través de *rootkit* realiza modificaciones en el programa sin ser detectado. Es el primer gusano conocido que incluye un *rootkit* para equipos PLC. *Siemens* ha puesto una herramienta de deteccion y eleminación de este gusano, además recomienda el contacto inemdiato con el soporte tecnico de la marca, actualizar los parches de *Microsoft* y evitar el uso de USB ajenos o no controlados.

Durante el arranque de un PC se comprueba que todos las partes funcionen de forma correcta *POST* normalmente después de esto se muestra el logo de la marca de la placa base mientras carga el sistema opertativo, algunos ciberdelincuentes cargaban en esa imagen software malicioso para que se ejecutara en el arranque.

Fuentes:

- Stuxnet
- LogoFAIL CVE-2023-40238

8) ¿Qué es un CPD? ¿Qué medidas de seguridad debe implementar y por qué?

*CPD (Centro de Procesamiento de Datos)* o *Data Center* en Inglés es un espacio (Sala/Edificio) que contiene la información necesaria para que una empresa u organización funcione correctamente. Suele verse en organizaciones de tamaño medio o grande.

La seguridad de un datacenter tiene dos grandes ramas, la seguridad física y la seguridad lógica. Además de tener una infraestructura adecuada al tipo de *Data Center* . En funcion del tipo los organismos reguladores piden una serie de requisitos como puede ser que tengan un SAI para no para ante una falta de suministro, que la refrigeración este doblada o doblar equipos para que si uno de ellos falla los datos sigan siendo accesibles y las aplicaciones que dependan de ellos no se vean comprometidas.

- **Seguridad Física.**
  - Control de acceso.
  - *Anti-tailing* (seguimiento de un persona).
  - Gestión de identidad.
  - Video vigilancia 24/7.
  - Alarmas.
  - Protección contra incendios.
  - Ubicación estratégica.
  - Soluciones anti-sísmicas.
  - Climatización.

- **Seguridad Lógica.**
  - Segmentación de riesgos.
  - Segmentación de redes.
  - *Firewalls* físicos y virtuales.
  - Sistemas de prevención de intrusos *IPS.*
  - Adecuación de permisos.
  - Controles integrales de seguridad.
  - Gestión de accesos privilegiados.
  - Soluciones de prevención de perdida de datos *DLP.*
  - Plan de recuperación de desastres *DRP.*
  - Correlación de eventos *SIEM.* (Detectar patrones y tendencias no habituales)

Fuentes:

- Centro de Procesamiento de Datos
- Organizacion que regula las normas de seguridad de los CPD 1
- Organizacion que regula las normas de seguridad de los CPD 2
- Seguridad Lógica Física de un DC
- Tailgating, Qué es ?
- SIEM, Security Information and Event Manager. Qué es?

Imágen del DC Marenostrum en Barcelona y un esquema de los componentes y su disposición.