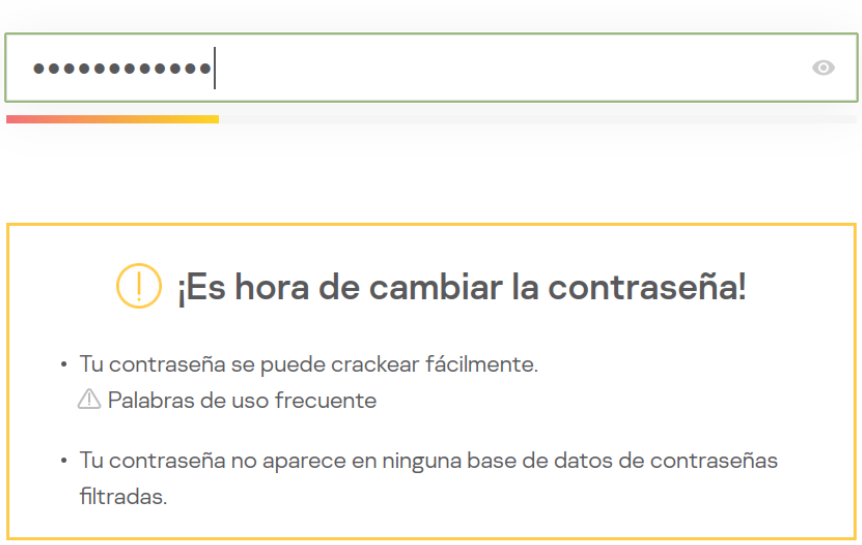
Seguridad informática | Tarea 1.2

Fecha de realización: 13 - 10 - 22

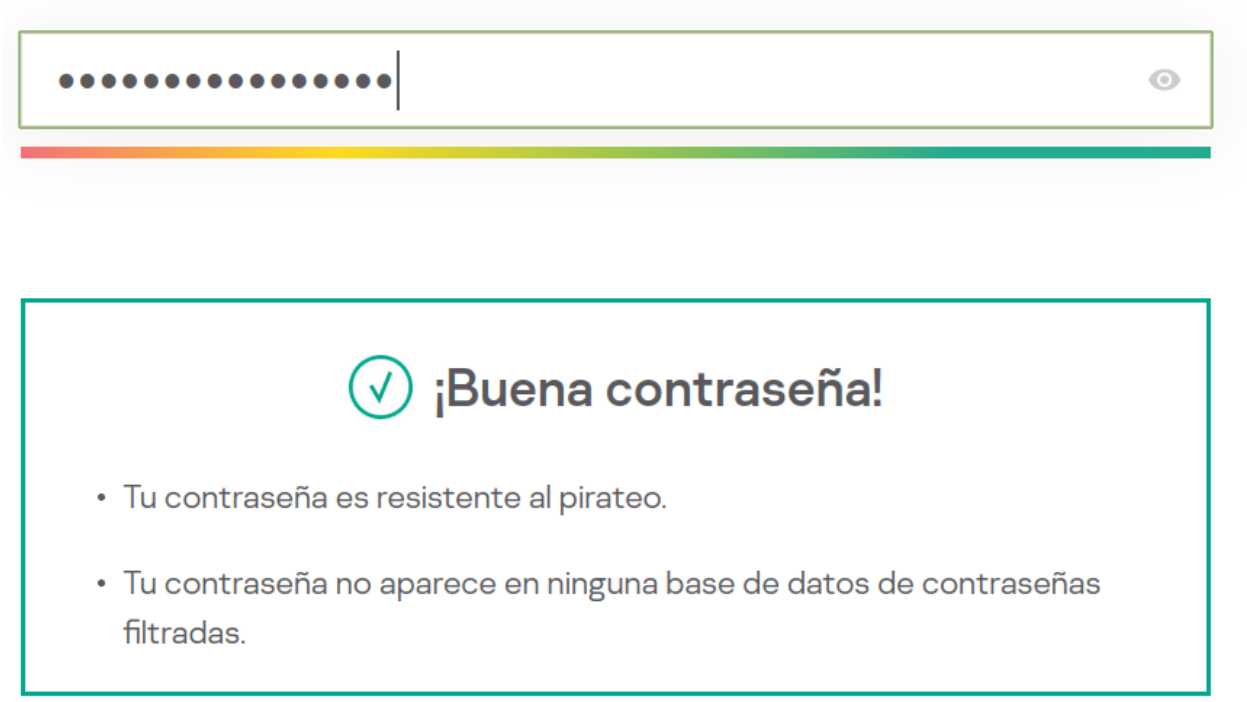
Indice

1. Comprobar con alguna aplicación la fortaleza de tus contraseñas más habituales: Por ejemplo en: https://password.kaspersky.com/es.

He probado a poner la contraseña que tiene mi madre en sus cuentas, y como podemos comprobar en las siguientes imágenes, es una mala contraseña:



Ahora voy a comprobar la mía, mi contraseña tiene aproximadamente 16 carácteres y varios signos, vamos a ver si es segura a continuación:



2. Imagina que la empresa en la que eres responsable de seguridad sufre un ataque a través del servidor Web utilizando una vulnerabilidad conocida. ¿Qué medidas tomarías?

Primero analizaría cuál ha sido la vulnerabilidad y si ha sido grave el ataque, a continuación haría una copia de seguridad de los datos más importantes de nuestro servidor. Más tarde, cerraría los puertos del servidor, añadiría actualizaciones para esas vulnerabilidades y una vez hecho todo, reiniciaría el servidor..

3. Busca algún Boletín de seguridad de Microsoft alguna vulnerabilidad: descríbela, di cuál es su clasificación y que medidas tomarías.

Boletín mensual de Microsoft - octubre 2022

Fecha de publicación: 13/10/2022
Importancia: 5 - Crítica

Recursos afectados:

- Active Directory Domain Services,
- Azure,
- Azure Arc,
- Client Server Run-time Subsystem (CSRSS),
- Microsoft Edge (Chromium-based),
- Microsoft Graphics Component,
- Microsoft Office,
- Microsoft Office SharePoint,
- Microsoft Office Word,
- Microsoft WDAC OLE DB provider for SQL,
- NuGet Client,
- Remote Access Service Point-to-Point Tunneling Protocol,
- Role: Windows Hyper-V,
- Service Fabric,
- Visual Studio Code,
- Windows Active Directory Certificate Services,
- Windows ALPC,
- Windows CD-ROM Driver,
- Windows COM+ Event System Service,
- Windows Connected User Experiences and Telemetry,
- Windows CryptoAPI,
- Windows Defender,
- Windows DHCP Client,
- Windows Distributed File System (DFS),

- Windows DWM Core Library,
- Windows Event Logging Service,
- Windows Group Policy,
- Windows Group Policy Preference Client,
- Windows Internet Key Exchange (IKE) Protocol,
- Windows Kernel,
- Windows Local Security Authority (LSA),
- Windows Local Security Authority Subsystem Service (LSASS),
- Windows Local Session Manager (LSM),
- Windows NTFS,
- Windows NTLM,
- Windows ODBC Driver,
- Windows Perception Simulation Service,
- Windows Point-to-Point Tunneling Protocol,
- Windows Portable Device Enumerator Service,
- Windows Print Spooler Components,
- Windows Resilient File System (ReFS),
- Windows Secure Channel,
- Windows Security Support Provider Interface,
- Windows Server Remotely Accessible Registry Keys,
- Windows Server Service,
- Windows Storage,
- Windows TCP/IP,
- Windows USB Serial Driver,
- Windows Web Account Manager,
- Windows Win32K,
- Windows WLAN Service,
- Windows Workstation Service.

Este es el boletín de vulnerabilidades de octubre 2022 de Microsoft, tiene una categoría 5 (crítica), y como vemos en las imágenes vemos todos los servicios que tienen esa vulnerabilidad. Para solucionarlo, Microsoft nos dice que en la mayor parte de los casos, el software afectado se actualizará automáticamente por defecto.

4. Analiza esta situación: Supón que en el ordenador portátil con cámara web integrada que tienes en tu habitación, no tiene cortafuegos activo, no hay instalado un antivirus y lo tienes siempre conectado a Internet (bajando algo). Y si un día te dejas sin querer el DNIe conectado?

Es posible que en esta situación me roben datos nacionales, y con esto suplantan mi propia identidad. Con esto es muy probable que pueda llegar a recibir una multa de la policía por algún delito que yo no he cometido, pero como me han suplantado la identidad, cuenta como que el delincuente es mi persona.

5. MALWARE: Diferencia entre Virus, Gusanos y Troyanos.

Los virus informáticos se incluyen en aplicaciones, videojuegos o archivos, para propagarse de un equipo a otro, infectándolos mientras que se propagan a otro dispositivo distinto. Al igual que los virus naturales de la vida diaria real, los virus informáticos se presentan en diversos grados según su gravedad. Algunos de estos, solo causan molestias leves, mientras que otros dañan el hardware, el software o los archivos. Casi todos los virus vienen incluidos con archivos ejecutables, como videojuegos piratas, aplicaciones ilegítimas, etc. Esto significa que el virus permanece en su equipo, pero no se verá afectado a menos que abra o ejecute ese programa malicioso. Tenemos que tener en cuenta que los virus no pueden propagarse sin la intervención del usuario que lo ejecuta. La mayoría de las veces, los usuarios propagan sin quererlo esos virus informáticos al compartir archivos infectados o enviar correos electrónicos que contienen el virus como archivo adjunto. Los virus dependen también del sistema operativo que estemos utilizando, hoy en día se hacen la mayoría de virus para Windows 10, ya que es el sistema operativo que usa la mayoría de usuarios comunes, y comúnmente, el archivo que a veces trae virus, utiliza una extensión .exe o .bat.

Los gusanos informáticos son un malware que se reproduce y se duplica para propagarse a ordenadores que no están infectados. Los gusanos a menudo hacen uso de partes de un sistema operativo que son automáticas e invisibles para el usuario común. Frecuentemente, sabemos que estamos infectados por un gusano cuando su replicación incontrolada consume muchísimos recursos de nuestro sistema, lo que ralentiza o detiene otras tareas que estemos ejecutando, incluso aunque el ordenador esté sin ejecutar ninguna de nuestras tareas, estos gusanos consumirán mucho.

Un ejemplo que podemos encontrar hoy día, es el gusano criptográfico ransomware WannaCry, que muchas de las personas que han investigado sobre este caso, piensan que es obra de ciberdelincuentes norcoreanos. WannaCry se llevó a cabo sobre las versiones de los sistemas operativos Microsoft Windows que usaban Server Message Block (SMBv1), un protocolo viejo y anticuado para compartir recursos. Este gusano, una vez que el sistema de destino estaba infectado, la infección de este instalaba un programa que encriptaba los archivos del usuario y solicitaba un rescate por dinero, casi siempre era donar criptomonedas a una cartera virtual. Más tarde buscaba y encontraba nuevas víctimas enviando solicitudes SMBv1, los usuarios que respondían eran infectados por el malware que no paraba de reproducirse, hasta que por fín a los meses se mitigó.

Para repeler este tipo de ataques, es sencillo y a la vez difícil, si vemos que nuestro ancho de banda consume mucho cuando no estamos haciendo nada, o nuestra memoria, significará que algo malo está pasando. Lo mejor será tener activadas en nuestro ordenador habitual las actualizaciones periódicas, contar con un buen antivirus, yo en lo personal uso AVG, tener activado el Firewall y protegernos del phishing de nuestro correo electrónico.

Un troyano es un tipo de malware, es un programa que destruye el sistema, o espía nuestros datos, movimientos… Este siempre está disfrazado de aplicación real. A diferencia de los virus, los troyanos no se reproducen a sí mismos, pero también pueden ser muy peligrosos. Además, este troyano abre una puerta trasera en el equipo infectado y permite que los usuarios o programas maliciosos puedan penetrar fácilmente al sistema y robar la información personal y confidencial. Por ejemplo, te descargas una aplicación de adobe, como photoshop, de un sitio que se ve que no es oficial. Lo empiezas a utilizar, y al mes, ves que se han cobrado de tu tarjeta 30 € sin motivo ni sentido, casi siempre lo que pasa es que el virus troyano, ha espiado la información bancaria del usuario, y ahora que tiene esos datos, el ciberdelincuente, hace uso de ellos, y roba algo de tu dinero

6. Que son el Phishing, Vishing y smishing?

Todos los actuales ataques de phishing comienzan con la víctima recibiendo un correo electrónico o un SMS al móvil en el que el remitente se está haciendo pasar por un banco, una empresa u otra organización real como paypal o instagram, con el objetivo de engañar a la víctima. Este correo electrónico / SMS incluye enlaces a un sitio web preparado por los criminales, que imitan a la perfección la empresa legítima y en el que se engaña a la víctima para que introduzca sus datos personales y su cuenta, y los atacantes la roban. Es fácil encontrar programas que automatizan esto, adjunto el enlace para ver el código de cómo sería un programa dedicado al phishing:

https://github.com/htr-tech/zphisher

El vishing es otra forma común en la que un usuario cae en un timo en la que los delincuentes intentan engañar a la víctima a través de una llamada telefónica, suplantando la identidad de otra persona o de una organización como una entidad bancaria como la caixa. El objetivo es robar la información personal, bancaria o convencer a las personas para que ellas mismas sean las que transfieran dinero a los ciberdelincuentes. El medio que estos delincuentes hacen uso es vía llamada telefónica. Al vishing se le conoce por ser la combinación entre la voz y utilizar también técnicas de phishing.

El smishing es otra forma de phishing en la que se utilizan teléfonos móviles como el medio principal de ataque. El ciberdelincuente realiza el ataque intentando obtener información personal, incluidos los números de la tarjeta de crédito o de la seguridad social. El smishing se realiza mediante mensajes de texto o SMS, esto hace que le demos su propio nombre "SMiShing". Un caso actual que podemos encontrarnos hoy en dia es el siguiente, un cliente de un banco recibe un mensaje de texto o whatsapp, donde el emisor del mensaje se hace pasar por su banco habitual, y en el mensaje le dice que se ha realizado una compra sospechosa con su tarjeta de crédito y que han detectado inicios de sesión en su cuenta inusuales. En el propio mensaje, le solicitan que se comunique con el banco por teléfono y le dan un número de teléfono falso al que llamar. El cliente llama al número falso y es ahí cuando el ciberdelincuente, haciéndose pasar por el banco, le pide su información confidencial bancario para supuestamente cancelar la compra y restablecer su contraseña. Con esto, el usuario ya habrá sido engañado y el ciberdelincuente, ya tendrá toda su información financiera.

7. Identifica, en la siguiente lista, los que sean malware:

- **Backbone: no es malware**
- **Keyloggers: los keyloggers son un tipo de malware, los cuales realizan un seguimiento y registran cada tecla que se pulsa en una computadora, a menudo sin el permiso ni el conocimiento del usuario**
- **Spool: es un malware, de echo todos los programas antivirus reconocen a Spool.exe como malware, por ejemplo Symantec lo identifica como un Downloader, y TrendMicro lo reconoce como un WORM_SOCKS.BL.**
- **Dialers: es un tipo de malware, es conocido específicamente como Android.Trojan.FakeInst, este dialer envía SMS a servicios de tarificación especial, y ha engañado a miles de usuarios haciéndose pasar por un parche para el ahorro de energía en dispositivos Android.**
- **Gusanos: es un tipo de malware, como ya hablamos en el ejercicio 5, es un malware que se replica para propagarse a otros ordenadores.**
- **Sniffer: no todos son malware, depende si se le da un uso ético o no. Son una herramienta de software o hardware que permite al usuario supervisar su tráfico en Internet en tiempo real y capturar todo el tráfico de datos que entran y salen de su equipo como por el ejemplo el programa Wireshark.**
- **Script: depende del uso que se le dé. Es un documento que contiene instrucciones, escritas en códigos de programación. Si se escriben instrucciones poco éticas, será un malware.**

- **Spam:** es un tipo de malware, es un mensaje de email no solicitado que se envía automáticamente a un gran número de direcciones al mismo tiempo.

- **Rootkits:** son un tipo de malware, es un paquete de software malicioso echo para permitir el acceso no autorizado a un equipo u otro software. Los rootkits son muy difíciles de detectar y pueden ocultar su presencia en un equipo infectado.

8. ¿Cuáles son las funciones de la agencia de protección de datos?.

La función principal de la AEPD es comprobar el cumplimiento de la legislación sobre protección de datos y controlar que se aplique correctamente, en especial sobre los derechos de información, acceso, rectificación, oposición y cancelación de datos.

9. Busca en algún documento oficial de toma de datos personales el aviso que detalla tus derechos sobre los datos que estás aportando.

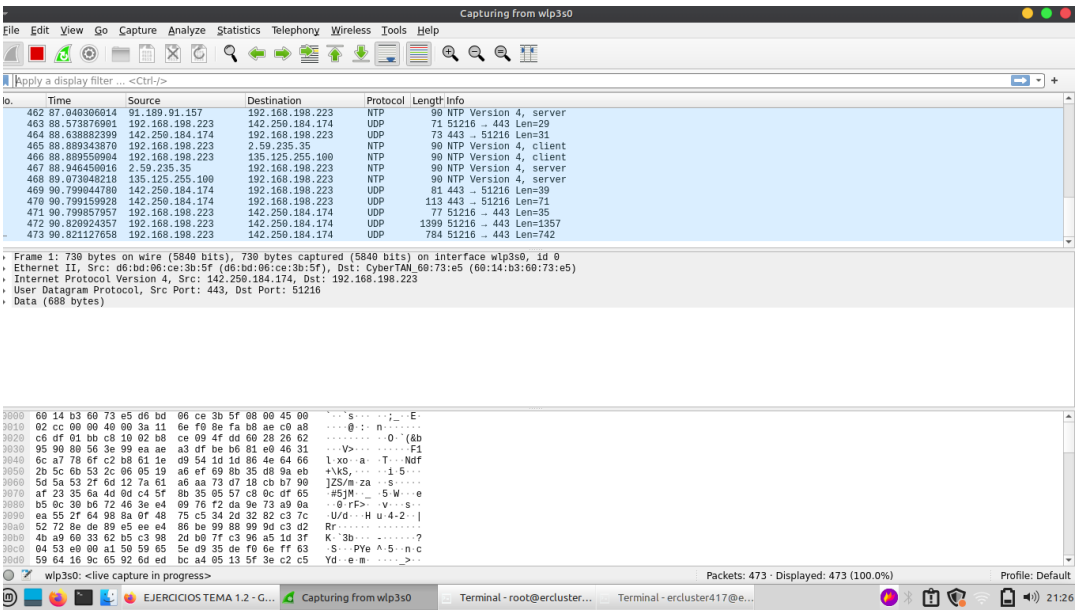
Este documento detalla mis derechos, y de qué manera y forma va a ser tratada mi información y mis datos personales.

10. Qué son las listas de Robinson. Para que sirven, quién puede pertenecer a ellas, cuál sería el proceso de inscripción. Son útiles en todos los casos.

La lista Robison te permite, de forma fácil, rápida y gratuita, evitar publicidad de empresas a las que no hayas dado tu consentimiento para que te envíen publicidad. Funciona para publicidad por teléfono, correo postal, correo electrónico y SMS/MMS. Puede pertenecer a ella cualquier persona que quiera que no le lleguen llamadas, SMS, etc, de servicios o productos que nunca ha solicitado.

En lo personal me inscribí mediante su página web, fue muy rápido y sencillo. Es efectivo contra empresas piratas, es decir, phishing y su variantes, cuando me llaman, digo que pertenezco a la lista robinson y automáticamente cuelgan la llamada.

11. Utilizar Wireshark para descubrir qué equipos están conectados a la red, elegir alguno y ver qué servicios tiene instalados y que versión, buscar luego si tiene alguna vulnerabilidad.



1393…	3118.6046385…	192.168.198.223	192.168.198.49	DNS	73 Standard query 0xfdb6 A www.amazon.es
1393…	3118.6048557…	192.168.198.223	192.168.198.49	DNS	73 Standard query 0xa848 AAAA www.amazon.es
1393…	3118.6050904…	192.168.198.223	192.168.198.49	DNS	72 Standard query 0xe13f A www.nike.com
1393…	3118.6052839…	192.168.198.223	192.168.198.49	DNS	72 Standard query 0x7318 AAAA www.nike.com

Aquí podemos ver como la ip 192.168.198.223 está haciendo uso de amazon y de nike, este es mi propio móvil, con el cuál estoy haciendo esta práctica para mostrar lo fácil que puede llegar a ser ver lo que un usuario está buscando y haciendo uso con su móvil.