TIPOS DE HACKERS

Álvaro Chirou
Digital Technology Teacher

01

BLACK HAT - SOMBRERO NEGRO

ESTOS SON DENOMINADOS CIBERDELINCUENTES, SON DE LOS MALOS. POR LO GENERAL, EL TÉRMINO SE UTILIZA PARA LOS HACKERS QUE IRRUMPEN EN REDES O COMPUTADORAS, CREAN VIRUS INFORMÁTICOS, ETC. LA MOTIVACIÓN DE HACKERS DE SOMBRERO NEGRO ES EL DINERO. ENTRE ELLOS HAY UNA SUBCLASIFICACIÓN (PHREAKERS Y CRACKERS)

Álvaro Chirou
Digital Technology Teacher

01

GREY HAT - SOMBRERO GRIS

EL HACKER DE SOMBRERO GRIS ES EL DEL PERFIL INTERMEDIO, REALIZA TAREAS DE SOMBRERO BLANCO Y DE SOMBRERO NEGRO. SI BIEN NO PUEDEN USAR SUS HABILIDADES PARA BENEFICIO PERSONAL TAMBIEN PUEDEN TENER BUENAS Y MALAS INTENCIONES.

Álvaro Chirou
Digital Technology Teacher

02

WHITE HAT - SOMBRERO BLANCO

SON DE LOS BUENOS, LLAMADOS HACKERS ÉTICOS, SON EXPERTOS EN SEGURIDAD INFORMÁTICA QUE SE ESPECIALIZAN EN PRUEBAS DE PENETRACIÓN Y OTRAS METODOLOGÍAS PARA ASEGURAR QUE LOS SISTEMAS DE INFORMACIÓN DE UNA EMPRESA SEAN SEGUROS.

Álvaro Chirou
Digital Technology Teacher

03

TOP 3 HACKERS MÁS FAMOSOS

Álvaro Chirou
Digital Technology Teacher

01

1 - Kevin Mitnick

Kevin David Mitnick es el hacker más famoso de la historia. Durante más de 15 años causó el pánico en las empresas y las agencias gubernamentales estadounidenses, hasta el punto de que se convirtió en el delincuente más buscado por el FBI.

Pero esas son cosas del pasado, actualmente es de total confianza y una autoridad mundial en formación sobre piratería, ingeniería social y concienciación en ciberseguridad. Tras ser condenado y pagar su deuda con la sociedad, Kevin Mitnick creó su propia compañía de seguridad, Mitnick Security Consulting, que hoy en día asesora a docenas de empresas americanas, y al propio gobierno.

Álvaro Chirou
Digital Technology Teacher

02

2 - Gary McKinnon

En 2002, el gobierno de los Estados Unidos acusó al escocés Gary McKinnon de llevar a cabo "el mayor hackeo de ordenadores militares de la historia". McKinnon hackeó 97 ordenadores de agencias de espionaje y de la NASA, durante más de un año. Se hacía llamar Solo, y dejaba mensajes en los ordenadores hackeados: "Vuestro sistema de seguridad es una basura. Soy Sólo, y continuaré actuando al más alto nivel".

Fué acusado de borrar ficheros críticos que desactivaron más de 2.000 ordenadores militares en Washington, durante 24 horas. También se le acusa de dificultar los suministros de munición durante el 11-S.

Álvaro Chirou
Digital Technology Teacher

03

3 - Albert González

De origen cubano, actualmente condenado a 20 años de carcel, criado en Estados Unidos, se convirtió en uno de los hackers más buscados entre 2005 y 2007.

Lider del grupo delictivo ShadowCrew, fue el responsable del robo de más de 170 millones de tarjetas de crédito, el más grande de la historia. Desde su web vendía también pasaportes falsificados, carnés de conducir, y otro material robado o falsificado. Incluso devolvían el dinero si las tarjetas robadas no funcionaban, como en un comercio tradicional.

Cuando fue detenido colaboró con la Justicia delatando a sus compañeros,con lo que pudo reducir su condena. Pero mientras denunciaba a sus cómplices y se mostraba arrepentido, al mismo tiempo estaba hackeando otras compañías como TJX, a la que robó 45 millones de dólares a través de las tarjetas de sus clientes.

Álvaro Chirou
Digital Technology Teacher

03

Técnicas para Escalar Privilegios Parte 1

Álvaro Chirou
Digital Technology Teacher

01

ABUSO DEL SUDOERS PARA ESCALAR PRIVILEGIOS

Cuando logramos acceso al sistema algo muy común que se realiza en la fase de post-explotación es escalar privilegios. Una de las técnicas más utilizadas para escalar privilegios es el abuso del sudoers, este nos permite escalar privilegios modificando el fichero que se encuentra en la ruta /etc/sudoers.

Álvaro Chirou
Digital Technology Teacher

02

Aquí el ejemplo trabajando con el usuario kali.
En el fichero sudoers ubicado en la ruta /etc/sudoers escribimos lo siguiente (Recordar que para poder modificarlo hay que ser root), en este caso para el ejemplo utilizamos el binario zip
kali ALL=(root) NOPASSWD: /usr /bin/zip
con el comando anterior le decimos que el binario zip se ejecute como usuario root sin proporcionar contraseña, ahora debemos ejecutar el comando que nos proporciona GTFobins.

Álvaro Chirou
Digital Technology Teacher

03

GTFobins es una página que contiene una lista seleccionada de binarios unix que se pueden utilizar para eludir restricciones de seguridad locales en sistemas mal configurados.
Aquí filtramos por permisos sudo y buscamos el binario zip.
Se nos lista esta opción:
sudo zip prueba /etc/hosts -T -TT 'sh #'

ejecutando esto como usuario normal elevamos privilegios y ahora somos usuario root sin proporcionar contraseña.

Álvaro Chirou
Digital Technology Teacher

04

Técnicas para Escalar Privilegios Parte 2

Álvaro Chirou
Digital Technology Teacher

01

ESCALANDO PRIVILEGIOS A TRAVÉS DE PERMISOS SUID

La segunda técnica de post-explotación que estaremos viendo es la de explotación de permisos SUID. Ésta técnica nos permitirá abusarnos de los permisos SUID mal asignados en algunos binarios, los cuales permiten poder escalar privilegios sin proporcionar una contraseña y convertirse en usuario root.

Álvaro Chirou
Digital Technology Teacher

02

En este ejemplo trataremos el binario de python, el cuál asignandole el permiso SUID con el comando chmod 4755 siendo el 4 el permiso SUID, este queda asignado con el mismo.

Podemos observar que la letra s le fue asignado al binario, lo cual indica que ya tiene el permiso SUID.

Álvaro Chirou
Digital Technology Teacher

03

Volvemos a la página anteriormente mencionada GTFObins, filtramos por permisos SUID y buscamos el binario de python.

Se nos lista esta opción:
python -c 'import os; os.execl("/bin/sh", "sh", "-p")'

ejecutando esto como usuario normal elevamos privilegios y ahora somos usuario root sin proporcionar contraseña.

Álvaro Chirou
Digital Technology Teacher

04

Técnicas para Escalar Privilegios Parte 3

Álvaro Chirou
Digital Technology Teacher

01

ESCALANDO PRIVILEGIOS A TRAVÉS DE LAS CAPABILITIES

La tercera técnica de post-explotación que estaremos viendo es el abuso y explotación de las capabilities. Las capabilities son aquellos permisos que dividen los privilegios del usuario del kernel o de los programas de nivel del kernel en pequeñas partes para que un proceso pueda tener suficiente potencia para realizar tareas específicas con privilegios.

Álvaro Chirou
Digital Technology Teacher

02

En este ejemplo trataremos el binario de perl, el cuál asignandole la capabilitie setuid que me permita cambiar el UID del usuario. Para asignar este tipo de capabilitie escribimos setcap
cap_setuid+ep /usr/bin/perl

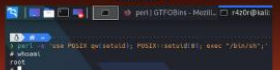
Podemos observar ahora a través de getcap /usr/bin/perl que la capabilitie para cambiar el UID le fué asignada.

Álvaro Chirou
Digital Technology Teacher

03

Volvemos a la página anteriormente mencionada GTFObins, filtramos por capabilities y buscamos el binario de perl.

Se nos lista esta opción:
perl -e 'use POSIX qw(setuid); POSIX::setuid(0); exec "/bin/sh";'



Ejecutando esto como usuario normal estamos seteando ahora el UID a 0 lo cual hace referencia a root y permite escalar privilegios, ahora somos usuario root sin proporcionar contraseña.

Álvaro Chirou
Digital Technology Teacher

04

ALVARO CHIROU

GASTON GALARZA

Prólogo.-

La seguridad informática es transversal a la tecnología. Es decir, donde se encuentre un dispositivo inteligente, debe de haber Ciberseguridad. Hoy se han detectado vulnerabilidades en autos, lavarropas, aspiradoras, televisores y todo dispositivo que se conecte a internet, además de computadoras y celulares. Todo esto atenta contra nuestra privacidad.

Existe una vulnerabilidad que tiene más de 20 años de antigüedad y sigue vigente, y es el Phishing, combinado con ingeniería social lo que hace el Ciberdelincuente, es abusar del analfabetismo tecnológico y desconocimiento en materia de seguridad de su víctima, para obtener sus contraseñas, datos personales o incluso, lograr que le transfiera dinero.

La forma de combatir esta vulnerabilidad es con la información, capacitación y formación en materia de seguridad, y no es necesario que seamos expertos, es cuestión de invertir unos minutos al día para saber a qué debemos estar atentos para evitar ser víctimas de un Criminal que busca robarnos.

Este libro busca eso, brindar conocimiento sobre aspectos genéricos de la seguridad informática que te ayuden a proteger tu información y a protegerte de los Ciberdelincuentes.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Índice

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Capítulo 23: Gamers: Buscados por los Cibercriminales

Capítulo 24: SKIMMING: Vacaciones en Peligro

Capítulo 25: Amenazas por Internet Episodio 1: Doxing

Capítulo 26: Puerta abierta a la Ciberdelincuencia

Capítulo 27: Modo Incógnito: ¿es realmente incógnito?

Capítulo 28: Autentificación en dos pasos: asegura más tu cuenta

Capítulo 29: Amenazas por internet Episodio 2: Phishing

Sección Rutas de Aprendizaje

Capítulo 30: Rutas de Aprendizaje: Seguridad y Desarrollo

Capítulo 31: Rutas de Aprendizaje: Red Team y Blue Team

Capítulo 32: Rutas de Aprendizaje: Python y Cloud

Sección: Programación

Así como aprendemos Lengua, Matemáticas o cualquier otra materia, deberíamos aprender a programar.

Con frecuencia se da a la confusión de que saber programación implica trabajar creando aplicaciones o páginas web, y esto no es así.

Saber programar implica desarrollar el pensamiento lateral, aprendemos a ver los problemas de una manera diferente y por ende, a resolverlos de una forma distinta o inclusive, encontrar soluciones donde antes no las veíamos.

El conocimiento no ocupa espacio y el cerebro es un “musculo” muy importante que hay que entrenar, todo lo que aprendemos son herramientas que jamás nadie nos podrá quitar. Y en lo que a programación se refiere, el conocimiento está al alcance de la mano de cualquiera, ¡aprovéchalo!

En esta sección les voy a compartir el motivo por el cual deben elegir uno de mis lenguajes favoritos, además de buenas prácticas en programación.

¿Debería aprender Python en 2021?

Cuando estamos iniciando en el mundo de la **programación**, nos encontramos con un enorme universo de tecnologías y herramientas que nos dejan inseguros sobre para dónde ir.

Nos encontramos tantos roles diversos: ***web front end, web back end, Inteligencia Artificial, seguridad informática, Machine Learning, desarrollo de videojuegos***… y así, el universo IT se expande más y más.

Entonces, enfrentamos los primeros dilemas: si realmente me quiero dedicar a esto, ¿qué debería estudiar? ¿Por cuál lenguaje empiezo? A lo largo de este capítulo intentaremos analizar las respuestas a estas preguntas, basados en uno de los lenguajes favoritos de hoy: **Python**.

Uno de los favoritos: Python

¿Pero que lo convierte en favorito? Este **lenguaje interpretado de alto nivel**, se ha visto potenciado en los últimos tiempos, ampliando su alcance y potencial en múltiples áreas. Pero además de esto, es un lenguaje con una ***curva relativamente baja de aprendizaje***, además que su sintaxis es bastante clara, lo que permite poder aplicar tu aprendizaje en **corto tiempo.**

Seamos honestos, una de las cosas más motivantes que hay, es poder realizar en la práctica las cosas que estas aprendiendo en teoría, todos lo sabemos. A causa de esto, es que en este artículo decidimos conocer un poco más este lenguaje.

Si estas iniciando en el área, o deseas cambiar de sector dentro de IT, definitivamente **Python** es el lenguaje que deberías aprender [Puedes aprenderlo en este curso]. Además de que viene en el mercado hace varios años ya, lo que significa que habrá múltiples áreas donde diversos productos requerirán mantenimiento, también tiene un campo de acción múltiple.

Otro de los factores influyentes, es la **enorme comunidad** que posee este lenguaje. Una gran cantidad de usuarios y desarrolladores, apoyándose, creando artículos, buscando soluciones a posibles problemas. Esto favorece tener una documentación completa, profunda y lo suficientemente clara, como para permitir que dar los primeros pasos, resulte más sencillo.

El lenguaje multipropósito por excelencia

Como lo lees. Uno de los lenguajes con más áreas efectivas de trabajo, es sin dudas **Python**.
Si eres amante de los **videojuegos**, podrás usar **Pygame** para desarrollar juegos en **Python**; si te gusta web, puedes optar por aprender **Django** para el **back end**. **Keras**, una red neuronal escrita en **Python**, suele utilizarse (aunque no exclusivamente) con **TensorFlow** para el desarrollo de **Deep Learning** en **Machine Learning**.

Podemos hablar de **Python** para **Inteligencia Artificial**, donde encontraremos múltiples bibliotecas, por ejemplo: **Aima**, para manejar algoritmos**, pyDatalog**: un motor de programación lógica, **SimpleAI**: la que provee una biblioteca de uso sencillo, fácil y probada.
Los usos de **Python**, no se limitan a los anteriores, sino que también es un excelente aliado para la seguridad informática. En este curso, podrás aprender ***Hacking con Python.***

El hecho de que sea tan amplio el alcance, permite que haya mayores oportunidades laborales y, por supuesto, con sueldos bastante buenos. Es importante destacar, también, que algunas de las empresas más grandes (como Google) utilizan Python de manera activa. Esto permite, garantiza y muestra, que tendremos trabajo al menos por unos años más en este bello lenguaje.

Buenas prácticas de programación

Con el auge de **Agile** como el favorito de la industria, las metodologías tradicionales van quedando obsoletas. Ahora, las personas del universo IT lidian constantemente con frases como ***"mejora continua", "excelencia técnica", "retrospección y revisión", "adaptabilidad"***.

Una forma recomendada de acercarse a cumplir con estas formas de trabajar, es apelar a las buenas prácticas de programación. Pero, ¿en qué consisten? ¿Cómo aplicarlas?

"Programar Bien" VS "Buenas Practicas"

La programación es apasionante y maravillosa, pero también polémica. Desde las discusiones sobre cuál es el mejor lenguaje, hasta que, si no programas o sabes de "x" lenguaje, entonces no eres un auténtico programador, las polémicas carecen de sentido, pero son constantes.

Si hablamos a grandes rasgos, podemos decir que **"programar bien"** es básicamente resolver un problema con la solución adecuada, de acuerdo a las circunstancias. Si el programa creado, resuelve el problema, podemos deducir que hicimos "bien" el trabajo, que programamos bien. Ahora bien, **¿es esto sinónimo de "buenas prácticas"?**

Buenas practicas

Denominaremos **"buenas prácticas"** al conjunto global de prácticas, que tiene como objetivo crear software de calidad óptima, de fácil lectura para personas que no son su creador y que pueda ser reutilizable. El propósito de este artículo es ayudarte a conocerlas y que puedas aplicarlas cuanto antes, para aumentar tu nivel como profesional.

Entonces, hablemos de algunas de las más conocidas y usadas, que son prácticamente un estándar (o deberían serlo), de los profesionales hoy.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Nombra las cosas correctamente:

Imagina que revisas un código y te encuentras con algo como
SI (a > b) {
MUESTRA “la persona es adulta”
}
Probablemente tu cara sea un poema a lo ilógico de la declaración.
Pero si te encuentras con
SI (Edad_Niño > Edad_Adultez) {
MUESTRA “la persona es adulta”
}

Claramente entiendes las diferencias, las variables y sabes que realiza esa porción de código. Aunque pueda resultar extraño, ejemplos como el primero (donde variables, funciones, etc.) son nombradas por una letra o dos, son reales. Una mala práctica que genera malas lecturas y cosas inentendibles, ocasionando un código ilegible.

Meter todo en un solo archivo

Esto, es algo más propio de programadores novatos: en un solo archivo, incluirán, por ejemplo, HTML, CSS, Js y PHP. Recuerdas que crear diversos archivos distintos permite reutilizar el código y si tienes un problema, solo cambiarlo en el archivo independiente correspondiente, para que el cambio impacte en todos.

Crea código ordenado y legible

Escribir porciones de código en una sola línea, no diferenciar/separar palabras, no seguir un orden lógico de ejecución al escribir código, son solo algunas de las cosas que pueden entorpecer la lectura y favorecer la creación de código espagueti o código basura.

Adopta los estándares empresariales

La empresa te dará una serie de estándares que debes adoptar lo antes posible. Nombres de archivos, comentarios, patrones a usar y otros, forman parte de lo que deberías hacer. No temas preguntar a tu referente que se espera de ti y cómo hacerlo.

Utiliza los comentarios apropiados

Eso permitirá que otras personas puedan ayudarte si te quedas atascado, o si necesitas realizar mantenimiento en el futuro

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Estas son solo algunas de las prácticas beneficiosas, que harán de ti un mejor profesional. Y tu ¿Qué otras prácticas conoces? Espero tus comentarios en mis canales.

Code Review

Dentro de lo que es el mundo de la programación, es un estándar de cada profesional, intentar aplicar buenas prácticas en su trabajo. Hay variadas, pero hoy hablaremos de una que no a todos les gusta realizar: **Code Review o Revisión de código.**

¿Qué es el Code Review?

Como (por ahora), todos los que escriben código son personas***, cometer errores es normal y, de hecho, forma parte del proceso sano y creativo***. Para corregir estos errores, se suelen usar una serie de pruebas manuales o automáticas para lidiar con esos defectos. Pero a veces, corremos el riesgo de que nosotros mismos no podamos notarlo fácilmente.

Para eso, se utilizan estas prácticas colaborativas de revisión de código. Es normal que ocurran de manera más frecuente en empresas agiles, con una clara inclinación al trabajo en equipo y equipos organizados. Pero ***¿en qué consisten? ¿Cómo benefician a los profesionales y a las empresas?***

Cómo se realiza

Dentro de equipos colaborativos, es normal utilizar sistemas de control de versiones. Esto permite diversas configuraciones. Una de las más usadas es usar un archivo como principal, mientras que los demás colaboradores trabajaran en **versiones derivadas del mismo**, pero sin que los cambios afecten directamente al principal.

Una vez que el programador concluyo su parte, envía esa porción del código a la guía principal **pendiente de revisión**. Antes de que esta modificación o adición sea agregada de manera definitiva al principal, pasara por una revisión de código para evitar errores.

Ocurre igual cuando se busca una versión nueva del software, ***se evitan realizar cambios directos*** a “producción”, dejando la nueva versión creada pendiente y permitiendo al examinador evaluar los **cambios entre cada versión.**
La más usada es la denominada **“revisión entre pares”**, donde una persona con habilidades técnicas y experiencia normalmente mayor al programador, revisa el código.

Se evalúan normalmente 5 aspectos:

- **Requerimientos alcanzados:** la lista de objetivos funcionales solicitados debería haberse llevado a cabo de manera exitosa.
- **Código correcto:** se evalúa que el código, variables, patrones, case o nomenclaturas concuerden con lo esperado, de acuerdo al lenguaje que se está utilizando
- **Arquitectura y lógica:** se busca cierta fluidez en el código, que trate de mantener el conjunto de "buenas prácticas" respetando los estándares planteados por la organización, sobre todo enfocándose en que en ocasiones se suele usar porciones de código extraídas de otros sitios
- **Reacción a errores:** acá se piensa un poco más como un usuario del futuro producto, intentando ver cómo se comporta el programa si se ingresaran parámetros distintos a los planteados (por ejemplo, un formulario donde se solicita un numero de celular y el usuario decide poner letras)
- **Optimización de código:** dentro de los lenguajes, en ocasiones se pueden usar prácticas variadas orientadas a mejorar la velocidad, funcionalidad o seguridad del código. Un desarrollador más experimentado, probablemente posea más experiencia en determinada situación y pueda brindar maneras alternativas y mejores de resolver una situación puntual

¿Aporta beneficios?

Cuando inicialmente se plantean solicitudes de revisión de código, la primera traba que se suele poner es: "pero nos demandara demasiado tiempo y ya estamos atrasados".

Acá hay dos conceptos que tenemos que recordar: primero, hay que intentar arreglar las cosas **ANTES** de que se rompan, y el tiempo "perdido" arreglando algo ahora, es mucho menos del tiempo (y recursos) que se gastarán cuando las fallas

sean demasiadas o múltiples usuarios de un producto ya publicado, afronten problemas.

Desde **Agile** como forma de trabajar, cuando los equipos son auto organizados y tienen la libertad de decir el "**COMO**" realizar algo, los tiempos y circunstancias sobre cuando realizaran este tipo de revisiones surgen de manera autónoma, lo que produce mejores resultados.

A pesar de que, en circunstancias puntuales, se recurre a utilizar un código con errores o en circunstancias no óptimas, la mayoría de las veces las revisiones de código se dan con frecuencia, permitiendo que ***el producto final salga en mejores condiciones*** y con menos probables errores desde su lanzamiento.

Por otro lado, el reto de tener que ponerse a leer y revisar un código ajeno, permite aumentar las habilidades de desarrollo y potenciar las habilidades analíticas y de resolución de problemas. También, beneficia al equipo en general, dado que ***aumenta el nivel de habilidades y de excelencia técnica*** que todos los miembros irán desarrollando a lo largo de los proyectos en los que participen.

Esto también permite potenciar la lógica de los programadores, y potenciar sus habilidades de entender requerimientos. Seamos honestos, ***no siempre tendremos los objetivos a cumplir con lujo de detalles.*** Para eso, a través de la revisión de código se potencia la comunicación entre miembros del equipo, lo que lograría analizar de manera interna los distintos requisitos a cumplir.

Consideraciones finales

Recuerda, siempre que la revisión de condigo forma parte de un ciclo de ***búsqueda de excelencia técnica de manera permanente.*** Algunas sugerencias finales relacionadas a esta excelente practica:

- **Si eres el revisor:** recuerda que es normal estar a la defensiva cuando estamos en una "evaluación". Se amable con tu manera de hablar, trata de ser objetivo y no hacer comentarios agresivos, humillantes o que generen malestar. Recuerda que todos cometemos errores y que las falencias en los programas no significan que tu compañero sea incompetente.
- **Si eres el revisado**: no tomes a título personal las sugerencias o correcciones que te hagan. Velas como una oportunidad única que puede potenciar tus habilidades a futuro. Si tienes la oportunidad, solicita correcciones cada "poco" contenido. No sobrecargues a tu revisor con múltiples archivos, mientras menos cosas, más a fondo se puede analizar.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Y tu ¿Qué opinas de la revisión de código? ¿la utilizas con frecuencia?
[Aquí encuentras mis redes sociales para enviarme tus comentarios]

Sección: Seguridad Informática

Nuestra vida se encuentra digitalizada, todos nuestros datos están en internet.

Hoy el Cibercrimen deja más dinero que el propio narcotráfico, y son nuestros datos los que venden.

Por esa razón hoy es clave aprender a protegerlos.

Así como nos enseñan que cuando cruzamos la calle, debemos ver hacia ambos lados, o que no tenemos que hablar con desconocidos, nos deberían de enseñar a como navegar de una forma segura, y que tampoco debemos establecer conversaciones con personas que no conocemos, ni compartir nuestra privacidad, de forma pública.

El fascinante mundo de la seguridad informática es apasionante, pero sumamente grande, hay mucho que aprender a tal punto que puede asustar, por eso es importante tomárselo con calma, y empezar por partes.

El objetivo de esta sección es sumergirte en diferentes ramas para que te vayas empapando y conozcas algunos de los aspectos de esta materia.

Hay mucho más para conocer y mucha información en internet que comparto de forma permanente, en formato video (Youtube, Udemy), imágenes (Instagram) e inclusive por escrito (este libro y artículos en mi web).

Elegir esta profesión es un estilo de vida y quienes la elegimos, la vivimos con mucha pasión, te invito que tú también lo hagas.

¿Debería usar el Firewall de Windows en 2021?

¿Por qué deberías tener activado y configurado correctamente el Firewall?

Seamos honestos: Windows, no es precisamente sinónimo de seguridad total. Cuando mencionamos este Sistema Operativo, normalmente sabemos que vamos a lidiar con distintas amenazas y posibles brechas. Para disminuir el potencial riesgo que enfrentamos, es crucial saber utilizar todas las herramientas de las que disponemos, entre ellas el subestimado Firewall de Windows.

¿Qué es el Firewall?

Es un dispositivo de seguridad cuyo propósito central es evitar que el malware se expanda por una red, pero también actúa impidiendo que terceros no autorizados ingresen al sistema.

Seguramente te habrás topado con el firewall, al conectarte o configurar una nueva red, y también al instalar un nuevo programa. Funciona a través de inspección y descarte.

¿Qué significa esto? Inspeccionara los paquetes de datos que ingresan, lo compara con un conjunto de parámetros establecidos por el usuario y de acuerdo a ello, si coinciden los admite, de lo contrario los descarta.

Se dividen en dos tipos: **lógicos y físicos**.

En este artículo, nos centraremos en los lógicos, dado que el **Firewall de Windows** entra en esta categoría.

Como habrás sospechado a estas alturas, los lógicos son un programa más de tu computadora, que puedes instalar y configurar de acuerdo a tus necesidades. Cuanto el firewall está debidamente configurado, al momento de instalar un

programa que requiera conexión a internet (pueden ser juegos, Skype, etc.) te preguntara si deseas permitir que dicho programa establezca la conexión. ¿Genial, cierto? Es como tener un amigo controlando quien, como y para que se conectara a internet. Esto resulta muy útil, dado que nosotros nos aseguramos así, de que solo los programas que deseamos se conecten efectivamente (y obvio, aquellos en los que confiamos).

Como mencionamos antes, utiliza un conjunto de reglas para que, de forma predefinida por ti, el programa sepa cómo actuar en distintas circunstancias de manera automática, por **ejemplo**:

Podrías armar una norma para aceptar determinado programa que requiera conectarse con sus servidores vía internet (como ser, Steam), rechazar conexiones y solicitudes de conexión remota, configurar el uso y apertura de puertos (podrías dejar algunos solo para conexión local, cerrar otros y demás).

Como seguramente sabrás, algunos programas, procesos e incluso elementos de hardware (como los escáneres vehiculares) requieren de ciertos puertos específicos activados para su correcto funcionamiento. Esto, requiere que configuremos de manera óptima nuestro firewall para favorecer el desempeño de ellos.

¿Qué ocurre si no está activado o está mal configurado?

Básicamente, **pierdes un gran aliado de seguridad.**
El ingreso de malware es mas probable, lo que puede ocasionar graves daños a tu equipo. También es más probable, que personas con malas intenciones tomen temporal o permanente control de tu equipo de manera remota. Sería como dejar tu casa con las puertas sin cerradura e irte a dormir. Puede que no ocurra nada y que despiertes sin nada extraño, pero la pregunta es:

¿vale la pena arriesgarse?

Si estás leyendo este libro, claramente la seguridad es importante para ti. Seguramente conoces múltiples programas espía, que pueden detectar las pulsaciones de tu teclado o se instalan para permitir control e inspección en modalidad remota, como los famosos troyanos RAT, y te preocupe su implementación contra ti. **Entonces ¡El firewall es un gran aliado!**

Si en alguna ocasión debes realizar alguna tarea que requiera que trabajes con firewall desactivado, lo más prudente seria optar por desconectarte de internet y, de ser posible, no instalar programas, especialmente de fuentes desconocidas. Recuerda, en seguridad, mientras más precavido seas, mejor. Debes pensar siempre, en adelantarte a posibles riesgos y amenazas.

Ten en cuenta estos detalles: cuando configuramos el firewall para que una aplicación esté permitida, es como abrir una pequeña ventana en un muro. Cada

vez que la aplicación lo requiera, esa ventana se abrirá y permanecerá así hasta que la aplicación deje de requerirlo. Pero, en el caso del puerto, las cosas son ligeramente diferentes.
Si una aplicación se asemeja a una ventana, un puerto sería algo más parecido a un túnel en el muro: desde que decidimos abrirlo hasta que decidimos cerrarlo de manera manual nosotros mismos, el túnel seguirá abierto. Un auténtico festín para los criminales cibernéticos. Por eso es necesario estar atento y realizar una configuración optima: debemos ponerles el camino difícil a los delincuentes.

Te recomendamos que revises tu configuración, seguramente concuerdes con nosotros en que dejar muchos túneles y ventanas siempre abiertas, no es una buena idea.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Antivirus

¿Cómo funcionan? ¿Para qué sirven? ¿Debería tener uno instalado?

Uno de los productos que normalmente se recomiendan que deberías tener instalados en tu equipo, son los **antivirus.** Pero, cuando leemos estas sugerencias, es normal que surjan diversas interrogantes. A lo largo de este artículo intentaremos resolver estas preguntas.

¿Cómo funcionan? ¿Para qué sirven?

Los **antivirus** son programas creados específicamente para proteger la computadora a través de detectar y eliminar el **malware** de tu dispositivo. Se denominan antivirus, a pesar de que hoy la mayoría soporta ***múltiples tipos de ransomware***, porque inicialmente fueron creados para resolver las amenazas de los virus.

Para lograr reconocer el malware, recorren dos caminos. En el **primero** realizan un proceso de comparación: utilizan una base de datos existente con múltiples señales y características específicas de distintos tipos de malware (denominadas «***firmas***«).

Estas bases de datos requieren actualizaciones permanentes, dado que los delincuentes utilizan cada vez métodos más diversos y rebuscados de crear malware.
A través de este proceso, se compara cada archivo de manera individual con la base de datos.

Si algún archivo coincide con una de las porciones de software malicioso registrado, el antivirus entra en acción, llevando una de las siguientes acciones:

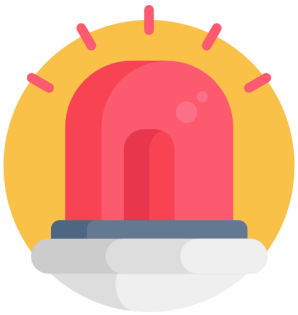
- **Reparar el archivo**: el antivirus intenta corregir el programa eliminando la porción de software malicioso
- **Ponerlo en cuarentena:** en esta instancia, el virus es aislado, se bloquea cualquier tipo de acceso a este software, lo que impide que el malware se ejecute y se extienda.
- **Eliminación de archivo:** cuando la porción maliciosa no puede eliminarse del programa, el antivirus solicitará al usuario autorización para eliminar el archivo del dispositivo.
- **Análisis de conducta**: en esta opción, el antivirus pone mayor supervisión y control sobre todos los programas en ejecución en el dispositivo. Si encontrara algún programa realizando acciones sospechosas, el antivirus notificará al usuario de esto y le sugiere distintas acciones que deberían llevarse a cabo.

El **segundo** camino que recorren, es el de monitorizar a nivel global los archivos guardados en nuestro dispositivo, enfocándose en encontrar patrones de comportamiento extraños o irregulares y/o alteraciones del sistema que permitan identificar un ***archivo malicioso.***

Este procedimiento tiene una **ventaja**: los virus que no están aún en la base de datos, aun así tienen patrones de comportamiento sospechoso,entonces esta monitorización permanente permite detectar estos comportamientos y brindar la posibilidad de aislar el archivo.

¿Cómo me puedo infectar?

Dentro del mundo IT, es común recurrir a la broma de : «es un error de capa 8», basado en el modelo OSI.



Desde luego, esta problemática no iba a ser la excepción. En la mayoría de las circunstancias, para que el malware ingrese a nuestro dispositivo, requiere una participación activa necesaria de nosotros, como Usuarios del dispositivo. Descargar cracks, contenido pirata, ingresar a sitios de dudosa seguridad, instalar programas de dudosa procedencia,seguir cualquier link que nos llega a nuestro email o descargar cualquier contenido que nos llega vía email sin verificar el emisor, son solo algunas de las maneras en
las cuales puedes recibir malware.

Entonces tomando esto en cuenta, surge la siguiente pregunta:

¿Debería tener uno instalado?

Es necesario dejar algo en claro: la mejor medida de prevención, no es el antivirus; somos **nosotros mismos**.

Nosotros como usuarios activos, siendo **precavidos** y **responsables** en el uso de nuestro dispositivo, somos los que definitivamente reducimos las posibilidades de recibir malware.

Recordemos que ***no existe ningún antivirus 100% efectivo***. Normalmente, las organizaciones cibercriminales crean malware a mayor velocidad de la cual las organizaciones pueden brindar respuestas al problema.

El ritmo y velocidad a la cual pueden reinventar los algoritmos detectores de amenazas no se compara al ritmo de creación de estas.

Desde aquí, **no podemos recomendarte de manera categórica**, más allá de toda duda razonable, un antivirus o marca en específico. Insistimos en recomendar el uso precavido y responsable de tus dispositivos en la red.

Configurar correctamente otras herramientas, como el **Firewall**, combinado con un **antivirus** y una conducta seria, responsable y precavida, disminuye las posibilidades de recibir malas noticias.

Por supuesto, como arma de prevención, instalar un antivirus ayuda al combo.

Pero recuerda, mantener tus dispositivos actualizados y sus programas correctamente configurados, unido a las medidas que vimos en el párrafo anterior, disminuirán notablemente las posibilidades de ser infectado de malware.

Recuerda que, sin importar cual uses, deberías tener actualizado permanentemente el programa, hacer análisis profundos rutinariamente y prevenir lo más posible conseguir riesgos innecesarios.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Malware episodio I: Ransomware

En esta nueva colección de artículos, profundizaremos en el principal enemigo de la era de la tecnología: el **Malware**.

Todos los dispositivos tecnológicos con sistema operativo pueden ser víctimas de uno de los tipos de Malware, lo que en la práctica significa que **todos estamos expuestos,** sin importar nuestro campo de acción: cajeros bancarios, computadoras del hogar, notebooks, computadores hospitalarios y otros.

Sin ser fatalistas o apocalípticos, hay que darle la dosis necesaria de respeto a estos peligrosos trozos de software cuyo único propósito es hacer daño en mayor o menor medida.

En estos artículos, obtendrás definiciones sobre que son, como actúan y cómo puedes prevenirte de ellos.

Qué es el Malware

Malware es un término que se usa de manera global para categorizar todo software creado con fines ilícitos o maliciosos.

El objetivo de estos programas es **atacar, intervenir, monitorizar o explotar** dispositivos, redes o servicios programables con el propósito de conseguir información o recursos.

Dañan dispositivos, roban datos, siembran el caos y arrasan con todo a su paso. Una vez que el objetivo está cumplido, los atacantes normalmente intentarán **chantajear** a la víctima para conseguir dinero, o bien utilizaran esta información para venderla al mejor postor en los sitios más oscuros de la red (aunque con el paso del tiempo, los ciberdelincuentes se han vuelto más descarados y pueden encontrarse sin mucho esfuerzo en la **Surface Web)**.

Los creadores de Malware pueden ser distintos grupos: ciberdelincuentes, hacktivistas, sectores de una empresa que crean el Malware de manera ética o incluso, gobiernos para atacar a gobiernos rivales.

Hay distintos tipos de Malware y en este artículo, pondremos el foco en uno que viene hace varios años bastante “de moda”: El **Ransomware**.
Empresas, entidades estatales, personas físicas; las víctimas se repiten por doquier y ***pareciera que nadie está a salvo.***

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Para que usan el Malware

Por supuesto, el propósito del mismo dependerá de los creadores.

- El **área ética** de seguridad informática de una empresa, puede desarrollar un malware para evaluar las vulnerabilidades de la corporación, para ver donde deberían reforzar las medidas preventivas. Pero tristemente, estos son los menos.
- Los **hacktivistas**, pueden perseguir causas a su modo de ver, nobles, por lo que el propósito de los Malware creados por ellos sirve para intentar dejar una lección o marcar un tema o lema de protesta.
- Los **ciberdelincuentes** (y los gobiernos cuando recurren a ello), tienen el firme propósito de dañar y nada más. El tipo de daño varia, algunos recurrirán a instalar programas de control en el dispositivo de la víctima. En otros casos, instalaran software de minado de criptodivisas. Algunos utilizaran estos sistemas para robar y subastar información de la víctima, como datos de tarjetas de crédito o causar chantajes con ello.

Qué es el Ransomware

¿Sabías que en varios reportes **IOCTA**, la **EUROPOL** mantuvo como mayor amenaza al **Ransomware**? Profundicemos en el primer tipo de Malware que veremos en esta colección.

El **Ransomware** es un tipo de software de rescate. El único propósito de este software es el chantaje o la extorsión hacia la víctima.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Cuando el **Ransomware** infecta el dispositivo, **cifrara** toda la información disponible en el disco (o incluso, si el dispositivo no es aislado a tiempo, puede expandirse a toda una red) y luego ejecutara un panel donde se exhibe los detalles del ataque **exigiendo el pago** de una recompensa para la liberación de la información.

En palabras simples, **bloqueara** el acceso a todos los archivos que poseas en tu computador, normalmente cambiando la extensión del archivo. Si tienes información o cosas valiosas y/o preciadas, sin dudas desearás recuperarlas.

Para poder acceder de nuevo a ellas, los delincuentes dejan instrucciones al respecto, las que normalmente son **que envíes dinero,** preferentemente en criptodivisas a una billetera virtual, prácticamente imposible de rastrear.
Estos delincuentes prometen que recuperaras el control de tu dispositivo inmediatamente después de recibir el pago (por qué claro, ***quien no confiaría en un delincuente que intenta extorsionarte o chantajearte, ¿no? Totalmente confiables ¡ja!)*** Pero, ¿es esto realmente así?

¿Recuperaré mis archivos?

Como dijimos antes**, ningún sentido ni lógica tiene poner tu confianza en meros delincuentes que intentan extorsionarte.**

El foco principal de ellos es ***obtener dinero, no tu bienestar.*** Si pagas el rescate, **no hay ninguna garantía** de que realmente te liberen los archivos.
Lo más probable es que soliciten nuevamente dinero (si estuviste dispuesto a pagar la primera vez, podrás hacerlo de nuevo, o incluso pagar más).

Pero hay otro problema en el que deberías pensar. Si ya llevas tiempo deambulando en temáticas de seguridad informática, conoces la Triada **CIA**.
Cuando tu dispositivo se ve afectado, **la disponibilidad y la integridad** de los datos que poseías se ven afectados **gravemente**.

¿Crees, más allá de toda duda razonable, que tus archivos no resultarán afectados? El Ransomware es algo impredecible. Hay casos donde, luego de

efectuado el pago, el contenido recuperado ***queda parcialmente dañado, haciéndolo practica o totalmente inutilizable.***

Tipos de Ransomware

Hay varios tipos dentro de estos productos maliciosos.

- **Cripto-malware o cripto-ransomware:** cifra los archivos y exige un rescate en criptodivisas. Uno de los más famosos en la historia fue el WannaCry, que llego al extremo de arriesgar cientos de vidas al atacar hospitales, impidiendo que médicos accedan a la información de los pacientes.
- **Scareware**: simula ser un software de protección (como un antivirus), que lanzara alertas permanentes y, en ocasiones bloqueantes, informando que se encontró una gran amenaza en tui dispositivo y que, por un pago, puede eliminar dicha amenaza.
- **Screen locker o bloqueador de pantalla:** al encender el dispositivo, se abrirá una ventana pretendiendo simular un sitio oficial de una autoridad (Policía, FBI, Fuerzas Armadas) indicando que el usuario fue encontrado realizando un delito y que, para recuperar el control de dicho dispositivo, deberá pagar una multa.
- **Doxware**: amenaza con publicar en la red los archivos confidenciales o privados del usuario. Varios famosos fueron víctimas de esto, cuando les exigían rescate para evitar que sus fotos intimas fueran publicadas.
- **Pin locker:** Ataca los dispositivos Android cambiando los patrones y/o PIN para evitar el acceso de los legítimos usuarios.
- **RaaS o Ransomware as a Service:** malware hospedado y gestionado de manera anónima por un ciberdelincuentes, que se encarga de toda la gestión: infecta dispositivos, cobra los pagos de las víctimas, gestiona los descifradores y se queda con una pequeña parte del rescate pagado.

¿Cómo protegerse?

Ya sea si te preocupa el uso **personal** o **empresarial**, las recomendaciones son similares:

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

- Mantén un **backup** de la información, que este en otra red y otro dispositivo, así si tu dispositivo o toda la red recibiera el ataque, podrías reestablecer todo desde otro lado.
- Mantén tus programas **actualizados**, con los últimos parches de seguridad que las empresas desarrollen
- **Desactiva** los programas o servicios que no utilices con frecuencia
- Asegúrate que las contraseñas sean **difíciles** de descifrar
- Procura mantener los accesos con **autenticación** de doble paso
- Utiliza cuando puedas, **VPN**
- **Capacita** a las personas con acceso a tus dispositivos en materia de seguridad

Si fuiste víctima de un ransomware, una excelente alternativa es visitar la siguiente página web:

https://www.nomoreransom.org/

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Malware Episodio II: Adware

Imagina la siguiente escena: estas muy cómodo, relajado, tu día de descanso. Enciendes la tv, listo para ver tu programa favorito. En los primeros 15 minutos de transmisión recibes 10 interrupciones para mostrar publicidad. ***¿Disfrutas más tu programa favorito gracias a la publicidad, o menos?*** Ahora, imagínate eso, multiplicado por 100.

En tu computador, el **Adware** funciona precisamente así: dándote enlaces publicitarios por, básicamente, cada clic que des. Decides abrir Facebook, ¡pum! Redirección a una página de publicidad. Abres Word, imposible: antes da clic en la publicidad. ¡Qué cosa más fastidiosa!

Definitivamente tu computador está infectado, por el siguiente tipo de **Malware** de esta serie: **Adware**. Analicemos que es, como funciona y como evitarlo.

Qué es el Adware

El **Adware** (hablando en el sentido más amplio del término) es un tipo de software, diseñado con el propósito de hacerle ganar dinero a su creador, a través de mostrar publicidad a la mayor cantidad de usuarios posibles. Hasta aquí, todo normal.

Algunos de estos, son usados de manera legítima (aunque molesta) por el propietario, para exhibir en programas para descargar, anuncios alrededor del contenido desarrollado. Una manera algo fastidiosa para el usuario, pero para nada ilegal y/o antiética. **Pero eso, es solo uno de los tipos que hay.**

Hay otro tipo de **Adware**, el cual comparte practicas con su hermano el **spyware** (del cual hablaremos en otro artículo), el cual monitorea tu comportamiento en los sitios que visitas o las teclas que pulsas. Luego, recopila esa información para brindarte anuncios personalizados o venderla a terceros.

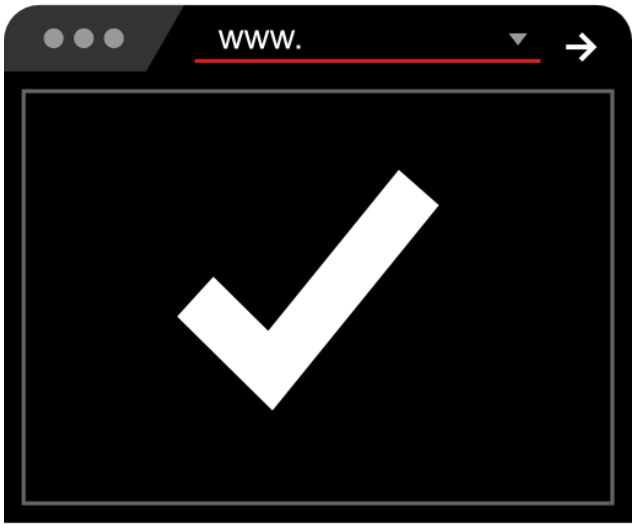
El peor tipo, además de realizarte seguimiento, es el que mencionamos en el único de este artículo: **toma control de tu dispositivo,** forzándote de manera

cíclica a ingresar a sitios de publicidad o ejecutando ventanas emergentes de manera permanente para conseguir rédito económico.
En el mundo del marketing, las publicidades se pagan de múltiples maneras: una de ellas es cuando los visitantes dan clic en el anuncio**(PPC**) o cuando ven más de 5 segundos un video. El **Adware**, intenta arrastrar todos los usuarios posibles a estos sitios para brindarle beneficios económicos a su propietario.

¿Cómo puedo infectarme de Adware?

Todos hemos utilizado alguna vez el patrón "**siguiente**". Admítelo, sabes de que hablo. Estas por instalar un programa, buscas el botón **"siguiente/next**" y lo pulsas hasta que llegue al final, sin evaluar el contenido, ni "extras" que se introduzcan ahí. Así que la primer medida de prevención es: se precavido, controla ***QUE*** bajas, de ***DONDE*** descargas y supervisa ***ATENTAMENTE*** el proceso de instalación.

Pero claro, no siempre será tan fácil. Algunos programas de dudosa procedencia, descargaran sin tu consentimiento ni conocimiento el Adware, así que te costara darte cuenta. ***Se precavido sobre los programas que descargues.***



Otra manera común de infectarse es a través de ***sitios web vulnerables***. Aquí tendrás un dilema mayor, dado que las vulnerabilidades se crean al momento del desarrollo del software.

En estas circunstancias, los programadores dejan vulnerabilidades (sin intención), aprovechadas por delincuentes, para llevar a cabo estas prácticas.
Estos ciberdelincuentes ***utilizan troyanos*** para que sea difícil de percibir que están instalando software malicioso en tu dispositivo.

En esta situación, la mejor alternativa es **la prevención:** no ingresar a sitios de dudosa procedencia, descargar de fuentes oficiales y no seguir cualquier link que se atraviesa.

Consideraciones finales

El **malware** en general, y el **Adware**, aprovechan malos comportamientos de los usuarios y descuidos, para explotarlo de manera económica. Si sospechas que tu **dispositivo** podría estar infectado de Adware, podrás recurrir a los antivirus como herramienta central para eliminarlos.

Algunas empresas proveedoras, poseen bases con datos de ***Adware reconocido***, así que en un escaneo los encontraran y eliminaran.
Otros tipos de Adware, están "atados" al programa principal, así que, ***eliminando el programa, desaparecerán los molestos anuncios y bloqueos***

Algunos usuarios optaron por formateo y reinstalación de SO, dado que, recuerda, el Adware se instala en tu dispositivo, no en el navegador.

Recuerda el modelo de **"Confianza Cero",** para mantener tus datos a salvo, y tu dispositivo sin **Malware**.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Malware episodio 3: Spyware

Cuando utilizamos nuestra computadora personal, normalmente nos sentimos relajados, confiados y tranquilos. Somos responsables en su uso, mantenemos buenas practicas, no descargamos cosas ilegales. Total, el hecho de estar a solas en casa, es garantía de que estamos lejos de miradas intrusivas. Todo está bien, ¿no?

Pues no. Olvidaste el **Spyware**. Esta herramienta ilegal, tan utilizada por varios gobiernos a nivel mundial como por ciberdelincuentes, siempre con propósitos delictivos, representa el volumen 3 de nuestra serie: **los famosísimos programas espías.**

Qué es

El spyware, como tal, es una palabra genérica para referirse al software de carácter malicioso que infecta un dispositivo, con el propósito de **recopilar y transmitir al propietario del Spyware**, información sobre el dueño del dispositivo, el uso del mismo, el uso que le da a internet y, en fin, cualquier cosa que se realice desde dicho dispositivo.

Dependiendo la complejidad del Spyware desarrollado, podemos encontrar versiones que solo registrarán datos mínimos, hasta los más avanzados que interfieren micrófonos y cámaras pudiendo captar todos los detalles. El principal problema de este software, a diferencia de los otros que hemos visto y que veremos, es que ***es creado para pasar desapercibido la mayor cantidad de tiempo posible.***

Con otros tipos de malware, percibiríamos mal funcionamiento o comportamiento errático de nuestro dispositivo, pero la fortaleza del Spyware es capturar la mayor cantidad de datos de acuerdo a la instrucción creada, ***dejando la menor cantidad de huellas (de ser posible, ninguna).***

Dado que los seguimientos se realizan gracias a largos periodos de rastreo y espionaje a la víctima, estos programas necesitan permanecer indetectables y ***recopilando todo lo posible, durante mucho tiempo.***

El otro problema es que, normalmente son desarrollados de manera que consuman recursos mínimos. A causa de esto, pueden desempeñarse durante mucho tiempo en segundo plano y la víctima no notaria su presencia. También, son creados de manera tal que permanezcan activos todo el tiempo que el dispositivo permanezca funcionando, ***lo que permite que todo lo que haga la victima desde su dispositivo, llegue a manos del ciberdelincuentes creador del spyware.***

Que tipos existen

A grandes rasgos, podríamos mencionar que existen los siguientes tipos (pero no son los únicos):

- **Keyllogers:** estos son creados de tal manera que detectan las pulsaciones de teclas, registran el acceso a sitios web, emails enviados e incluso algunos avanzados, pueden obtener los documentos que se han enviado a imprimir o escanear en los equipos de la red. Un auténtico riesgo.
- **Infostealers**: los “ladrones de información” se encargan de escanear periódicamente el dispositivo para obtener toda la información posible: datos del usuario, contraseñas, historiales de búsqueda, archivos multimedia y todo lo que pueda ser redituable para el atacante. Algunos envían la información directamente al servidor del ciberdelincuente, mientras otros guardan la información de manera local para obtenerla posteriormente. Algunos, increíblemente avanzados, escanean el dispositivo de la víctima, consiguen información específica, la envían y luego ejecutan una especie de autodestrucción, desapareciendo del equipo de la victima
- **Red Shell:** este término se usa para abarcar a un conjunto de programas que se instalan durante la instalación de un videojuego. Estos programas se instalan sin conocimiento ni consentimiento del jugador y rastrean la actividad en línea de los jugadores, capturando los detalles y reenviándolos a los interesados.
- **Password Stealers:** los “ladrones de contraseñas” se encargan de escanear dispositivos, pero con el firme propósito de capturar la mayor cantidad de contraseñas posibles. Normalmente unirán los usuarios con las contraseñas

correspondientes, a la espera del proceso para el que fueron creados: enviar la información o almacenarla de manera local, encriptada.

Cómo puedo infectarme

Teniendo en cuenta que estos maléficos programas buscan recabar la mayor cantidad de información, es lógico suponer que cualquiera puede ser víctima de él. Recordando además que, la fortaleza de ellos es pasar desapercibido, en condiciones normales probablemente no notemos que de hecho tenemos un spyware.

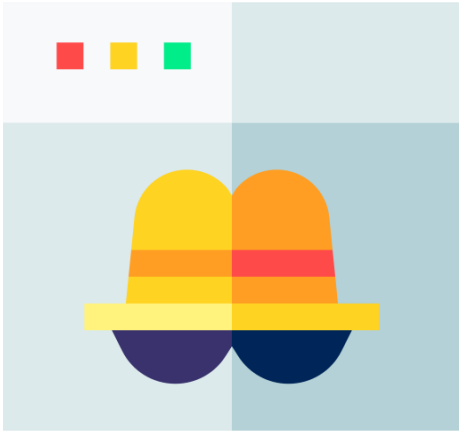
De todas formas, se ha visto en varias ocasiones que los **Spyware** provocan ralentizaciones en el dispositivo o en la velocidad de internet (debido al consumo por transferencia de archivos). Otras señales que pueden hacernos sospechar, es notar comportamientos inusuales en el dispositivo, como iconos movidos de lugar o nuevos, búsquedas o inicios redirigidos, ventanas emergentes sin explicación y similares.

Las formas en las cuales el Spyware llega a nosotros, **es muy parecida a la de cualquier malware:** enganchado a software “legítimo”, sitios webs maliciosos o fraudulentos, envíos de emails con contenido orientado a la víctima, pero con el spyware en segundo plano y similares.

Muchos de los programas antivirus hoy, tienen maneras de detectar ciertos tipos de Spyware instalados en el dispositivo.Es importante notar que, no solo el S.O. Windows puede verse afectado, también dispositivos móviles y otros SO de computador pueden ser víctimas de ellos.

De todas formas, recalcamos que el uso prudente, consiente y responsable del dispositivo, es la mejor herramienta de prevención para evitar el malware.

Espero que hayas disfrutado la lectura de este capítulo y que sirva para que puedas actuar de manera precavida y evitar así*, ser víctima de este peligroso Malware.*



La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Malware Episodio 4: Virus

“Creo que los virus informáticos deberían ser considerados como vida. Quizás dice algo sobre la naturaleza humana que la única forma de vida que hemos sido capaces de crear hasta ahora sea puramente destructiva. Habla elocuentemente de lo que es crear vida a nuestra propia imagen.”- ***Stephen Hawking***

Con esas palabras de uno de los científicos más grandes de la historia humana, iniciamos el cuarto capítulo de esta serie, donde hablaremos de estas interesantes, pero potencialmente destructivas cosas creadas por los humanos: **los virus informáticos.**

¿Qué es un Virus Informático?

Para resumir, un virus informático es un programa malicioso, creado con propósitos negativos, que actúa de manera muy similar a un virus en las personas: se dedica a saltar de un individuo a otro mientras se replica sin control, consumiendo los recursos disponibles y causando estragos en el camino.

Pero, como con muchos virus actuales, hay maneras de combatirlos y (por desgracia para nosotros), hay cientos de ellos y están por todos lados. Esto, es importante destacarlo para no desatar medo de manera innecesaria: ***podemos combatir los virus informáticos***.

Una de las cosas terribles y negativas que ocurren con los virus informáticos, es **lo tristemente rápido que pueden replicarse,** infectando no solamente el dispositivo del usuario si no muchos otros dispositivos, expandiendo el daño, la destrucción y la expansión a la vez de estos virus, sin que el usuario sepa o dé su consentimiento.

¿Cómo puedo infectarme?

Los virus, ***creados con mucho esmero por ciberdelincuentes,*** necesitan de un dispositivo huésped para replicarse y vivir. Para esto, es que normalmente la persona que crea y/o expande el virus, necesita unir dicho virus a algún software legítimo, para infectar a otro. Entre otros, puede unir el virus a archivos de texto, instaladores, enlaces malasios y otras múltiples maneras.

Si tuviéramos que hablar de su ciclo de vida, **podríamos dividirlo en 5 etapas,** pero antes es necesario realizar una aclaración importante: algunos virus quedan latentes, esperando que la víctima realice una serie de comandos especifica y/o ejecute una acción específica. Otros virus, al momento de entrar al dispositivo objetivo, inmediatamente empiezan con el ataque dañino.

Entonces, las fases del Virus serian:

- **Fase de infiltración:** desde el momento que el virus ingresa, mientras permanece oculto entre los archivos del dispositivo, esperando el momento/comando de activación.
- **Fase de expansión:** los virus, antes de ser detectados, necesitan expandirse todo lo posible. Para ello, se clonan sucesivamente. Algunos más modernos, tienden a modificarse levemente para evitar la detección, mientras continúan clonándose a toda velocidad.
- **Fase de explosión o ejecución:** En estos momentos, el virus se activa, liberando la carga útil y negativa, causando el ultimo destello destructivo en el dispositivo.
- **Fase de activación o despertar:** los virus se activan normalmente, luego de una acción o situación específica. Algunos requieren que el usuario de clic en él. Otros se activan cuando se abre el navegador o se reinicia “x” cantidad de tiempo, para distraer el origen de la infección.
- **Fase de detección o eliminación:** en esta fase, los daños ya son elevados en el dispositivo, por lo que es evidente para el usuario que algo va muy mal. A continuación, el usuario lo detecta, lo elimina y recupera el control de su dispositivo.

Los virus informáticos, al igual que los biológicos, son múltiples, de múltiples categorías y cada día surgen nuevos. No tiene sentido vivir asustado por caer en uno de estos, lo importante es ver medidas bajo las cuales podemos protegernos.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

¿Cómo protegernos?

- Nunca es suficiente recalcar lo importante que es mantener un nivel de uso responsable muy elevado.
- Ser precavido es algo muy importante para poder mantenerse a salvo de estos peligrosos programas.
- Evita descargar programas de cualquier sitio, lo mejor es de fuentes conocidas.
- No ingreses a cualquier link que se atraviese, especialmente por mensajes personales o emails.
- Utiliza un buen antivirus.
-

Pero, detectar y eliminar un virus/malware quedará para un próximo artículo.

Espero que este artículo te haya gustado. Recuerda dejarme tus opiniones en mis RRSS.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Python en la Seguridad Informática: ¿Se usa para el hacking?

Si tuviéramos que hablar de un lenguaje con una curva relativamente baja de aprendizaje, con una sintaxis bastante amigable para el programador, multipropósito, seguramente se nos vendría a la mente **Python**.

Y no es para menos. Este lenguaje, en cualquier búsqueda que hagas sobre ***lenguajes más usados, figura entre los primeros.*** Posee una versatilidad diferenciadora y lo podremos encontrar en las industrias más variadas: desarrollo web, desarrollo de videojuegos, inteligencia artificial, machine learning, data science y por supuesto, **seguridad informática.**

Python y la seguridad informática

Si llegaste esperando un tutorial de hacking, **lo tendremos pronto.** Pero en este artículo, vamos a sentar las nociones del por qué se usa en seguridad y, como se usa. Las bases son fundamentales, vayamos paso a paso.

- Una de las ventajas de este lenguaje open source, es **la comunidad**. Esta comunidad colaborativa es responsable de la creación de múltiples herramientas que han servido para diferentes propósitos.
- Otra ventaja que presenta, es ser un lenguaje **interpretado multiplataforma**. No necesitaras mucha complejidad para empezar a desarrollar, ni herramientas demasiado específicas para usarlo de manera general.
- Hay que destacar también, la claridad de su **sintaxis**. En entornos agiles y colaborativos, especialmente donde cada minuto cuenta y genera diferencia, como en seguridad, poder leerlo fácilmente es todo un detalle sumamente importante.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Estas ventajas para los desarrolladores éticos, también representan una ventaja para los **ciberdelincuentes**. En los últimos años reforzaron sus métodos y estrategias, multiplicando el uso de **Python** creando scripts para ataques ddos, ataques de fuerza bruta, inyección SQL y similares.

Como se relaciona Python con hacking

Al ser un lenguaje tan versátil nos ofrece diferentes motivos por los cuales es escogido en seguridad informática:

- Puedes **escanear vulnerabilidades** de tus objetivos
- Podrías **crear keyloggers** para registrar las pulsaciones de teclado de la computadora
- Es posible **desarrollar Ransomware** con este lenguaje
- Permite **automatizar** tareas y crear scripts para auditorias
- Muchas herramientas se crean con Python

Herramientas de Hacking

Una parte muy importante dentro de la seguridad informática, es el área de **hacking**.

Recordemos que es importante potenciar y desarrollar el **lado ético** de esta disciplina, sin olvidar la clasificación de hackers, ***no todos son delincuentes.***

Teniendo esto en cuenta, dentro de las funciones éticas de un **hacker**, ocasionalmente pueden utilizar ***algunas herramientas.*** Mencionaremos 5 de las usadas hoy:

- **Libmap/Nmap**: es una herramienta cuya función principal es escanear los puertos, para verificar cuales están abiertos de nuestros dispositivos.
- **Scapy**: es una herramienta de envío, rastreo y falsificación de paquetes. Cuenta con Wireshark, Nmap, Arpspoof, entre otros escáneres de red, para facilitar sus labores.
- **Cryptogaphy**: herramienta que se centra en propósitos criptográficos
- **Requests/Beautiful Soup**: Este módulo es normalmente usado para crear herramientas en Python. Ayuda a los desarrolladores a enviar HTTP sin codificación, se usa para extraer datos de HTML y XML.
- **Impacket**: es una colección de clases que sirve para trabajar con protocolos de red.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Pronto creare más artículos ***(algunos con ejercicios prácticos)*** para favorecer tu desarrollo profesional dentro del **Hacking Ético.**

Cursos Gratis Online en: https://achirou.com/cursos-gratis
Contenido Gratuito en mis redes: https://achirou.com/redes-sociales
LinkedIn de Gastón Galarza: https://www.linkedin.com/in/gastongalarza/

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

La Nube Volumen I: Introducción

En el mundo actual, pareciera que hay un concepto de moda: **La Nube**. Basta una búsqueda superficial en plataformas educativas y proveedoras de servicios tecnológicos y es común encontrar las palabras **Cloud**, acompañado de múltiples conceptos: **Cloud Computing, Cloud Security, Cloud Storage, etc.**

Pero, realmente ¿Qué es **La Nube**? ¿Es segura? A lo largo de este capítulo intentaremos resolver estas y otras interrogantes, intentando brindarte lo que siempre hacemos aquí: herramientas y conocimiento para tu desarrollo profesional y personal. Y te dejo un curso totalmente gratuito de Introducción a la Nube

¿Qué es La Nube?

Empecemos por lo primero. El concepto de "**Nube**" puede resultar complicado. Si vienes de la época de los '80,'90 seguramente recordaras como fuente de almacenamiento los famosos disquetes. La industria evoluciono, saltamos de ellos a los CD, luego a los Pendrive USB y Memorias extraíbles, discos externos y todo fue, dada la necesidad de tener mayor capacidad de almacenamiento debido **al aumento de tamaño de los datos que consumimos y necesitamos.**

Es que, al fin y al cabo, hablamos de esto: **Datos**. Donde, como y cuando guardarlos. Pero, más importante que lo anterior, viene la duda de cómo mantenerlos seguros, a salvo, incorruptibles e inviolables. Ante esta problemática, la solución que se ocurrió fue la creación de La Nube.

Para explicarlo simple, **La Nube** no es una entidad física accesible directa, si no es una red de almacenamiento de servidores remotos a nivel mundial configurada de tal manera que actué como un único ecosistema.

Puede sonar contradictorio decir que no es una entidad física, sino una red de servidores (obviamente físicos) a la vez, pero no te preocupes, tiene sentido. Piensa en lo siguiente: cuando decides hacer una copia de los videos de tu móvil en tu computadora, conectas el USB y sincronizas los datos.

Evidentemente, accedes ***de manera directa a un único dispositivo físico*** (el HD o SSD que tengas instalado) y sabes que, cuando necesites esos datos, bastara con conectarte al computador y buscar el contenido.Pero, cuando hablamos de **"La Nube"**, ***no tenemos acceso directo de manera física*** al lugar donde almacenamos el contenido. Tendremos que tener acceso vía online al centro de almacenamiento.

Hay, bajo norma general, 4 tipos distintos de Nube:

- **Pública**: las usadas por proveedores de servicios para almacenamiento de datos en gran escala, para compartirlos vía Internet, como Netflix.
- **Privada**: usada para acceso limitado, a veces también por corporaciones, suele almacenarse de manera local, pero permite el acceso a sus empleados, no se comparte de manera libre.
- **Híbrida**: es una nube que comparte información entre privadas y públicas, acorde a la necesidad
- **Comunitaria**: permite solamente que distintas entidades u organizaciones relacionadas, puedan entrecruzar datos con facilidad

Pero, ¿dónde están los datos? Como dijimos antes, esta red de alcance mundial interconectada, hace que tus datos puedan estar en **cualquier parte del globo**, y no necesariamente estén siempre en el mismo lugar. La **ventaja** de esto, es que podrás conectarte en línea desde, donde y cuando tu desees. La **desventaja**, es que a diferencia de tu computador que puedes controlarlo de manera directa, no podrás controlar de manera física el servidor donde este tus datos alojados. Entonces, pasemos a la siguiente pregunta:

¿Es segura?

Bueno, la respuesta a ello es más complicada de lo que parece. Las nubes públicas, son básicamente de acceso a cualquier persona.

Por supuesto, ***no significa que cualquier persona tiene acceso a tus datos,*** para ello cada persona debe crearse una cuenta independiente. Pero,

como vimos en la clasificación, no hay mayores restricciones para su uso.

Esto, evidentemente significa que ingresaran usuarios con buenas y malas intenciones.

Hay toda un área específica, relacionada a Seguridad en **La Nube.** Es un conjunto de ***controles, buenas practicas, normas,*** protocolos, tecnologías y procedimientos que tienen un único propósito: proteger datos, aplicaciones y todo lo relacionado a la gestión de ellos.

Esta área, se enfoca en proteger el acceso a los datos almacenados en esta enorme red. Cuando nosotros, como empresa o persona individual, usamos nube pública, vamos a encontrarnos con estas bases:

- El almacenamiento físico deja de estar bajo nuestra supervisión directa
- Solo pagarás por lo que usas, no tendrás espacio ocioso
- Reducirás costos en tu día a día
- Estarás permanentemente interconectado a otros datos (aunque no tengas acceso a ellos)

Estos factores, resultan claramente ambiguos. No pueden considerarse ni pros ni contras. Ceder el control total de tus datos a terceros, a pesar de que te brinde beneficios económicos, significa que, si algún delincuente lograra acceder a la red interconectada a través de credenciales, tendría claramente acceso a datos de toda la red.

Esto significa, que las buenas practicas que las empresas proveedoras realizan, estarán (o deberían estar) centradas en la seguridad ***EN La Nube,*** no solo en el acceso.

¿Es La Nube siempre la mejor solución?

Nuevamente, la respuesta es **DEPENDE**. Si necesitas acceso a los datos 24/7, siempre, sin importar la circunstancia, quizás la mejor solución sea almacenamiento local.

¿Por qué decimos eso? Imagina que un hospital decidiera recurrir **SOLAMENTE** a la nube como fuente de almacenamiento.

Si se presentara algún inconveniente como un corte de luz general y sostenido en el tiempo, o un cataclismo (digamos, a propósito de este ejemplo extremo, un huracán) que ocasione que **temporalmente** las comunicaciones estén interrumpidas (puede ser en la ciudad donde está el hospital o en el servidor de **La Nube** donde estén alojados esos datos), ese hospital perdería el ***acceso total*** a esos datos hasta que el asunto sea resuelto. Si hablamos de un hospital, donde ***la vida*** de las personas puede depender de ***esos datos,*** evidentemente el asunto es complicado.

Si crees que el ejemplo es muy exagerado, basta recordar el incidente de **Amazon AWS**, con fecha de ***31 de agosto de 2019, en Virginia del Norte, Estados Unidos de Norteamérica.*** Ese día un problema con el suministro eléctrico ocasiono que los servidores permanecieran fuera de servicio un periodo de ***1:45 hrs.***

Pero, lo peor no fue el no poder subir datos o acceder a ellos. Lo peor fue que, según reportes oficiales, la interrupción eléctrica provoco **daños de hardware irrecuperables,** lo que ocasiono que aproximadamente **el 0.5% de los datos** alojados allí, **se perdieran para siempre.** Quizás, el 0.5% no parezca un número elevado, pero, si ese 0.5% fueran ***TUS DATOS MAS IMPORTANTES***,

¿Qué pasaría?

Otro detalle crucial para tener en cuenta, es que, en la mayoría de los **TyC** de los acuerdos, las empresas ofrecen diversas garantías sobre el acceso al servicio, ***PERO NINGUNA GARANTIA SOBRE LA INCORRUPTIBILIDAD DE LOS DATOS.*** Curioso. ¿A qué crees que se deba? Déjame un comentario, al respecto.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

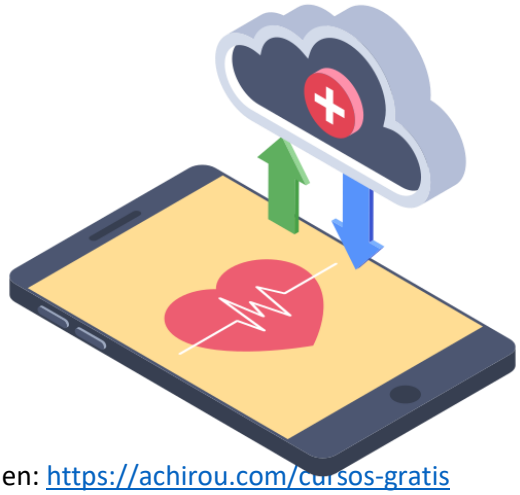
La Nube Volumen II: Medidas de protección

En el artículo anterior tuvimos una introducción a **La Nube**. Estuvimos viendo problemas reales de diversas situaciones que deberías tener en cuenta. Pero, supongamos que decidiste usar servicios **Cloud** como respaldo de tu información personal o empresarial. **¿Qué deberías tener en cuenta?** Te dejo también este curso gratis de "Introduccion a la Seguridad Informatica en La Nube"

A NIVEL EMPRESARIAL

Desde luego, las medidas corporativas y personales comparten principios en común, pero a nivel **corporativo** la cantidad de datos que manejes y el flujo de personas que acceden a ellos será mayor. Dadas estas particularidades, desde acá sugerimos las siguientes cosas a tener en cuenta:

- Ofrecen un **software certificado y reconocido**, con todas las normas de seguridad y calidad (por ejemplo, certificaciones ISO)
- Ofrecen contratos legales superiores a los simples TyC, de preferencia poder firmar un **Acuerdo de Nivel de Servicios (SLA)** que te den ciertas garantías
- Brindan **soporte 24/7**. Es crucial, sobre todo si perteneces a industrias criticas (como la sanitaria).
- Que ofrezcan políticas y reglas claras sobre los derechos de acceso, y medidas **personalizables**, para poder dar mayor seguridad.
- El trato y gestión de tus datos **mientras y después,** de ser cliente.
- Si el proveedor hace **controles periódicos, auditorías externas o tiene prácticas de Hacking Ético frecuente,** para garantizar supervisión frecuente de las vulnerabilidades.



Cursos Gratis Online en: https://achirou.com/cursos-gratis
Contenido Gratuito en mis redes: https://achirou.com/redes-sociales
LinkedIn de Gastón Galarza: https://www.linkedin.com/in/gastongalarza/

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

A NIVEL PERSONAL

- Procura utilizar **contraseñas de +8 caracteres,** mezclados entre mayúsculas, minúsculas y símbolos (por ahora, las contraseñas con estas condiciones o superiores han demostrado ser relativamente seguras)
- No subas i**nformación demasiado detallada, sensible o que pueda ser usada en tu contra**, o que puedas necesitarla para salvar tu vida. Recuerda, los datos pueden desaparecer allí.
- Utiliza el **cifrado** como herramienta:
  -si puedes utiliza **cifrado de extremo a extremo**
  -opta por cifrar los datos **antes de subirlos** y mantén las claves de cifrado a buen resguardo y **nunca** en el mismo lugar donde guardes los datos
- Revisa todas las medidas de seguridad, no dejes las que vienen por defecto, **profundiza y personaliza** los controles y medidas.
- Activa el F2A(factor doble de autentificación o **autentificación en dos pasos)**, si te da la opción.

PARA AMBOS NIVELES

- **Limita el acceso** a la información, algunos proveedores te dan posibilidad de crear distintos perfiles, así que configura los accesos y permisos en estos perfiles. No todos deberían tener acceso a todos los datos, menos aún a editar o eliminar los mismos.
- **Realiza Backus o copias de seguridad frecuentes** y no las guardes en el mismo lugar ni empresa.
  Opta ***o por tener copias locales o utilizar otro proveedor que NO use*** la misma infraestructura del primero
- **Usa todas las herramientas que puedas (y te provean)** para asegurar que tienes control total: ***anti spam, anti spyware, antivirus, anti malware, firewall correctamente configurado, etc.***
- **Se responsable y consciente** (y enseña a las personas a tu alrededor a serlo), en el uso de la información, los datos y La Nube.

- Haz **revisaciones periódicas de los servicios que posees**, controla y elimina aquellos que no uses.

CONCLUSIONES FINALES

La nube en si, como vimos, no es la herramienta definitiva ni representa necesariamente la mejor opción para solucionar tus problemas. Analiza si realmente es conveniente recurrir a un servicio **Cloud**, analiza la empresa y analiza tu comportamiento y el de tu entorno.

Algunas cosas que podrías consultarles serian:

- ***¿En qué ubicación física mantendrán mis datos?***
- ***¿Dónde y cada cuanto realizan copias de seguridad?***
- ***¿Qué política tienen sobre el resguardo y mantenimiento de los dispositivos y los datos?***
- ***¿Realizan actualizaciones de software, hardware y auditorías externas con frecuencia?***
- ***¿Qué políticas tienen sobre la conservación de datos después de la finalización del contrato?***
- ***¿Qué tan personalizada es la atención hacia mi empresa/persona en caso de tener emergencias?***

Teniendo estas cosas en cuenta, veras que ***una buena gestión*** de almacenamiento de datos, parte por una buena gestión de selección del proveedor. Hay muchas opciones en el mercado, elige **la que mejor se adapte a tus necesidades** y recuerda, no siempre economizar es buena idea, pero tampoco es real que lo más caro es siempre mejor.

No olvides el backup ;)

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Informática Forense

¿Qué es? ¿Cómo funciona?

Dentro del maravilloso mundo de la Seguridad Informática, las áreas de trabajo son variadas. Una de las áreas que se destacan por ritmo dinámico de trabajo y por el tipo de contenido que se realiza, es la dinámica forense. Pero ¿En qué consiste? ¿Cómo se realiza? Te dejo este curso gratis de Introducción.

Que es la Informática Forense

Es el conjunto de procesos enfocados a ***obtener, recolectar, preservar, analizar y presentar*** información electrónica guardada en dispositivos electrónicos de pruebas legamente admisibles para las autoridades de determinado país.

Es normalmente aplicada como **oposición** a la gestión de las organizaciones delincuenciales. La mayoría de los crímenes realizados hoy, debido a la interconectividad tan elevada que tenemos, dejan una huella cibernética: imágenes, videos, audios, textos.

Estas prácticas de **ciberseguridad** permiten detectar, encontrar y analizar diversas pruebas relacionadas a los delitos, lo que permite ampliar la cantidad de pruebas obtenidas en circunstancias diversas.

Como rama de la **seguridad informática**, tiene distintas técnicas, tácticas y métodos, pero todos apuntan a los mismos propósitos: **obtener evidencias de manera incorruptible e inalterable,** para facilitar los procesos legales.

Tomando estos detalles en cuenta, nos quedan claras dos cosas importantísimas:

- ***en primer lugar***, la informática forense puede ser considerada una disciplina “auxiliar” totalmente ética de la Justicia Estatal;

- ***en segundo lugar***, deducimos que, como profesionales de la seguridad informática, sería muy importante poder aprender la mayor cantidad de técnicas para resolver problemas de índole diversa, recuerda que la delincuencia no duerme.

¿Funciona?

En los últimos años, **múltiples casos** fueron resueltos con colaboración de esta disciplina. Personas inocentes pudieron demostrar su ausencia de delito gracias al análisis de sus dispositivos, y muchos culpables fueron capturados por los patrones de escritura, mensajes o videos que había en sus dispositivos.

En los procedimientos legales de hoy, no es extraño leer que se usan los dispositivos de los acusados para resolver los detalles pertinentes o **aportar la evidencia necesaria** para la resolución.
Las maneras de proceder, permiten que, dentro de los márgenes esperables, la información sea **almacenada, recolectada y analizada** de manera bastante parcial. El detalle crucial es que los análisis y pruebas se realizan siempre sobre las copias obtenidas de los datos disponibles.

Los datos originales de los dispositivos obtenidos en evidencia, y los dispositivos como tal, deben quedar **totalmente inalterables y a resguardo**, para evitar que sean corrompidos.

Por todo lo mencionado, obviamente necesitaremos que el dispositivo y la información queden intactas, por lo que a veces, este camino de búsqueda de evidencias se encuentra con trabas conocidas normalmente como ***"informática anti-forense",*** un conjunto de prácticas que tiene el propósito de entorpecer posibles búsquedas a futuro de procedimientos judiciales. Prácticas como **sobre-escritura de datos, ofuscación de código o destrucción de datos** son solo algunas de las que se intentan usar.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

¿Cómo se realiza?

Básicamente se sigue una línea de tiempo relativamente similar:

1. Se **recopila** la mayor cantidad de datos relacionados al suceso en orden, teniendo en cuenta la posibilidad de destrucción de datos (como al cerrar sesión o reiniciar los dispositivos)
2. Se realizan **copias** de los datos contenidos para pasar a mantener bajo custodia segura los datos. Mantener este procedimiento detallado, permite mostrar en el procedimiento judicial, que los datos permanecen íntegros, para que el análisis pueda ser considerado evidencia valida.
3. En algunas copias realizadas, se realizarán diversos **análisis** utilizando técnicas y herramientas variadas, intentando obtener las evidencias necesarias para trazar comportamientos, contactos realizados o patrones establecidos que permitan encontrar la relación entre el individuo y el crimen que se cometió.

Con toda la información disponible, el forense analiza la información y arma un informe que intentara resolver preguntas como estas:

- ***¿Qué fue lo que ocurrió?***
- ***¿Qué programas, sistemas o dispositivos están involucrados en la situación?***
- ***¿Quiénes son los propietarios?***
- ***¿Para que usan estos dispositivos, con qué nivel de información sensible y critica?***
- ***¿Cuál es el probable daño o delito que se realizó con esto?***

Este informe presentado de manera objetiva, **se realiza de manera clara y concisa**, pensando en ser presentado a personal ajeno a la tecnología.
Como vemos, en esta disciplina es crucial tener una ***ética y normas morales elevadas, además de elevados conocimientos técnicos,*** dado que los datos pueden verse afectados por manipulaciones delincuenciales para distorsionar los sucesos.

¿Te gustaría revisar algunas herramientas que se usan en **Informática Forense?**

Déjame un comentario en el canal así podemos hacer un video relacionado a ellas.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Historias de Hackers, Episodio I

El Fantasma de los Cables

A lo largo de la historia de la tecnología, distintas personas desarrollaron habilidades y actividades increíbles en el mundo de la **Ciberseguridad**. En este artículo conoceremos a uno de ellos que, aunque empezó en el lado criminal, reacomodó su vida y se convirtió en un increíble aliado del ***lado ético de la Seguridad Informática.***

Qué son los hackers

El término **Hacker**, normalmente se usa para englobar a todas las personas que realizan actividades cibernéticas delictivas, pero ***no es así.*** Un hacker es un **profesional de la seguridad informática** que posee avanzados conocimientos y experiencia para realizar diversas cosas en relación a dispositivos, entornos o sistemas, con el propósito de provocar cosas distintas de su propósito original o evaluar el comportamiento de determinado sistema sometido a presión.

Hay aquellos que tienen predilección por las actividades delictivas, llamados normalmente **Black Hat**, y hay otros con una ética y moral desarrollada que trabajan del lado de la ley, llamados **White Hat.**

Hay otras categorías, como **Red Team, Blue Team, Green Hat, Grey Hat**, pero a estas categorías las analizaremos en profundidad en otro artículo. En este conoceremos a uno que empezó como Black Hat, pero hoy se destaca por sus habilidades del ***lado del hacking ético.***

El Fantasma de los Cables

Kevin Mitnick, nacido el 6 de agosto de 1963 en EEUU, es un profesional de seguridad informática, desempeñándose hoy como consultor con un fuerte en la ingeniería social, muy conocido en la industria por múltiples episodios relacionados a él.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Cuando tenía 12 años se enfrentó a los primeros cambios y dudas en su vida. Noto que el transporte público que utilizaba a diario funcionaba en base a tarjetas perforadas para los viajeros.
Gracias a esto se le ocurrió la idea de que **contando con su propio perforador** podría viajar por la ciudad libremente.

Obtuvo uno de estos aparatos perforadores y tarjetas de viaje y gracias a ello pudo dedicarse a realizar sus viajes sin gastos. A los 16 años tuvo su episodio como "**hacker**" al entrar sin autorización al sistema administrativo de su escuela, solo para "ver cómo funcionaba" y por, sobre todo, si podría realizarlo.

Poco tiempo después, accedió de manera ilegal a la red Ark, de la compañía Digital Equipment Corporation, lo que le dio 12 meses de prisión un par de años después del hecho. Poco tiempo después de salir de la cárcel, accedió a la red de Pacific Bell, para obtener códigos de activación telefónica e información múltiple de la empresa. Los datos sustraídos, se supone, tenían un valor de **$US 200.000. Desde 1982** en adelante, múltiples empresas fueron atacadas por él. El North American Air Defense Command, Microcorp Systems en 1987, redes, sistemas, centrales telefónicas, etc.

Mientras era buscado por las agencias gubernamentales, incluso cometió falsificaciones de licencia de conducir y similares. Su historia parece una película de acción: ***persecuciones con helicóptero y un ser fantasma que desaparecía en cuestión de horas o, directamente, era irrastreable.*** Con el auge de los dispositivos móviles (o celulares), las dificultades para encontrarlo fueron aún mayores, dado que con sus conocimientos simplemente escapaba del control de las autoridades.

Caída y resurgimiento del Cóndor Fantasma

El **Fantasma de los Cables**, como decidió autodenominarse, o **Cóndor**, como le decían otras personas, encontró el inicio de su caída definitiva en 1994.
Ingresó al computador de **Tsutomu Shimomura,** un físico computacional, experto en seguridad informática pero además **White Hat**, al que desde luego no le hizo mucha gracia. Este hacker ético se propuso como meta personal, capturarlo.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Empezó a rastrear los movimientos de Mitnick, lo que lo llevo a encontrarlo en relaciones ilegales directas (o sea, las había hackeado) con empresas de telecomunicaciones, a saber, **InterNex, The Well y Netcom.**
En conjunto con ellas y habiendo dado notificación al **FBI**, empezaron a acorralar a Kevin, mientras monitoreaban sus actividades, basadas entre otras, en crear múltiples claves de acceso con contraseñas random, pero en cuentas con permisos de uso avanzados en las tres empresas.

El **16 de febrero,** el Fantasma se había convertido en un ser real, y atrapado. Ese día, se llevó a cabo su arresto. Pero, Kevin tenia preparados ciertos trolleos para su "amigo" Tsutomu. Durante la noche del 15 de febrero y primeras horas del 16, estaban supervisando permanentemente sus dispositivos y comunicaciones. **Tsutomu descubrió movimientos inusuales** desde el dispositivo de Kevin, en la red de comunicaciones. Nadie sabía que ocurría, hasta que horas después del arresto de Kevin, cuando Tsutomu llega a su domicilio encuentra una serie de mensajes con tono asiático, enviados por Kevin en tono de burla, ante la inminencia de su arresto. Pero, eso no era todo. ***8 horas después del arresto*** y antes que la voz se corriera, mientras Kevin permanecía en custodia e imposibilitado de comunicarse, ***Tsutomu recibiría una llamada en su domicilio con tono de burla.***

La voz era clara e inconfundible: **Kevin estaba burlándose una vez más.** Hubo otra señal enviada por Kevin durante la madrugada del 16 de febrero, pero nunca se descubrió el destino de ella.

La leyenda del muchacho superaba la coherencia, y el miedo que despertaba era superior a la lógica.

Creían que solo a través de silbar o decir palabras a través del teléfono, podría activar la red de misiles nucleares NORAD, así que para evitar eso, un juez le dicto 46 meses de sentencia, de los cuales ***los 8 primeros, los pasaría en aislamiento total.***

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Años después de su liberación, ya reformado, se dio cuenta que, del lado ético, podría seguir realizando sus actividades, pero ahora para ayudar a otras personas y proteger a indefensos. Gracias a eso decidió crear su propia empresa de seguridad, **Kevin Mitnick Consulting,** dedicada a la consultoría sobre ingeniería social y pruebas de pentesting e intrusión a corporaciones.

Y tu ¿Qué opinas del Cóndor? Déjame tus comentarios en mis canales.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Grave déficit de profesionales de Ciberseguridad a nivel mundial

Imagina una enorme guerra entre el bien y el mal. La batalla es larga y permanente. Pero, mientras las fuerzas del mal aumentan sus filas permanentemente, las fuerzas del bien poco a poco reciben cada vez menos guerreros. Si tuviéramos que contar de manera sencilla el panorama actual de la **seguridad informática,** sería muy parecido a la oración inicial.

Con el auge de la tecnología, la mayor disponibilidad y expansión de los medios tecnológicos, los frentes de batalla se multiplicaron: ***videojuegos, dispositivos móviles, computadoras, relojes***… hoy, la tecnología está presente en cada campo de la vida, al alcance de todos. A causa de esto, los lugares posibles de brechas son cada vez mayores, y mayores las posibilidades de atacar a alguien.

Esto nos deja con una necesidad urgente: mayor cantidad de profesionales de la seguridad informática dispuestos y disponibles para trabajar de manera exitosa repeliendo y auxiliando cada posible vulnerabilidad o brecha en el **mundo IT.** El problema radica en que no es tan fácil encontrar a los que puedan solucionar estas dificultades.

¿A qué se debe el déficit?

Los factores son diferentes y múltiples, pero veamos algunos de ellos:
La universidad: los planes desactualizados de formación profesional, ocasiona que cada persona, apenas se gradúa, se encuentre varios años atrasado a nivel tecnología (y más en ciberseguridad). Esto significa que, el profesional deberá seguir formándose de manera inmediata, ***para estar aun así atrasado a los ciberdelincuentes.***

Además de lo mencionado, en América Latina el acceso a la universidad no es para todos. Los gastos que ocasiona y la dificultad de costearlos, además de matrículas y mensualidades, obliga a muchas personas a optar por trabajar fuera de la universidad.

El tiempo: El proceso de formación de una persona, hasta que domina las áreas de IT (y seguridad informática), tiende a ser largo y agotador, aunque apasionante. Nada se aprende en cuestión de horas, lo que motiva que muchas personas por diversos factores, deban abandonar sus estudios (formales o no).

El alcance: la seguridad informática esta ***(o debería estar)*** presente en cada uno de los aspectos de la vida diaria de una empresa. Esto, por supuesto, nos expone a mayores cantidades de posibles problemas. Por otro lado, ***muchas personas ajenas al mundo de IT tienen una resistencia al cambio y no le dan la seriedad debida ni toman con la seriedad que se merece*** los asuntos relacionados a la seguridad, lo que complica y vuelve más lento los procesos de creación de medidas de seguridad.

Requisitos absurdos: muchas empresas buscan ***auténticos unicornios***, prefieren dejar puestos vacantes que contratar a personas con conocimientos medios y capacitarlos. Eso obliga a los profesionales a buscar más contenido profesional que demanda más tiempo, para conseguir puestos iniciales.

Necesidad urgente: muchas otras empresas, ofrecen a estudiantes de primeros ciclos, pasantías rentradas y trabajo permanente luego, lo que ocasiona que muchas de ellas no concluyan su formación (aunque si eres de IT, sabes muy bien que **somos autodidactas por excelencia).**

Brecha actual

Las cifras varían, pero todas coinciden en lo mismo: **la necesidad de profesionales capacitados es alarmante**. Diversos estudios muestran que los expertos en **Red Team y Blue Team (entre otras áreas)** necesarios rodean los 4 millones aproximadamente.
4 millones de puestos vacantes. Esta tendencia no tiene miras a solucionarse al corto plazo. Hay una sola alternativa para esto: capacitarse, estudiar y avanzar. Recuerda que, en mi sitio, en la sección **“**Rutas de Aprendizaje**”,** encontrarás rutas completas del **Red Team** y el **Blue Team.** Es una buena oportunidad para profesionalizarse.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Latinoamérica y el mundo, en Peligro

Durante 2020, la vida de la sociedad a lo largo de todo el planeta, afronto grandes cambios. Uno de los más notables, fue el auge del uso de la tecnología a gran escala. Todos, suponíamos que eventualmente nuestras vidas estarían mucho más regidas por la tecnología, pero la pandemia global aumento los tiempos de implementación.

Esto, ocasionó otro problema gravísimo: **el aumento absurdo de la ciberdelincuencia.** Esta terrible problemática, unida a la falta de profesionales en la industria a nivel global ocasiono resultados desastrosos.

El Ransomware sigue invicto

Varias empresas a nivel internacional, se dedican a realizar estudios de acuerdo a las influencias de distintos tipos de malware y el impacto en la sociedad. Uno de los que se mantiene ya hace varios años en el Top 3(y, de hecho, primero), en ranking de daños y amenazas, es **el Ransomware.**

En el 2020, fueron varios los países, ciudades y empresas que se vieron afectadas por ataques de diversos Ransomware, causando daños económicos e incluso arriesgando la vida de personas en el proceso. América Latina no podía ser la excepción: desde centros gubernamentales hasta grandes cadenas de comercio, ***los ataques se repitieron con velocidad por doquier.***

El Problema en América Latina

Los países latinoamericanos, como todos sabemos, se caracterizan por vivir tiempos económicos y sociales complejos. La crisis económica y humanitaria en varios, es agobiante. Esto, como es de suponer, hace que la región se caracterice por tener inversiones a nivel general, más bien escasas.

Por supuesto, la seguridad informática no iba a ser la excepción. Tanto empresas como estados, prefieren darles prioridad a otros aspectos y ***desplazar la ciberseguridad a lugares secundarios.***

Cursos Gratis Online en: https://achirou.com/cursos-gratis
Contenido Gratuito en mis redes: https://achirou.com/redes-sociales
LinkedIn de Gastón Galarza: https://www.linkedin.com/in/gastongalarza/

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Esta decisión, desde luego, tendría consecuencias devastadoras. Los informes actuales, indican los siguientes números:

- En América Latina, **se registraron 41 MIL MILLONES** de intentos de ataques (muchísimos de ellos, exitosos).
- Alrededor del **70% de los ataques se dirigen a empresas,** el 30% restante impacta en personas
- **El Ransomware y el Pishing** son los favoritos de la ciberdelincuencia, aunque los otros tipos se utilizan igualmente

Las técnicas de la ciberdelincuencia, están avanzando a pasos agigantados. Ahora, con el auge de la **Inteligencia Artificial, Machine Learning y similares**, los ciberdelincuentes tienen en sus manos una gama mayor de herramientas para coordinar y realizar ataques. Esto, unido a las tan famosas prácticas de Ingeniería Social, hace que los ataques sean cada vez más complejos y difíciles de detectar. Esto, unido al analfabetismo tecnológico, expone a millones de personas a riesgos elevados e impensados en su vida diaria.

El otro factor preocupante, ***son las vulnerabilidades***. ¿Por qué decimos esto? Con el auge de IoT y la necesidad de la conectividad para trabajadores en remoto, los ciberdelincuentes intentan explotar todas las vulnerabilidades posibles, para conseguir beneficios económicos a costa de las personas.

Si tomamos en cuenta que, las pérdidas por distintos ataques a nivel mundial representan un aproximado de $1 MIL MILLONES de dólares (lo que equivale al 1% del PBI MUNDIAL), evidentemente nos encontramos con un oscuro negocio más que lucrativo.

Es por ello que, hoy más que nunca, la necesidad de formación de más profesionales en ***Seguridad Informática es urgente y debería ser prioritario.*** Recuerda que tengo una sección de cursos y rutas completas, para que puedas unirte al lado ético de la batalla.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

IoT: un nuevo reto de Seguridad Informática

Con el auge de las nuevas tecnologías, la sociedad en general gira hacia una mayor necesidad de conectividad y, por supuesto, un mayor alcance. Hoy en día, las personas y empresas, utilizan múltiples dispositivos que se conectan entre ellos o a internet.

Esto, desde luego, plantea toda una gama de nuevos retos para los profesionales de la seguridad informática, que ahora deben lidiar con frentes cada vez más amplios y variados. Los problemas se agravan al notar que, a causa del contexto de pandemia actual, las tendencias del teletrabajo son una realidad cada día de mayor alcance.

IoT en crecimiento

Con el anuncio de la ***tecnología 5G y el WI-FI 6,*** la cantidad de dispositivos relacionados a IoT crecerá a ritmos increíbles. Diversos análisis estiman que ***para 2025 habrá 21.500 millones de dispositivos IoT a nivel mundial.***

Por diversos motivos, entre ellos la practicidad, las empresas están empezando a usar dichos dispositivos, en variadas circunstancias, pero compartiendo varias cosas en común: la cantidad de datos sensibles que se transmiten entre ellos. Y, como bien sabemos, los datos equivalen a dinero. En realidad, ***los ciberdelincuentes transforman esos datos, en dinero de manera ilegítima.***

Los riesgos de los datos

Las condiciones generales de **IoT** son sumamente complejas, y los entornos o ecosistemas, muy variados. Básicamente, casi todos los dispositivos que componen un sistema IoT, ***pueden recibir, transmitir y generar datos sobre sí mismos, sobre el entorno, sobre los usuarios y sobre las características de uso.***

La integración y usos de IoT en la vida diaria, es profunda. Con el auge de la tecnología **Blockchain**, múltiples empresas brindan soluciones con dispositivos interconectados basados en esta.

Otras, utilizan sensores inteligentes que permiten ampliar el alcance de adquisición de datos.

Las mismas vulnerabilidades de siempre

Mientras que se expande el uso y consumo de estos sistemas, nos encontramos con nuevos desafíos y viejas problemáticas. Es normal que, en estos entornos, convivan dispositivos totalmente diferentes, con capacidades y formas de interactuar distintas, lo que **supone un reto al momento de plantear estándares de manejo generalizados.**
Una de las graves problemáticas que se enfrentan (y uno de los principales problemas) pasa por el mismo dispositivo IoT. Ocurre con frecuencia, que, por inexperiencia o impericia, se retrasan las actualizaciones del firmware de cada uno, lo que deja el dispositivo susceptible a ataques o malfuncionamiento.

Por otro lado, tenemos el mismo punto débil de siempre: **el factor humano**, con sus múltiples falencias:

- Mal uso de contraseñas
- Dispositivos con configuraciones erróneas o deficientes
- Servicios innecesarios, susceptibles de ser vulnerados
- Conexiones externas sin factores de verificación o autentificación
- Mala gestión de la información personal

- Poco o nulo control de acceso a dispositivos susceptibles o claves

Para concluir, tenemos **errores desde una mirada empresarial y corporativa:**

- Dispositivos que cumplen su función, con amplias falencias, pero más económicos
- Poca capacitación del personal afectado
- Toman medidas reactivas y no preventivas, en seguridad informática

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

- Ven a la seguridad no como eje, si no como elemento alternativo
- Poca claridad en roles y responsabilidades
- Como hacer frente a la situación
  Cada empresa o persona evaluara lo que considere mejor para desenvolverse en diversas situaciones, pero desde acá consideramos que las siguientes sugerencias deberían aplicarse para reducir posibles riesgos:
- Darle un lugar prioritario a la gestión integral desde una mirada de seguridad informática amplia
- Controlar periódicamente los dispositivos, el ciclo de vida y el desempeño de acuerdo al rol para el cual se lo necesita
- Contar con personal profesional (y desarrollar planes de capacitación y actualización continua), para permitir a los mismos, estar mejor preparados para sobrellevar diversas amenazas.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Como adquirir experiencia en Seguridad Informática: Retos CTF

Informática tiene una particularidad extendida: si no prácticas, no aprendes. El contenido teórico es amplio y los campos de acción son vastos, pero si no metes manos a la masa, se vuelve muy difícil conseguir profundizar el nivel como profesional. Hoy hablaremos de una forma de adquirir habilidades: **los retos Capture The Flag (CTF).**

Qué son

Los retos de **Captura la Bandera**, a grandes rasgos, se caracterizan por enfrentar a equipos que luchan entre ellos en diversos retos, con el objetivo de capturar algo (una "bandera"), demostrando así las habilidades de "hacking" que se poseen. Estas "banderas", son código que, de obtenerlos primeros, nos otorgan una serie de puntos máxima. De hacerlos segundos, o terceros, el puntaje será menor.

Por supuesto, el premio esta directamente relacionado a la complejidad del tema en cuestión y al puesto que tengamos al obtenerlo. Mientras más difícil el reto, y mejor posicionados estemos, **mayor será el premio.**

El juego lo gana normalmente quien más puntos adquirió, pero el problema es que los **CTF** son limitados por tiempo. Pueden durar desde algunas horas hasta varios días, pero no son ilimitados.

Varios ocurren los fines de semana, así que, si vas a sumarte a uno, asegúrate de disponer de tiempo libre y prepárate para manejar la situación.

Para qué sirven

Las modalidades de los retos CTF son amplias, pero destacaremos dos (los más usados):
El Jeopardy: modo todos contra todos. Se plantean situaciones para que todos los grupos ataquen de la manera más rápida posible la situación. El equipo que

logre obtener la mayor cantidad de puntaje en el menor tiempo posible, gana el reto.
Modo Versus o Attack-Defense: en este tipo, cada equipo debe proteger sus servidores de ataques, a la vez que ataca servidores de equipos rivales. Ganará el reto quien más servidores logre romper repeliendo la mayor cantidad de ataques. Normalmente cada servidor conseguido otorga puntos, mientras que cada vez que te atacan con éxito, te quitan puntos.

Si bien el principal propósito es ganar, es una excelente oportunidad para profundizar en conceptos o aprender nuevos. Las temáticas suelen ser variadas, de acuerdo a los organizadores e incluso dentro del mismo juego, puedes necesitar disponer de variados conocimientos. Normalmente las áreas que tendrás que resolver son:

- Criptografía
- Esteganografía
- Hacking Web
- Análisis Forense
- OSINT
- Exploiting
- Reversing
- Pentesting
- Programación

Si quieres profundizar en tus conocimientos o aumentar tus habilidades, es una excelente oportunidad para hacerlo.

¿Que necesito para realizarlos?

Lo fundamental: tiempo. Luego necesitarás conocimientos (dependiendo el nivel del reto), que podrán ir de básicos a avanzados. A continuación, una computadora preparada para ello. Te recomendamos utilizar una con SO Linux, aquí te menciono las distribuciones que pueden facilitarte el reto:

- **Backbox**
- **Kali Linux**
- **BuqTraq**
- **Parrot Security OS**
- **BlackArch**

Luego de esto, necesitarás verificar la posibilidad de que existan retos activos. Te dejo una recopilación de sitios que conseguimos en múltiples lugares

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

- **Ctf365**
- **Natas**
- **Overthewire**
- **Hacking-Lab**
- **Pwnable.Kr**
- **XSS Games**
- **Io**
- **Smashthestack**
- **Microcorruption**
- **Reversing.Kr**
- **Hack This Site**
- **W3challs**
- **Pwn0**
- **Puzzles!**
- **Exploit Exercises**
- **Ringzer0 Team Online Ctf**
- **Crackmes**
- **Hellbound Hackers**
- **Try2hack**
- **Hack.Me**
- **Hackthis!!**
- **Enigma Group**
- **Google Gruyere**
- **Hack The Box**
- **Game Of Hacks**
- **Root Me**
- **Ctftime**
- **Pentesterlab**

Ahora, todo queda en tus manos.
¿Ya decidiste ponerte manos a la obra? Seguramente nos encontraremos en algún reto. ¡Te veré pronto!

Cursos Gratis Online en: https://achirou.com/cursos-gratis
Contenido Gratuito en mis redes: https://achirou.com/redes-sociales
LinkedIn de Gastón Galarza: https://www.linkedin.com/in/gastongalarza/

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Pentesting: Ideal para evaluar tu empresa

Los ciberdelincuentes se actualizan de manera permanente, buscando como conseguir dinero. Pero desde luego, no se caracterizan por su pasión por el trabajo duro y decente. Al contrario, son oportunistas: ***aprovecharán brechas, descuidos y vulnerabilidades en tu empresa o equipos para poder obtener recursos con los cuales extorsionarte o venderlos para obtener dinero fácil.***

Para evitar esto, los hackers de sombrero blanco y otros expertos en seguridad informática, desarrollan habilidades igualmente ofensivas pero con características éticas. Una de las estrategias usadas, es la que veremos hoy: **el Pentesting.**

En qué consiste

Los hackers éticos, desarrollan estos **Test de intrusión** que tiene como eje central, intentar ingresar a los sistemas de tú empresa. Por supuesto, al ser un servicio brindado por profesionales, ***se negocian a nivel contractual los alcances del "ataque", donde tu determinas hasta donde y en que partes se podrá realizar el análisis.***

El hacker, intentará ingresar a tus datos con el firme propósito de evaluar la resistencia y el comportamiento del sistema sometido a presión, para luego en un informe asentar las recomendaciones de protección ideal en vista de los defectos que se encuentren.

Un detalle a destacar es que ***cada Pentesting es único,*** debe ser personalizado en función de las necesidades y características del entorno o empresa a evaluar.

Hay que entender que los hackers éticos ***intentarán simular de la manera más cercana y precisa posible, un ataque de hacking real en manos de ciberdelincuentes.*** Por esto, es que las condiciones contractuales deben ser claramente definidas de acuerdo a un análisis especifico de la empresa y sus colaboradores, para detectar de mejor manera posibles puntos de ingreso.

Etapas Principales

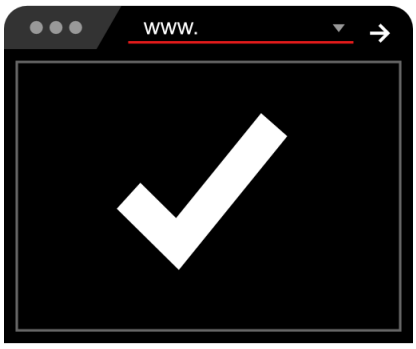
Análisis: esta etapa, recibe distintos nombres de acuerdo al equipo. Puede ser llamada planificación o evaluación, pero el objetivo es el mismo: evaluar la situación y establecer las metas. Esto, es por escrito, en el contrato entre ambas partes, donde se detallará:

- Necesidad a cubrir/evaluar
- Objetivos que se pretenden alcanzar
- Limite y alcance del ataque
- Duración del ataque
- Consentimiento y conocimiento explícito del ataque

Detección: el equipo de intrusión, analizara la estructura completa de la red o el sistema a evaluar. Con esto, encontrará servidores, equipos, herramientas de seguridad, aplicaciones e incluso algunos test localizan las clases de usuario que tiene el sistema (usuario, súper usuario, administrador, etc.).
Las herramientas que pueden usar para esto, son variadas y dependen de múltiples factores. El propósito de esta etapa es encontrar vulnerabilidades, debilidades y fallas conocidas y comunes, o particulares.

Intrusión: esta etapa, llamada también ataque o test, es el momento en el cual el equipo, con lo adquirido en la etapa anterior, se centra en intentar entrar al sistema, aprovechando el conocimiento adquirido. El ataque tiene múltiples formas de llevarse a cabo y es crucial que este tipo de test se mantengan lo más discreto y confidencial posible. Alertar a los miembros de la empresa de que sufrirán un ataque, se aleja de la realidad y puede manipular los resultados finales.

Informe: llamada también reporte, es el momento en el cual el equipo de hackers éticos presenta sus conclusiones finales sobre la situación general. Este informe lleva un resumen detallado de las actividades realizadas, las vulnerabilidades halladas, el grado critico de las mismas y cómo afecta de manera global y específica a la empresa.



Errores frecuentes

Evaluar de manera general a una empresa, no es tarea fácil. A causa de ello, pueden ocurrir diversos errores debido a inexperiencia o falta de un correcto análisis.
Entre los errores más frecuentes podríamos encontrar los siguientes:
Informes defectuosos o deficientes: Es crucial que el equipo de intrusión realice informes lo más completo y detallados posibles, pero orientados a gente de IT, así que deberían ser redactados con lenguaje sencillo y claro. Normalmente las personas que toman las decisiones en las empresas, poseen poco conocimiento técnico, pero son los que deciden realizar cambios.
No realizar un informe óptimo, impactara de manera directa en las consecuencias de la empresa, de los usuarios y del contenido o los datos que manejen.

Errores de priorización: En ocasiones, debido al conocimiento que posee el pentester, suele ocurrir que los ataques se dan en base al fuerte del hacker y no en base a lo realmente preocupante. No profundizar debidamente con el cliente sobre los propósitos de esto, puede ocasionar graves fallos de interpretación.

Técnica y tecnología obsoleta: Los cibercriminales están a la vanguardia siempre. Usar técnicas obsoletas o tecnología que ya quedo fuera de vigencia, puede dar resultados erróneos, mostrando en el informe una empresa segura cuando podría ser todo lo contrario. Es necesario que los profesionales éticos estén al tanto de los nuevos avances para ser más efectivos en su rol.

No es necesario recordar que este tipo de pruebas deben permanecer confidenciales totalmente. Los profesionales de seguridad informática deben caracterizarse por su ética y moral férrea, para poder manejar información confidencial y no usarla para dañar.

Ventajas de realizar Pentesting con frecuencia

Algunas ventajas que puedes encontrar, son:

- Permite a las empresas establecer mejores medidas de seguridad
- Auditar el nivel de cercanía con estándares y certificaciones de seguridad
- Asegurar que la empresa puede seguir siento competitiva con el estándar alto en el mercado
- Analizar el verdadero nivel y alcance en áreas de seguridad informática de la empresa

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Desde aquí, te recomendamos que realices prácticas de Pentesting con frecuencia en tu empresa para evaluar y corregir las cosas que sean necesarias.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Herramientas para Seguridad Informática

Te traemos una recopilación de herramientas totalmente gratuitas de ambas ramas para que puedas potenciar tu desarrollo profesional. Recuerda que, ***si no sabes usar estas herramientas, en mis formaciones profesionales aprenderás a usarlas.***

Pentesting

Una de las partes importantes al hacer **Pentesting** es detectar las vulnerabilidades en el sistema del objetivo, para poder evaluar sus vulnerabilidades y establecer las mejores estrategias a futuro. La mejor forma de hacer esto, es utilizar diversos escáneres de vulnerabilidades para facilitar tu trabajo. ***Un escáner es un software creado para detectar cualquier vulnerabilidad que pueda tener un sistema, edificio o red de manera automática.***

(Dale Click a la imagen, podrás ver las fases de forma gráfica)

Aquí te dejamos la recopilación de algunos gratuitos y bastante útiles.

- **Nmap**: Este escáner es un clásico dentro de las herramientas más conocidas. Potente, multiuso y relativamente sencillo de manejar, te permite detectar host dentro de una red local, descubrir otros hosts en Internet parta ver si están conectados a esta red, permite encontrar que sistema operativo usa un host especifico, que firewall tiene e incluso escanear puertos para detectar algún proceso que se esté ejecutando por fuera del firewall.

Las mejores partes del Nmap son que es OpenSource, con una interfaz clara e intuitiva llamada **Zenmap** e incluso, usando scripts **NSE** disponibles en múltiples lugares, podremos potenciar el alcance de Nmap para aumentar el alcance de sus funciones.
Entre las cosas que podrás realizar, son atacar servidores **SSH**, **FTP** y **Samba**, además de escanear múltiples vulnerabilidades de público conocimiento.

- **Nikto**: una poderosa herramienta que, a diferencia de muchos escáneres, el nivel de detalle en los resultados de los escáneres es muy elevado. Esto, permite realizar una mejor estrategia y un mejor resultado en el Pentesting, al disponer de mayor cantidad de datos.
- **Uniscan**: herramienta que viene por defecto en Kali Linux, es un poderoso escáner que permite realizar seguimientos de huella digitales, realizar diversas funciones de manera remota e incluso listar múltiples características de cualquier servidor.
- **Metasploit/VMAP:** hay que aclarar ***que VMAP es un módulo para Metasploit, que posee de manera global, múltiples similitudes con Uniscan.*** Metasploit es un poderoso escáner que tiene una variante llamado **Metasploit Framework**, que viene instalado por defecto en varias distribuciones de Linux como Kali. Los hackers éticos utilizan esta herramienta con frecuencia debido a su posibilidad de realizar escáneres múltiples, obteniendo resultados positivos y con un buen nivel de detalle.
- **Seccubus**: es una herramienta poderosa, pero no es un escáner como tal. Seccubus es una poderosa arma que recopila algunos escáneres sumamente poderosos, permitiendo poder realizar muchas acciones y aprovechar el pleno potencial de todas las otras herramientas desde un solo lugar. Algo interesante de esta, es poder programar eventuales análisis automáticos para asegurarnos que seguimos manteniendo los estándares de seguridad y las buenas practicas.

Informática Forense

Esta apasionante disciplina, como vimos en el artículo, ***requiere que los datos recopilados sean precisos e inalterables,*** dado que son usados como evidencia, normalmente en procedimientos judiciales. Te dejo este curso totalmente gratis (click aqui). Con este propósito, veremos herramientas múltiples para tratar de conseguir estos objetivos.

Para empezar, puedes usar sistemas operativos específicos para seguridad informática. Entre los más destacados, tenemos a los S.O. **Caine, Kali Linux y Deft Zero.**
La mayoría de ellos, vienen por defecto con varias aplicaciones que te servirán para esto. Aquí profundizaremos en algunas de ellas que pueden o no, venir por defecto instaladas, pero tiene en común que son de acceso gratuito.

Para análisis forense

- **RAM Capturer y Magnet RAM Capture:** ambas herramientas comparten propósito: obtener y conseguir la información disponible en la **RAM** y volcar esos datos a otro dispositivo. Es útil hacer esto porque normalmente los datos de inicio de sesión suelen alojarse aquí
- **MAGNET Web Page Saber y FAW:** ambas permiten adquirir información de determinado sitio web, en determinado momento. Podemos descargar el sitio, imágenes e incluso descargar el código fuente, dependiendo cual aplicación elijamos usar.
- **Autopsy y The Sleuth Kit:** son aplicaciones que se usan para analizar los dispositivos y ver el volumen de datos y los sistemas de archivos que se usaron en ellos.

Para comprobar integridad

- **HashMyFiles**: cada archivo se compone de bit. Estos bits generan un hash único. Cualquier alteración de estos bits genera invariablemente una alteración de los hashes. Esta herramienta permite calcular de manera exacta los hashes correspondientes a determinado archivo, garantizando así por comparar el hash de los archivos, la integridad de los mismos.
- **Browser History Capturer (BHC) y Browser History Viewer (BHV):** BHC captura el historial de navegación web de los principales navegadores, de cualquier SO Windows, mientras que BHV nos permite extraerlo y verlo para poder examinar huellas de delitos.
- **Wireshark:** un famoso y excelente analizador de protocolos de red que permite hacer un análisis a profundidad de una red local. Nos permite inspeccionar los paquetes capturados y usando TShark podemos ver esta información en una línea de comandos.

En próximos artículos estaremos hablando de otras herramientas que podrás utilizar para poder desarrollar otras actividades dentro de la seguridad informática.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Certificaciones de Hacking Ético

En el mundo tecnológico de hoy, las certificaciones existen casi para cada rama de la tecnología. Por supuesto, la seguridad informática no podía ser la excepción. En este artículo hablaremos de algunas certificaciones disponibles, para que puedas certificar tus conocimientos como **Hacker Ético.**

Certificaciones CEH eJPT y OSCP

(Dale click a la imagen y accede al video donde hablamos de este tema)

Dentro de las certificaciones **Certified Ethical Hacker (CEH**) podemos encontrar distintas. Optar por una u otra, dependerá directamente de nuestros intereses.

Las CEH, tienen un costo aproximado de $850(al día de hoy, a dólar USA), se dividen en dos:

El examen ANSI: consistente en 125 preguntas, configuradas de manera Multiple Choice, enfocadas de manera totalmente teórica. Esta certificación se basa en evaluar que poseas los conocimientos necesarios, demostrando así que, por supuesto, ser un Hacker Ético (un experto en Seguridad Informática) no se trata solo de romper, si no que requiere múltiples conocimientos técnicos que permitan entender el “POR QUE” pasan las cosas.

El CEH Practical, basada en distintos restos, complementarios con contenido teórico.

eJPT, ***con un costo de $200***(al día de hoy, a dólar USA). Esta certificación, aunque no es muy valorada, es una excelente certificación a nivel práctico. La certificación se obtiene exclusivamente resolviendo los retos (similares a los establecidos en TryHackMe, por ejemplo.)

Las **CEH** tienden a ser más valoradas por el área de **RRHH** (sin generalizar, por supuesto), pero como vemos, el asunto de que certificación habría que elegir, dependerá de distintos factores y, por supuesto, el objetivo que tenemos al intentar estas certificaciones.

La certificación **eJPT**, la podríamos considerar el paso intermedio antes de ir por la **OSCP**, por los requisitos para aprobar que requieren.

OSCP: podemos identificarla fácilmente con la frase "Try Harder". Es más importante establecer un camino de razonamiento evaluando la individualidad de los problemas, antes que aprender de memoria los pasos para resolver algo. La tecnología avanza, las vulnerabilidades evolucionan y las formas de solucionarlas también. A causa de esto, esta certificación es muy interesante.

La OSCP tiene un costo de entre $1000 y $1400(al día de hoy, dólar USA). Es un examen de laboratorio, practico, de 24 horas de duración. El objetivo es explotar varias máquinas para conseguir archivos de prueba de los objetivos dados, para ganar puntos. Hay 100 puntos en juego, pero se aprueba con 70 puntos.

Esta certificación es un auténtico reto, evaluará tus conocimientos prácticos, teóricos y además, tu capacidad para una correcta gestión del tiempo.

¿Son necesarias para trabajar?

Elegir una certificación requiere un profundo análisis de tu parte, para ver cuál es más compatible con tus objetivos a alcanzar. Como vimos aquí, los departamentos de RRHH tienden a valorar algunas de ellas, pero no es un requisito obligatorio para adquirir trabajo. En tu caso tendrás que evaluar relación costo/beneficios de adquirirlas.

Espero que hayas disfrutado este capítulo y que tomes la mejor decisión para tu futuro.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Sección: Seguridad Para Todos

Hoy han aumentado significativamente los casos de cibercrimen, donde no solo son las victimas las empresas, sino también personas comunes, amigos, conocido, familiares.
Donde a través de métodos como ser Ingeniería social, Phishing, Vhishing (llamado telefónico), etc, Consiguen robar nuestro dinero a través de estafas, obtener información personal nuestra para después aplicar una ingeniería social más avanzada, pedir préstamos a nuestro nombre o estafar a nuestros familiares con nuestros datos.
Por ello es importante asimilar la seguridad informática como cultural, de esa forma evitaremos que nos estafen a nosotros o a nuestros seres queridos.
Tristemente la mayoría de las personas son hijos del rigor, y hasta que no pagamos las consecuencias no reaccionamos.
Lamentablemente en este campo una vez que eso sucede, muchas veces es irremediable la situación.
Es por esa razón que agregamos esta sección, para generar consciencia sobre las diferentes situaciones que pueden presentarse ante un cibercriminal.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Menores en Peligro: Grooming

Aprende a Proteger a los más indefensos.

Inauguramos una nueva sección del blog: **Seguridad para Todos**. La Seguridad Informática, también está profundamente relacionada a problemáticas sociales. Sabemos muy bien casos donde adultos caen en técnicas y tácticas de Ingeniería Social, Pishing y similares, con terribles consecuencias para su vida. Ahora, si esas son las consecuencias en adultos, imagina que pasa con los infantes y adolescentes.

¿Qué es el Grooming?

Se dice **Grooming** al acto delictivo de parte de una persona adulta de acosar con firmes propósitos de incluir a menores en actividades sexuales.

Es un proceso que demora tiempo y estrategias de parte del delincuente:

Primero intenta generar un vínculo de profunda confianza con el menor.

Luego intenta seducirlo para cometer actos sexuales (iniciando con charlas eróticas, quizás, para solicitar posteriormente fotos o videos), posteriormente genera un sentimiento de culpa en el para así aislarlo de su red de contención.

Por último, el ciclo termina con amenazas contra su integridad o la de sus seres queridos, logrando así que los actos se repitan.

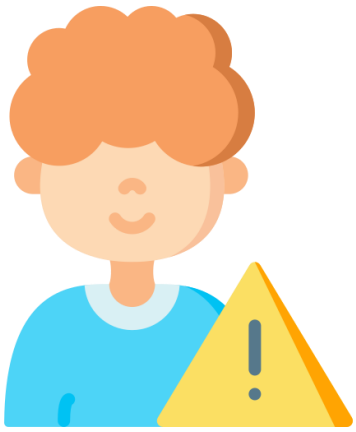
En la modalidad online, estos depredadores actúan solicitando fotos o video y luego extorsionando y amenazando a los pequeños. El principal problema de esta modalidad, es que el estrés mental hace que sea más difícil huir.

Cursos Gratis Online en: https://achirou.com/cursos-gratis
Contenido Gratuito en mis redes: https://achirou.com/redes-sociales
LinkedIn de Gastón Galarza: https://www.linkedin.com/in/gastongalarza/

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

¿Cómo podemos prevenirlo?

La represión nunca es la respuesta. En este caso, el mejor camino, es **la educación.**
Primero, reforzar los lazos afectivos, desarrollando un mayor nivel de confianza.
Segundo, es crucial enseñarles a los pequeños los riesgos reales de internet y como pueden usar las redes de manera responsable.
Tal como la lección de "Nunca aceptes caramelos de desconocidos", tenemos que **enseñar a los pequeños**, a ser precavidos en el uso de tecnología, sobre todo aceptando la frase de "si algo suena demasiado bueno como para ser real, probablemente no sea real".



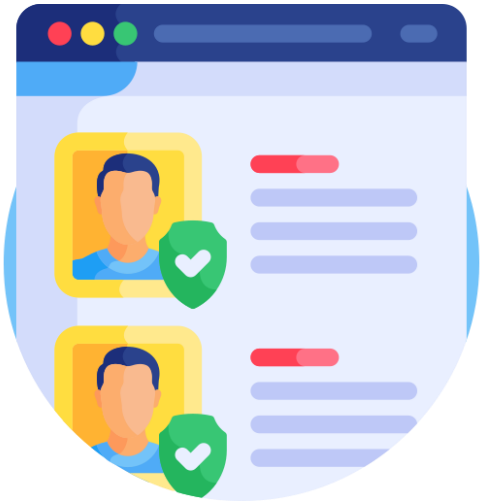
Recuerda **capacitarte**, como adulto, en prevención:

- No compartas datos que permitan identificarte y geolocalizarte(o a tus pequeños).
- Mantén un nivel alto de seguridad y confidencialidad en tus propias redes sociales, cuentas de usuario o contraseñas.
- Aprende sobre cómo funcionan las conexiones y comunicaciones en internet, esto te permitirá enviar datos de manera más segura, reduciendo la posibilidad de sufrir ataques basados en Ingeniería Social.
- Es buena idea utilizar un software de control parental, para los dispositivos que el menor utilizará sin supervisión.
- Enséñale y configuren juntos, las opciones de privacidad en redes sociales, para que desde pequeño sepa cómo debe protegerse.
- Presta especial atención a señales de alerta en el menor, que puedan inducir a una detección temprana: cambios de humor, cambios de rutina, frustración generalizada.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

¿Y si ya pasó?

- La **comprensión y contención** es lo primero que debe ocurrir.
- No sometas a tu pequeño o pequeña, a una catarata de preguntas y consejos interminables, créeme, suficiente **vergüenza, estrés y miedo** tiene en ese momento.
- Recopila toda la evidencia que puedas, en la mayoría de los países el grooming es delito.
- No bloquees el usuario ofensor, procura sacar imágenes, videos, textos y conversación de esos diálogos. Serán una excelente evidencia para cuando quieras acudir a la fiscalía o policía.
- Haz la denuncia con las autoridades competentes.



La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Gamers: Buscados por los Cibercriminales

Durante todo el 2020, la pandemia de Covid forzó a un importante porcentaje de personas a nivel mundial a pasar largas horas en sus domicilios. Esto, desemboco que, como muchos antes del Covid, recurrieran a fuentes de entretenimiento para mitigar las horas, por ejemplo: **los videojuegos.**

Debido a la disponibilidad de ellos en múltiples plataformas, costos no tan elevados y la posibilidad de jugar multijugador online, hizo de los videojuegos uno de los predilectos entretenimientos.

Pero esto también, ocasiono un problema mayor: debido a las posibilidades de compras online, los cibercriminales decidieron poner a los Gamers como objetivo central.

Gamers en Peligro

Los **gamers**, como comunidad general, son personas comprometidas, dedicadas y que ponen muchas horas de esfuerzo en determinado objetivo.

Muchos de ellos gastan una cantidad bastante interesante de dinero a nivel global, lo que como era de esperarse, atraería a los delincuentes como moscas a la miel. El trabajo de los criminales, se fue adaptando a las realidades actuales. Los ataques se volvieron más específicos.

En la antigüedad, no era extraño descargar un crack de un videojuego que tuviera introducido un virus o similar en su interior.
Ahora, los delincuentes suelen compartir “ayudas y trucos”, incluso los famosos “mods” pero que traen en su interior, porciones de código malicioso.

Un ejemplo de esto fue **Syrk**, un **ransomware** ideado para jugadores de Fornite que cifraba los datos de los jugadores hasta que pagaban un rescate (**NOTA NECESARIA**: Recuerda que pagarle a un delincuente NO garantiza que te

devolverá tus datos, y aun cuando te los devuelva, nada garantiza que lleguen íntegros, **NO CONFIES EN ELLOS**).

Las plataformas de usuarios, como **Steam**, **Epic Games** o **Ubisoft Connect**, también son un objetivo muy buscado por ellos.
Analicemos por ejemplo a **Steam**. Con más de 100 millones de usuarios mensuales, es una fuente favorita de recursos para delincuentes. El **malware Steam Stealer**, presume de hackear y obtener unas 77.000 cuentas cada mes, con pérdidas millonarias a nivel mundial.

Kaspersky afirma haber encontrado mil tipos de malware distintos enfocados al sitio. También han reportado otro tipo de problemática terrible: el robo de identidad.

Robo de identidad y otros problemas

De acuerdo al informe realizado por **Kaspersky**, con una investigación relacionada por **Savanta** en noviembre de 2020, encontró que aproximadamente **el 12% de los jugadores a nivel mundial** (varios millones de jugadores), sufrieron este tipo de delito, lo que ocasiono pérdidas de **347.000 millones de dólares USA.**

Se encuestaron a 5.031 jugadores de 17 países y los resultados fueron:

- **El 19% fue víctima de acoso**
- **El 33% tuvo que jugar contra cheaters**
- **El 31% sufrió episodios de estrés y ansiedad derivados de las causas anteriores.**

Consejos finales del Informe

Para evitar robos, daños, problemas y complicaciones, Kaspersky a través de su informe adjunta los siguientes consejos:

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

- **Comprar siempre de fuentes oficiales**: eso evita la posibilidad de descargar malware o de que los datos de tus tarjetas de crédito caigan en malas manos.
- **Asegúrate que la oferta es real:** las grandes plataformas ofrecen ocasionalmente descuentos o productos gratis. Pero asegúrate de que la oferta es real, no es extraño que a través del Email se utilicen técnicas de ingeniería social o pishing para enviar cosas fraudulentas. Lo mejor es ingresar directamente a la plataforma y buscar los descuentos o ingresar los códigos promocionales.
- **Infórmate sobre las políticas de devoluciones de las plataformas.**
- **Utiliza una tarjeta de débito/crédito exclusiva para compras online**: evita que, en caso de sufrir un robo, los atacantes accedan a todo tu dinero.

- **Utiliza una conexión segura**: conéctate siempre desde tu red domiciliaria, asegura tu red y es una buena opción usar VPN de refuerzo.
- **Protege tus cuentas**: Activa doble factor de autenticación si se puede, trata de evitar iniciar sesión en plataformas con tus RRSS.
- **Protege tus dispositivos**: Se atentó con lo que descargas, utiliza software de protección para tus dispositivos y configúralos correctamente.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

SKIMMING: Vacaciones en Peligro

A veces, la frontera entre la **seguridad física** y la **seguridad informática**, son difusas. Uno de los puntos donde estos límites se borran, es en el **Skimming**. ¿Pero qué es esto?

La peor pesadilla de los Turistas

Una de las cosas que más miedo, desazón y frustración produce al momento de estar de vacaciones, es recibir una notificación de tu banco, donde te detallan consumos que no realizaste. Cuando esto ocurre, las señales del delito del que hablamos hoy, son evidentes: **Clonación de tarjetas de crédito/debito.**

Como habrás sospechado ya, **Skimming** es el término por el cual se conoce al delito consistente en ***robar información y clonar tarjetas de débito/crédito*** a través de dispositivos físicos. ¿Pero cómo se realiza esto?

Skimmer Y Shimmer

Skimmer es el nombre que se le da a un dispositivo físico en apariencia similar a un posnet (el típico aparato por donde se pasan las tarjetas).

Este dispositivo va superpuesto a la ranura del posnet o cajero automático, permitiendo que la tarjeta de crédito pase primero por el Skimmer antes de ingresar al posnet, facilitando así la **clonación** de los datos (específicamente el pin y los detalles de la banda magnética).

Otros dispositivos, los **Shimmers**, más avanzados aún, van dentro o debajo de la ranura del cajero, permitiendo así un espacio para que la tarjeta de la víctima ingrese, duplicando sus datos.

Estos dispositivos son especialmente **peligrosos** dado que extraen la energía de bajo voltaje que aparece cuando se introduce la tarjeta, lo que permite que estos dispositivos ilegales funcionen de manera prácticamente indefinida.

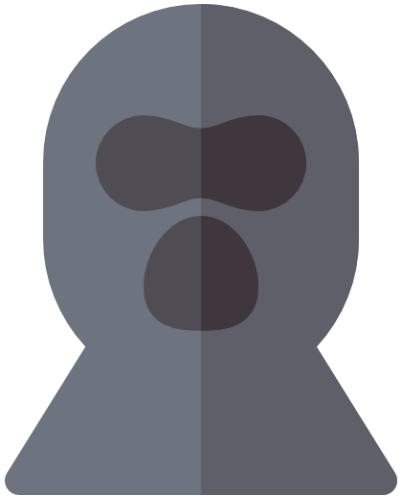
La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Como obtienen los datos

Normalmente ambos dispositivos tienen en común ciertas cosas:

- Ambos poseen una parte que puede detectar las **pulsaciones** del teclado de la víctima, registrando así el pin de la tarjeta
- Poseen también un **microcontrolador** y un espacio de almacenamiento
- Algunos dispositivos ultra pequeños, requieren la instalación de una **cámara pequeña**, en ángulo que permita captar las pulsaciones del **PIN** de la tarjeta. Cuando la tarjeta es de banda magnética solamente, los dispositivos clonaran la **banda y el pin**.

  Cuando la tarjeta es de **chip**, el funcionamiento es distinto. Los cajeros normalmente envían una pequeña dosis de corriente eléctrica al chip, lo que ocasiona una respuesta. El **Shimmer** lo que hace, es capturar esta respuesta (como si de interceptar una señal wifi se tratara) y almacenarla. Lo curioso de este método es que envía los datos y las claves del usuario, lo que "facilita" el acto delictivo.
  El peligro de estos shimmers es que, una vez la tarjeta es retirada del terminal, el dispositivo permanece inactivo, lo que hace ***difícil identificarlo.***



Como recuperan los datos

Como mencionamos antes, algunos dispositivos tienen un espacio de **almacenamiento**, por lo cual los delincuentes pasan luego a recuperar los datos. En otro tipo de dispositivos, los delincuentes utilizan una **tarjeta en blanco** especial que, a modo de USB, se pone en el cajero y **descarga** los datos capturados. Los más avanzados tienen maneras de enviar los datos capturados vía **bluethoot**.

En la antigüedad, se creían que las únicas tarjetas vulnerables eran las que tenían banda magnética, creyendo que las nuevas con chips no los serian.

Lamentablemente las técnicas avanzadas de la delincuencia demostraron que esto no es tan así.
Desde luego, las tarjetas con chip son mucho **más seguras** que las bandas magnéticas, dado que las señales emitidas con el chip van cifradas con algoritmos como **Triple-DES, SHA o RSA**, pero eso no significa que sean inviolables. Son una buena opción dado que los dispositivos para lograr obtener datos de ellas son bastante más difíciles de construir, pero aun así hay casos donde se han encontrado, como mencionamos antes.

¿Cómo evitar la clonación?

Como recomendamos en artículos anteriores, la mejor arma es **la prevención**.

- Los delincuentes prefieren cajeros al paso, en **zonas poco transitadas,** fuera de sedes bancarias o grandes comercios supervisados. Por tanto, la mejor opción para evitar esta opción, es recurrir a cajeros dentro de las sedes bancarias o grandes centros comerciales.
- **Revisa las bocas del terminal** donde pondrás la tarjeta para detectar partes extras o partes sueltas, lo que delataría posibles agregados. Si son pagos en comercios, intenta visualizar que el posnet **no tenga dispositivos extras** pegados alrededor.
- Procura **tapar el panel, entrecruzar los dedos o poner una mano sobre la que usaras para teclear** el ***PIN*** para intentar evitar que una posible cámara pueda ver lo que escribes.
- La otra opción es pagos en estilo **contactless**, cuando tengas una tarjeta compatible.
- Puedes recurrir a pagos vía **e-commerce** (¡cuidado con el ***pishing***!).
- Ten activados métodos de **control de gastos** y **revisa tu resumen periódicamente,** para evitar que los consumos pasen desapercibidos.
- **Usa tu tarjeta sabiamente**, no la pongas en lugares físicos innecesarios (eso de paso cuidará tus ahorros ;))

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Amenazas por Internet Episodio 1: Doxing

Si pensabas que solamente el Malware podía ser una amenaza en la red, piensa de nuevo. Los ciberdelincuentes se valen de toda una serie de herramientas y técnicas para obtener beneficios ilegales.
En esta ocasión, hablaremos de **Doxing(o Doxxing)**, una peligrosa táctica de los delincuentes en línea.

Qué es

Dentro del mundo del internet, ves tras ves se dice que una de las grandes ventajas del mismo, es ***el anonimato.*** Pero esto no es tan así. **Las cosas que realizamos en la web, dejan una huella**. Aun cuando intentemos borrar toda nuestra información, a ojos expertos siempre se puede encontrar algo más.

El Doxing, es una forma en la cual los atacantes obtienen información privada de una persona, para luego extorsionarla o en el peor de los casos, hacerla pública. El objetivo final, es conseguir dinero a cambio del silencio o, en peores circunstancias, simplemente dañar la imagen y reputación de una persona.

Nueva era de acoso

Las normas morales y la ética, tienen una grave disputa contra el Doxing. Uno de los graves problemas es el efecto rebaño, que es tan frecuente en este tipo de ataques.
Las técnicas del Doxing se han usado con frecuencia solo con ansias de venganza o deseo de revancha ante determinada situación.

Podríamos decir, que ***estas estrategias de Doxing surgían*** cuando en una discusión online, uno de los aludidos recurría a buscar información contra el otro para desprestigiar sus argumentos. Las cosas pronto escalaron. En ocasiones se

utilizaron como medidas de venganza ante grupos ideológicos, pero los problemas fueron que a veces las víctimas no eran las directas involucradas, lo que ocasiono daños irreparables a la reputación de personas inocentes.

El anonimato de actuar en manadas, les dio a personas inescrupulosas las herramientas que necesitaban. Lo siguiente solo fue desarrollar habilidades en computación, para rastrear los movimientos online de las víctimas y sus familiares.

Y así llegamos al peligro que tenemos hoy: ***personas que obtienen de manera ilegal contenido, mensajes y fotos intimas o privadas de las víctimas y luego extorsionan a las victimas o publican las mismas.***

Como funciona

Las reglas son simples: buscar en el pasado o presente de las personas, información o datos que puedan ser usados en su contra. Luego el camino variará de acuerdo al propósito de estas personas inescrupulosas: si buscan desacreditar a nivel profesional a alguien (como un artista o político), esa información se unirá a mentiras descaradas o medias verdades para romper la reputación de la persona.

Luego intentaran expandir lo más posible esto y por supuesto, contagiar a la mayor cantidad de personas posibles de expandir este rumor.
Si el propósito es conseguir dinero, **se procederá a la extorsión.** La victima recibirá un llamado, mensaje o email indiciando que se tiene cierta información y que, de no depositar dinero, la información será publicada.

Los doxxers más avanzados, con conocimientos de ciberseguridad o programación, utilizarían tácticas de ingeniería social y similares, para profundizar en el nivel de información adquirido.

Las formas de obtener información, varían desde los datos que la misma víctima de, hasta el que se obtienen en rrss, chats simulando ser otra persona, rastros en

el uso, etc.

Cómo prevenirlo

- **La cautela** es la principal arma en estos casos. Desgraciadamente, si eres víctima de Doxing, tu información preciada está en manos de ellos. Pero si aún no, estas a tiempo.
- Mantén tus rrss **en privado**
- **Evita** sitios, servicios o cosas dudosas
- **Mantén actualizados y correctamente configurados** tus SO, antivirus, Firewall y toda medida que sirva de protección.

Recuerda que ser precavido, significa entre otros, no publicar más información en las rrss de la estrictamente necesaria.

Actúa cautelosamente en internet, los delincuentes no descansan.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Puerta abierta a la Ciberdelincuencia

Con el auge del trabajo remoto, los ataques de las organizaciones de ciberdelincuencia aumentarían en frecuencia, alcance y peligrosidad. En diversos artículos mencionamos que ser precavido y responsable en el uso de tus dispositivos, es una buena manera de prevenir ataques. Pero ¿sabías las maneras en las cuales pueden acceder a tu sistema o dispositivo?
Aquí te dejaremos 5 de las formas más comunes de entrar.

Qué ganan ellos

La delincuencia lucra con datos. O bien utilizarán tus datos para vendérselos a terceros (datos de tarjeta de crédito, cuentas bancarias, identificación para falsificar identidad y otros) o bien utilizarían tus datos para extorsionarte y/o estafarte (imágenes intimas, datos encriptados, etc.).

No sorprende, entonces, que el objetivo central de estos delincuentes sea acceder a tus dispositivos o cuentas y poder buscar la mayor cantidad de datos posibles de ti, guardados normalmente en tus dispositivos de confianza.

Primer amenaza: El Malware

Una de las mayores amenazas (y de las más rentables), es **el Malware.** En este blog estamos analizando varios tipos distintos de Malware, si no los leíste, revisa en **“Artículos de Seguridad”** donde encontraras otros artículos del tema.
El problema de esta amenaza, es la cantidad abismal de formas distintas que pueden utilizar los delincuentes para perjudicar a las víctimas.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Para prevenir este método, **la prudencia y ser precavido** es crucial, pero, además, activar los distintos softwares de protección que existen serian cruciales para poder estar protegido de esto. En los artículos de ***tipos de malware*** profundizamos en formas de evitar esto.

Segunda amenaza: Errores en RRSS

Ciertas tácticas de **Ingeniería Social y Pishing,** requieren tener bastante información de la víctima. Para ataques dirigidos, los atacantes recolectan información del objetivo. Lo común, es aprovechar las huellas que deja cada usuario en redes sociales, revelando información sensible al respecto.

Fotografías demasiado personales, dejar datos de contacto privados en foros abiertos, posteos revelando cosas laborales/personales, ***todo sirve para que los atacantes obtengan información*** lo suficientemente grande como para crear ataques difíciles de descubrir.
Recuerda que para evitar esto, lo mejor es mantener las reglas de privacidad lo más estrictas posibles, evitando dar datos de más en las ***RRSS***.

Tercer amenaza: Falta de mantenimiento

Es normal que, mientras los dispositivos funcionan, no les prestemos demasiada atención. Pero la ciberdelincuencia actúa de manera totalmente opuesta: revisan y se actualizan de manera permanente, para obtener la mayor cantidad posible de vulnerabilidades de nuestros dispositivos.

Como sospecharás, si ellos encuentran fallas y brechas y tú no actualizas ni revisas, estas dejando una puerta abierta de manera permanente a los ciberdelincuentes.

Los desarrolladores atrás de dispositivos y sistemas operativos, ***lanzan actualizaciones y parches con frecuencia,*** para mejorar la seguridad o reparar errores y vulnerabilidades. Presta atención a tus dispositivos, dale mantenimiento con frecuencia y recuerda actualizar apenas estén disponibles para estar lo más protegido posible.

Cuarta amenaza: candados débiles

Imaginemos que el método de cifrado o las contraseñas se asemejan a candados. Si usamos un cifrado inadecuado o una contraseña débil (o la misma en varios lugares), nos encontraremos con una terrible amenaza: tener un candado débil y pequeño es como dejar puertas abiertas al delincuente. será fácil acceder a tus datos para los delincuentes.

Recuerda no compartir contraseñas entre sitios, cambiarlas con frecuencia y usar contraseñas alfanuméricas de al menos 8 dígitos (cuando sea posible).

Quinta amenaza: No usar el F2A

Algunos sitios y aplicaciones, ***permiten usar un factor de doble autentificación o F2A.*** En resumidas cuentas, para poder acceder a determinado perfil o app, necesitaremos autorizar el acceso a través de una app tercera o código enviado vía email o número de celular.

Resulta algo “molesto” iniciar en una cuenta de ésta manera, por lo cual muchos usuarios prefieren no usarlo. Grave error.

Este tipo de verificación, dificulta mucho más a los atacantes acceder a tus perfiles, dado que necesitarían acceso a 2 cuentas distintas con dos contraseñas distintas.

Si mezclamos contraseñas fuertes con F2A cuando esté disponible, unido a ser precavido y responsable en el uso de tus dispositivos, tendrás una forma de complicarle el camino mucho más a los delincuentes.

Espero que tomes en cuenta las recomendaciones de este capítulo y que te sirva para aumentar tus habilidades en la protección de tus datos.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Modo Incógnito: ¿es realmente incógnito?

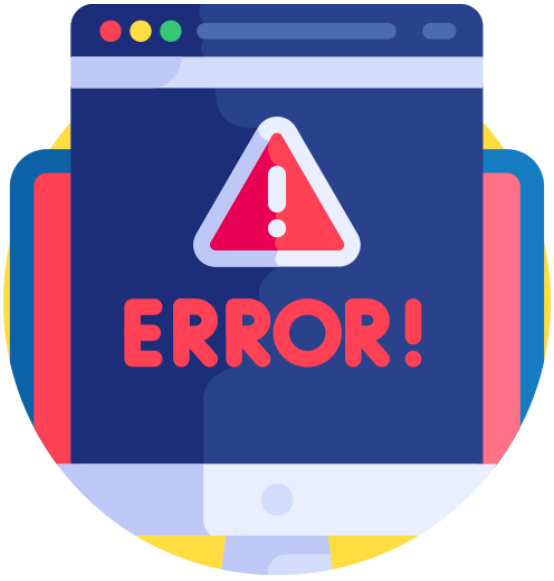
Por muchas razones, a veces necesitamos mantener un nivel de privacidad y anonimato muy alto al navegar por internet. Cuando los navegadores lanzaron los famosos **"Modo Incógnito"** muchos celebraron, pero, ¿te da realmente el anonimato que necesitas?

¿Qué datos almacenan? ¿Qué datos pueden verse?

Hay que dejar ciertas cosas en claro desde el primer momento. Cuando nos conectamos a internet desde un dispositivo, lo que hacemos es **enviar y recibir múltiples paquetes de datos de manera continua y permanente.** Es común que entremos a determinado sitio, desde una sesión iniciada y descarguemos contenido o carguemos contenido.

Por supuesto, si necesitamos anonimato, es menos probable que deseemos cargar o descargar cosas, para evitar posibles riesgos.
Los administradores de sitios web, los proveedores de servicios de internet, la organización (si estas en una red laboral) son sólo algunas de las entidades que pueden tener acceso a algunos o muchos de los datos que transfieras.

De la misma manera, los archivos que descargues o los sitios que desees poner como favoritos, quedaran disponibles y visibles para cualquier persona que pueda acceder a ese dispositivo.



¿Me protege del Malware?

Definitivamente no. El modo incognito no aísla tu dispositivo de la red ni de los riesgos. Si te conectas desde un dispositivo con un keylogger, por ejemplo, aun cuando realices la conexión desde modo incognito, las pulsaciones quedaran grabadas en ese Malware, dejando tus datos al descubierto.
También podemos mencionar que, si descargas algo que tenga, por ejemplo, Ransomware, definitivamente dañaras tu dispositivo e incluso dispositivos

relacionados o conectados a la red (dependiendo el comportamiento del Ransomware).

Por supuesto, si hablamos del caso del Spyware, la navegación incógnita es totalmente susceptible a ser víctima de estos tipos de Ransomware. Todos los datos que envíes, cargues o muestres en modo incognito, si eres víctima del Spyware, serán filtrados a este software.

Dentro de las malas prácticas del uso de dispositivos e internet, está el considerar el modo incognito como una especie de escudo protector, un comodín que protege tus datos en todas las comunicaciones.

Definitivamente no es así. El modo Incognito en realidad es una manera de que ciertos datos permanezcan visibles solo temporalmente y al cerrar sesión se borren. Entonces, es importante preguntar si es realmente útil, de acuerdo a nuestras necesidades.

Entonces ¿Qué datos bloquea?

Ten en cuenta que la prudencia y ser precavido, son características centrales que deberías tener al momento de realizar una navegación por internet. Evita entrar a cualquier enlace, descargar cosas de cualquier sitio y por sobre todas las cosas, evita dejar tus datos libremente en cualquier enlace. Dejar tu email, numero de celular o datos de RRSS, te expone a terribles peligros que pueden derivarse del manejo poco responsable de internet.

Pero ciertamente, los datos almacenados de manera local en la navegación, quedaran sin almacenarse. Historial de navegación, cookies, historial de descarga y cosas relacionadas a datos temporales quedaran disponibles solamente mientras la sesión de incognito dure.
Es conveniente usarla, entonces, cuando desees que determinado comportamiento no quede registrado en un dispositivo.
Y a ti ¿realmente te resulta conveniente usar este tipo de navegación?
Desde aquí, como siempre recomendamos que seas prudente, responsable y precavido en el uso de tus dispositivos conectados a internet.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Autentificación en dos pasos: asegura más tu cuenta

Dentro de las medidas de protección de las cuentas, la correcta gestión de contraseñas es crucial. Que tenga (de ser posible) más de 8 dígitos alfanuméricos, que no se repita entre varias cuentas, que se cambie con frecuencia. Pero a veces, esto no es suficiente. Si por algún error se filtra tu contraseña, tu cuenta estará en riesgo. Para evitar esto, en muchas aplicaciones y servicios online puedes activar otra medida de seguridad: el doble factor de autentificación, o la autentificación en dos pasos (F2A). Hablaremos de esto, en este artículo.

¿Qué es el F2A?

En condiciones normales, para iniciar sesión puedes usar un nombre de usuario y una contraseña. Pero si lo que deseas es aumentar tu nivel de seguridad y la aplicación o web te lo permite, ***el F2A entra en juego.***
Esta capa extra de seguridad, varía en cada aplicación. Una vez ingresado usuario y contraseña, vamos a necesitar resolver una medida más de seguridad. En algunas, es una pregunta de seguridad. En otras, puede ser un token, un código enviado a nuestro móvil o email, un dispositivo físico como USB, etc.

En algunos artículos, se diferencia la verificación en dos pasos (aquella que utiliza algo que envían, como un SMS) de la autentificación en dos pasos (que utiliza algo que tienes, como tus huellas digitales o tu rostro). Ambas tienen el mismo propósito, aunque por supuesto, ***el F2A es más seguro que la verificación,*** dado que al ser algo que te envían por email o SMS, puede ser interceptado, mientras que el F2A al ser algo que tú ya tienes, sería difícil ser interceptado.

En algunos dispositivos nuevos, el hecho de poder usar el patrón más la huella digital, permiten agregar capas extras de seguridad permanente. Lo bueno, es que muchas aplicaciones y sitios nos permiten guardar un dispositivo como “de

confianza", lo que significa que cuando iniciemos sesión desde ese dispositivo, ***no será necesario usar el F2A.***

Desde luego, en estos casos es necesario recalcar que el dispositivo "de confianza" debería ser de uso exclusivo nuestro, totalmente asegurado (de ser posible con huella y código seguro) y **extremar las medidas de prevención al usarlo.**

¿Es infalible?

En el mundo de hoy, nos hemos acostumbrado a buscar blancos o negros. Pero como sabemos, en el ámbito de la tecnología esto no es tan simple. Lo cierto es que estas medidas de seguridad, representan otra barrera de protección, pero la verdad es que **nada es totalmente seguro.** Pero combinando un comportamiento precavido y responsable, con una contraseña segura y una activación correcta del F2A, definitivamente complicarán más las cosas para posibles atacantes.

No es necesario activar el F2A en absolutamente todos los sitios o apps (aunque nunca está de más hacerlo), pero **te recomendamos que la actives en los sitios cruciales,** donde guardes información muy importante o manejes dinero (ya sabes: Fornite, Cuentas Bancarias, Google Drive, Gmail, etc.).

Recuerda de todas formas, que el ser precavido y responsable en el uso de tus dispositivos, evitará o disminuirá las posibilidades de caer en manos de un atacante.

Podemos recomendarte también, que en las aplicaciones con F2A externo, revises la aplicación ***Autenticator***, que te permite servir como capa extra, dotando códigos de un solo uso, temporales y variables.

Para concluir, es necesario recordar que esta medida no exime mantener contraseñas seguras, cambiarlas con frecuencia y no repetirlas.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Amenazas por internet Episodio 2: Phishing

En el mundo actual, los ciberdelincuentes afinan la puntería cada vez más para obtener dinero de victimas desprevenidas o asustadas. En este camino de corrupción y delincuencia, deciden utilizar una gama de estrategias para conseguir sus fines. Hoy hablaremos de una de ellas: **El Phishing.**

¿Qué es el Phishing?

Este término se utiliza para denominar las estrategias de los ciberdelincuentes, consistentes en intentar engañar a la gente a través de envíos de mensaje/email, fingiendo ser otra persona o entidad, intentando obtener algo de la víctima o conseguir que la persona haga algo: ***información, dinero, instalar Malware o ceder datos cruciales.***

En la mayoría de estos casos, se le solicita a la persona acceder a un link o descargar algo y ejecutarlo, con el objetivo de cumplir sus oscuros objetivos. Esta táctica de ***Ingeniera Social***, se lleva a cabo de distintas maneras.

Una de ellas, es enviar correos electrónicos simulando ser una entidad legal (normalmente financiera, como bancos), en el que se detalla que hay alguna circunstancia o situación que requiere un reajuste (por ejemplo, indicar que es necesario cambiar la contraseña).

Por supuesto, ***se adjunta un link para "facilitar" el trabajo de la persona***, pudiendo cambiar la contraseña desde ese link. Al dar clic en este link, se abrirá una pestaña que, dependiendo las habilidades del ciberdelincuente, puede ser

asombrosamente parecida a la entidad que intentaban suplantar.

Esto, hace más probable que la víctima no note nada extraño, ingresando los datos que necesitan. Al enviar estos datos, la web marcará un error y se redireccionará al sitio real, mientras que los datos de acceso le llegarán al ciberdelincuente.

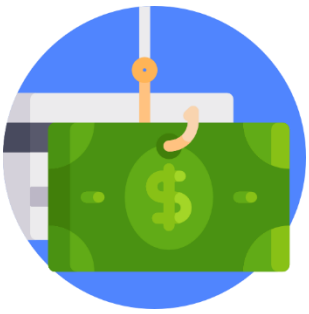
¿Es peligroso?

A diferencia del Malware, el Phishing no es una amenaza activa permanente. Requiere que la víctima, y solo la víctima, literalmente regale/entregue sus datos a los delincuentes. Es normal que ocurran situaciones donde recibas Phishing. Pero a menos que cedas tus datos, los atacantes no podrán obtener tu información de ninguna manera.

Es importante destacar que, dependiendo de tu trabajo y/o rol laboral, puede que recibas con más frecuencia ataques de Phishing dirigidos **(hablaremos en otro artículo del famoso Whaling).**

¿Cómo identificarlo?

- Una forma simple de reconocer un intento de phishing, es una antigua y famosa frase: “si algo parece demasiado bueno para ser cierto, es que probablemente es demasiado bueno para serlo”.
- Otro detalle crucial, que puede ayudar para detectar estos fraudulentos ataques, es leer cuidadosamente el mensaje. Normalmente cometerán errores ortográficos o de coherencia escrita.
- Revisa atentamente las direcciones de email o el link al que se supone, deberías dar clic. Poniendo el mouse sobre el enlace, normalmente te debería dar una vista previa del enlace. Si dudas, no des clic a ningún enlace.
- La urgencia en la forma de escribir el texto, representa otra señal de probable Phishing: necesitas hacer algo urgente, para evitar algo terrible o ganar algo increíble.



La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Hay algunos consejos finales para protegerte y/o evitarlo:

- Cuando recibas un email de alguna entidad solicitando tus credenciales, dirígete por fuera de dicho email directamente al sitio de confianza de tu entidad y verifica allí si deberías tomar alguna acción.
- No caigas presa del pánico o la urgencia, reflexiona antes de decidir. Como mencionamos antes, la urgencia es una de las herramientas usadas por los delincuentes. No cedas a la presión.
- Intenta no descargar nada, a menos que puedas verificar el remitente o sea algo que efectivamente estuvieras esperando recibir.
- Cambia tus contraseñas con frecuencia
- Se precavido, usa tus dispositivos de manera responsable y navega con mucha precaución.

Y tu ¿estas preparado para detectar el Phishing? Te dejo este desafío, para poner a prueba tus habilidades de detección. Cuéntanos tus puntajes.

Desafío de Phishing

Espero que hayas disfrutado este capítulo, déjame tus opiniones en mis redes sociales.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Sección: Rutas de Aprendizaje

Una de las preguntas más frecuentes que recibo es:
¿Cómo inicio mi formación profesional en seguridad informática?
¿Qué conocimientos debo tener?
Por ello es que te comparto esta sección en donde vamos a hablar de que conocimientos debes tener y en qué orden puedes ir adquiriéndolos.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Rutas de Aprendizaje: Seguridad y Desarrollo

Cuando damos nuestros primeros pasos en el mundo de la tecnología, es común sentirnos abrumados por la variedad de temáticas que podemos abarcar. En estos artículos iremos viendo dos de las rutas de aprendizaje recomendadas para mantener un orden en la formación.

Hay ciertos detalles a destacar: la tecnología avanza, por ende, los cursos también. Las rutas de aprendizaje no serán estáticas, irán adaptándose y evolucionando de acuerdo a los mejores contenidos que surjan.

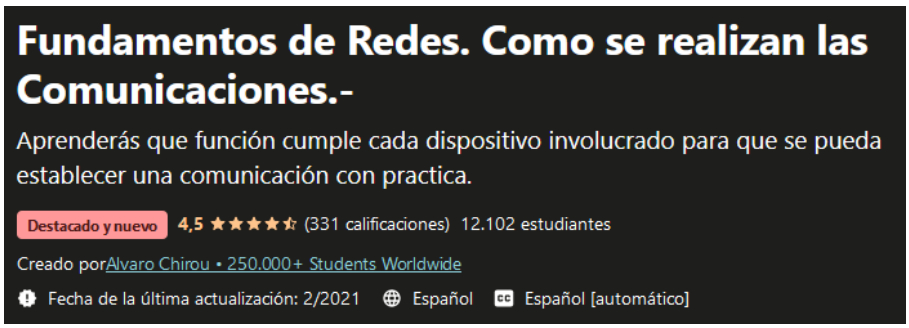
Ruta de Seguridad Informática

La seguridad informática, como disciplina dentro de la tecnología, es enorme. Sería imposible abarcar todo el contenido en un curso. Es normal que las personas dentro de este mundo se especialicen en alguna de las ramas de esta disciplina y profundicen con sus conocimientos, habilidades y experimentación, de esta manera irán adquiriendo experiencia.

En la sección de rutas, al acceder a esta ruta específica, podrás aprender desde los fundamentos, los conocimientos que necesitas para poder desarrollarte como un profesional de la seguridad informática.

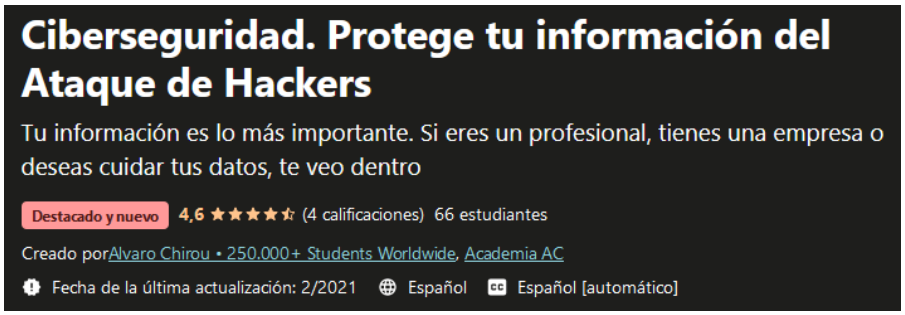
No solo eso, además al realizar los cursos de esta rama adquirirás la práctica necesaria para poder realizar los test, ejercicios y análisis como un profesional. Dale un vistazo por ti mismo a esta Ruta tan apasionante, donde iniciaremos el recorrido desde «Fundamentos de Redes» y «Ciberseguridad. Protege tu información del ataque de los Hackers».

Dale click a cada imagen, te llevará directamente al curso.



Cursos Gratis Online en: https://achirou.com/cursos-gratis
Contenido Gratuito en mis redes: https://achirou.com/redes-sociales
LinkedIn de Gastón Galarza: https://www.linkedin.com/in/gastongalarza/

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.



Especialidades

Dentro de esta ruta, debido a la magnitud de la disciplina, ***podrás elegir diversas especialidades para profundizar,*** de acuerdo a tu gusto y criterio.

Algunas a las cuales podrás optar, son

- **Especialidad en Espionaje**
- **Especialidad en Programación**
- **Especialidad en Hacking**

Las especialidades irán profundizando con el correr del tiempo, permitiéndote desarrollar nuevas habilidades gracias a tu esfuerzo y vocación. ***Han sido pensadas de manera tal, que el proceso de aprendizaje gradual resulte más llevadero, sin importar tu nivel de conocimiento previo o familiaridad con la materia.***

Ruta de Desarrollo

Los programadores y testers pertenecen a un sector de la tecnología que, por sus habilidades y conocimientos, se encuentran en auge en el mercado

Cursos Gratis Online en: https://achirou.com/cursos-gratis
Contenido Gratuito en mis redes: https://achirou.com/redes-sociales
LinkedIn de Gastón Galarza: https://www.linkedin.com/in/gastongalarza/

laboral. Por supuesto, el mundo del desarrollo es grande y muy variado, por lo que no es fácil elegir un camino al inicio.

Para poder responder a esta necesidad de orientación, **eh creado esta** ruta de aprendizaje donde de manera frecuente iremos desarrollando distintas formaciones para potenciar tu desarrollo profesional. El propósito central de esta ruta, es que puedas desempeñarte, de acuerdo a tu gusto, dentro de la industria de la tecnología, en una de las variadas ramas que podrás encontrar.

Como tester, tendrás a tu cargo la gestión y verificación de la calidad de los productos creados. Sera tu responsabilidad que cada aplicación o sitio, cumpla con los más altos estándares de calidad (de acuerdo a los criterios de cada empresa) y deberás dar el visto bueno a las creaciones de los desarrolladores.

Necesitarás habilidades, ojo crítico y conocimientos profundos no solo de lenguajes, si no de herramientas específicas orientadas a estresar e intentar romper programas, para garantizar que el flujo de trabajo y el funcionamiento, cumple con las expectativas ideales al pensar este programa.

Como desarrollador/programador, tendrás a tu cargo la gestión completa de la creación, serás el profesional que estará a cargo de transformar una visión abstracta en algo concreto, utilizable y, por sobre todas las cosas, que sea agradable para los usuarios finales.

Es un rol que requiere conocimientos de lenguajes, habilidades de pensamiento lógico y secuencial y capacidad de poder transformar en cosas reales ideas y pensamientos.

Para muchos, **los programadores son verdaderos artistas,** encargados de mantener buenas practicas al escribir el código que permitirá la creación de las ideas más extravagantes o de las soluciones más urgentes.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Espero que puedas aprovechar los conocimientos que obtendrás en estas rutas de aprendizaje, para poder cumplir tus metas de un nuevo trabajo o de un trabajo mejor.

¡Empieza ahora tu formación profesional!
Te dejo, un abrazo digital.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Rutas de Aprendizaje: Red Team y Blue Team

Cuando damos nuestros primeros pasos en el mundo de la tecnología, es común sentirnos abrumados por la variedad de temáticas que podemos abarcar. En estos artículos iremos viendo dos de las rutas de aprendizaje recomendadas para mantener un orden en la formación.

Hay ciertos detalles a destacar: la tecnología avanza, por ende, los cursos también. Las rutas de aprendizaje no serán estáticas, irán adaptándose y evolucionando de acuerdo a los mejores contenidos que surjan.

Ruta de Aprendizaje Blue Team

Dentro del mundo de la **Seguridad Informática,** los profesionales se deciden por múltiples orientaciones. Una de las especialidades, es el llamado **Blue Team**. Este equipo, ***es el encargado de la gestión proactiva de la Seguridad Corporativa de manera Defensiva.*** Puedes revisar la ruta completa ¡aqui!

Buscan encontrar patrones y comportamientos de sistemas, aplicaciones y usuarios para encontrar posibles agresores y/o posibles incidencias, vulnerabilidades o fallos. Buscan realizar evaluaciones de manera permanente, para adelantarse a posibles fallas.

En caso de que haya ocurrido un ataque, realizan análisis forenses, trazabilidad de vectores de ataques, propuestas de soluciones y medidas de detección para futuras incidencias.

Dentro de la Ruta de Aprendizaje, empezaremos por **“Fundamentos de Redes”** y continuaremos con **“Introducción Teórica a la Seguridad Informática en La**

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Nube". Los niveles siguientes empiezan a orientarnos a la protección de la información y de la organización de ataques de ciberdelincuentes.

Si te interesa proteger a las empresas, organizaciones e información de los usuarios, sistemas y aplicaciones, esta Ruta es para ti.

Ruta de Aprendizaje Red Team

Otra de las especialidades dentro de la Seguridad Informática, es el **Red Team**. ***Este equipo, es el encargado de la Seguridad Corporativa de manera Ofensiva.***

Trabajan en conjunto con el Blue Team en múltiples ocasiones, de manera que puedan, bajo entornos controlados, simular posibles escenarios de ataques.
Revisa la ruta completa, desde aqui.

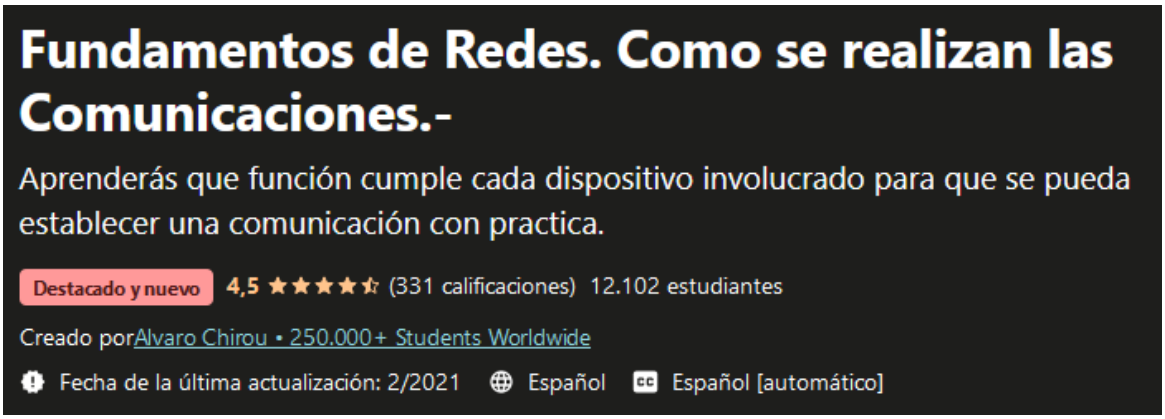
El **Red Team** ocupa el rol de Atacantes en esta situación, buscando "atacar" a través de un proceso de emulación, las aplicaciones y sistemas de la Organización. Esto, permite al Blue Team poder analizar distintas estrategias de cómo están trabajando y donde están las posibles falencias, pudiendo defenderse y reforzar las fallas bajo una situación controlada.

Dentro de la **Ruta de Aprendizaje**, empezaremos por ***"Fundamentos de Redes"*** y continuaremos con ***"Introducción Teórica a la Seguridad Informática en La Nube"***.

Los niveles siguientes empiezan a orientarnos a técnicas y tácticas de ataque para planificar estrategias que sirvan para mejorar la Organización. Si prefieres

establecer estrategias ofensivas y ver cómo se pueden explotar vulnerabilidades para apoyar a los conocimientos del Blue Team, esta ruta es para ti.
Espero que puedas aprovechar los conocimientos que obtendrás en estas rutas de aprendizaje, para poder cumplir tus metas de un nuevo trabajo o de un trabajo mejor.

Si das click en cada imagen, te llevará directamente al curso.



¡Empieza ahora tu formación profesional!

Te dejo, un abrazo digital.

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Rutas de Aprendizaje: Python y Cloud

Cuando damos nuestros primeros pasos en el mundo de la tecnología, es común sentirnos abrumados por la variedad de temáticas que podemos abarcar. En estos artículos iremos viendo dos de las rutas de aprendizaje recomendadas para mantener un orden en la formación.
Hay ciertos detalles a destacar: la tecnología avanza, por ende, los cursos también. Las rutas de aprendizaje no serán estáticas, irán adaptándose y evolucionando de acuerdo a los mejores contenidos que surjan.

Ruta de Aprendizaje Python

En esta ruta aprenderás todas mis formaciones profesionales basadas en este lenguaje, aunque no es necesario que cumplas con el orden que te planteo acá. Verás 3 ramas: **Seguridad Informática, Análisis de Datos y Extracción de Datos.** Dependiendo el curso que elijas, te orientarás hacia un área. Por supuesto, podrás iniciar tu formación con el curso de **Master en Python**, donde sentarás las bases de este potente lenguaje.

Dale clic a la imagen para ir directo al curso.

Master en Python 3.x. Aprende de 0 a EXPERTO con Práctica.

En este curso aprenderás desde las bases hasta POO en Python Versión 3. Empieza a Aprender ya Mismo de forma Gratuita.

Recuerda que Python es un increíble lenguaje multifunción, con una curva de aprendizaje relativamente baja. Dominando Python podrás profundizar en ***creación de videojuegos, Machine Learning, Inteligencia Artificial, análisis de datos y mucho más.***

Cursos Gratis Online en: https://achirou.com/cursos-gratis
Contenido Gratuito en mis redes: https://achirou.com/redes-sociales
LinkedIn de Gastón Galarza: https://www.linkedin.com/in/gastongalarza/

La mejor Protección en Seguridad Informática, es tu Conocimiento.-
Entre más sepas, más segura estará tu información de los Ciberdelincuentes.

Ruta de Aprendizaje Cloud

Debido al auge de los **entornos Cloud**, se necesita conocimientos de estos entornos para poder trabajar de manera efectiva en el rubro IT. Por supuesto, no es requisito excluyente, pero a medida que más y más empresas cada vez optan por este tipo de entornos para resguardar sus datos, la necesidad de tener al menos, los conocimientos fundamentales, se hace presente.

A lo largo de esta ruta, encontrarás distintos niveles e incluso certificaciones, que te permitirán prepararte para adquirir los conocimientos que necesitas para desarrollarte con éxito en tu trabajo de manera más efectiva o introducirte en la industria IT de manera exitosa.
Empezarás con este curso gratis para luego avanzar en tu formación ***(recuerda dar clic a la imagen).***

Es importante notar que, estas dos rutas te permitirán desarrollarte como un profesional todoterreno. Podrás elegir seguir el camino de especializarte en una, o por el contrario, podrás optar por caminar libremente por múltiples rutas, **las mencionadas aquí y las que vimos en artículos anteriores.**

Junto a esto, y realizando las practicas necesarias, podrás desarrollar todo tu potencial y ser un excelente profesional.

¡Empieza ahora tu formación profesional!

Te dejo, un abrazo digital