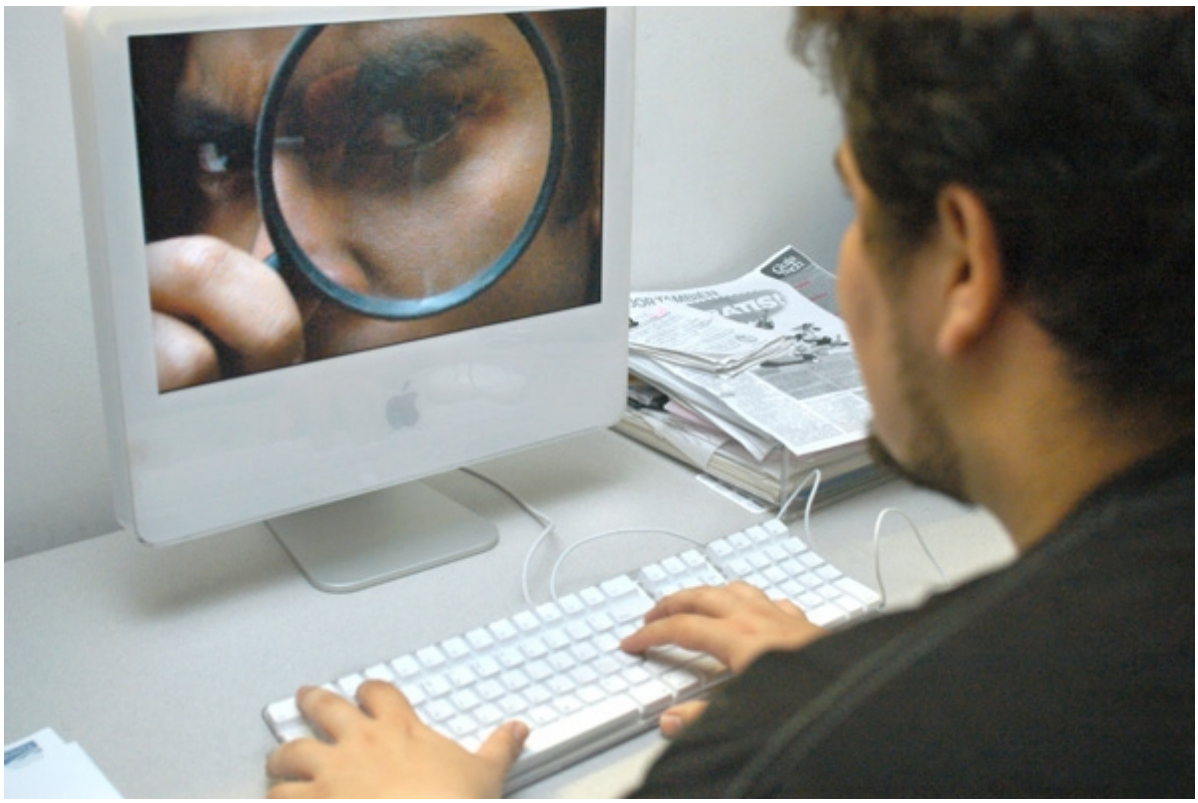
Como siempre, posponiendo el labo. Perdonen pero me lleva mucho tiempo y no tengo un lugar considerable para realmente darle la atención que se merece. Lo tengo por la mitad hasta ahora.

Quería mencionar que por más antisociales que sean, pueden pertenecer a una misma comunidad. Yo en particular, ando en varios grupos en Facebook porque es fácil de ver y rápido de usar. Pueden usar lo que les plazca.

Les dejo el link de un grupo de un amigo: Seguridad Linux/Kali

Hagamos una **introducción a la privacidad.**



“¿Privacidad? Eso es para gobiernos y empresas de alta gama. ¿A quién le va a importar mi privacidad?”

Un delincuente no siempre necesita de algun objetivo de gran valor. Veamos un ejemplo:

Una persona entra a la casa. Prende el Smart TV, agarra un poco de gaseosa de la heladera y de repente suena el teléfono fijo. Contesta.

Víctima: -”Hola.”

Delincuente: -”Tenemos a tu vieja. Apagá los celulares y hace todo lo que te ordene. ¿Me entendiste?”

V: -”¿Perdón? ¿Quién habla?”

D: -”Callate y hace lo que te digo o le vuelo la cabeza. Apagá los dos celulares que tenés encendidos.”

La víctima apaga 1 de los dos celulares, y con el otro intenta marcar al 911 a escondidas.

D:-”Te falta apagar uno. Es una advertencia”.

Apaga el celular, luego de que la llamada no se pudiese concretar, ya frustrado por la situación y asustado por su familiar.

V:-”Ya está. ¿Qué tengo que hacer? Por favor no le hagas nada a mi vieja.”

D:-”Anda al cuarto de tus viejos y fijate en el armario o en la cómoda que ahí hay plata. Pone todo en una bolsa de basura y llevalo a la plaza más cercana. Rápido que te estamos vigilando, no cortes el teléfono.”

V:-”Ahí va, ahí va. Lo estoy haciendo rápido.”

Pasan 5 minutos y la víctima no puede encontrar el dinero.

D:-”¿Qué está pasando? Estás tardando demasiado. Te dije que lo hagas rápido. ¿No entendés?”

V: -Ya desesperado -”¡No encuentro nada! No sé, hay muchas cosas.”

Hay ruido en la puerta. La víctima pensando que era el ladrón se paraliza y se asusta, buscando a toda máquina. Pero quien entra no era ningún criminal, era su madre.

V:-”¿Mamá? ¿Qué hacés acá?”

M:-”Es mi casa ¿O no?”

La víctima se desconcierta y habla por el teléfono.

V:-”A ver, pasame con mi vieja.”

D:-”Está amordazada. ¿Y la plata?”

La víctima lo insulta y corta el teléfono, dándose cuenta de que no era más que una cruel estafa.

Fin de la historia.

Les comento que esta historia esta basada en un hecho real, de Buenos Aires, Argentina.

¿Y se dieron cuenta por qué es tan importante la privacidad de nuestros datos e información?

Analizemos la historia. Lo primero que sucede es que la persona que entra a la casa, prende el **Smart TV**. Estos dispositivos generalmente están conectados **en red** o tienen algún tipo de conexión **bluetooth**. Si es lo primero, suponiendo que alguien pudo entrar en nuestra red, es fácil de identificar si el televisor está encendido o apagado, mandando una petición simple y esperando algún mensaje. Si fuese lo segundo, es aún más fácil que esto. Ya que ni siquiera hay que entrar a la red, sino que simplemente hacer una lectura de los dispositivos con bluetooth en el aire.

Incluso, algunos televisores, son fabricados de tal manera que la contraseña bluetooth de éstos, no son configurables. Es decir que **siempre** tendrá la que viene **por defecto**. Así que tan solo con buscar el manual en internet del modelo especificado, se puede entrar y vulnerar el dispositivo.

Hasta aquí tuvimos **4 supuestas fugas de privacidad** (digo supuestas porque no podemos hacer un análisis a fondo):

-Red sin contraseña o con clave débil.

-Televisor con configuraciones por defecto.

-Se sabe públicamente quien es la madre de la víctima.

-Se conoce el teléfono fijo con la dirección y el nombre de la víctima.

Sigamos analizando. Al parecer, el delincuente tiene algún aparato para conocer el estado de los celulares. La policia tiene acceso a éstos. Entonces ¿Cuál es la fuga? Simple. **Saben el número o los números de celulares.** Así pueden decir cuantos debe apagar.

Por lo próximo, el delincuente le dio a la víctima indicaciones sobre donde debía buscar. Pero finalmente no encontró nada. ¿Qué pasó? Lo que pasó es que el delincuente hizo una **petición estandar**. **¿Quién no tiene un armario o una cómoda en la habitación?** Y ya sabrán que la gran mayoría de las personas guardan cosas escondidas en esos lugares. Esto también es parte de un ataque de **ingeniería social.**

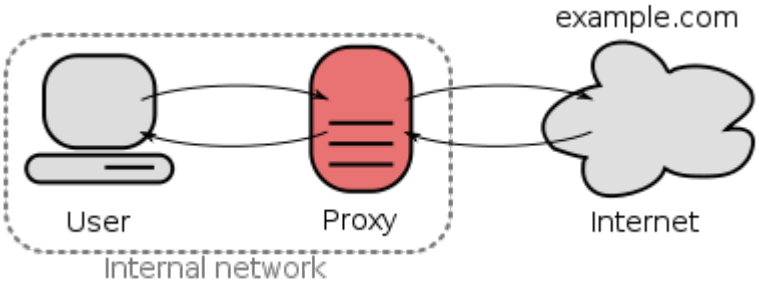
En fin. ¿Vieron qué fácil se puede lograr un ataque usando información? Y este intento de estafa, fue algo **arriesgado** ya que tuvo que interactuar con la víctima. A veces, nuestros datos viajan a través del aire sin ningún tipo de protección y estos pueden ser recolectados sin esfuerzo. Además, muchas veces no lo elegimos. Un ejemplo claro es el televisor inteligente de LG que **envía todos nuestros datos, como qué vemos y donde estamos, a la compañía fabricante.** Si quieren leer más de este televisor pueden ver la entrada en el blog del chema alonso. Link: http://www.elladodelmal.com/2013/11/tu-no-miras-la-tv-ella-te-mira-ti.html

Esto no es todo. Quienes tengan **redes sociales**, aprendan que su información tales como su número asociado, su nombre y apellido, sus caras, sus amigos, sus lugares frecuentados, sus gustos, sus cosas, pueden estar navegando por la red, siendo alojada en algún servidor o siendo vista por personas ajenas. **Facebook guarda toda nuestra información, aunque eliminemos nuestro perfil.** Imaginen el desastre si algún hacker o agencia, se concentrara en tener estos datos. Peor aún, la **NSA** (googlear para más información) **intercepta** millones de mensajes de textos a diario, tiene acceso a todos los smartphone con android y hasta puede entrar a una red wifi sin necesidad de una computadora. Entonces,**¿Cómo nos protegemos?**

De algunas cosas como la NSA es complicado. Podemos intentar cifrar todas nuestras comunicaciones al máximo, pero quizás eso no sea suficiente.**Quizás a lo que apuntamos podría ser el delincuente común** y desconocido, y no a una agencia internacional con un alto presupuesto y personal.

Además de cifrar, deberíamos proteger nuestra información para no publicarla en nuestras redes sociales. Tampoco hace falta dejar la ubicación de google en el celular todo el tiempo, o andar registrándonos en todas las páginas con nuestros datos verdaderos. **Ni hablar de las tarjetas de crédito**, chats públicos, metadatos en los archivos que subimos, bases de datos públicas.

Imaginen además que si a nosotros nos importa nuestra privacidad, lo que le importará pasar como anónimo, al delincuente, porque de ello **depende su libertad**. Mientras el delincuente realiza el ataque, nosotros deberíamos intentar recolectar información para realizar un contraataque o la denuncia correspondiente (más que nada en países donde el contraataque no es legal). Si nosotros somos el **atacante**, debemos proteger nuestra **identidad** a toda costa. Imaginen que nosotros nos comunicamos directamente con una computadora para hacer un ataque, haciendo fuerza bruta. Esto quiere decir que vamos a intentar muchas veces loguearnos al sistema. **Pero el servidor nos va a reconocer y toda información que nosotros mandemos, como nuestra IP, va a ser guardada.** Una de las formas de hacer que esto no suceda es utilizar un **proxy**.



Proxy

Esto es colocar una pc en medio de la atacante y la víctima. Esto quiere decir que la máquina víctima únicamente va recibir un ataque como si fuese de la máquina proxy y no de nuestra pc. Por lo tanto nuestra IP estará protegida. **Eso sí, nuestra IP quedará en el servidor proxy, por lo que es importante conocer si el proxy loguea todos los ingresos, o si es realmente anónimo.** También existen proxys que son bien regulados, y hasta venden sus datos, así que ojo con éstos.

Ultrasurf. Para los **Linuxeros**, podemos disponer de **proxy Squid**. Y para ambos, existen **proxys webs** con los cuales únicamente serán para conectar a páginas, pero también lo vale como herramienta.

Cualquier cosa pueden mandarme mail a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente:

1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

Roadd.
