Bienvenidos! Para aquel que no estuvo en Taringa! cuando comencé a realizar estos tutos, le comento de que va mi intención.

Espero armar un grupo de estudio, comenzando desde lo teórico y escencial (que vamos a tener que aprender temas de muchas ramas), y llegar, si todo se da bueno, a que los alumnos puedan aprender -y no parar nunca de ello- sobre la realidad de esta hermosa técnica.

Este curso es abierto a todos. El requisito indispensable es saber operaciones con fracciones matemáticas (no pienso darles un cursito de matemática de primaria), ya que va a ser necesario para aprender sobre física general.

Primero lo primero. **¿Qué es el Hacking?**

Este es un tema controversial, para todos los que están en contacto con este mundo. Porque se han creado falsas historias, por la no creencia de las historias que aparecen y por los desacuerdos que existen.

El tema es que **nadie** puede realmente decir la etimología de la palabra y entonces **no** dar una **definición** realmente **exacta**.

Vamos a tomar un acuerdo sobre cómo voy a tomar **YO** la definición.

Un **hacker** es una persona con grandes **conocimientos** de tecnología, que logra **aprovechar** el comportamiento de los objetos para su beneficio, utilizando **técnicas** basadas en lo que saben.

"Ok. Entonces ¿Qué pasa si uso un programa hecho por otra persona y clickeo un botón para kakear un jueguito en feisbuk? ¿Soy kaker? "

No, Manolo, no sos "kaker" ya que no sabés que es lo que estas haciendo. Es como creer que porque cortaste un tomate, sos chef.

Ah, y además la palabra "kaker" no es un término válido en el hacking. "Kaker", viene de (por lo menos así lo vi yo) la mismísima T!

Bien, ya que empezamos a tomar un poco de consciencia, sigamos.

Dentro de la "juerga" del hacking, aparecen distintas **clases** de personas (que en realidad, existen en todas las clases de ciencias, pero ya que el hacking está muy apegado a internet, se ve mucho más claro). Y por eso tenemos que **clasificar** a las personas según su**intención**.

Lammer: persona que **cree** ser un hacker, y se **autoproclama** como tal pero que en realidad no lo es. Además puede venir con expansiones como idiotez, trollcidad(? y la arrogancia.

Esta persona es **peligrosa** por la cantidad de **desinformación** que puede llegar a repartir y es **tóxica** por la actitud que toma.

Script-kiddie: este ente, descarga todo lo que se le antepone en el paso, instala 300 toolbar en su navegador, ejecuta programas sin saber qué hacen detrás y busca "como hakear fb" en google. Generalmente, termina **infectando su misma PC** y quedando

como un lindo **target** para troyanos.

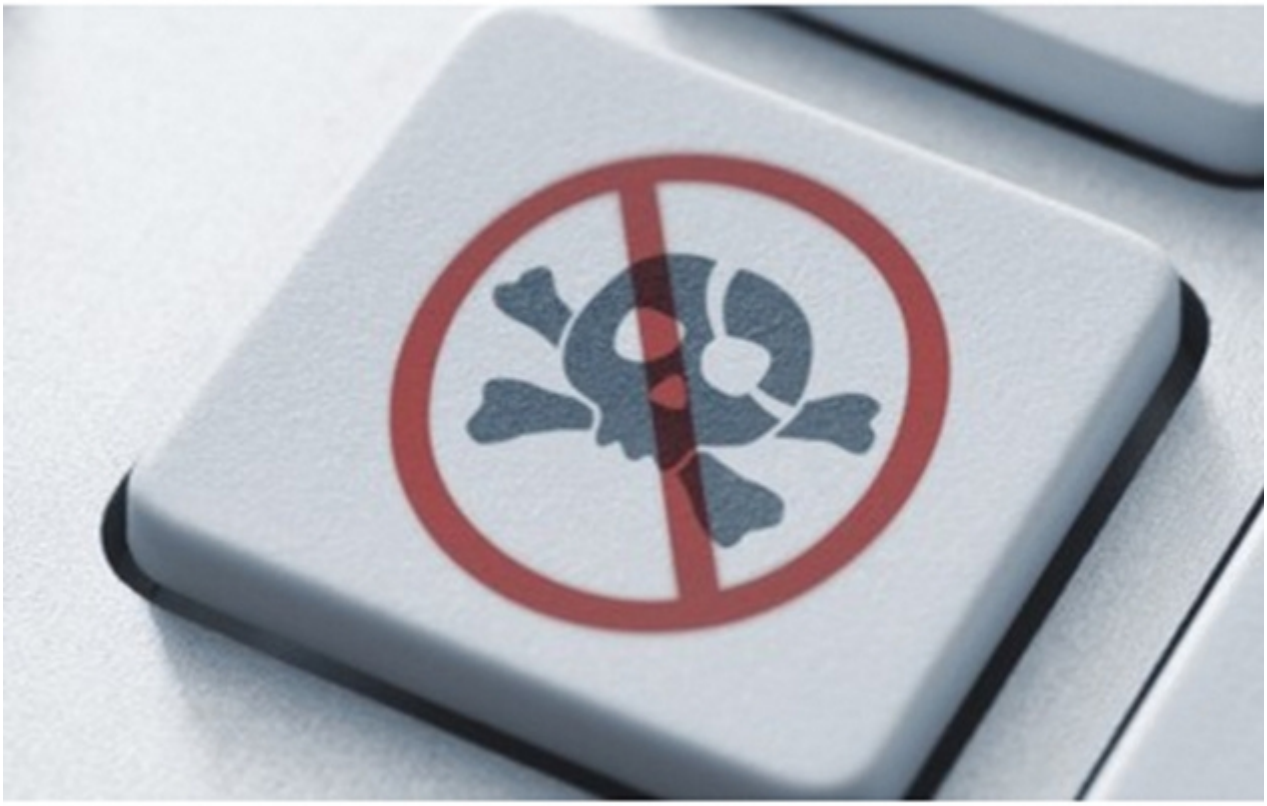
Black hat: hacker con malas intenciones. Roban tarjetas de crédito, expanden **malware**, **roban** información, venden falsificaciones, cometen **estafas**, etc. Los que saben lo que hacen, llegan a producir un buen pozo de jubilación propio. Los demás son perseguidos, encontrados y muertos o **encarcelados**.

White hat: hacker con buenas intenciones. Trabajan para empresas, o son simples **autómatas**. **Encuentran** vulnerabilidades de sistemas y las **reportan** para que las arreglen si es que no las arreglan ellos mismos. Aunque ayudan con la seguridad, también pueden ser o no partidarios del conocimiento libre y reportan a la comunidad externa sus conocimientos.

Sé que andan pululando por internet varios términos más, pero los que se usan son esos nomá'.

Esos términos los voy a usar seguido en estos post que iré haciendo, así que vayan haciéndose familiares a ellos (no se como se escribe familiarizándose, o como sea).

Saben, que una de las cosas que nos apetecen a **TODOS** los usuarios de la tecnología general, es el **malware** (se pronuncia "málwar". Para los brutos del inglés, o partidarios del brutish inglish, vayan aprendiendo este idioma que es elemental para estos estudios).



Entonces **clasifiquemoslos**:

Virus: malware hiperconocido. Generalmente se usa esta palabra para definir a todo el tipo de malware que existe, pero éste tiene características propias. Para entenderlo, vamos a verlo como la gripe, virus biológico, ya que éste sólo cambia el lugar donde hace los estragos.

El virus es un programa, que **infecta ejecutables** y que tiene la habilidad de **reproducirse** (mejor dicho sería propagarse) hacia otros sistemas o archivos.**Generalmente** tienen comportamientos **destructivos**.

Troyano: éste está mal visto (como todo en el hacking, esta pintado de amarillo), y realmente hay una información volando por ahí que hace una equivocación del verdadero comportamiento que tiene un troyano y cuando identificar a un malware como tal.

Un troyano, es código que está **oculto** dentro de las entrañas de un software que dice ser algo más. Claramente, están usando el ingenio social para hacer que una persona caiga y ejecute código sin saberlo. Famosísimos por entrar en los cracks de software pirateado, haciendo que la gente que no puede pagar por estos (o no quiere), termine cerrando el antivirus y ejecutando el código pensando que el antivirus está equivocado. Se usan para ocultar otros tipos de malware.

Backdoor: ya que lo nombramos, vamos a definirlo. Un backdoor, es una manera de dejar "la puerta trasera abierta". Yo sé que esta definición, ahora mismo para quien no tiene conocimientos, es un poco difícil de entender. Pero vamos a quedarnos con eso, con que

es la instalación de una **puerta trasera permanente**, para **garantizarle** al atacante, el **acceso** al sistema cuando quiera hacerlo, **sin** tener la **dependencia** de una vulnerabilidad a parte. Muchas veces viene oculto como un troyano, pero también se usa cuando tiene el acceso a un sistema determinado y quiere volver a entrar en tiempos posteriores y así no tiene que depender de si el sistema de seguridad fue o no parcheado.

Spyware: este tipo de malware es bastante conocido en el ámbito de los internautas habituales, porque es fácil de obtenerlo. Es un programita que roba **información**de navegación, para luego crear estadísticas en masa y venderte publicidad (por ejemplo). Es malware, porque uno no acepta estos términos, o no lo sabe y además usan los recursos de tu sistema para trabajar, por lo que en masa suelen ser bastante poco amigables. Algunos instalan cosas molestas como toolbars, o programas que se inician con el sistema operativo; y otros, están molestando invisiblemente.

Keylogger: demasiado conocido, es difícil de no haberlo visto si tienen más de 20 años, porque en la época que los cyber eran recurridos, éstos abundaban de verdad. Lo que hacen estos bichitos, es **capturar** y guardar todo lo que hagas con las **teclas**, o el mouse. También pueden tener mas funcionalidades como enviar la información a cierto lugar, obtener capturas de pantalla, vista de la webcam, escucha del micrófono conectado, etc. ¡Ojo! Éste tiene un hermano gemelo, llamado de la misma forma pero que funciona por**hardware**, es decir que va conectado como un ps2, entre el teclado y la cpu y guarda todo en una memoria que luego se puede acceder con una combinación de teclas específica.

Adware: estos son creíblemente odiados. Sirven para hacer **propagandas**, generar **plata**. Y el comportamiento habitual es el de mostrarte propaganda en el navegador, u obligarte a usar ciertos buscadores que te implanta como predefinidos.

Worm: también llamados **gusanos**, tienen la habilidad de **duplicarse** a si mismos. Aunque a diferencia de los virus, estos residen en la **memoria** del sistema y **no** tiene la necesidad de **infectar** programas. Se propagan rápido y por diferentes medios. Estos son los que **generan lentitud** en la conexión a internet y en el sistema general. Se utiliza para descargar más malware.

Rootkit: bueno estos son complicados de definir para gente que no recién está empezando. Pero digamos que el rootkit, es un **kit** de**herramientas**, que le permite al atacante **entrar** a un sistema con la mayor cantidad de **privilegios** posibles y **ocultarse** del sistema total. Para esto utiliza una serie de técnicas, editando partes del sistema operativo para su beneficio.

Bug: bueno acá voy a entrar en discordia con algunos del ámbito. El bug, lo considero un malware. ¿Por qué? Bueno el bug es un **mal funcionamiento de código**, es decir que el bug es cuando un programa no hace lo que debería hacer, porque no está desarrollado correctamente.

"Pero no es intencional! Un hacker no hizo ese bug para que vos tengas un mal funcionamiento, es mala suerte."
Bueno Manolo, de a poco vas haciendo preguntas más inteligentes. Pasa, que el bug

puede generar destrucciones en el sistema, instalar backdoors en el mismo y encima le crea una facilidad a un atacante para vulnerar nuestro sistema. Así que viendo el comportamiento, debería considerarse malware.

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

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

1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

Roadd.
