Introducción a la seguridad informática y al hacking:

Este documento tiene la intención de dar un conjunto de lecturas y artículos a considerar antes de dar nuestros primeros pasos en el mundo del hacking.

Con mucho afecto a B3LI4D y a Esteban por ser quienes me apuntaron en la dirección correcta.

Entrando nosotros a un mundo donde los grandes hackers , aquellos que construyeron los pilares de este mundo sopesan la idea de retirarse.

Los cuales iniciaron ya sea con defacements, convivir en BBS y posteriormente en los famosos IRC, en países cuyo brazo legal procuraba más las leyes del mecanismo ferroviario que las intrusiones a los sistemas de cómputo.

Aquellos niños genio del pasado, entre los cuales habría existido más de uno que en pro de su curiosidad llego a cruzar los bordes de la legalidad, que a dia de hoy trabajan en “evil-corp” y tienen un sueldo fijo.

Ahora nosotros entramos a un mundo más estandarizado, donde los recursos sobran y la mediocridad abunda más aún. Ya existen plazas con nombres estándar y certificaciones estándar.

Al inicio pareciera que pocos buenos recursos existen y que la mayoría de lo encontrado nos resulta ininteligible. Al buscar un término encontramos mil más que nos son desconocidos.

Para aquellos que se encuentren en dicha situación, les aseguro que con tiempo y un buen plan de estudio veran que las pocas gotas de conocimiento que les son alcanzables, se convertirá en un mar de temas a su alcance aunque totalmente infinito.

Este mar les permitirá ver de forma más clara los pasos a su próxima meta. Quiero asegurar, el mar no será de conocimientos ya obtenidos, sino de nuevos horizontes a alcanzar.

¿Qué es hacking?, ¿Qué es ser un hacker?

Antes de entrar a este mundo, es importante conocer lo que realmente es un hacker y tener las motivaciones correctas. De otro modo es muy probable terminemos como script-kiddies, buscando tutoriales de phishing en vez de entender el conocimiento que hay detrás de las acciones que realizan y creyendo que hay gran valía en hacer carding.

La definición de hacker variaría de autor en autor, más la ietf lo definió como : “A person who delights in having an intimate understanding of the internal workings of a system”. Podemos extraer de la cita anterior que la palabra no da necesariamente un contexto moral

y más aún, no menciona que tenga relación con la ciberseguridad. Habla de amor por el conocimiento, habla de curiosidad.

Podemos leer la definición completa, y otras importantes como cracker en el siguiente recurso:

https://tools.ietf.org/html/rfc1392

Leer los manifiestos de otros hackers nos puede inspirar y mostrar la actitud correcta: humildad y pasión por el conocimiento.

The Mentor nos dará la visión de los primeros hackers, dando la rebeldía que debe tener un hacker,más aún muestra como no debe llevarnos los deseos egoístas, sino el deseo de aprender.
http://phrack.org/issues/7/3.html

¿Que se necesita para ser un hacker? Lester, un hacker de antaño, nos mostrará los pilares:
http://www.netcomunity.com/lestertheteacher/doc/mimanifiesto.txt

En el siguiente artículo, Roadd nos habla sobre la naturaleza del hacking, y el cómo bordear las cosas es parte de esta cultura.
https://hackingd0.blogspot.com/2016/04/carta-los-aspirantes.html

¿Edad necesaria? ¿Necesito ser un niño que aprendió a programar antes de comer?
https://veteransec.com/2018/09/11/how-i-landed-my-first-infosec-job-in-a-competitive-market-advice-and-takeaways/

En este artículo, Heath Adams (The cybermentor) nos habla sobre todo el camino que lo llevó a ser un senior pentester. Spoiler: “Trabaja duro”

Ahora la pregunta de siempre: ¿cómo empezar?

Tiempo, todo esto no es más que el paso del tiempo, experiencias y robar horas de sueño. Al final del día, se resumirá en el “try harder” que muchas veces veremos como respuesta.

Este video lo ejemplifica bastante bien:
https://www.youtube.com/watch?v=2TofunAI6fU

Como lo mencionado anteriormente, cualquier cosa que aprendamos nos será de provecho, más es sabido que algunos temas necesarios para esta área (y por lo menos básicos) son los siguientes:

-Inglés (A dia de hoy, el 99% de lo que leo está en inglés)
-Programación
-Redes de datos
-Bases de datos
-Sistemas operativos (incluyendo uso de Linux)
-Matemáticas discretas
-Criptografía
-Web
-Hardware
-Privacidad y anonimato

¿Es la seguridad algo tecnológico?

Aunque muchos veteranos en el área consideran dirían que sí. No considero la seguridad y el hacking una disciplina que sea totalmente tecnológica, para prueba de esto: human hacking (Ingenieria social).

Hay grandes lecturas de este tema, pero aquellas que nunca deben faltar es:

Christopher Hadnagy - The science of Human Hacking.
Este libro nos llevará a los pilares de la ingeniería social y como poder influenciar a las personas. También es muy recomendable su podcast, el cual se puede encontrar en:
https://www.social-engineer.com/

Kevin Mitnick, el arte del engaño.

Entonces, la seguridad es más bien una disciplina de manejo de riesgo.

Comunidades:

Antes de entrar a una comunidad, debemos saber que las comunidades bien mantenidas no responderán a ciertas preguntas:

¿Cómo ser un hacker?, ¿Pueden hackear el celular de mi novia? ¿Cómo aprender x,y,z?, ¿Cómo hackear una red social?, ¿Pueden enseñarme de carding?

Aquí hay una guía que nos mostrará como aproximarnos a estas comunidades.
http://www.catb.org/~esr/faqs/smart-questions.html

Un consejo que aplicaría a las comunidades y cursos que busquemos, es recordar que antes de buscar herramientas, deberemos entender lo que queremos hacer en palabras de un “cibernauta”: “Antes de buscar hacer un ataque en redes, busca entender todo lo que pasa desde que escribes un mensaje desde tu computadora hasta que este le llega al remitente”.

La frase anterior aunque fácil a primera vista se separa en distintos temas (Y sus millones de subtemas):

- Programación
- Sistemas Operativos
- Redes
- Bases de datos
- etc.

Antes de buscar pagar cursos, y lecturas. Debemos recordar que buscamos conocimientos profundos, no aprender herramientas (Al menos no al principio). Es entonces, antes de buscar aprender python, buscaremos aprender programación, los paradigmas de programación, etc. Antes de buscar aprender kali, buscaremos aprender a usar linux, y veremos que no es necesario utilizar dicha distribución.

Entonces, podremos muchas veces reconocer un recurso bueno de uno malo en esos términos: “Curso de hacking con kali”, seguramente habla de un curso donde aprenderemos herramientas y seremos deslumbrados por espejos con brillo sin conocer la explicación detrás de nuestras acciones y comandos.

“Dont learn to hack, hack to learn”. No buscamos depender de la automatización, nosotros automatizamos. El deseo profundo de entender cómo funcionan las cosas es lo que nos lleva a ser hackers.

Algunas comunidades y recursos varios (y mis opiniones sobre estas):
comunidades
El orden en que son mencionadas es totalmente intencional, no debemos buscar las ultimas sí no contamos con sólidos conocimientos base.

-The tin Hat
Para temas de privacidad y movimientos sociales en la red (cuenta igual con dominio .onion)
Lo más enriquecedor de este sitio son sus artículos, aunque una pequeña minoría de estos son patrocinado por soluciones de anonimato y privacidad:
https://thetinhat.com/

Telegram es el nuevo IRC: Muchas comunidades (Y grandes personas) comparten sus conocimientos a través de esta red social. Posiblemente encuentres entusiastas de tu edad e incluso que hablen tu mismo idioma.

-Hacking desde 0:
Esta es de las comunidades a mi parecer mejor mantenidas. Dentro de su blog cuentan con clases gratuitas las cuales serán muy útiles para dar nuestros primeros pasos.
https://hackingd0.blogspot.com/?m=1

-Undercode:

Considero esta comunidad tiene un gran foro y liberan una revista gratuita llamada underdocs. Solo no recomiendo su grupo de telegram, ya que este no está tan filtrado de script kiddies
https://underc0de.org/

-The cybermentor:

Es un gran profesor, tiene cursos gratuitos en youtube sobre distintos tópicos y un curso de pentesting en udemy. Cursos como “pentesting for noobs” nos dan una introducción a la metodología y herramientas que se usarán en este día a día..

Recomiendo revisar su canal de youtube, twitch y el curso de udemy que este ofrece:

https://www.twitch.tv/thecybermentor
https://www.youtube.com/c/thecybermentor

-Vulnhub:

Este sitio está lleno de recursos (laboratorios, retos, etc) para iniciarnos en el pentesting, e internet está lleno de resúmenes (write-ups) los cuales nos pueden ayudar inicialmente a adquirir la metodología.
https://www.vulnhub.com/

-HackTheBox:

Una vez que tenemos ciertos conocimientos base, podemos acercarnos a comunidades como hackthebox. Cabe aclarar, el reto mismo de entrada no es algo que debamos falsear, de no pasarlo, muy seguramente no estamos preparados para ingresar a esta plataforma.
https://www.hackthebox.eu/

-IppSec:

Este canal de youtube cuenta con buenos writeups, los cuales nos enseñarán como un pentester resuelve las máquinas que a nosotros nos parece imposibles. Su página contiene búsqueda temática, donde podemos aprender distintas formas de explotar vulnerabilidades o las nociones básicas de ciertos servicios.
https://ippsec.rocks/

Volviendo a la analogía del mar, es el momento de zarpar a nuestras primeras aventuras. Happy Hacking!

-Héctor Espino