7 PASOS PARA ser un Pentester

Karina Astudillo B.

7 PASOS PARA SER UN PENTESTER

Qué debes hacer para convertirte en Hacker Ético

Por:

Karina Astudillo B.

https://www.KarinaAstudillo.com

Nota de descargo

Dedicatoria

A Dios y a mi amada familia, por ser mis pilares de soporte y mis fuentes de inspiración.

Tabla de contenido

Prólogo

En la actualidad las amenazas informáticas están a la orden del día, leemos frecuentemente en los periódicos titulares acerca de robos de identidad, fraudes electrónicos, clonación de tarjetas de crédito, intrusiones en sitios web, ciberacoso en las redes sociales, etc.

Ante estos peligros los usuarios se hacen preguntas como ¿Puedo comprar de forma segura a través de Internet? ¿Qué hago si suplantan mi identidad? ¿Cómo protejo a mis hijos del ciberacoso?

Por otro lado, los empresarios se plantean interrogantes como ¿Puedo evitar que roben nuestra información? ¿Cómo recupero la reputación ante mis clientes si hackean mi red? ¿Existen formas de determinar si mis sistemas son vulnerables y prevenir hackeos?

Y frente a todas estas dudas, es el deber de los profesionales en seguridad informática plantear soluciones que permitan darle tranquilidad tanto a las organizaciones como a los usuarios, para que puedan hacer uso del Internet y de sus sistemas informáticos sin caer presos de la paranoia.

Tal vez suene a broma, pero tengo amigos tan paranoicos, debido a eventos negativos que han vivido, que cuando reciben un correo informativo de su Banco tienen miedo siquiera de abrirlo porque piensan que con sólo abrir el mensaje van a tomar control de su computador y les van a robar sus credenciales.

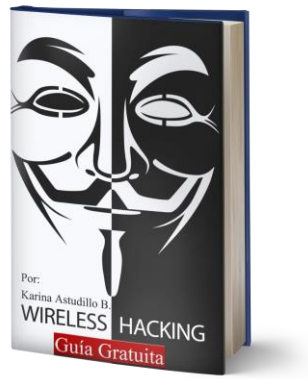
En realidad, comprendo su paranoia, pues en algún momento fueron víctimas de phishing[i] u otras estafas electrónicas, pero quienes trabajamos en sistemas sabemos que usualmente se requieren más pasos que solamente abrir un mensaje de correo para capturar credenciales o poder explotar una vulnerabilidad que nos dé control remoto de un computador.

Debido a esto, hoy más que nunca, se necesitan expertos en seguridad informática que puedan detectar potenciales huecos de seguridad y prevenir posibles intrusiones o amenazas informáticas, antes de que estas se materialicen. Me refiero por supuesto a los hackers éticos o también denominados pentesters.

Por tanto, si es usted un entusiasta de la seguridad informática que desea convertirse en pentester lo invito a seguir leyendo.

Regalo para mis lectores

En agradecimiento por haber obtenido este libro, quiero obsequiarle mi Guía GRATUITA sobre Hacking de Redes Inalámbricas.



Si no la tiene aún, puede conseguirla en: https://www.academia-hacker.com/libros

¿Por qué se necesitan pentesters o hackers éticos?

Muy simple, para defender a las personas y empresas de hackers maliciosos - también llamados crackers - dispuestos a usar sus conocimientos para efectuar estafas electrónicas, causar daños a la información, suplantar identidades, liberar malware, etc., con el ánimo de perjudicar a las personas y corporaciones y lucrar a sus expensas.

De hecho, de acuerdo con el Europe's Cybersecurity Skills Gap Report de 2019[ii], la demanda global por expertos en ciberseguridad supera con creces la oferta en los países de forma global, representando esto una enorme oportunidad para quienes deseen convertirse en hackers éticos.

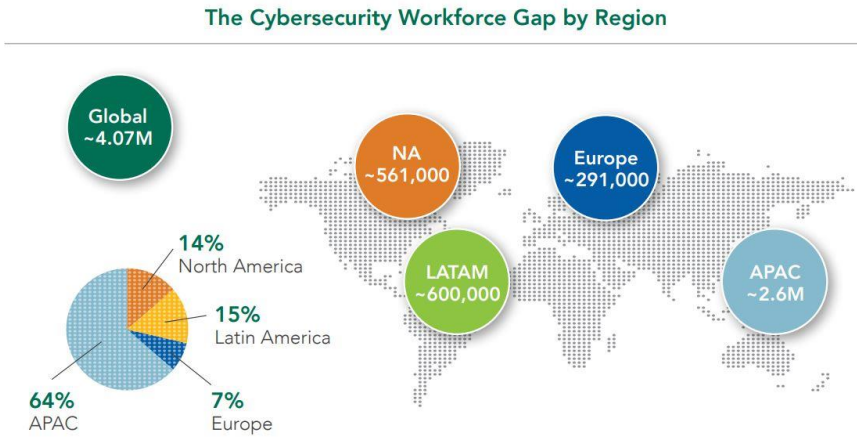


Figura 1 – Brecha de trabajadores en ciberseguridad por región. Fuente: Europe's Cybersecurity Skills Gap Report 2019.

¿En qué consiste el trabajo de un pentester o hacker ético?

El objetivo de un pentester o hacker ético es efectuar pruebas de intrusión controladas sobre la infraestructura informática de una organización, para detectar vulnerabilidades o huecos de seguridad que puedan explotarse y, posterior a ello, emitir un informe de auditoría que incluya recomendaciones de remediación para mitigar las posibles amenazas a la seguridad de la información.

En consecuencia, un pentester debe pensar y actuar como lo haría un cracker o hacker malicioso, pero sin afectar la operatividad de los activos informáticos del cliente y actuando de forma ética.

Las empresas y los profesionales de seguridad informática que se dedican a brindar servicios de hacking ético usualmente firman contratos formales - previo a la ejecución de las pruebas de intrusión - que incluyen cláusulas sobre confidencialidad para garantizarle al cliente la seguridad de su información.

Por este motivo, es muy importante que los consultores que conduzcan las pruebas de intrusión o pentesting estén altamente calificados en materia de seguridad informática, pero que además tengan un código de conducta profesional alineado con valores éticos en el tratamiento de la información de sus clientes.

¿Cuál es el salario de un pentester o hacker ético?

Los ingresos de un hacker ético profesional pueden variar mucho, dependiendo del país en el que trabaje, pero de acuerdo a la empresa PayScale el salario promedio anual de un pentester en Estados Unidos es de USD$118,922.[iii]

Lamentablemente, no nos fue factible encontrar datos estadísticos respecto a salarios de expertos en seguridad informática en Latinoamérica.

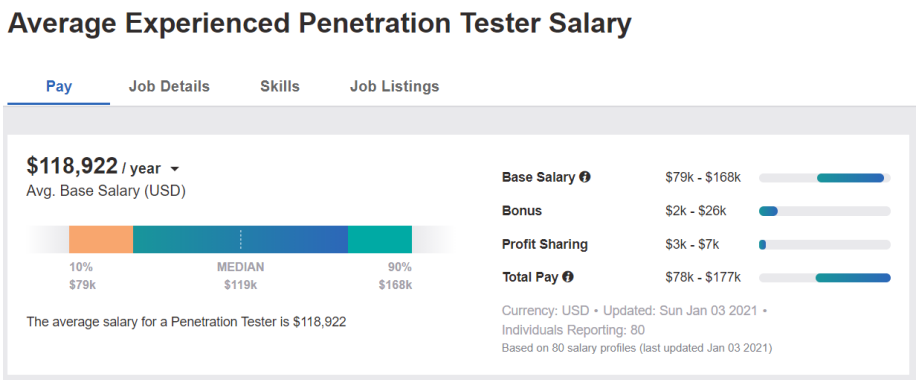


Figura 2 - Salarios de un pentester en Estados Unidos. Fuente: PayScale.

Los 7 pasos para convertirse en pentester o hacker ético

Si está pensando usted en sumarse a los expertos en seguridad informática a nivel mundial y convertirse en hacker ético profesional, de acuerdo con mi experiencia hay 7 pasos que debe seguir para lograrlo:

Figura 3 - Los 7 pasos para ser un pentester. Fuente: la autora.

Paso 1: Adoptar mentalidad de hacker ético

Pensar como un hacker ético implica varios elementos:

Figura 4 - La mentalidad de un hacker ético.

PENSAR FUERA DE LA CAJA

Efectuar tareas de pentesting requiere en ocasiones de mucha creatividad para poder detectar vulnerabilidades que podrían pasar desapercibidas para el común de los mortales.

Por ello, es importante que el aspirante a hacker ético mantenga su curiosidad y desarrolle su creatividad, sin limitarse a simplemente creer lo que le reportan las herramientas de software.

En el día a día, la capacidad para ir más allá y *"pensar fuera de la caja"* será lo que diferencie a un pentester competente de un simple "script kiddie"[iv].

Hasta hace unas décadas atrás se creía que la creatividad era una habilidad poseída por unos pocos iluminados y que no podía enseñarse a alguien a ser creativo. Sin embargo, estudios actuales sugieren que algunos aspectos de la creatividad podrían en efecto enseñarse y por tanto aprenderse[v].

Edward De Bono, autor del libro "El pensamiento lateral"[vi], propone el uso de ejercicios y técnicas para ejercitar la mente y así fomentar la creatividad.

DISFRUTAR DE RESOLVER PROBLEMAS COMPLEJOS

Además de ser creativo, un hacker ético debe estar dispuesto a enfrentarse a problemas complejos sin sentirse frustrado o estresarse. Por el contrario, a los pentesters de corazón encontrarse con un objetivo difícil de hackear les resulta divertido y los anima a dedicarse más a la búsqueda de huecos de seguridad que puedan explotarse.

Por tanto, si es usted de los que se desanima al primer contratiempo, tal vez la profesión de hacker ético no sea para usted. Pero si es usted persistente, ¡entonces está en la ruta adecuada!

MANTENER VALORES ÉTICOS Y RESPETAR LA CONFIDENCIALIDAD

Al ejercer la profesión de hacker ético se topará a menudo con información confidencial que de revelarse a terceros podría afectar seriamente la imagen de sus clientes e, inclusive, generarles pérdidas económicas.

Por este motivo, las empresas se cuidan mucho de con quién hacen negocios, en especial cuando la contratación de un servicio podría traer consecuencias negativas si el mismo no se brinda con el profesionalismo del caso.

En este sentido es primordial establecer una buena reputación profesional, respetando siempre la confidencialidad de sus clientes, obrando en base a las mejores prácticas recomendadas por la industria y respaldando sus acciones mediante acuerdos legales que garanticen a los clientes que se mantendrá las reservas del caso si durante el pentesting llegara a sus manos información restringida.

COLABORAR CON PROYECTOS DE CÓDIGO ABIERTO

Aunque este no es un paso obligatorio para convertirse en pentester, colaborar con proyectos de código abierto puede ayudarlo a usted de varias formas:

- Comprendiendo cómo funcionan internamente librerías y herramientas populares usadas por numerosos sitios web y organizaciones a nivel mundial.
- Enterándose de primera mano cuando se descubre una vulnerabilidad en el código de uno de estos proyectos.
- Teniendo acceso a otros desarrolladores experimentados que suelen colaborar en estos proyectos y de los que puede aprender.

COMPARTIR INFORMACIÓN ÚTIL CON LA COMUNIDAD

A pesar de que este paso tampoco es obligatoriamente requerido para convertirse en un hacker ético, compartir información es parte de la cultura hacker y es una forma de devolver a la comunidad lo que aprendemos de ella.

Por otro lado, compartir información gratuitamente puede ayudarlo a ganar popularidad dentro de la comunidad de seguridad informática, lo que a su vez redunda en marketing de boca en boca.

Paso 2: Aprender los fundamentos técnicos

Para poder comprender conceptos sobre seguridad informática y especializarse luego en hacking ético, es necesario contar previamente con una sólida base de conocimientos técnicos sobre:

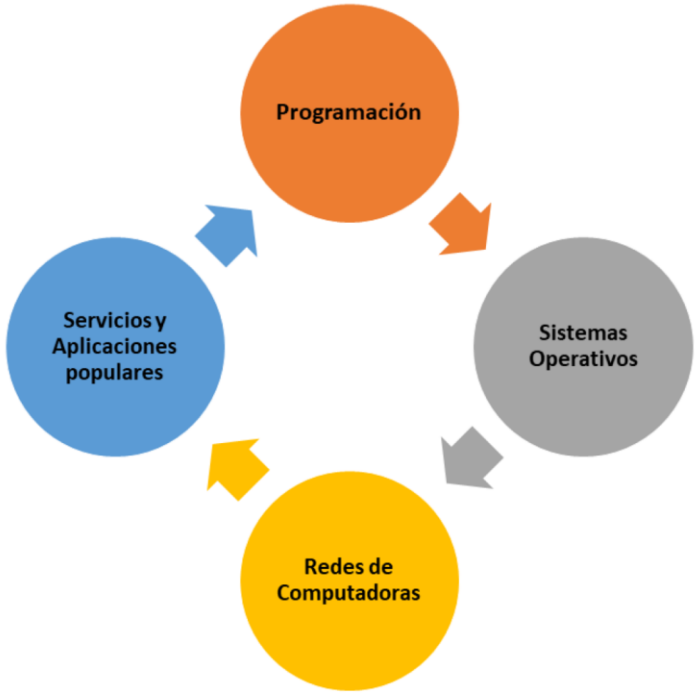


Figura 5 - Fundamentos técnicos requeridos por un pentester.

Lo anterior se debe a que durante un hacking ético se detectan y explotan vulnerabilidades sobre la infraestructura informática de una organización, y esa infraestructura está mayoritariamente compuesta de equipos de comunicaciones y servidores interconectados en red, los cuales son un conjunto de hardware más software. Y dentro del software necesario para que estos dispositivos puedan funcionar se hallan sistemas operativos, servicios y aplicaciones.

Por ende, se vuelve evidente que un pentester debe conocer sobre todos estos temas para poder realizar un buen trabajo.

APRENDER A PROGRAMAR

Si en realidad es su deseo convertirse en hacker ético deberá aprender a programar y conocer diversos lenguajes de programación, scripting y bases de datos.

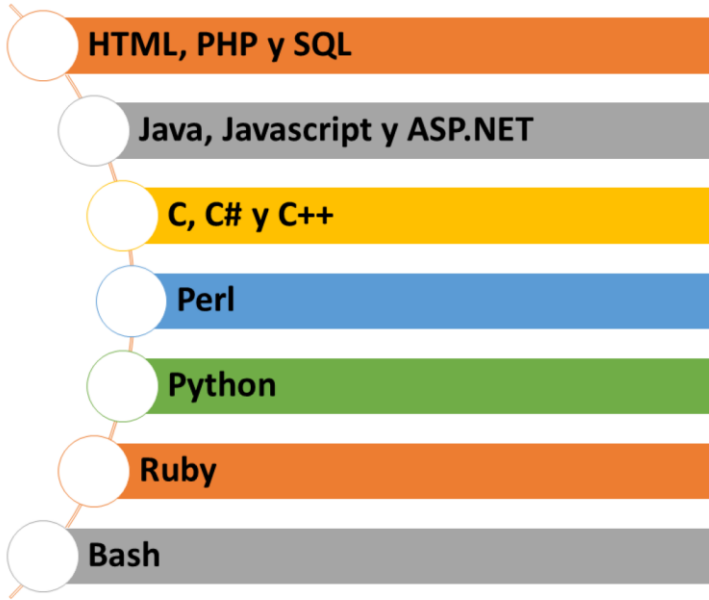


Figura 6 - Lenguajes populares de programación

Algunos de estos lenguajes son necesarios porque son ampliamente utilizados en servidores web o por aplicaciones populares (ej: html, php, sql, java, javascript, asp.net, etc.), mientras que otros son más bien utilizados para escribir exploits[vii] o para realizar ingeniería inversa[viii].

Si usted es un estudiante o profesional de la carrera de computación o sistemas, seguramente tendrá al menos una materia de programación dentro de su malla curricular. No obstante, si no es este su caso, no se desanime, no es necesario cursar una carrera universitaria para aprender a programar (que no lean esto mis colegas de la ESPOL).

De hecho, existen muchas plataformas educativas de gran prestigio que ofrecen cursos de programación gratuitos o pagados de forma online, de modo que ni siquiera tendrá que dejar la comodidad de su hogar para aprender a programar, en tanto cuente con un computador con acceso a Internet.

Estos son algunos de los MOOCs[ix] más populares que incluyen entre sus programas cursos de programación:

- **Udemy:** https://www.udemy.com/
- **Codecademy:** https://www.codecademy.com/
- **Coursera:** https://www.coursera.org/
- **EdX:** https://www.edx.org/es
- **Udacity:** https://www.udacity.com/
- **Lynda:** https://www.lynda.com/

APRENDER SOBRE SISTEMAS OPERATIVOS

Como mencionábamos previamente, todos los dispositivos de red tienen componentes de hardware y software, de los cuales el sistema operativo es sin duda el elemento medular.

De acuerdo con Stallings (2012),[x] los sistemas operativos proveen una interfaz a los usuarios para que los mismos puedan interactuar con las aplicaciones y que estas a su vez sean capaces de utilizar los recursos de hardware de un computador.

Figura 7 - Sistemas operativos populares

Dado que los sistemas operativos son codificados en un lenguaje de programación por desarrolladores humanos (al menos a la fecha, hasta que las AI[xi] estén más maduras), no están libres de errores y los mismos pueden conllevar huecos de seguridad con niveles de riesgos bajos, medios o altos.[xii]

Estos son unos pocos ejemplos de vulnerabilidades graves relativas a sistemas operativos:

- **Autenticación abierta:** autenticarse en el sistema operativo sin suministrar credenciales.
- **Elevación de privilegios posible:** capacidad de convertirse en usuario administrativo desde una cuenta limitada sin conocer la clave del usuario administrador.
- **Susceptibilidad DoS:** denegación de servicios.
- **Remote File Upload:** subir/descargar información confidencial sin necesidad de autenticarse.

Para mantenerse al tanto de las últimas vulnerabilidades descubiertas, tanto en sistemas operativos como en aplicaciones, conviene revisar las siguientes fuentes:

- **Mitre Common Vulnerabilities and Exposure:** https://cve.mitre.org/

- **US National Vulnerability Database:** https://nvd.nist.gov
- **CERT Vulnerability Notes Database:** http://www.kb.cert.org/vuls/
- **Rapid 7 Vulnerability and Exploit Database:** https://www.rapid7.com/db

Adicionalmente, los fabricantes de equipos de comunicaciones, servidores, sistemas operativos y aplicaciones suelen tener boletines de noticias en donde publican los procedimientos de remediación o parches que deben aplicarse cuando descubren una vulnerabilidad en sus productos.

He aquí un listado de boletines de seguridad de algunos de los fabricantes más populares:

- **Boletines de seguridad de Microsoft:** https://technet.microsoft.com/en-us/security/bulletins.aspx
- **Boletín de seguridad de Android:** https://source.android.com/security/bulletin/
- **Boletines de seguridad de la comunidad Linux:** http://www.linuxsecurity.com/content/section/3/170//engarde_advisory-4135.html
- **Actualizaciones de seguridad de Apple:** https://support.apple.com/en-us/HT201222
- **Avisos de seguridad de Palo Alto Networks:** https://securityadvisories.paloaltonetworks.com/
- **Alertas de seguridad de Cisco Systems:** https://tools.cisco.com/security/center/publicationListing.x
- **Avisos de seguridad de Checkpoint:** https://www.checkpoint.com/security-advisories-subscription/

Finalmente, no siempre los creadores de sistemas operativos o las organizaciones oficiales como el CERT o el NIST, son los primeros en enterarse de las vulnerabilidades informáticas. En muchos casos las vulnerabilidades son descubiertas por terceros, y dependiendo de la ética de ese tercero puede ser que decida reportarla al fabricante para darle oportunidad de liberar un parche antes de compartirla con el público, que decida venderla como vulnerabilidad de día cero a una empresa de seguridad cuyo negocio sea la venta de exploits, que decida escribir un exploit él mismo para aprovechar la vulnerabilidad en silencio y lucrarse hasta que esta se haga pública, o que opte por vender el exploit al mejor postor en sitios ilícitos de la dark web[xiii].

Debido a lo anterior, es importante que el lector se suscriba a blogs de seguridad informática no sólo de los chicos buenos, sino inclusive de los crackers del lado oscuro de la fuerza. Este es un periódico electrónico gratuito sobre noticias de seguridad informática que publico semanalmente y al que el lector puede suscribirse si lo desea:

- **Seguridad Informática Fácil - Noticias:** http://news.seguridadinformaticafacil.com

Si desea aprender a usar y administrar sistemas operativos, lo invito a buscar entre los cursos gratuitos y pagados, publicados por los diferentes MOOCs listados en la sección previa.

APRENDER SOBRE REDES DE COMPUTADORAS

Sin redes de computadoras no estaríamos interconectados y no existiría el Internet… tiemblo sólo de pensar cómo pude vivir mi infancia sin Internet, de hecho juraría que sentí un escalofrío cual película de terror escribiendo estas líneas.[xiv] En fin, una red de computadoras es un conjunto de dispositivos de cómputo que pueden compartir recursos a través de un medio de comunicación.[xv]

Y puesto que nuestro objetivo como pentesters es probar las vulnerabilidades de la infraestructura informática de una organización, pues es seguro que esa infraestructura consistirá de diversos dispositivos de cómputo interconectados en red.

Debido a esto, es de sentido común que un pentester deba conocer conceptos sobre redes de computadoras para poder efectuar su trabajo de forma eficiente y responsable.

Estos son algunos conceptos básicos que sí o sí un hacker ético debe conocer:

- Tipos de redes de computadoras y medios de comunicaciones
- Modelos de arquitectura de red (OSI, TCP/IP)
- Direccionamiento IPv4, IPv6 y cualquier versión futura que aparezca
- Protocolos de comunicaciones (capas 1 a 7)

Aparte de los cursos disponibles en los MOOCs antes mencionados, vale destacar la iniciativa de un reconocido fabricante de comunicaciones que tiene a su haber, de forma global desde hace ya 20 años, programas de capacitación para promover los conocimientos sobre redes de computadoras y, dicho sea de paso, popularizar su marca y sus certificaciones internacionales. Me refiero a Cisco Systems:

- **Cisco Networking Academy Program (CNAP):** https://www.netacad.com/

Mi empresa, Elixircorp, representa diversas marcas de comunicaciones entre las que ya no está Cisco, dado que dejamos de vender sus productos hace ya varios años, y aunque he sido instructora del programa CNAP desde el 2003, también lo he sido para otras marcas reconocidas. Por tanto, les puedo asegurar que mi mención al programa CNAP no la hago con ningún fin comercial, sino porque en mi larga trayectoria profesional he visto pocos fabricantes que le pongan tanta dedicación y esmero a sus programas de capacitación como Cisco.

SERVICIOS Y APLICACIONES POPULARES

Además de aprender sobre protocolos de comunicaciones como TCP, UDP, RIP, OSPF, BGP, etc., es importante poner atención especial a aquellos más populares que se encuentran en la capa 7 del modelo OSI… me refiero por supuesto a los servicios y aplicaciones.

¿Pero por qué la diferencia en la terminología? ¿No son los servicios aplicaciones acaso? En efecto, los servicios son aplicaciones que tienen la particularidad de implementar capacidades de comunicación. Estas capacidades de comunicación suelen implementarse en la modalidad cliente-servidor, pero nada impide que se lo haga en modo peer-to-peer.[xvi]

Algunos servicios populares que un pentester debería comprender:

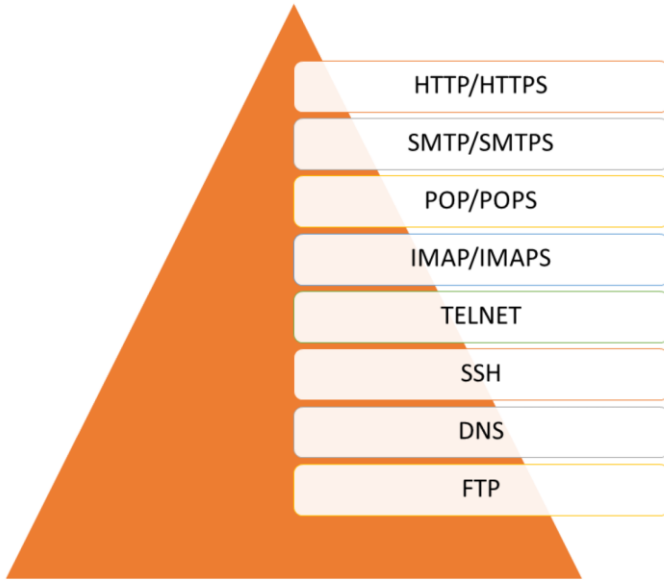


Figura 8 - Servicios populares.

Algunas aplicaciones que conviene revisar:

- Apache Web Server
- Microsoft Internet Information Services (IIS)
- Nginx
- Wordpress
- Joomla

- Drupal
- Sendmail
- Zimbra
- Adobe Flash
- Adobe Acrobat Reader
- Firefox
- Chrome
- Internet Explorer
- Microsoft Outlook
- Thunderbird
- My SQL
- MS SQL
- Oracle DB

Paso 3: Aprender sobre Seguridad Informática

Dado que el Hacking Ético es parte de una rama más amplia, como lo es la Seguridad Informática, un pentester debe adentrarse en sus conceptos, puesto que los mismos le resultarán muy útiles a la hora de ejecutar pruebas de intrusión.

¿Y qué es la Seguridad Informática? También llamada ciberseguridad, es el área de la informática que se relaciona con la protección de los activos informáticos e involucra aspectos de seguridad de la información[xvii] como son la disponibilidad, integridad y confidencialidad de la misma.[xviii]

Dentro del área de seguridad informática hay muchas subramas en las que un profesional puede especializarse, entre las que destacan las siguientes:

- **Hacking Ético:** ejecución de pruebas de intrusión controladas sobre la infraestructura informática de una organización, con el fin de efectuar recomendaciones de remediación para solventar las vulnerabilidades halladas.
- **Cómputo Forense:** extracción y análisis de evidencia digital, utilizando técnicas forenses de manejo de evidencia, para determinar por qué ocurrió un evento, cómo sucedió, determinar responsabilidades, recuperar información y efectuar recomendaciones para evitar que este se repita a futuro.
- **Auditoría de Sistemas:** consiste en el análisis y recopilación de información para determinar si un sistema de información cumple con criterios de seguridad, determinar las posibles brechas presentes y cómo solventarlas.
- **Auditoría de Código:** se trata del análisis detallado del código fuente de programas para determinar si estos cumplen con las mejores prácticas de codificación referentes a mantenibilidad, seguridad, eficiencia, portabilidad y confiabilidad.

- **Auditoría de Procesos:** estas consisten en la revisión de procesos y procedimientos para determinar si se cumple con una norma o estándar, detectar no-conformidades y realizar recomendaciones para alcanzar el cumplimiento. La auditoría de procesos puede centrarse solamente en el área de sistemas (COBIT, ITIL, SAS-70), en procesos de comercio electrónico con tarjetas de crédito (PCI-DSS) o en la seguridad de toda la cadena de valor de la organización (ISO-27001/27002).

Si el lector desea especializarse en Seguridad Informática puede comenzar tomando cursos a través de las plataformas educativas online (MOOCS) indicados en el Paso 2 de este libro, o puede optar por registrarse en una carrera formal en una universidad.

Si el lector está en Ecuador, la Escuela Superior Politécnica del Litoral (ESPOL) ofrece la Maestría en Seguridad Informática Aplicada (MSIA), programa en que se dictan materias relacionadas con todas las subramas mencionadas previamente.

De igual forma mi empresa, Elixircorp, dicta talleres especializados en Seguridad Informática abiertos al público en Guayaquil y Quito y en modalidad in-house[xix] en otras ciudades *dentro y fuera de Ecuador*.

Paso 4: Aprender a efectuar Pruebas de Intrusión

Al fin hemos llegado al meollo del asunto: la ejecución de pruebas de intrusión, también denominadas bajo el nombre de hacking ético.

¿Pero qué es un hacker? De forma general un hacker es un experto en un tópico dado que no necesariamente es seguridad informática. Por tanto, se puede ser un *Life Hacker*, un experto en usar trucos o tips para mejorar la productividad o eficiencia, un *Windows Hacker*, alguien que sabe todos los atajos de Windows para optimizar su uso, un *Growth Hacker*, un experto en tomar empresas en fase de desarrollo y hacerlas crecer, etc.

En relación con nuestro tópico de interés, un hacker es un experto en seguridad que se especializa en efectuar pruebas de intrusión en sistemas informáticos. Y aunque ha habido mucha confusión entre el público debido a un mal uso del término por parte de cierta prensa, el ser hacker no implica ser un delincuente informático. Los hackers que pertenecen al lado oscuro de la fuerza se denominan crackers o hackers de sombrero negro (black-hat-hackers), y - para evitar confusiones - los chicos buenos nos auto denominamos hackers éticos o hackers de sombrero blanco (white-hat-hackers).

¿Y en qué consiste un hacking ético? ¿Y cómo se diferencia de un hacking no-ético? Para ello debo referirme al famoso Círculo del Hacking, que no es nada más que las fases que sigue un hacker para penetrar en sistemas informáticos:

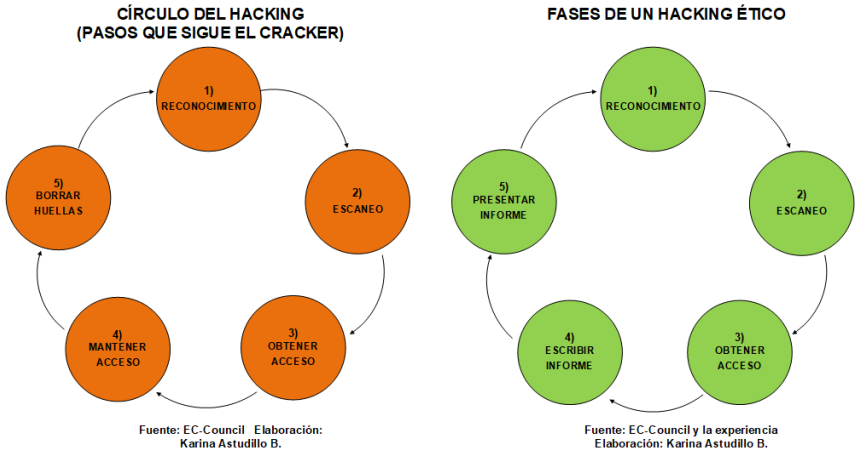


Figura 9- Círculo del Hacking. Fuente: Figura 1. Astudillo, K. (2016) Círculo del Hacking. Reproducida de HACKING ETICO 101: Cómo hackear profesionalmente en 21 días o menos! 2da Edición (Pág 13). Editorial CREATESPACE.

Como se desprende del gráfico anterior, tanto hackers éticos como crackers ejecutan por igual las 3 primeras fases de un hacking y hay una variación en las 2 últimas fases.

Todo hacking empieza con un reconocimiento, en el cual se trata de recopilar la mayor cantidad posible de información sobre el objetivo o víctima, como, por ejemplo: a qué se dedica la organización, ubicación de oficina matriz y sucursales, principales directivos, números de teléfono, correos electrónicos, nombre del dominio de la organización, nombres de hosts, direcciones IP, etc.

Luego, en la fase de escaneo, se trata de recabar más información sobre los hosts descubiertos en la fase previa como: versiones de sistemas operativos, puertos abiertos, versiones de aplicaciones, vulnerabilidades presentes, riesgos asociados, exploits disponibles, etc.

Posteriormente, en la fase de obtener acceso, se explotan las vulnerabilidades detectadas durante el escaneo. Pero aquí vale aclarar que crackers y pentesters obran de diferente manera. Mientras al cracker sólo le interesa conseguir su objetivo de penetrar las defensas de su víctima ya sea para robar información, efectuar una estafa electrónica, usarlo como intermediario para atacar a un tercero, o simplemente hacer daño… el hacker ético efectuará un análisis minucioso de las vulnerabilidades presentes para determinar cuáles son seguras de explotar sin causar daño a la operatividad del cliente.

Sobre hacking ético hay mucha información gratuita publicada en Internet de forma un tanto escueta, y lamentablemente la gran mayoría está solo en idioma inglés, lo que complica su

aprendizaje a los iberoamericanos que no dominan esta lengua. Estos son algunos blogs en idioma español que presentan información sobre pentesting:

- **Blog de Seguridad IT - Elixircorp:** http://blog.elixircorp.com/
- **Blog de Open-Sec:** http://ehopen-sec.blogspot.com/
- **El Lado del Mal:** http://www.elladodelmal.com/
- **DragonJAR:** https://www.dragonjar.org/blog

También los MOOCS mencionados en el Paso 2 tienen cursos relacionados con hacking ético que el lector puede revisar. O, si me lo permite el lector, lo invito a visitar mi academia, **Academia Hacker (https://www.academia-hacker.com)**, en donde encontrará videocursos y cursos live-online sobre pentesting, cómputo forense y ciberseguridad.

Paso 5: Aprender a realizar ingeniería inversa

La ingeniería inversa de software es el proceso de aprender cómo está hecho un programa y cómo funciona internamente, a través de la extracción y el análisis de sus partes.[xx]

Aplicado a nuestra área de interés, la ingeniería inversa de una aplicación X nos permitirá conocer si existen vulnerabilidades o huecos de seguridad en el código que podamos explotar a través de la elaboración de un exploit.

Puesto que es posible explotar vulnerabilidades conocidas utilizando exploits elaborados por terceras partes, como por ejemplo los incluidos con frameworks de explotación[xxi], la ingeniería inversa de software es un tópico avanzado al que usualmente se recurre cuando no se logra

encontrar puntos vulnerables de acceso a la red objetivo o cuando nos enfrentamos a vulnerabilidades de día-cero para las que no existen aún exploits disponibles.

La ingeniería inversa nos será sumamente útil además si un cliente nos contrata para auditar la seguridad de una aplicación o si tenemos que analizar malware.

Paso 6: Obtener Certificaciones Internacionales

Una vez usted haya ganado conocimientos y experiencia tanto en Seguridad Informática como en Hacking Ético, será el momento apropiado para obtener certificaciones internacionales en estas áreas.

¿Pero por qué certificarse? Pues, porque poseer una o varias certificaciones internacionales en tópicos especializados le brindará un aval ante los potenciales clientes que aún no conocen la calidad de su trabajo.

En la tabla siguiente se muestran varias certificaciones relacionadas con Seguridad Informática:

Certificación	Organización
Certified Information *Systems* Security *Professional (CISSP)*	*ISC²*
Systems Security Certified Practitioner (SSCP)	*ISC²*
Certified Information Security Manager (CISM)	*ISACA*
Global Information Assurance Certification (GIAC)	*GIAC*
Information Technology Security	*Brainbench*

Tabla 1 - Certificaciones de Seguridad Informática. Fuente: Tabla 17. Astudillo, K. (2018) Certificaciones de Seguridad Informática (general). Reproducida de HACKING ETICO 101: Cómo hackear profesionalmente en 21 días o menos! 2da Edición (Pág 270). Editorial Createspace.

Y estas son algunas de las certificaciones más reconocidas en materia de Hacking Ético:

Certificación	Organización
Certified Ethical Hacker *(CEH)*	*EC-Council*
Open Professional Security Tester (OPST)	*ISECOM*
Offensive Security Certified Professional (OSCP)	*Offensive Security*
Certified Penetration Tester (CPT)	*IACRB*
Penetration Tester (GPEN)	*GIAC*

Tabla 2 - Certificaciones de Hacking. Fuente: Tabla 20. Astudillo, K. (2018) Certificaciones de Hacking Ético. Reproducida de HACKING ETICO 101: Cómo hackear profesionalmente en 21 días o menos! 2da Edición (Pág 271). Editorial CREATESPACE.

Algunas de las certificaciones antes mencionadas son más fáciles de obtener que otras, pero sin importar por cual decida empezar lo importante es que empiece.

Paso 7: Actualizarse constantemente

Hoy en día casi todas las carreras demandan una constante actualización de parte de los profesionales de su rama y el hacking ético no es la excepción. Cada día se desarrollan nuevas aplicaciones, se actualizan los sistemas operativos, se inventan nuevos dispositivos de cómputo, se descubren nuevas vulnerabilidades, etc.

En consecuencia, no es posible para un pentester dejar de actualizar sus conocimientos, porque de lo contrario junto con ellos se volverá obsoleto y no podrá efectuar pruebas de intrusión de forma eficiente, lo que resultará en pérdida de reputación y el fin de su carrera.

Ante ello un último consejo, trabaje en lo que ame. Si es usted un entusiasta de la tecnología y la seguridad informática, créame que se divertirá muchísimo efectuando pruebas de intrusión y lo mejor será que sus clientes le pagarán por divertirse ;-)

Recursos útiles

- **US-CERT:** https://www.us-cert.gov/
- **NIST (National Institute of Standards and Technology):** https://www.nist.gov/
- **ISO-27001 Standard:** https://www.iso.org/isoiec-27001-information-security.html
- **Portal en español sobre ISO-27001:** http://www.iso27000.es/
- **COBIT Standard:** https://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx
- **ISO/IEC 2000 Standard:** https://www.iso.org/standard/51986.html
- **Kali Linux Hacking Distro:** https://www.kali.org.
- **Back Box Linux Hacking Distro:** https://backbox.org/
- **Blog de Seguridad IT:** https://karinaastudillo.com/blog
- **Revista Infosecurity:** https://www.infosecurity-magazine.com/
- **Revista Security Magazine:** http://www.securityweek.com/
- **Revista Cyberdefense Magazine:** http://www.cyberdefensemagazine.com/
- **Curso gratuito sobre el framework de pentesting Metasploit:** https://www.offensive-security.com/metasploit-unleashed/

Acerca de la autora

Karina Astudillo B. es una consultora de sistemas especializada en seguridad informática, redes y sistemas UNIX/Linux y es la autora del Bestseller, "Hacking Ético 101 - Cómo hackear profesionalmente en 21 días o menos!".

Karina es Ingeniera en Computación, MBA, y cuenta con certificaciones internacionales como: Certified Ethical Hacker (CEH), Computer Forensics US, CCNA R&SW, CCNA Security, CCNA Wireless, Hillstone Certified Security Professional (HCSP), Cisco Certified Academy Instructor (CCAI), Sun Certified Solaris System Administrator (SCSA), Palo Alto ASE & PSE Platform F y VmWare VTSP & VSP.

Inició su carrera en el mundo de las redes en el año 1995, gracias a una oportunidad de trabajo en un proyecto con IBM en su alma máter, la Escuela Superior Politécnica del Litoral (ESPOL). Desde entonces el mundo de las redes, los sistemas operativos y la seguridad, la fascinaron al punto de convertirse en su pasión.

Años más tarde, luego de adquirir experiencia trabajando en el área de servicio al cliente de la corporación transnacional ComWare, fundó Consulting Systems, empresa especializada en brindar servicios y capacitación sobre ciberseguridad.

Paralelamente a la consultoría, Karina siempre ha tenido una pasión innata por enseñar, gracias a lo cual surgió la oportunidad de vincularse con la docencia como profesora de la Facultad de Ingeniería en Electricidad y Computación (FIEC) allá por el año 1996.

En la actualidad es instructora del programa Cisco Networking Academy y de los programas de Maestría en Sistemas de Información (MSIG) y Maestría en Seguridad Informática Aplicada (MSIA) de FIEC-ESPOL.

Debido a esta experiencia docente consideró incluir como parte de la oferta de su empresa, programas de preparación en seguridad informática, entre ellos talleres de Hacking Ético. Al publicar el éxito de estos talleres en su página web, empezó a recibir solicitudes de estudiantes que se encontraban en ciudades y países diferentes que preguntaban por los cursos, sólo para desilusionarse cuando se les contestaba que sólo se dictaban de forma presencial en Ecuador.

Fue entonces cuando nació la idea de escribir libros y montar una academia online sobre ciberseguridad para poder transmitir – sin límites geográficos - los conocimientos dictados en los talleres de Consulting Systems.

En sus momentos de esparcimiento Karina disfruta leer sobre ciencia ficción, viajar, compartir con su familia y amigos y escribir sobre ella en tercera persona ;-D

Comuníquese con Karina Astudillo B.

Siéntase libre de consultar a la autora o realizar comentarios sobre sus libros y cursos en:

Websites:

- https://www.KarinaAstudillo.com
- https://www.Consulting-Systems.tech
- https://www.Academia-Hacker.com

Email: karina@karinaastudillo.com
Twitter: https://www.twitter.com/KAstudilloB
Facebook: https://www.facebook.com/KAstudilloB
Instagram: https://www.instagram.com/KAstudilloB
YouTube: https://www.youtube.com/c/KAstudilloB

Otros libros de Karina Astudillo

Encuéntralos en:

https://www.academia-hacker.com/libros

Terminología

Amenaza

Una amenaza en materia de seguridad informática se refiere a la posibilidad de que ocurra un evento que perjudique la seguridad de la información.

Las amenazas pueden ser:

- **Externas:** si son ejecutadas desde fuera de la organización. Ej.: desde Internet.
- **Internas:** si provienen del interior de la empresa. Ej.: un empleado descontento.
- **Estructuradas:** si se planifican con antelación.
- **No-estructuradas:** si no existe planificación alguna.

Ataque

Un ataque es una agresión contra la seguridad de la información que, dependiendo de su éxito o fracaso, podría traer resultados nefastos para la organización.

Existen muchos tipos de ataques específicos, pero de forma general los podemos clasificar en cuatro grandes grupos:

- **Interrupción:** el atacante impide el flujo normal de información. Este es un ataque a la disponibilidad de la información.
- **Intercepción:** el intruso captura la información. Este ataque es hacia la confidencialidad.
- **Modificación:** el agresor cambia la información. Aquí se agrede la integridad de la información.
- **Fabricación:** en este caso el atacante crea información falsa, por lo que se afecta la autenticidad de la información.

Cracker o Black Hat Hacker

Este es el término usado comúnmente para referirse a una persona a la que le gusta romper la seguridad de los sistemas informáticos, sin contar con autorización para hacerlo. Los motivos pueden ser diversos, desde el mero deseo de satisfacer el ego y decir "pude romper X o Y sistema", obtener dinero ilícito ejecutando fraudes electrónicos, o inclusive realizar protestas políticas. A este último tipo de cracker también se le llama hacktivista. Como ejemplo de hacktivistas podemos citar al grupo Anonymous, el cual realiza protestas de índole político infiltrándose en sistemas de gobierno o a través de ataques de denegación de servicio.

Exploit

Un exploit es un procedimiento que permite aprovechar una vulnerabilidad dada. Dicho procedimiento consiste en una serie de pasos que se ejecutan en un orden preciso y pueden requerir el uso de conexiones hacia puertos de aplicativos, envío de paquetes con datos especiales (payloads), ejecución de scripts, etc.

Gray Hat Hacker

La traducción literal es "hacker de sombrero gris" y nos recuerda al doble agente de las series televisivas sobre espionaje; es decir que se trata de un personaje que puede actuar con fines ofensivos o defensivos dependiendo de sus intereses. Usualmente se trata de un black hat hacker "reformado", que brinda sus servicios como auditor de seguridad y que eventualmente sucumbe a la tentación de introducirse en un sistema remoto sin autorización.

Hacker

El término hacker se refiere a una "persona que disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas" (IETF (1993), RFC 1392 – Internet Users\x27 Glossary, recuperado en 2017, de http://tools.ietf.org/html/rfc1392).

Este punto es importante puesto que la desinformación creada por alguna mala prensa ha colocado en la mente del público la creencia errada de que todos los hackers se dedican a infiltrarse en sistemas informáticos con el objetivo de hacer daño, lo cual no es cierto. El término hacker por sí solo no emite ningún juicio de valor, por lo que podemos ser hackers tanto los auditores de seguridad informática que implementamos técnicas defensivas y también aquellos que decidieron unirse al lado oscuro de la red.

Pentesting o Hacking ético

El término pentesting viene de las palabras inglesas penetration, que significa penetración, y testing que significa probar; por lo que si tradujéramos literalmente, contarle a nuestra mamá que nos ganamos la vida haciendo penetration testing podría causarle preocupación; de ahí que el término en español más adecuado sea hacking ético o bien, pruebas de intrusión.

Hecha esta aclaración, vale indicar que nos referimos al proceso de realizar un ataque controlado sobre la infraestructura informática de una organización, de la que previamente hayamos obtenido la autorización bajo un contrato formal. El objetivo de realizar una auditoría de hacking ético es probar las defensas de la organización desde el punto de vista de un cracker, pero sin causar daño a los sistemas auditados, ni a la información del cliente y emitir un reporte de remediación que le permita a la empresa tomar los correctivos necesarios. Para ello el auditor debe estar calificado y tener los conocimientos y la experiencia necesarios para llevar a cabo el ataque de manera segura y culminar la auditoría con éxito.

Seguridad Informática

Es un área de la informática que se enfoca en proveer mecanismos que permitan garantizar la confidencialidad, integridad y disponibilidad de la información.

La confidencialidad avala que la información puede ser consultada o accedida solamente por quien está debidamente autorizado, la integridad certifica que la misma no ha sido modificada sin autorización y la disponibilidad garantiza – valga la redundancia - que siempre esté disponible cuando se requiera.

Si uno de estos ítems falla, entonces la información no está segura.

VM (virtual machine)

En español "máquina virtual", se refiere a una tecnología de software que permite emular un computador y ejecutar programas como si fuese un equipo real. La principal aplicación de las máquinas virtuales es la posibilidad de tener más de un sistema operativo ejecutándose a la par en una misma máquina física.

Al software que hace posible instalar máquinas virtuales en una máquina física se le denomina comúnmente hipervisor.

Algunos hipervisores conocidos son:

- **VmWare Workstation Player:** https://www.vmware.com/products/workstation-player.html
- **Oracle VirtualBox:** https://www.virtualbox.org/
- **Microsoft Hyper V:** https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v
- **Xen Server:** https://xenserver.org/
- **Qemu:** https://www.qemu.org/

Vulnerabilidad

Se refiere a una debilidad que podría conllevar que se comprometa la seguridad de la información.

Las vulnerabilidades pueden ser de tres tipos:

- **Tecnológicas:** cuando son inherentes a la tecnología implementada. Ej.: Se publica una falla en el aplicativo X que permite a un intruso tomar control de un sistema Y.
- **De configuración:** en este caso la vulnerabilidad se presenta debido a una mala configuración de un sistema que abre la puerta a una posible explotación. Ej.: El administrador de red deja abierto en el firewall el puerto del servicio de Escritorio Remoto de Windows del servidor de Directorio Activo.

- **De política:** aquí la inexistencia de una política de seguridad o la falta al no seguirla provoca la vulnerabilidad. Ej.: La puerta del centro de datos permanece sin seguro y cualquiera puede ingresar al área de los servidores corporativos.

White hat hacker

O también llamado "hacker de sombrero blanco". En este perfil encajamos los administradores de redes y consultores de seguridad informática que utilizamos nuestros conocimientos sobre sistemas con propósitos defensivos.

Notas y Referencias

[i] El phishing es un tipo de estafa electrónica en la cual se envía un mensaje de correo falso a la víctima, haciéndole creer que procede de una fuente confiable, el cual incluye enlaces a sitios maliciosos los cuales son réplicas de sitios reales. Una vez en el sitio web falso a la víctima se le roban sus credenciales o se le inyecta código malicioso (malware) en el computador.

[ii] Reynolds, C. (2019, November 07). Europe's Cybersecurity Skills Gap Has Doubled: Report. Retrieved January 30, 2021, from https://www.cbronline.com/news/cybersecurity-job-gap

[iii] Salaries. (n.d.). Retrieved January, 2021, from https://www.payscale.com/research/US/Job=Penetration_Tester/Salary/df83bfdb/Experienced

[iv] Se denomina script kiddie a alguien que se limita a usar software de hacking sin conocer en realidad conceptos de seguridad y networking, ni saber el trabajo que hacen por detrás dichas herramientas.

[v] McWilliam, E. L. (2007). Is creativity teachable? Conceptualising the creativity/pedagogy relationship in higher education.

[vi] Bono, E. D. (1986). El pensamiento lateral: manual de creatividad. México, D.F.: Paidós.

[vii] Un exploit es una secuencia de pasos, a menudo automatizada en un programa o script, que permiten explotar una vulnerabilidad en un componente de hw/sw o inclusive en una persona, si hablamos de ingeniería social.

[viii] La ingeniería inversa es un procedimiento mediante el cual se toma un producto terminado y se lo descompone para entender cuáles son sus componentes, cómo funcionan y cómo interactúan entre ellos. Aplicada al ámbito de seguridad informática la ingeniería inversa de un programa le permitirá al hacker conocer como este funciona e inclusive podría permitirle encontrar fallas de programación susceptibles de explotarse.

[ix] El término MOOC viene de las siglas en inglés, Massive Online Open Courses, que traducido al español significa Cursos Abiertos Masivos En-Línea.

[x] Stallings, W. (2012). Operating systems: internals and design principles. Boston, Mass: Prentice Hall.

[xi] AI viene de las siglas en inglés Artificial Intelligence, es decir Inteligencia Artificial.

[xii] Se dice que una vulnerabilidad tiene nivel de riesgo alto cuando el impacto es grave y la explotación es relativamente fácil de ejecutar. Una vulnerabilidad tiene riesgo medio cuando el impacto es moderado y la ejecución puede ser compleja. Y una vulnerabilidad tiene riesgo bajo cuando el impacto es bajo, aunque la explotación de esta pueda ser sencilla.

[xiii] La dark web o también denominada Internet oscura, es el nombre que se le da a partes del Internet que se ocultan de forma expresa de los buscadores para no ser indexadas. La dark web es parte de la deep web (las páginas de Internet que no pueden accederse a través de buscadores). Para navegar en la dark web se requieren buscadores especiales como por ejemplo el conocido Tor. Empero, cabe aclarar que no toda la dark web es mala, si bien enmascarar operaciones ilícitas es uno de los usos que se le da, también existen porciones de la dark web que tienen otro tipo de contenidos. Ver artículo https://www.genbeta.com/web-20/47-paginas-onion-para-visitar-el-lado-amable-de-la-deep-web

[xiv] Sí, no descubrí el Internet hasta que ingresé a la ESPOL en 1992. Y sí, mis canas son reales, no son pintadas para estar a la moda, aunque admito que lo parecen. Tampoco soy tan mayor, por si acaso ;-)

[xv] Stallings, W., & Manna, M. M. (2014). Data and computer communications. Harlow: Pearson.

[xvi] Para más información sobre estos y otros temas le sugiero revisar las secciones de “Recursos Útiles” y “Terminología” de este libro.

[xvii] Seguridad de la Información es un tópico más amplio que la Seguridad Informática, puesto que la información puede hallarse no sólo en medios informáticos sino también en otras fuentes como el papel, las personas, etc.

[xviii] Bishop, M. (2016). Information Security. Lecture Notes in Computer Science. doi:10.1007/978-3-319-45871-7.

[xix] Los talleres in-house son cursos intensivos de 4-8 horas diarias, para grupos dentro de las instalaciones del cliente. Elixircorp ha dictado con éxito talleres y conferencias y ha implementado proyectos de consultoría en Costa Rica, Colombia, Perú, Estados Unidos y Ecuador.

[xx] Cipresso, T., & Stamp, M. (2010). Software reverse engineering. In Handbook of Information and Communication Security (pp. 659-696). Springer Berlin Heidelberg.

[xxi] Los frameworks de explotación son herramientas de software que incluyen herramientas para faciitar la ejecución de todas las fases de un hacking ético. Ejemplos: Metasploit, Core Impact, Immunity Canvas.