HACKER'S PURPLEBOOK

RED

Luis Roberto de León Elizondo

La ley prohíbe
fotocopiar este libro

HACKER'S PURPLEBOOK
© Luis Roberto de León Elizondo

MARCAS COMERCIALES. Las designaciones utilizadas por las empresas para distinguir sus productos (hardware, software, sistemas operativos, etc.) suelen ser marcas registradas. WhiteSuit Hacking(WSH) ha intentado a lo largo de este libro distinguir las marcas comerciales de los términos descriptivos, siguiendo el estilo que utiliza el fabricante, sin intención de infringir la marca y solo en beneficio del propietario de la misma. Los datos de los ejemplos y pantallas son ficticios a no ser que se especifique lo contrario.

WhiteSuit Hacking es marca comercial registrada.

Se ha puesto el máximo empeño en ofrecer al lector una información completa y precisa. Sin embargo, WhiteSuit Hacking Editorial no asume ninguna responsabilidad derivada de su uso ni tampoco de cualquier violación de patentes ni otros derechos de terceras partes que pudieran ocurrir. Esta publicación tiene por objeto proporcionar unos conocimientos precisos y acreditados sobre el tema tratado. Su venta no supone para el editor ninguna forma de asistencia legal, administrativa o de ningún otro tipo. En caso de precisarse asesoría legal u otra forma de ayuda experta, deben buscarse los servicios de un profesional competente.

País: México
Teléfono: +52 1 81 2320 5330
Correo electrónico: *ventas@whitesuithacking.com*
Internet: *www.whitesuithacking.com*
ISBN: 9798745610455

ÍNDICE

Tabla de contenido

INTRODUCCIÓN

Estoy seguro de que la gente se da cuenta que me gusta enseñar cada vez que alguien toma un curso conmigo. Mínimo yo puedo decir que cada vez que alguien me da las gracias por entender algo, siento una autentica satisfacción propia. Mi sueño es ser CIO/CISO/CTO de una empresa internacional, y pues, aún qué bien ya me he encargado de un área de TI, creo que un CIO de clase mundial debe de conocer de varios temas: Tecnología, Administración, Gestión y Seguridad.

Así que yo he enfocado mis estudios en esas áreas, pues creo que el CIO no puede quedarse atrás con temas de tecnología en general. Debe de saber administrar sus recursos y entender la parte del negocio de la organización. Debe de trabajar correctamente y saber comprobar que su gestión es correcta y realmente entender de seguridad, pues los crímenes hoy en día evolucionan a donde ya no es necesario un arma, solo se necesita un PC con acceso a internet y ya eres capaz de tumbar economías.

Con este libro espero que aprendas lo que a mí me hubiera encantado conocer cuando entre a este mundo de “infosec”, ya que planeo tocar temas de ataque y defensa, también conocidos como equipo rojo y equipo azul. Los cuales juntos hacen el equipo purpura. Lo necesario que debe de tener el área de TI.

¿PARA QUIÉN ES ESTE LIBRO?

Aún que no esté pensado este libro como libro de introducción a la seguridad informática, quise hacerlo apto también para que cualquier persona que quiera adentrarse pueda hacerlo, pero el objetivo principal es que aquellas personas que les encanta los temas de explotación puedan reforzar sus conocimientos y aprendan las responsabilidades y la importancia de un blue team. Así mismo, hay miembros de blue team que en su vida han tocado Kali Linux, es importante que ellos aprendan del mundo de hacking y las tareas que hace un hacker ético y las técnicas en las que se apoya para lograr su cometido.

¿QUIÉN SOY?

Mi nombre es Luis, desconozco si compras el libro porque ya me conocías o no, así que déjame presentarme. He tenido proyectos con Empresas privadas, Academia y Gobierno. Llevo cientos de alumnos que han pasado por mis clases los cuales siempre salen contentos de cada una de las sesiones, así como he dado conferencias para distintas universidades, empresas y eventos públicos.

Adicionalmente, si deseas tomar alguna **certificación** o **curso**, actualizarte con noticias y nuevas cosas en nuestro **blog**, o requieres algún **servicio profesional de ciberseguridad**, puedes encontrarnos/contactarnos en **whitesuithacking.com**,

ESTRUCTURA DEL LIBRO

El libro este compuesto de dos partes Azul y Roja.

En el apartado Azul puedes encontrar todo relacionado a las acciones que puede hacer el área de sistemas para mejorar la seguridad, acciones relacionadas a un SOC. Básicamente todo lo que sea para DEFENDER.

En el apartado rojo veras múltiples maneras de atacar, temas relacionados a explotar y obtener acceso a sistemas. Claro, todo esto de manera ética. Ahí se ve todo lo que es relacionado a ATACAR.

Esta es la parte roja del libro, puedes leerte cualquiera de las dos primero, la que te llame más la atención a ti. Veras que cada una se complementa y al final tendrás un gran panorama de ambas partes y podrás decidir qué camino tomar en tu sendero en el mundo de la seguridad informática. En este libro puedes notar como te llevo de la mano y de repente te suelto sin aviso alguno, que si bien puede ser algo cruel y puede llegar a frustrarte de vez en cuando te servirá para aprender a solucionar problemas, una vez teniendo las bases. Es común no conocer todos los comandos y todas las herramientas, no te preocupes por ello. Lo importante es aprender a superar tus propios límites y saber que, si te llegas a atorar, puedes: analizar la situación, tomar un descanso y sobre todo usar Google.

Material y comunidad

Primero que nada, me gustaría mencionar 4 cosas:

1. Este es un libro técnico, por lo tanto, tiene poca o nula utilidad si no tienes las herramientas mencionadas en el libro.

2. **Todo** el material que requieres estará disponible en la página **https://whitesuithacking.com/materialmorado**

3. Con el fin de proteger nuestra propiedad intelectual, dichas herramientas están cifradas con una contraseña personal, dicha contraseña te debió haber llegado a tu correo al hacer la compra de este libro.

4. Tenemos una comunidad de hackers en Telegram privada a lectores de nuestros libros y alumnos de nuestras certificaciones y cursos, donde podrás aprender todavía más, y compartir tus conocimientos, sugiero ingresar, para hacerlo, descarga Telegram, ingresa al grupo **@wshgrupo**, y dile tu contraseña al bot para obtener el ingreso.

Ahora sí, con esa información en mente, continúa leyendo el libro.

El libro consta de 2 **partes**

En esta parte veremos sobre Red Team y técnicas usadas por los atacantes

¿Cuáles pueden ser las acciones de un Red Team?

Seguridad ofensiva

Atacar para defender.

Hacking Ético

Atacar a la organización con permiso previo escrito y cumpliendo un código de ética establecido basado en que es lo que puede hacer y que es lo que no.

Explotación de vulnerabilidades

¡Explotar cosas! Esto quiere decir buscar vulnerabilidades y demostrar cómo son explotadas, estas pueden ser en páginas web, servidores, servicios o cualquier punto de entrada posible. Es la parte más divertida de esto.

Pruebas de penetración

De la mano con el hacking ético, encontrar vulnerabilidades explotarlas y documentarlas para previamente ser corregidas.

Pruebas de caja negra

Probar los ataques sin ninguna información previa, como alguien completamente externo a la organización.

Ingeniería Social

Uso de las personas para obtener información, esto es una de las grandes diferencias entre una prueba de penetración y un miembro de un red team completo.

HACKER'S PURPLEBOOK

BLUE

Luis Roberto de León Elizondo

ÍNDICE

Contenido

INTRODUCCIÓN

Recuerdo muy bien aquella primera vez que me atreví a tomar un curso de ciberseguridad. Estaría mintiendo si no reconociera que en aquel momento estaba nervioso, entusiasmado y honestamente desubicado de mi ecosistema natural. Venga, mi carrera es Relaciones Internacionales, no tiene nada que ver con informática, en ese momento era algo tan ajeno como empezar a estudiar medicina o querer hacer un curso de ingeniería civil, entonces seguramente se puede entender desde qué ámbito emanaban mis preocupaciones.

El momento de mi llegada al GHOST fue tenue, rodeado de otras personas que pronto se convertirán en hackers y profesionistas de la seguridad. No fue hasta que Luis comenzó que realmente me hizo click: "Este muchacho es hacker como el de las películas". Con esa pequeña realización comencé a permitirme ser seducido por el conocimiento que nos ofrecía Luis. Una y otra vez, los alumnos lo bombardeaban de preguntas y dudas, pero Luis se mantenía firme, distribuyendo respuestas como si fuera tan sencillo como tronar palomitas.

Ese curso para mi todo lo cambio, me abrió las puertas a algo maravilloso, pero mejor aún tantito fue la oportunidad de que Luis Elizondo fuera el guía que me llevo a acariciar los conocimientos de la alta ciberseguridad, la verdadera Seguridad de la Información.

Si eres alguien quien ya se dedica a esto, o conoces bien las prácticas y las actividades de la ciberseguridad, entenderás a que me refiero: nuestro campo es uno que se ve envuelto de misticismo y expectativa, aquellos quienes no conocen de verdad, muchas veces se van con la finta del entendimiento de Hollywood del hacker (que realmente, rara vez se asemeja a lo que sale en las películas).

Es por eso, que la experiencia de tener a Luis como maestro es algo inolvidable. Luis

logra darle esa magia (casi como lo hace Hollywood) a la ciberseguridad. Es alguien a quien admiro mucho porque tiene un genuino amor por lo que hace y por lo que ensena. Realmente, creo difícil encontrar a un maestro tan apasionado como Luis, y siendo muy honestos, también creo difícil encontrar a un maestro más hábil que este. Es por esto, que siempre reconoceré a Luis como mi maestro y mentor, pues fue él quien me enseño el camino, y me sigue llevando de la mano hasta hoy fecha.

Aparte, este libro tiene una característica inmensamente importante, ofrece apoyo a ambos aquellos que se dediquen a seguridad ofensiva, así como aquellos que se dedican a la seguridad defensiva (y vaya que ambos pueden aprender uno del otro).

Te invito a que a lo largo de este libro te permitas sorprenderte, aprender cosas distintas y más que nada, que te retes a mejorar y ampliar tu conocimiento en cualquier dado momento. Pues, si esto lo haces bien, para el final de estas páginas serás un profesionista de ciberseguridad único, más hábil y con un buen repertorio de herramientas que usar.

Esa… es la magia de Luis Elizondo.

Con mucho aprecio, los dejo en manos de la gran sabiduría de mi maestro,

Cristóbal Cárdenas

Profesor de la Escuela de Ciberseguridad

Facultad de Derecho y Criminología – Universidad Autónoma de Nuevo León (UANL)

El libro consta de 2 **partes**

En este apartado veremos sobre acciones que un Blue team realiza, aquellos que se encargan de defender, aplicar políticas y reglas de seguridad para evitar que la información sea comprometida.

¿Qué acciones realiza un blue team?

Seguridad defensiva

Configurar e instalar diferentes herramientas que ayuden a la seguridad.

Protección de la infraestructura

No solo hay que cuidar un firewall, si no donde se almacena la información físicamente.

Control de daños

Es mejor vivir con la mentalidad de que un día seremos atacados. La cuestión aquí es… ¿Qué tanto daño nos puede hacer? Para esto hay que buscar como disminuir dicho impacto en caso de que un ataca se llegue a materializar

Respuesta de incidentes

Una vez que se materialice el riesgo ¿Qué vamos a hacer? ¿Cuál va a ser el tiempo de respuesta? ¿Qué impacto puede tener este?

Modelado de amenazas

Una buena documentación y análisis a que somos susceptibles siempre es bienvenido. Este no es el mismo para cada quien, todo depende de los departamentos y giros de los negocios, no es la misma seguridad que tendrá una empresa desarrolladora de software a una empresa que se dedica al maquilado. Todo esto son factores que hay que tener en cuenta.