MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Webinar Gratuito Hacking Ético

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital

e-mail: ReYDeS@gmail.com

Febrero 2018

Presentación

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics y Cybersecurity Management.

Ha sido instructor y expositor en OWASP Perú Chapter, instructor y expositor en PERUHACK, además de expositor en 8.8 Lucky Perú. Cuenta con más de catorce años de experiencia y desde hace diez años labora como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

https://twitter.com/Alonso_ReYDeS

http://www.reydes.com

https://www.facebook.com/alonsoreydes/

reydes@gmail.com

https://www.linkedin.com/in/alonsocaballeroquezada/

Agenda

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

- Mentalidad de los Profesionales
- Amenazas, Vulnerabilidades y Riesgos
- Hacking, Pruebas, Evaluaciones, Auditorias
- Definición de Hacking Ético
- Pruebas de Penetración
- Evaluación de Vulnerabilidades
- Auditorías de Seguridad
- Realizar un Hacking Ético o PdP
- Arreglar las Vulnerabilidades Descubiertas
- Tipos de Hacking Ético y PdP
- Tipos Adicionales de Prueba
- Fases de un Ataque
- Metodologías para Pruebas

Mentalidad de los Profesionales

Se “rompen” computadoras forzándolas a hacer cosas, las cuales los diseñadores quienes lo implementaron o desarrollaron, y administradores de sistemas, no planificaron era factible hacerlas.

Profesionales exitosos en hacking ético y pruebas de penetración, deben mantener un mentalidad la cual implique dos conceptos al parecer contradictorios.

- Pensar de manera peculiar, ser pragmático, y hacer las cosas de manera diferente.

- Al mismo tiempo, ser minucioso, metódico y cuidadoso, hacer buenas anotaciones, además de hacer un trabajo repetible.

El buen balance entre estos dos puntos es crucial para el éxito.

Amenazas, Vulnerabilidades y Riesgos

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

- **Amenaza:** Agente o actor el cual puede causar daño.
- **Vulnerabilidad:** Falla la cual alguien puede explotar para causar daño.
- **Riesgo:** Donde la amenaza y la vulnerabilidad se sobreponen.
- **Exploit:** Código o técnica utilizada por una amenaza para aprovecharse de una vulnerabilidad.

El trabajo de un profesional en pruebas de penetración, es modelar las acciones de las amenazas reales para encontrar vulnerabilidades.

Luego, con un diseño controlado, explotar estas vulnerabilidades para determinar el riesgo real para la organización.

Finalmente recomendar las defensas apropiadas, lo cual pueda ser integrado en las operaciones de la organización objetivo.

Hacking, Pruebas, Evaluaciones, Auditorias

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Muchas personas utilizan ciertos terminos como si fuesen sinónimos, o sin un significado definido.

- **Hacking Ético** (Ethical Hacking)
- **Pruebas de Penetración** (Penetration Testing)
- **Evaluaciones de Seguridad** (Algunas veces solamente denominado "Auditorías de Seguridad")
- **Auditorias de Seguridad**

Todo esto conduce a mucha confusión.

Se debe tener por lo tanto la capacidad para diferenciarlos, reconociendo el hecho de otras personas no pueden hacerlo.

Definición de Hacking Ético

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Hacking: (Tradicional) Manipular la tecnología para forzarla a hacer algo para lo cual no fue diseñada.

Hacking: (Siniestro) Irrumpir en sistemas de computadoras y redes sin permiso.

El añadir la palabra“Ético” antes de la palabra “Hacking”, supuestamente anula la connotación siniestra del termino.

Hacking Ético: Utilizar técnicas de ataque por computadora para encontrar fallas de seguridad, realizado con el permiso de los propietarios del objetivo, siendo el propósito principal mejorar su seguridad.

De acuerdo a la Wikipedia, un “Hacker de Sombrero Blanco” es frecuentemente utilizado como un sinónimo de Hacker Ético.

Pruebas de Penetración

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Se enfoca en encontrar vulnerabilidades de seguridad en el entorno objetivo, lo cual permitirá a un atacante penetrar la red o los sistemas de computadoras, como también robar información.

- Utilizar herramientas y técnicas similares a las de los criminales
- Para prevenir un robo, se necesita pensar como un ladrón
- El objetivo es la penetración; comprometer sistemas objetivo y obtener acceso hacia la información; para determinar el impacto en la empresa

La prueba de penetración es un subconjunto del hacking ético. Implica modelar las técnicas utilizadas por los atacantes del mundo real.

- Encontrar vulnerabilidades
- Bajo circunstancias controladas explotar estas fallas
- En un profesional, manera segura de acuerdo a un alcance y contrato
- Para determinar el riesgo e impacto potencial para la empresa
- Todo con el objetivo de ayudar a la organización a mejorar su seguridad

Evaluación de Vulnerabilidades

También denominado como “Evaluaciones de Seguridad”. Para algunas personas los términos se utilizan como sinónimos:

Evaluación de seguridad = Evaluación de vulnerabilidades = PdP

Pero existen algunas diferencias.

Prueba de Penetración: Se enfoca en irrumpir o robar datos.

Evaluación de Seguridad/Vulnerabilidades: Se enfoca en encontrar vulnerabilidades de seguridad, lo cual podría o no ser utilizado para irrumpir o robar datos.

- Las pruebas de penetración frecuentemente tienen la intención de ir más profundamente y enfocarse en problemas técnicos
- Las evaluaciones son más amplias, y frecuentemente incluyen políticas explícitas y revisión de procedimientos

Auditorías de Seguridad

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Las auditorias implican realizar pruebas contra un conjunto riguroso de estándares.

Casi siempre se hace con listas de verificación (checklists) detalladas.

Aunque algunas personas han creado listas de verificación para pruebas de penetración y evaluaciones de seguridad, estos tienden a no tener la profundidad y rigurosidad de una auditoría.

Para nuestros propósitos no se abarcarán temas de auditorías en Hacking Ético o Pruebas de Penetración.

Pero algunos conceptos y técnicas abarcadas podrían ser útiles para los auditores.

Realizar un Hacking Ético o PdP

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

¿Porqué realizar un Hacking Ético o Pruebas de Penetración?.

Para encontrar vulnerabilidades antes de estas sean encontradas por los atacantes maliciosos.

Para tener una mejor comprensión del riesgo real para la organización.

Para tener y resaltar un punto para los tomadores de decisiones sobre la necesidad de acciones o recursos.

Encontrar (y explotar) fallas en las pruebas de penetración, frecuentemente ofrece más pruebas reales sobre la necesidad de acción; comparado con otros métodos para el descubrimiento de vulnerabilidades.

Arreglar las Vulnerabilidades Descubiertas

No todas las vulnerabilidades descubiertas pueden ser arregladas.

Se sugiere poner énfasis para arreglar todas las vulnerabilidades con un riesgo alto.

No obstante la seguridad de la información es sobre la gestión de riesgos.

Las organizaciones puede decidir; para propósitos de la empresa; aceptar el riesgo en lugar de mitigarla.

Esta es la razón por la cual es necesario presentar los hallazgos en términos de la empresa.

Todo esto se incluyen en un reporte final.

Tipos de Hacking Ético y PdP

- **Pruebas para servicios de red**
  (Muy común)
- **Pruebas para el lado del cliente**
  (Menos común, pero vitalmente importante)
- **Pruebas para aplicaciones web**
- **Pruebas de seguridad inalámbrica**
- **Pruebas de ingeniería social**
  (Por correo electrónico o por teléfono)
- **Pruebas remota de marcado de teléfono**
  (No muy común actualmente)

Tipos Adicionales de Pruebas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Pruebas de seguridad física

Pruebas para el robo de equipos

Ataques para en análisis de la criptografía.

- Romper o evadir la encriptación de datos locales o tráfico interceptado
- O analizar mecanismo para la protección de derechos de copia.

Pruebas para la seguridad de productos
(Algunas veces denominado como pruebas de software “shink-wrapped”).

Fases de un Ataque

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Los atacantes maliciosos y profesionales en Hacking Ético, se basan en varias etapas para realizar los ataques.

- Reconocimiento
- Escaneo
- Explotación

Los atacantes maliciosos frecuentemente van más allá, con etapas como:

- Mantener el acceso con puertas traseras y rootkits
- Cubrir huellas con canales encubiertos y edición de logs

Estas etapas no siempre son seguidas en un orden. Los mejores atacantes saltan entre ellas conforme se presentan las oportunidades.

Sin embargo, para realizar una prueba profesional, no se debe olvidar retroceder para analizar cualquier etapa previamente obviada.

Metodologías para Pruebas

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Diversas organizaciones han publicado metodologías libres para realizar pruebas de penetración y escaneo de redes.

Los procesos deben abarcar todos los aspectos de estas metodologías.

Pueden proporcionar documentación original útil para formalizar un plan personalizado de pruebas.

Algunas de las metodologías más valiosas e interesantes son:

- Open Source Security Testing Methodology Manual (OSSTMM)
- Penetration Testing Execution Standard (PTES)
- NIST Sepecial Publication 800-115. Technical Guide to Information Security Testing and Assessment
- Open Web Application Security Project (OWASP) Testing Guide
- Penetration Testing Framework

Más Información

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Sitio Web

http://www.mile-sec.com

Correo Electrónico

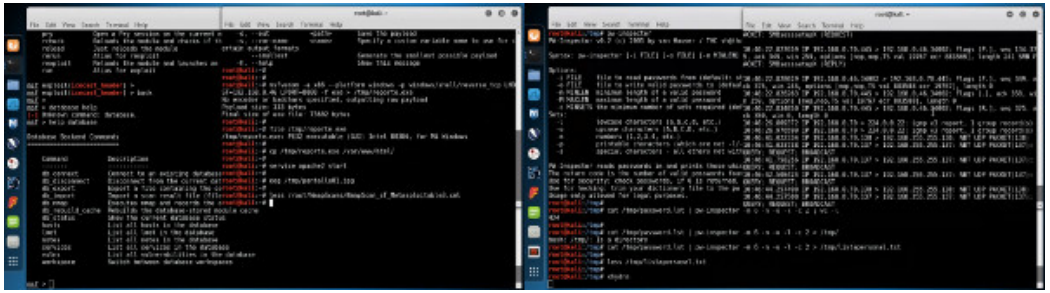
informes@mile-sec.com

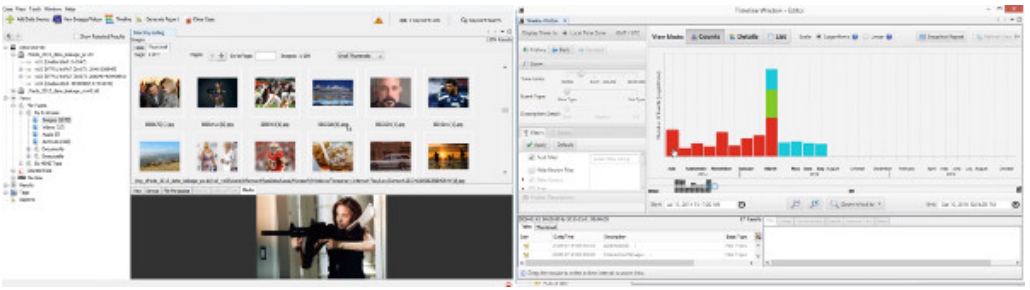
Redes Sociales

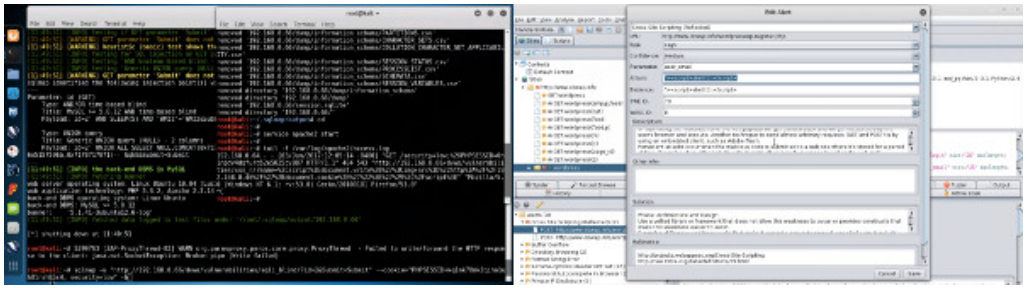
https://www.facebook.com/mileseceirl

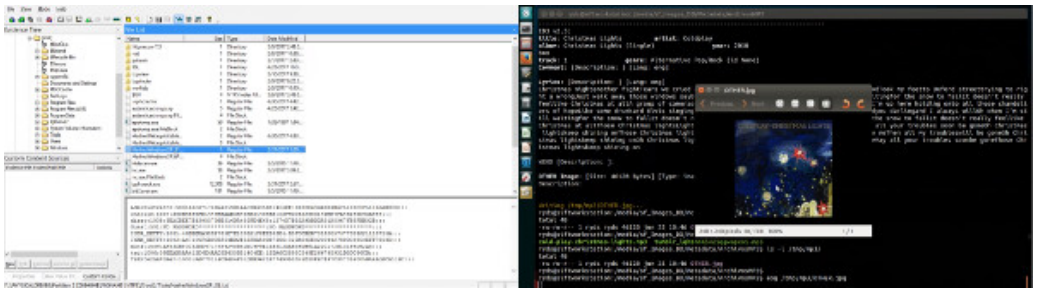
https://twitter.com/mileseceirl

https://www.linkedin.com/in/milesec/









¡Muchas Gracias!

Webinar Gratuito Hacking Ético

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital

e-mail: ReYDeS@gmail.com

Febrero 2018