

Webinar Reconocimiento de Sistemas en Internet

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital

Sitio web: <http://www.mile-sec.com> | Correo: capacitacion@mile-sec.com

2019

Sobre MILE-SEC

MILESEC E.I.R.L, es una empresa Peruana fundada en el año 2017. La cual está netamente dedicada a brindar servicios de capacitación a empresas, instituciones, organizaciones y profesionales, en las áreas de seguridad de la información y tecnologías de la información (T.I.), tales como; pruebas de penetración, hacking ético, evaluación de vulnerabilidades, forense de computadoras y forense digital. Así mismo brinda servicios de consultorías especializadas en todas las áreas antes mencionadas.

Durante estos años ha realizado capacitaciones presenciales y consultorías tanto públicas cuanto privadas para Ecuador y Perú, en las ciudades de Lima, Cusco y Trujillo. Así mismo realiza capacitaciones en su plataforma virtual.



mile-sec

Capacitación y Consultoría en Hacking Ético & Forense Digital



Inicio Empresa Servicios Cursos Blog Eventos Aula Virtual Pagos Contactarnos



Presentación

MILESEC E.I.R.L, es una empresa de capitales Peruanos fundada en el año 2017, la cual está netamente dedicada a proporcionar servicios de capacitación a empresas, instituciones, organizaciones y profesionales, en las áreas de seguridad de la información y tecnologías de la información (T.I), tales como; Pruebas de Penetración (Penetration Testing), Hacking Ético (Ethical Hacking), Evaluación de Vulnerabilidades (Vulnerability Assessment), Forense de Computadoras (Computer Forensics) y Forense Digital (Digital Forensics). Así mismo brinda servicios de consultorías especializadas en todas las áreas antes mencionadas.

Durante estos años ha realizado capacitaciones presenciales y consultorías tanto públicas cuanto privadas para Ecuador y Perú, en las ciudades de Lima, Cusco y Trujillo. Así mismo ha realizado capacitaciones online o virtuales.

Leer más: 59 lecturas



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



Correo electrónico: informes@mile-sec.com
Teléfono Móvil: +51 972 213 381
Facebook: <https://www.facebook.com/mileseceir/>
Twitter: <https://twitter.com/mileseceir/>
LinkedIn: <https://www.linkedin.com/in/milesec/>
Instagram: <https://www.instagram.com/mileseceir/>
Youtube:

<https://www.youtube.com/channel/UC704j0kizdZdMYwWWSZEQmA>

Cursos

- Fundamentos de Forense Digital
- Zed Attack Proxy
- PenTesting Web con Kali Linux
- PenTesting con Kali Linux
- Fundamentos de Metasploit
- Fundamentos de Nmap
- Fundamentos de Hacking Web
- Fundamentos de Hacking Ético

Menú

- Servicios
- Empresas
- Cursos
- Blog
- Conferencias
- Webinars
- Talleres
- Aula Virtual
- Pagos
- Contactarnos

Blog

- La información cuantica puede romper la seguridad de internet y hacerlo irrelevante
- Fuga de datos personales en FIFA 20
- Instagram lanza una herramienta para que los hackers no puedan robar la cuenta
- Vulnerabilidad 0 Day y exploit brinda control total sobre Android
- Microsoft informa de que hackers iraníes intentaron atacar la cuenta de un aspirante a la Casa Blanca.

Más

Ciente



Ciente



Ciente



Redes Sociales

 <https://www.facebook.com/mileseceirl/>

 <https://twitter.com/mileseceirl>

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

 <https://www.instagram.com/mileseceirl/>

 <https://www.youtube.com/channel/UC7Q4j0kizdZdMYwnWSZEqmA>

 <http://www.mile-sec.com/>

 informes@mile-sec.com / mileseceirl@gmail.com

Temario

- Reconocimiento
- Determinar el Alcance de las Actividades
- Obtener la Autorización
- Información Públicamente Disponible
- Enumeración Whois
- Enumeración DNS
- Reconocimiento de la Red

¿Qué es el Reconocimiento?

El reconocimiento sistemático y metódico de una organización permite a los atacantes crear un perfil muy completo sobre la postura de seguridad de la organización.

Utilizando una combinación de técnicas y herramientas, acompañados con una alta dosis de paciencia y criterio, los atacantes pueden tomar una entidad desconocida y reducirla a un rango específicos de dominios, bloques de red, subredes, routers y direcciones IP individuales directamente conectados hacia Internet, como también otros detalles pertinentes a su postura de seguridad.

Aunque existen muchos tipos de técnicas para el reconocimiento, estos principalmente están orientadas al descubrimiento de información relacionada con entornos como; Internet, intranet, acceso remoto, y extranet.

¿Porqué es Necesario?

Por una razón básica; proporciona una imagen exacta de aquello lo cual ven los atacantes maliciosos. Y si se conoce aquello lo cual ven los atacantes maliciosos, se conoce cuales son las potenciales exposiciones de seguridad en el entorno. Y cuando se conoce cuales exposiciones se tienen, se conocer como prevenir la explotación.

Los atacantes maliciosos son muy bueno metiéndose en la mente de otros. Son metódicos y sistemáticos para obtener todas las piezas de información relacionadas a las tecnologías utilizadas en el entorno. Sin una metodología para realizar este tipo de reconocimiento, se perderían piezas de información relacionadas a tecnologías específicas o de la organización, pero los atacante no.

El reconocimiento es una de las tareas más arduas para intentar determinar la postura de seguridad de una entidad, y tiene a ser más tediosa comparado con otras otras posteriores etapas. Sin embargo es una de las etapas más importantes, debiendo ser realizadas de manera controlada y precisa.

Reconocimiento en Internet

Aunque muchas técnicas de reconocimiento son similares entre tecnologías (Internet e intranet), este webinar se orienta en el reconocimiento de las conexiones de una organización hacia Internet.

El proporcionar una guía paso a paso es difícil, debido a esta actividad puede conducir hacia muchas rutas. Sin embargo se mencionan las etapas fundamentales para completar un análisis de reconocimiento más profundo.

Muchas de estas técnicas pueden ser aplicadas hacia otras tecnologías.

Reconocimiento en Internet

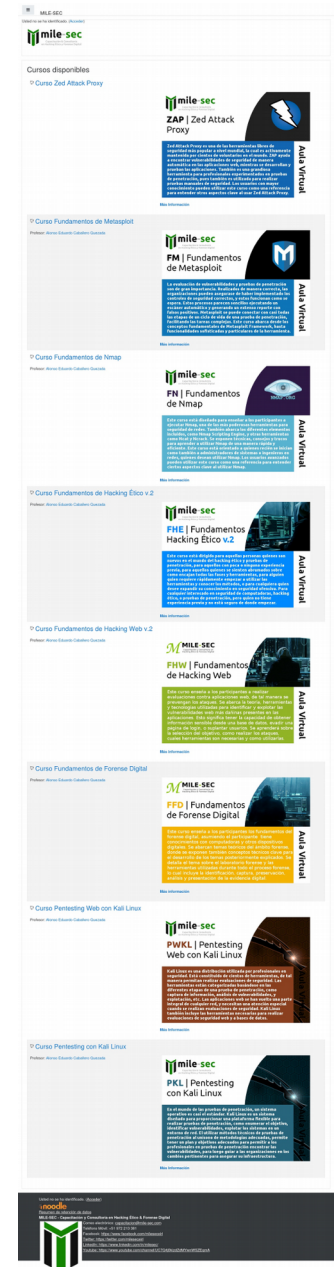
- Determinar el alcance de las actividades
- Obtener la autorización pertinente
- Información disponible públicamente: Sitio web de la empresa, organizaciones relacionadas, detalles de ubicación, información de los empleados, eventos actuales, información de archivo, motores de búsqueda y relaciones de datos, otra información de interés.
- Enumeración Whois: Búsquedas relacionadas al dominio, búsquedas relacionadas a la dirección IP.
- Consultas DNS: Transferencias de zona, determinar los registros DNS.
- Reconocimiento de la red: Trazado de la ruta.

Aula Virtual

Todos los cursos están disponibles en el Aula Virtual

- Curso Zed Attack Proxy
- Curso Fundamentos de Metasploit
- Curso Fundamentos de Nmap
- Curso Pentesting Web con Kali Linux
- Curso Pentesting con Kali Linux
- Curso Fundamentos de Hacking Web v.2
- Curso Fundamentos de Hacking Ético v.2
- Curso Fundamentos de Forense Digital v.2

<http://www.mile-sec.com/cursos>



Webinar Reconocimiento de Sistemas en Internet

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital

Sitio web: <http://www.mile-sec.com> | Correo: capacitacion@mile-sec.com

2019