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

Webinar Gratuito
Seguridad Física

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

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

Enero 2019

Sobre MILE-SEC

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

MILESEC E.I.R.L, es una empresa de capitales Peruanos fundada en el año 2017, 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 Penetracion, 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 ha realizado capacitaciones online o virtuales.


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

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

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

https://twitter.com/mileseceirl

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

Temario

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

- Introducción
- Identificar vulnerabilidades básicas de seguridad física
- Determinar con precisión vulnerabilidades físicas en una oficina
- Construir una infraestructura
- Utilidades
- Disposición y uso de una oficina
- Componentes de red y computadoras

Introducción

Se puede percibir la seguridad de la información más dependiente de las políticas no técnicas y procesos de la empresa, comparado con las soluciones de hardware y software técnico, por lo cual muchas personas y proveedores abogan.

La seguridad física, la cual implica la protección de propiedad física, se acompasa con los componentes técnicos y no técnicos, ambos de los cuales deben ser abarcados.

La seguridad física es algunas pasada por alto, pero es un aspecto crítico en un programa para la seguridad de la información. La capacidad de asegurar la información depende de la capacidad de asegurar físicamente la oficina, el edificio, o el campus.

No se recomienda irrumpir o ingresar directamente, lo cual podría ser necesario para probar completamente ciertas vulnerabilidades de seguridad física, en lugar de ello se debe aproximar a ciertas áreas y ver cuan lejos se puede llegar.

Identificar vulnerabilidades básicas de seguridad física

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

Muchas vulnerabilidades de seguridad física dependen de factores como:

- Tamaño del edificio
- Número de edificios o ubicaciones de oficinas
- Número de empleados
- Ubicación y número de entradas a los edificios y puntos de salida
- Lugares como cuartos de servidores, gabinetes de cableado, y centros de datos

Algunos ejemplos de vulnerabilidades en seguridad física son:

- No hay un recepcionista en el edificio quien vigile entradas y salidas
- No se requiere registro de un visitante o acompañarlo para acceder al edificio
- Los empleados confían en los visitantes quienes se visten con uniformes de proveedores, o dicen trabajar en el edificio
- Cámaras de video, control de acceso, y sistemas de central de datos accedibles a través de la red, etc.

Determinar con precisión vulnerabilidades físicas en oficina

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

Muchos potenciales puntos de explotación en seguridad física pueden parecer improbables, pero pueden ocurrir en organizaciones las cuales no ponen atención en los riesgos de seguridad física.

Los atacantes maliciosos pueden explotar tales vulnerabilidades, incluyendo debilidades en la infraestructura del edificio, disposición de la oficina, acceso al cuarto de computadoras, y el diseño.

Además de estos factores, considerar la facilidad de proximidad hacia la asistencia de emergencia local (policía, fuego y ambulancia), y las estadísticas de crímenes en el área, de tal manera se puede entender mejor contra quien se enfrenta.

Se deben buscar ciertas vulnerabilidades cuando se evalúe la seguridad física de una organización. No es necesario invertir o gastar mucho en equipo. Dependiendo del tamaño de las oficinas, estas pruebas podría no tomar mucho tiempo. Lo principal es determinar si los controles de seguridad física son adecuadas.

Construir una infraestructura

Puntos de ataque

- ¿Están las puertas abiertas?
- Los huecos en la parte inferior de las puertas
- ¿Sería fácil forzar las puertas abiertas?
- ¿De qué está hecho el edificio o centro de datos?
- ¿Existen puertas o ventanas de vidrio?
- ¿Están las puertas, ventanas, etc, conectados a un alarma?

Medidas correctivas

- Puertas fuertes y seguros
- Paredes sin ventanas alrededor del centro de datos
- Vigilar continuamente los sistemas de alarmas con cámaras en las áreas
- Iluminación
- Trampas humanas (mantraps)
- Cercas

Utilidades

Puntos de ataque

- ¿Existe equipo para protección de poder en el lugar?
- ¿Cuando la energía falla, que ocurre con los mecanismos de seguridad física?
- ¿Donde se ubican los dispositivos para detección y supresión de fuego?
- ¿Donde se localizan las válvulas de agua y gas?
- ¿Están los cables locales de telecomunicaciones sobre la tierra?

Medidas correctivas

- Asegurar los principales controles de utilidad están cerrados y en áreas aseguradas
- Asegurar cualquier dispositivo accedible sobre la red o Internet han sido evaluados por temas de seguridad
- Asegurarse de cualquiera cerca al edificio no pueda acceder a ningún control

Disposición y uso de una oficina

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

Puntos de ataque

- ¿Existe un recepcionista o guardia de seguridad en las puertas?
- ¿Los empleados tiene información confidencial en sus escritorios?
- ¿Dónde están ubicados los depósitos para basura?
- ¿Cuan seguro son los cuartos de correo y copias?
- ¿Son los CCTV o cámaras IP vigilados en tiempo real?
- ¿Están fortalecidas las cámaras de red y DVRs de ataques?
- ¿Cuales controles de acceso existen sobre las puertas?

Medidas correctivas

- Un recepcionista o guardia de seguridad para vigilar
- Una entrada de salida y entrada al centro de datos
- Áreas seguras para la basura
- Vigilar las áreas críticas con CCTV y cámaras IP
- Uso limitado de claves y códigos de paso, etc.

Componentes de red y computadoras

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

Puntos de ataque

- Obtener acceso a red y enviar correos maliciosos como usuario logueado
- Obtener y romper contraseñas directamente desde la computadora
- Colocar cajas de penetración “Pwnie Express”
- Robar archivos desde la computadora mediante un dispositivo USB
- Ingresar a un cuarto de computadoras no bloqueados, servidores, etc.
- Salir con diagramas de red, lista de contactos, planes de recuperación
- Obtener números de teléfonos, IDs de circuitos, otro equipo

- Conectar una computadora ejecutando un analizador de tráfico
- Instalar un analizador de tráfico en una computadora existente

- Un método fácil es instalar un software para administración remota
- Utilizar una dirección IP pública para enlazarse desde el interior

- ¿Cuan fácilmente se puede acceder a las computadoras en ciertas horas?
- ¿Las computadoras y laptops están aseguradas en los escritorios?, etc.

Componentes de red y computadoras (Cont.)

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

Mecanismos correctivos

- Los usuarios sean conscientes de aquello en lo cual fijarse
- Requerir a los usuarios bloquear sus pantallas
- Asegurar la utilización de contraseñas fuertes
- Requerir a los usuarios de laptops aseguren sus sistemas con cables a los escritorios
- Requerir todas las laptops utilicen tecnología para encriptación
- Mantener cerrados los cuartos de servidores y gabinetes de cableado
- Mantener un inventario del hardware y software dentro de la organización
- Asegurar adecuadamente los medios de cómputo
- Escanear por puntos falsos de acceso inalámbrico
- Utilizar trampas de cable y bloqueos
- Utilizar un borrador en masa sobre medios magnéticos

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

Webinar Gratuito
Seguridad Física

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital
e-mail: ReYDeS@gmail.com

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

Enero 2019