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

Webinar Gratuito

Finalizar una Prueba de Seguridad

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

Marzo 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

- Juntar los resultados
- Priorizar vulnerabilidades
- Crear los reportes
- Poner los reportes en acción
- Aplicar parches
- Fortalecer los sistemas
- Evaluar la infraestructura de seguridad
- Automatizar el proceso de Hacking Ético
- Vigilar uso malicioso
- Tercerizar las evaluaciones de seguridad
- Otros esfuerzos en seguridad

Introducción

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

La etapa del reporte en una evaluación de seguridad, es una de las partes más críticas. Es lo último lo cual se deberá hacer después de ejecutar las pruebas, encontrar los problemas de seguridad, y dejar todo como estaba.

Se debe invertir tiempo y esfuerzo en analizar y documentar aquellos hallazgos, para asegurarse las vulnerabilidades en seguridad son eliminadas , y la información esté más segura como resultados de todo esto. El reporte es un elemento esencial para la vigilancia continua requerida por la seguridad de la información y gestión de riesgos.

El reporte incluye todos los hallazgos para determinar cuales vulnerabilidades necesitan ser arregladas, o cuales no son muy relevantes. El reporte también debe incluir un informe para la gerencia o el cliente, sobre los diversos temas de seguridad encontrados, como también recomendaciones específicas para realizar las mejoras.

El informe también muestra como se aprovechó el tiempo, esfuerzo y dinero en las pruebas de seguridad.

Juntar los resultados

- Categorización de vulnerabilidades de las herramientas de seguridad
- Conocimiento como un profesional de seguridad / TI
- El contexto de la vulnerabilidades y como actualmente impacta a la empresa

Hallazgos no técnicos

- Vulnerabilidades de ingeniería social
- Vulnerabilidades de seguridad física
- Vulnerabilidades de TI y operaciones de seguridad

Hallazgos técnicos

- Infraestructura de red
- Sistemas operativos
- Reglas del firewall
- Bases de datos
- Aplicaciones web, etc.

Priorizar vulnerabilidades

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

Priorizar las vulnerabilidades de seguridad encontradas son criticas porque muchos problemas podrían no ser factible de ser arreglados, y otras podrían no merecer el esfuerzo en su arreglo. Podría no ser factible eliminar algunas vulnerabilidades por diversas razones técnicas, y podría no permitirse el esfuerzo de eliminar otras. O simplemente la empresa puede tener un cierto nivel de tolerancia. Cada situación es diferente.

Se necesita considerar dos factores principales para cada una de las vulnerabilidades descubiertas

- Probabilidad de explotación
- Impacto si es explotado

Cada vulnerabilidad debe ser categorizada, utilizando un criterio de Alto, Medio y Bajo, donde 1 es una baja prioridad y 5 es la mayor.

Crear los reportes

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

Cada reporte debe contener la siguiente información:

- Fechas de las pruebas realizadas
- Pruebas realizadas
- Resumen de las vulnerabilidades descubiertas
- Lista en prioridad de las vulnerabilidades requeridas a ser arregladas
- Recomendaciones y pasos específicos sobre como arreglar los agujeros de seguridad encontrados

Evitar personas no autorizadas accedan al reporte final

- Entregar el reporte y documentación relacionada, además de archivos, únicamente a aquellos en la empresa quienes tengan la necesidad de conocerla
- Enviar el reporte final electrónicamente, encriptar todos los adjuntos, como la documentación y los resultados de prueba, utilizando tal vez un formato zip encriptado, o servicios más seguros.

Poner los reportes en acción

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

Como se puede percibir, las vulnerabilidades de seguridad obviamente deben ser arregladas, pero frecuentemente esto no queda muy claro. Cuando se revisan las vulnerabilidades encontradas, se debe considerar las siguientes variables.

- Cuan crítico es el sistema vulnerable
- Cual información sensible o procesos de la empresa están involucrados
- Si la vulnerabilidad puede ser arregladas
- Cuan fácil es arreglar la vulnerabilidad
- Si se puede desconectar el sistema para arreglar el problema
- Cuando tiempo, dinero y esfuerzo está involucrado en comprar nuevo hardware o software, o reequipamiento en los procesos de la empresa para arregla los agujeros

Se sugiere enfocarse en las mas críticas primero, es decir aquellas con un alto impacto y alta probabilidad de ocurrencia.

Aplicar parches

A continuación se detallan algunos parches para mantener el sistema seguro:

- Asegurarse todas las personas y departamentos están involucrados en aplicar los parches en los sistemas de la organización
- Tener procedimientos formales y documentados, implementados para procesos críticos
- Hacer políticas y tener procedimientos implementados para probar los parches, antes de aplicarlo en lo servidores de producción

Existen herramientas comerciales y libres para desplegar los parches, y mantenerse actualizado con los mismos. Aunque la sugerencia es utilizar estas aplicaciones cuando sea una red muy grande, o se utilicen en la red diversos sistemas operativos, y diversas aplicaciones web de terceros instalados.

Fortalecer los sistemas

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

Además de parchar los sistemas, se debe estar seguro los sistemas están fortalecidos, desde la perspectiva de las vulnerabilidades de seguridad, en la cual los parches no pueden arreglar.

Muchas personas creen únicamente con aplicar los parches sus sistemas están seguros. Incluso algunos administradores de red ignoran las prácticas para fortalecimiento recomendadas de organizaciones como NIST.

Pero también considerar, el fortalecimiento de los sistemas no es una solución para los ataques maliciosos. Debido a cada sistema y cada organización tienen necesidades diferentes, no existen una solución para todos los casos, de tal manera se debe tratar de encontrar un balance de todo aquello disponibles para elevar la seguridad.

* https://csrc.nist.gov/publications/sp
* https://www.cisecurity.org/

Evaluar la infraestructura de seguridad

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

Una revisión global de la infraestructura de seguridad de los sistemas

- Buscar como ha sido diseñada toda la red
- Mapear la red utilizando la información obtenida desde las pruebas de seguridad
- Pensar sobre las perspectivas para corregir las vulnerabilidades, e incrementar la seguridad global de la organización
- Pensar en las políticas y procedimientos de seguridad en la organización

Mirar la seguridad desde una perspectiva de alto nivel y una perspectiva no técnica proporciona una nueva visión de los agujeros de seguridad. Al principio requiere tiempo y esfuerzo, pero después de establecer una línea base de seguridad, es mucho más fácil administrar las nuevas amenazas y vulnerabilidades.

Automatizar el proceso de Hacking Ético

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

Es factible automatizar muchos procesos del Hacking Ético, por ejemplo:

- Hacer barridos de red con ping y escaneos de puertos, para mostrar cuales sistemas están disponibles y aquello ejecutándose
- Pruebas para romper contraseñas, intentando acceder hacia aplicaciones web externas, servidores remotos, etc.
- Escaneos de vulnerabilidades para verificar parches ausentes, malas configuraciones, y agujeros explotables.
- Explotación de vulnerabilidades

Algunas etapas y fases, como enumeración, pruebas contra aplicaciones web, ingeniería social, o seguridad física, no pueden ser completamente automáticos. Siempre se necesita estar involucrado en ellos.

Vigilar uso malicioso

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

Vigilar los eventos relacionados a la seguridad es esencial para los esfuerzos de la seguridad.

Sin embargo, desplazarse manualmente a través de los archivos de logs, no es la mejor manera de vigilar el sistema. Considerar lo siguiente:

- Encontrar eventos de seguridad crítica en los logs es difícil sino imposible.
- Dependiendo del tipo de equipo de seguridad y logging utilizado, se podría no detectar algunos eventos de seguridad.

En lugar de lo anterior se sugiere:

- Habilitar sistemas de logging cuando esto sea razonable y posible.
- Registrar los eventos de seguridad utilizando syslog, sobre un dispositivo de una sola escritura y múltiples lecturas.

Tercerizar las evaluaciones de seguridad

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

- ¿Está el proveedor de seguridad de su lado o del lado de los proveedores?. ¿El proveedor intenta vender sus productos o es neutral?
- ¿Cuales otros servicios de seguridad o TI ofrece el proveedor?. ¿El proveedor se enfoca únicamente en seguridad?
- ¿Cuales son las políticas de contrato y terminación del proveedor?
- ¿El proveedor entiende las necesidades de la empresa?
- ¿Cuan bien se comunica el proveedor?
- ¿Se conoce exactamente quien realiza las pruebas?
- ¿El proveedor tiene la experiencia para recomendar medidas prácticas y efectivas para las vulnerabilidades encontradas?
- ¿Cuales son los motivos de la organización?

Otros esfuerzos en seguridad

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

El Hacking ético a través de la evaluación de seguridad, no es la solución completa ni total para la seguridad de la información. No garantiza la seguridad, pero ciertamente es un gran inicio. Las pruebas deben estar integradas como parte de un programa global de seguridad, lo cual incluye:

- Información de alto nivel sobre las evaluaciones de riesgos
- Sólidas políticas y estándares de seguridad, las cuales se apliquen y cumplan adecuadamente
- Sólidos planes para la continuidad de la empresa y respuesta de incidentes
- Concientización efectiva de seguridad e iniciativas de entrenamiento

Estos esfuerzos pueden requerir contratar más personal o subcontratar más ayuda de seguridad. No olvidar entrenarse a si mismo y a los colegas. Esta es área de educación constante.

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

Webinar Gratuito

Finalizar una Prueba de Seguridad

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

Marzo 2019