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

Webinar Gratuito

Introducción al Hacking Ético

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital

e-mail: ReYDeS@gmail.com

Octubre 2018

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, la cual está netamente dedicada a brindar servicios de capacitación, relacionados con las áreas de seguridad de la información y tecnologías de la información, tales como; Pruebas de Penetracion (Penetration Testing), Hacking Ético (Ethical Hacking), Evaluación de Vulnerabilidades (Vulnerability Assessment), Forense de Computadoras (Computer Forensics) y Forense Digital (Digital Forensics). Bbrinda servicios de consultorías especializadas en todas las áreas mencionadas.

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

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

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

https://twitter.com/mileseceirl

Temario

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

- Definiendo un Hacker
- Definiendo un Usuario Malicioso
- Hacking Ético versus Auditoría
- Consideraciones Políticas
- Cumplimiento y Regulaciones
- Entender la Necesidad de Evaluar los Sistemas
- Entender los Peligros Enfrentados por los Sistemas
- Ataques No Técnicos
- Ataques a la Infraestructura de Red
- Ataques al Sistema Operativo, Aplicación y Otros Ataques Especializados
- Trabajar de manera Ética
- Respetar la Privacidad
- No Dañar los Sistemas
- Formular un Plan
- Seleccionar las Herramientas
- Ejecutar el Plan
- Evaluar los Resultados

Definiendo un Hacker

"Hacker" tiene dos significados.

- Tradicionalmente, a los "Hackers" les gusta jugar con software y sistemas electrónicos. Los Hackers disfrutan explorando y aprendiendo como funcionan los sistemas de cómputo. Les encanta descubrir nuevas maneras de trabajar, mecánicamente y electrónicamente.

- En años recientes, los Hackers han adquirido un nuevo significado, alguien quien maliciosamente irrumpe en los sistemas para beneficio personal. Técnicamente estos criminales son "Crackers" (Hackers criminales). Los Crackers romper o irrumpen en sistemas con intenciones maliciosas. El beneficio buscado puede ser fama, robo de propiedad intelectual, ganancia económica, o incluso la venganza. Modifican, eliminan y roban información, como también desconectan redes completas, lo cual frecuentemente hace a grandes corporaciones y agencia gubernamentales ponerse de rodillas.

Definiendo un Usuario Malicioso

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

Un usuario malicioso, implica un empleado descontento, contratista, interno, u otro usuario fraudulento, quien abusa de sus privilegios de confianza, es un término común en los círculos de seguridad, y en los titulares sobre brechas de seguridad.

El problema no es necesariamente los usuario “Hackeen” los sistemas internos, sino los usuarios quienes abusan de sus privilegios de acceso en computadoras otorgado. Los usuario hurgan a través de los sistemas de bases de datos críticos, para recopilar información confidencial, enviar por correo electrónico información confidencial del cliente hacia la competencia, u hacia otro lugar en la nube, así mismo eliminar archivos confidenciales de los servidores, los cuales probablemente no se necesitaba tener acceso en primera instancia. También esta el ignorante informate ocasional, cuya intención no es maliciosa, pero causa problema de seguridad, moviendo, borrando, o dañando información sensible. Incluso un error en el teclado puede tener consecuencias terribles en el mundo de los negocios.

Hacking Ético versus Auditoría

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

Muchas personas confunden las pruebas de seguridad mediante la perspectiva del Hacking Ético, con auditorías de seguridad, pero existe una gran diferencia. La auditoría de seguridad involucra comparar las políticas de seguridad de la compañía (o requerimientos para cumplimiento) con lo actualmente implementado. La intención de una auditoría de seguridad es validar la existencia de los controles de seguridad, típicamente utilizando una perspectiva basada en el riesgo. La auditoría frecuentemente involucra revisar los procesos de la empresa, y en muchos casos, podría nos ser muy técnico. Frecuentemente se refiere a un auditoría de seguridad como una lista de verificación de seguridad, porque usualmente se basa en listas de verificación.

Las evaluaciones de seguridad basadas alrededor de Hacking Ético, se enfocan en las vulnerabilidades factibles de ser explotadas. Esta perspectiva de prueba validad los controles de seguridad no existen o son ineficientes. Un Hacking Ético puede ser técnico y no técnico, y aunque se use una metodología, es menos formal a una auditoria.

Consideraciones Políticas

Si se elige hacer un Hacking ético, una importante parte del programa de gestión del riesgo de información de la empresa, realmente necesita tener una política documentada de pruebas de seguridad. Tales políticas delinean quien realiza las pruebas, el tipo de pruebas a realizar, la frecuencia para realizar las pruebas. Los procedimientos específicos de las pruebas de seguridad, podrían describirse en las metodologías. Se puede considerar la creación de un documento de estándares de seguridad, las cuales describan las herramientas utilizadas, y las personas específicas quienes realizarán las pruebas. También se puede listar las fechas estándares para las pruebas, como una vez cada trimestre para los sistemas externos, y pruebas bianuales para los sistemas internos, es decir aquello lo cual funcionen para la empresa.

Cumplimiento y Regulaciones

Las propias políticas internas podrían dictar como gestionar las vistas de las pruebas de seguridad, pero también se necesita considerar, las leyes y regulaciones a nivel de país, región o internacional.

Existen muchas leyes en Estados Unidos:

- HIPPAA
- HITECH
- GLBA
- NERC
- CIP
- PCI DSS

Así mismo en latinoamerica existen muchos países en donde también se aplican regulaciones y temas de cumplimiento.

Entender la Necesidad de Evaluar los Sistemas

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

Con el aumento de Hackers, y sus conocimientos en expansión, además del número creciente de vulnerabilidades descubiertas y otras desconocidas, eventualmente todos los sistemas de cómputo y aplicaciones podrían ser “hackeadas”, o comprometidas de algunas manera. El proteger los sistemas de los chicos malos, y no únicamente de vulnerabilidades genéricas conocidas por todos, es absolutamente crítico.

Los objetivos globales para las pruebas de seguridad son:

- Priorizar los sistemas, de tal manera se pueda enfocar los esfuerzos en los más relevantes
- “Hackear” los sistemas de una manera no destructiva
- Enumerar las vulnerabilidades y, de ser necesario, probar la gestión de vulnerabilidades existe, y puede ser explotada.
- Aplicación los resultados para remover las vulnerabilidades, y asegurar mejor los sistemas

Entender los Peligros Enfrentados por los Sistemas

Una de las cosas generalmente a conocer es, los sistema están bajo ataque de Hackers a nivel mundial, y usuarios maliciosos a través de la oficina; también se debe entender, los ataques específicos contra los sistemas son posibles.

Muchas vulnerabilidades de seguridad no son críticas por si mismas. Sin embargo, explotar varias vulnerabilidades al mismo tiempo, pueden abarcar todo el sistema o el entorno de la red.

La complejidad es el enemigo de la seguridad.

Las posibles vulnerabilidades y ataques han crecido enormemente en años recientes, debido a la virtualización, computación en la nube, e incluso medios sociales. Estas tres cosas solas han añadido una complejidad inconmensurable al entorno de TI.

Ataques No Técnicos

Las explotaciones involucrándo manipular personas; usuarios finales, e incluso uno mismo; son las grandes vulnerabilidades dentro de cualquier computadora o infraestructura de red. Los humanos confían por naturaleza, lo cual puede conducir a explotaciones de ingeniería social. La ingeniería social es la explotación de la naturaleza confiada del ser humano, para ganar información, frecuentemente mediante phishing, para propósito maliciosos.

Otros ataques efectivos contra los sistemas de información son los físicos. Los Hackers irrumpen dentro de las edificios, salas de cómputo, y otras áreas conteniendo información crítica o propiedad, para robar computadoras, servidores, y otro equipo valioso. Los ataques físicos pueden también incluir el buscar en la basura, en busca de propiedad intelectual, contraseñas, diagramas de red, y otra información.

Ataques a la Infraestructura de Red

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

Los ataques contra la infraestructura de red pueden ser fácilmente realizados, porque muchas redes pueden ser alcanzadas desde cualquier lugar del mundo, a través de Internet.

Algunos ejemplos de ataques a la infraestructura de red son los siguientes:

- Conectarse hacia una red a través de un punto de acceso inalámbrico conectado detrás del firewall
- Explotar debilidades en los protocolos de red, como TCP/IP y SSL
- Inundar la red con muchas peticiones, creando una negación de servicio (DoS), para peticiones legítimas
- Instalar un analizador de red sobre un segmento de red, y capturar cada paquete el cual viaja a través de esta, revelando información confidencial en texto plano

Ataques al Sistema Operativo

El Hacking al sistema operativo, es el método preferido de los chicos malos. Los ataques al sistema operativo constituyen una gran porción de los ataques, simplemente porque cada computadora tiene un sistema operativo, y los sistemas operativos son susceptibles a muchas explotaciones bien conocidas, incluyendo vulnerabilidades sin parchar por años.

Algunos sistemas operativos tienden a ser mas seguros comparados con otros. Pero en todos ellos existe la posibilidad de identificar vulnerabilidades y explotación.

Algunos ejemplos de ataques al sistema operativo son:

- Explotar parches ausentes
- Atacar los sistemas de autenticación incorporados
- Romper la seguridad del sistema de archivos
- Romper las contraseñas e implementaciones débiles de encriptación

Ataques a la Aplicación y Otros Ataques Especializados

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

Las aplicaciones tienen un alto indice de ataque por parte de los Hackers. Programas (como software para servidor de correo y aplicaciones web) son frecuentemente atacados. Por ejemplo.

- Aplicaciones HTTP y SMTP son frecuentemente atacados, porque muchos firewalls y otros mecanismos de seguridad son configurados para permitir acceso hacia estos servicios, hacia y desde Internet, incluso cuando existe encriptación TLS o SSL.

- Se incrementan los ataques contras las aplicaciones móviles, dada su relevancia en las empresas.

- Archivos inseguros conteniendo información sensible están dispersos a través de las estaciones de trabajo y recursos compartidos. Los sistemas de bases de datos también contienen diversas vulnerabilidades, las cuales puede explotar un usuario malicioso.

Trabajar de manera Ética

La palabra ético en este contexto significa trabajar con altos valores y moral profesional. Ya sea se esté realizando pruebas de seguridad contra sistemas propios, o para alguien quien ha contratado servicios, todo debe ser hecho para apoyo de los objetivos de la compañía. No se permiten agendas ocultas. Esto también incluye reportar todos los hallazgos sin importar si generará o no una reacción política.

La fiabilidad es el principio máximo. También es la mejor manera de poner (y mantener) a las personas de su lado, en el apoyo al programa de seguridad. La mala utilización de la información está absolutamente prohibida. Esto es hecho por los chicos malos. Estos recibirán una multa o pueden ir a prisión por sus malas acciones.

Siempre se debe mantener la ética por sobre todo.

Respetar la Privacidad

Se debe tratar la información recopilada con el mayor respeto. Toda la información obtenida durante las pruebas; desde fallas en las aplicaciones web, contraseñas en texto plano, hasta información identificable personalmente, y más allá debe mantenerse privada. Nada bueno puede resultar de indagar información confidencial de la corporación o vida privada de los empleados.

Involucrar a otros en los procesos. Emplear un sistema de vigilar al vigilante, el cual ayude a generar confianza para los proyectos de evaluaciones de seguridad. Documentar es la clave, entonces, documente todo.

No Dañar los Sistemas

Uno de los más grandes errores percibidos por quienes intentan evaluar sus propios sistemas, es inadvertidamente dañar los sistemas los cuales están intentando mantener en funcionamiento. Aunque actualmente no sucede tan frecuentemente como era antes, dada la resistencia actual de los sistemas. Sin embargo, una pobre planificación y agenda puede tener consecuencias negativas.

Aunque no es probable, se cree condiciones de DoS en los sistemas cuando se realicen las pruebas. El ejecutar muchas pruebas rápidamente puede causar el sistema se bloquee, corrupción de datos, reinicios, y más. Esto es especialmente verdadero cuando se prueba sitios web y aplicaciones. No se debe apresurar y suponer una red o host específico puede manejar todo aquello generado por las herramientas de red y escaners de vulnerabilidades.

Utilizar un Proceso de Hacking Ético

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

Como prácticamente cualquier proyecto de seguridad o TI, se necesita un plan para las pruebas de seguridad. Se ha mencionado la acción sin planificación es la raíz de todas las fallas. Temas estratégicos y tácticos en el proceso de Hacking Ético, necesitan ser determinados y haber sido acordados. Para asegurar el éxito de los esfuerzos, se debe dedicar un tiempo para planificar de antemano cualquier cantidad de pruebas, desde una simple prueba de descifrado de contraseñas del sistema operativo contra algunos servidores, hasta la evaluación de vulnerabilidades completas de un entorno web.

Si se elige contratar a un Hacker “reformado” para trabajar durante estas pruebas, o para obtener una perspectiva independiente, se debe tener mucho cuidado. Se deben evaluar los pros y contras, pues los recursos para Hacking Ético siempre deben ser confiables.

Formular un Plan

Tener la aprobación para las pruebas es esencial. Se debe asegurar de se esta haciendo esto de manera conocida y visible, al menos para los jefes. El obtener el aval para el proyecto es el primer paso. Esto es como los objetivos de evaluación serán definidos. Este aval puede venir del gerente, un ejecutivo, el cliente, etc Se necesita tener un respaldo de el plan. Pues las pruebas podrían ser llamadas inesperadas, si alguien dice jamas haberlas autorizado. Incluso podría existir una denuncia.

Un bien definido alcance incluye la siguiente información:

- Sistemas específicos a ser evaluados
- Riesgo involucrado
- Fechas para realizar las pruebas y tiempo total
- Si se intentará ser detectado
- Conocer los sistemas antes de iniciar las pruebas
- Acciones a tomar cuando una gran falla sea detectada

Seleccionar las Herramientas

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

Asegurarse de utilizar las herramientas correctas para las tareas:

- Para romper contraseñas, se necesitan herramientas para romper contraseñas, como 0phrack o John The Ripper

- Para un análisis profundo de una aplicación web, un escaner de vulnerabilidades (como Arachni, Zed Attack Proxy, etc.), es más apropiado a un analizar de red (Como Wireshark y otro).

Cuando se seleccionen las herramientas de seguridad, se sugiere revisar otras opiniones de diferentes fuentes. Entre algunas de las herramientas comerciales y open source se tienen: Cain y Abel, Air-crack, Nexpose, OpenVas, John The Ripper, 0phrack, Metasploit Framework, ZAP, etc.

Es importante seleccionar las herramienta basándose en los requerimientos de las pruebas. Y leer toda su documentación, la cual puede ser archivos, guías, videos, evaluaciones, etc.

Ejecutar el Plan

Las buenas pruebas de seguridad requieren persistencia. El tiempo y la paciencia son importantes. También, el ser cuidadoso cuando se realizan las pruebas de Hacking Ético. Un criminal en la red, o un empleado aparentemente benigno, quien mira por encima del hombro aquello suscitándose, puede utilizar esta información contra la empresa.

Se debe asegurar que no existan Hackers en los sistemas antes de iniciar. Asegurarse de todo sea tranquilo y privado cuando sea posible. Esto es critico cuando se transmita y almacenen los resultados de las pruebas.

Se debe iniciar con la perspectiva más amplia y afinar los resultados.

1. Buscar en Internet el nombre de la organización, los nombres de las computadoras, y direcciones IP
2. Afinar el alcance, enfocarse en sistemas específicos a evaluar.
3. Afinar aún más con un ojo más crítico.
4. Realizar los ataques y explorar las vulnerabilidades.

Evaluar Resultados

Evaluar los resultados para ver aquello descubierto, asumiendo las vulnerabilidades no se han hecho evidentes hasta este punto. Aquí es donde el conocimiento cuenta. La habilidad para evaluar los resultados y correlacionar las vulnerabilidades específicas descubiertas mejorará con la práctica. Se terminará conociendo los sistemas mucho más en comparación a otros. Esto hace el proceso de evaluación sea más sencillo.

Enviar el reporte formal hacia la gerencia o al cliente, describiendo los resultados y cualquier recomendación necesaria de compartir. Mantener también a las partes informadas para demostrar los esfuerzos, y el dinero ha sido bien invertido.

Continuidad

Cuando se finalizan las pruebas de seguridad, el cliente necesita implementar las recomendaciones, para asegurarse los sistemas están seguros. De otra manera el tiempo, dinero, y esfuerzo invertido en el Hacking Ético será un desperdicio. Tristemente este escenario es muy frecuente.

Continuamente aparecen nuevas vulnerabilidades. Los sistemas de información continuamente cambian y se vuelven más complejos. Las nuevas vulnerabilidades y códigos de explotación son descubiertos regularmente. Los escaners de vulnerabilidades mejoran y mejoran. Las pruebas de seguridad son una instantánea de la postura de seguridad de los sistemas. Con el tiempo todo puede cambiar, especialmente cuando se actualiza software, añaden sistemas de cómputo, o aplican parches. Se debe planificar pruebas regulares y consistentes, por ejemplo una vez al mes, bimensual o semestralmente.

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

Webinar Gratuito

Introducción al Hacking Ético

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital

e-mail: ReYDeS@gmail.com

Octubre 2018