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

# Webinar Gratuito

# Bases de Datos y Sistemas de Almacenamiento

**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/

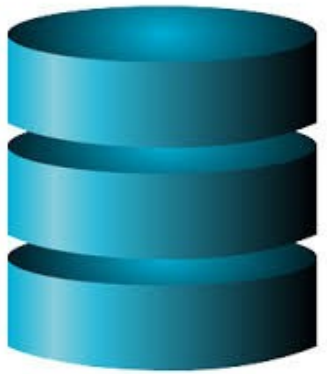
https://twitter.com/mileseceirl

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

# Temario

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

- Buceando en las bases de datos
- Seleccionar las herramientas
- Encontrar bases de datos en la red
- Romper contraseñas de bases de datos
- Escanear bases de datos por vulnerabilidades
- Seguir las mejores prácticas para minimizar riesgos de seguridad en bases de datos
- Apertura sobre sistemas de almacenamiento
- Seleccionar las herramientas
- Encontrar sistemas de almacenamiento en la red
- Erradicar texto sensible en los archivos de red
- Seguir las mejores prácticas para minimizar riesgos de seguridad en almacenamiento



# Introducción



Los ataques contra los sistemas de bases de datos y sistemas de almacenamiento pueden ser muy serios, porque es donde “lo bueno” se localiza, y aquellos con intenciones maliciosas también conocen esto.

Estos ataques pueden ocurrir a través de Internet o sobre una red interna, cuando los atacantes externos o internos maliciosos explotan cualquier número de vulnerabilidades. Estos ataques pueden ocurrir también a través de aplicaciones web mediante una inyección SQL.

# Buceando en las bases de datos

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

Sistemas de bases de datos, como el Servidor Microsoft SQL, MySQL, y Oracle, se han escondido detrás de la escena, pero su valor y sus vulnerabilidades finalmente han llegado al primer plano. Sí, incluso el poderoso Oracle quien clamó algunas vez ser “no hackeable” es susceptible hacia explotaciones similares a su competencia.

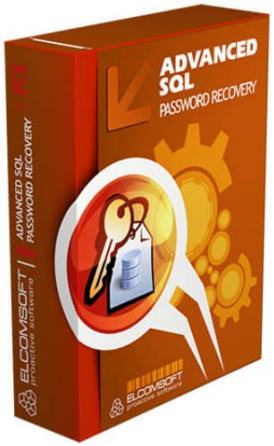
Con la gran cantidad de requerimientos para regulación gobernando la seguridad en base de datos, casi ninguna empresa puede ocultarse de los riesgos encontrándose dentro de esta, pues prácticamente todas las empresas (grandes y pequeñas) utilizan algún tipo de base de datos, ya sea de forma interna u hospedada en la nube.

# Seleccionar las herramientas

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

Como con las redes inalámbricas, sistemas operativos, y similares, se necesitan buenas herramientas, si se requiere encontrar problemas de seguridad en bases de datos. Algunas de estas herramientas son:

- Advanced SQL Password Recovery
- Cain & Abel
- Nexpose
- SQLPing3




* https://www.elcomsoft.com/asqlpr.html
* http://www.oxid.it/cain.html
* https://www.rapid7.com/products/nexpose/
* http://www.sqlsecurity.com/downloads

# Encontrar bases de datos en la red



La primera etapa para descubrir vulnerabilidades en bases de datos es figurar donde están localizados en la red. Esto podría parecer divertido, pero muchos administradores de red no son conscientes de bases de datos ejecutándose en sus entornos. Esto es especialmente cierto para ediciones de software para bases de datos como SQL Server Express, el cual cualquiera puede descargar y ejecutar en la red.

Frecuentemente se encuentran datos sensibles de producción como tarjetas de crédito y otra información, siendo utilizados en bases de datos de prueba, los cuales están completamente abiertas a cualquier abuso de un interno malicioso o atacantes externos. Utilizar datos sensibles de producción en áreas no controladas hacia la red como de ventas, desarrollo de software, y evaluación de la calidad, es una brecha de datos esperando ocurrir.

* http://www.petefinnigan.com/tools.htm

# Romper contraseñas de bases de datos

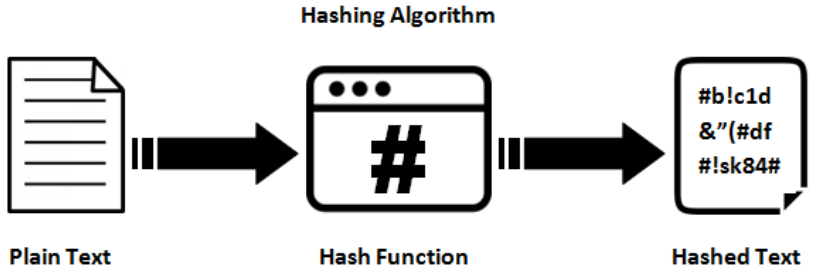


Algunas herramientas proporcionan funcionalidades para realizar un ataque basado en diccionario. Muchas veces es factible utilizar el usuario por defecto “sa”, e intentar una gran cantidad de contraseñas.

Adicionalmente existen herramientas las cuales pueden ser utilizadas para tratar romper los hashes de las contraseñas obtenidas, siendo un requisito previo obtener estos hashes por algún mecanismo.

Cualquiera de estas herramientas son muy importantes para demostrar las debilidades básicas correspondiente a la seguridad en bases de datos.

Una de las deficiencias más obvias pero comunes, es encontrar un sistema de base de datos sin una contraseña. Siendo este uno de los escenarios más terribles.



# Escanear bases de datos por vulnerabilidades

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

Como con los sistemas operativos y aplicaciones web, algunas vulnerabilidades en bases de datos pueden ser explotadas utilizando las herramientas adecuadas. Con estas se pueden explotar vulnerabilidades como:

- Desbordamiento de buffer
- Escalado de privilegios
- Hashes de contraseñas accedibles a través de cuentas por defecto o no protegidas
- Métodos habilitados débiles de autenticación

Existen diversos escáneres comerciales  para realizar verificaciones profundas contra bases de datos, incluyendo auditorias para derechos de usuario en SQL Server, Oracle, entre otros.

* https://www.trustwave.com/en-us/services/security-testing/appdetectivepro/

# Mejores prácticas para minimizar riesgos de seguridad en BDs

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

- Ejecutar bases de datos en servidores dedicados
- Verificar vulnerabilidades de seguridad en el sistema operativo subyacente
- Asegurar las bases de datos caen dentro del alcance de parches y fortalecimiento del sistema
- Requerir contraseñas fuertes en cada sistema de bases de datos
- Utilizar permisos apropiados para archivos y compartidos
- Eliminar datos sensibles antes de ser utilizados en entornos de no producción, como desarrollo o QA
- Verificar las aplicaciones web por inyección SQL y vulnerabilidades relacionadas

# Apertura sobre sistemas de almacenamiento

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

Los atacantes maliciosos está realizando un creciente número de ataques relacionados al almacenamiento, utilizando varios vectores de ataques y herramientas para romper dentro de entornos para almacenamiento. Por lo tanto se necesita conocer las técnicas y herramientas para utilizarlas en la evaluación de los entornos para almacenamiento.

Existen errores de percepción y mitos relacionados con la seguridad en los sistemas para almacenamiento como “Storage Area Networks” (SAN), CIFS, y sistemas “Network Attached Storage” (NAS) basadas en NFS, entre otros. Muchos administradores de red y almacenamiento creen la “encriptación o RAID es igual a seguridad en almacenamiento”, “Un atacante externo no puede alcanzar un entorno para almcenamiento”, “Los sistemas son resilentes”, o “La seguridad está por todos lados”.

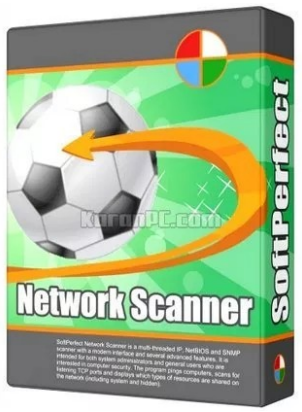
Estas son creencias muy peligrosas, y no se debe confiar y creer los ataques nunca tendrán como objetivo los sistemas críticos para almacenamiento.

# Seleccionar las herramientas



Existen algunas herramientas para probar la seguridad de almacenamiento.

- Nmap
- SoftPerfect Network Scanner
- FileLocator Pro
- Nexpose


* https://nmap.org/
* https://www.softperfect.com/products/networkscanner/
* https://www.mythicsoft.com/
* https://www.rapid7.com/products/nexpose/

# Encontrar sistemas de almacenamiento en la red



Para buscar vulnerabilidades relacionadas al almacenamiento, se debe primero figurar aquello lo cual está allí. La mejor manera de hacer esto es utilizando un escáner de puertos, idealmente un escáner de vulnerabilidades todo en uno. También, dado muchos servidores de almacenamiento tienen servidores web incorporados, se pueden utilizar herramientas para el entorno web, de tal manera se descubran fallas a este nivel. Se pueden utilizar estos escáneres de vulnerabilidades para ganar un punto de apoyo dentro de áreas necesarias a ser inspeccionadas profundamente, tales como autenticación débil, sistemas operativos sin parches, XSS, entre otros.

Una vulnerabilidad de almacenamiento comúnmente pasado por alto, es muchos sistemas de almacenamiento pueden ser accedidos desde ya sea un segmento DMZ, desde la red interna o viceversa.

También se deben realizar escaneos básicos para permisos de archivos y compartidos.

# Erradicar texto sensible en los archivos de red



Una vez encontrados recursos abiertos, se requiere escanear por información sensible almacenada.

- Registros médicos de empleados
- Números de tarjetas de crédito de clientes
- Reportes financieros corporativos
- Código fuente
- Archivo maestro de bases de datos

- Fechas de nacimiento
- Números de documentos de identificación
- Números de tarjetas

- Txt
- Doc, docx
- Rtf
- Xls, xlsx
- pdf

# Mejores prácticas para minimizar riesgos en almacenamiento

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

- Verificar los sistemas operativos subyacentes por vulnerabilidades de seguridad
- Asegurarse los almacenamientos de red (sistemas SAN y NAS) caen dentro del alcance de parches y fortalecimiento
- Requerir contraseñas fuertes en las interfaces para la gestión del almacenamiento
- Utilizar permisos adecuados en archivos y compartidos
- Educar a los usuarios sobre donde almacenar información sensibles, y sus riesgos
- Identificar cualquier dato sensible en producción antes de ser utilizado en desarrollo o QA
- Utilizar un firewall de red

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

# Webinar Gratuito

# Bases de Datos y Sistemas de Almacenamiento

**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