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

Webinar Gratuito
Contraseñas

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
- Entender las vulnerabilidades en las contraseñas
- Vulnerabilidades en contraseñas organizacionales
- Vulnerabilidades técnicas en contraseñas
- Romper contraseñas
- Romper contraseñas de la manera antigua
- Romper contraseñas con herramientas de alta tecnología
- Romper archivos protegidos por contraseñas
- Entender otras maneras de romper contraseñas
- Medidas correctivas generales para romper contraseñas
- Almacenar contraseñas
- Crear políticas de contraseñas
- Tomar otras medidas correctivas
- Asegurar los sistemas operativos
- Windows y Linux

Introducción

El Hacking a las contraseñas es una manera común y fácil utilizada por los atacantes para obtener acceso no autorizado hacia la red, computadoras, o acceso a la aplicación. Muchos reportes aún reafirman las contraseñas débiles son la raíz de muchos problemas de seguridad.

Aunque las contraseñas fuertes; idealmente, extensas y fuertes frases de paso son difíciles de romper (o adivinar), son fáciles de crear y mantener, los administradores de red y los usuarios frecuentemente descuidan esto. Por lo tanto, las contraseñas son el eslabón más débil en toda la cadena relacionada a la seguridad de la información. Las contraseñas se basan en el secreto. Una vez se haya comprometido una contraseña, su propietario original no es la única persona quien puede acceder hacia el sistema. Es aquí cuando comienzan a suceder cosas malas.

Los atacantes externos y usuarios maliciosos tienen muchas maneras de obtener contraseñas. Pueden obtener contraseñas simplemente solicitándolas, o mirando sobre el hombro de los usuarios mientras escriben sus contraseñas.

Entender las vulnerabilidades en las contraseñas

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

Cuando se hace un balance sobre el costo de la seguridad y el valor de la información protegida, la combinación de un ID de usuario y una contraseña secreta es usualmente adecuada. Sin embargo las contraseñas dan un falso sentido de seguridad. Los chicos malos conocen esto, e intentan romper contraseñas, como un paso más para lograr irrumpir dentro de los sistemas de cómputo.

Uno de los más grandes problemas al dejar únicamente la seguridad a las contraseñas, es más de una persona puede conocerla. Algunas veces esto es intencional; frecuentemente no. La parte más preocupante es no hay manera de conocer quien, aparte del propietario de la contraseña, la conoce.

Existen dos tipos generales de vulnerabilidades en las contraseñas:

- Vulnerabilidades organizacionales o de usuario.
- Vulnerabilidades técnicas.

Vulnerabilidades en contraseñas organizacionales

La naturaleza humana desea conveniencia, especialmente cuando se trata de recordar cinco, diez, o docenas de contraseñas para el trabajo y la vida diaria. Este deseo de conveniencia hace a las contraseñas, una de las barreras más fáciles de derribar para un atacante. Las claves para contraseñas seguras son; fáciles de recordar y difíciles de romper. Sin embargo muchas personas sólo se enfocan en la parte de recordar. Usuarios utilizar la contraseña “password”, “abc123”, o no le colocan contraseña, aunque parezca increíble. En las organizaciones se puede encontrar todo esto.

A menos los usuarios sean educados y recuerden utilizar contraseñas fuertes, las contraseñas usualmente son:

- Fáciles de adivinar
- No frecuentemente cambiadas
- Reutilizadas para muchos puntos de seguridad
- Escritas en lugares inseguros

Vulnerabilidades técnicas en contraseñas

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

Frecuentemente se pueden encontrar serias vulnerabilidades técnicas después de explotar vulnerabilidades en las contraseñas.

- Esquemas de encriptación débiles
- Programas almacenando las contraseñas en memoria, archivos inseguros, bases de datos accedibles
- Bases de datos sin encriptar, proporcionando acceso directo hacia información sensible a cualquiera.
- Aplicaciones de usuario mostrando contraseñas en la pantalla mientras se escriben.

La “National Vulnerability Database” NVD, de los Estados Unidos , aproximadamente identifica más de 4,500 vulnerabilidades relacionadas a las contraseñas.

* National Vulnerability Database: https://nvd.nist.gov

Romper contraseñas

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

El romper las contraseñas es uno de los “hacks” más satisfactorios para los chicos malos. Esto alimenta el sentido de exploración y deseo de resolver un problema. Es posible no exista un deseo de explorar las contraseñas de todos pero es útil abordar el romper las contraseñas con esta mentalidad. Entonces ¿Dónde se debería empezar para probar las contraseñas de u sistema?. Generalmente funciona la contraseña de cualquier usuario. Después de obtener una contraseña, se puede frecuentemente obtener las otras, incluyendo las contraseñas de los administradores o “root”.

Las contraseñas de los administradores son una mina de oro. Con acceso administrativo no autorizado, se puede hacer virtualmente cualquier cosa en el sistema. Cuando se busca por vulnerabilidades en las contraseñas de la organización, se recomienda primero intentar obtener el nivel de acceso más alto posible, como la del administrador, a través de método más discreto posible. Así como lo hacen los criminales.

Se pueden utilizar maneras de baja tecnología y herramientas de alta tecnología para explotar vulnerabilidades, y obtener las contraseñas.

Romper contraseñas de la manera antigua

Un hacker puede utilizar métodos con baja tecnología para romper contraseñas. Estos métodos son los siguientes:

- **Ingeniería Social.** Toma ventaja de la natural confianza del ser humano para ganar información, la cual luego puede ser utilizada maliciosamente.

- **Mirar sobre el hombro.** Es el acto de mirar por el hombro de alguien más, para aquello escrito por la persona, es un ataque efectivo y poco técnico.

- **Inferencia.** Es simplemente adivinar la contraseña desde la información conocida sobre el usuario, como fecha de nacimiento, serie favorita, etc.

- **Autenticación Débil.** Atacantes externos e internos maliciosos pueden obtener, o simplemente evitar utilizar contraseñas, aprovechándose de sistemas operativos inseguros o no requiriendo contraseñas.

Romper contraseñas con herramientas de alta tecnología

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

El romper contraseñas con alta tecnología involucra utilizar un programa para intentar adivinar las contraseñas, mediante todas las combinaciones posibles. Estos métodos de alta tecnología son automáticos, después de acceder a los archivos o bases de datos de contraseñas y computadoras.

- **Software para romper contraseñas.** Cain y Abel, “ElcomSoft”, pwdump, THC-Hydra. 0Phrack, John The Ripper, RainbownCrack. Windows (C:\Windows\system32\config\ “SAM”, “ntds.dit”). En GNU/Linux. (“/etc/passwd”y “/etc/shadow”).

- **Ataques por diccionario.** Utiliza archivos conteniendo contraseñas comunes.

- **Ataques por fuerza bruta.** Podrían romper prácticamente cualquier contraseña, teniendo el suficiente tiempo.

- **Ataques arcoiris.** Utiliza tablas arcoiris para romper diversos hashes de contraseñas.

Romper archivos protegidos por contraseñas

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

Podría sorprender cuan vulnerable son los archivos protegidos por contraseñas, como documentos de texto, hojas de cálculo, y archivos comprimidos.

Romper archivos

Muchos archivos protegidos por contraseñas pueden ser rotos en cuestión de segundos o minutos. Se debe de demostrar esta vulnerabilidad de seguridad a los usuarios y gerentes.

Romper los archivos protegidos por contraseñas es relativamente simple. Pues existen herramientas comerciales y libres las cuales son factibles de utilizar.

Se recomienda realizar estas pruebas para romper las contraseñas de archivos, sobre archivos los cuales se capturen con un filtro de contenido o herramienta para el análisis del tráfico de red. Así se puede determinar cuan bien lo usuarios respetan las políticas.

Entender otras maneras de romper contraseñas

Se tienen otras maneras de romper (o capturar) contraseñas técnicamente y a través de ingeniería social.

- **Capturar pulsaciones del teclado.** Se puede utilizar software y hardware para obtener las pulsaciones.
- **Almacenamiento débil de las contraseñas.** Algunas aplicaciones antiguas almacenan las contraseñas en texto plano.
- **Analizador de red.** Olfatea la red en busca de contraseñas cifradas o en texto plano.
- **Contraseñas débiles del BIOS.** Algunas configuraciones permiten evadir este mecanismo de protección.
- **Contraseñas débiles en el limbo.** Explotar cuentas de usuario creadas o configuradas por un administrador de red, para pruebas.

Medidas correctivas generales para romper contraseñas

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

Una contraseña para un solo sistema, usualmente es igual a contraseñas para muchos otros sistemas, porque muchas personas utilizan la misma (o similar) en cada sistema el cual utilizan. Por esta razón, podría considerarse instruir a los usuarios a crear diferentes contraseñas para diferentes sistemas, especialmente aquellos sistemas protegiendo información más sensible. La única desventaja a esto, es un usuario con múltiples contraseñas, podría estar tentado a escribirla, lo cual quita todo sus beneficios.

Las contraseñas fuertes son importantes, pero se necesita tener un balance en seguridad y conveniencia:

- No se puede esperar los usuarios memoricen contraseñas insánamente complejas, y cambiarla cada semana.
- No se debe permitir contraseñas débiles o algo sin contraseña, así se tengan políticas para las contraseñas, se debe preferir utilizar frases de paso fuertes (combinaciones de palabras factibles de ser recordadas fácilmente), las cuales deban ser cambiadas pocas veces.

Almacenar contraseñas

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

Si se tiene la elección entre contraseñas débiles las cuales los usuarios puedan memorizar, y contraseñas fuertes las cuales los usuarios deban escribir. Se recomienda escribir las contraseñas y almacenar la información de manera segura. Usuarios entrenados almacenan las contraseñas escritas en un lugar seguro, no en el teclado, o archivos protegidos por contraseñas fáciles de “romper”.

Los usuarios deben almacenar sus contraseñas en cualquiera de estas ubicaciones:

- Un gabinete asegurado.
- Encriptación completa del disco, lo cual previene un intruso acceda al sistema operativo y las contraseñas almacenadas en el sistema.
- Herramientas para la gestión segura de contraseñas.

Las aplicaciones no son infalibles a ataques.

Y nunca contraseñas en “hojitas de notas”-

Crear políticas de contraseñas

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

- Demostrar como crear contraseñas seguras
- Mostrar las consecuencias de utilizar contraseñas débiles o el compartir contraseñas
- Construir un diligente programa de concientización sobre ataques de ingeniería social.

- Números, letras mayúsculas, minúsculas, caracteres especiales.
- Palabras mal escritas o crear acrónimos desde una frase u oración.
- Caracteres de puntuación para separar palabras o acrónimos.
- Cambiar contraseñas cada 6 o 12 meses, o inmediatamente se existe algún compromiso.
- Utilizar diferentes contraseñas para cada sistema.
- Utilizar longitudes variables para las contraseñas
- No utilizar palabras comunes o incluidas en un diccionario.
- No reemplazar caracteres obvios, E por 3, o I por 1.
- No reutilizar la misma contraseña después de cuatro o cinco cambios.
- Utilizar protectores de pantalla protegidas por contraseñas
- No compartir las contraseñas

Tomar otras medidas correctivas

A continuación algunas medidas correctivas recomendadas:

- Habilitar la auditoría de seguridad, para ayudar a vigilar y rastrear ataques de contraseñas.
- Mantener los sistemas actualizados
- Conocer los IDs de usuarios.

Considerar lo siguiente cuando se configure una cuenta:

- Utilizar bloqueo de cuenta.
- Si se permite autoreiniciar la cuenta, no debe ser un periodo corto.

Otros mecanismos de protección a contraseñas incluyen:

- Métodos fuertes de autenticación
- Reinicio automático de contraseñas
- Contraseña protegiendo el BIOS del sistema

Asegurar los sistemas operativos

Se pueden implementar diversos mecanismos de seguridad en los sistemas operativos, para asegurarse las contraseñas están protegidas.

Regularmente se debe realizar pruebas para romper contraseñas de baja y alta tecnología, para asegurarse los sistemas estén tan seguros como sea posible, tal vez como parte de un auditoria dos veces al añol, cada cuatro meses o mensual, de las contraseñas locales y del dominio.

Windows y Linux

Windows

- Algunas contraseñas en Windows pueden ser obtenidas simplemente leyendo el texto plano, o rompiendo texto cifrado en el registro.
- Mantener seguras todas las copias de respaldo de la base de datos SAM.
- Deshabilitar el almacenamiento de hashes LM en Windows, para contraseñas inferiores a 15 caracteres.
- Utilizar políticas de seguridad locales y grupales, para tratar de eliminar contraseñas débiles antes de ser creadas.
- Deshabilitar sesiones nulas en Windows, y habilitar el firewall.
- En Windows XP, no permitir enumeración anónima de cuentas.

Linux

- Asegurarse el sistema utiliza contraseñas SHA
- Ayudar la prevenir la creación de contraseñas débiles.
- Verificar el archivo /etc/passwd por entradas duplicadas con UID de root.

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

Webinar Gratuito
Contraseñas

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