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

Webinar Gratuito
Dispositivos Móviles

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

Febrero 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
- Dimensionar las vulnerabilidades móviles
- Romper contraseñas de laptops
- Seleccionar las herramientas
- Medidas correctivas
- Romper teléfonos y tables
- Romper contraseñas iOS
- Medidas correctivas en contra de romper contraseñas

Introducción

La computación móvil es un nuevo objetivo para las empresas, y consecuentemente también para el “Hacking”. Todos parecieran tienen un dispositivo móvil o similar, ya sea para uso personal o de empresa; aunque frecuentemente ambos.

Si no son adecuadamente asegurados, los dispositivos móviles conectados hacia la red de la empresa, representan miles de islas sin protección con información flotante fuera de control.

Debido a todos los teléfonos, tablets, y laptops ejecutan numerosas plataformas de sistemas operativos y aplicaciones, un número infinito de riesgo están asociados con la computación móvil.

En lugar de divagar en todas estas variables, se abarcan algunas de las más comunes fallas de seguridad móvil, las cuales impactan a los usuarios y empresas.

Dimensionar las vulnerabilidades móviles

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

Es ideal encontrar y arreglar aquellos inconvenientes evidentes en la red. Es allí donde se empiezan a obtener beneficios. Las siguientes debilidades móviles en teléfonos, laptops, y tablets deben estar al frente y al centro en la lista de prioridades.

- No encriptación
- Encriptación pobremente implementada
- No contraseñas para iniciar los dispositivos
- Contraseñas fáciles de adivinar (o romper)

Para otras tecnologías y sistemas (aplicaciones web, sistemas operativos, y similares), se puede usualmente encontrar la herramienta de prueba necesaria. Sin embargo, para encontrar fallas relacionadas al ámbito móvil, existen pocas herramientas disponibles. No es de sorprender las herramientas más caras frecuentemente permitan descubrir fácilmente las más grandes fallas.

Romper contraseñas de laptops

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

De hecho, una de las más grandes amenazas a la seguridad de cualquier empresa son las laptops sin encriptar. Dados todos los titulares y concientización sobre esta vulnerabilidad de seguridad, es inexcusable aún se encuentre este escenario tan frecuente en las empresas.

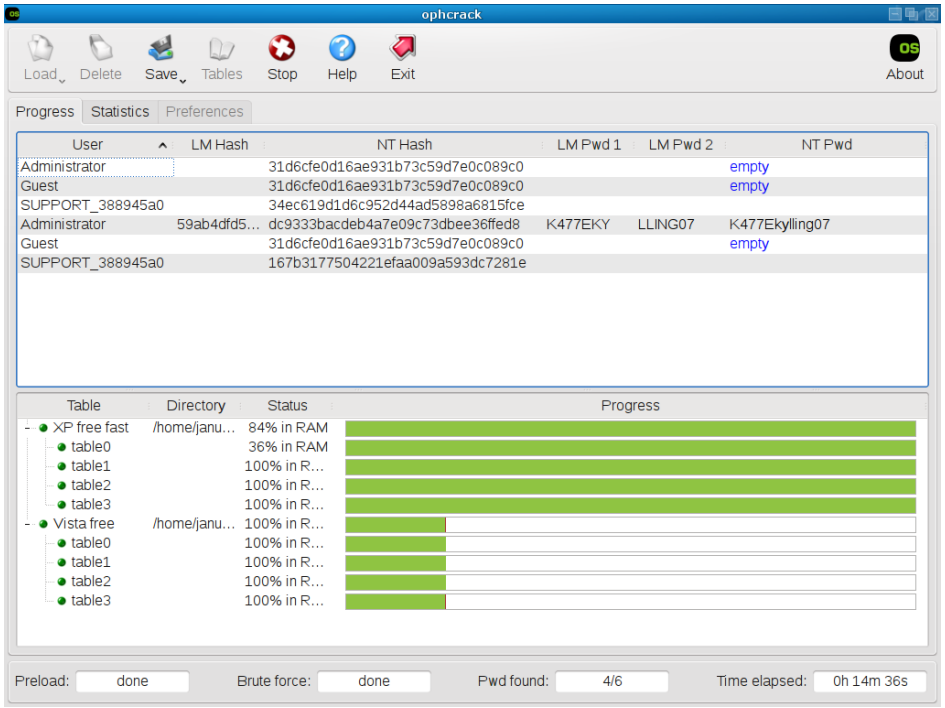
Es importante seleccionar las herramientas adecuadas para intentar romper las contraseñas en laptops utilizando Linux, Windows o Mac OS X.

Seleccionar las herramientas

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

Existen diversas herramientas para demostrar el riesgo asociado con ejecutar laptops sin encriptar. Algunas de ellas son las presentadas a continuación.

- Elcomsoft System Recovery
- WinHex
- AccessEnum
- Passware Kit Forensics
- Ophrack



* http://www.elcomsoft.com/esr.html
* http://www.winhex.com/winhex/
* https://docs.microsoft.com/es-es/sysinternals/downloads/accessenum
* https://www.passware.com/
* http://ophcrack.sourceforge.net/

Medidas correctivas

La mejor salvaguarda contra un atacante malicioso utilizando un programa para redefinir la contraseña en un sistema, es encriptar los dispositivos de almacenamiento, ya sea con soluciones incorporadas en el propio sistema operativo, como un producto de un tercero.

Las contraseñas al momento de iniciar el sistema (BIOS) también son de ayuda, pero podrían ser fáciles de evadir. Pues para evitarlo se podría retirar el dispositivo de almacenamiento y acceder a este desde otra máquina.

También es necesario asegurarse, personas no autorizadas no accedan físicamente hacia las computadoras. Cuando un atacante malicioso obtiene acceso físico a las computadoras, y estas no están encriptadas, las consecuencias pueden ser terribles. La encriptación no es una solución absoluta, pero minimiza el riesgo.

* https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview
* https://www.winmagic.com/products

Romper teléfonos y tablets

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

Con BYOD (Bring Your Own Device), se debe confiar los usuarios están tomando buenas decisiones sobre seguridad, y se debe descubrir como gestionar cada dispositivo, plataforma y aplicación. Esta gestión de administración es el más grande desafío enfrentado por los profesionales en TI. Para complicar aún más el tema, existen delincuentes informáticos, criminales, ladrones, quienes hacen todo lo mejor para explotar la complejidad en todo esto, los cuales crean serios riesgos para la empresa. La realidad es muy pocas empresas (y personas), tienen sus teléfonos y tablets debidamente protegidos.

Muchos proveedores claman sus soluciones MDM (Mobile Device Management), son las respuesta a los problemas en teléfonos y tablets. Hasta cierto punto es cierto. Los controles MDM separan la información personal de la comercial, además de asegurar los controles de seguridad adecuados estén habilitados en todo momento, para ayudar a dar el gran salto en la seguridad móvil en la empresa.

* https://www.ibm.com/security/mobile/maas360
* https://www.air-watch.com/

Romper contraseñas iOS

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

Podría ser aventurado decir muchas de las contraseñas en teléfonos y tablets (en realidad son sólo de cuatro dígitos o códigos de acceso), pueden ser adivinados. Un dispositivo móvil puede perderse o puede ser robado, y la persona quien lo tenga sólo debe intentar algunas combinaciones básicas de números, como 1234, 1212, o 0000... y listo. El sistema es desbloqueado.

Muchos teléfonos y tablets ejecutando iOS y Android están configurados para limpiar o hacer “wipe” del dispositivo, si la contraseña incorrecta es ingresado un número determinado de intentos; como por ejemplo 10. Un control de seguridad razonable de hecho. ¿Pero que más puede ser hecho?. Algunas herramientas comerciales puede ser utilizadas para romper contraseñas simples o PINs, para luego recuperar la información perdida o robada desde dispositivos, o aquellos bajo una investigación forense.

* https://www.elcomsoft.com/eppb.html
* https://www.elcomsoft.com/eift.html

Medidas correctivas en contra de romper contraseñas

La manera más sencilla de prevenir la acción para intentar romper contraseñas es exigir; y fortalecer continuamente, contraseñas fuertes como PINs multi dígitos constituidos de 5 o más números, o mejor aún, frases de paso complejas, las cuales sean muy fáciles de recordar, pero prácticamente imposibles de romper.

Los controles MDM pueden ayudar a aplicar esta política. Es probable se reciba un rechazo por parte de los empleados y la gerencia, pero es la única acción segura para ayudar a prevenir este ataque.

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

Webinar Gratuito
Dispositivos Móviles

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

Febrero 2019