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

Webinar Gratuito

Sistemas de Comunicación y Mensajería

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 a las vulnerabilidades en sistemas de mensajería
- Reconocer y contabilizar ataques de correo electrónico
- Bombas de correo electrónico
- Banners
- Ataques SMTP
- Mejores prácticas para minimizar los riesgos en seguridad de correo electrónicos
- Entender voz sobre IP
- Vulnerabilidades VoIP
- Medidas correctivas contra vulnerabilidades VoIP

Introducción

Los sistemas de comunicación como correos electrónicos y Voz sobre IP (VoIP) frecuentemente crean vulnerabilidades, las cuales son pasadas por alto por las personas. ¿Porqué?.

El software de mensajería, ya sea a nivel del servidor y el cliente, es vulnerable porque los administradores de la red, frecuentemente creen los firewalls y software antivirus, es lo necesario para mantenerse alejado de los problemas, o simplemente olvidan asegurar los sistemas.

Introducción a las vulnerabilidades en sistemas de mensajería

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

Muchos ataques contra los sistemas de mensajería son sólo pequeñas molestias; otros puedes infligir un serio daño a la información, y reputación de la organización. Los ataques contra los sistemas de mensajería incluyen:

- Transmitir malware
- Hacer caer los servidores
- Obtener control remoto de las estaciones de trabajo
- Capturar información mientras viaja a través de la red
- Examinar los mensajes de correo electrónico almacenadas en los servidores y estaciones de trabajo
- Obtener información sobre tendencias de mensajería mediante los archivos de log o un analizador de red, lo cual puede alertar a un atacante sobre las conversaciones entre personas y organizaciones
- Capturar y retransmitir conversaciones telefónicas
- Obtener información interna sobre la configuración de al red, como nombres de host y direcciones IP

Reconocer y contabilizar ataques de correo electrónico

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

Los ataques a continuación mencionados, explotan las vulnerabilidades de seguridad más comunes en correos electrónicos. Las buenas noticias es la factibilidad de eliminar o minimizar muchas de estas, hasta el punto de la información no esté en riesgo.

Algunos de estos ataques requieren un conocimiento básico sobre metodologías de Hacking; obtener información pública, escanear y enumerar los sistemas, además de encontrar y explotar las vulnerabilidades. Otros pueden ser realizados enviando mensajes de correo electrónico o capturando tráfico.

Bombas de correo electrónico

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

Los ataques bomba de correo electrónico crean una condición de negación de servicio (DoS), contra el software de correo electrónico, e incluso la red y conexión a Internet, tomando una gran cantidad de ancho de banda, y algunas veces, requiriendo grandes cantidades de espacio de almacenamiento. Las bombas de correo electrónico pueden hacer caer el servicios, y proporcionar acceso no autorizado como administrador, y sí, incluso con las capacidades casi ilimitadas de almacenamiento actual.

Adjuntos

El servidor de correo electrónico puede ser impactado por una interrupción completa del servicio con, sobrecarga de la capacidad de almacenamiento, bloqueo de ancho de banda.

Conexiones

Un ataque utilizando una inundación de correos electrónicos se realiza en ataques de spam y otros intentos de DoS.

Banners

Cuando se ataca un servidor de correo electrónico de una empresa, un atacante primero realiza una captura básica del baner, para ver aquello factible de ser descubierto, como el software del servidor de correo en funcionamiento. Esta es una de las pruebas más críticas para encontrar lo conocido por el mundo sobre los servidores SMTP, POP3 y IMAP

Obtener información

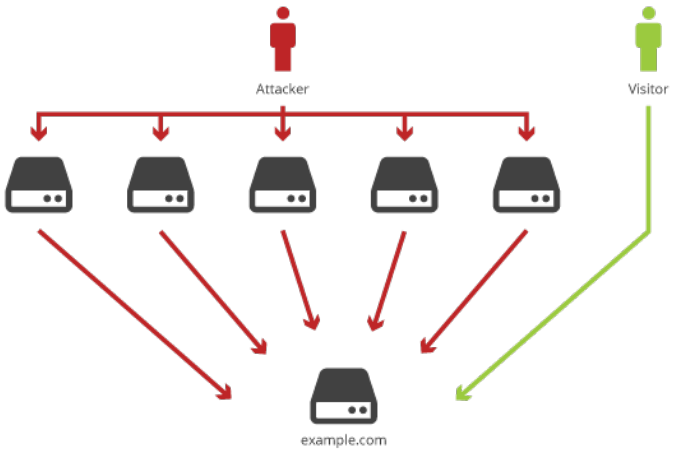
El tipo de software y versión del servidor son frecuentemente muy obvios, y proporcionan al atacante algunas ideas sobre posibles ataques, especialmente si se busca en una base de datos de vulnerabilidades conocidas.

Menciona también el banner de los servidores de correo electrónico puede ser cambiado por el administrador, para ocultar o exponer información incorrecta sobre la versión del servidor.

Ataques SMTP

Algunos ataques explotan debilidades en SMTP. Este protocolo de comunicación de corro electrónico; el cual data de hace tres décadas, fue diseñado para funcionalidad no la seguridad.

- Enumeración de cuentas
- Retransmisión
- Exposición de cabeceras del correo
- Capturar tráfico
- Malware



* https://www.tamos.com/products/nettools/?route=information/freeproduct&information_id=13
* https://github.com/laramies/theHarvester
* https://www.vandyke.com/products/securecrt/index.html
* https://www.monkey.org/~dugsong/dsniff/
* http://www.oxid.it/cain.html

Mejores prácticas para minimizar los riesgos en correo electrónicos

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

Soluciones software

- Usar software antimalware en el servidor de correo
- Aplicar los últimos parches de seguridad en el SO y servidor web
- Encriptar (donde sea razonable)
- Políticas para los usuarios no abran correos sospechosos ni adjuntos
- Plan para los usuarios quienes ignoren u olviden las políticas

Directrices de operación

- Poner los servidores de correo detrás de un firewall sobre un segmento diferente de Internet y de la LAN interna (DMZ)
- Fortalecer deshabilitando protocolos y servicios en el servidor
- Ejecutar escaneos de malware sobre los mensajes entrantes y salientes
- Registrar todas las transacciones con el servidor para investigación
- Para correo web, evaluar y asegurar adecuadamente el servidor web
- Requerir contraseñas fuertes

Entender voz sobre IP

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

Una tecnología ampliamente utilizada actualmente en las empresas es Voz sobre IP (VoIP). Ya sea se trate de sistemas VoIP internos o sistemas para usuarios remotos, los servidores VoIP, teléfono ligeros, y otros componentes relacionados tienen su propio conjunto de vulnerabilidades en seguridad.

Como la mayoría de las cosas relacionadas a la seguridad, muchas personas no han pensado sobre los problemas de seguridad, rodeando las conversación de voz atravesando las redes o Internet, pero ciertamente esto debe ser detectado. No debe de preocuparse, pues no es demasiado tarde para arreglar las cosas. Solo recordar, sin embargo, incluso se apliquen medidas de protección, los sistemas de VoIP necesitan ser incluidos como parte de las pruebas de seguridad global de manera continua.

Vulnerabilidades VoIP

Como con cualquier tecnología o conjunto de protocolos de red, los atacantes maliciosos están siempre tratando de figurar como romperlo. VoIP ciertamente no es diferente. De hecho dado el hecho tratarse de conversaciones telefónicas y disponibilidad del sistema, hay mucho por perder. Estos sistemas tienen vulnerabilidades similares a otros sistemas.

- Configuración por defecto
- Parches ausentes
- Contraseñas débiles

- Escanear por vulnerabilidades
- Capturar y grabar tráfico del tráfico de voz

* https://www.rapid7.com/products/nexpose/
* https://www.netsparker.com/
* http://www.oxid.it/cain.html
* https://www.voip-info.org/sipsak
* http://www.voipsa.org/Resources/tools.php

Medidas correctivas contra vulnerabilidades VoIP

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

Bloquear VoIP puede ser complicado. Sin embargo se puede comenzar bien, segmentando la red de voz dentro de una VLAN, o incluso una red física dedicada si se ajusta al presupuesto.

Aislar cualquier sistema conectado hacia Internet, de tal manera no todos puedan conectarse a esta. También se debe asegurar todos los sistemas relacionados a VoIP se refuerzan según las recomendaciones del proveedor, y prácticas ampliamente aceptadas, como la NIST SP800-58, ademas el software y el firmware son parchados en periodos regulares y consistentes.

* https://csrc.nist.gov/publications/detail/sp/800-58/final

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

Webinar Gratuito

Sistemas de Comunicación y Mensajería

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