MITSUBISHI ELECTRIC CORPORATION
PUBLIC RELATIONS DIVISION
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokio 100-8310 (Japón)

PARA SU PUBLICACIÓN INMEDIATA **N.º 3649**

Para su comodidad, le ofrecemos la traducción de la versión oficial en inglés de este comunicado de prensa únicamente a modo de referencia. Si desea conocer más detalles, consulte el texto original en inglés. En caso de que ambas versiones difieran, prevalecerá el contenido de la versión en inglés.

Consultas de los clientes

Information Technology R&D Center
Mitsubishi Electric Corporation

www.MitsubishiElectric.com/ssl/contact/company/rd/form.html

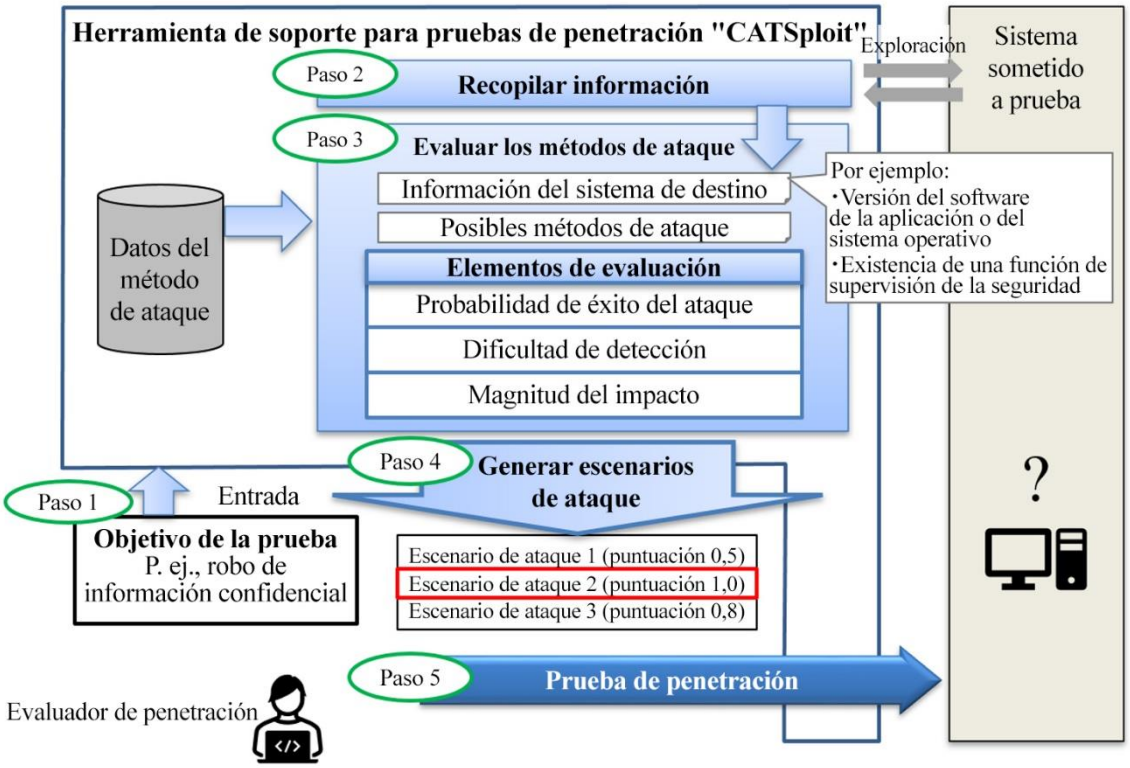
Consultas de los medios

Public Relations Division
Mitsubishi Electric Corporation

prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric desarrolla la primera herramienta del mundo de soporte para pruebas de penetración que genera escenarios de ataque desde la perspectiva de los piratas informáticos

Se espera que mejore la resistencia a los ciberataques de todos los productos conectados a redes



Ejemplo de uso de la herramienta de soporte durante las pruebas de penetración

TOKIO, 5 de diciembre de 2023 – Mitsubishi Electric Corporation (TOKIO: 6503) ha anunciado hoy el desarrollo de la primera[1] herramienta del mundo de soporte para pruebas de penetración[2], CATSploit, que genera automáticamente escenarios de ataque basados en los objetivos de las pruebas de un especialista en pruebas de penetración, como el robo de información confidencial, para evaluar la eficacia de los ataques de prueba. Utilizando los escenarios de ataque y los resultados de las pruebas resultantes (puntuaciones), incluso los ingenieros de seguridad sin experiencia pueden realizar fácilmente pruebas de penetración.

En los últimos años, los sistemas de control, incluidas las infraestructuras, los equipos de las fábricas, etc., están cada vez más conectados a las redes, lo que aumenta el riesgo de interrupciones, como cortes de electricidad o paradas del transporte público, debido a ciberataques. La necesidad de aplicar medidas de seguridad en esos sistemas se ha vuelto urgente. Además, las normas ISA/IEC 624433[3] exigen que se realicen pruebas fuzzing[4] de seguridad (pruebas de exploración de vulnerabilidades mediante datos aleatorios) y de penetración en los sistemas y equipos para evaluar su resistencia a los ciberataques, incluidas las vulnerabilidades debidas a errores de implementación o configuración. Las pruebas de penetración son muy sofisticadas y requieren la participación de hackers de sombrero blanco[5] para atacar realmente el sistema o producto que se está probando, pero estas personas, que deben poseer niveles muy altos de conocimientos, son escasas y difíciles de encontrar.

Mitsubishi Electric, centrándose en los factores que los hackers de sombrero blanco tienen en cuenta a la hora de seleccionar sus vectores de ataque, ha desarrollado ahora una herramienta de soporte para pruebas de penetración que genera listas de posibles escenarios de ataque y su eficacia (expresada en forma de puntuaciones numéricas).

Los detalles de la herramienta se presentarán el 6 de diciembre (11:00 h, hora local) durante la Black Hat Europe 2023 Arsenal de Londres, que tendrá lugar los días 6 y 7 de diciembre.

Características

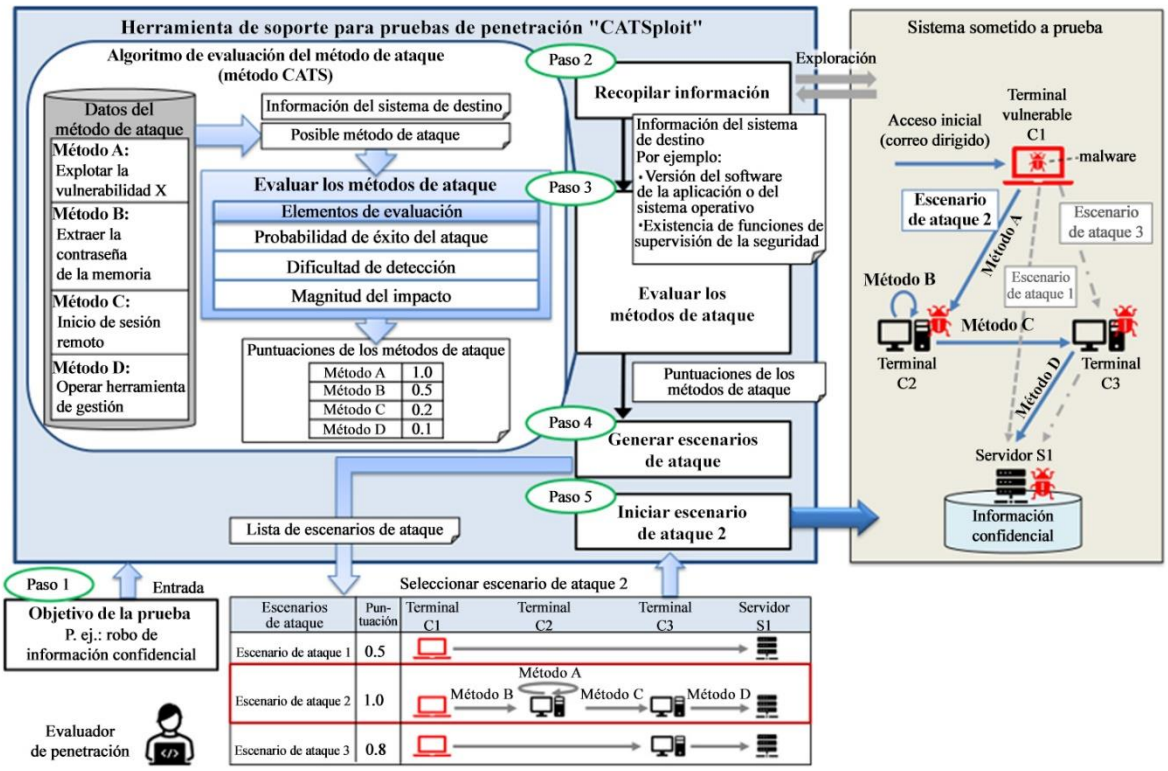
1) Genera automáticamente escenarios de ataque desde la perspectiva del hacker de sombrero blanco

- Mitsubishi Electric se centró en los factores que los hackers de sombrero blanco tienen en cuenta a la hora de elegir sus métodos de ataque, como la probabilidad de éxito del ataque, la dificultad de detección y la magnitud del impacto. Al ajustar los objetivos para pruebas específicas, el sistema es capaz de generar automáticamente escenarios que muestran los pasos necesarios para implementar un ataque con el fin de alcanzar dichos objetivos.

[1] Según el estudio realizado por Mitsubishi Electric, a fecha de 5 de diciembre de 2023
[2] Prueba para confirmar si un sistema o equipo puede verse comprometido por un ataque real
[3] Normas de seguridad para sistemas de control industrial
[4] Método de prueba para detectar defectos o vulnerabilidades del software mediante la introducción de datos no válidos o incorrectos
[5] Hackers éticos que utilizan conocimientos avanzados y tecnología informática para identificar problemas de seguridad, etc.

2) ***Las pruebas óptimas evalúan la eficacia de los escenarios de ataque desde la perspectiva de un hacker de sombrero blanco***

- El método CATS[6], propiedad de Mitsubishi Electric, calcula la eficacia de cada método de ataque (expresada como una puntuación numérica) desde la perspectiva de un hacker de sombrero blanco, a partir de la cual se propone una lista de escenarios de ataque para poder seleccionar el escenario más eficaz (puntuación más alta).
- La evaluación CATS tiene en cuenta no solo la información conocida del sistema, como el sistema operativo, la versión de la aplicación y los dispositivos de supervisión de la seguridad, sino también la información que falta del sistema, lo que ayuda a realizar escenarios de ataque que reproducen fielmente el punto de vista de un atacante real.
- La evaluación automatizada de escenarios de ataque susceptibles de ser utilizados por hackers de sombrero blanco permite a los ingenieros de seguridad menos experimentados realizar pruebas de penetración con facilidad.



Herramienta de soporte para pruebas de penetración CATSploit

[6] Puntuación de técnicas de ciberataque: Método exclusivo de Mitsubishi Electric para evaluar la eficacia de los vectores de ataque

Desarrollo futuro

Para mejorar aún más la resistencia a los ciberataques de los sistemas y dispositivos desarrollados por Mitsubishi Electric, la empresa continuará investigando y desarrollando esta nueva herramienta con el objetivo de utilizarla para las pruebas de seguridad reales de los productos de la empresa para 2026.

###

Acerca de Mitsubishi Electric Corporation

Con más de 100 años de experiencia en el suministro de productos fiables y de alta calidad, Mitsubishi Electric Corporation (TOKIO: 6503) es un líder mundial reconocido en la fabricación, comercialización y venta de equipos eléctricos y electrónicos utilizados en el procesamiento de la información y las comunicaciones, en el desarrollo espacial y las comunicaciones por satélite, en los aparatos electrónicos de consumo, en la tecnología industrial, en la energía, en el transporte y en los equipos de construcción. A través del espíritu "Changes for the Better", Mitsubishi Electric se esfuerza por enriquecer la sociedad con tecnología. La empresa registró unos ingresos por valor de 5003,6 mil millones de yenes (unos 37,3 mil millones de dólares estadounidenses*) en el ejercicio fiscal finalizado el 31 de marzo de 2023. Si desea obtener más información, visite www.MitsubishiElectric.com

*Las cantidades en dólares estadounidenses se han convertido a partir de yenes a un tipo de cambio de ¥134 = 1 dólar estadounidense, el tipo de cambio aproximado del mercado de divisas de Tokio a 31 de marzo de 2023