Endpoint Detection and Response by Moving Target Defense Techniques.

Trabajo terminal No. 2023-A067

Alumno: Delgado Alarcón Alan Ignacio
Directores: Aguirre Anaya Eleazar, Cortez Duarte Nidia Asunción
e-mail: adelgadoa1700@alumno.ipn.mx

Resumen – En este trabajo terminal se realizará el diseño de una estrategia para un control de seguridad bajo el paradigma de Defensa de Blanco con base en Movimiento (MTD - Moving Target Defense) para protección de sistemas Terminales (Endpoints, termino usado de facto). Esta estrategia se diseñará con la integración de las técnicas para el control y la aplicación de algoritmos de Transición suave (Soft Handover).

Dentro de las investigaciones de MTD [13], uno de los problemas reportados es el tiempo de inactividad o interrupción que presenta un sistema durante el proceso de movimiento. Para resolver este problema, se propone integrar un algoritmo de transición suave, que se basa en la iniciación de la siguiente conexión antes de romper la conexión actual, proporcionando tiempos de no disponibilidad teóricos cercanos o iguales a cero durante la ejecución de un movimiento.

Para la integración, pruebas del control de seguridad, y con el fin de considerar las condiciones de un entorno de producción real, se diseñarán varios experimentos y casos de aplicación. Así se podrán obtener resultados que permitan evaluar el funcionamiento del control de seguridad en condiciones cercanas a ambientes productivos.

Palabras clave – Cybersecurity, Moving Target Defense, Operating Systems Security, Handover Techniques.

1. Introducción

Un control de seguridad es un mecanismo diseñado para abordar las necesidades específicas por un conjunto de requisitos de seguridad [1]. Este se integra por controles de gestión, de operación y técnicos definidos para un sistema, que protegen la confidencialidad, integridad y la disponibilidad del sistema, sus componentes, procesos y datos [2].

La técnica de Defensa de Blanco con base en Movimiento (MTD – Moving Target Defense) es el concepto de diseñar, planear y controlar el cambio a través de múltiples dimensiones de un sistema, con el objetivo de aumentar la incertidumbre y la complejidad aparente de los ataques, disminuir la superficie de oportunidad e incrementar los costos en los esfuerzos de un ataque [3].

Un Equipo Terminal de circuito de Datos (EDT – Equipment Data circuit Terminal utilizado frecuentemente como Endpoint) es aquel dispositivo final, que comparte datos en una red. Los dispositivos más comunes que se asocian a este término son computadoras, laptops, teléfonos inteligentes, servidores, sistemas basados en nube [4], dispositivos del Internet de las Cosas (IoT – Internet of Things), sensores, etc. Los EDT se caracterizan porque contienen datos, almacenan credenciales de cuentas de usuario, y enlaces a otros sistemas en la red [4].

La Detección y Respuesta en Endpoint (EDR – Endpoint Detection and Response) es un sistema formado por distintas herramientas que realizan un análisis en los comportamientos de los eventos en EDT para identificar comportamientos potencialmente maliciosos. Puede generar respuestas en los EDT afectados, priorizar los riesgos y proporcionar guías de remediación personalizadas [14].

Las técnicas de Transición (Handover o Handoff techniques) en redes móviles, se definen como el proceso de transferir una llamada de voz o una sesión de datos de un nodo inalámbrico (Wireless) a otro. El objetivo principal es, mantener la continuidad de la sesión desde un punto de vista de aplicaciones, mientras se acepta un pequeño periodo de corte en la conexión física [15].

Las técnicas de MTD propuestas hasta el momento buscan hacer a un sistema dinámico, menos determinista e impredecible frente a ciberataques al cambiar continuamente la superficie de ataque. Al momento se han publicado numerosos trabajos relacionados los cuales involucran varias facetas de MTD [5], enfocadas en aplicaciones como redes de computadoras, IoT, Redes Definidas por Software (SDN – Software Define Networking), aplicaciones de software (servicios web, aplicaciones en dispositivos móviles), redes eléctricas y radares. También se cuenta con modelos para la evaluación del desempeño, y efectos tanto económicos como en la seguridad de las técnicas de MTD [6].

Sin embargo, todavía faltan análisis e investigaciones que aborden el área de los EDR utilizando MTD. Dentro de estas investigaciones y modelos, los acercamientos se centran en los entornos de rotación de sistemas operativos, diversificación de máquinas virtuales, aleatoriedad en servidores web, propuestas empíricas, entre algunos otros. Por lo que, al momento, no hay modelos, prototipos o propuestas enfocadas en los controles de seguridad para EDR utilizando técnicas de MTD.

Si bien el mecanismo de MTD es prometedor, actualmente hay poca investigación que demuestre que los sistemas MTD pueden funcionar de manera efectiva en ambientes de producción. Cuantificar los efectos de los MTD sobre la disponibilidad sigue siendo principalmente un problema abierto [12].

Dentro de los modelos reportados, uno de los obstáculos no triviales en la implementación de técnicas MTD es el cómo manejar la posible degradación del rendimiento (por ejemplo, interrupciones de la disponibilidad del servicio) y mantener una calidad de servicio (QoS – Quality of Service) aceptable en un sistema habilitado para MTD [7].

Derivado de lo anterior, este trabajo terminal se centrará en el desarrollo dedicado a la protección de los sistemas operativos en EDT. Esto por medio de la creación y diseño de una estrategia MTD y la integración de técnicas para un control de seguridad que aplique el paradigma de MTD en los EDT, especialmente en los sistemas operativos. Además de reducir el tiempo de no disponibilidad del servicio en los sistemas en cada movimiento (conjunto de nuevos parámetros o propiedades) que el control determine realizar para que sea cercano a cero, haciendo uso de técnicas y algoritmos de transición (Handover / Handoff).

2. Objetivo

Diseñar una estrategia para el movimiento de EDT en un control de seguridad preventivo EDR, integrando el paradigma de MTD y técnicas de Transición suave para minimizar la no disponibilidad durante el movimiento.

- Identificar la superficie de movimiento.
- Diseñar una estrategia de MTD aplicado al control de seguridad.
- Definir el caso de estudio para las pruebas del modelo.

3. Justificación

La naturaleza estática en los sistemas tradicionales puede hacer que un sistema sea más propenso a sufrir de un ataque con resultados exitosos, ya que los atacantes tienen el tiempo suficiente para identificar los vectores de ataque potenciales, explotar vulnerabilidades y, en última instancia, obtener un acceso no autorizado en el sistema [6].

La defensa de blanco con base en movimiento (MTD) se ha convertido en uno de los temas que cambian el juego al proporcionar estrategias defensivas asincrónicas. A diferencia de las soluciones de seguridad tradicionales que se centraban en eliminar vulnerabilidades, MTD hace que un sistema sea dinámico e impredecible al cambiar continuamente la superficie de ataque para confundir [9].

Además, los ataques a menudo son dirigidos a los EDT, porque un EDT comprometido puede ser un punto de entrada que de otro modo sería segura. Una de las mayores amenazas a los EDT se deriva del hecho de que los EDT son la última línea de defensa [4].

Los EDT son difíciles de proteger en la configuración empresarial. Sin embargo, los especialistas encargados de proteger los sistemas EDT tiene que encontrar una manera de proteger estos dispositivos de los ataques y evitar que comprometan la red, actualmente se hace uso de tecnologías como Antivirus o los sistemas de Detección y Respuesta de Endpoint (EDR – Endpoint Detection and Response).

Sin embargo, al momento no hay ningún modelo, prototipo o investigación enfocada en los controles de seguridad para EDR utilizando técnicas de MTD.

Por estas razones, surge la necesidad de diseñar un control que ayude a los especialistas encargados de la seguridad dentro de los Centros de Operaciones de Seguridad (SOC – Security Operation Centre) a, ampliar las medidas preventivas en los sistemas e infraestructuras criticas dentro de la red como los EDT.

4. Productos o Resultados esperados

Productos

- Estrategia de movimiento de EDT por EDR.
- Proceso de la evaluación del control.

Resultados

- Reducir el tiempo de no disponibilidad en el movimiento
- Ampliar la superficie de movimiento de ETD para EDRs con movimiento de blanco a la reportada en el estado del arte.

5. Metodología

Derivado de la falta de propuestas para controles de EDR que apliquen el paradigma de MTD, modelos funcionales MTD en producción y resultados reportados sobre el rendimiento de estos mismos, es necesario realizar una investigación que sustente la propuesta de solución de este trabajo terminal.

La disponibilidad de los EDT se podrá mantener durante los movimientos que realice el control de seguridad EDR, si se integran en el mismo: la estrategia de movimiento diseñada y el algoritmo de transición suave que permitan minimizar el tiempo de no disponibilidad del EDT en tiempos cercanos a cero en cada movimiento que el control EDR realice.

Por eso, en este trabajo terminal se propone el uso del método científico y el método experimental para determinar los requisitos de diseño y las pruebas de funcionalidad que garanticen el cumplimiento de los objetivos que se plantean en este trabajo. Cada método aportará una visión que complementarán el proceso de investigación propuesto para este trabajo terminal.

El método científico reúne una serie de características que permiten la obtención de nuevo conocimiento científico. Es el único procedimiento que no pretende obtener resultados definitivos y que se extiende a todos los campos del saber.

Las etapas del método científico corresponden de manera general con las del proceso del pensamiento reflexivo, como son: 1) Definición y comprensión de una dificultad, 2) Búsqueda de una solución provisional, 3) Verificación de los resultados obtenidos, y 4) Diseño de un esquema mental en cuanto a situaciones futuras para las que la situación actual será pertinente [10].

Por otra parte, en el método con enfoque experimental se manipulan una o más variables de estudio, para controlar el aumento o disminución de esas variables y su efecto en las conductas observadas. Esto se lleva a cabo en condiciones rigurosamente controladas, con el fin de describir de qué modo o por qué causa se produce una situación o acontecimiento particular [11].

Para este trabajo terminal se definen las siguientes etapas en el método experimental:

1ra etapa	análisis y revisión del estado del arte
2da etapa	diseño de experimentos
3ra etapa	ejecución de experimentos
4ta etapa	análisis de resultados
5ta etapa	diseño de la estrategia de movimiento
6ta etapa	pruebas y análisis de resultados

6. Cronograma

Nombre del alumno: Delgado Alarcón Alan Ignacio

ACTIVIDAD	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN
Revisión del estado del arte en MTD y EDR											
Revisión del estado del arte sobre las superficies de movimiento reportadas											
Revisión de los algoritmos / técnicas de transición suave											
Identificación de la superficie de movimiento											
Definición de los casos de estudio para pruebas											
Selección de las técnicas de movimiento											
Diseño de experimentos											
Diseño del ambiente de experimentación											
Instalación, configuración y calibración de ambiente de experimentación											

Presentación de TT1											
Ejecución de los experimentos											
Análisis y discusión de los resultados											
Diseño de la estrategia de movimiento											
Desarrollo del prototipo de la estrategia											
Diseño del ambiente de pruebas											
Instalación, configuración y calibración de ambiente de pruebas											
Ejecución de pruebas con el control de seguridad											
Análisis de resultados											
Presentación de TT2											
Redacción del documento de TT											

7. Referencias

[1] "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach", NIST Special Publication 800-160, vol. 2, n.º 1, p. 67, diciembre de 2021. Accedido el 18 de abril de 2022. [En línea]. Disponible: https://doi.org/10.6028/NIST.SP.800-160v2r1

[2] "Cybersecurity Framework Manufacturing Profile" NISTIR 8183. Septiembre 2017. Accedido el 26 de abril de 2022. [En línea]. Disponible: https://doi.org/10.6028/NIST.IR.8183

[3] National Institute Standards and Technology. "Moving target defense - Glossary | CSRC". NIST Computer Security Resource Center | CSRC. https://csrc.nist.gov/glossary/term/moving_target_defense (accedido el 19 de abril de 2022).

[4] Bromiley, M. (18 abril de 2022). 2022 SANS Protects: The Endpoint. SANS Institute. https://www.sans.org/white-papers/2022-sans-protects-endpoint/

[5] Cho, J.H., Sharma, D.P., Alavizadeh, H., Yoon, S., Ben-Asher, N., Moore, T.J., Kim, D.S., Lim, H., Nelson, F.F.: Toward proactive, adaptive defense: A survey on moving target defense. IEEE Communications Surveys & Tutorials 22(1), 709–745 (2020)

[6] H. Alavizadeh, S. Aref, D. S. Kim y J. Jang-Jaccard, "Evaluating the Security and Economic Effects of Moving Target Defense Techniques on the Cloud", en IEEE Transactions on Emerging Topics in Computing, doi: 10.1109/TETC.2022.3155272.

[7] D. S. Kim, M. Kim, J. -H. Cho, H. Lim, T. J. Moore y F. F. Nelson, "Design and Performance Analysis of Software Defined Networking Based Web Services Adopting Moving Target Defense", 2020 50th

Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S), 2020, pp. 43-44, doi: 10.1109/DSN-S50200.2020.00024.

[8] M. Carvalho y R. Ford, "Moving-Target Defenses for Computer Networks", en IEEE Security & Privacy, vol. 12, no. 2, pp. 73-76, Mar.-Apr. 2014, doi: 10.1109/MSP.2014.30.

[9] H. Alavizadeh, J. Jang-Jaccard y D. S. Kim, "Evaluation for Combination of Shuffle and Diversity on Moving Target Defense Strategy for Cloud Computing", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2018, pp. 573-578, doi: 10.1109/TrustCom/BigDataSE.2018.00087.

[10] Asensi-Artiga V, Parra-Pujante A. El método científico y la nueva filosofía de la ciencia. An. Documentación. https://revistas.um.es/analesdoc/article/view/2251. (accedido 20 de abril de 2022)

[11] A. Marradi, "Método experimental, método de la asociación y otros caminos de la ciencia", Paradigmas: Una Revista Disciplinar de Investigación, vol. 5, n.º 1, 2013, art. n.º 1.

[12] Warren Connell, Luan Huy Pham, and Samuel Philip. Analysis of Concurrent Moving Target Defenses. In Proceedings of the 5th ACM Workshop on Moving Target Defense MTD '18). Association for Computing Machinery, New York, NY, USA, 21–30. 2018. DOI: https://doi.org/10.1145/3268966.3268972. (accedido 20 de abril de 2022)

[13] Cai, G.-l., Wang, B.-s., Hu, W. y Wang, T.-z. (2016). Moving target defense: state of the art and characteristics. Frontiers of Information Technology & Electronic Engineering, 17(11), 1122–1153. https://doi.org/10.1631/fitee.1601321

[14] "Securing Picture Archiving and Communication System (PACS): Cybersecurity for the Healthcare Sector", NIST Special Publication 1800-24A, vol. A, n.º 1, p. 180, diciembre de 2020. Accedido el 29 de abril de 2022. [En línea]. Disponible: https://doi.org/10.6028/NIST.SP.1800-24

[15] S. Kuklinski, Y. Li, and K. T. Dinh, “Handover management in SDN-based mobile networks,” 2014 IEEE Globecom Workshops, GC Wkshps 2014, no. March, pp. 194–200, 2014, Accedido el 29 de abril de 2022. doi: 10.1109/GLOCOMW.2014.7063430

8. Alumno y Directores

CARÁCTER: Confidencial
FUNDAMENTO LEGAL: Artículo 11 Fracc. V y Artículos 108, 113 y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.
PARTES CONFIDENCIALES: Número de boleta y teléfono.

Delgado Alarcón Alan Ignacio — Alumno de la carrera de Ing. en Sistemas Computacionales en ESCOM, Boleta: 2018306041, Tel. 7791107378, email adelgadoa1700@alumno.ipn.mx

Firma:

Aguirre Anaya Eleazar. Dr. en Comunicaciones y Electrónica de la ESIME Culhuacán en 2012, M. en C. en Ingeniería en Microelectrónica en 2003, Ing. en Computación de la ESIME Culhuacán en 2000, Profesor Investigador y jefe del laboratorio de Ciberseguridad del CIC/IPN. Áreas de Interés: Seguridad en redes, Seguridad en sistemas operativos, Forense digital, Pruebas intrusivas . Tel 57-29-6000 ext. 56607, email eaguirre@cic.ipn.mx.

Firma:

Cortez Duarte Nidia Asunción. Dra. en Educación de la UEM en 2021. Maestra en Ciencias en Computación CINVESTAV-IPN 2009. Ing. en Sistemas Computacionales de ESCOM, Profesora de ESCOM/IPN (Dpto. de Ingeniería en Sistemas Computacionales.). Áreas de Interés: criptografía, seguridad de información, hardware reconfigurable, aritmética computacional, diseño digital. Tel. 57-29-6000 ext. 52032, email ncortezd@ipn.mx.

Firma: