Diego Esteban Quintero Rey
Modelos estocásticos y simulación en computación y comunicaciones
ME01
Proyecto Final: Implementación de un enfoque basado en teoría de juegos para contrarrestar amenazas persistentes avanzadas

PROBLEMA

DESCRIPCIÓN

Implementación de un enfoque basado en teoría de juegos para contrarrestar amenazas persistentes avanzadas, de acuerdo con la propuesta expuesta en [1] por los autores Stefan Rass, Sandra König Y Stefan Schauer.

OBJETIVOS

Implementar la metodología propuesta en [1] y realizar el experimento que se presenta en la sección 9 de [1] para comprobar si se obtienen resultados similares.

Objetivos específicos:

- Implementar las funciones y componentes necesarios para realizar el experimento presentado en la sección 9 de [1], el cual no depende de la topología del sistema.
- Implementar las funciones y componentes necesarios para realizar experimentos que dependan de la topología del sistema.

JUSTIFICACIÓN

Las amenazas persistentes avanzadas (APTs) abarcan una variedad diversa de métodos de ataque, que van desde la ingeniería social hasta las explotaciones técnicas. La naturaleza variada y a menudo encubierta de las APTs plantea un desafío significativo para la seguridad práctica contemporánea del sistema. Esto se debe a que la información sobre los ataques, el estado actual del sistema o los motivos de los atacantes suele ser poco clara, incierta y, en ocasiones, completamente indisponible.

La teoría de juegos emerge como un marco natural para modelar el conflicto entre atacantes y defensores. Este estudio explora una clase generalizada de juegos de matriz como una herramienta para mitigar riesgos en la defensa contra amenazas persistentes avanzadas (APTs). A diferencia de la teoría de juegos y decisiones tradicional, nuestro modelo está diseñado específicamente para capturar y gestionar la completa incertidumbre inherente a las APTs. Esto incluye factores como desacuerdos entre evaluaciones de riesgos cualitativas de expertos, motivos adversarios desconocidos e incertidumbre sobre el estado actual del sistema (como la profundidad de la penetración del atacante en las capas protectoras del sistema).

En términos prácticos, los modelos de APT basados en la teoría de juegos pueden derivarse directamente de análisis de vulnerabilidad topológica, junto con evaluaciones de riesgos siguiendo estándares comunes como la familia ISO 31000. Teóricamente, estos modelos presentan propiedades distintas en comparación con los modelos clásicos de teoría de juegos. La solución técnica presentada en este trabajo puede tener significado independiente en el campo [1].

La creciente diversidad, conectividad y apertura de los sistemas de información actuales a menudo ofrecen a los ciberatacantes numerosas vías para infiltrarse en un sistema. Las medidas de seguridad actuales suelen depender de herramientas y técnicas semiautomáticas, como el análisis de vulnerabilidad topológica (TVA), para identificar y abordar vulnerabilidades. Sin embargo, este progreso se acompaña de la evolución simultánea y mejora de ataques relacionados. Las Amenazas

Persistentes Avanzadas (APTs) se adaptan naturalmente a la creciente diversidad de medidas de seguridad ejecutando ataques sigilosos y diversos, con el objetivo de permanecer "bajo el radar" hasta que el sistema objetivo haya sido infiltrado, infectado y sea vulnerable al ataque previsto. Las contramedidas pueden ser demasiado tarde para ser efectivas una vez que se detecta el ataque, ya que el daño ya ha ocurrido.

Mitigar las APTs a menudo no es solo cuestión de precauciones técnicas, sino también de combatir a un oponente invisible e influencias externas en el sistema, principalmente debido a que la APT permanece oculta. Por lo tanto, la efectividad de cualquier medida de seguridad depende del estado actual del sistema y de cuán avanzada haya llegado a ser la APT. El aspecto económico se vuelve particularmente desafiante e incierto, ya que cuantificar el rendimiento de las inversiones en seguridad es casi imposible teniendo en cuenta diversos factores fuera de la influencia del oficial de seguridad [1].

REFERENCIAS

[1] Rass S, König S, Schauer S (2017) Defending Against Advanced Persistent Threats Using Game-Theory. PLOS ONE 12(1): e0168675. https://doi.org/10.1371/journal.pone.0168675