UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

AUTORES:

Ing. Ángela Bermeo

Ing. Israel Nolivos

Ing. Juan Carlos Larenas

Ing. Saúl Alajo

TUTOR:

Ing. Ronie Stalin Martínez Gordon, Mtr.

ANÁLISIS COMPARATIVO DE HERRAMIENTAS SIEM OPEN SOURCE MEDIANTE TTPS DE RED TEAMING DE EVASION

QUITO – ECUADOR | 2024

Resumen

El proyecto de tesis aborda la creciente importancia de la seguridad informática en el contexto empresarial, en un mundo cada vez más dependiente de la tecnología y la conectividad. Se contextualiza el avance tecnológico desde la popularización de las computadoras en los años 70 hasta la era actual de la inteligencia artificial, destacando cómo las empresas han migrado hacia la digitalización de sus procesos y operaciones. Este progreso tecnológico ha provocado nuevas amenazas, especialmente en el ciberespacio, donde los ciberdelincuentes buscan acceder, manipular o dañar la información de las organizaciones con motivaciones económicas.

El resumen también hace referencia a la evolución de los ataques cibernéticos, desde los primeros virus informáticos hasta las técnicas más sofisticadas utilizadas por los hackers modernos. Se subraya la importancia de la seguridad de la red empresarial, que se ve constantemente expuesta a posibles amenazas debido a su conexión con la red pública global. Además, se menciona la relevancia histórica de los ciberataques en el contexto de la guerra fría, donde las potencias económicas utilizaron la ciberguerra como un medio para obtener ventajas estratégicas.

Para abordar estos desafíos, el proyecto propone la combinación de dos técnicas: TTPs (tácticas, técnicas y procedimientos) de Red Teaming y el uso de herramientas SIEM (Security Information and Event Management). Estas técnicas pretenden evaluar la seguridad de los sistemas informáticos empresariales y fortalecer sus defensas contra posibles ataques. Se discute cómo el Red Teaming permite identificar vulnerabilidades en la infraestructura tecnológica, mientras que las herramientas SIEM permiten detectar y prevenir actividades irregulares en tiempo real mediante la correlación de datos.

La revisión de la literatura se centra en estudios comparativos de herramientas SIEM de código abierto disponibles en el mercado, destacando sus características, fortalezas y limitaciones. Se mencionan herramientas como OSSIM, SPLUNK, WAZUH, que ofrecen diferentes enfoques para la gestión de eventos de seguridad y la detección de amenazas cibernéticas.

En resumen, el proyecto de tesis busca contribuir significativamente a la seguridad informática empresarial al proponer una estrategia integral que combine técnicas de evaluación de seguridad con herramientas avanzadas de gestión de eventos de seguridad. Esto permitirá a las organizaciones mantener sus sistemas seguros y cumplir con los estándares de calidad en términos de seguridad de la información.

Palabras Claves: Ciberataque, virus SIEM, herramienta, informática, atacante, víctima, máquina, hardware, software, interfaz.

Abstract

The thesis project addresses the growing importance of computer security in the business context, in a world increasingly dependent on technology and connectivity. The technological advance is contextualized from the popularization of computers in the 70s to the current era of artificial intelligence, highlighting how companies have migrated towards the digitalization of their processes and operations. This technological progress has caused new threats, especially in cyberspace, where cybercriminals seek to access, manipulate, or damage the information of organizations with economic motivations.

The summary also refers to the evolution of cyber-attacks, from the first computer viruses to the most sophisticated techniques used by modern hackers. The importance of the security of the corporate network is underlined, which is constantly exposed to potential threats due to its connection to the global public network. Furthermore, the historical relevance of cyberattacks is mentioned in the context of the Cold War, where economic powers used cyberwar as a means to obtain strategic advantages.

To address these challenges, the project proposes the combination of two techniques: Red Teaming TTPs (tactics, techniques and procedures) and the use of SIEM (Security Information and Event Management) tools. These techniques aim to evaluate the security of business computer systems and strengthen their defenses against possible attacks. It is discussed how Red Teaming makes it possible to identify vulnerabilities in the technological infrastructure, while SIEM tools make it possible to detect and prevent irregular activities in real time through data correlation.

The literature review focuses on comparative studies of open source SIEM tools available on the market, highlighting their characteristics, strengths and limitations. Tools such as OSSIM, SPLUNK and WAZUH are mentioned, offering different approaches to security event management and cyber threat detection.

In summary, the thesis project seeks to contribute significantly to enterprise cybersecurity by proposing a comprehensive strategy that combines security assessment techniques with advanced security event management tools. This will allow organizations to keep their systems secure and meet quality standards in terms of information security.