UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES: **L**ozano Carriel Miguel Angel.

Minga Lozano Adrián Alejandro.

Vizueta Aldaz Andrés Xavier.

Zuleta Cadena Jefferson Lenin.

Análisis, implementación y comparación de 3 herramientas SIEM (Splunk, Alien Voult OSSIM, Wazuh) dentro de un entorno controlado

QUITO – ECUADOR | 2024

RESUMEN

A lo largo de este proyecto se realizó la instalación, manipulación y comparación de tres herramientas SIEM (Splunk, Alien Voult Ossim, Wazuh), con el objetivo de someterlas a diferentes ataques y comparar sus rendimientos con diferentes indicadores, cabe recalcar que se levantaron entornos simulados dentro de máquinas virtuales en la cual los tres programadas trabajaban con arquitecturas similares para no afectar los indicadores.

La arquitectura que se desarrolló fue la de tres máquinas virtuales para cada herramienta, simulando un agente atacante, otro como un agente de servidor y por último un agente cliente. En cada caso el agente atacante trataba de atacar al cliente y mediante el agente servidor se monitoreaba todo el proceso de ataque.

Dentro de cada herramienta SIEM, se levantaron reglas de seguridad para evitar los intentos de ataques hacia el cliente.

Palabras claves: Splunk, Alien Voult Ossim, Wazuh, rendimiento, máquinas virtuales.

ABSTRACT

Throughout this project, the installation, manipulation and comparison of three SIEM tools (Splunk, Alien Voult Ossim, Wazuh) was carried out, with the aim of subjecting them to different attacks and comparing their performance with different indicators. It should be noted that environments were created. simulated within virtual machines in which the three programmed ones worked with similar architectures so as not to affect the indicators.

The architecture that was developed was three virtual machines for each tool, simulating an attacking agent, another as a server agent and finally a client agent. In each case the attacking agent tried to attack the client and the entire attack process was monitored through the server agent.

Within each SIEM tool, security rules were created to prevent attempted attacks on the client.

Keywords: Splunk, Alien Voult Ossim, Wazuh, performance, virtual machines.