UIDE
Powered by
Arizona State University

Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTOR: Ing. Carlos Alejandro Clavijo Salazar

Ing. Carlos Alfredo Solórzano Ramón

Ing. Jonathan Enrique Sanmartín Pangay

Ing. Roberto Andrés Castro Arreaga

TUTOR: Ing. Jaime Bladimir Ibarra Jiménez

Detección de ataques Informáticos mediante un SIEM Open Source Wazuh para los Servicios Digitales de la Banca Web.

QUITO – ECUADOR | 2024

RESUMEN

El presente proyecto consiste en detectar ataques informáticos a un servidor de banca web en línea con diversos hosts conectados en la misma red, para ello se creará un laboratorio, donde se instalará el servidor web, clientes, firewall y SIEM Wazuh. Este será el encargado de monitorear y notificar eventos y ataques comunes como denegación de servicio, inyección SQL, XSS, malware y fuerza bruta. Se analizará la eficacia de Wazuh ante diferentes ataques, su facilidad a la integración con otros componentes de seguridad (firewalls, antivirus, notificaciones). Se realizarán pruebas controladas para simular ataques, y se analizará la capacidad de Wazuh para detectar y alertar sobre estos incidentes, proporcionando información detallada sobre cada evento.

Además, se proporcionarán recomendaciones para optimizar el rendimiento de Wazuh y se analizará su escalabilidad para diferentes entornos de red. Este enfoque integral permitirá evaluar Wazuh como una solución SIEM, eficaz para mejorar la seguridad de una organización, emitiendo un informe sobre los ataques que han sido reconocidos y notificados por Wazuh.

ABSTRACT

The present project consists of detecting computer attacks on an online web banking server with various hosts connected to the same network. For this purpose, a laboratory will be created, where the web server, clients, firewall and Wazuh SIEM will be installed. This will be responsible for monitoring and reporting common events and attacks such as denial of service, SQL injection, XSS, malware and brute force. The effectiveness of Wazuh against different attacks and its ease of integration with other security components (firewalls, antivirus, notifications) will be analyzed. Controlled tests will be carried out to simulate attacks, and Wazuh's ability to detect and alert about these incidents will be analyzed, providing detailed information about each event.

Additionally, recommendations will be provided to optimize Wazuh's performance and its scalability for different network environments will be analyzed. This comprehensive approach will allow Wazuh to be evaluated as a SIEM solution, effective in improving the security of an organization, issuing a report on the attacks that have been recognized and reported by Wazuh.