UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

COMPARACIÓN DE SISTEMA DE DETECCIÓN DE INTRUSOS BASADOS EN CLIENTES (HIDS) PARA LA DETECCIÓN DE ATAQUES DOS EN SERVIDORES WEB.

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor(a) (es):

Bach. Ramírez Ramos Luis Robert

ORCID: https://orcid.org/0000-0002-5994-2700

Asesor(a):

Mg. Mejía Cabrera Heber Iván

ORCID: https://orcid.org/0000-0002-0007-0928

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú 2021

RESUMEN:

La motivación por la cual se realizó esta investigación, es debido a que actualmente estamos viviendo en una era tecnológicamente dependiente, tanto en nuestra vida cotidiana como en nuestros centros laborales, por ende el aumento de delincuentes cibernéticos a la par, nos conlleva a implementar mecanismos de seguridad que puedan detectar para mitigar un ataque a nuestros distintos servidores, en los cuales se almacenan todo tipo de información vulnerable e importante para una persona, empresa o un país entero.

Una de las tecnologías que ayudan en la lucha contra los ataques cibernéticos provocados por los hackers son los Sistemas de Detección de Intrusos (IDS), herramienta recientemente emergente contra la lucha de distintos ataques como los Ataques de Denegación de Servicios (DoS y DDoS), hacia nuestros equipos tecnológicos para robar o alterar información sensible para sus dueños.

La presente investigación tiene por título “COMPARACIÓN DE SISTEMA DE DETECCIÓN DE INTRUSOS BASADOS EN CLIENTES (HIDS) PARA LA DETECCIÓN DE ATAQUES DDOS EN SERVIDORES WEB”, cuya finalidad es emplear y comparar dos sistemas de detección de intrusos a nivel de host, los cuales son Open Source, en un servidor web para poder obtener como resultado cuál de los dos HIDS es más eficiente frente a este tipo de ciberataque llamado Denegación de Servicios.

La resultante de la investigación es la superioridad de IDS OSSEC WIZUH en comparación al IDS TRIPWIRE ENTERPRISE frente a ataques de Denegación de Servicios (DoS), dirigidos a un servidor web según las métricas mencionadas implementadas en este trabajo, OSSEC terminó el análisis 3 segundos más rápido que su contrincante TRIPWIRE.

La conclusión más relevante al que nos podemos referir es la gran importancia que tienen estos mecanismos de seguridad para poder detectar cuando nos están tratando de perjudicar en el ciberespacio, existen IDS más conocidos como Snort o Suricata, sin embargo, ya no son Open Source y requieren una gran cantidad de recursos para su implementación.

Palabras Clave: Ciberataque, Open Source, HIDS, Seguridad, Host, Servidores, Información Vulnerable, DDOS, Detectar, Mitigar.

ABSTRACT:

The motivation for which this research was carried out is due to the fact that we are currently living in a technologically dependent era, both in our daily lives and in our work centers, therefore the increase in cyber criminals at the same time leads us to implement mechanisms of security that it can detect to mitigate an attack on our different servers, in which all kinds of vulnerable and important information for a person, company or an entire country are stored.

One of the technologies that help in the fight against cyber-attacks caused by hackers is the Intrusion Detection Systems (IDS), a recently emerging tool against the fight against different attacks such as Denial of Service Attacks (DoS and DDoS), towards our technological equipment to steal or alter sensitive information for their owners.

This research is entitled "COMPARISON OF CLIENT-BASED INTRUDER DETECTION SYSTEM (HIDS) FOR DETECTING DDOS ATTACKS ON WEB SERVERS", whose purpose is to use and compare two host-level intrusion detection systems, which They Are Open Source, in a web server to be able to obtain as a result which of the two HIDS is more efficient against this type of cyberattack called Denial of Services.

The result of the investigation is the superiority of IDS OSSEC WIZUH compared to IDS TRIPWIRE ENTERPRISE against Denial of Service (DoS) attacks, directed at a web server according to the mentioned metrics implemented in this work, OSSEC began the analysis for 3 more seconds faster than his opponent TRIPWIRE.

The most relevant conclusion that we can refer to is the great importance of these security mechanisms to be able to detect when they are trying to harm us in cyberspace, there are better known IDS such as Snort or Suricata, however, they are no longer Open Source and it requires a large amount of resources for its implementation.

Keywords: Cyberattack, Open Source, HIDS, Security, Host, Servers, Vulnerable Information, DDOS, Detect, Mitigate.