UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

"Trabajo de grado previo a la obtención del Título de Ingeniero en Sistemas y Computación"

Título:

ESTUDIO DE TÉCNICAS Y HERRAMIENTAS PARA LA PREVENCIÓN Y DETECCIÓN DE INTRUSIONES A NIVEL DE APLICACIÓN EN LA RED DE DATOS DE LA UNACH

Autora:

Nelly Janeth Yuquilema Heredia

Directora:

Ing. Pamela Buñay

Riobamba – Ecuador

2016

Los miembros del Tribunal de Graduación del proyecto de investigación de título: **ESTUDIO DE TÉCNICAS Y HERRAMIENTAS PARA LA PREVENCIÓN Y DETECCIÓN DE INTRUSIONES A NIVEL DE APLICACIÓN EN LA RED DE DATOS DE LA UNACH**, presentado por: Nelly Janeth Yuquilema Heredia y dirigida por: Ing. Pamela Buñay.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en la cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

Ing. Fernando Molina

Presidente del Tribunal **Firma**

Ing. Pamela Buñay

Miembro del Tribunal **Firma**

Ing. Javier Haro

Miembro del Tribunal **Firma**

DERECHO DE AUTORÍA

La responsabilidad del contenido de este trabajo investigativo, corresponde exclusivamente a Nelly Autora Heredia y como director de tesis a Ing. Pamela Buñay. Los derechos de autoría pertenecen a la Universidad Nacional de Chimborazo.

Nelly Janeth Yuquilema Heredia

C.I: 060412256-4

AGRADECIMIENTO

Agradezco a Dios, por cada día de vida.

Agradezco a la Universidad Nacional de Chimborazo, a la Facultad de Ingeniería, escuela de Sistemas y Computación por el aporte en mi formación profesional.

De manera especial todos los profesores por su orientación.

A mi familia por siempre brindarme su apoyo y sobre todo un sentimiento de gratitud a mi abuelita Celina quien con amor y comprensión me ha acompañado en esta larga travesía.

DEDICATORIA

A mi familia.

A mi hermana.

DERECHO DE AUTORÍA iii
AGRADECIMIENTO iv
DEDICATORIA v
RESUMEN xii
SUMARY xiii
INTRODUCCIÓN 1

CAPÍTULO I

MARCO REFERENCIAL

1.1. TÍTULO DEL PROYECTO 2
1.2. PROBLEMATIZACIÓN 2
1.2.1. IDENTIFICACIÓN Y DESCRIPCIÓN DEL PROBLEMA 2
1.2.2. ANÁLISIS CRÍTICO 3
1.2.3. PROGNOSIS 3
1.2.4. DELIMITACIÓN 4
1.2.5. FORMULACIÓN DEL PROBLEMA 4
1.2.6. HIPÓTESIS 4
1.2.7. Identificación De Variables 4
1.3. OBJETIVOS 4
1.4. JUSTIFICACIÓN 5

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA

2.1. Introducción 7
2.2. Introducción a la seguridad de la información 7
2.3. Introducción a las intrusiones 8
2.3.1. Concepto de intrusiòn 8
2.3.2. Impacto de los intrusiones 9
2.3.3. Tipos de intrusiones 10
2.3.3.1. Sondas (vigilancia y exploración) 10
2.3.3.2. Denegación de servicio (denial of service) 10
2.3.3.3. Remotos a local (r2l) 14
2.3.3.4. Usuario como root (u2r) 14
2.3.4. Intrusiones desde de punto de vista de la procedencia 14
2.4. DETECCIÓN Y PREVENCIÓN DE INTRUSIONES 15

2.4.1. Sistemas para detección y prevención de intrusiones 16
2.4.2. Arquitectura de un IDPS 16
2.4.3. Técnicas de análisis de los IDPS 17
2.4.3.1. Uso indebido 17
2.4.3.2. Anomalías 18
2.4.4. IDPS según la localización del sensor 19
2.4.4.1 Tiempo real (in-line) 19
2.4.4.2 Fuera de tiempo (off-line) 19
2.4.5. SISTEMAS PARA LA DETECCIÓN PREVENCIÓN DE INTRUSIONES BASADOS EN RED (NIDPS) 20

CAPÍTULO III

ANÁLISIS DE LAS TECNICAS Y DESCRIPCIÓN DE HERRAMIENTAS nIDPS DE OPEN SOURCE

3.1. ESTUDIO DE LAS TÉCNICAS DE ANÁLISIS 22
3.1.1. Determinación y descripción de las técnicas a comparar 22
3.1.1.1 Técnica de análisis: uso indebido 22
3.1.1.2 Técnica de análisis: anomalías 23
3.1.2. Indicador de evaluación 23
3.1.3. Descripción del criterios de evaluación y sus parámetros 23
3.1.4. Ponderación de evaluación 25
3.1.5. Desarrollo comparativo 26
3.1.5.1. Desarrollo de evaluación del Indicador 1: características generales para definir técnicas de análisis 26
3.1.6. Resultados de la evaluación del Indicador 1 26
3.1.7. Selección del tipo de técnica 27
3.2. DESCRIPCIÓN DE HERRAMIENTAS PARA LA DETECCIÓN Y PREVENCIÓN 28
5.5.1. Determinación de las herramientas nIDPS open source a comparar 28
5.5.2. Descripción de las herramientas nIDPS open source 29
3.2.2.1 Snort 29
3.2.2.1.1 Arquitectura básica 30
3.2.2.1.2 Ventajas 32
3.2.2.1.3 Debilidades 32
3.2.2.2 Suricata 33
3.2.2.2.1 Características 34

3.2.2.2.2 Arquitectura básica 34
3.2.2.2.3 Ventajas 35
3.2.2.2.4 Debilidades 35

CAPÍTULO IV

ANÁLISIS DE REQUERIMIENTOS Y SITUACIÓN ACTUAL DE LA UNACH

4.1. Introducción 37
4.2. Situación actual de la UNACH 37
4.3. Topología lógica de la red 38
4.4. Descripción de la red de datos 39
4.5. Determinación de la ubicación del nIDPS 41
4.6. Requerimientos 42
4.6.1. Con respecto al hardware 42
4.6.2. Con respecto al sistema base 42
4.6.3. Con respecto a las interfaces de red 42
4.6.4. Con respecto a herramientas adicionales 43

CAPÍTULO V

METODOLOGÍA

5.1. TIPO DE ESTUDIO 45
5.1.1. Según el objeto de estudio 45
5.1.2. Según la fuente de investigación 45
5.1.3. Según las variables 45
5.2. POBLACIÓN Y MUESTRA 45
5.2.1. Población 45
5.2.2. Muestra 46
5.3. OPERACIONALIZACIÓN DE VARIABLES 46
5.3.1. Descripción de Indicadores 47
5.4. PROCEDIMIENTOS 48
5.4.1. Fuentes de información 48
5.4.2. Técnicas de investigación 48
5.4.3. Instrumentos 49
5.4.4. Procedimientos de la información 50
5.4.4.1. Creación de un ambiente de pruebas 50
5.4.4.2. Recolección de información. 57
5.5. PROCESAMIENTO Y ANÁLISIS 59

5.5.1. Procesamiento y análisis de los indicadores de la variable independiente 59
5.5.1.1. Indicador 1: Funciones 60
5.5.1.2. Resultados generales de la evaluación Funciones 66
5.5.1.3. Indicador 3: Desempeño 67
5.5.1.4. Indicador 2: Seguridad 68
5.5.2. Procesamiento y análisis del indicador de la variable dependiente 79
Primer ambiente: con fuente de datos trafico de la red UNACH 80
5.5.2.1.1. Interpretacion de alertas activadas 83
CAPÍTULO VI
RESULTADOS Y DISCUSIÓN
6.1. RESULTADOS 91
6.1.1. Análisis de los resultados obtenidos 91
6.1.2. Comprobación de la hipótesis 95
6.2. DISCUSIÓN 102
CAPITULO VII
CONCLUSIONES Y RECOMENDACIONES
7.1. CONCLUSIONES 104
7.2. RECOMENDACIONES 107
CAPÍTULO VIII
PROPUESTA
8.1. Tilulo de la propuesta 108
8.2. Introduccion 108
10. ANEXOS 115
10.1. Tabla de índices T-student 115
10.2. Alertas de intrusiones visualizadas mediante Sguil 115
10.3. Soporte Geo IP de Snort mediante Squert 116
10.2. Guìa 116

ÍNDICE DE FIGURAS

Figura I: Taxonomía de denegación de servicio *11*
Figura II: Ataque SynFlood *12*
Figura III: Arquitectura básica de IDS/IPS *17*
Figura IV: Resultados de la evaluación para el criterio1 ..... *27*
Figura V: IDS actuales *28*
Figura VI: Logo Snort 2.9.8 ..... *29*
Figura VII: Componentes de Snort *31*
Figura VIII: Logo Suricata *33*
Figura IX: Componentes de Suricata *35*
Figura X: Esquema general de la UNACH *38*
Figura XI: Funcionamiento básico de DNS *39*
Figura XII: Ataques de reconocimiento externo al servidor DNS de la UNACH utilizando sitios web *40*
Figura XIII: Ataque de reconocimiento externo al servidor HTTP e la UNCH utilizado Nikto *40*
Figura XIV: Configuración del puente (bridge) en el dispositivo dedicado al IDPS *43*
Figura XV: Esquema lógico del escenario de simulación *51*
Figura XVI: Reglas en el Firewall *54*
Figura XVII: Archivo de configuración named.conf *54*
Figura XVIII: Archivo de configuración named.conf *55*
Figura XIX: Componentes de los dispositivos nIDPS en el escenario de simulación *55*
Figura XX: Reporte Endpoints del trafico capurado utilizando NetworkMiner *59*
Figura XXI: Reporte Endpoints por protocolo UDP del trafico capurado utilizando Wireshark *59*
Figura XXII: Posibilidad de detección de ataques *69*
Figura XXIII: Escaneo con detección de servicios utilizando nmap *70*
Figura XXIV: Análisis del comportamiento capturado utilizando Wireshark *70*
Figura XXV: Ejecución del ataque Nikto *71*
Figura XXVI: Alertas generadas por el nIDPS Suricata *72*
Figura XXVII: Alertas generadas y filtradas por el nIDPS *73*
Figura XXVIII: Ejecución del ataque de inundación al puerto DNS utilizando Hping3 ..... *76*
Figura XXIX: Comportamiento de la red durante el ataque de inundciòn al puerto53 utilizando Hping3 ..... *76*
Figura XXX: Alertas generadas por el nIDPS Suricata y Snort para el ataque de Inundación con Hping3 ..... *77*
Figura XXXI: Funcionamiento de Barnyard2 con Suricata *81*
Figura XXXII: Funcionamiento de Snorby con el nIDPS Suiricata *82*
Figura XXXIII: Funcionamiento de Barnyard2 con Snort *82*
Figura XXXIV: Análisis de peticiones DNS en el trafico capturado utilizando Wireshark *85*
Figura XXXV: Análisis de peticiones DNS no sospechosas en el trafico capturado utilizando Network Miner *85*
Figura XXIX: Análisis de peticiones HTTP en el trafico capturado utilizando Wireshark *88*
Figura XXXVII: Resumen evaluaciòn del indicador 1 ..... *91*
Figura XXXVIII: Distribuciòn del total de intrusiones detectas de acuerdo a los 3 archivos capturados *94*

INDICE DE TABLAS

Tabla 1: Comparación ventajas e inconvenientes de las técnica de análisis Uso indebido-Anomalías 24
Tabla 2: Tabla poderación de evaluación para técnicas de analisis 25
Tabla 3: Evaluación del criterio1 para técnicas de uso indebido y anomalías 26
Tabla 4: Promedio de evaluación del Indicador 1: Características generales para definir el uso de técnicas de análisis 26
Tabla 5: FODA Técnica de Uso indebido 27
Tabla 6: Operacionalizaciòn de variables 47
Tabla 7: Especificacion general del escenario de pruebas utilizando Virtual Box 51
Tabla 8: Descripciòn de las sistemas virutalizados 53
Tabla 9: Tabla de ponderación de evaluación 60
Tabla 10: Resumen de evaluación general- herramientas nIDPS 66
Tabla 11: Resumen de evaluación Desempeño 68
Tabla 11: Descripciòn de intrusiones detectadas en el ambiente de pruebas para ataque DOS y Monitorizaciòn 77
Tabla 13: Intrusiones detectadas con Suricata en el primer escenario 81
Tabla 14: Intrusiones detectadas con Snort en el primer escenario 82
Tabla 21: Descripciòn de intrusiones detectadas en la red de datos institucional 89
Tabla 16: Descripciòn de evaluaciòn del indicador 2 92
Tabla 17: Resumen evaluaciòn del indicador 2 93
Tabla 18: Resumen evaluaciòn del indicador 2 93
Tabla 19: Cantidad total de intrusiones detectas por Snort y Suricata 93
Tabla 20: Cantidad de intrusiones detectas por Snort y Suricata contanto los VP y FP 94
Tabla 21: Datos numèrico para el indicador 1 95
Tabla 22: Datos numèrico para el indicador 2 97
Tabla 21: Tabla resumen de la cantidad intrusiones VP detectados con Snort y Suricata 99

RESUMEN

El presente documento detalla la investigación de las herramientas software open source más usuales dedicados a la prevención y detección de intrusiones a nivel de red (nIDPS) con el objetivo de proponer una solución alternativa de seguridad para de la red de servidores de la Universidad Nacional de Chimborazo "UNACH".

El estudio de los nIDPS open source que monitoricen los eventos de red en busca de patrones característicos de ataques y atenúen las consecuencias, permite detectar y prevenir intrusiones o intentos de intrusiones que atenten a la disponibilidad de servicio.

El parámetro evaluado es el número de intrusiones detectadas con la herramienta Snort y Suricata utilizando la técnica de análisis de uso indebido.

.

UNIVERSIDAD NACIONAL DE CHIMBORAZO

FACULTAD DE INGENIERIA

CENTRO DE IDIOMAS

Lcda. Ruth Molina 14 de Marzo del 2016

SUMARY

This document details the research of the tools software open source most common dedicated to the prevention and intrusion detection network level (nIDPS) with the aim of proposing an alternative security solution for network servers of the Universidad Nacional de Chimborazo "UNACH".

The study of open source nIDPS that monitor network events looking for characteristic patterns of attacks and mitigate the consequences, to detect and prevent intrusions or intrusion attempts that threaten to service availability.

The evaluated parameter is the number of detected intrusions with Snort and Suricata tool using the analysis technique misuse.

CENTRO DE IDIOMAS
COORDINACION

INTRODUCCIÓN

La continua evolución de nuevos métodos de ataques, nuevas formas de vulnerar sistemas, herramientas cada vez más sofisticadas de ataques logran eludir mecanismos tradicionales de seguridad implementados, las fallas de seguridad provenientes del interior de la red, facilitan la intrusión a los cada vez más habilidosos atacantes; por consiguiente prevenir tales ataques y/o posibles fallas en la administración de la red es un reto ambicioso.

La red institucional de la UNACH no está exento de potenciales ataques informáticos donde puede verse involucrado información sensible y/o recursos de red. Bajo la premisa de que ningún dispositivo es 100 % seguro es imperativo analizar mecanismos de seguridad complementarios a los ya bien conocidos mecanismos de seguridad tradicionales que proporcionen una línea de defensa profunda, actúen en etapas tempranas que permitan la monitorización, análisis, detección y respuesta ante comportamientos maliciosos. Los sistemas de prevención y detección de intrusiones se han convertido en una necesidad actual.

CAPÍTULO I

MARCO REFERENCIAL

1.1.TÍTULO DEL PROYECTO

Estudio de técnicas y herramientas para la prevención y detección de intrusiones a nivel de aplicación en la red de datos de la unach

1.2.PROBLEMATIZACIÓN

1.2.1. IDENTIFICACIÓN Y DESCRIPCIÓN DEL PROBLEMA

La Universidad Nacional de Chimborazo centraliza la gestión de su red institucional en el CTE (Centro de Tecnologías Educativas), el cual se encarga de los principales servicios informáticos, las tecnologías de la información y la comunicación. En el campus "Edison Riera" se encuentra el Data Center lugar físico de administración de la red.

Con el fin de proteger los servicios académicos institucionales de: sitios web, repositorio digital (DSPACE), B-Learning, correo institucional y sistemas de red informática, cuenta con una infraestructura física segura además de una arquitectura lógica con mecanismos de seguridad tradicionales.

Para la detección de intrusiones de ataques externos se emplea el firewall empresarial de Cisco ASA 5525 que a su vez tiene la funcionalidad de IDS permitiendo monitorizar eventos de red en tiempo real y para proteger de intrusiones internas utiliza mecanismos de autenticación de usuarios, mecanismos de listas de control de acceso (ACL), proxy, diferentes Vlans y VPNs.

A pesar de los mecanismos de seguridad implementados, se han registrado aunque no de manera concurrente, incidentes que atentan a la disponibilidad del sistema

de nombres de dominio (DNS), esto han provocado: interrupción de las actividades normales de manera parcial o total del servidor DNS y lentitud de navegación hacia internet.

El último incidente notable ocurrió en el cuarto trimestre del año 2015 en el que por ataques de denegación de servicio, el servidor DNS se mantuvo fuera de disponibilidad por aproximadamente 10 minutos.

1.2.2. ANÁLISIS CRÍTICO

Principalmente los ataques de denegación de servicio (DOS) se basan en el continuo descubrimiento de vulnerabilidades en los protocolos TCP/IP y servicios que las aprovechan, fallas de configuraciones de servidores y debilidades de los mecanismos de defensa desplegados en la red.

Si bien los ataques DOS, no son nuevos en el ámbito informático, la indisponibilidad que representa es crítico debido a la relación exposición de servicios de las entidades a internet.

1.2.3. PROGNOSIS

A través del presente estudio sobre técnicas y herramientas de detección y prevención de intrusiones, se podrá determinar una técnica de análisis adaptable a la red de datos de la UNACH que permita detectar patrones característicos de ataques de denegación de servicio más usuales, aportar mediante un estudio una herramienta alternativa de código libre que permita a los administradores de red supervisar, predecir el progreso de una intrusión y tomar medidas de prevención adecuadas en el momento oportuno, además elaborar una guía sobre las amenazas o ataques más comunes de denegación de servicio con el fin de mejorar su postura de seguridad.

1.2.4. DELIMITACIÓN

Las herramientas para la prevención y detección de intrusiones se restringen al estudio de herramientas software distribuidas bajo la licencia GLP que actúen como IDS e IPS basados en red.

Los ataques se restringen a la problemática actual de denegación de servicio al sistema de nombres de dominio (DNS) de la institución con direccionamiento IPV4.

En la estructura de lo posible se propone la implementación de un IDPS de código abierto como solución alternativa.

1.2.5. FORMULACIÓN DEL PROBLEMA

¿Cómo el estudio de herramientas open source nIDPS Snort y Suricata permitirá prevenir y detectar intrusiones a la red de datos de la UNACH?

1.2.6. HIPÓTESIS

La utilización de la herramienta nIDPS open source Suricata brinda mejores prestaciones que la herramienta nIDPS open source Snort para detectar y prevenir las intrusiones en la red de datos de la UNACH.

1.2.7. Identificación De Variables

Variable dependiente

- Herramientas nIDPS open source.

Variable independiente

- Detección y prevención de intrusiones en la red de datos de la UNACH.

1.3. OBJETIVOS

General

- Estudiar las técnicas y herramientas para la prevención y detección de intrusiones a nivel de aplicación en la red de datos de UNACH.

Específicos

- Determinar los ataques que ocurren frecuentemente en la red de Datos de la UNACH.
- Estudiar las herramientas nIDPS open source Snort y Suricata.
- Determinar las caracteristicas que permitirán identificar la mejor herramienta nIDPS open source.
- Establecer un escenario de simulación para ejecutar ataques.
- Elaborar una guía para la prevención y detección de intrusiones a nivel de aplicación en la red de datos.

1.4. JUSTIFICACIÓN

La seguridad de la información se ha convertido actualmente en un campo necesario-obligatorio para todo tipo de organización, donde la indiscutible necesidad de la interconectividad e interoperabilidad que exige el mundo digital actual requiere el uso de tecnologías que permitan compartir y transferir información, con ello, el desafío inevitable de proteger la misma.

Pese a los mecanismos de seguridad implementados en la UNACH, algunos incidentes o ataques a uno de los servicios críticos como el ofrecido por sistema de nombres de dominio (DNS) no logran ser eludidos proactivamente. Razón por la que se hace imperativo realizar una investigación sobre mecanismos complementarios-esenciales en una arquitectura de seguridad como son los sistemas de prevención y detección de intrusiones con el fin de incidir positivamente en la elección de estas herramientas y reforzar el nivel de seguridad actual de la institución.

Como existe una gran variedad de herramientas nIDPS en el mercado de la seguridad informática son objeto en el presente trabajo dos herramientas software open source. La empresa Cisco propone Snort, que es una herramienta madura muy potente, ampliamente documentada y eficiente en la detección correcta de distintas técnicas de evasión y malware. Open Source Information Security

Fundation (OISF) expone Suricata que constituye una herramienta que adopta características innovadoras de las técnicas de detección.

La creación de un escenario virtual permite efectuar el análisis experimental sobre las herramientas nIDPS, frente a los ataque DOS más habituales, previamente entendidos y modelados.

Finalmente se contribuye con una guía para la implementación de una herramienta nIDPS open source aplicado a la red de datos de la UNACH.

La presente investigación además de ofrecer una solución alternativa con sistemas nIDPS distribuidos bajo licencia GLP a uno de los problemas reales y actuales de la UNACH tendrá un efecto social puesto sirve de base para solucionar problemas similares a los expuestos.

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA

2.1.Introducción

En este apartado se detallan conceptos básicos que permitan un mejor entendimiento de lo referente a: intrusiones en la una red de datos, las técnicas y herramientas que permiten la prevención y detección de intrusiones.

2.2.Introducción a la seguridad de la información

La seguridad de la información, consiste en asegurar los recursos de un sistema/red y su uso adecuado.

Los objetivos principales son asegurar la integridad, disponibilidad y confidencialidad así mismo como objetivos generales el control y la autenticidad.

- **La Integridad** es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado.
- **La Disponibilidad** es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas.
- **La Confidencialidad** es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño o volverse obsoleta
- **El Control** permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.
- **La Autenticidad** permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen.

Mecanismos de seguridad

Para el autor (Areitio Bertolín, 2008) los mecnismos de seguridad consisten en una serie de medidas clasificables en cuatro: la disuasión, consiste en crear un

ambiente de advertencias para evitar la violación de seguridad; la prevención consiste en medidas para tratar de detener a los intrusos, este estado incluye la aplicación de cortafuegos, biometría y otros para permitir que solo los usuarios autorizados puedan tener acceso a las instalaciones o sistema; la detección permite que si un intruso ha superado los anteriores estados o está en proceso de logar el acceso al sistema, se emitan alertas que pueden ser tiempo real o almacenadas para su posterior análisis; por último el estado de respuesta es un mecanismo de efecto posterior que consiste en tratar de detener y / o prevenir daños futuros o el acceso a una instalación.

2.3. Introducción a las intrusiones

El concepto de ataque e intrusión se tratan de la forma similar en el campo de la seguridad informática, por lo tanto una intrusión es todo acto que atenta contra los objetivos de principales de la seguridad informática (disponibilidad, integridad, confidenciabilidad, y autenticidad). (Areitio, 2008, pág. 162) Un ataque es un intento de intrusión y una intrusión es el resultado de un ataque exitoso incluso si el éxito es parcial. (Salinas, 2005).

2.3.1. Concepto de intrusiòn

Una intrusión se define como un conjunto de acciones deliberadas o dirigidas que comprometen algunos aspectos de la información, para los autores (Whitman & Mattord, 2012) un ataque tiene como fin lograr un resultado no autorizado, realizar actividades incorrectas o hacer uso indebido de un sistema o red. De manera general un ataque puede ser:

- **Directo:** un atacante que utiliza un dispositivo personal para romper la seguridad.
- **Indirecto:** el atacante administra equipos comprometidos de manera autónoma o bajo el control directo para utilizarlos como plataforma y lanzar ataques.
- **Activo:** el atacante toma acciones intencionadas para acceder a la información.

- **Pasivo:** Accede a información sensible no destinada para sí, mediante herramientas de olfateo (sniffers) recopilan información como contraseñas, tráfico de red y cualquier información relevante para el atacante.
- **Interno:** provienen de dentro de la organización.
- **Externo:** el origen es generalmente redes externas como internet.

2.3.2. Impacto de los intrusiones

Con respecto al impacto producido al ser víctima de un ataque varía en función del sector de una organización y la dimensión de su objetivo de negocio. Las consecuencias comprometen aspectos cualitativos y cuantitativos como: Perdidas económicas: cuando un servicio web o recurso de red es interrumpido de sus actividades normales en un determinado período de tiempo, representa un impacto económico, deterioro de productos y/o servicios; Deserción de clientes: la insatisfacción de los clientes o potenciales clientes provoca la deserción y búsqueda de otras empresas que garanticen un buen servicio; Perdida de reputación: incide en la degradación de confianza por parte de clientes, potenciales clientes y población en general; Actividades jurídicas: si un cliente se ve afectado por la falta de disponibilidad de los servicios es posible que tomen acciones legales con el fin de una restitución económica debido a la falta o ineficiencia de protección tomadas por parte de la organización. (Bosworth, Kabay, & Wayne, 2014)

Los tipos de amenazas genéricos según el estándar ISO 7498-2 citados por los autores como (Areitio Bertolín, 2008) y (Fung & Boutaba, 2013) son: interrupción, interpretación, modificación y fabricación; donde la interrupción hace que un objeto se pierda disponibilidad total o parcial; acceder a un determinado objeto de un sistema es conocido como interceptación; si además de acceder a un objeto este es modificado o destruido completamente se trata de la amenaza de modificación y la fabricación corresponde a conseguir que el objetivo inicial sea similar a un nuevo objeto fabricado en que se sea difícil la distinción entre el objeto original y el nuevo.

2.3.3. Tipos de intrusiones

En 1998 DARPA Programa de Evaluación de Detección de Intrusos gestionado por el MIT cataloga la amplia gama en ataques o intrusiones en:

- Sondas
- Denegación de servicio (DoS)
- A distancia en Local (R2L)
- Usuario como Root (U2R)

2.3.3.1. Sondas (vigilancia y exploración)

Este tipo de ataque escanea un sistema con el objetivo de recopilar información (IP vàlidas, servicios habilitados, etc y obtener de esta manera una lista de posibles vulnerabilidades que pueden ser utilizados en el lanzamiento de un ataque a maquinas o servicios. Dicho de otra manera estos ataques ponen a prueba un objetivo potencial recopilando información para una posible intrusión. Son inofensivas hasta que descubra la vulnerabilidad y la use. (Fung & Boutaba, 2013, pág. 45)

Ejemplos de ataques de sondeo incluyen: Escaneo de los equipos de la red para un servicio en un puerto específico de interés (IPsweep), herramientas de mapeo de red (nmap), etc. (Lazarevic, Kumar, & Srivastava, 2005, págs. 25-26)

2.3.3.2. Denegación de servicio (denial of service)

Un ataque de denegación de servicio conocido por sus siglas en inglés (Denial of service) se caracteriza por un intento explícito de denegar a los usuarios legítimos el uso de un servicio o recurso. (Centro Criptogràfico Nacional de España, 2013)

Para el autor (Fung & Boutaba, 2013) este tipo de ataque tiene como objetivo hacer a un sistema o red incapaz de proporcionar servicios normales bloqueando o degradado la disponibilidad de recursos a usuarios legítimos en un periodo de tiempo.

De acuerdo a Macías, es una acción o conjunto de acciones tomadas por una entidad malintencionada, que envía determinados mensajes hacia uno de los destinatarios o el propio canal de la comunicación de forma que interfiere en su

funcionamiento habitual, impidiendo el acceso de manera total o parcialmente a un determinado servicio ofertado. (Macìa, 2007, págs. 16-18).

Se infiere de acuerdo a lo expuesto por los autores Macìas y (Fung & Boutaba, 2013) que este tipo de ataque tiene no tiene como finalidad conseguir acceso, sino el de inhabilitar un servicio o recurso informático, degradando la disponibilidad de manera total o parcial de recursos a usuarios legítimos en un periodo de tiempo.

La taxonomía de los ataques DOS, se representa mediante la siguiente figura:

Figura I: Taxonomía de denegación de servicio

Fuente: (Centro Criptogràfico Nacional de España, 2013, pág. 9)

Los objetivos de un ataque de denegación de servicio pueden ser: a nivel de dispositivo, que aprovechan errores o debilidades de hardware; a nivel de router, que que envían tramas; a nivel de SO, que provechan las limitaciones inherentes a la manera en que los sistemas operativos implementan los protocolos. Un ejemplo de este es el ataque de ping de muerte (ping-of-death); a nivel de aplicación; que aspiran dejar fuera de servicio a un host proveedor de algún servicio consumiendo gran parte los recursos disponibles de este y como consecuencia impiden el uso legítimo a usuarios reales, mediante el uso de explotación de bugs en aplicaciones

como consecuencia impiden el uso legítimo a usuarios reales, mediante el uso de explotación de bugs en aplicaciones.

El origen de ataque toma en cuenta las direcciones IP que originan el tráfico para DOS.

- **Direcciones validas:** direcciones fácilmente identificables.
- **Direcciones falsa:** (IP Spoofing) falsear el origen del ataque alterando la cabecera IP. Las inundaciones de datagramas IP que puede ser; UDP (peticiones sin conexión de los puertos disponibles), ICMP (crean mensajes de error y control de flujo) y TCP (peticiones con conexión).
    - **Smurf:** Para inundar con peticiones de respuesta a la víctima se envían paquetes ICMP ECHO a direcciones de difusión y conseguir la amplificación con una dirección de origen falsa.
    - **Fraggle:** similar a Smurf pero con peticiones UDP. Consume ancho de banda incluso si en la red no está activada ECHO.
    - **Inundación SYN:** Este ataque se centra en desertar conexiones no terminadas, de esta manera se añade la cola de respuestas del servidor se va llenando y limita el acceso del servicio los host legítimos. (Scarfone, Grance, & Masone, 2015, pág. 89)

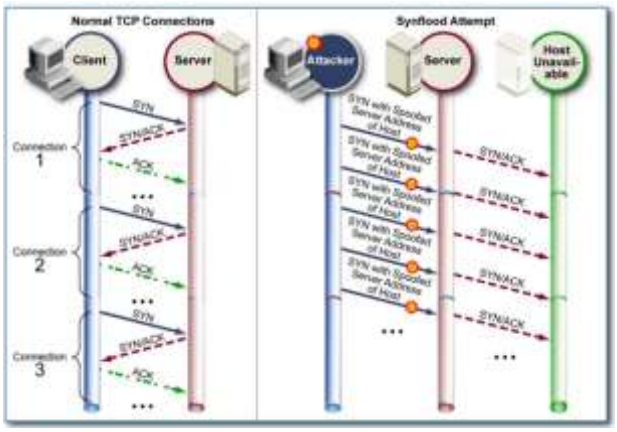


Figura II: Ataque SynFlood

Fuente: (Scarfone, Grance, & Masone, 2015)

- **Desbordamiento de buffer**: (Buffer-overflow) Aprovecha fallos en los programas enviando cadenas monumentales de datos validos. Los buffer o

pequeños espacios en memoria limitada son creados para contener una cantidad específica de datos (bytes), cuando un programa intenta escribir más información de la soportada se produce un desbordamiento o bug. El atacante puede desbordar los bug adyacentes, explotando: los errores en la programación, la capacidad de datos que se encuentran en la cola de ejecución en la memoria intermedia (RAM) o con la adición de datos que puede contener código que le permita corromper o sobrescribir los datos válidos retenidos en ellos. La finalidad es desencadenar acciones específicas, tales como daños en los archivos del usuario o proporcionar al usuario de acceso root.

- **Consumo de ancho de banda:** agotamiento de los recursos de sistema como: CPU y memoria, se realiza principalmente mediante el envío masivo de peticiones con el fin de colapsar el ancho de banda del sistema víctima.

Para los autores (Douligeris & Serpanos, 2007) y (Fung & Boutaba, 2013) la frecuencia e intensidad de los ataques DOS se refieren a los flujos de tráfico empleado de los cuales se describen: en que utilizan pocos bytes generalmente en exploits o formularios (one-shot), flujo constantes característicos por una red botnet (Constantes), flujo variante en función del tiempo (fluctuante) y finalmente el flujo ampliado en función del tiempo (incremental). Dos últimos mencionados son de difíciles de detectar.

El trafico dependiendo de sus características pueden ser: filtrable reconocidos fácilmente por el firewall, no filtrable que constituye al trafico legitimo o con pequeñas variaciones como inundaciones a peticiones DNS y el trafico mas complejo de distinguir consisten en el no caracterizable que comprende una mezcla de paquetes TCP SYN, TCP ACK, ICMP ECHO, ICMP ECHO REPLY y paquetes UDP probablemente podría ser identificado, pero sólo después de un considerable periodo de tiempo y esfuerzo.

El origen de los mensajes de denegación de servicio implica una clasificación simple como son los Dos y DDos. El primer tipo mencionado se refiere a una sola fuente generadora del ataque, mientras que el segundo se caracteriza por el uso de

uno o varios computadores que lanzan un ataque coordinado sobre un mismo objetivo, usando la tecnología cliente/servidor se despliegan a través de internet. (CISCO Systems, Inc, 2014)

Para autores como (Douligeris & Serpanos, 2007), (Fung & Boutaba, 2013) la estrategia de ataques DDOS se compone de un mínimo de cuatro elementos como son: el atacante real, maquinas manipuladoras o maestros que cuentan con programas que controlan uno o varios agentes o zombis, agentes demonios de ataque que generan el flujo de paquetes hacia un objetivo y el host destino o victima

2.3.3.3. Remotos a local (r2l)

De acuerdo a (Paliwal & Gupta, 2012) los atacantes ingresan al sistema con una cuenta de usuario normal y/o aprovechan la vulnerabilidades encontradas en un recurso o servicio con el fin de ganar privilegios como superusuarios. Generalmente este tipo de ataque son externos (internet).

2.3.3.4. Usuario como root (u2r)

El atacante obtiene los datos necesarios de un usuario legítimo, con los que puede iniciar sesión y pretende escalar privilegios hasta posicionarse como usuario root.

A diferencia de los ataques R2L que provienen de un sistema exterior, en los U2R el atacante encuentra en el sistema y buscan obtener más privilegios. (Lazarevic, Kumar, & Srivastava, 2005, pág. 26)

2.3.4. Intrusiones desde de punto de vista de la procedencia

Los atacantes son individuos que atentan a la seguridad informática. Desde el punto de vista de la procedencia de un ataque tenemos:

- **Personas internas:** conocidas en el campo se seguridad como *insiders*, que son las personas que alteran los recursos desde el interior desde la organización como los usuarios, empleados y terceras personas.
- **Personas externas:** individuos que inician un ataque fuera del perímetro de seguridad como internet. En este contexto tenemos:

- **Hackers:** individuo que domina el campo informático,- a través de un entendimiento total de un sistema o red busca, puede descubrir el modo de intrusión e incluso difunde esta información. Comprende el primer eslabón debido a la habilidad y deseo de penetración ante un sistema.
- **Crackers:** individuos sinónimos de rotura tanto a herramientas de software como sistemas, fascinados por romper la protección anticopia de herramientas de software con licencia y difundirlos en internet. Generalmente en este contexto son capaces de crear programas y herramientas de hardware para sus propósitos.
- **Lamers:** individuos que inicialmente no poseen conocimientos de métodos de ataques hasta que se autoeducan en internet. Utilizan herramientas y métodos para lanzar un ataque.
- **Copyhackers:** individuos que generalmente crackean hardware.
- **Script kiddie:** es un término adoptado para individuos no cualificados en el campo informático que hacen uso de scripts de ataques preparados por otras personas los cuales no entienden completamente.
  Newbie: un novato en el mundo de hackeo.

2.4. DETECCIÓN Y PREVENCIÓN DE INTRUSIONES

La detección de intrusiones es el proceso de monitorización de eventos informáticos que ocurren en un sistema de red y el análisis de los signos de posibles incidentes, que son violaciones o amenazas inminentes de las políticas de seguridad informática establecidas. (Scarfone & Mell, 2007).

La prevención de intrusiones son medidas defensivas que detienen o intentan atenuar las consecuencias negativas producidos por los ataques informáticos en una red cuando se haya detectado. Opera en un campo más profundo de lo que hace la detección de intrusiones puesto que es capaz de descifrar protocolos y establecer ciertos criterios que se consideren necesarios para mantener la seguridad.

Los sistemas de detección y prevención de intrusiones son una tecnología de software, hardware o una combinación de ellos que automatizan la prevención y

detección de intrusiones en un sistema o red informática. (Scarfone & Mell, 2007, pág. 37)

2.4.1. Sistemas para detección y prevención de intrusiones

Los sistemas de detección y prevención de intrusiones son una combinación de los sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS), por lo tanto automatizan el proceso para la detección de intrusiones que consiste en la monitorización de eventos informáticos (Scarfone & Mell, 2007) y el proceso de prevención que corresponden a medidas defensivas que detienen o intentan atenuar las intrusiones utilizando respuestas reactivas o proactivas aplicadas a su entorno (Ghorbani, Lu, & Tavallaee, 2009). De acuerdo a (Cisco System, 2004) son: Terminar sesión (TCP Reset) o descartar lo paquetes mas severos.

El National Institute of Standars and Tecnhonology diferencia a los IDPS en cuatro tipos: (NIST; R. Bace; P. Mell, 2008)

- Network-based IDPS: (nIDPS) Supervisa el tráfico de red, una porción de red o un dispositivo en particular.
- Wireless IDPS: supervisa el tráfico inalámbrico.
- Network Behavior Analysis IDPS (NBA): analiza el comportamiento de red, identificando el tráfico inusual propio de amenazas generadas por ataques como DOS, malware entre otras.
- Host-based IDPS: (hIDPS): supervisa las actividades sospechosas realizadas dentro de un host.

2.4.2. Arquitectura de un IDPS

Los sistemas para la prevención de detección de intrusiones se basan en los siguientes componentes:

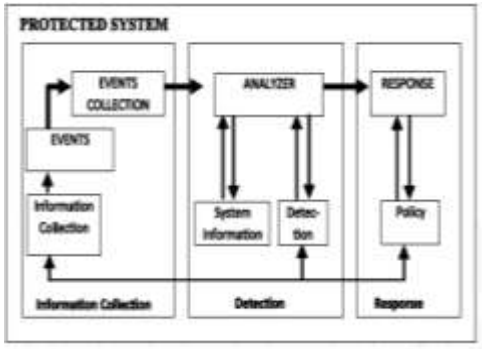


Figura III: Arquitectura básica de IDS/IPS

Fuente: (Perez, 2011)

1. **Dispositivo de recopilación de datos (sensor):** recoge datos del sistema supervisado.
2. **Detector:** procesa los datos obtenidos del o los sensores para identificar actividades de intrusión.
3. **Base de conocimiento (base de datos)** contiene información recopilada por el sensor, pero en formato preprocesado (por ejemplo, la base de conocimientos de los ataques y sus firmas de seguridad)
4. **Dispositivo de configuración** proporciona información sobre el estado actual del sistema de detección y prevención de intrusiones (IDPS)
5. **Componente de respuesta** inicia acciones cuando se detecta una intrusión.

2.4.3. Técnicas de análisis de los IDPS

Básicamente se utilizan dos criterios para el análisis: detección de manifestaciones de actividades ataque es decir buscar la ocurrencia de este (uso indebido) y la definición de lo que se considera un comportamiento normal del sistema/red y la búsqueda de actividades que sean anormales o poco usuales. (Anomalías)

2.4.3.1. Uso indebido

Detecta actividades que sigan patrones de ataques conocidos llamados firmas, o que utilicen métodos para aprovechar vulnerabilidades conocidas en el sistema/red.

Los autores (Lazarevic, Kumar, & Srivastava, 2005) mencionan que el método más común de uso indebido es el basado en firmas de seguridad. Este método recopila los eventos por el sensor para ser comparados con el contenido de una base de datos de firmas (similar a la base de datos de un antivirus), si se encuentra similitudes se genera una alarma caso contrario se consideran como actividades legítimas. (Kruegel, Valeur, & Vigma, 2005)

2.4.3.2. Anomalías

De acuerdo a (Scarfone & Mell, 2007) la técnica de anomalías es el proceso comparativo de las definiciones de patrones establecidos como "normal" contra eventos "anormales", es decir eventos observados cuya desviación de patrones supere un cierto umbral respecto a un perfil almacenado asumiéndolo como intrusión. Es factible describir a un perfil como métrica de comportamientos normales, pueden clasificarse en: estáticos o dinámicos.

El perfil estático se genera durante un periodo de entrenamiento y significa que una red o segmento de red se mantiene constante, aunque es muy posible que experimente ciertos cambios con el tiempo, en cuyo caso el comportamiento del perfil "normal" inicial será incorrecto necesitando ser generado periódicamente. En cambio el perfil dinámico se ajusta constantemente de acuerdo a los eventos adicionales aunque son susceptibles cuando el atacante altera lentamente la cantidad y frecuencia de actividad maliciosa el sistema puede incluir erróneamente al perfil "normal".

Para (Ghorbani, Lu, & Tavallaee, 2009) el perfil y el detector de anomalías son tomados como componentes del IDPS. El perfil es creado a partir de técnicas de modelado específicos como: estadística, basado en firma, minería de datos, entre otras. En el primer método nombrado su marco de detección es el análisis estadístico, el perfil se desarrolla mediante el control de características de la actividad típica durante un periodo de tiempo como por ejemplo el porcentaje promedio de ancho de banda de red sobre el uso de correo electrónico durante horas típicas de trabajo, o nivel de uso de procesador para un host en un periodo determinado. En cambio el método basado en firma se evalúa patrones como reglas y no como cantidades numéricas tal como lo hace el método estadístico.

El componente de detección de anomalías decide el punto máximo de desviación de las actividades observadas y qué porcentaje de estas actividades debe ser marcado como “anormal”.

2.4.4. IDPS según la localización del sensor

Se clasifica de acuerdo al tiempo transcurrido entre los eventos monitorizados y el análisis de estos, se consolidan dos tipos: tiempo real y fuera de tiempo.

En esta clasificación solo los IDS pueden ser implementados en tiempo real y fuera de tiempo. Los IPS solo serán implementados en tiempo real o en línea.

2.4.4.1 Tiempo real (in-line)

En este modo el análisis de los eventos es en tiempo real o casi tiempo real porque operan en flujos de tráfico continúo de la red; posibilitando tomar acciones que afecten o detengan el progreso de un ataque detectado debido a que rinde resultados suficientemente rápidos. Este tipo predomina en los IDS basados en red (NIST; R. Bace; P. Mell, 2008)

Ventaja

- Genera alarmas en cuanto se detecta un ataque lo cual favorece para la toma de acciones que afecten el progreso de este.

Desventajas

- Los requisitos de velocidad son mucho más altos que los IDS modo offline.

2.4.4.2 Fuera de tiempo (off-line)

El modo fuera de tiempo o llamado también “por lotes” realiza un análisis posterior de los eventos. Este modo de tiempo predomina en los IDS basados en host debido a que usan pistas de auditoria del sistema que se registraron como archivos.

Ventajas

- Los datos fuera de tiempo pueden ser estudiados en busca de vulnerabilidades existentes para corregirlas.

Desventaja

- Reprime el desempeño de las respuestas activas.

2.4.5. SISTEMAS PARA LA DETECCIÓN PREVENCIÓN DE INTRUSIONES BASADOS EN RED (NIDPS)

Los nIDPS supervisan eventos en una porción de red o red, es factible desplegar una o más interfaces de red conectadas a puntos estratégicos que faciliten monitorizar y analizar el tráfico malicioso tanto interno como externo de una red para muchos nodos.

De manera general los sistemas de detección de intrusos basado en red poseen las siguientes ventajas y desventajas: (NIST; R. Bace; P. Mell, 2008)

Ventajas

- El despliegue de los IDPS con buenos recursos para su operación maximiza su efectividad.
- Unos pocos bien situados nIDSs pueden controlar una gran red.
- El despliegue de los nIDS tienen poco impacto en una red existente, puesto que suelen ser dispositivos pasivos que escuchan en una interfaz de red sin interferir con el funcionamiento normal.
- Los nIDS puede ser muy seguros contra los ataques e incluso invisibles para muchos atacantes.
- Los nIPS pueden comunicarse directamente con el cortafuegos lo cual permite un análisis más profundo y toma medidas más activas de bloqueo o reconfiguración para evitar la intrusión.
- Un nIPS bien configurado constituyen una solución adecuada que reacciona automáticamente mejorando el nivel de precisión antes las intrusiones.

Desventajas

- Puede tener dificultades para procesar todos los paquetes en una red de gran tamaño o muy congestionados, un ataque lanzado durante los períodos de alto tráfico es posible que sea exitoso.
- En redes segmentadas mediante ruteadores que subdividen la red en segmentos pequeños y proporcionan enlaces dedicados, suponen un gran

inconveniente en cuanto a escoger el lugar más adecuado de sensores. (García, Herrera, & Perramón, 2004).

- La mayoría de los ruteadores no proporcionan puertos de monitoreo universales y esto limita el rango de monitoreo de un sensor IDS basado en red a un solo host. Incluso si proporcionan dichos puertos de monitoreo, a menudo el único puerto no puede reflejar todo el tráfico que atraviesa el conmutador.
- Generalmente no pueden analizar la información cifrada.
- Un IPS mal configurado puede descontinuar la conectividad de toda una red.

CAPÍTULO III

ANÁLISIS DE LAS TECNICAS Y DESCRIPCIÓN DE HERRAMIENTAS nIDPS DE OPEN SOURCE

En este capítulo se realiza un análisis de características de las herramientas software open source que permiten la prevención y detección de intrusiones basados en red. Además se realiza un estudio de las técnicas utilizadas por los nIDPS de código abierto.

3.1. ESTUDIO DE LAS TÉCNICAS DE ANÁLISIS

3.1.1. Determinación y descripción de las técnicas a comparar

En base a lo expuesto en el marco teórico los sistemas de detección y prevención de intrusiones utilizan dos técnicas: uso indebido y anomalías. Por lo tanto, el estudio comparativo se basa en estas dos técnicas mencionadas.

3.1.1.1 Técnica de análisis: uso indebido

A continuación se describe las ventajas y desventajas de mencionadas de acuerdo a varios autores.

Ventajas

- Son muy efectivos detectando ataques por lo que su tasa de falsos positivos es baja. (Kruegel, Valeur, & Vigma, 2005)
- Detectan con rapidez y precisión el uso de herramientas o técnicas sobre un determinado ataque. De esta manera el administrador de red puede priorizar medidas correctivas. (Kaushik, 2011)
- Pueden dar pautas de seguimiento a los problemas de seguridad encontrados en sistema/ red.

Desventajas

- Sólo actúa para ataques conocidos y registrados en la base de datos, para cualquier variación de un ataque requiere una nueva firma y un nuevo registro. (Kruegel, Valeur, & Vigma, 2005)
- No detectan amenazas informáticas desconocidas. (Lazarevic, Kumar, & Srivastava, 2005)

3.1.1.2 Técnica de análisis: anomalías

Las ventajas e inconvenientes de este tipo de técnica son:

Ventajas

- En teoría son capaces de detectar ataques previamente desconocidos. (Kruegel, Valeur, & Vigma, 2005)
- Actúa eficazmente contra ataques bien conocidos.

Inconvenientes

- Suele generar falsos positivos debido a la actividad benigna que se desvía del perfil "normal", especialmente en ambiente dinámicos.
- En la detección de anomalías por el método estadístico puede reconocer un comportamiento intrusivo como un comportamiento normal debido a los datos insuficientes. (Areitio, 2008, pág. 288)
- La construcción del perfil preciso es complejo puesto que el entorno monitorizado puede cambiar durante un período de tiempo, requiriendo un nuevo perfil. (Kumar, Chandak, & Dewanjee, 2014)

3.1.2. Indicador de evaluación

Se considera enfatizar la presente evaluación en las características generales, propuestas por: (Areitio, 2008) y (NIST; R. Bace; P. Mell, 2008)

3.1.3. Descripción del criterios de evaluación y sus parámetros

Este estudio toma en cuenta características importantes de cada una de las técnicas de análisis más habituales utilizadas por los sistemas para la detección y prevención de intrusiones basados en red. En base a las siguientes premisas concernientes al descubrimiento de intrusiones en función de: minimización de detección errónea, maximización de la correcta detección de intrusiones, facilidad de despliegue, rapidez de despliegue y otros aspectos descritos a continuación:

- Facilidad de despliegue
- Minimización de detección errónea: representa a la ausencia o mínima cantidad de falsos positivos.
- Maximización de detección correcta: grado de confianza en relación a que las intrusiones sean detectadas correctamente, a esta definición corresponde falsos negativos.
- Rapidez de despliegue: representa si existe un periodo de entrenamiento requerido antes de la implementación y uso de la técnica.
- Precisión de detección de intrusiones habituales: si la técnica detecta eficazmente intrusiones o ataques habituales y bien conocidos.
- Optimización con respeto al tiempo: el tiempo que representa procesar los eventos y emitir alertas de coincidencia para ataques.

Para este tipo de estudio, se sustenta además de las ventajas y desventajas expuestas en la descripción, en la comparación descrita por (Areitio, 2008) que se muestra en la siguiente tabla.

Tabla 1: Comparación ventajas e inconvenientes de las técnica de análisis Uso indebido-Anomalías

	Uso indebido	Anomalías
Ventajas	-Efectivo en detectar ataques ampliamente conocidos. -Genera poco número de falsos negativos -Genera poco número de falsos positivos -Facilita al administrador de red iniciar procedimientos de gestión de incidentes para solucionar problemas de seguridad -Diagnostica de manera rápida y precisa el uso de una herramienta o técnica de ataque especifica	Detecta comportamiento anómalos sin conocimiento específico de los detalles Producen información que pueden utilizarse para definir nuevas firmas de seguridad para los IDPS de uso indebido

Inconvenientes	-Detecta ataques conocidos -Requiere de actualizaciones de firmas -Están diseñadas para utilizar firmas bien definidas, lo que impide detectar variantes de ataques comunes.	Gran número de falsos positivos Gran número de falsos negativos Requiere un periodo considerable y complejo para la fase de entrenamiento, que inclusiveo siempre es el correcto.

Fuente: (Areitio, 2008, págs. 354-355)

3.1.4. Ponderación de evaluación

Con el fin de efectuar la evaluación se utiliza el método de evaluación sumaria escala de Likert y para ello se crea la siguiente tabla con valoraciones que consideran cualitativamente, cuantitativamente y en una escala porcentual. La escala gradual es de 0 a 5 puntos de acuerdo al cumplimiento de los indicadores expuestos.

Tabla 2: Tabla poderación de evaluación para técnicas de analisis

Calificación cualitativo	**Valor asignado**	**Porcentaje**
No existe (N/A)	0	0%
Malo	1	20%
Regular	2	40%
Bueno	3	60%
Muy bueno	4	80%
Excelente	5	100%

Fuente: Autora

3.1.5. Desarrollo comparativo

3.1.5.1. Desarrollo de evaluación del Indicador 1: características generales para definir técnicas de análisis

La valoración cuantitativa de los criterios evaluados para las técnicas de análisis se detalla en la siguiente tabla:

Tabla 3: Evaluación del criterio1 para técnicas de uso indebido y anomalías

Características o Indicador a evaluar	**Uso indebido**	**Anomalía**
Facilidad de despliegue	4	2
Minimización de detección errónea	5	3
Maximización de detección correcta	4	4
Rapidez de despliegue	4	2
Precisión de detección de intrusiones habituales	5	4
Optimización con respeto al tiempo	3	2

Fuente: Autora

Para el Indicador de optimización de tiempo se guía en la tesis de detección de intrusiones basada en técnica de anomalias (Naranjo & Macìas, 2014) , donde cita que un IDS con técnica de uso indebido tarda 0.02 milisegundos y un IDS con técnica de anomalías (de minería de datos) tarda 0.08 milisegundos.

3.1.6. Resultados de la evaluación del Indicador 1

El resultado promedio de la evaluación de las técnicas de análisis de detalla mediante la siguiente tabla:

Tabla 4: Promedio de evaluación del Indicador 1: Características generales para definir el uso de técnicas de análisis

Técnica	**Promedio**	**Porcentaje**
Uso indebido	3,33	66,60%
Anomalías	2,33	46,60%

Fuente: Autora

De acuerdo a lo expuesto se determina que la técnica de análisis de uso indebido cumple con los criterios analizados en un 66.60% frente la técnica de anomalías que cumple con un 46.66%.

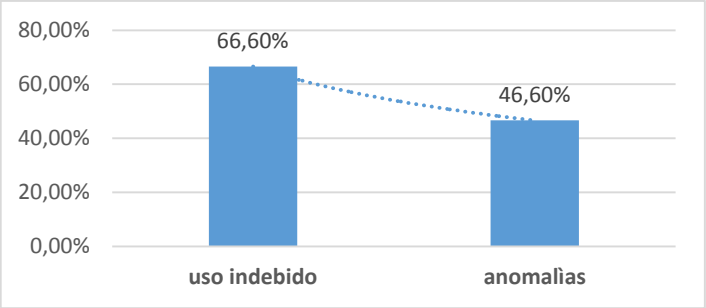


Figura IV: Resultados de la evaluación para el criterio1
Fuente: Autora

3.1.7. Selección del tipo de técnica

A partir de los resultados expuestos anteriormente se determina que la técnica uso indebido proporciona una mayor cantidad de ventajas, de acuerdo a la evaluación de facilidad de despliegue, minimización de detección errónea, maximización de detección correcta de intrusiones, rapidez de despliegue, facilidad de uso, precisión de detección de intrusiones habituales y optimización con respecto a tiempo de detección. La técnica de uso indebido constituye un 66.60% en comparación con la técnica de anomalía que se posiciona con un 46.66%

Como aporte personal se construye una tabla FODA sobre el la técnica de análisis uso indebido para el IDPS.

Tabla 5: FODA Técnica de Uso indebido

Fortalezas	**Oportunidades**
Menor alertas de falsos positivos No requiere un periodo de entrenamiento.	Fácil de diseñar Requiere de afinación.
Debilidades	**Amenazas**
Precisa firmas actualizadas	No detecta ataques nuevos

Fuente: Autora

3.2. DESCRIPCIÓN DE HERRAMIENTAS PARA LA DETECCIÓN Y PREVENCIÓN

5.5.1. Determinación de las herramientas nIDPS open source a comparar

En mundo de la seguridad informática existen varias herramientas software distribuidos bajo la licencia open source. Las herramientas Bro IDS, Snort, NFR, Suricata y Dragón son mencionadas en el artículo "Recent Advances in Intrusion Detection Systems: An Analytical Evaluation and Comparative Study" de la revista International Journal of Computer Applications, describe mediante la siguiente figura las herramientas software IDS actuales.

Intrusion Detection Technique	Network Usage	Throughput	Speed	Large User Community	IPS Capability	Open Source	Installation/ Deployment	Analysis GUI	Operating system	Parameters
Anomaly Based	Less	Maximum	Faster	No	No	Yes	Typical	Less	Unix	Bro
Signature based	Medium	Moderate	Fast	Yes	Yes	Yes	Easy	Many	Win/Unix/Mac	Snort
Signature based	Less	Moderate	Medium	-	No	Yes	Easy	Less	Unix	NFR
Signature based	Very Less	Maximum	Faster	No (Emerging)	Yes	Yes	Intermediate	Many	Win/Unix/ Mac/BSD	Suricata
Host based	Medium	Maximum	Fast	Less	No	No	Easy	Standalone	Unix	Dragon Squire

Figura V: IDS actuales
Fuente: (Kumar, Chandak, & Dewanjee, 2014)

En la figura muestran cinco herramientas software IDS, sin embargo, Snort y Suricata son los únicos que poseen capacidad IPS. Debido al objetivo del trabajo de investigación presente se toman en cuenta estas dos herramientas.
Además esta selección se respalda bajo las siguientes razones:

- El instituto SANS dedicado la formación de seguridad informática, en el estudio denominado "Open Source IDS High Performance Shootout" orientado a la búsqueda de herramientas IDS basados en red de alto rendimiento que compitan con soluciones comerciales, referencia a Suricata y la solución preferida Snort como candidatos viables para satisfacer la demanda actual de redes con ancho de banda de 1,10 Gbps o el próximo de 40 Gbps. (SANS, 2015)

- Para Albin, Snort se ha convertido en un estándar en el campo de la seguridad informática para motores de detección de intrusos basados en firmas (Albin, 2011), por casi una década esta solución no tenía contrincante hasta el lanzamiento de Suricata advertido como motor de detección/prevención de intrusiones de próxima generación que adopta nuevas características.
- En el artículo en línea de (Damaye, 2015) referente a los motores de detección/prevención de intrusiones basados tanto en técnicas habituales como uso indebido y anomalías tanto Snort como Suricata, tienen diferente enfoque, para los cuales las reglas oficiales conocidas como Vulnerability Research Team (VRT) y Emerging Thearts (ET) son normas complementarias y necesarias que permiten optimizar la detección de ataques.

5.5.2. Descripción de las herramientas nIDPS open source

3.2.2.1 Snort

Figura VI: Logo Snort 2.9.8
Fuente: (The CISCO Online Privacy Statement, 2016)

Snort es una aplicación que está disponible bajo la licencia GPL, desarrollada por Martin Roesh 1998,es usada principalmente como: IDS/IPS de red y host, analizador de encabezados de protocolo (sniffer) y logging que registra los paquetes de red además almacena en un archivo para su posterior análisis. Snort IDPS permite el tráfico de red para los partidos contra un conjunto de reglas definidas por el usuario y realiza varias acciones en base a lo que ve. (Cisco and/or its Affiliates, 2014). Es notable mencionar que es capaz de analizar en tiempo real el tráfico registros de paquetes en redes IP capturando datos desde la red y aplicándolo reglas a los datos o las anomalías previamente definidas.

Página oficial: https://www.Snort.org/

Versión estable: 2.9.8 (Actualizado a Febrero 2016)

Características

- Posee más de 300000 reglas.
- Puede ser instalado en los host minimizando la interrupción normal de estos.
- Posee un lenguaje de reglas sencillo y flexible, por lo que es posible la creación de nuevas reglas.

Modos de operación

- Packet Sniffer: captura los paquetes de la red.
- Packet Logger: registra los paquetes en el disco.
- Network-based IDS: Snort permite analizar el tráfico de una red.
- Inline Mode (IPS): obtiene paquetes de iptables en lugar de forma libpcap y los iptables transmiten los paquetes basado en reglas de Snort que utilizan tipos de reglas específicas en línea

3.2.2.1.1 Arquitectura básica

Snort combina múltiples componentes lógicos que trabajan de manera conjunta y bajo un mismo formato para detectar ataques particulares y así generar alertas.

- Sniffer
- Decodificador
- Preprocesador
- Motor de detección
- Módulo de alertas y salida

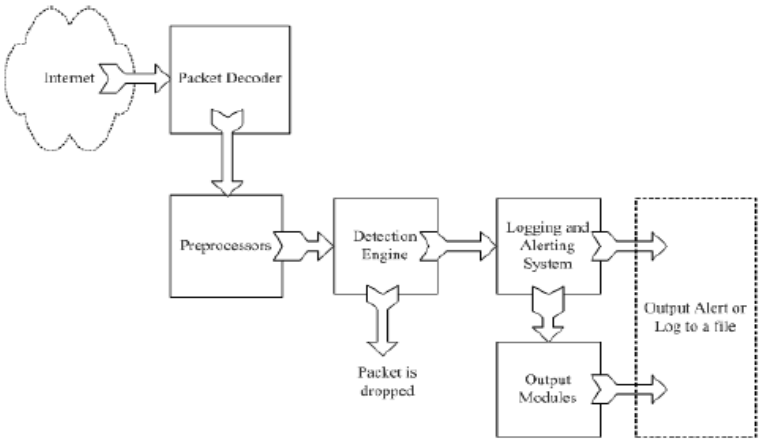


Figura VII: Componentes de Snort
Fuente: Rehman, Rafeeq Ur (2003)

El paquete Sniffer "olfatea" el tráfico que circula por una red, mediante la "lectura" de datagramas lo cual se consigue colocando una interfaz en modo promiscuo que permite a la NIC de un dispositivo leer todo el tráfico y no solo el directamente dirigido a ella.

El módulo de adquisición de datos (DAQ) funciona como una capa de abstracción entre las librerías de captura de paquetes y Snort. El DAQ recolecta promiscuamente datos de la red y lo pasa junto al motor de decodificación.

El decodificador analiza lo que está en cada paquete desde de la capa enlace de datos hasta la capa de aplicación, almacena esta información en la estructura de datos y trasmite a los demás elementos que componen la arquitectura. Snort decodifica en su totalidad TCP/IP para otros protocolos de red se identifica hasta la capa 2, sin hacer uso de ello.

El preprocesador (Preprocessors) Interactúa con el paquete en un contexto pertinente de diseño para su interpretación adecuada en el motor de detección antes que pueda ser analizado y realizar alguna operación. Reorganiza, arregla, modifica, normaliza y presenta datos relevantes del paquete para que sea analizado eficazmente. De acuerdo a la configuración el procesador es capaz de alertar condiciones anómalas.

El motor de detección (the detection engine) aplica las reglas configuradas en busca de patrones de actividades intrusivas, para tomar acciones como generar alertas o descartar el paquete. El desempeño del motor detección depende de: número de reglas, cuán robusto sea la maquina en la que se está ejecutando Snort y carga de la red.

Finalmente el módulo de alertas y salidas (the output and alerting module) realiza diferentes operaciones dependiendo de cómo se haya configurado. Controla el tipo de salida generada por el logging y el sistema de alertas además de permitir almacenarlas en distintos tipos como SNMP, syslog, enviar emails, generar XML, modificar la configuración en el router o firewalls, e interactuar con la base de datos, entre otras.

3.2.2.1.2 Ventajas

- Permite la configuración de múltiples archivos de configuraciones (vlan Id)
- Permite realizar diferente configuración si múltiples instancias de Snort
- Crea instancias de configuraciones únicas.
- Alta disponibilidad de documentación en internet.

3.2.2.1.3 Debilidades

- El motor de análisis es menos potente que soluciones comerciales como las de ISS o de Cisco. (Royer J. , 2004)
- Requiere una automatización manual de firmas. (Royer J. , 2004)
- Uni-Threaded

Preprocesadores Snort

Permiten añadir más funcionalidades, se ejecutan antes de que el motor de detección sea llamado, pero después de que el paquete sea decodificado.

Los preprocesadores se cargan y se configuran en el archivo de configuración principal de acuerdo a la siguiente semántica: preprocessor <name>: <options>

Session: módulo de gestión de sesiones.

Stream: módulo de reensamblaje TCP y UDP.

- Transport Protocols TCP, UDP
- Target-Based: manejo de los datos y otras anomalías TCP superpuestas.
- Stream API: reensamblaje de capa de aplicación.
- Anomaly Detection: Anomalías de protocolo TCP, tales como datos de paquetes SYN.

sfPortscan: detecta la primera fase de un ataque a la red (reconocimiento), en esta fase un atacante determina qué tipos de protocolos o servicios de red es compatible con una gran cantidad. Este es el lugar tradicional donde un portscan lleva a cabo. Esta fase supone el host atacante no tiene conocimiento previo de los protocolos o servicios son compatibles con el objetivo; de lo contrario, no sería necesario esta fase.

HTTP Inspect: decodificador genérico de HTTP que inspeccionan el trabajo en solicitudes de los clientes y respuesta de los servidores, DNS: decodifica respuestas DNS y puede detectar vulnerabilidades como desbordamiento rdata DNS de cliente, ARP Spoof Preprocessor: ARP decodifica paquetes ARP y detecta ataques ARP, peticiones ARP unicast e inconsistencias del mapeo IP, Normalizer: útil cuando se utiliza Snort en modo inline. Este preprocesador consiste en traducir los diferentes tipos de formatos de alertas que genera el motor de detección a un formato estándar que Snort inline entenderá. Existen normalizaciones para IPv4, IPv6, ICMP4, ICMP6, TCP y TTL. SIP Preprocessor: control de la capa de aplicación que administra la iniciación de sesión y Reputation Preprocessor: protege la red desde una lista negra (IPs no deseadas o desconocidas), permitiendo el paso sólo a algunas IPs de confianza (lista blanca). Estas listas se cargan desde archivos externos con buena o mala reputación

3.2.2.2 Suricata

Figura VIII: Logo Suricata

Fuente: (The Open Information Security Foundation (OISF) , s.f.)

Suricata es una herramienta IDPS basado en reglas y motor de seguimiento de seguridad de próxima generación, desarrollada por OISF (Open Information Security Foundation) una organización sin fines de lucro, sus distribuidores secundarios y su comunidad. El primer proyecto estuvo disponible en Junio 2010 con la primera versión estable, desde su aparición ha dado pasos agigantados desde entonces y posicionándose como una herramienta competidora con Snort debido a que implementa algunas mejoras.

Página oficial: http://suricata-ids.org/

http://openinfosecfoundation.org/index.php/download-suricata

Última versión estable: Suricata 3.0 lanzado en Enero 2016

3.2.2.2.1 Características

- Multi-threading: esta característica permite ejecutar el procesamiento de varios procesos/ subprocesos de manera simultánea, de esta manera definir una arquitectura multinúcleo y administrar cada núcleo del procesador para que se encargue de uno o más hilos.
- Estadísticas de rendimiento: modulo que permite llevar un conteo de variada información y presentarlos como estadísticas al administrador.
- Detección automática de protocolos: facilita la implementación de reglas utilizando palabras claves de los protocolos como FTP, HTTP, TLS, SMB.
- Modulo Log HTTP: lleva un registro de las peticiones http y las almacena en un formato log apache.

3.2.2.2.2 Arquitectura básica

- Capturador de paquetes.
- Decodificador
- Detección/comparación de firmas
- Procesamiento de eventos y salida de alertas

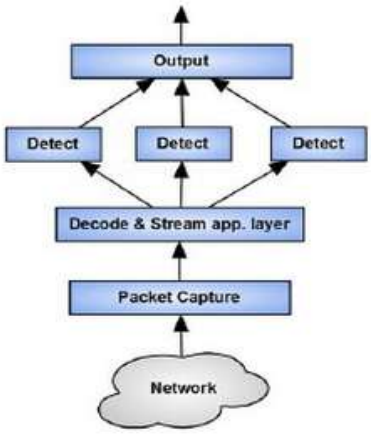


Figura IX: Componentes de Suricata
Fuente: Open Info Security Foundation (2013)

El capturador de paquetes es el componente que adquiere los paquetes de red a analizar, esto puede ser directamente desde la tarjeta de red o mediante tráfico pregrabado. El siguiente proceso es del decodificador que prepara los paquetes de red para que luego el Stream app. Layer genere un seguimiento del flujo de los paquetes montándolos a la cola de espera para que un determinado hilo invoque el paquete. Con el fin de invocar un paquete cada hilo utiliza una función de Handler que busca y reemsambla un paquete en un hilo.

Después de comparar las firmas de paquetes con las firmas de intrusión predefinidos y determinar el tipo de reglas aplicados se produce los registros de salida.

3.2.2.2.3 Ventajas

- Altamente eficaz en la detección de ataques que siguen patrones definidos
- Compatible con la reglas de snort
- Soporta IPv6
- Disponible bajo la licencia GLP v2

3.2.2.2.4 Debilidades

- Descarga manual de la actualización de reglas de seguridad en el sitio web oficial Emerging Threats.
- Bajo nivel de detección para nuevos tipos de ataques.

- No posee una interfaz administrativa.
- Opera a base de líneas de comando.
- Poca documentación en internet

.

.

CAPÍTULO IV

ANÁLISIS DE REQUERIMIENTOS Y SITUACIÓN ACTUAL DE LA UNACH

En esta sección de detallan los factores a tomar en cuenta para un posible despliegue de un sistema nIDPS open source basado en técnicas de uso indebido para la red de datos de la UNACH.

4.1.Introducción

En este apartado se representa los factores a tomar en cuenta para despleguar un nIDPS basado en conjunto de reglas que permita monitorizar el tráfico real de la red de datos de la UNACH.

La sistematización de pasos en realiza en base a los siguientes puntos:

- Determinación del estado actual de la red
- Determinación de la ubicación del nIDPS
- Requerimientos
- Instalación y configuración del nIDPS
- Instalación y configuración de módulos externos
- Pruebas
- Implementación

4.2.Situación actual de la UNACH

La Universidad Nacional de Chimborazo se inicia como extensión de la Universidad Central del Ecuador, por el lapso de 44 años, y a partir de 1995 como universidad autónoma. Actualmente cuenta con 32 carreras que funcionan en cuatro Facultades: Ciencias de la Educación, Humanas y Tecnologías (12), Ciencias de la Salud (7), Ingeniería (8) y Ciencias Políticas y Administrativas (5). En la Unidad de Formación Académica Profesionalizante, bajo la modalidad

semipresencial funcionan 5 y el Instituto de Posgrado que oferta maestrías en diferentes áreas.

Dispone de una moderna infraestructura física, distribuida en cuatro campus universitarios: “La Dolorosa”, “Edison Riera R.”, “Centro” y “Guano”.
El Centro de Tecnologías Educativas (CTE) de la UNACH ubicado en el campus “Edison Riera R.”, es un organismo académico administrativo, encargado de los principales servicios informáticos y las tecnologías de la información y la comunicación. Administra un Data Center, lugar físico que permite la interconexión y administración la red institucional.
Actualmente la institución pertenece al Consorcio Ecuatoriano de Desarrollo de Internet Avanzado (CEDIA), el mismo que contrato a la empresa TELCONET como proveedor de servicios de internet.
La topología lógica se basa en el modelo jerárquico de tres niveles: capa de núcleo, capa de distribución y la capa de acceso.

4.3.Topología lógica de la red

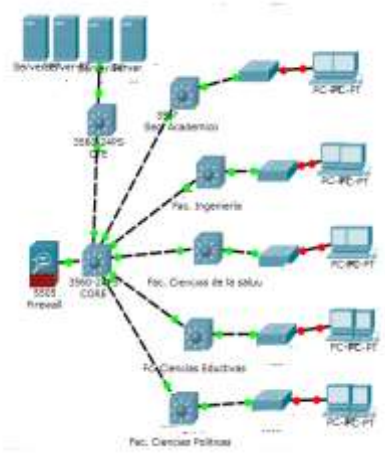


Figura X: Esquema general de la UNACH
Fuente: UNACH (2016)

Descripción Física

Capa núcleo:
- Blade 6500 Cisco

Seguridad
- Firewall Cisco serie ASA con características de IDS

Capa de distribución
- Switches Cisco Catalyst Serie 3750

Capa de acceso

- Switches Cisco Serie 2960

Tipo de cableado

- Cat. 6

4.4.Descripción de la red de datos

La red institucional se encuentra distribuida en diferentes VLAN para la red de Estudiantes, Servidores y Docentes.

Ancho de banda

- Distribución 10 Gb para las facultades
- Distribución para la red de servidores es de 30 Gb

Como el objetivo de la investigación se centra en la red de servidores se realiza un análisis descriptivo de esta porción de red.

La red cuenta con 25 servidores distribuidos para diferentes servicios entre ellos los principales se son: servidor DNS, aulas virtuales, correo institucional, autentificación de la red inalámbrica Radius, web el resto corresponde a diferentes proyectos de la UNACH.

En vista a la problemática actual de la UNACH de ataques DOS al sistema de dominio de nombres se describe la función del DNS y se realizan pruebas de monitorizaciòn para comprobar la seguridad actual.

El DNS gestiona nombres de los equipos principales y servicios de red organizados en jerarquía de dominios y sus direcciones IP asociada. Se utilizan en las redes TCP/IP, como internet, y permite localizar equipos o servicios con nombre descriptivos. Mediante la siguiente figura se presenta el funcionamiento básico de DNS a través de una consulta sencilla.

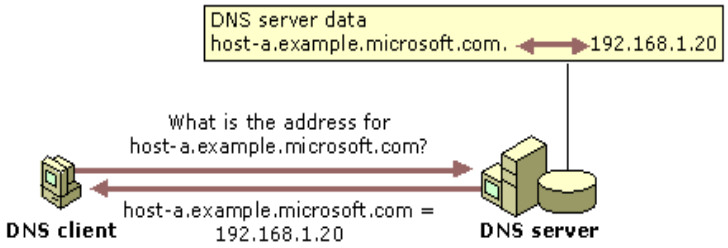


Figura XI: Funcionamiento básico de DNS

Fuente: (Microsoft Corporation, 2016)

Situación actual del servidor DNS de la UNACH mediante un ataque externo de reconocimiento utilizando dos sitios web.

http://www.yougetsignal.com/tools/open-ports/

Figura XII: Ataques de reconocimiento externo al servidor DNS de la UNACH utilizando sitios web

Fuente: Autora

La figura anterior muestra las configuraciones del servidor DNS y aportado mediante un ataque monitorización. Además del sitio anterior http://centralops.net/co/ también proporciona información no adicionada.

El servidor HTTP de la UNACH se encuentra desplegado en el sistema operativo Centos con BIND de acuerdo a los resultados obtenidos con la herramienta NIKTO

Escaneo de vulnerabilidades

Figura XIII: Ataque de reconocimiento externo al servidor HTTP e la UNCH utilizado Nikto

Fuente: Autora

4.5.Determinación de la ubicación del nIDPS

Para los autores Douligeris y Serpanos, las posibles ubicaciones para desplegar un nIDPS son:

- **Delante del firewall**: El trafico entrante es analizado antes de pasar por un primer filtro como el firewall en el cual probablemente se descartaràn algunos paquetes. Por lo tanto el trafico a monitorear no es el real. Esta implementacion puede resultar contraproducente y genera un mayor numero de alertas. (Douligeris & Serpanos, 2007, págs. 140-142)
- **Detras del firewall:** El trafico entrante es monitorizado despues de pasar por un primer filtro como el firewall por lo tanto el trafico a analizar es el que no ha ido descartado. Esta implementacion permite ademas de verificar el funcionamiento del firewall, monitorizar el trafico real de la red. (Douligeris & Serpanos, 2007, pág. 142)
- **En el firewall:** implementar el un mismo dispositivo el IDPS y firewall. Esta implementaciòn requiere una buen cantidad de recursos.

Se estima conveniente desplegar el nIDPS en la red de servidores detrás del firewall, lo que permitirá que el tráfico entrante a analizar pase por un primer filtro y no colapse el sistema nIDPS con peticiones que pueden ser descartas en el firewall.

Esta ubicación permite además de verificar el funcionamiento del firewall, monitorizar las intrusiones que no han sido descartas o vistas por el firewall.

(peticiones)

Trafico de interno-externo → Firewall Cisco → nIDPS → red de servidores

(respuestas)

Trafico de red de servidores→ nIDPS→ Firewall Cisco → tráfico interno-externo

4.6.Requerimientos

4.6.1. Con respecto al hardware

Luego de realizar el entendimiento de la red general de institucional y de la porción de red a proteger, los requerimientos hardware mínimos con respecto al despliegue de un nIDPS son:

La memoria RAM debe ser con una capacidad mayor al ancho de banda de la red o porción de red a proteger. En vista que se pretende proteger la red la red de servidores con ancho de banda de 30 Gb. Se concluye que el nIDPS debe ser de mínimo 32 Gb.

En relación al número de tarjetas, el nIDPS requiere de mínimos 2, una para la entrada de tráfico y otra para la salida de tráfico, es recomendable utilizar una tercera tarjeta de red dedicada para administración.

El tipo de cableado debe ser el mismo del utilizado en la red institucional es decir categoría 6.

Con respecto a la capacidad de almacenamiento depende de los tipos de formatos de salidas que se requiera, por ejemplo si activamos como salidas unified2, pcap, o log, el sistema volcggará las alertas en el directorio propuesto y esto consumirá la capacidad de almacenamiento del sistema dedicado a nIDPS. La capacidad requerida mínima es de 1 Tb.

4.6.2. Con respecto al sistema base

El sistema operativo a utilizar como nIDPS es independiente, pero se recomienda el uso de GNU-LINUX Ubuntu, siguiendo la line de software libre de esta investigación.

4.6.3. Con respecto a las interfaces de red

Debido a que el nIDPS trabaja en modo inline se crea un puente lógico entre las dos tarjetas de red a utilizar.

En los sistemas operativos basado en Linux se requiere instalar el paquete bridge-utils para este proceso, desde la consola el comando es: sudo apt-get install bridge-utils. La configuración del puente entre las dos interfaces se realiza en el

archivo de interfaces /etc/network/interfaces, con el fin de que configuración sea adicionadas desde el encendido.

Las configuraciones de interfaces de red en modo puente se realizan entre: dos tarjetas para ejemplificar esta configuración se utiliza a la interfaz eth1 y eth2, donde br0 es el nombre del puente.

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto br0
iface br0 inet static
address 192.168.3.1
netmask 255.255.255.0
network 192.168.3.0
bridge_ports eth1 eth2
bridge_maxwait 0
```

Figura XIV: Configuración del puente (bridge) en el dispositivo dedicado al IDPS
Fuente: Autora

Se recomienda en el uso de bridge desactivar las siguientes características

- ethtool --offload <interfaz> rx off tx off
- ethtool -K <interfaz> gso off
- ethtool -K <interfaz> gro off

4.6.4. Con respecto a herramientas adicionales

Es importante mencionar que además del modelo propuesto del nIDPS Suricata con la técnica de análisis de uso indebido, adicionalmente y como aporte personal se propone el uso de módulos externos que permitan gestionar las alertas de manera visual.

- nIDPS (sensor) y salida de alertas en formato unified2
- Modulos externos adicionales
    - Front-end como modulo visual de comunicación
        - Modulo colector de alertas
        - Sistema gestor de base de datos

En este apartado se repasa de manera breve el front-end Snorby, aunque es posible instalar otros mucho más complejos y completos.

Como módulo de comunicación y gestión de alertas se implementa Snorby, que es un front-end gràfico muy sencillo, con una interfaz gráfica intuitiva, que gestiona alertas de Suricata o Snort y permite crear estadísticas de estas.

Snorby requiere del módulo colector de alertas (Barnyard2) y un sistema Gestor de base de datos.

Barnyard2 es un script de uso libre que permite leer y procesar los archivos unified2 para posteriormente almacenar en la base de datos.

Un sistema gestor de base de datos permite gestionar de los incidentes monitorizados por el IDPS. Suricata y Snort soportan las bases de datos: MySQL, PostgreSQL, Oracle, MSSQL, y cualquier dase de datos UNIX ODBC. Siguiendo la línea del software libre se toma a consideración a PostgreSQL y MySQL.

Selección del Sistema Gestor de Base de Datos

Mysql ofrece una arquitectura que proporciona: rapidez, facilidad de personalizar o configurar y reutilización de código dentro del software. Ha logrado un sistema de administración con mayor velocidad, compactación, estabilidad y facilidad de despliegue.

Entre las características líderes que inciden en la selección de este RDBMS:

- Ligero
- Rendimiento rápido en consultas
- Facilidad de configuración
- Estabilidad

De acuerdo a que la cantidad de alertas esperadas son relativamente pocas, se selecciona como sistema gestor de base de datos relacional a (DBMS) a Mysql.

Finalmente se crea un gráfico representativo que mejora en entendimiento del nIDPS y los módulos externo adicionales.

CAPÍTULO V

METODOLOGÍA

5.1.TIPO DE ESTUDIO

Para la realización del presente estudio se tomaron a consideración varios tipos de investigación, los mismos que se detallan a continuación:

5.1.1. Según el objeto de estudio

- **Investigación de Campo:** debido a la recolección de la fuente de información y proceso de análisis del tráfico.

5.1.2. Según la fuente de investigación

- **Investigación de Cuasi-experimental:** debido a que se trabaja con grupos intactos, además, los contenidos a ser enviados no serán tomados al azar, sino que se los tendrá definidos antes de realizar dicho ambiente de pruebas.

5.1.3. Según las variables

- **Investigación Descriptiva:** debido a que se realiza una descripción de las características del objeto de estudio.
- **Investigación experimental:** se pretende estudiar en partes del objeto de investigación.

5.2.POBLACIÓN Y MUESTRA

5.2.1. Población

La población concerniente a esta investigación corresponde a las herramientas nIDPS open source.

5.2.2. Muestra

Debido a que los criterios preestablecidos de la investigación son las herramientas nIDPS open source se utiliza el método No Probabilístico con lo cual se selecciona como muestra a Snort y Suricata. Ademas esta selección se sustenta en base a los siguientes criterios:

- Snort y Suricata son IDS e IPS a nivel de red de código abierto, operan en múltiples sistemas operativos, trabajan de manera similar puesto Suricata está inspirado en Snort. (Damaye, 2015)
- Snort y Suricata son candidatos viables que satisfacen la demanda actual de redes con ancho de banda de alto rendimiento. (SANS, 2015)
- Snort y Suricata compiten efectivamente con soluciones comerciales. (SANS, 2015)
- Snort y Suricata poseen la capacidad de trabajar tanto como IDS, IPS y juntos (Kumar, Chandak, & Dewanjee, 2014)
- Suricata revolucionó los motores de detección y prevención de intrusiones con la implementación de nuevas e innovadoras características. (The Open Information Security Foundation (OISF) , s.f.)
- El motor de detecciones Snort es ligero y estable, puede ser implementado en cualquier nodo de la red con la minina interrupción posible. (CISCO Systems, Inc, 2014)

Métodos y técnicas

Las técnicas que se sustenten el desarrollo de la investigación son:

- Observación
- Recopilación de información
- Pruebas

5.3.OPERACIONALIZACIÓN DE VARIABLES

A través de la utilización de las variables establecidas se precisan las dimensiones e criterios que resultan relevantes para obtener el resultado esperado.

Tabla 6: Operacionalizaciòn de variables

Variable	Tipo	Definición conceptual	Dimensión	Indicadores
Herramientas nIDPS open source	Independiente	Herramientas que automatizan la detección y prevención de intrusiones aplicados al tráfico de red o una porción de red.	Snort Suricata	Funciones Desempeño Seguridad
Detección de intrusiones en la red de datos de la UNACH	Dependiente	Todo acto e intento que atente a disponibilidad, integridad y confidencibilidad de los recursos de una red informática.	Cantidad de anomalías o intrusiones que modeladas y observadas	Cantidad de intrusiones detectadas

Fuente: Autora

5.3.1. Descripción de Indicadores

Luego de haber efectuado la operacionalizacion de las variables involucradas en el tema investigativo se procede a realizar una descripción y evaluación de los indicadores de las variables que la conforman. Estos indicadores serán apoyados en pruebas realizadas en un ambiente de simulación posteriormente descrito.

Indicadores determinados para la variable independiente

Los indicadores de las herramientas nIDPS open source que son tomados en cuenta en la investigación conciernen a la Funciones presentes y aportados por las herramientas, desempeño y seguridad.

- **Funcionalidad:** se formaliza mediante un estudio teòrico de laas Comparación de las funciones con respecto a los protocolos de red utilizados y estructura de los archivos de configuración presentes en las herramientas nIDPS que faciliten el proceso de detección y prevención de

intrusiones a nivel de red. Estos parámetros influyen directamente con la cantidad de intrusiones que podrían ser detectadas y prevenidas.

Los parámetros que serán evaluados inciden directamente en la cantidad de intrusiones detectadas y prevenidas en relación a mòdulos de salida de las intrusiones o adición de aplicaciones extendidas y/o plugins.

- **Desempeño:** Este indicador evalúa la capacidad de las herramientas nIDPS para trabajar en condiciones estresantes como puede ser: horas pico de tráfico sin disminuir su rendimiento.
- **Seguridad:** Este indicador refiere a la posibilidad de detección correcta (sensibilidad) y por el contrario la posibilidad de no detectar intrusiones (VN).

Indicadores determinados para la variable dependiente

Para la variable independiente: detección de intrusiones en la red de datos de la UNACH, el indicador es:

- **Cantidad de intrusiones detectadas:** Este indicador determina el número de intrusiones detectadas.

5.4. PROCEDIMIENTOS

5.4.1. Fuentes de información

a) **Primarias**: Como fuente de información primaria consta la captura de tráfico a la red de servidores específicamente al servidor DNS de la UNACH con el fin de determinar intrusiones, además de tráfico generado por los ataques modelados.
b) **Secudarias:** Las fuentes secundarias se obtendrá de la información digital de libros, paper e internet.

5.4.2. Técnicas de investigación

De campo: permite la observación de los resultados que se obtienen al generar la monitorización de eventos de red con las herramientas nIDPS open source Snort y Suricata.

Documental: Permite la recopilación de información de las teorías que sustentan el estudio de los fenómenos y procesos. Incluye el uso de instrumentos definidos según la fuente documental a que hacen referencia.

5.4.3. Instrumentos

Como instrumentos para la recopilación de información constan las herramientas utilizadas para la recolección de datos (captura de tráfico), las herramientas para generar ataques y la observación utilizada como una guía de observación.

Los instrumentos requeridos para la recolección de datos del presente trabajo corresponden a las herramientas que permitan capturar, visualizar y analizar el tráfico de red. Además se debe contar con una herramienta que permita retransmitir el tráfico capturado desde un dispositivo hacia el prototipo.

- **Tcpdump:** herramienta mediante línea de comando para capturado de tráfico de red.
- **Tcpreplay:** suite de herramientas para retransmisión de tráfico.
- **Wireshark:** Herramienta para análisis de protocolos red.
- **Networ Miner:** Analizador de archivos pcap.

Para la realización de ataques

Se emplea una serie de herramientas disponibles en la distribución Kali Linux, que representa una reconstrucción completa de BackTrack Linux. El proyecto está dirigido a pruebas de penetración y de auditoria de seguridad. (Offensive Security, 2015)

Los instrumentos requeridos corresponden a las herramientas que permitan realizar ataques para ello se utilizan:

- **Hping3:** herramienta de línea de comando inspirada en el ping, manipula paquetes a través del protocolo TCP/IP, ensambla paquetes y analiza. Permite además el envío de paquete TCP, UPD , ICPMP Y RAW_IP. (Sanfilippo, hping, 2006)

- **Nmap:** herramienta que permite realizar la exploración de redes y sondeo de seguridad/ puertos e implementa técnicas de exploración de inactividad. (Nmap, s.f.)
- **Metasploit:** proyecto open source de seguridad informática (RAPID-7, 2016)

La encuesta verbal realizada con el administrador de red institucional manifiesta que la porción de red de servidores de la institución representa la red que desea a proteger.

5.4.4. Procedimientos de la información

Los procedimientos utilizados en la investigación comprenden: la creación de un escenario de simulación como ambiente de pruebas y la recopilación de la información. La primera corresponde a la creación de un escenario virtual con el fin de retransmitir el tráfico en una red virtualizada incluyendo las herramientas nIDPS open source que se pretende investigar y la segunda consiste en la captura de tráfico de la porción de red correspondiente a la red de servidores de la UNACH.

Básicamente el procesamiento de la fuente de datos primaria correspondiente a la captura de tráfico de la institución consiste en la utilización de este, en un ambiente que incluya herramientas nIDPS, por consiguiente se procede a crear un ambiente de pruebas con este fin y describir el proceso de recolección de la fuente de datos.

5.4.4.1. Creación de un ambiente de pruebas

El escenario de simulación es creado para con el objetivo de procesar el tráfico capturado de la red de servidores de la UNACH para que pueda ser analizado por las dos herramientas nIDPS en modo inline.

El escenario se crea utilizando la herramienta Virtual Box, con respecto a las características físicas de mi computador personal como anfitrión que posee las siguientes características: Equipo portátil con sistema operativo windows8, Inter Core™ i5-2410M, Procesador 2,30 GHz, 64 bits, Memoria RAM 8 GB DDR3, CPU 1 Tb y Adaptador de red 802.11n Broadcom.

El esquema lógico cuenta con varios segmentos de red que representan: la red interna (LAN), red de servidores y red externa (WAN). Además cuenta con dispositivos que hacen las funcionalidades de router-firewall, un dispositivo nIDPS con Snort y un nIDPS con Suricata.

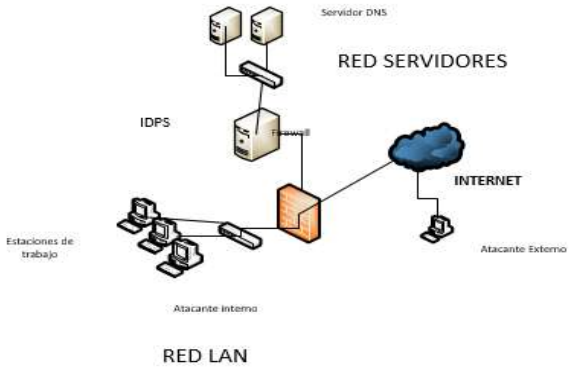


Figura XV: Esquema lógico del escenario de simulación

Fuente: Autora

Para la descripción de los segmentos de red y dispositivos generales se realiza la siguiente tabla:

Tabla 7: Especificacion general del escenario de pruebas utilizando Virtual Box

Descripción	Conexión de red	Características VM
Firewall	Bridge Red interna (RED SERVIDORES) Red interna (LAN)	Sistema Ubuntu 14.04 64 bits Memoria RAM de 4 Gb. Disco duro de 50 Gb. 3 tarjetas de red (WAN, RED SERVIDORES y LAN)
IDPS Snort	Red interna (RED SERVIDORES) Red interna (RED LAN) (se crea un puente entre las dos tarjetas)	Sistema Ubuntu 14.04 64 bits. Memoria RAM 4 Gb. Disco Duro de 100 GB 2 tarjetas de red para el modo inline Y 1 tarjeta de red para la administración. 2 procesadores 2 nuevles
IDPS Suricata	Red interna (RED SERVIDORES) Red interna (RED LAN) (se crea un puente entre las dos tarjetas)	Sistema Ubuntu 14.04 64 bits. Memoria RAM 4 Gb. Disco Duro de 100 GB 2 tarjetas de red para el modo inline Y 1 tarjeta de red para la administración. 2 procesadores 2 nuevles
Switch		Emulación de un Smith virtual incluido en Virtual Box y denominado como RED INTERNA para interconectar varios equipos a una misma red. Se crean dos redes internas denominada LAN y RED SERVIDORES.
Red		Constan de servidores HTTP y DNS

Servidores		
LAN		Constituye las estaciones de trabajo de usuarios legítimos y un dispositivo de prueba de caja gris (Kali Linux)

Fuente: Autora

Con respecto a la red de servidores:

- Servidor DNS implementado en el sistema operativo Centos y utilizando la herramienta Bind (DNS recursivo).
- Servidor HTTP, que se realiza utilizando DVMA

Con respecto a la red de LAN:

- Un dispositivo a ejecutarse como usuario legítimo de la red.
- Un dispositivo de pruebas de caja gris, que simula ataques que pueden ser realizados por un miembro de la organización.

Con respecto a dispositivo nIDPS:

- Se crean dos dispositivos con las mismas características para hacer las funciones de IDPS con técnica de uso indebido, en el primer dispositivo se instala la herramienta Snort 2.9.8 y en el segundo Suricata con la versión 2.0.10.
- Se localiza al IDPS detrás del dispositivo firewall-ruteador, que interconectan las redes LAN a RED DE SERVIDORES y viceversa.
- Snort y Suricata tendrán las mismas configuraciones de acuerdo al escenario propuesto y son similares a la red de la UNACH.

De acuerdo al conjunto de reglas:

- Para obtener resultados comparables sobre los indicadores a investigar, se hace uso de las reglas de Emerging Threats para las ambos nIDPS, las cuales son distribuidas bajo la licencia BSD.
  Snort EmergingThreats Snort-2.9.0 disponible en (ProofPoint Inc., 2015)
  Versión: 8245 actualizada a la fecha 2016-03-22
  Suricata EmergingThreats Suricata disponible en (ProofPoint Inc., 2015)
  Versión: 8245 actualizada a la fecha 2016-03-22

La cantidad de reglas para ambas herramientas son 1.170 para Snort y 1.193 para Suricata, actualizadas al año 2016. Sin embargo se hace énfasis y uso para las intrusiones DOS, DNS, SCAN, etc.

El escenario planteado permite efectuar ataques DOS al servidor DNS y HTTP internos y externos.

Con respecto al direccionamiento general:

- LAN 172.30.0.0/16 gw (172.30.0.1)
- RED SERVIDORES 192.168.150.0/24 gw(192.168.150.1)
- WAN 192.168.1.0/24

Tabla 8: Descripciòn de las sistemas virutalizados

RED	**Tipo**	**S.O.**	**IP**
Red servidores	Servidor http	Ubuntu 14.04 (Damm Vulnerable Web App DVMA)	192.168.150.6
	Servidor DNS	Centos 6.4 (Bind 9.8.2rc1)	192.168.150.100 192.168.150.55
LAN	Estación atacante	Kali Linux 3.18	172.30.128.5
	Estación normal	Windows 7	172.30.128.168
WAN	Salida internet		192.168.1.4
Firewall		Iptables (ubuntu 14.04)	192.168.150.1 (RED SERVIDORES) 172.30.0.1 (LAN) 192.168.1.4(salida a internet)

Fuente: Autora

De acuerdo a los servicios simulados

Reglas en el Firewall

El dispositivo que hace de firewall consta de 3 tarjetas de red; donde eth0 es de tipo adaptador puente (a la tarjeta de red inalámbrica del anfitrión), eth1 es de tipo red interna denominada RED_SERVIDORES y finalmente eth2 de tipo red interna denominada LAN. Las reglas creadas en el firewall, permiten el acceso desde la red la LAN a todos los servicios de RED SERVIDORES a la LAN y acceso internet.

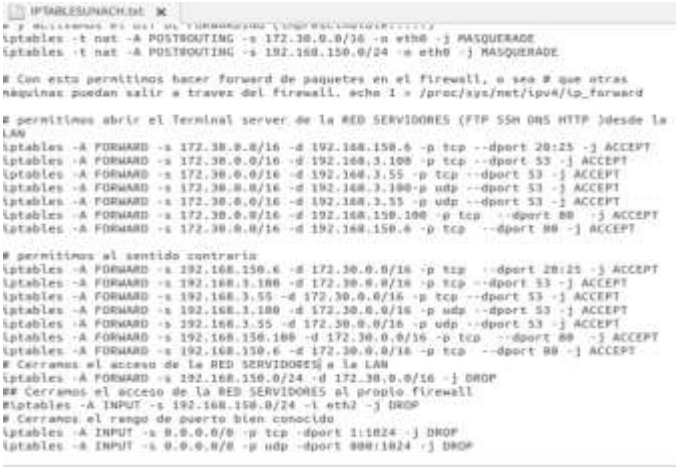


Figura XVI: Reglas en el Firewall

Fuente: Autora

Servidores DNS Y HTTP

Para crear el servidor DNS se utiliza bind 9.8.rcl, instalado en sistema linux Centos se instala con el siguiente comando: sudo yum install bind*. Las configuraciones en el archivo /etc/named.conf, direcciona a la IP correspondiente a este servidor expuestas anteriormente.

Figura XVII: Archivo de configuración named.conf

Fuente: Autora

Como servidor HTTP se utiliza "Damn Vulnerable Web Application (DVWA)", que está diseñado como una plataforma de aprendizaje de seguridad web.

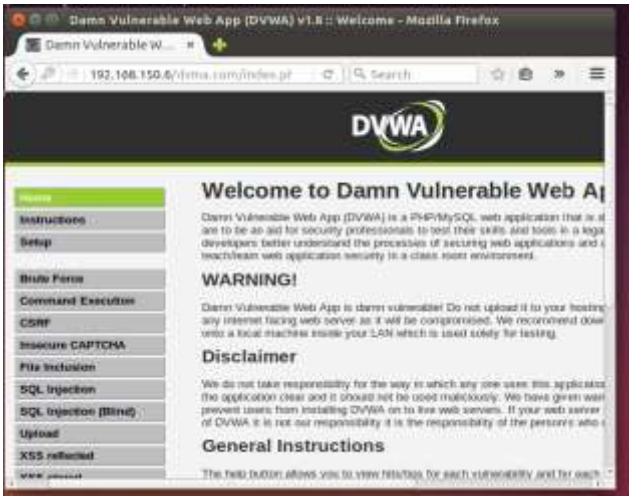


Figura XVIII: Archivo de configuración named.conf

Fuente: Autora

nIDPS Snort y Suricata

Los dispositivos empleados para hacer de nIDPS se encuentran individualmente instalados con los siguientes componentes que permitan visualizar y gestionar las alertas generadas y encontradas.

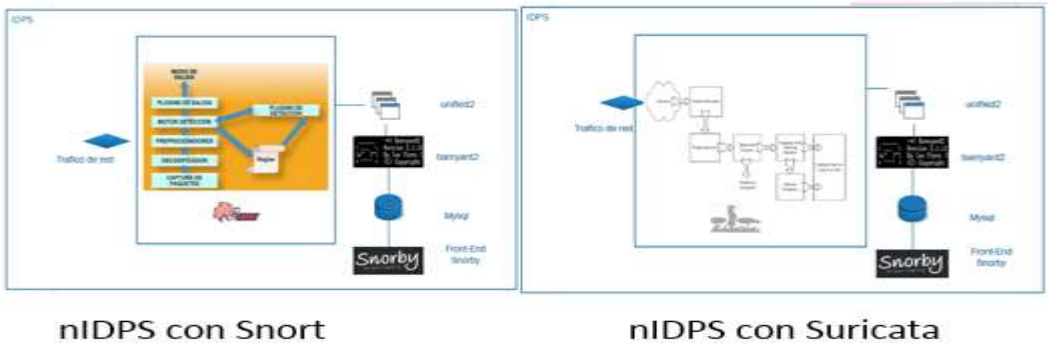


Figura XIX: Componentes de los dispositivos nIDPS en el escenario de simulación

Fuente: Autora

Con el fin de tener niveles comparables de detección y prevención de intrusiones; Tanto Snort y Suricata son configurados para que utilicen las reglas de seguridad Emerging Thread versión 8245.

Emerging Threats (ET) es el organismo que pone a disposición reglas desarrolladas y distribuidas bajo la licencia GLP y BSD a los usuarios de la comunidad para ser utilizadas sin restricciones. Es importante notar que ET ha

publicado reglas exclusivas para Suricata los cuales aprovechan sus implementaciones.

Teóricamente estas reglas Snort son totalmente compatibles con Suricata sin embargo se han realizado pruebas y Suricata presenta problemas con al menos 50 reglas y no permite iniciar Suricata hasta que se eliminen estos problemas.

Validez de la reglas de seguridad

La validez de las firmas de seguridad se encuentran sustentadas en diversos organizamos que referencian vulnerabilidades y están determinadas en el archivo reference.conf, se mencionan los que a consideración personal son los más importantes.

Las principales referencias se muestran a continuación:

config reference: bugtraq http://www.securityfocus.com/bid/
config reference: bid http://www.securityfocus.com/bid/
config reference: cve http://cve.mitre.org/cgi-bin/cvename.cgi?name=
config reference: cve http://cvedetails.com/cve/
config reference: arachNIDS http://www.whitehats.com/info/IDS
config reference: McAfee http://vil.nai.com/vil/content/v_
config reference: nessus http://cgi.nessus.org/plugins/dump.php3?id=
config reference: et http://doc.emergingthreats.net/
config reference: etpro http://doc.emergingthreatspro.com/
config reference: osvdb http://osvdb.org/show/osvdb/
config reference: exploitdb http://www.exploit-db.com/exploits/

A continuación se detallan las dos referencias principales que tanto los nIDPS Snort y Suricata utilizan:

CVE (Common Vulnerabilties and Exponsures)

Se refieren a vulnerabilidades de seguridad expuestas y reconocidas públicamente, el organismo encargado de mantener actualizadas es el Department of Homeland Security de los Estado Unidos.

- Las alertas se clasifican en varios identificadores únicos:
- Numero identificador CVE (CVE-2003-0065)
- Estado actual “entry o candidate”

- Descripción
- Referencias pertinentes

El estado actual denominado como "Candidate" indica que el reporte de una nueva vulnerabilidad pretende ingresar al listado de CVEs pero está en proceso de análisis, mientras el estado "entry" indica que el reporte de vulnerabilidad es considerado como verdadero y sustentado por varios estudios.

BID Bugtrap ID

La comunidad Security Focus publica de manera gratuita problemas de seguridad mediante la información que circula en sus listas de correo (suscripción gratuita)

Los identificadores Bugtraq están relacionados conjuntamente con los identificadores CVE y proporcionan un volumen alto de información al día sobre vulnerabilidades para las diferentes plataformas y servicios.

Cada Bugtraq contiene:

- Identificador único
- Información general sobre el bug como por ejemplo el número identificador de CVE con el que se relaciona y el software que afecta.
- Discusiones en la lista de mails de Security Focus que trataron sobre el problema
- El exploit para el problema
- La solución y
- Referencias.

5.4.4.2. Recolección de información.

Como fuente de datos primaria se captura de tráfico real de la red de servidores de la UNACH, el cual, fue facilitado con la ayuda de Ing. Javier Haro, administrador del DATA CENTER de la institución.

El procedimiento de captura consistió en configurar un puerto del switch CISCO 3750 perteneciente a la red de servidores como portmirroring:

```
(config)#monitor session ID source ?
        interface SPAN source interface
        remote SPAN source Remote
```

vlan SPAN source VLAN

(config)#monitor session 1 source interface gi<<interfazde origen>> rx

(config)#monitor session 1 destination interface fa<<Interfaz de destino>>

(config)#monitor session 1 source vlan 1 - 10 rx

Donde interfaz de origen representa la asignada y utilizada para la red de servidores (gi23) y la interfaz de replica de tráfico es una fastethernet en la que se localiza el dispositivo de captura (pc personal). Utilizando la herramienta Wireshark se realiza la captura el cual corresponde a diferentes días en tres horarios distintos por lo tanto se tiene tres archivos de captura en formato (pcap) los cuales pertenecen al siguiente horario:

HORA1: 9am-11am , HORA2: 11pm-13pm y HORA3: 13pm-15pm

Es importante mencionar que debido a que el computador portátil está localizado en la red de servidores, el tráfico entrante corresponde a sólo al permitido por el firewall.

Interpretación de la información

Todos los archivos capturados fueron analizados individualmente con la herramienta Wireshark y NetworkMiner. Los resultados obtenidos son:

El total de direcciones IP encontradas son: 74 tanto con direccionamiento IPv4 e IPv6, la siguiente figura muestra el reporte de direcciones.

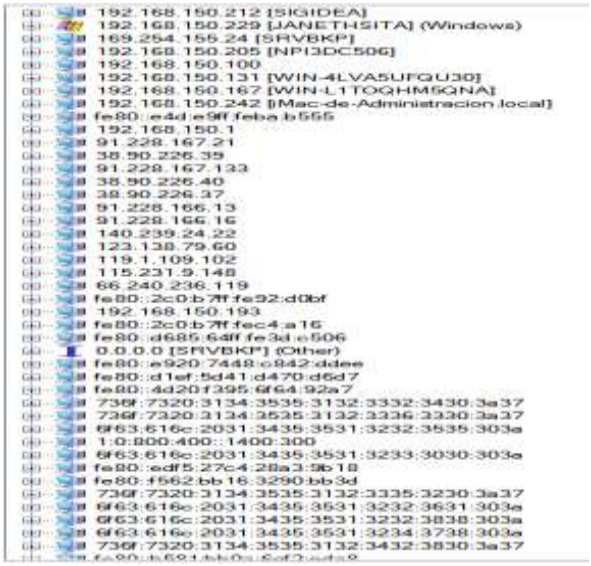


Figura XX: Reporte Endpoints del trafico capurado utilizando NetworkMiner

Fuente: Autora

Wireshark proporciona estadísticas referentes al uso de protocolos, la siguiente figura muestra los resultados obtenidos del uso de protocolo UDP.

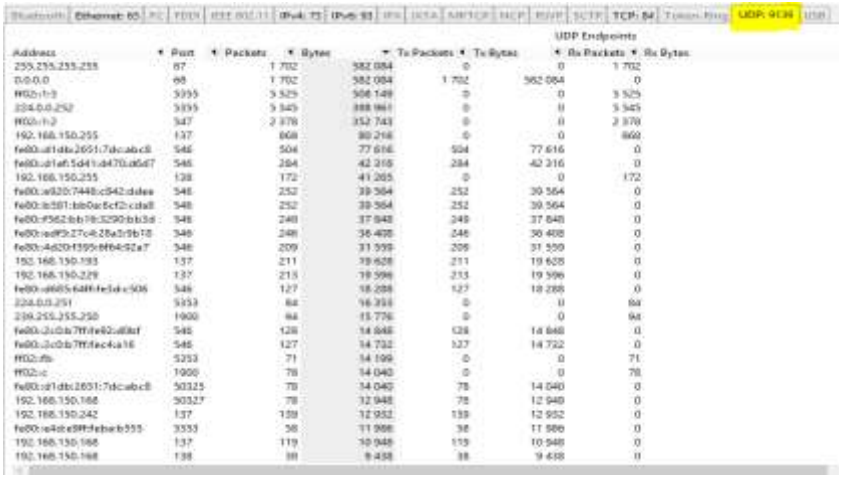


Figura XXI: Reporte Endpoints por protocolo UDP del trafico capurado utilizando Wireshark

Fuente: Autora

Los archivos pcap se encuentran desglosados por protocolo de red, lo que me permite tener una idea aproximada de las reglas que debería activarse si Snort y Suricata encuentran patrones característicos de actividad maliciosa. La siguiente tabla muestra de manera detallada el desgloce.

5.5.PROCESAMIENTO Y ANÁLISIS

5.5.1. Procesamiento y análisis de los indicadores de la variable independiente

La variable independiente es representada por las herramientas nIDPS open source. En este apartado se realiza un análisis de las herramientas nIDPS open source en función de cada indicador, el cual a su vez contiene diferentes parámetros.

Es importante mencionar que este estudio se formaliza con la versión 2.9.8 de Snort y 2.9.10 de Suricata. Asi mismo Así mimo se utiliza una tabla de ponderación de evaluación para estimar valores cuali-cuantitativos y porcentuales.

5.5.1.1. Indicador 1: Funciones

Con el fin de efectuar la evaluación de este indicador se considera la siguiente tabla fundamentada en el método de evaluaciones sumarias (escala de Likert), en la que se crea una escala con valores graduales de 0 a 5 puntos, de acuerdo al cumplimiento de los criterios expuestos. Además cada valor está representado por su respectiva valoración cualitativa y porcentual.

Tabla 9: Tabla de ponderación de evaluación

Calificación cualitativa	Valor asignado	Porcentaje
No existe (N/A)	0	0%
Deficiente	1	20%
Regular	2	40%
Aceptable	3	60%
Muy bueno	4	80%
Satisfactorio	5	100%

Fuente: Autora

La tabla creada anteriormente se describe de mejor manera.

Deficiente: esta cualidad cuyo equivalente cuantitativo es igual a 1, será otorgada a las herramientas que no cumplan o cumplan de manera deficiente con el objetivo del criterio.

Regular: Esta cualidad cuyo equivalente cuantitativo es 2, será otorgado a la herramienta que cumpla de manera insuficiente el criterio.

Aceptable: Esta cualidad cuyo equivalente cuantitativo es 3, será otorgado a la herramienta que cumplan parcialmente el criterio.

Muy aceptable: Esta cualidad cuyo equivalente cuantitativo es 4, será otorgado a la herramienta que cumpla casi en su totalidad el criterio.

Satisfactorio: Esta cualidad cuyo equivalente cuantitativo es 5, será otorgado a la herramienta que cumpla en su totalidad el criterio.

N/A: No aplicable para la asignación de un valor cuantitativo o no posee ese Indicador o característica evaluada.

Comparación de las funciones inherentes presentadas por las herramientas nIDPS, que inciden directamente con la detección y prevención de intrusiones son:

- **Automatiza protocolos de red:** capacidad de las herramientas nIDPS de detectar ciertos protocolos de red mediante palabras clave. Este criterio es importante debido a que representa: facilidad en el momento de escribir, entender o personalizar reglas de seguridad. El uso de protocolos que utilizan puertos por defecto y los que utilizan un puerto no tradicional lo cual podría implicar actividades malintencionadas.
- **Gestiona distintos módulos salida:** Capacidad que consiste en procesar varios módulos de salida para las alertas generadas que permitan determinar mediante un previo análisis una intrusión como verdaderos o falso positivo a investigación y asociación de los eventos monitorizados. Este parámetro personalmente se considera importante debido a que registra en log información referente a: cabeceras de los paquetes IP y de los protocolos encapsulados, datos de aplicación relevantes, paquetes IP en bruto.
- **Soporte IPV6:** este criterio es tomado en cuenta debido a que existe una red convergente en la institución, por lo tanto es importante considerar una herramienta nIDPS que soporte tanto IPV4, IPV6 o ambas y que emita alertas detectadas y prevenidas.
- **Aplicaciones extendidas:** este criterio se refiere las aplicaciones externas en las que puedan ser incorporadas los nIDPS y que proporcionen una representación visual de los datos de intrusión como son los NMS, SIM, SIEM,
- **Subherramientas para respuestas activas:** Describe herramientas adicionales que permitan al nIDPS además de descartar el trafico catalogado como muy peligroso, reconfigurar el firewall con el fin de bloquear el tráfico de la dirección origen del ataque por un periodo de tiempo.

- **Reputación IP:** con esta característica es posible compartir información de direcciones IP de mala reputación con otras organizaciones y soluciones de seguridad disminuyendo de esta manera los falsos positivos.
- **GeoIP:** capacidad de generar archivos que contienen información de la procedencia de una alerta utilizando geo localización. Los cuales pueden ser visualizados con Google Earth o cualquier herramienta similar.

Los autores (Appala & Avadhani, 2013) consideran la identificación de protocolos como base primordial al momento de seleccionar un nIDPS, debido a la efectividad implicada para la detección de intrusiones y minimización de uso de reglas.

Personalmente se considera importante la gestión de salida puesto consiste en procesar varios formatos de salida que ayuden con información que permitan catalogar una intrusión como verdadero o falso positivo. Además varios tipos de formatos permiten la asociación de los eventos monitorizados con otros sistemas se seguridad como auditori passiva.

Protocolos de red

Suricata 2.9.10 automatiza la detección de protocolo utilizando palabras clave para protocolos más usados como IP, TCP, UDP, ICMP, FTP, HTTP, TLS, SMB, SMB2, SSL, DCERPC, SMTP, SSH Y DNS. En cambio en la version 2.9.8 de Snort utiliza las palabras clave para los siguientes protocolos por defecto: IP, ICMP, TCP, UDP (Cisco and/or its Affiliates, 2014). Sin embargo en Snort es posible añadir preprocesadores, el código de estos se deben ejecutar antes del motor de detección, pero después de que el paquete ha sido codificado.

Se evalúa la cantidad de protocolos de red con los que la herramienta trabaja por defecto, es decir, que una vez instalado el motor de detección podrá ser utilizado, sin la necesidad de añadir preprocesadores o módulos externos para poder utilizar ciertos protocolos de red.

Palabras clave para la detección de protocolos usados por Snort 2.9.8: 4

Palabras clave para la detección de protocolos usados por Suricata 2.9.10: 14

Para la valoración se ha utilizado el número de protocolos de cada herramienta. El valor más significativo se toma como el 100% siendo 14. En base a ello, se realiza una regla de tres para evaluar la disponibilidad de detección automática de protocolo de Suricata con respecto a Snort.

$$\frac{14}{4} = \frac{100\%}{x} => \frac{100}{8}(4) = 28.57\%$$

La detección automática de protocolos en Snort 2.9.8 es el 28.57% cuya valoración cualitativo es Regular que corresponde al valor cuantitativo de 2, con respecto a Suricata 2.9.10 que es el 100% por lo tanto la valoración cualitativo correspondiente es Satisfactorio y al valor cuantitativo de 5.

Gestión de salida:

Los módulos de salida permitidos en Suricata, para las intrusiones detectadas o prevenidas son: Alertas basadas línea de registro (fast.log), Eve (Extensible Event Format), registro de salida para su uso con Barnyard (unified.log), salida de alerta para su uso con Barnyard (unified.alert), salida de alerta para su uso con Barnyard2 (unified2.alert), un registro basado en línea de las peticiones HTTP (http.log), un registro basado en la línea de consultas DNS y respuestas (dns.log), registro de paquetes (pcap-log), detallado alertas del registro (alert-debug.log), la producción de alertas para Prelude (alert-prelude), Stats Syslog y Drop.log, una información basada en la línea de paquetes perdidos y EVE que corresponde a alertas tipo HTTP y eventos DNS.

Por su parte Snort hace uso de 8 tipos de salida para las alertas que son: alert_syslog, alert_fast, alert_full, alert_unixsock, log_tcpdump, csv, unified 2, log null.

Snort por su parte hace uso de 8 tipos de salida para las alertas detectadas y prevenidas, entre las cuales son: alert_syslog, envía alertas al syslog, contiene cabeceras de los paquetes completos de los eventos monitorizados que han sido detectado y prevenidos, sin embargo ofrece una gran falencia con respecto a que ralentiza considerablemente a Snort que a su vez pierde paquetes. Esto se debe

principalmente a que Snort es mono hilo, por lo tanto procesador del sistema hardware no procesa màs de unas tantas peticiones a la vez.

Soporte IPV6

Snort 2.9.8 soporta IPV6 siempre y cuando será compilado con la opción ENABLE-IPV6, sin embargo Suricata 2.9.10 tiene soporte nativo de IPV6.

Cumplen satisfactoriamente con el Indicador = Si la herramienta soporta IPV6

Acoplamiento con sistemas de seguridad más complejos.

En vista que las aplicaciones extendidas utilizan como base inicial a los nIDPS se considera factible mencionar que la gestión de alertas detectas y prevenidas por las herramientas juegan un papel importante en la absorción de los nIDPS por sistemas de seguridad más completos como los NSM (network system manager), SIEM (Security Information and Event Management) para se mencionan a manera de ejemplo algunas herramientas open source y comerciales.

Security onion (NMS), Ossim (SIEM), Prelude (SIM), Aanval (SIEM), Cisco ISE (SIEM), AlienVault USM (SIEM), Splunk(SIEM) y openIDS (NMS).
Los SIEM intentan proporcionar una visión completa de la red en una organización, concentrando en una única plataforma las funciones esenciales de los SIM y SEM. Este tipo de herramientas con sutiles variaciones comparten funcionalidades que de manera general según (SANS Institute InfoSec Reading Room, 2006)

Fundamentado en las páginas web oficiales de las dos herramientas se induce que las alertas de detección de Suricata 2.9.8 pueden ser integradas a todas las herramientas SIEM o NMS distribuidas de manera gratuita sin embargo aún no es posible integrarlas con herramientas comerciales como Cisco ISE y Splunk. Debido a ello se le otorga la valoración cualitativa de Aceptable.

Snort 2.9.8 es compatible con todas las herramientas descritas anteriormente por lo que se le otorga el valor cualitativo de Muy Aceptable.

Acogen a suherramientas como módulos de respuestas activas

Los nIDPS pueden absorber a su vez subsistemas o plugins pequeños que utilicen las alertas generadas y detectadas para reconfigurar dispositivos de enrutamiento que incidan en la prevención de intrusiones de manera más activa.

De acuerdo a los sitios web oficiales tanto de Snort como Suricata, con respecto a los proyectos adicionales, plugins o soluciones que permiten reformar las reglas impuestas en el firewall existen:

Para Snort: Iblock es un demonio de Linux que bloquea a los anfitriones infractores a través de iptables y SnortSam es un plugin ligero que permite a Snort trabajar conjuntamente con el firewall como: Checkpoint Firewall-1, Cisco PIX firewalls, Cisco Routers (using ACL's or Null-Routes), Former Netscreen, now Juniper firewalls, IP Filter (ipf), available for various Unix-like OS' entre otros.

Es importante mencionar que Snort_inline es una versión modificada de Snort mantenida por William Metcalf y Victor Julien, acepta paquetes de iptables y utiliza nuevos tipos de reglas para decidir si el paquete se permite o niega basado en las reglas de Snort. Sin embargo esta no cuenta en el sitio web oficial.

Para Suricata: En el sitio web oficial de Suricata se menciona la integración con Snortsam y iblock, pero cabe mencionar que estos fueron construidos explícitamente para Snort y que Suricata se adapta a estos.Por lo tanto la valoración para Suricata es de Aceptable

Soporte de reputación IP

El módulo reputación IP de Suricata 2.9.10 permite almacenar y distribuir el grado de reputación positiva o negativa de ciertas direcciones IP clasificadas en categorías de listas blancas, listas negras y escala de peligrosidad, (Sourceforce, 2012)

En Snort 2.9.8 admite Reputación IP mediante el uso de preprocesadores externos el cual debe ser instalados y configurados en el archivo principal de snort.conf, direccionando al directorio localizado las listas blancas y listas negras que por lo general son de extensión .rules

GeoIP

Con respecto a la característica que permita adicionar información sobre la procedencia de una alerta, Snort 2.9.8 utiliza el preprocesador llamado GeoIP, el cual crea un archivo con extensión .kml con los datos de geo localización con el fin de verificar la procedencia de las alertas, además cuenta con una herramienta de reporte denominada SnoGe que trabaja con Google Earth, esta se encuentra disponible en sitio web oficial. Por otro lado Suricata 2.9.10 también posee esta característica que puede habilitarse al momento instalar la herramienta "--enable-geoip", esta característica le permite coincidir en la fuente de destino de un paquete por país.

Tanto Snort como Suricata soportan características de Geo-IP que permitirá al administrador de red localizar geográficamente la dirección origen de las intrusiones producidas. Ambas herramientas prometen un estado de seguridad bastante aceptable. Snort y Suricata proporcionan información adicional para detectar y prevenir intrusiones provenientes de direcciones IP aceptadas como inseguras, así adición de información en las alertas para una investigación geo localizada de las intrusiones detectadas y prevenidas, esta información puede ser analizada y visualizadas mediante la adaptación de módulos pertinentes a este fin.

5.5.1.2. Resultados generales de la evaluación Funciones

Para presentar los resultados del estudio comparativo se realiza la siguiente tabla descriptiva, la que muestra de manera resumida los indicadores y sus respectivos parámetros evaluados.

Tabla 10: Resumen de evaluación general- herramientas nIDPS

Criterios	Snort		Suricata	
	Evaluacion		Evaluacion	
	Cualittivo	Cuantitativo	Cualittivo	Cuantitativo
Automatiza protocolos de red	Regular	2	Satisfactorio	5
Gestiona distintos modulos de salida	Aceptable	3	Muy Aceptable	4

Soporta IPV6	Satisfactorio	5	Satisfactorio	5
Son acogidos por sistemas de seguridad mas complejos	Satisfactorio	5	Muy Aceptable	4
Acogen a subherramientas para como modulos de respuestas activas	Muy aceptable	4	Aceptable	3
Soportan reputación IP	Muy aceptable	4	Muy aceptable	4
Soportan GeoIP	Satisfactorio	5	Satisfactorio	5
Promedio		4		4,28571429

Fuente: Autora

5.5.1.3. Indicador 3: Desempeño

El indicador de toma en cuenta el desempeño de la herramienta en condiciones estresantes, horas pico de tráfico o situaciones en el que se comprometa de manera licita o ilícita los recursos de red posiblemente por ataques DOS no detectados (VN). Lo indicado seria que el sistema sea capaz de procesar el tráfico de manera normal, rápida y eficiente.

Básicamente el correcto desempeño de la herramienta nIDPS open source se relaciona directamente con las características del sistema hardware/software en el que se encuentre implementado y el entorno a proteger.

A medida de prueba se replicar tráfico desde el dispositivo firewall en el escenario de simulación hacia la red de servidores tanto para Snort y Suricata. Para controlar el número de intrusiones esperadas se replica a diferentes velocidades utilizando

la herramienta tcpreplay –t (máxima velocidad) –L número de repeticiones a replicar.

Los archivos estadísticos snort.stats y stats.log de Snort y Suricata respectivamente no proporcionan esta información. capture.kernel.ifdrops o capture.kernel.drop (modo IPS), capture-kernel_packerts en Suricata y en Snort pkt_drop_percent, would_tcp::ips_data (Modo IPS), kpackets_sec.discard. Si utilizar algún benchmarking. El archivo pcap replicado es el mismo en los 5 pruebas tiene un total de 22104 paquetes con un promedio por paquetes capturado de 221.188 bytes.

Tabla 11: Resumen de evaluación Desempeño

Speed	**nIDPS**	**Paq.Mb**	**Tiempo**	**Total paquetes procesados**	**% paq. Per**	**Max Carga CPU**
En tiempo real (sin parámetros) –L8	Snort	3.13	6,45	220452	0%	88
	Suric	3.13	5.32	220452	0%	78
--mbps500 –L 8	Snort	3.13	8,58	220452	0%	90
	Suric	3.13	6,12	220452	0%	76
--mbps800 –L 8	Snort	3.13	18,45	220452	0%	89
	Suric	3.13	25,19	220452	0%	70
--mbps1100 –L	Snort	2,84	40,1	19840,68	9%	98
	Suric	2,91	45,4	15431,64	7%	87
--topspeed -L 8	Snort	2,66	128,2	33067,8	15%	96,2
	Suric	2,77	135.45	28658,76	13%	136,4

Fuente: Autora

5.5.1.4. Indicador 2: Seguridad

Este indicador refiere a la posibilidad de detecccion correcta (sensibilidad) y por el contrario la posibilidad de no detectar intrusiones (VN). De acuerdo al problema investigado se considera importante simular en el ambiente de pruebas ataques DOS y monitorización.

Sensibilidad

El indicador de sensibilidad es mencionado por varios autores entre ellos: (Elhamahmy, Hesham, Elmahdy, & Saroit, 2010) y (Banerjee, Batra, & Arya, 2012).Se refiere a la capacidad de nIDPS en clasificar los eventos de entrada correctamente como normal o intrusiva. A un nivel abstracto el objetivo esperado es implemetar una herramienta 100 sensible, sin embargo es una utopia este concepto.

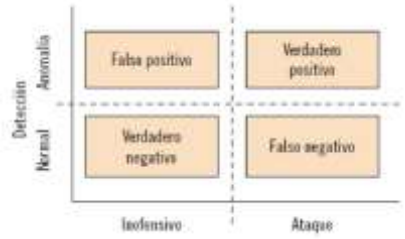


Figura XXII: Posibilidad de detección de ataques

Fuente: Chinaco,E (2015)

El valor de sensibilidad es la posibilidad (valores porcentuales) de predecir casos positivos es decir intrusiones catalogadas como verdaderas positivas VP y está determinado por la división entre el número total de VP y la sumatoria de VP + FN (falsos negativos). El valor será un valor menor 1, que multiplicado por 100 es el valor porcentual. Mientras el valor sea más cercano a 1 la herramienta se aproxima a un valor sensible de 100%.

Especificidad

Representa la posibilidad que de predecir instanacias negativas. La formula es simple y esta formula está representada por el total de VN dividido para total de VN+ FP.

Debido a que el estudio se centra en atques DOS y monitorización, me parece factible modelar unos pocos ataques de este tipo.

Ataques generados en el ambiente de pruebas

La herramienta Nmap que permite la exploración de redes y sondeo de seguridad/ puertos. Nmap –o –Sv 192.168.150.100

Figura XXIII: Escaneo con detección de servicios utilizando nmap

Fuente: Autora

El comportamiento de la red se visualiza en la siguiente grafica de Wireshark

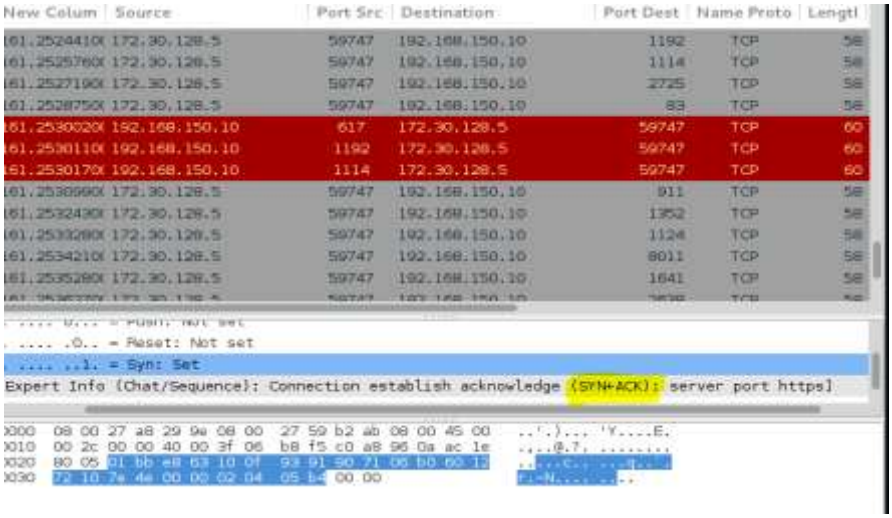


Figura XXIV: Análisis del comportamiento capturado utilizando Wireshark

Fuente: Autora

Suricata y Snort reportan las siguientes reglas:

2	nIDPS:br0	172.30.128.5	192.168.150.55	GPL SCAN PING NMAP	03/15/2016	1
2	nIDPS:br0	172.30.128.5	192.168.150.55	ET SCAN NMAP -sS window 1024	03/15/2016	1
2	nIDPS:br0	172.30.128.5	192.168.150.55	ET SCAN NMAP -sA (1)	03/15/2016	1

Snort y Suricata reportan dos reglas (sid:469 y 582) de manera correcta (VP), sin embargo ambas reportan la regla con sid: 538, la cual se denomina como falso positivo debido a que el ataque no refiere el parámetro –sA correspondiente la técnica de escaneo solo de solicitudes ACK.

Por lo tanto la valoración está dada de la siguiente manera:

Snort = sid:469 (VP:9), sid:582 (VP:9) y sid: 538(FP:1)

Suricata= sid:469 (VP:9), sid:582 (VP:9) y sid: 538(FP:1)

NIKTO

La herramienta de escaneo de vulnerabilidades HTTP es personalmente catalogada como muy agresiva puesto con un único ataque Nikto realiza internamente exhaustivos test de escaneo que incluyen a más de 32000 ficheros, debido a esto es considerados como potencialmente peligroso.

El periodo de tiempo empleado depende del grado de vulnerabilidad que permita el servidor HTTP, como en este ejemplo el servidor es DVMA y es intencionalmente vulnerable el tiempo es relativamente corto. En ambiente reales el ataque dependerá de diferentes factores. En la figura siguiente se muestra la ejecución del ataque.

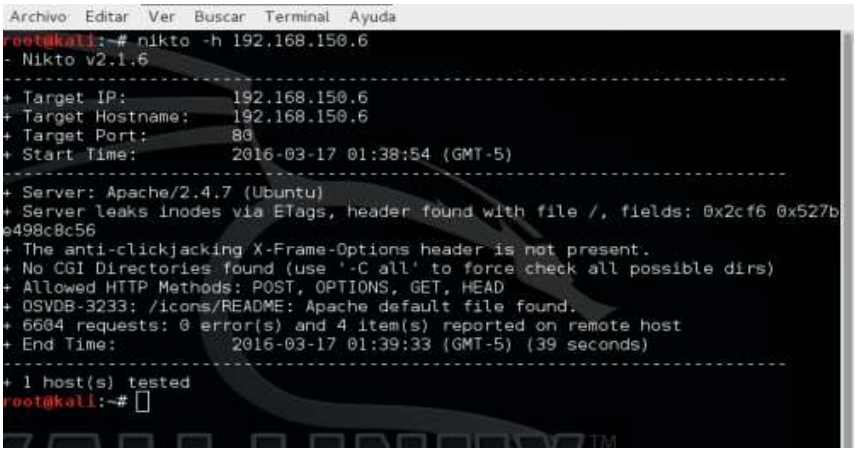


Figura XXV: Ejecución del ataque Nikto
Fuente: Autora

La regla esperada es:

SID:2677=tcp(msg:"ET SCAN Nikto Web App Scan in Progress"; flow:to_server,established; content:"(Nikto"; fast_pattern:only; http_header; pcre:"/^User-Agent\x3a[^\r\n]*?\(Nikto/Hmi"; threshold: type both, count 5, seconds 60, track by_src; reference:url,www.cirt.net/code/nikto.shtml;

reference:url,doc.emergingthreats.net/2002677;classtype:web-application-attack;)

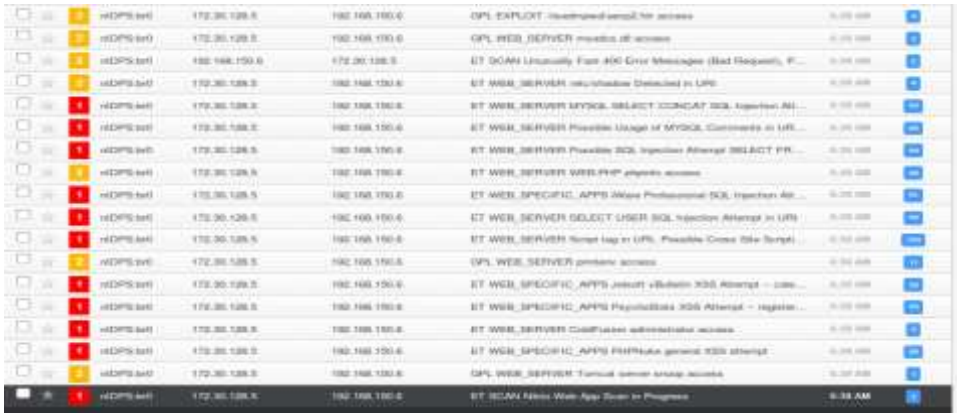


Figura XXVI: Alertas generadas por el nIDPS Suricata

Fuente: Autora

Las mismas reglas son detectadas tanto por Snort y Suricata en la figura anterior se resalta de color oscuro la regla de NIKTO en progreso. Es factible mencionar que la regla con la opción ALERT no descarta el evento y deja una puerta abierta a la ejecución de por lo menos 130 unicas reglas con una cantidad que oscila entre 1000 a 1500 alertas en cada nIDPS.

La regla correspondiente a Nikto se considera como VP es decir se tiene un 1 VP, y las reglas registradas posteriores a se catalogan de la misma manera.

Comprobacion en modo prevención de intrusiones

Como se ha mencionado anteriormente este ataque se considera como potencialmente peligroso por lo tanto se procede a ejecutar el mismo ataque que activa la misma regla pero a diferencia del caso anterior la acción de la regla se recataloga como DROP con el fin de prevenir la ejecución de este ataque. Como se ha demostrado la red de institución no restringe efectivamente.

La regla reconfigurada es:

DROP tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"ET SCAN Nikto Web App Scan in Progress"; flow:to_server,established; content:"(Nikto"; fast_pattern:only; http_header; pcre:"/^User-Agent\x3a[^\r\n]*?\(Nikto/Hmi"; threshold: type both, count 5, seconds 60, track by_src;

reference:url,www.cirt.net/code/nikto.shtml;
reference:url,doc.emergingthreats.net/2002677;classtype:web-application-attack;)

La regla en el nIDPS se filtra lo que significa que el evento es descartado. En la siguiente figura se detalla los eventos generados y la manera que el nIDPS los filtra.

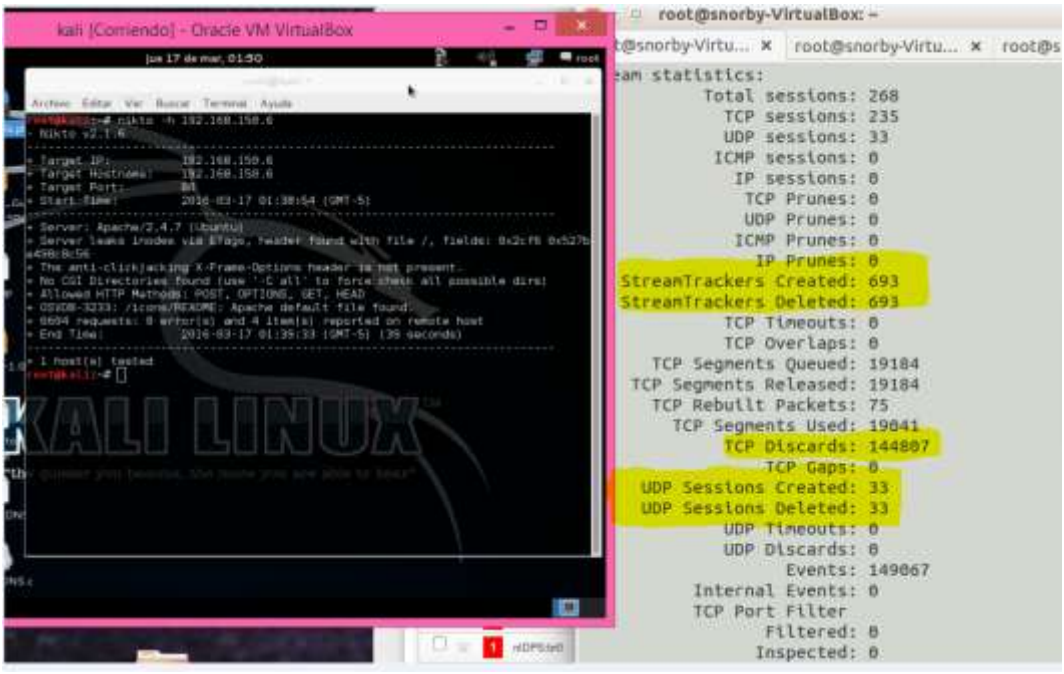


Figura XXVII: Alertas generadas y filtradas por el nIDPS
Fuente: Autora

DOS

Para realizar este ataque se utiliza la herramienta THC-Hydra, este utiliza un listado de posibles contraseñas denominado diccionario el cual puede ser creado o utilizar de alguno disponible en la red. El objetivo es buscar de un login exitoso.

TCH-Hydra intentar crackear por fuerza bruta la contraseña de varios protocolos como: TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MYSQL, REXEC,RSH, RLOGIN, entre muchos otros.

El comando utilizado en este ataque para forzar la el ingreso mediante el protocolo SSH al servidor DNS de la red de servidores es: hydra –l root –P log.text ssh://192.168.150.100

La opción –l define a un único usuario (en este ejemplo el usuario root) con el cual se comprobarán múltiples contraseñas definidas en un archivo de texto creado, la opción -P define un diccionario de posibles contraseñas.

Para ejemplificar el ataque se crea el diccionario sencillo denominado log.txt, este contiene unas 10 posibles contraseñas, la octava contraseña es la verdadera. Por lo tanto el ataque finaliza satisfactoriamente en el 8 intento de admisión.

Análisis de las reglas esperadas

El ataque de fuerza bruta debe activar dos reglas concernientes a: reconocimiento e intento de admisión, por lo tanto las reglas las reglas esperadas son:

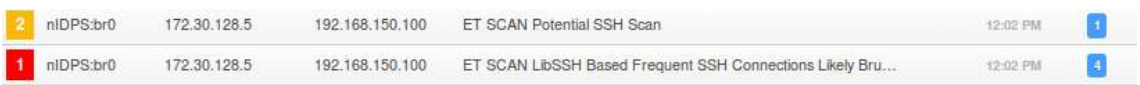
SID:2001219= tcp (msg:"ET SCAN Potential SSH Scan"; flags:S,12; threshold: type both, track by_src, count 5, seconds 120; reference:url,doc.emergingthreats.net/2001219; classtype:attempted-recon;)

SID:2006546 = ssh (msg:"ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack"; flow:established,to_server; content:"SSH-"; content:"libssh"; within:20; threshold: type both, count 5, seconds 30, track by_src; reference:url,doc.emergingthreats.net/2006546; classtype:attempted-admin;)

Es importante mencionar que la regla con SID 2006546 con Suricata se define directamente como SSH, sin embargo en Snort se define como TCP y el nIDPS analiza y registra la misma regla.

La cantidad de advertencias esperadas para la alerta con sid:2001219 es por lo menos 1 y para sid:2006546 es n número de alertas dependiendo a la cantidad de posible combinaciones de contraseña, el nIDPS contarà a partir de la quita combinación realizada debido al parámetro count 5 de la regla.

Reglas activadas con Suricata



Reglas activadas con Snort

Cantidad de alertas:

Snort: 1 reconocimiento y 1 de intento de admisión

Suricata: 1 de reconocimiento y 4 alertas de intento de admisión (4 VP)

En consideración con las reglas aceptadas como VP de Suricata. Snort no reconoce la misma cantidad de reglas por lo que es posible determinar que Snort provee 2 VP y 3 alertas catalogadas como verdaderos negativos.

Interpretación: Snort y Suricata detectan la actividad de fuerza bruta correctamente, sin embargo la cantidad de reglas esperadas y catalogadas como verdaderos positivos son: 1 para intento de reconocimiento y 4 alertas para intento de admisión tomando en cuenta el Indicador descrito anteriormente del ataque.

DOS Basado en inundación a puerto TCP/IP

Ataque inundaciones de peticiones al servidor DNS, utilizando la herramienta hping3 comprende la utilización de la siguiente línea de comandos:

La herramienta Hping3 està inspirada en el ping, manipula paquetes a través del protocolo TCP/IP, ensambla paquetes y analiza. Permite además el envìo de paquetes TCP, UPD , ICPMP Y RAW_IP.

Los parámetros utilizados en los ataques tienen las siguientes funciones:

–rand-source permite realizar una serie de ping únicos modificando la dirección IP origen.

–S activa el flag Syn

-p puerto

–flood permiten enviar paquetes en tiempo real de manera masiva

-i u1000 segundos de intervalo (ux=µsegundos)

Hping3 –rand-source –S –p 53 –flood 192.168.150.100

```
ot@kali:~# hping3 -p 53 -S --rand-source --flood 192.168.150.100
ING 192.168.150.100 (eth0 192.168.150.100): S set, 40 headers + 0 data bytes
ing in flood mode, no replies will be shown
```

Figura XXVIII: Ejecución del ataque de inundación al puerto DNS utilizando Hping3

Fuente: Autora

El comportamiento de la red muestra peticiones al puerto 53 y ausencia o invalidez de ACK, por lo tanto las reglas esperadas deben referirse a los parámetros (ICMP Y ACK).

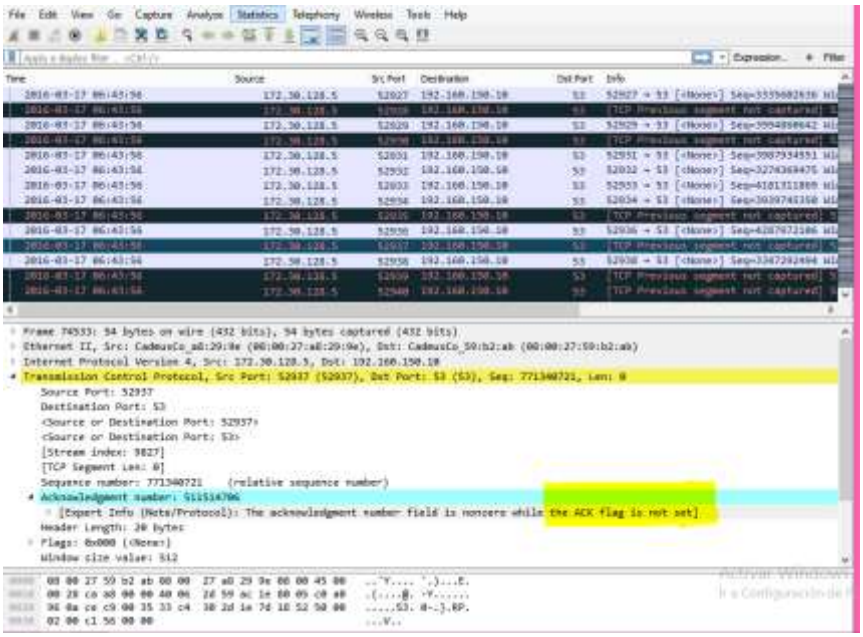


Figura XXIX: Comportamiento de la red durante el ataque de inundciòn al puerto53 utilizando Hping3

Fuente: Autora

Los parámetros resaltados muestran las anomalías encontradas durante el ataque en progreso. Los nIDPS registran las siguientes reglas:

N. Sensor	Direccion IP origen/destinno	Descripción de la regla	Horario	Num. Alertas
Alerta registradas por Suricata:				
3 nIDPS:br0	192.168.150.55	172.30.128.5	SURICATA STREAM Packet with invalid ack	1:14 PM
3 nIDPS:br0	192.168.150.55	172.30.128.5	SURICATA STREAM SHUTDOWN RST invalid ack	1:14 PM
Alertas registradas con Snort				

Figura XXX: Alertas generadas por el nIDPS Suricata y Snort para el ataque de Inundación con Hping3

Fuente: Autora

Reglas registradas

SID: 486= icmp (msg:GLP ICMP_INFO DestinationUnreachable Communication with Destination Network is Admministratie Prohibited; classtype:misc-activity)

SID:2210046= tcp (msg:"Stream Shutdown RST invalid ack"; stream-event:rst_invalid; classtype:protocol-command-decode;)

SID:2210045= tcp (msg:"Stream packet with invalid ack"; stream-event: pkt_invalid_ack; classtype:protocol-command-decode;)

Interpretación: Suricata es la única que registra acontecimientos referidos a las malformaciones de peticiones ACK y respuestas RST, que de acuerdo al análisis realizado con Wireshark las alertas se consideran como VP. También se consideran como VP a la regla con SID:486 puesto al inicio de ataques si se realiza una escaneo de ICMP.

Snort solo registra alertas del escaneo ICMP las cuales son consideradas como VP, sin embargo claramente muestra mal definidas los parámetros de IP origen/destino. Por lo tanto todas las alertas referidas hacia direcciones IP que no sean explicitas a la IP de la estación atacante interna serán consideradas como FP.

Snort sid: SID: 486 (VP: 24), SID:2210046 (VP: 0) y SID:2210045 (VP:0)

Suricata sid: SID: 486 (VP:24, FP:4), SID:2210046(VP: 10) y SID:2210045(VP: 10)

Tabla 12: Descripciòn de intrusiones detectadas en el ambiente de pruebas para ataque DOS y Monitorizaciòn

SID	Clasificación	Descripción	Regla coincidente	Snort	Suricata

				VP	FP	VP	FP
sid:469	bad-unknown	172.30.128.5 -> 192.160.150.100 172.30.128.5 -> 192.160.150.55	GLP Scan Ping Nmap	9		9	
sid:582	bad-unknown	172.30.128.5 -> 192.160.150.100 172.30.128.5 -> 192.160.150.55	GLP Scan Nmap –sS Windows 1024	9		9	
Sid 538	bad-unknown	172.30.128.5 -> 192.160.150.100 172.30.128.5 -> 192.160.150.55 Varios puertos dest	GLP Scan Nmap –sA (-1)		1		1
:2677	web-application-attack	192.169.128.5 -> 192.160.150.6	ET SCAN Nikto Web App Scan in Progress	1		1	
sid: 1219	attempted-recon	192.169.128.5 -> 192.160.150.100	ET SCAN Potential SSH Scan	1		1	
sid: 6546	attempted-admin	192.169.128.5 -> 192.160.150.100	ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack	1		5	
Sid:486	misc-activity	192.169.128.5 -> 192.160.150.100 192.169.128.5 -> 192.160.150.55	GLP ICMP_INFO DestinationUnreachable Communication with Destination Network is Admministratie Prohibited	24		24	4
Sdi: 0046	protocol-command-decode	192.169.128.5 -> 192.160.150.100 192.169.128.5 -> 192.160.150.55	Stream Shutdown RST invalid ack"; stream-event:rst_invalid; classtype:protocol-command-decode;)			10	
sid:10045	web-application-attack	192.169.128.5 -> 192.160.150.100 192.169.128.5 -> 192.160.150.55	Stream packet with invalid ack"; stream-event: pkt_invalid_ack; classtype			10	
TOTAL				45	1	69	5

Fuente: Autora

Interpretaciòn: Tanto Snort y Suricata prometen un buen desempeño en detectar ataques de monitorización con un resultado de 97% para Snort y 090% Para Suricata.

5.5.2. Procesamiento y análisis del indicador de la variable dependiente

La variable dependiente concerniente a la investigación está representado: por la cantidad de intrusiones detectadas en la red de datos de la UNACH.

Como se menciono mediante una figura anterior los Verdaderos positivos (VP): representan las intrusiones detectadas o prevenidas cuantificables en la que la actividad es intrusiva y es detectada correctamente. Los Falsos positivos (FP): intrusiones detectadas o prevenidas cuantificables representa que la actividad no es intrusiva y se indica como tal, es decir estas alertas no representan peligro para la seguridad. Las siglas VP y FP serán utilizadas a partir de esta sección.

La complejidad que representa clasificar una alerta detectada como VP o FP implica analizar exhaustivamente la información recabada por el nIDPS y volcada en el o los módulos de salida activados. En el momento de utilizar o activar cada regla o conjunto de reglas es necesario tener motivos fundamentados y claros de uso, por otra parte algunas reglas, específicamente las que no son sustentadas por organismos de seguridad suelen presentarse con grandes números predecesores característicos de las alertas FP.

El análisis pertinentemente influirá en tomar medidas como desctivar la regla, reafinar la regla a nuestro entorno o eliminar la regla, hay que tener en cuenta que una regla con decenas o centenas de apariciones puede enmascarar un problema mucho más severo o efectivamente FP.

Los criterios personalmente propuestos son:

- Priorizar el análisis a las alertas de intrusiones que estén sustentadas y referenciadas a los organizamos de vulnerabilidades como CVE y Security Focus.
- Priorizar el análisis a las alertas detectadas que estén catalogadas como prioridad 1 o 2. (classification.conf)
- Comprender la regla de la alerta generada.
- Observar directamente las alertas en el fron-end. Para descartar direcciones y puerto origen-destino que o pertenezcan a nuestra red.
- Verifcar que las alertas con payload (efectivamente cuenten con este)

- Verificar mediante herramientas adicionales los archivos de salida (pcap, unified2, log y de manera general alertas en texto plano). Los pcap se los puede visualizar directamente con Wireshak o Frameworks forenses (Network Miner, xplico u otro que maneje) los log con herramientas de auditoria sysloy y los unified2 como se mencionó antes para almacenar en la BBDD del front-end.
- Reensamblar los archivos pcap dudosos con herramientas que permitan de cierto modo visualizar el proceso de negociación mediante gráficas o herramientas de análisis forense de redes (NFAT)
- Personalmente se sugiere se utilizar entornos de seguridad más completos como las plataformas NMS o SIEM que unifican en un sólo sistema varias herramientas de seguridad.

Para esta investigación se utilizó de Security Onion que si bien no automatiza un informe final, aporta con información valiosa para clasificar las intrusiones como VP, FP e inclusive como FN.

Primer ambiente: con fuente de datos trafico de la red UNACH

El procesamiento consiste en retransmitir el tráfico capturado (archivo pcap) en el escenario de simulación desde el dispositivo firewall hacia la red de servidores. La herramienta utilizada es tcpreplay y el comando es: tcpreplay –intf1=eth1 <hora1.pcap>. La interfaz eth1 corresponde de acuerdo al esquema del escenario de simulación a la interfaz de conexión firewall/red de servidores. Otra manera es que individualmente el nIDPS Snort y Suricata admitan leer y procesar a los archivos pcap directamente (análisis pasivo), esto se logra mediante la opción –pcap-single o –r (modo abreviado) seguido de la ubicación local del archivo.

La siguiente imagen detalla al módulo colector de alertas Barnyard2 en funcionamiento y corresponde al proceso de almacenamiento de los archivos de salida de Suricata (unified2) para la visualización con Snorby.

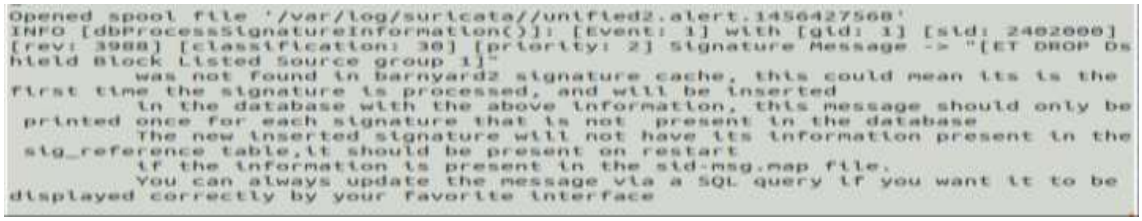


Figura XXXI: Funcionamiento de Barnyard2 con Suricata
Fuente: Autora

Nótese que los archivos de salida en Suricata se configuraron con el nombre unified2.alert, el número seguido representa time_stamp que es el identificador que corresponde a fecha y hora de las alertas dado por la herramienta nIDPS.

Los resultados obtenidos tras el procesamiento son presentados en la tabla siguiente:

Tabla 13: Intrusiones detectadas con Suricata en el primer escenario

	Paquetes leídos/bytes	**Mòdulo de salida (unified2, syslogy +)**	**Número de ataques o intrusiones detectados**
Hora 1	6033/471504	unified2.alert 1456452835	67
Hora 2	5690/454021	Unified2.alert.1456453223	55
Hora 3	36742/3383317	Unified2.alert.1456454339	39
Totales			161

Fuente: Autora

La siguiente imagen corresponde al front-end Snory con Suricata en funcionamiento.

Figura XXXII: Funcionamiento de Snorby con el nIDPS Suiricata
Fuente: Autora

El proceso en Snort comprende el mismo descrito para Suricata correspondiente la retrasmisión de tráfico. Los siguientes comandos muestran la utilización de archivos pcap como fuente de datos directa: snort –c /usr/local/etc/snort/snort.conf –r hora1.pcap, de la misma manera se repite el proceso para hora2 y hora3.pcap.

La ejecución del modulo colector de alertas Barnyard2 se muestra en la siguiente figura. El nombre configurado para el tipo de salida unified2 en Snort es snort.log.

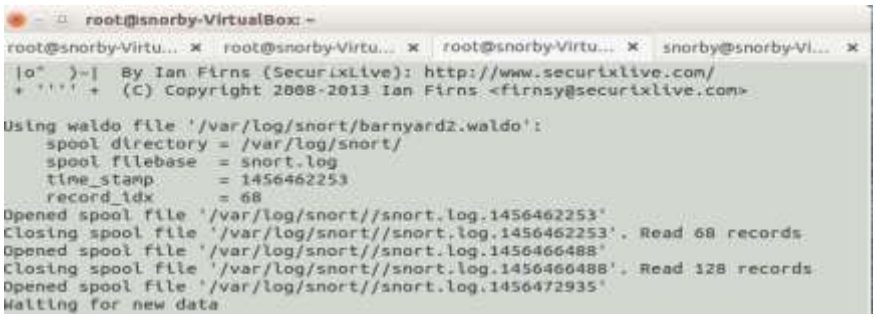


Figura XXXIII: Funcionamiento de Barnyard2 con Snort
Fuente: Autora

Los resultados obtenidos tras el procesamiento son descritos mediante la tabla siguiente.

Tabla 14: Intrusiones detectadas con Snort en el primer escenario

	Paquetes leídos/bytes	**Modulos de salida (Unified2, pcap,log,+)**	**Número de ataques o intrusiones detectados**
Hora 1	6033/471504	snort.log.145644232	60
Hora 2	5690/454021	snort.log.1456458524	25
Hora 3	36742/3383317	snort.log.1456454339	25
Totales			110

Fuente: Autora

5.5.2.1.1. Interpretacion de alertas activadas

El total de reglas únicas activadas son 10, el número de alertas varía en función de cada evento. En esta sección se analiza las reglas más notables para catalogarlas como verdaderos positivos o falsos positivos son:

Para: alert udp any 53 -> $HOME_NET any (msg:"ET DNS Excessive NXDOMAIN responses
- Possible DNS Backscatter or Malware Domain Generation Algorithm DNSLookups"; byte_test:1,&,128,2; byte_test:1,&,1,3; byte_test:1,&,2,3;threshold: type both, track by_src, count 50, seconds 10; reference:url,doc.emergingthreats.net /bin/view/Main/2008470; classtype:bad-unknown;sid:2008470; rev:5;)
Para comprender la regla se procede a detallar las partes que las integran, es decir, el headers (la cabecera) y options (opciones presentes).

Rule headers: la cabecera comprende: alert udp any 53 -> $HOME_NET any. El tipo de acción definida es “alertar”, el protocolo de red analizado es UDP, regla refiere a los eventos procedentes de la red externa o cualquiera “any” en el puerto 53 direccionados “->” a la red monitorizada en este caso a la red de servidores en cualquier puerto destino.

Rule options: las opciones de la regla compreden:

- msg: mensaje a imprimir
- byte_test: comprueba un campo de byte contra valores específicos
- threshold: umbrales lógicos admitidos
- reference: referencias de la regla en este caso el url de Emerging Threats (ET)
- classtype: categorización de la regla.
- sid: identicador de regla “2008470”
- rev: revisiones de la regla.

El mensaje es “ET DNS respuestas excesivas de NXDomain- Posible retrodispersión de DNS o algoritmo de generación de dominio DNS por Malware” los parámetros que activan la regla son:

Byte_test: esta opción se incluye en la categoria payload detection (carga útil) y permite comprobar valores específicos binarios o convertir cadenas de bytes a sus equivalentes binarios. La sintanxis es:

byte_test:<bytes to convert>, [!]<operator>, <value>, <offset>

Donde los bytes a convertir toman valores de 1 a 10, el operador lógico utilizado es “and” representado por “&”, valor calculado toma al intervalo 1 a 4294967295 (2^{32} máximo valor binario) y la offset (desviación) toma valores entre -65535 a 65535 (umbral de valores para el tamaño de paquetes IP) que significan el número de bytes dentro de payload para iniciar a procesar. La opción de la regla byte_test:1,&,128,2; corresponde a realizar un seguimiento y comprobación de byte que lea el byte 1 a partir del byte 2 dentro del paquete, lo convierte a un número y se asegure que no sea muy grande es decir valor de 128.

Threshold: el parámetro umbral es una parte integral de esta regla, se definen los parámetros both para analizar los eventos ocurridos en un intervalo de tiempo n y verificar las apariciones del suceso para únicas direcciones IP de origen. En 10 segundos se registran por lo menos 50 peticiones coincidentes.

classtype: la clasificación de la alerta es malo-desconocido. En el archivo classification.conf la descripción corresponde a “Potentially Bad Traffic” con un nivel de gravedad de 2.

rev:5 representa el número revisiones o refinamiento de la regla, es decir que la regla se ha modificado unas 5 veces, este número está estrechamente ligado con la actualización de la regla.

Para validar y aceptar esta regla como verdadero positivos se realiza un análisis del tráfico. La figura siguiente muestra la comprobación de eventos referentes a la activación de la regla.

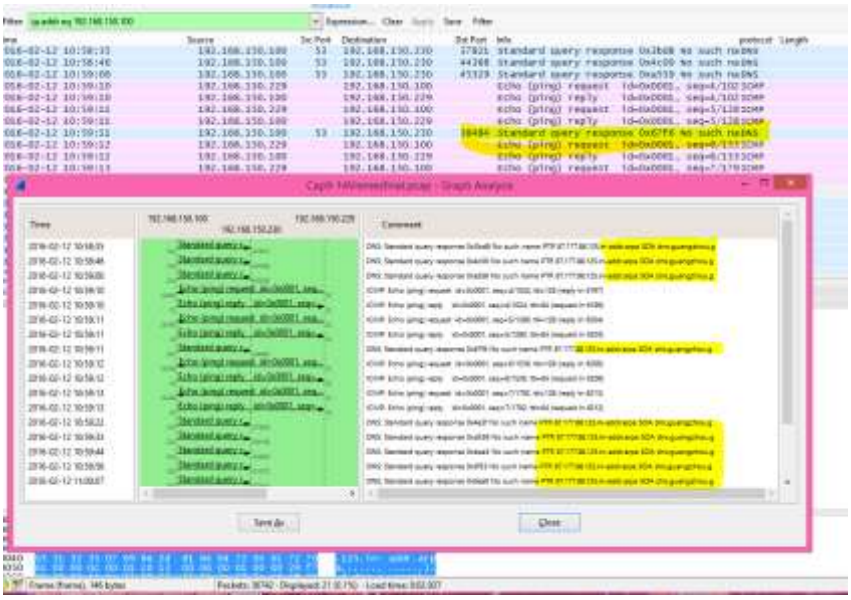


Figura XXXIV: Análisis de peticiones DNS en el trafico capturado utilizando Wireshark

Fuente: Autora

Con base a la investigación y verificación anterior las reglas se aceptan como verdaderos positivos.

Snort y Suricata detectan la regla con sid:2200094 está activa conjuntamente la regla sid:2200029, ambas determinan errores de longitud zero de las direcciones IPV6, considerando que no son objeto de estudio y que para comprobarlas necesitaríamos un escenario implementado con IPV6 no disponible en esta investigación, estas se reconocen como verdaderas.

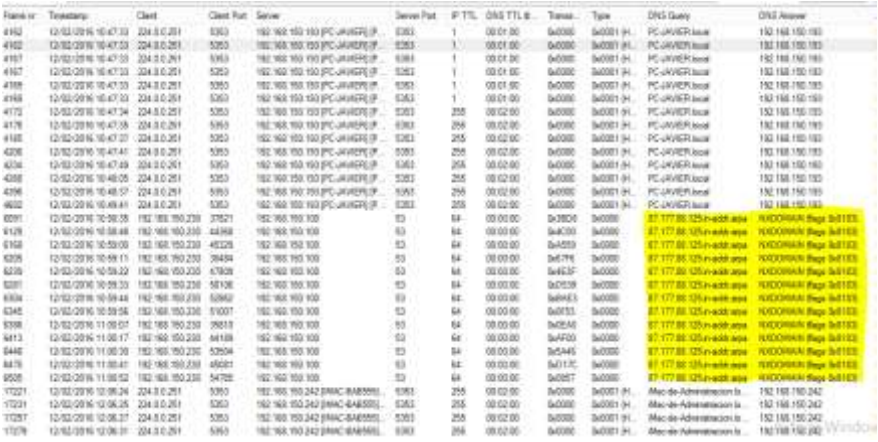


Figura XXXV: Análisis de peticiones DNS no sospechosas en el trafico capturado utilizando Network Miner

Fuente: Autora

Para: alert udp $DNS_SERVERS 53 -> any any (msg:"ET DNS Standard query response, Name Error"; pcre:"/..[\x81\x82\x83\x84\x85\x86\x87]\x83/"; reference:url,doc.emergingthreats.net/2001117; classtype:not-suspicious; sid:2001117; rev:5;)

Rule headers: la cabecera comprende: alert udp $DNS_SERVERS 53 -> any any. El tipo de acción definida es “alertar”, el protocolo de red analizado es UDP, regla refiere a los eventos procedentes de la o las direcciones IP definidas como Servidor DNS en el puerto 53 direccionados hacia“->” a la red externa o cualquier red no coincidente con la red protegida en cualquier puerto destino.

Rule options: las opciones de la regla comprende:

- msg: mensaje a imprimir“ET DNS Standard query response, Name Error”.
- pcre: conjunto de funciones de coincidencia de expresiones compatibles de Perl.
- reference: referencias de la regla en este caso el url de Emerging Threats (ET)
- classtype: categorización de la regla “not-suspicious” no sospecho
- sid: identicador de regla “2001117”
- rev: revisiones de la regla (5 veces)

El classtype: se cataloga como y se cataloga con un nivel de gravedad de 3 de acuerdo al archivo classification.conf. La figura anterior es utilizada para validar la regla sid:2001117 que Snort y Suricata clasifican como eventos no sopechosos, la regla es tomada como Falso positivo debido a que no representa mayor peligro. Puesto el proceso se denomina peticiòn inversa 0.168.192.in-addr.arpa con el dominio especial in-addr.arpa, además de acuerdo al horario de petición inversa hay un rango de 6 a 8 minutos.

Regla: udp (msg:"ET DNS Standard query response, Name Error"; pcre:"/^..[\x81\x82\x83\x84\x85\x86\x87]\x83/";
reference:url,doc.emergingthreats.net/2001117;)

Existe una regla que solo activa Suricata (Sid:2400004), esta monitoriza el protocolo TCP en busca eventos de peticiones anormales en la que se encuentran

el flag ECN (notificación de congestión explicita) y CWR (congestión de ventana reducida), ambos flag están diseñados para tener más poder de procesamiento de paquetes habituales y por lo tanto se utilizan comúnmente en ataques de denegación de servicio. En la figura se encuentran resaltados los parámetros sobre la negociación de servicio al puerto 8080.

alert ip [91.215.136.0/23,91.216.3.0/24,91.217.10.0/23,91.220.35.0/24,91.220.62.0/24,91.220.163.0/24,91.223.89.0/24,91.226.97.0/24,91.229.210.0/24,91.230.110.0/24,91.230.252.0/23,91.234.36.0/24,91.235.2.0/24,91.236.74.0/23,91.236.120.0/24,91.236.213.0/24,91.237.198.0/24,91.238.82.0/24,91.239.24.0/24,91.239.238.0/24] any -> $HOME_NET any (msg:"ET DROP Spamhaus DROP Listed Traffic Inbound group 5"; reference:url,www.spamhaus.org/drop/drop.lasso; threshold: type limit, track by_src, seconds 3600, count 1; classtype:misc-attack; flowbits:set,ET.Evil; flowbits:set,ET.DROPIP; sid:2400004; rev:2528;)

Descripción: El tipo de alerta es DROP las direcciones de origen son publicas y pertenecen a un sitio web de Spamhaus que refieren a herramientas para realizar ataques “Hijacked” a a router el puerto de respuesta receptiva es cualquier puerto y la variable $HOME_NET es la red monitorizada de igual manera hacia cualquier puerto. La regla catalogada como de mala reputación (reputación IP), además la alerta se activa cuando la coneccion de haya establecido 6 minutos. El parámetro Flowbits refiere a un intercambio de datos no solicitados por lo que la lerta se activa.

A pesar que la regla está presente en Snort, este no detecta ni registra.

Las configuraciónes son idénticas en los dos nIDPS por lo tanto se infiere que Snort no monitoriza esta intrusión.

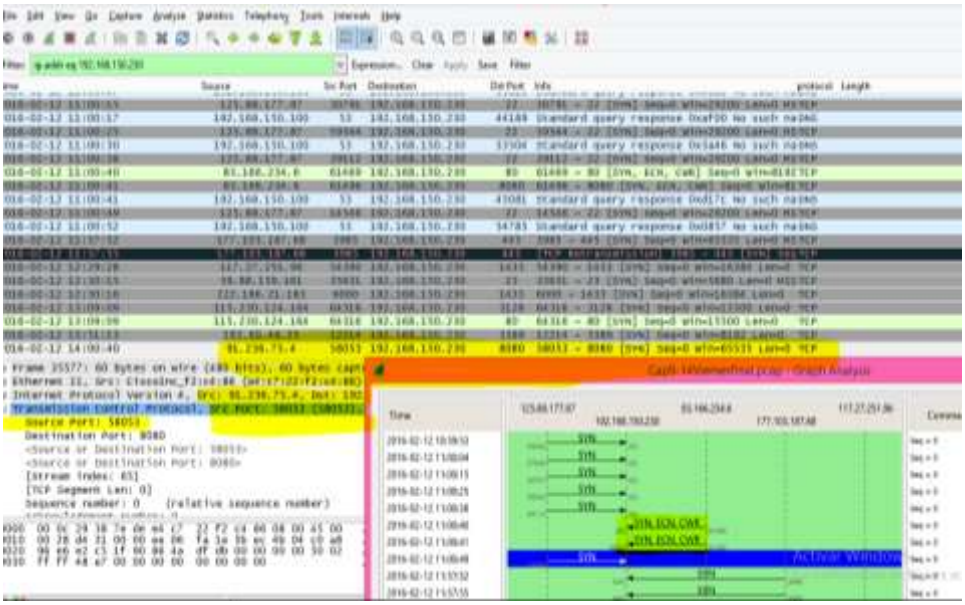


Figura XXXVI: Análisis de peticiones HTTP en el trafico capturado utilizando Wireshark

Fuente: Autora

Se observan múltiples peticiones concurrentes de inicio de sesión para la conexión TCP, enbebidas con las peticiones ECN Y CWR.El Syn tiene valor por llot tanto la Como se puede ver en la toma, tenemos los siguientes datos en los campos del encabezado TCP: Source port: puerto de origen 64316, el cliente recibe las espuestas en este puerto. Destination port: puerto de destino 80, es a donde se envía la solicitud del cliente. bit SYN: El bit SYN encendido, es utilizado para iniciar el saludo de tres vías o “Three-Way Handshake”. Que en otras palabras es decirle al servidor web que deseamos conversar con él. Sequence number: ISN (Initial Sequence Number) número de secuencia inicial del cliente con 1 y con FIN de 0.

Tras el análisis se realiza una tabla general en la que mencionan la cantidad de alertas detectadas por los nIDPS y clasificadas como verdaderos positivos (VP) o falsos positivos (FP).

Tabla 15: Descripciòn de intrusiones detectadas en la red de datos institucional

SID	Clasificación	Descripción	Regla coincidente	Snort						Suricata					
				H1		H2		H3		H1		H2		H3	
				VP	FP	VP	FP	VP	FP	VP	FP	VP	FP	VP	FP
sid:2200094	Null	Direcciones IPV& 0::143 – ff022::16:0 Fe80::e920:7448:c842:c842:ddee:143 -> ff02::16:0 F562:bb16:3290:bb3d :546 -> ff02::1:2:547	IPv6-icmp msg:"Zero length padN option" (IPV6) IPV6-iCMP msg: “ICMP6 unknown type” sid:2200029	21		8		8		21		8		8	
Sid:2008 470	bad-unknown (prioridad 2)	192.168.150.230:54785 192.168.150.100:80 (múltiples puertos)	udp (msg:"ET DNS Excessive NXDOMAIN responses - Possible DNS Backscatter or Domain Generation Algorithm Lookups";	13						13					
Sid 24020000	misc-activity (prioridad 2)	183.60.48.25:12214 ->192.168.150.230:3389 64.125.239.204:57831 ->192.168.150.230:80	Tcp msg:"ET DROP Dshield Block Listed Source group 1	2				5		2		1		5	

Sid:20011 17	Not suspicuos (prioridad 3)	192.168.150.100:53 -> 192.168.150.230:54785(Puertos de destino)	Msg("El DNS Stndard query response, Name Error")		12		2				12		2		
sid:2 4033 22	misc-attack (prioridad 2)	64.125.239.27:50214 -> 192.168.150.137:80	msg:"ET CINS Active threat intelligent poor reptutation IP TCP group 12							9		12			
Sid:24 00004	misc-activity (prioridad 2)	91.236.75.4:58053 ->192.168.150.230:8080	tcp (msg:"ET DROP Spamhaus DROP Listed Inbound group 5)							1					
Sid:24033 58	Misc-attack (prioridad 2)	64.125.239.204:57831 -> 192.168.150.223:80 64.125.239.235 -> 192.168.150.235:80	"Et CINS Active Threat intelligent Poor Reputation Ip TCP"							1					1
sid:2009 714	web-application-attack	172.30.128.5:56999 192.159.159.6:80	http (msg:"ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt")	3		9		15		3		9		16	
sid:2009 714	web -application-attacks	172.30.128.5:56999 192.159.159.6:80	http (msg:"ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt)	4		6		5		6		8		6	
sid:2 1009 81	web-application-attack	1.1.1.11:6851 192.168.150.55:27876	http (msg:"GPL EXPLOIT unicode directory traversal attempt"; flow:to_server,established;)	1	4			3		5		26		15	
TOTAL				45	16	23	2	36	0	61	12	64	2	50	1

Fuente: Autora

CAPÍTULO VI

RESULTADOS Y DISCUSIÓN

6.1.RESULTADOS

6.1.1. Análisis de los resultados obtenidos

El proceso de realiza tanto para la variable dependiente como para la independiete, en la variable independiente el análisis concierne a las intrusiones encontradas con las dos herramientas, por lo tanto el proceso se realiza con el escenario de simulación con fuente de datos de la UNACH.

INDICADOR 1:

Los resultados de la evaluación teórica en función de los valores se represetan de la siguiente figura.

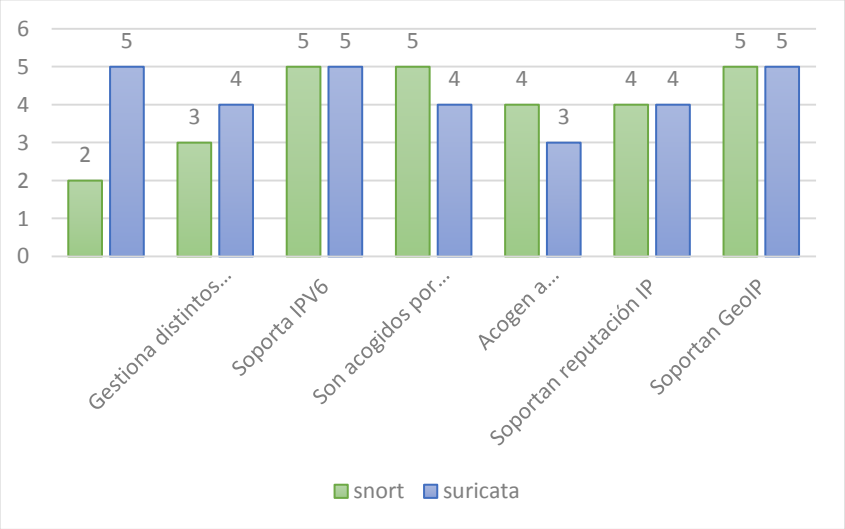


Figura XXXVII: Resumen evaluaciòn del indicador 1
Fuente: Autora

El promedio resultado de la evaluación es: 4 puntos para Snort y 4,29 para Suricata.

Cabe mencionar que es un estudio teorico, sustentado principalemente por los sitios web oficiales de las herramientas nIDPS open source. En el aparatado de Anexos se adjunta imágenes sobre el criterio de: Soporte GEOIP y sistemas acoplamientdo a sistemas de seguridad utilizando Security Onion como (NSM).
Finalmente de acuerdo a los resultados porcentuales y generales obtenidos de 8 aspectos englobados en 3 criterios se estipula que: Suricata es la solución más prometedora con un porcentaje total de 87,5% frente a 83.75 % de Snort. La diferencia de los resultados generales evaluados teóricos entre Snort y Suricata es sutil.

INDICADOR 2: Desempeño

Los resultados obtenidos de este indicador, de acuerdo a las pruebas realizadas corresponde al total del paquete 220452 (100%) y la cantidad esperada de intrusiones detectadas y prevenidas para Snort es 110 y 161 para Suricata.

Tabla 16: Descripciòn de evaluaciòn del indicador 2

Pruebas a:	Snort			Suricata		
	Paq total	Porc. Perdidos	Intr.	Paq total	Porc. Perdidos	Intru.
En tiempo real	220452	0%	110	220452	0%	161
mbps500	220452	0%	110	220452	0%	161
mbps800	220452	0%	110	220452	0%	161
mbps1100	198421	9%	91	15431	7%	149
+mbps1100	18067	15%	76	28658	17%	126

Fuente: Autora

La tabla anterior describe que las herramientas en ambientes con ancho de banda considerable sufren pérdidas de paquetes. Sin embargo se observa que bajo el mismo trafico de red, Snort detecta un número menor de intrusiones. Lo indicado sería que las herramientas no pierdan paquetes. Snort por su parte es más ligero, en ambientes con ancho de banda considerables tiende a dejar pasar paquetes de red sin monitorizar lo cual en consideración a la posibilidad de descartar o eliminar los paquetes es la solución óptima en un estado inline. A Suricata le toma más tiempo procesar la misma información pese a su características de multihilos.

Para valorar se considera a Suricata con un desempeño regular. En el quinta prueba con ancho de banda mayo a un Mb.

El rendimiento de las herramientas nIDPS en diferentes anchos de banda es:

Tabla 17: Resumen evaluaciòn del indicador 2

Pruebas a:	Snort			Suricata		
	Paq total	Porc Perdidos	Intr.	Paq total	Porc Perdidos	Intru.
En tiempo real	220452	0%	110	220452	0%	161
mbps500	220452	0%	110	220452	0%	161
mbps800	220452	0%	110	220452	0%	161
mbps1100	19842	9%	91	15432	7%	149
+mbps1100	33068	15%	76	37477	17%	126

Fuente: Autora

Para su valoración se describe la siguiente tabla.

Tabla 18: Resumen evaluaciòn del indicador 2

Prueba en:	Snort		Suricata	
	Cualidad	**Cuantitativo**	**Cualidad**	**Cuantitativo**
En tiempo real	Satisfactorio	5	Satisfactorio	5
mbps500	Satisfactorio	5	Satisfactorio	5
mbps800	Satisfactorio	5	Satisfactorio	5
mbps1100	Aceptable	3	Aceptable	3
+mbps1100	Aceptable	3	Regular	2

Fuente: Autora

INDICADOR 3: Seguridad

Con respecto al rendimiento se realiza los mismo calculos

Tabla 19: Cantidad total de intrusiones detectas por Snort y Suricata

	Número total de intrusiones detectados	
	Con Snort	**Con Suricata**

Hora 1	60	67
Hora 2	25	55
Hora 3	25	39
Totales	110	161

Fuente: Autora

A continuación se muestra mediante una figura la representación de la tabla sobre el número de intrusiones detectadas para los nIDPS Snort y Suricata.

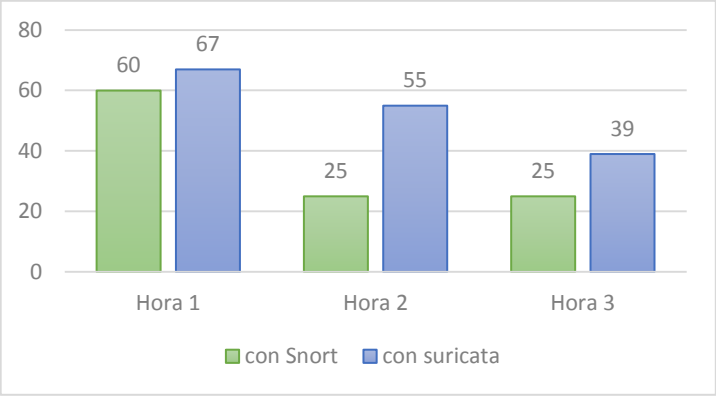


Figura XXXVIII: Distribuciòn del total de intrusiones detectas de acuerdo a los 3 archivos capturados

Fuente: Autora

De la cantidad de intrusiones con el nIDPS Snort y Suricata detalladas como intrusiones verdaderos positivos (VP) y falsos positivos (FP) con respespecto a tres horarios distintitos.

Tabla 20: Cantidad de intrusiones detectas por Snort y Suricata contanto los VP y FP

	Con Snort		**Con Suricata**	
	VP	**FP**	**VP**	**FP**
Hora1	44	16	55	12
Hora 2	23	2	53	2
Hora 3	25	0	38	1
Totales	**92**	**18**	**146**	**15**

Fuente: Autora

Los resultados de la sensibilidad se calculan de: TVP/(TVP+TFP) para Snort es: 0,836 y 0,91 para Suricata. En valores porcentuales es: 83% y 91% respectivamente.

6.1.2. Comprobación de la hipótesis

La verificación de la hipótesis se realiza con la prueba estadistica T-Student de dos colas, debido a que el estudio se centra en las dos herramientas y existen dos conjuntos de datos con muestras menores a 30.

- Hipótesis de investigación “hi”

La utilización de la herramienta nIDPS open source Suricata brinda mejores prestaciones que la herramienta nIDPS open source Snort para detectar y prevenir las intrusiones en la red de datos de la UNACH.

- Hipotesis de investigación “h0”

La utilización de la herramienta nIDPS open source Suricata no brinda mejores prestaciones que la herramienta nIDPS open source Snort para detectar y prevenir las intrusiones en la red de datos de la UNACH.

Nivel de significancia

Luego de haber establecido las hipótesis tanto de investigación como la nula se debe determinar el nivel de significancia, para el caso de este análisis se ha utilizado un nivel de 5% (0,05) para la obtención de un nivel de confianza que se considere aceptable.

Con respecto a las funciones

Los datos numéricos a utilizar son:

Tabla 21: Datos numèrico para el indicador 1

	Snort	Suricata
Criterio 1	2	5
Criterio 2	3	4
Criterio 3	5	5
Criterio 4	5	4

Criterio 5	4	3
Criterio 6	4	4
Criterio 7	5	5

Fuente: Autora

Para comprobar la hipótesis se utiliza la formula general:

$$t = \frac{\bar{X} - \bar{Y}}{\sqrt{\frac{(n-1)S_1^2+(m-1)S_2^2}{n+m-2}}\sqrt{\frac{1}{n}+\frac{1}{m}}}$$

Donde

n=7

m=7

Factor nivel de confianza ∞=0.05

X= promedio de ataques detectados

Y= promedio de ataques detectados

S1= covarianzas muestrales de con Snort

S2= covarianzas muestrales de con Suricata

Cálculos de las covarianzas S1 y S2 se realizan de acuerdo a la siguiente formula:

$$S_1 = \frac{1}{n}\sum_{i-1}^{n}(X_1 - \bar{X})^2$$

Los cálculos son

Media	4	4,28571429
Varianza	1,33333333	0,57142857
Observaciones	7	7
Varianza agrupada	0,95238095	
Diferencia hipotética de las medias	0	
Grados de libertad	12	
Estadístico t	-2,54772256	
P(T<=t) una cola	0,29696205	
Valor crítico de t (una cola)	1,78228756	
P(T<=t) dos colas	0,59392409	

Valor crítico de t (dos colas)	2,17881283

Interpretación:

Valor de la tabla de t-Student Tcritico =2,17 se encuentra en Anexos.

Si ($T_{obtenida}$)> ($T_{critico}$) se rechaza la H_0.

La t Student calculada es de -2,54 y la de la tabla tabulada (crítica) a 12grados de libertad es 2,17 y un nivel de significancia de 0,05, por tanto se desecha la hipótesis nula y se acoge la hipótesis del trabajo. En la sección anexos se detalla la tabla de T-student

- 

  - -2,17 x 2.17

La $T_{obtenida}$ >$T_{critica}$ se rechaza H0 y se acepta Hi.

-2,54 es > 2,17 o -2,17 cae en la zona de rechazo de Ho y se acepta Hi

Hi= La utilización de la herramienta nIDPS open source Suricata brinda mejores prestaciones que la herramienta nIDPS open source Snort para detectar y prevenir las intrusiones en la red de datos de la UNACH.

Con respecto al desempeño

Los datos nùmericos a utilizar son:

Tabla 22: Datos numèrico para el indicador 2

	Snort	Suricata
En tiempo real	5	5
mbps500	5	5

mbps800	5	5
mbps1100	3	3
+mbps1100	3	2

Donde:

n y m son 5

GL =8 resultado de (n+m-2)

Los resultados obtenidos son:

	Variable 1	*Variable 2*
Media	4,2	4
Varianza	1,2	2
Observaciones	5	5
Varianza agrupada	1,6	
Diferencia hipotética de las medias	0	
Grados de libertad	8	
Estadístico t	0,25	
P(T<=t) una cola	0,404443723	
Valor crítico de t (una cola)	1,859548038	
P(T<=t) dos colas	0,808887445	
Valor crítico de t (dos colas)	2,306004135	

Interpretación:

Valor de la tabla de t-Student Tcritico =2,30 se encuentra en Anexos.

Si ($T_{obtenida}$)> ($T_{critico}$) se rechaza la H_0.

La t Student calculada es de 0,25 y la de la tabla tabulada (crítica) a 8 grados de libertad es 2,30 y un nivel de significancia de 0,05, por tanto se desecha la hipótesis nula y se acoge la hipótesis del trabajo. En la sección anexos se detalla la tabla de T-student

- 

- 2,30 x 2.30

La $T_{obtenida} > T_{critica}$ se rechaza H0 y se acepta Hi.

0,25 es > 2,30 o -2,30 cae en la zona en la que se aceptación de la Ho.

Hi= La utilización de la herramienta nIDPS open source Suricata no brinda mejores prestaciones que la herramienta nIDPS open source Snort para detectar y prevenir las intrusiones en la red de datos de la UNACH.

Con respecto a la seguridad

Se puede evaluar simplemente los valores obtenidos para la sensibilidad de Snort y Suricata. La conclusión será Suricata brinda mejores prestaciones. Se cree convenientes realizar un cálculo sobre los resultados obtenidos con Snort y Suricata de intrusiones VP.

Tabla 23: Tabla resumen de la cantidad intrusiones VP detectados con Snort y Suricata

	No. Intrusiones detectadas como VP	
	con Snort	**con Suricata**
Hora1	44	55
Hora 2	23	53
Hora 3	25	38

Fuente: Autora

Para comprobar la hipótesis se utiliza la formula general:

$$t = \frac{\bar{X} - \bar{Y}}{\sqrt{\frac{(n-1)S_1^2+(m-1)S_2^2}{n+m-2}}\sqrt{\frac{1}{n}+\frac{1}{m}}}$$

Donde

n=3

m=3

Factor nivel de confianza ∞=0.05

X= promedio de ataques detectados

Y= promedio de ataques detectados

S1= covarianzas muestrales de con Snort

S2= covarianzas muestrales de con Suricata

Cálculos de las covarianzas S1 y S2 se realizan de acuerdo a la siguiente formula:

$$S_1 = \frac{1}{n}\sum_{i-1}^{n}(X_{1-}\bar{X})^2$$

La covarianza muestral y se obtiene con la sumatoria de la observación menos la media elevada al cuadrado y multiplicado por el número de observaciones menos uno como se ve en la formula anterior.

Cálculos y resultado de S1 (Con Suricata)

	S1=con Snort
$S2_1$=1/3(44-30.666)^2	88,89
$S2_2$=1/3(23-30.666)^2	29,39
$S2_3$=1/3(25-30.666)^2	16,055
$S_{T2=}$S1-S2+S3+S4+S5	**134,333**

Cálculos y resultado de S1 (Con Suricata)

	S1=con Snort
$S1_1$=1/3(55-48.666)^2	20,88
$S1_2$=1/3(53-48,666)^2	9,38
$S1_3$=1/3(38-48,666)^2	56.88
$S_{T1=}$S1-S2+S3+S4+S5	**86,33**

Cálculos de grado de libertad

Para dos colas GL es igual a= n+m-2 => 3+3-2=4

Obtener la t tabulada

T tabulado

Para obtener la t tabulada buscamos en la tabla de t-student con grados de libertad = 4 y Nivel de significancia = 0.05. La tabla T-student se encuentra en la sección anexos.

Cálculos obtenidos son: $x = \frac{30{,}667-48{,}667}{\sqrt{((3-1)S1^2+(3-1)S2^2)/(3+3-2)}\sqrt{(\frac{1}{3}+\frac{1}{3})}}$ t= -2.99

Se detalla los valores obtenidos.

	Variable 1	*Variable 2*
Media	30,66666667	48,6666667
Varianza	134,3333333	86,3333333
Observaciones	3	3
Varianza agrupada	110,3333333	
Diferencia hipotética de las medias	0	
Grados de libertad	4	
Estadístico t	-2,98769601	
P(T<=t) una cola	0,051898683	
Valor crítico de t (una cola)	2,131846786	
P(T<=t) dos colas	0,103797365	
Valor crítico de t (dos colas)	2,776445105	

Interpretación:

Valor de la tabla de t-Student Tcritico =2,7765 se encuentra en Anexos.

Si ($T_{obtenida}$)> ($T_{critico}$) se rechaza la H_0.

La t Student calculada es de -2.99 y la de la tabla tabulada (crítica) a 4 grados de libertad es 2,7765 y un nivel de significancia de 0,05, por tanto se desecha la hipótesis nula y se acoge la hipótesis del trabajo. En la sección anexos se detalla la tabla de T-student

- 

- -2.7765 x 2.7764

La $T_{obtenida}$ >$T_{critica}$ se rechaza H0 y se acepta Hi.

-2.99 es > 2,776 o -2,776 cae en la zona de rechazo de la Ho y se acepta la Hi.

Hi= La utilización de la herramienta nIDPS open source Suricata brinda mejores prestaciones que la herramienta nIDPS open source Snort para detectar y prevenir las intrusiones en la red de datos de la UNACH.

6.2.DISCUSIÓN

La discusión se basa en diferentes aspectos estudiados en la investigación:
A pesar que Suricata es relativamente nuevo mantiene una buena reputación por su característica más relevante de reconocer y monitorizar mayor cantidad de protocolos en consideración a Snort. De acuerdo a los protocolos de red con los cuales trabaja Suricata permitirá mejorar la detección de intrusiones al servidor DNS de la UNACH puesto cuenta dentro de sus protocolos al 53 propio del servidor DNS.
En base al análisis de aplicaciones extendidas se llega a determinar que Snort la solución preferida por muchos años y hace poco adquirida por CISCO, es mucho más versátil y adaptable ante sistemas propietarios como Splunk y firewall propios de CISCO, lo cual es una ventaja que permitirá trabajar con el firewall desplegado en la UNACH, sin embargo con respecto al nivel de seguridad ofrece un menor porcentaje de predicción.

Snort ofrece buenos resultados en el desempeño general con respecto a Suricata.

En base a los resultados obtenidos, Suricata mejora la detección y prevención de intrusiones en comparación a Snort. Una prueba factible de mencionar es: en ataques de DOS comprobados, Snort no activa ni alerta reglas de seguridad esperadas a pesar de que estas se encuentra habilitadas. Mencionadas situaciones pasan tanto en los dos escenarios y principalmente se ha presentan en ataques DOS.

Snort y Suricata son igualmente sensibles ante ataques de monitorización.

Snort no detecta ciertos ataques DOS a pesar de tener activadas las reglas.

CAPITULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES

La red de la UNACH no restringe adecuadamente ataques de reconocimiento externos que se pueden realizar desde Sitios web y herramientas de escaneo de vulerabilidades como Nikto y NESSUS. Una consulta utilizando el sitio web centralops.net permite obtener información sensible sobre el estado de configuración del servidor DNS.

En base a los resultados obtenidos del tráfico monitorizado con la herramienta Suricata se determina que no solo, se registran ataques de denegación de servicio al servidor DNS, si no, intrusiones coincidentes al uso de escaneo de vulnerabilidades hacia el servidor http, paquetes de red coincidentes con un posible falseamiento de DNS. Con base al escaneo externo realizado se determina que la red de datos de UNACH proporciona información sensible ante herramientas de vulnerabilidades como NIKTO y consulta de información sensible sobre el estado de configuración del servidor DNS mediante el uso de sitios web.

Si bien Snort y Suricata son nIDPS de código abierto que cumplen las mismas funciones, ambas cuentan con fortalezas y debilidades, entre la cuales se mencionan las siguientes:

- Snort limita el uso y escritura de firmas de seguridad a los protocolos de red ICMP, IP, TCP y UDP. Suricata en cambio permite una mayor granularidad de protocolos de red en los que constan: IP, TCP, UDP, ICMP, FTP, HTTP, TLS, SMB, SMB2, SSL, DCERPC, SMTP, SSH Y

DNS, por lo tanto permite determinar de manera màs específica el comportamiento de red.

- La arquitectura multihilos de Suricata aprovecha las prestaciones hardware de los dispositivos físicos actuales con multiprocesadores y múltiples núcleos, con ello, es posible una mayor velocidad de análisis.
- Snort no requiere de muchas prestaciones hardware por lo que en el momento de implementarlo en dispositivos con múltiples núcleos no hará uso de ellos.

Los parámetros que permiten determinar e identificar la mejor herramienta nIDPS se basan en características y propiedades inherentes presentadas, al desempeño y probabilidad de seguridad de las nIDPS para detectar ataques, así mismo constituyen un aspecto importante el ámbito en que se pretende desplegar, por ejemplo si se pretende proteger una red de servidores en la que consten un servidor DNS, es recomendable considerar una herramienta que automatice y permite monitorizar el protocolo DNS y su puerto por defecto o algún otro puerto no habitual configurado.

Los parámetros que permiten determinar e identificar la mejor herramienta nIDPS se basan en características y propiedades inherentes a las herramientas consideradas y principalmente a los requerimientos del entorno.

La creación de un escenario de simulación permite modelar y entender el funcionamiento de ataques en un ambiente controlado con el fin de entender de mejor manera la forma de protegernos antes los ataques. Una de las ventajas es además de modelar ataques es afinar el Indicador de las alertas que deben activarse durante determinado ataques.

La elaboración de una guía permite identificar los parámetros a tomar en cuenta para el despliegue de u nIDPS con el uso de la técnicas de análisis de uso indebido.

7.2. RECOMENDACIONES

Se recomienda recatalogar el tipo de acción definida como “ALERT” a “DROP” para todas las firmas de seguridad potencialmente peligrosas e inicialmente definidas para solo alertar. Un ejemplo factible es la alerta correspondiente al escaner de vulnerabilidades exhaustivo utilizando NIKTO o NIKTO2, que incluye dentro de un único ataque a más de 32000 ficheros de escaneos internos. Por lo tanto en el nIDPS analiza a por lo menos 25000 alertas agrupadas en 130 ùnicas.

Es recomendable seleccionar una herramienta nIDPS de acuerdo al entorno, por ejemplo si se pretende proteger una red de servidores o red DMZ en la que conste un servidor DNS, es importante considerar la herramienta que automatice y permita monitorizar el protocolo DNS y su puerto por defecto o algún otro puerto no habitual configurado.

Las configuraciones del nIDPS Suricata y Snort deben ser cuidadosamente aplicadas para reducir al máximo los falsos positivos.

Se recomienda habilitar solo las reglas pertinentes a los servicios u objetivos a proteger, para de esta forma no saturar el sistema con firmas de seguridad inecesarias, por ejemplo, si el entorno de red no cuenta con el servicioVOIP, las firmas de seguridad correpondientes no debería ser habitadas.

Si la red monitorizada cuenta con servicios que no se desea analizar es recomendable crear una lista de confianza (listas blancas) en la que se indica al nIDPS que los eventos de red dirigidos hacia la dirección IP o rango IP son confiables.

Realizar comprobaciones y actualizaciones periódicas de las firmas de seguridad implementadas en el nIDPS, con el fin de descartar reglas obsoletas de la base de datos de intrusiones y maximizar la efectividad del sistema implementado.

Utilizar plugins adicionales que permitan bloquear activamente direcciones IP que registran alertas más severas.

CAPÍTULO VIII

PROPUESTA

8.1.Tilulo de la propuesta

Implementacion de un nIDPS basado en técnica de uso indebido para la red de servidores de la UNACH.

8.2.Introduccion

En esta sección se detalla un grupo de requerimientos a seguir para la implementación de un nIDPS basado en técnica de uso indebido, para la red de servidores de la UNACH.

La finalidad es: permitir monitorizar en tiempo real eventos de red de datos cableada de servidores que el firewall ha dejado pasar y que tienen como objetivo solicitar algún tipo de servicio al servidor DNS o a otro servidor.

Un sistema nIDPS basado en técnica de uso indebido permitirá al adminsitrador de la red de datos de la UNACH monitorizar eventos de red de tiempo real que el firewall ha dejado pasar y buscar coincidencias de patrones que coincidan con algún tipo o intento de intrusión par tomar medidas defensivas como descartar el paquete.

Objetivos

Implementar un nIDPS de open source basado en técnica de análisis de uso indebido.

Especìficos

Analizar la situación actual de la red de la UNACH

Determinar la ubicación de nIDPS

Instalar y configurar la herramienta nIDPS y sus reglas de seguridad.

Fundamentacion de la propuesta

El estudio de las herramientas nIDPS open source promoverà las bases necesarias para la implementación de un nIDPS y fomentarà la investigación de posteriores desarrollos de temas asociados.

Descripcion de la propuesta

El análisis de cada uno de los requerimientos que se necesitan automatizar se encuentran detallado en el capitulo IV definido como sistematización de pasos.

9. Bibliografía

Electric Sheep Fencing LLC . (2015). *Sense*. Retrieved from pfSense Portal - Commercial Support, Services, and Membership: https://www.pfsense.org

Albin, E. (2011). A Comparative Analysis of the Snrot and Suricata Intrusion-Detection Systems. Monterrey, California, EU. doi:7540-01-280-5500

AlienVault. (2010). AlienVault Installation Guide.

Appala, C., & Avadhani, P. (2013, Jan- March). A Comparison of Two Intrusion Detection Systems. *IJCST, 4*, 313-318. doi:0976-8491

Areitio, J. (2008). *Seguridad de la Información: Redes, informática y Sistemas de Información.* Madrid, España: PARANINFO Cengage Learnning. doi:978-84-9732-502-8

Bosworth, S., Kabay, M., & Wayne, E. (2014). *Computer Security Hanbook.* Estados Unidos, New Jersey: JOHN WILEY & SONS, INC. doi:ISBN 978-1-118-85174-6

Centro Criptogràfico Nacional de España. (2013, Junio). GUÍA DE PROTECCIÓN CONTRA. *GUÍA DE SEGURIDAD DE LAS TIC* . (G. d. Presidencia, Ed.) España. doi:(CCN-STIC-820)

Cisco and/or its Affiliates. (2014). *Writing Snort Rules*. Retrieved from Snort User Manual 2.9.7.

Cisco System. (2004). *Cisco Secure Intrusion Detection System.* Retrieved from CISCO SYSTEM: www.cisco.com/go/offices.

CISCO Systems, Inc. (2014). *CISCO 2014 Annual Security Report.* California. Retrieved from http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

Damaye, S. (2015, Mayo 06). *Wiki about Network and Web Applications Security, Ethical Hacking and Network Forensics.* Retrieved from Aldeid.com: www.aldeid.com/wiki/Suricata-vs-snort

Douligeris, C., & Serpanos, D. (Eds.). (2007, June 15). Network Security Current Status and Future Directions. (1). Canada: Wiley-IEEE Press. doi:ISBN 978-0-471-70355-6

Fossl, M. (2011, Abril). Symantec Internet Security Threat Report. (S. Corp, Ed.) *Symantec Enterprice Security, 16*, 3-18. doi:21182883

Fung , C., & Boutaba, R. (2013). *Intrusion Detection Networks: A key Collaborative Security.* Broken Sound Parkway NW,: CRC Press. doi:13: 978-1-4665-6413-8

García, J. A., Herrera, J. J., & Perramón, X. T. (2004). *Aspectos avanzados de seguridad en redes* (Primera ed.). Barcelona.

Ghorbani, A. A., Lu, W., & Tavallaee, M. (2009). *Network Intrusion Detection and Prevention Concept and Techniques.* Canada, New York: Springer . doi:10.1007/978-0-387-88771-5

Google Company. (2014). *Google Code Archive*. Retrieved from rule2alert: https://code.google.com/archive/p/rule2alert/

Hayes, B. (2015, Febrero). *TechTarget global network of technology-specific websites*. Retrieved from Types of intrusion detection products: Suite vs. best-of-breed: http://searchsecurity.techtarget.com/

Holden, G., Herbert, J., & Mattord, R. D. (2004). *Guide to Firewalls and Network Security - Intrusion Detection and VPNs* (Second ed.). (C. T. Learning, Ed.) Canadá: Nick Lombardi.

IARIA. (2011). The Fifth International Conference on Digital Society. *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines*, (pp. 187-192). Gosier, Guadeloupe, France. doi:ISSN: 2308-3956

IBM Corporation. (2013, June). Intrusion detection and prevention system (IDPS). *IBM Global Technology Services*, 4. doi:SED03081-USEN-02

International Journal of Advanced Research in Computer and Communication Engineering. (2012, Agosto). A brief study and comparison of Snort and Bro Open Source Network Itrusion Detection Systems. *IJARCCE, 1*, 383-386. doi:ISSN : 2278 – 1021

International Telecommunication Union. (2012). *Understanding CyberCrime: Phenomena, Challenges and Legal Response.* Switzerland: Telecommunacion Developed Bureau. doi:CEP 70070-940

Kaushik, S. (2011). Detection of Attacks in an Intrusion Detection. *International Journal of Computer Science and Information Technologies (IJCSIT), 2*(3), 982-986. doi:0975-9646

Khubeb Siddiqui, M., & Naahid, S. (2013). Analysis of KDD CUP 99 Dataset using Clustering based Data. *International Journal of Database Theory and Application, 6*(05), 23-34. doi:2005-4270 IJDTA

Koziol, J. (2003). *Intrusion Deteccio with Snort.* (H. Stephen , & A. Bryce , Eds.) Indiana: Sams Publishing. doi:2002110728

Kruegel, C., Valeur, F., & Vigma, G. (2005). *Intrusion Detection and Correlation Challenges and Solutions* (Ilustrada ed.). Boston: Springer Science + Business Media, Inc. doi:0-387-23399-7

Kumar, A., Chandak, S., & Dewanjee, R. (2014, Enero). Recent Advances in Intrusion Detection Systems: An Analytical Evaluation and Comparative Study. *International Journal of Computer Apllications , 86*(4), 32 -37. doi:(0975 - 8887)

Lazarevic, A., Kumar, V., & Srivastava, J. (2005). Intrusion Detection: A Survey. In A. Lazarevic, V. Kumar, & J. Srivastava, *Managing Cyber Threats: Issues, Approaches, and Challenges* (Quinta ed., pp. 20-30). EEUU: Springer Publisher. doi:ISBN-10: 0-387-24226-0

Macìa, G. (2007, 08 13). Ataques de Denegacion de servicio a baja tasa contra servidores. Granada, España: Universidad de Granada. doi:978-4-338-4368-5

Microsoft Corporation. (2016). *Microsoft MSDN* . Retrieved Enero 2016, from Definición de DNS: https://msdn.microsoft.com/es-es/library/cc787920(v=ws.10).aspx

Minella, J. (2010, Noviembre). *TechTarget* . Retrieved from IDS vs. IPS: How to know when you need the technology: http://searchsecurity.techtarget.com/tip/IDS-vs-IPS-How-to-know-when-you-need-the-technology

Ministerio de Defensa Español. (2011). *Ciberseguridad. Retos y amenazas a la seguridad nacioal en el ciberespacio.* España: Ministerio de Defensa Dirección general de Relaciones Institucionales. doi:978-84-9781-622-9

Naranjo, R., & Macìas, V. (2014). *Modelo basado en las tecnicas de mineria de datoas aplicda a la deteccion de atques en las redes de datoas de la facultad de informatica y electronica.* Riobamba: ESPOCH.

NIST; R. Bace; P. Mell. (2008, Febrero 20). NIST Guide to Intrusion Detection and Prevention Systems (IDPS). *Intrusion Detection Systems*(Special Publication). Gaithersburgo, Estados Unidos. Retrieved from http://www.nist.gov/

Nmap. (n.d.). *Nmap Security Scanner*. (G. Lyon, Editor) Retrieved from Nmap.org: https://nmap.org/

Offensive Security. (2015). *Kali Linux 2.0*. Retrieved from Official Kali Linux Documentation: https://www.kali.org/

Paliwal, S., & Gupta, R. (2012, Diciembre). Denial-of-Service, Probing & Remote to User (R2L) Attacks Detection using generic Algorithm. *International Journal of Computer Applications, 60*(19), 57-62. Retrieved Marzo 2015

Pappas, N. (2008, Abril 2). SANS Institute InfoSec Reading Room. *Network IDS & IPS Deployment Strategies*. Retrieved Marzo 2015

Perez, R. (2011). An Agent Based Intrusion Detection System. In Dr. Skrobanek, Pawel;, & P. Skrobanek (Ed.), *Intrusion Detectión Systems* (p. 90). Colombia: InTech. doi:978-953-307-167-1

Pihelgas, M. (2012). A comparative analysis of open source intrusion detection systems. *2012*. Tallinn, Estonia.

Piper, S. (2011). *Intrusion Prevention System for Dummies.* EEUU: Wiley Publishing, Inc. doi:978-1-118-00474-6

Ponemon Institute. (2014, Mayo). 2014 Cost of Data Breach Study: Global Analysis. *Ponemon Institute© Research Report*, 28. Michigan, USA. doi:SEL03027-USEN-00

ProofPoint Inc. (2015). *ProofPoint*. Retrieved from Theat Intelligence.

RAPID-7. (2016). *METASPLOIT: PENETRATION TESTING TOOL* . Retrieved from PENETRATION TESTING TOOL: http://www.rapid7.com/

Rehman, R. U. (2003). *Intrusion Detection Systems Advanced IDS Techniques Using Snort, Apache, MySql, Php and ACID.* New Jersey: Prentice Hall PTR. doi:ISBN 0-13-140733-3

Royer, J. (2004). *Seguridad en la Información de empresa: riesgos, amenazas, prevención y soluciones.* Barcelona, España: ENI. doi:2746023040, 9782746023048

Royer, J. (2004). *Seguridad en la informática de empresa : riesgos, amenazas, prevención y soluciones.* Cornellà de Llobregat, Barcelona: ENI Editions. doi:2-7460-2304-0

Salinas, R. (2005, Febrero). Sistemas de Deteccion de Intrusos. (ITI – Instituto Tecnológico de Informática, Ed.) *Actualidad TIC*(6), 12-15.

Sanfilippo, S. (2006). *hping*. Retrieved from http://www.hping.org/

Sanfilippo, S. (n.d.). *die.net*. Retrieved from Hping3(8)- Linux man page: http://linux.die.net/man

SANS. (2015, Febrero 02). *Open Source High Perfomance Shootout.* Retrieved from SANS: http://www.sans.org/reading-room/whitepapers/intrusion/

SANS Institute InfoSec Reading Room. (2006, Diciembre 23). A practical application of SIM/SEM/SIEM Automating Theat Identification.

Scarfone, k., & Mell, P. (2007, Febrero). Guide to Intrusion Detection and Prevention Systems (IDPS). *Recommendations of the National Institute of Standards and Techonology*, 127. (N. I. NIST, Ed.) Gaithersburg, Estados Unidos. doi:208999-8930

Scarfone, K., Grance, T., & Masone, k. (2015, Agosto 6). Computer Security Incident Handling Guide. *Computer Security Division (Information Technology Lab)*. USA. Retrieved from http://csrc.nist.gov/groups/SMA/fisma/

Sourceforce. (2012, 06). *Enterprise-Ready Open Source Projects*. Retrieved from Metasploitable is an intentionally vulnerable Linux virtual machine: http://sourceforge.net/projects/metasploitable/files/Metasploitable2/

Stalling, W. (2004). *Fundamentos de Seguridad en Redes.* Madrid, España: Pearson Educaciòn.

Stonesoft Corp. (2005, 09). StoneGate IPS Intrusion Detetion and Analysisfor Active Response. Finland. doi:SGIRG_20050928

Suricata. (n.d.). Retrieved from http://jasonish-suricata.readthedocs.org/en/latest/configuration/suricata-yaml.html

The CISCO Online Privacy Statement. (2016). *Snort*. Retrieved from Cisco and/or its affiliates. Snort.: https://snort.org/

The Open Information Security Foundation (OISF) . (n.d.). *Suricata Open Source IDS/IPS/NSM engine*. Retrieved from http://suricata-ids.org/

University of California. (2009, September). *UCI KDD Archive*. Retrieved from UCI Knowledge Discovery in Databases Archive: https://kdd.ics.uci.edu/

Whitman, M., & Mattord, H. (2012). *Principles of information security* (Cuarta ed.). Boston, USA: Cengage Learning Customer. doi:0: 1-111-13821-4

Wold Journal Science and Technology. (2012, Abril 21). A survey on Intrusion Detection Techniques. *NCETIT 2012*, 1 - 7. doi:2231 – 2587

10. ANEXOS

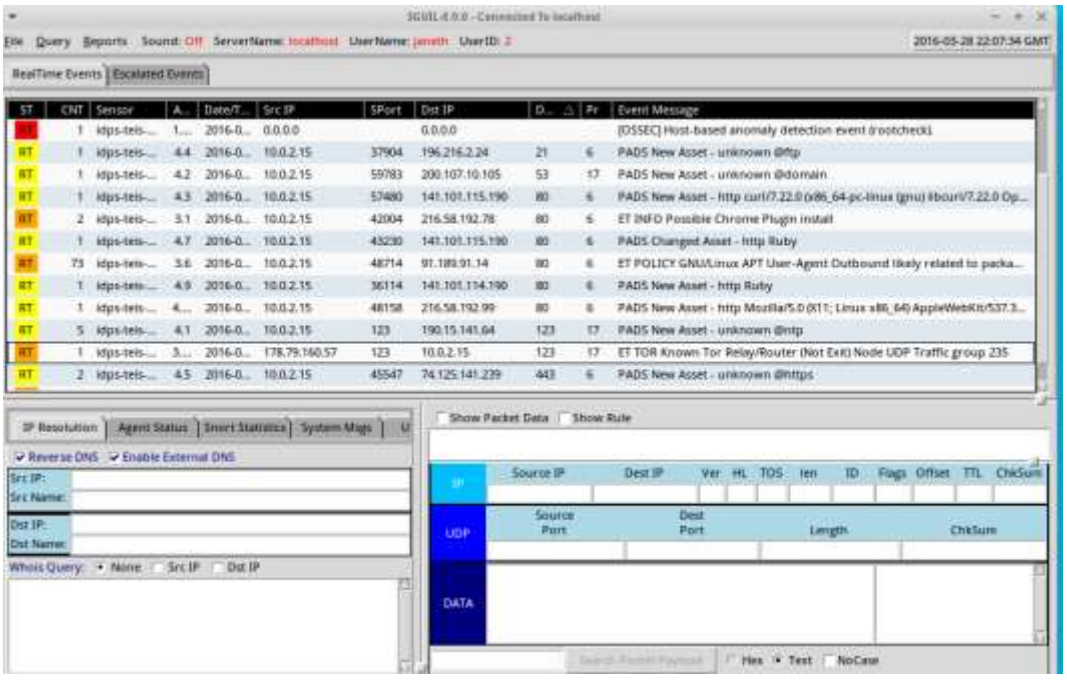
10.1. Tabla de índices T-student

Tabla índice T-student

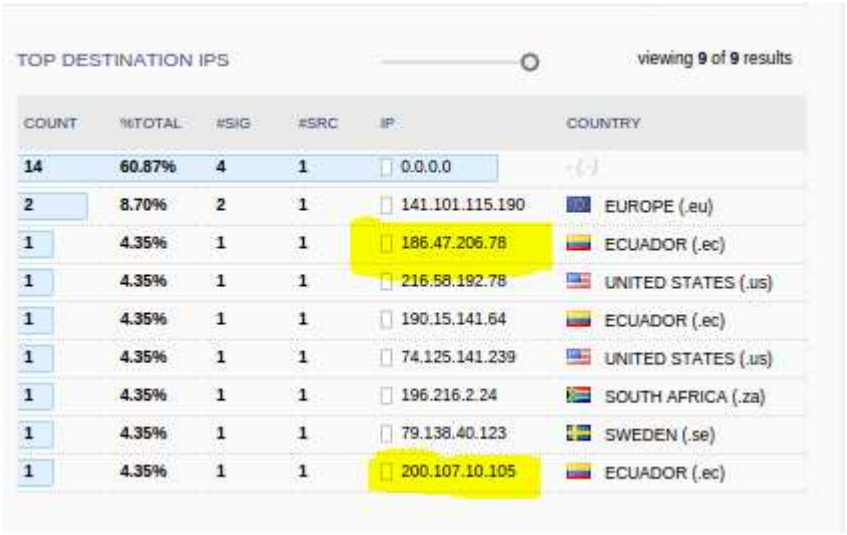
Tabla de la t de Student.
Contiene los valores t tales que $p[|t| > t] = \alpha$,
donde n son los grados de libertad.

$n \setminus \alpha$	0,90	0,80	0,70	0,50	0,30	0,20	0,10	0,05	0,02	0,01	0,001
1	0,1584	0,3249	0,5095	1,0000	1,9626	3,0777	6,3137	12,7062	31,8210	63,6559	636,5778
2	0,1421	0,2887	0,4447	0,8165	1,3862	1,8856	2,9200	4,3027	6,9645	9,9250	31,5998
3	0,1366	0,2767	0,4242	0,7649	1,2498	1,6377	2,3534	3,1824	4,5407	5,8409	12,9244
4	0,1338	0,2707	0,4142	0,7407	1,1896	1,5332	2,1318	2,7765	3,7469	4,6041	8,6101
5	0,1322	0,2672	0,4082	0,7267	1,1558	1,4759	2,0150	2,5706	3,3649	4,0321	6,8688
6	0,1311	0,2648	0,4043	0,7176	1,1342	1,4398	1,9432	2,4469	3,1427	3,7074	5,9587
7	0,1303	0,2632	0,4015	0,7111	1,1192	1,4149	1,8946	2,3646	2,9979	3,4995	5,4081
8	0,1297	0,2619	0,3995	0,7064	1,1081	1,3968	1,8595	2,3060	2,8965	3,3554	5,0414
9	0,1293	0,2610	0,3979	0,7027	1,0997	1,3830	1,8331	2,2622	2,8214	3,2498	4,7809
10	0,1289	0,2602	0,3966	0,6998	1,0931	1,3722	1,8125	2,2281	2,7638	3,1693	4,5868
11	0,1286	0,2596	0,3956	0,6974	1,0877	1,3634	1,7959	2,2010	2,7181	3,1058	4,4369
12	0,1283	0,2590	0,3947	0,6955	1,0832	1,3562	1,7823	2,1788	2,6810	3,0545	4,3178
13	0,1281	0,2586	0,3940	0,6938	1,0795	1,3502	1,7709	2,1604	2,6503	3,0123	4,2208
14	0,1280	0,2582	0,3933	0,6924	1,0763	1,3450	1,7613	2,1448	2,6245	2,9768	4,1403
15	0,1278	0,2579	0,3928	0,6912	1,0735	1,3406	1,7531	2,1315	2,6025	2,9467	4,0728
16	0,1277	0,2576	0,3923	0,6901	1,0711	1,3368	1,7459	2,1199	2,5835	2,9208	4,0149
17	0,1276	0,2573	0,3919	0,6892	1,0690	1,3334	1,7396	2,1098	2,5669	2,8982	3,9651
18	0,1274	0,2571	0,3915	0,6884	1,0672	1,3304	1,7341	2,1009	2,5524	2,8784	3,9217
19	0,1274	0,2569	0,3912	0,6876	1,0655	1,3277	1,7291	2,0930	2,5395	2,8609	3,8833
20	0,1273	0,2567	0,3909	0,6870	1,0640	1,3253	1,7247	2,0860	2,5280	2,8453	3,8496
21	0,1272	0,2566	0,3906	0,6864	1,0627	1,3232	1,7207	2,0796	2,5176	2,8314	3,8193
22	0,1271	0,2564	0,3904	0,6858	1,0614	1,3212	1,7171	2,0739	2,5083	2,8188	3,7922
23	0,1271	0,2563	0,3902	0,6853	1,0603	1,3195	1,7139	2,0687	2,4999	2,8073	3,7676
24	0,1270	0,2562	0,3900	0,6848	1,0593	1,3178	1,7109	2,0639	2,4922	2,7970	3,7454
25	0,1269	0,2561	0,3898	0,6844	1,0584	1,3163	1,7081	2,0595	2,4851	2,7874	3,7251
26	0,1269	0,2560	0,3896	0,6840	1,0575	1,3150	1,7056	2,0555	2,4786	2,7787	3,7067
27	0,1268	0,2559	0,3894	0,6837	1,0567	1,3137	1,7033	2,0518	2,4727	2,7707	3,6896
28	0,1268	0,2558	0,3893	0,6834	1,0560	1,3125	1,7011	2,0484	2,4671	2,7633	3,6739
29	0,1268	0,2557	0,3892	0,6830	1,0553	1,3114	1,6991	2,0452	2,4620	2,7564	3,6595
30	0,1267	0,2556	0,3890	0,6828	1,0547	1,3104	1,6973	2,0423	2,4573	2,7500	3,6460
40	0,1265	0,2550	0,3881	0,6807	1,0500	1,3031	1,6839	2,0211	2,4233	2,7045	3,5510
60	0,1261	0,2542	0,3867	0,6786	1,0452	1,2958	1,6706	2,0003	2,3901	2,6603	3,4602
120	0,1258	0,2534	0,3853	0,6765	1,0403	1,2886	1,6577	1,9799	2,3578	2,6174	3,3734
∞	0,126	0,253	0,385	0,674	1,036	1,282	1,645	1,96	2,326	2,576	3,291

10.2. Alertas de intrusiones visualizadas mediante Sguil



10.3. Soporte Geo IP de Snort mediante Squert



TOP DESTINATION IPS — viewing 9 of 9 results

COUNT	%TOTAL	#SIG	#SRC	IP	COUNTRY
14	60.87%	4	1	0.0.0.0	-(-)
2	8.70%	2	1	141.101.115.190	EUROPE (.eu)
1	4.35%	1	1	186.47.206.78	ECUADOR (.ec)
1	4.35%	1	1	216.58.192.78	UNITED STATES (.us)
1	4.35%	1	1	190.15.141.64	ECUADOR (.ec)
1	4.35%	1	1	74.125.141.239	UNITED STATES (.us)
1	4.35%	1	1	196.216.2.24	SOUTH AFRICA (.za)
1	4.35%	1	1	79.138.40.123	SWEDEN (.se)
1	4.35%	1	1	200.107.10.105	ECUADOR (.ec)

10.2. Guìa

GUÍA

DESPLIEGUE DE LA HERRAMIENTA nIDPS OPEN SOURCE UTLIZANDO LA TÉCNICA DE ANÁLISIS DE USO INDEBIDO

Año

2016

Indice

1. Aspectos a considerar 119
1.1. Entendimiento de la red 120
1.1.1. Conocimiento de red 120
1.1.2. Ubicación del sensor 121
1.1.3. Preparaciòn de interfaces 121
1.2. Despliegue del nidps 122
1.2.1. Instalación del nIDPS suricata 123
1.2.2. Configuración 124
1.2.3. Incluir reglas de seguridad 124
1.2.4. incluir reglas personalizadas 125
1.2.5. Medidas de prevención de ataques 125
1.2.6. Comprobacion y uso 127

Tabla de ilustraciones

Ilustración 1: Aspectos generales 119
Ilustración 2: Aspectos sobre el conocimiento de la red 120
Ilustración 3: Aspectos generales para el despliegue del nIDPS 122

GUÍA

Introducción

La presente guía se crea para brindar a administradores de red, los pasos a considerar para implementar el mecanismo de seguridad complementaria utlizando un nIDPS de código abierto,

La presente guía se formaliza con la utilización el sistema operativo Ubuntu 14.04 de 64 bits como sistemas base para la instalación de la herramienta Suricata.

1. Aspectos a considerar

Para la presente guía crea una visualización global de los aspectos a tomar en cuenta para implementar un nIDPS basado en la técnica de análisis de uso indebido. Para lo expuesto se ha determinado en los siguientes:

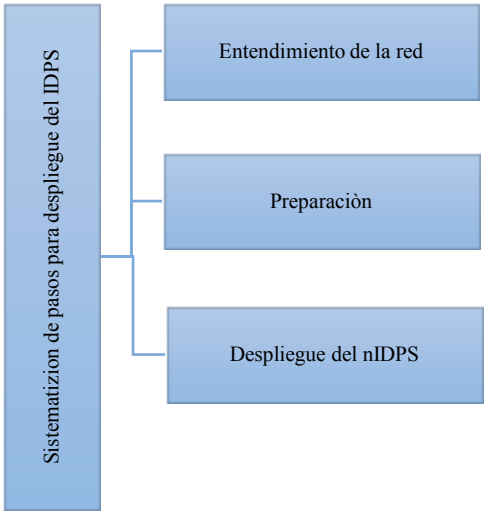


Ilustración 1: Aspectos generales

Descripción de los requerimientos hardware

Memoria RAM

La memoria RAM del sistema autónomo en que se despliega el IDPS depende de varios factores:

- Servicios soportados por la red (tipo de tráfico)

- Cantidad de trafico

Almacenamiento

Se debe tomar en cuenta que el espacio de almacenamiento depende el o los tipos de salida a utilizar. Por ejemplo si activamos que las salidas sean solo en formato UNIFIED2 es considerablemente bajo a que las salidas sean UNIFIED2, PCAPs, LOG u otros adicionales.

Tarjetas de red

Como requerimiento mínimo son dos tarjetas de red: una de entrada y otra de salida de tráfico. Si se desea contar con una red de gestión dedicado es necesaria una tercera tarjeta de red.

Se debe tomar en cuenta que el sensor y el modulo colector de alertas se instalan en el mismo dispositivo. Mientras que el fron-end o adicionales se pueden desplegar en el mismo dispositivo o en uno independiente.

1.1.Entendimiento de la red

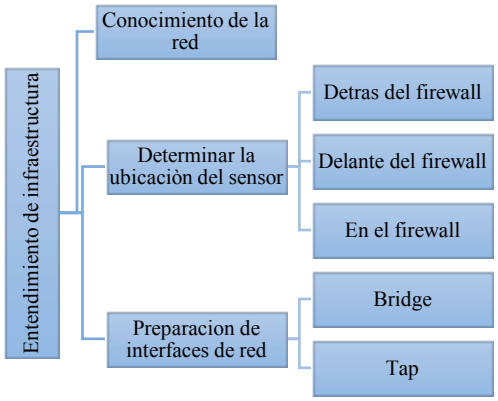


Ilustración 2: Aspectos sobre el conocimiento de la red

1.1.1. Conocimiento de red

El proceso de conocimiento de la red tiene como fin, identificar los aspectos relacionados con la red a proteger, como: dispositivos hardware, software, servicios (tipo de tráfico), políticas de seguridad, topología de red y ancho de banda.

El objetivo tener un Indicador concreto del estado y funcionamiento de la red que se pretende proteger es importante para el correcto despliegue de una herramienta de seguridad nIDPS, para ello se puede basar en la documentación existente sobre la red de la entidad o empresa.

En base a lo expuesto se determina la porción de red a proteger y el lugar de despliegue del sensor.

1.1.2. Ubicación del sensor

Se debe procurar que el lugar de implementación del sistema IDPS sea una ubicación estratégica donde todo el tráfico a monitorear pase por este, queda a Indicador del personal de administracion de redes. A continuación se mencionan las siguientes opciones:

- **Delante del firewall**: El trafico entrante es analizado antes de pasar por un primer filtro como el firewall en el cual probablemente se descartaràn algunos paquetes. Por lo tanto el trafico a monitorear no es el real. Esta implementacion puede resultar contraproducente y genera un mayor numero de alertas.
- **Detras del firewall:** El trafico entrante es monitorizado despues de pasar por un primer filtro como el firewall por lo tanto el trafico a analizar es el que no ha ido descartado. Esta implementacion permite ademas de verificar el funcionamiento del firewall, monitorizar el trafico real de la red.
- **En el firewall:** implementar el un mismo dispositivo el IDPS y firewall. Esta implementaciòn requiere una buen cantidad de recursos.

1.1.3. Preparaciòn de interfaces

Preparación de interfaces consiste en configurar las interfaces en modo inline, para lo cual los métodos empleados son: lógico o físico.

El modo lógico consiste en la colocación del dispositivo en modo puente y el método físico consiste en la utilización de network taps (puerto de acceso de pruebas)

- Bridge: requiere instalar los paquetes: vtun bridge-utils uml-utilities
- Taps: dispositivos de escucha de red.

Se recomienda en el uso de bridge desactivar las siguientes características

- ethtool --offload <interfaz> rx off tx off
- ethtool -K <interfaz> gso off
- ethtool -K <interfaz> gro off

1.2. Despliegue del nidps

Para la presente guía se toma en cuenta las siguientes consideraciones:

- Instalación manual del sensor
- Distribución utilizada es Ubuntu Linux con una arquitectura de 64 bits.

El enfoque de este documento es crear una visión general de la instalación de otras distribuciones con la variación de sus propios comandos y directorios que estos presenten.

La fase del despliegue del IDPS corresponde a la instalación de la herramienta Snort para ello los pasos sugeridos son:

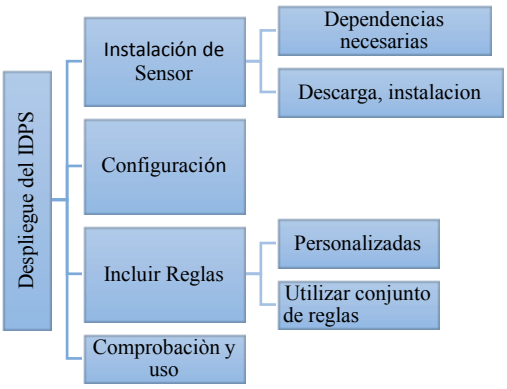


Ilustración 3: Aspectos generales para el despliegue del nIDPS

1.2.1. Instalación del nIDPS suricata

La instalación puede ser de manera manual automática, sólo funcional en sistemas basados en Debian con (apt-get install suricata) o de manera manual. Para la presente guía se emplea la instalación de manera manual, la cual, se divide en dos subetapas: la primera fase describe los requisitos previos como paquetes o dependencias necesarias antes de la instalación, en la segunda parte se describe la descarga, instalación y preparación del sistema propiamente.

Pre instalación y dependencias necesarias

Bison: analizador general.

Libpcap: librería de programación para paquetes TCP/IP.

Pcre: librería con funciones de encuentro de patrones.

Libpcre3: biblioteca de expresiones compatibles con Perl5 (archivos ejecutables regulares)

Libdnet: proporciona una interfaz simplificada de rutinas de redes de bajo nivel como: manipulación de direccionamiento de red, arp, búsqueda de interfaz de red, paquetes IP, tramas de Ethernet, entre otras.

Libssl: proporciona los archivos de firmas MD5 y SHA.

```
sudo apt-get install gcc libpcap-devel pcre-devel-libyaml devel archivo-devel
 zlib-devel jansson-devel nss-devel libcap-ng-devel libnet-devel python-
devel libnetfilter_queue-devel epel-release
```

Se debe tomar en cuenta que las dependencias epel-release y libnetfilter_queue-devel son necesarias para el modo IPS

Descarga, instalación y preparación de Suricata

```
wget http://www.openinfosecfoundation.org/download/suricata-2.0.8.tar.gz
tar -xvzf suricata-2.0.10.tar.gz
cd suricata-2.0.11
```

```
./configure –enable-nfqueue –prefix=/usr –sysconfdir=/etc/ --localstatedir=/vars
make && make install-rules
ldconfig
```

El comando install-rules permite descargar automáticamente las reglas y crear todos los directorios necesarios.

Directorio principal de configuración de Suricata: /etc/suricata

- suricata.yaml
- classification.config
- reference.config
- theshold.config
- sig-msg.map

Directorio de los distintos tipos de alertas: /var/log/suricata

- fast.log (archivo de alertas)
- http.log
- stats.log (estadísticas de Suricata)

1.2.2. Configuración

Las configuraciónes se realizan en el fichero suricata.yaml.

-**Establecer las variables de red**: especificación de la red o redes sobre las cuales actuará el Suricata.

-Plugins de salida: tipos específicos de salida de alertas (unified, unified2, tcpdump, etc)

-Habilitar reglas o firmas de seguridad.

1.2.3. Incluir reglas de seguridad

La sintaxis de las reglas se componen de dos partes: cabecera y opciones, en donde la cabecera son definiciones estáticas y las opciones permiten describir las posibles reglas a coincidir.

<cabecera>< optiones>

Cabecera: (cabecera de regla) Tipo de regla (acción), protocolo, dirección-origen, puerto origen, dirección-destino y puerto destino.

Opciones: (opciones de regla) cuenta con más de 50 opciones disponibles entre ellas: mensaje a mostrar (msg), contenido (content:), sid: Id de regla (sid:), numero de revision (rev:), entre otras.

Ejemplo de regla:

Alert tcp any any -> $HOME_NET 80 (msg: “Coincidencia GET”; content:”47 45 54”; sid: 10001; rev:1; clasification: icmp_event;)

Suricata para su modo IDPS provee las siguientes tipos de reglas con las acciones de:

- **ass:** Ignora el paquete
- **Reject:** bloquea el paquete, almacena el registro y además envía una repuesta de reseteo para las comunicaciones TCP o puerto rechazado para las comunicaciones UDP.
- **Drop:** bloquea de paquete y lo registra.
- **Alert:** Almacena registro de los paquetes

1.2.4. incluir reglas personalizadas

Para incluir reglas personalizadas se crea un fichero con extensión .rules (como por ejemplo local.rules) en las que estas deben ser:

- Una regla por línea.
- Si existe una nueva clasificación se debe incluir en el fichero classification.config
- Habilitar las reglas personalizadas en el archivo snort.conf utilizando la sintaxis “include $RULE_PATH/local.rules”

1.2.5. Medidas de prevención de ataques

En esta sección se menciona parámetros de configuración para prevenir intrusiones:

Es importante prevenir un colapso de peticiones porque lo que se recomienda crear un límite para las sesiones concurrentes.

```
max_sessions: 262144          # 256k concurrent sessions
prealloc_sessions: 32768      # 32k sessions prealloc'd
midstream: false              # do not allow midstream session
pickups
async_oneside: false          # do not enable async stream handling
inline: yes
```

Para prevenir ataques de DOS.

```
host-os-policy:
  windows: [0.0.0.0/0]
  bsd: []
  bsd_right: []
  old_linux: []
  linux: [10.0.0.0/8, 192.168.1.100,
"8762:2352:6241:7245:E000:0000:0000:0000"]
  old_solaris: []
  solaris: ["::1"]
  hpux10: []
  hpux11: []
  irix: []
  macos: []
  vista: []
  windows2k3: []
```

Configuracion de flujo

```
emergency_recovery: 30                  #Percentage of 1000
prealloc'd flows.
prune_flows: 5
```

Prevenir flujos en tiempo muertos

La configuración se realiza para los protocolos de red TCP; UDP; ICMP y por defecto. Suricata distingue tres estados. Para TCP, estos son: Nuevo, establecer y cerrar, para UDP único nuevo y establecido. Para cada uno de estos estados Suricata puede emplear diferentes tiempos de espera. (Suricata, s.f.)

Por ejemplo:

```
flow-timeouts:

  default:
    new: 30                     #Time-out in seconds after the
last activity in this flow in a New state.
    established: 300            #Time-out in seconds after the
last activity in this flow in a Established
                                #state.
    emergency_new: 10           #Time-out in seconds after the
last activity in this flow in a New state
                                #during the emergency mode.
```

```
    emergency_established: 100  #Time-out in seconds after the
last activity in this flow in a Established
                                #state in the emergency mode.
  tcp:
    new: 60
    established: 3600
    closed: 120
    emergency_new: 10
    emergency_established: 300
    emergency_closed: 20
  udp:
    new: 30
    established: 300
    emergency_new: 10
    emergency_established: 100
  icmp:
    new: 30
    established: 300
    emergency_new: 10
    emergency_established: 100
```

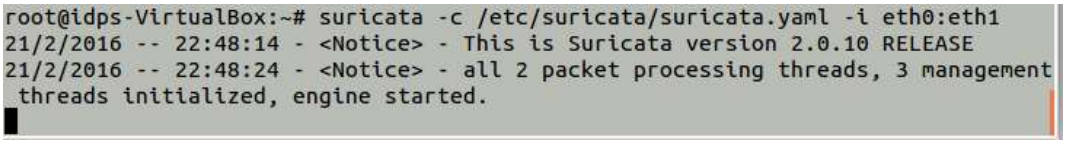
Configurar IP Defrag para procesar paquetes de red fragmentados.

```
  defrag:
  max-frags: 65535
  prealloc: yes
  timeout: 60
```

1.2.6. Comprobacion y uso

sudo suricata -c /etc/suricata/suricata.yaml -T -i eth0:eth1 --init-errors-fatal

Verificar el funcionamiento



Donde:

-T Testeo y report de configuración actual.

-c corresponde a la ubicación del archivos de configuración principal

-i interfaces a utilizar

-i interfaz de red