FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE HERRAMIENTAS PARA EL CONTROL DE VULNERABILIDADES INFORMÁTICAS E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y ALERTA TEMPRANA PARA UNA EMPRESA DE CONSTRUCCIÓN.

AUTOR

Santiago David Guachamín Guevara

AÑO

2020

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE HERRAMIENTAS PARA EL CONTROL DE VULNERABILIDADES INFORMÁTICAS E IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y ALERTA TEMPRANA PARA UNA EMPRESA DE CONSTRUCCIÓN.

Trabajo de titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones

Profesor Guía

Msg. Iván Patricio Ortiz Garcés

Autor

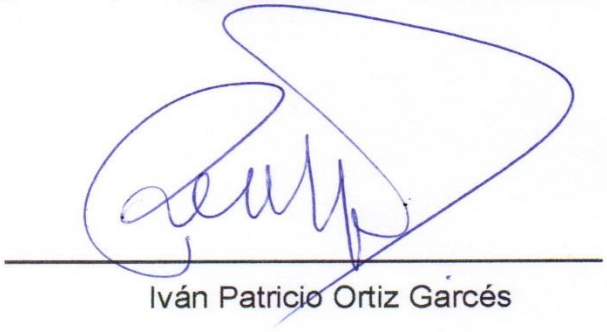
Santiago David Guachamín Guevara

Año

2020

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido este trabajo, Análisis de herramientas para el control de vulnerabilidades informáticas e implementación de un sistema de monitoreo y alerta temprana para una empresa de construcción, a través de reuniones periódicas con el estudiante, Santiago David Guachamín Guevara, en el semestre 2020-10, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".



Iván Patricio Ortiz Garcés

Magíster en Redes de Comunicaciones

CI: 060235677-6

DECLARACIÓN DEL PROFESOR CORRECTOR

Declaro haber reviso este trabajo, Análisis de herramientas para el control de vulnerabilidades informáticas e implementación de un sistema de monitoreo y alerta temprana para una empresa de construcción, de Santiago David Guachamín Guevara, en el semestre 2020-10, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación".

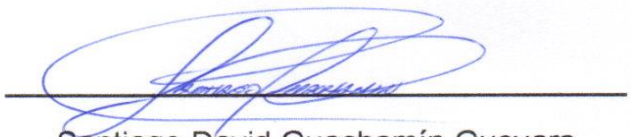
Milton Netpalí Román Cañizares

Magister en Gerencia de Redes y Telecomunicaciones

C.I. 050216344-7

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

"Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes".



Santiago David Guachamín Guevara

CI: 172160930-1

AGRADECIMIENTO

En primer lugar, agradezco a Dios por permitirme tener y disfrutar de la compañía de mi familia, también a personas especiales a las que agradezco por su amistad, apoyo, ánimo y en especial la compañía de mi enamorada Valeria gracias por tus enseñanzas, mensajes de apoyo y por estar ahí en las buenas y malas.

Santiago Guachamin

DEDICATORIA

En cada una de las letras de este proyecto va dedicado con mucho amor a mi madre Jenny quien ha estado conmigo en todo momento y es uno de los pilares fundamentales en mi vida quien me respaldado incondicionalmente para alcanzar esta meta.

También se la dedico a mi hijo Jherik, probablemente en estos momentos no comprendas mis palabras o lo que te quiero decir, pero cuando seas capaz te des cuenta lo que significas para mí, porque eres la razón que me levante día tras día para superar todos los obstáculos que se presente porque eres mi principal motivación.

Santiago Guachamin

RESUMEN

Hoy en día con la era de la transformación digital, las empresas enfrentan un gran reto para la protección de sus datos. De acuerdo con la empresa Fortinet, se producen más de 545.000 intentos de intrusión de las redes cada minuto. (Juniper Research, 2018, pág. 28). Aun así, las estrategias de protección dentro de las empresas todavía no son consideradas como un punto importante lo cual conlleva graves consecuencias.

Con lo anteriormente mencionado, en el presente proyecto se muestra una de las muchas soluciones que puede aplicar una empresa para la protección de sus datos como es la implementación de un software de monitoreo para detectar vulnerabilidades en la red.

Se empieza con detalles de los conceptos básicos acerca de la seguridad de la información y sus principales amenazas, con el fin de tener la temática necesaria de los aspectos importantes de la seguridad, las amenazas y conocer la norma o estándar que sirven para generar un control riguroso.

Continuando con un análisis de las herramientas de monitoreo conocidas a nivel mundial y sus principales características, que servirán como guía para una empresa que quiera realizar este tipo de implementación. Se debe conocer el proceso de gestión de amenazas y vulnerabilidades tomando como base la norma técnica ecuatoriana ISO 27005 la cual detalla los procedimientos para tratarlos.

Una vez seleccionada la herramienta a ser utilizada la cual es analizada en el capítulo 2, se procede con la implementación en la red de la empresa Bagant Ecuatoriana, esta herramienta muestra los resultados finales de las pruebas y el comportamiento del sistema.

ABSTRACT

Today, with the era of digital transformation, companies face a great challenge in protecting their data. According to the Fortinet Company, there are more than 545,000 network intrusion attempts every minute (Juniper Research, 2018, p. 28). Even so, protection strategies within companies are still not considered an important issue, which can have serious consequences.

With the above mentioned, in the present project shows one of the many solutions that a company can apply for the protection of its data, as it is the implementation of a monitoring software to detect vulnerabilities in the network.

It begins with details of the basic concepts about information security and its main threats, in order to have the necessary subject matter of the important aspects of security, the threats and to know the norm or standard that serves to generate a rigorous control.

Continuing with an analysis of the monitoring tools known worldwide and their main characteristics, which will serve as a guide for a company that wants to carry out this type of implementation. The process of managing threats and vulnerabilities must be known, based on the Ecuadorian technical standard ISO 27005, which details the procedures for dealing with them.

Once the tool to be used is selected, which is analyzed in Chapter 2, the implementation of the Bagant Ecuadorian company network is carried out; this tool shows the final results of the tests and the behavior of the system

ÍNDICE

INTRODUCCIÓN 1

1. CAPÍTULO I: MARCO TEÓRICO 5

1.1. Definiciones y Terminología 5

1.1.1. Navegación Anónima 5

1.1.2. Hacktivista 5

1.1.3. Script Kiddie 5

1.1.4. Sniffer 5

1.2. Hash 6

1.3. Malware 6

1.3.1. Bot 6

1.3.2. Botnet 6

1.3.3. Rootkit 6

1.3.4. Ransomware 6

1.3.5. Troyano 7

1.3.6. Virus 7

1.3.7. Gusano 7

1.4. Deep Web 7

1.4.1. Nivel 1: 8
1.4.2. Nivel 2: 9
1.4.3. Nivel 3: 9
1.4.4. Nivel 4: 9
1.4.5. Nivel 5: 9
1.5. Ingeniería Social 9
1.6. Intrusión Física 9
1.7. Seguridad Integral 10
1.8. Hacking Ético 10
1.8.1. Fases del hacking 10
1.8.1.1. Fase 1: Reconocimiento 11
1.8.1.2. Fase 2: Escaneo 11
1.8.1.3. Fase 3: Obtención de datos (explotación) 12
1.8.1.4. Fase 4: Mantener Acceso 12
1.8.1.5. Fase 5: Limpiar Huellas 13
1.9. Vulnerabilidad 13
1.10. Amenazas 15

1.11. Norma INEN-ISO 27005 18

2. CAPITULO II. ANÁLISIS DE HERRAMIENTAS DE SOFTWARE LIBRE Y PROPIETARIO 19

2.1. Herramientas de software libre para el control de vulnerabilidades 19

2.1.1. Acunetix 19

2.1.1.1. Como funciona Acunetix Web Vulnerability: 20

2.1.1.2. Empresas que han implementado el software 21

2.1.2. OpenVas 22

2.1.2.1. Características 22

2.1.2.2. Requerimientos mínimos para instalar en una máquina virtual 23

2.1.2.3. Casos de estudio 23

2.2. Herramientas de software propietario para el control de vulnerabilidades 23

2.2.1. InsightVM 23

2.2.1.1. Características 23

2.2.1.2. Empresas que han implementado el software 26

2.2.2. Nessus 27

2.2.2.1. Características 27

2.2.2.2. Ventajas de usar Nessus 28

2.2.2.3. Empresas que han implementado el software 28

2.2.2.4. Costo del sistema 29

2.3. Herramientas de software libre para el monitoreo de amenazas 30

2.3.1. Security Onion 30

2.3.1.1. Funciones Principales 34

2.3.1.2. Requerimientos mínimos del sistema 34

2.3.1.3. Ventajas y Desventajas 35

2.3.2. OSSIM 36

2.3.2.1. Requerimientos mínimos del sistema 36

2.3.2.2. Tipos de Implementación 36

2.3.2.3. Empresas que han implementado el software 39

2.4. Herramientas de software propietario para el monitoreo de amenazas 40

2.4.1. AlienVault 40

2.4.1.1. Características 40

2.4.1.2. Empresas que han implementado el software 41

2.4.1.3. Requerimientos mínimos para instalar AlienVault 42

2.4.2. SolarWinds 44

2.4.2.1. Características 44

2.4.2.2. Requerimientos del sistema 48

2.4.2.3. Costo del sistema 49

2.5. Determinación de la herramienta a utilizar 49

3. CAPÍTULO III: ANÁLISIS DE VULNERABILIDADES Y BRECHAS DE SEGURIDAD 53

3.1. Causas de las vulnerabilidades 53

3.1.1. Diseño de los protocolos utilizados en las redes 53

3.1.2. Programación 53

3.1.3. Políticas de seguridad deficientes 53

3.2. Proceso de gestión de riesgos de seguridad 54

3.2.1. Establecimiento del contexto 55

3.2.1.1. Criterios de evaluación de riesgo 55

3.2.1.2. Criterios de la aceptación del riesgo 55

3.2.2. Valoración del riesgo 56

3.2.3. Análisis del riesgo 56

3.2.3.1. Introducción a la identificación del riesgo 56

3.2.4. Estimación del riesgo 57

3.2.4.1. Metodologías para la estimación del riesgo 57

3.2.4.2. Valoración de las consecuencias 58

3.2.4.3. Valoración de los incidentes 58

3.2.5. Evaluación del riesgo 59

3.2.6. Tratamiento del riesgo 59

3.2.7. Aceptación del riesgo 61

3.2.8. Comunicación del riesgo 61

3.2.9. Monitoreo y revisión del riesgo 62

4. CAPÍTULO IV: IMPLEMENTACIÓN DEL CENTRO DE MONITOREO 63

4.1. Topología de la red 63

4.2. Diagrama de Implementación 65

4.3. Implementación 68

4.3.1. Sistema Operativo 69
4.3.2. Red 71
4.3.3. Sensores y Servidores 72
4.4. Pruebas y Resultados 73
4.4.1. Violación de alerta 75
4.4.2. Virus 77
4.4.3. Ataque de fuerza bruta 79
4.4.3.1. Diagrama de Simulación de ataque 80
4.4.4. Ping de la Muerte 82
4.4.5. Owasp 84
5. CONCLUSIONES Y RECOMENDACIONES 85
5.1. Conclusiones 85
5.2. Recomendaciones 86
REFERENCIAS 88

ÌNDICE DE FIGURAS

Figura 1. Niveles de la Deep Web 8

Figura 2. Funcionamiento Acunetix 21

Figura 3. Agente de Punto Final 24

Figura 4. Paneles en vivo 25

Figura 5. Priorización de riesgo 25

Figura 6. Evaluación de infraestructura virtual y en la nube 26

Figura 7. Alertas Snort 31

Figura 8. Rendimiento de Suricata 31

Figura 9. Cola de alertas en la pestaña de eventos 32

Figura 10. Verificación de paquetes de una IP 33

Figura 11. Tráfico de la red 33

Figura 12. Trafico de la red con NetworkMiner 34

Figura 13. Dispositivo todo en uno 37

Figura 14. Dispositivo todo en uno y sensor remoto 38

Figura 15. Diseño complejo con sus componentes 39

Figura 16. Capacidades esenciales de AlienVault 41

Figura 17. Monitoreo de red 45

Figura 18. Análisis de ruta. 46

Figura 19. Herramienta de mapeo de red 47

Figura 20. Mapas de calor inalámbricos 47

Figura 21. Alertas de monitoreo 48

Figura 22. Cuadrante Mágico para información de seguridad y gestión de eventos ……..52

Figura 23. Proceso de gestión del riesgo de la seguridad de la información 54

Figura 24. Actividad para el tratamiento del riesgo 60

Figura 25. Diagrama de red Bagant Ecuatoriana 64

Figura 26. Diseño de red con Security Onion 66

Figura 27. Pantalla de Arranque 69

Figura 28. Selección de Idioma 69

Figura 29. Tipo de Instalación 70

Figura 30. Configuración Zona Horaria. 70

Figura 31. Registro de usuario y contraseña 71

Figura 32. Configuración de la red 71

Figura 33. Dirección ip 72

Figura 34. Sub mascara de Red..... 72

Figura 35. Modo de configuración 72

Figura 36. Nombre de Usuario a interfaces 73

Figura 37. Contraseña a interfaces 73

Figura 38. Máquina virtual Security Onion..... 74

Figura 39. Máquina virtual kali linux 74

Figura 40. Máquina virtual Windows Server 2012 75

Figura 41. Herramienta Squert 75

Figura 42. Alertas encontradas 76

Figura 43. Regla de acceso en el firewall 76

Figura 44. IP intentando ingresar a spotify 77

Figura 45. Comando para ejecutar el virus zeus 77

Figura 46. Envió de paquetes de forma masiva 78

Figura 47. Alerta de virus en Security Onion 78

Figura 48. Eventos de alerta de virus 79

Figura 49. Archivo Diccionario de datos 79

Figura 50. nmap a la ip de servidor 80

Figura 51. Diagrama de ataque 81

Figura 52. Herramienta medusa 81

Figura 53. Alerta de fuerza Bruta 82

Figura 54. Descripción ddos.bat 82

Figura 55. Ejecución del archivo .bat 83

Figura 56. Alerta generada por ping de la muerte. 83

Figura 57. Pentesting owasp 84

Figura 58. Alerta pentesting owasp 84

ÍNDICE DE TABLAS

Tabla 1. Clasificación de las vulnerabilidades según su función de gravedad. 14

Tabla 2. Tipos de atacantes 15

Tabla 3. Tipos de ataques. 16

Tabla 4. ¿Cómo actúan los ataques? 17

Tabla 5. Listado de empresas de acunetix vulnerability. 21

Tabla 6. Listado de empresas de InsightVM 26

Tabla 7. Listado de empresas de Nessus. 29

Tabla 8. Listado de precios del sistema. 29

Tabla 9. Ventajas y desventajas Security Onion. 35

Tabla 10. Listado de empresas de Ossim 40

Tabla 11. Listado de empresas de AlienVault 42

Tabla 12. Requerimientos de hardware 42

Tabla 13. Requerimientos mínimos para máquinas virtuales 43

Tabla 14. Navegadores soportados para AlienVault 44

Tabla 15. Requisitos del sistema máquina virtual 48

Tabla 16. Comparación de los sistemas Open Source para monitoreo 50

Tabla 17. Descripción de hardware de la empresa Bagant Ecuatoriana. 67

Tabla 18. Direccionamiento IP de las interfaces..... 68

INTRODUCCIÓN

El manejo de la tecnología de la información y todas las actividades de la naciones y sociedad en general, han hecho que la dependencia sobre el internet y el uso del ciberespacio constituya una puerta de acceso para que se realicen ciber delitos y nuevas amenazas, en este escenario no hay fronteras, ni actores, ni lindero para que estas nuevas amenazas puedan afectar la seguridad de una empresa o de un estado. Por consecuencia, ha habido grandes pérdidas económicas surgiendo la necesidad de que las empresas fomenten políticas y planificación en este nueva era de ciber seguridad. (Arturo, 2019, pág. 157)

El ambiente digital en que se está desarrollado el mundo debe tener en cuenta los riesgos que día a día se presenta en el uso de las redes ya que todos los procesos que se llevan generan productividad en cualquier mercado. En la actualidad el uso de la información hace que la sociedad esté enlazada a través del internet, permitiendo que las personas se conecten a través de las redes y sean blancos potenciales para los ciber delincuentes. (Arturo, 2019, pág. 158)

Una empresa de construcción es aquella a que se dedica a proveer soluciones al sector de la construcción, elevación y de carrocerías de carga a nivel nacional (Bagant Ecuatoriana Cía. Ltda, 2019).

Para ofrecer su servicio de manera eficiente hacia sus clientes cuenta con un departamento de ventas, la misma que está conformada por personas capacitadas en el área de construcción que le brindaran asesoramiento a sus necesidades con el apoyo de la área de TI.

La compañía cuenta con un sistema ERP centralizado administrado por el departamento de TI el cual permite tener un control de inventario de los productos que posee la empresa en las diferentes sucursales.

El sistema SAP ERP ofrece una gran diversidad de opciones de uso al poseer diferentes módulos como por ejemplo; contabilidad financiera, gestión de materiales, planificación de productos, etc. (SoftDoit, s.f).El mismo que dentro de la compañía es muy importante ya que controla y administra todas las funciones que día a día la empresa ejerce para dar un servicio de excelente calidad a sus clientes.

Adicionalmente, la empresa cuenta con equipos de infraestructura necesarios para facilitar la labor diaria de sus empleados, estos junto con el SAP ERP deben ser constantemente monitoreados ya que son vulnerables a ataques relacionados con la seguridad de la información; lo cual puede provocar pérdidas económicas, filtrado de información confidencial de sus clientes y por lo tanto perdida de estos.

Alcance

El presente proyecto pretende, realizar un análisis de las herramientas de software libre y propietario que existen en la actualidad en el mercado que serán utilizadas para verificar y controlar las vulnerabilidades.

Identificar las vulnerabilidades, brechas de seguridad y mantener el sistema de alerta temprana a fin de tomar las medidas de prevención necesarias.

Utilizar las herramientas investigadas para implementar un centro de monitoreo dentro de la organización y poder corregir las vulnerabilidades existentes dentro de la misma.

Justificación

Hoy en día, las compañías enfrentan más riesgos que nunca en un mundo diverso, complejo y versátil. Una mejor intuición de los riesgos tradicionales y emergentes que se presentan día a día, puede ayudar al personal de TI a crear y priorizar estrategias para salvaguardar la información para que esta no caiga en manos indebidas.

Debido a los diferentes sucesos que han afectado a las empresas en materia de seguridad en distintos periodos de tiempo, las decisiones tomadas para salvaguardar la integridad de la información no han sido suficientes, se requiere realizar un análisis de riesgos y vulnerabilidades para identificar y tratar los riesgos.

Este análisis de herramientas para el control de vulnerabilidades permitirá mejorar y fortalecer políticas de seguridad de la información en la compañía, para lo cual el personal de TI deberá implementar controles a usuarios, restricciones en la red, implementación de técnicas de sensibilización a usuarios en el manejo de la información ya sea este de manera local o en red, que a futuro favorecerán a una mejor gestión de la información.

Es importante para la empresa la implementación de este proyecto ya que la misma tiene información que es manejada en el trabajo diario y la pérdida de integridad de esta información puede provocar daños económicos, falta de confiabilidad de la empresa y por lo tanto se pueden perder clientes importantes.

Objetivo General

Analizar las herramientas necesarias para el control de vulnerabilidades internas y externas e implementar un centro de monitoreo y alerta temprana para una empresa de construcción.

Objetivos Específicos:

1. Analizar las herramientas de software libre y propietarias necesarias para el control de vulnerabilidades internas y externas.
2. Detectar las posibles vulnerabilidades y brechas de seguridad que afectan al normal desempeño de la compañía
3. Implementar un sistema de monitoreo y alerta temprana de vulnerabilidades y ataques de seguridad

Metodología:

En el proyecto se aplicará los siguientes métodos:

El método inductivo se utilizará para realizar un análisis de las herramientas de software libre y propietario que existen en la actualidad en el mercado, esto permita realizar un control y monitoreo de vulnerabilidades que posee la compañía y así deducir las amenazas, vulnerabilidades y brechas de seguridad para luego realizar las acciones correctivas correspondientes.

Se utilizará el método experimental al momento de realizar la implementación de acuerdo con los criterios, utilidades, características de la herramienta analizada previamente, en donde se dispondrá de la infraestructura y equipos de la compañía para realizar un monitoreo de las vulnerabilidades y brechas de seguridad encontradas dentro de la red y de esta manera tomar acciones correspondientes a las amenazas encontradas.

1. CAPÍTULO I: MARCO TEÓRICO

En este capítulo, se detallará conceptos básicos sobre seguridad de la información, vulnerabilidades, hacking ético, tipos de virus y como están conformados.

1.1. Definiciones y Terminología

Existen términos que deben ser especificados, en base al hacking ético y seguridad informática, entre ellos se va a definir las vulnerabilidades, ataques, software malicioso, etc.

1.1.1. Navegación Anónima

La navegación anónima se trata de acceder a sitios de internet evitando la detección online del dispositivo o persona que lo esté realizando. Muchas personas indagan por anonimato por una diversidad de motivos, algunos de estos puedes ser legales o legítimos y en otros casos no.

1.1.2. Hacktivista

Es aquella persona o grupo de personas que mediante el uso de las redes informáticas y redes sociales buscan rendir protesta con fines políticos o sociales a través de la irrupción, sea este leal o ilegal.

1.1.3. Script Kiddie

Persona que desconoce sobre informática y que utiliza scripts o programas desarrollados por otras personas para realizar ataques a sistemas, redes informáticas con el fin de impresionar a las demás personas.

1.1.4. Sniffer

Es una aplicación destinada para las redes informáticas que se encarga de capturar y analizar los paquetes (entrada/salida) que son enviados en una red.

1.2. Hash

Es un algoritmo aritmético que codifica una cadena de caracteres (texto, documento, archivo) con la misma longitud y los codifica y a partir de lo cual no se podrá descifrar la información original.

1.3. Malware

El malware o software malicioso describe a cualquier tipog de programa o código informático cuya función es dañar el sistema operativo o causar un mal funcionamiento, dentro de esta categoría podemos encontrar los siguientes:

1.3.1. Bot

Un bot es un software que su principal función es realizar tareas repetitivas a través de una conexión a internet, cuya tarea por parte de una persona seria irrealizable o tediosa.

1.3.2. Botnet

Un botnet está conformado por una red de equipos infectados por software malicioso, que son controlados por una persona que tiene el rol de atacante y una vez que un equipo es infectado se dice que es un robot o zombi.

1.3.3. Rootkit

Es un conjunto de programas que permiten a los hackers frecuentemente conseguir ilícitamente acceso y robar información del equipo de la persona infectada sin ser detectados.

1.3.4. Ransomware

Es un software que al infectar el equipo le da acceso al hacker la facultad de bloquear el dispositivo desde una ubicación remota y encriptar los archivos de la

víctima y lanzar mensajes de información solicitando el pago para restablecer la información por medio de una moneda virtual.

1.3.5. Troyano

Un troyano es un tipo de malware que a menudo se disfraza de software legítimo e inocente cuya función es que al ejecutarlo le brinda al hacker acceso remoto al equipo afectado.

1.3.6. Virus

Un virus informático es un software dañino que principalmente ataca los archivos de arranque y se replica así mismo para continuar con la propagación.

1.3.7. Gusano

Es un malware que tiene la cualidad de duplicarse a sí mismo, albergarse en diferentes ubicaciones del computador. Su principal característica es propagarse y afectar al mayor número de equipos y dispositivos posibles.

1.4. Deep Web

Su definición es internet profunda y está compuesta por todo aquel contenido del internet que por diferentes motivos no se encuentra indexado con los motores de búsqueda que se encuentran en el mercado, el contenido de esta plataforma está relacionado con las drogas, tráfico de órganos y pornografía infantil, etc.

Como se puede visualizar en la Figura 1, indica los 5 niveles que tiene la Deep Web las mismas que serán detalladas:

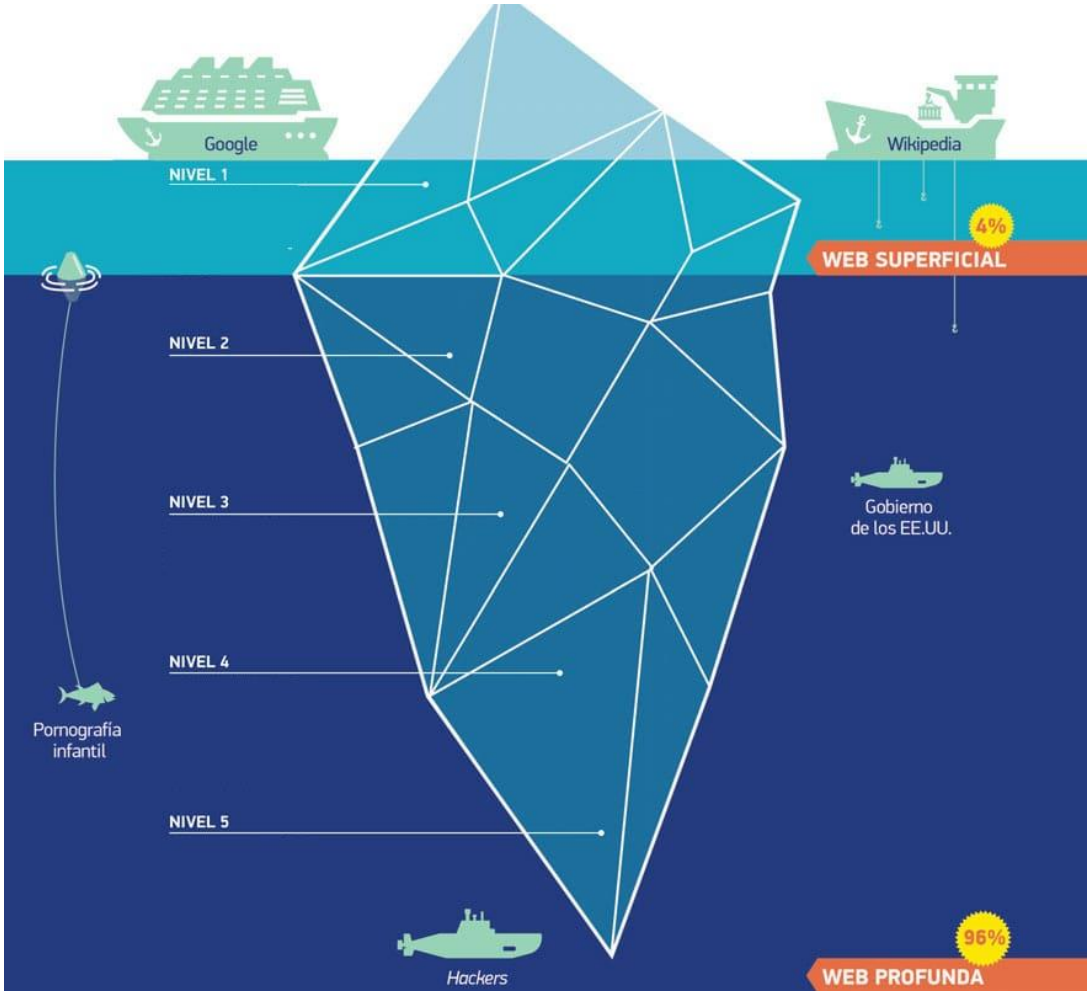


Figura 1. Niveles de la Deep Web
Adaptado de (Mejor antivirus, 2018).

1.4.1. Nivel 1:

Se puede acceder a las páginas web por medio de los buscadores convencionales, toda persona con acceso a internet tiene la facultad de realizar la navegación.

1.4.2. Nivel 2:

Aquí se pueden encontrar las páginas que no han sido indexadas a los tradicionales buscadores para poder realizar las consultas. Es decir, se necesita acceder por medio de una contraseña o son páginas difíciles de encontrar.

1.4.3. Nivel 3:

Los navegadores comienzan a toparse con la parte ilegal de la red, en este nivel es donde se realiza la piratería, aquí se debe utilizar un proxy para ingresar de manera anónima.

1.4.4. Nivel 4:

En este nivel todos los sitios web son monitoreados por el Gobierno de los Estados Unidos de América, ya que la mayor parte de su contenido es ilegal por ejemplo se localiza páginas con pornografía infantil.

1.4.5. Nivel 5:

En esa zona más profunda de internet se hallan sitios que solamente se pueden acceder por medio de TOR (The Onion Router; el navegador TOR permite enmascarar la dirección IP del navegante, actúa de manera similar a un servidor proxy), todo su contenido es ilegal y existen departamentos de inteligencia estatal que buscan quienes son las personas que navegan por estos sitios. (Antivirus, 2018)

1.5. Ingeniería Social

La ingeniería social es el conjunto de técnicas que usan los hacker para obtener información confidencial de las víctimas como contraseñas, datos bancarios también infectando sus dispositivos electrónicos con malware y accediendo a sitios infectados.

1.6. Intrusión Física

Son los accesos que los sistemas informáticos realizan de forma remota o física ya sea en un ambiente de pruebas o de producción.

1.7. Seguridad Integral

Es aquella que globaliza la seguridad laboral, digital, física, humana y sobre todo posibilitando un diseño para una estrategia corporativa única, optimizando el diseño para utilizar los recursos del trabajo.

1.8. Hacking Ético

Cuando tratamos de hacking ético nos referimos a la gestión de efectuar pruebas de intrusiones controladas sobre una red de equipos informáticos; es sostener que el consultor o *pentester*, actuara como un cracker para logra encontrar vulnerabilidades en los equipos explotados con el fin de descubrir las brechas de seguridad que se deben implementar.

La principal característica del hacking ético es de proveer a empresas o instituciones el conocimiento que deben tener para protegerse de ciber ataques y conseguir los siguientes propósitos:

- Adelantarse a posibles atacantes, detectando y reparando las diferentes vulnerabilidades que existan y puedan llevarse a acabo en un ataque.
- El Instruir a empleados, delegados y profesionales el conocimiento necesario sobre ciber seguridad.
- Incremento de la seguridad informática como la actualización de software, planes de contingencia y establecer políticas de respaldo de información y copias de seguridad, etc.

1.8.1. Fases del hacking

Las fases del hacking se dividen en 5 fases. Un hacker ético realiza técnicas similares a la de un hacker malicioso las cuales son:

1.8.1.1. Fase 1: Reconocimiento

Se trata de obtener la mayor cantidad de datos posible del objetivo, a mayor cantidad de información el objetivo más eficiente el ataque. En esta fase hay dos modos: activo y pasivo.

El modo pasivo se trata de obtener información sin el consentimiento del usuario mediante técnicas de hackeo como ingeniería social, sniffing, o mediante la vigilancia de las instalaciones con el fin de recolectar información sobre los empleados, acceso, infraestructura, etc. (Sanchez G. , 2019)

El modo activo implica sondear la red para detectar equipos individuales, direcciones IP y los servicios que brindan. Este modo es más riesgoso a la detección que del modo pasivo. (Sanchez G. , 2019)

Ambos modos, activo, pasivo tiene la finalidad de obtener información útil para llevar a cabo el ataque. Esto permite a un hacker encontrar ciertas vulnerabilidades y deficiencias en los servicios y sistemas y aprovechar estas deficiencias para obtener acceso a la información (Sanchez R. C., 2019, pág. 1)

1.8.1.2. Fase 2: Escaneo

En la fase escanear es una fase pre-ataque esto consiste en tomar la información que se realizó en la fase de reconocimiento y utilizar para examinar la red, el hacker puede emplear herramientas para su explotación que incluyen:

- Scanner de Puertos.
- Scanner de vulnerabilidades
- Barrido de ping.
- Mapeos de red, etc.

Con el fin de conseguir cierta información para poder realizar un ataque contra el objetivo y estos son:

- Versión del sistema operativo
- Sistemas instalados
- Direcciones IP
- Cuentas de usuario, etc. (Sanchez R. C., 2019, pág. 2)

1.8.1.3. Fase 3: Obtención de datos (explotación)

En esta fase se utiliza la información para la explotación de las vulnerabilidades encontradas en las fases anteriores y así poder acceder al objetivo.

La explotación puede ocurrir de forma:

- LAN (Local Area Network)
- Offline (sin estar conectado)
- Internet

Y se puede incluir técnicas como:

- Ataques Man-in-the-middle
- Desbordamiento de buffer
- DoS
- DDoS
- Sesión Hijacking (Secuestro de sesión)

Pueden ser ataques a:

- Sistema Operativo
- Aplicaciones de escritorio
- Aplicaciones Web

1.8.1.4. Fase 4: Mantener Acceso

Una vez efectuada la invasión en el sistema a través de deficiencia encontrada, la finalidad del hacker es mantenerse dentro del mismo, para seguir obteniendo más información, encontrar nuevas vulnerabilidades y poder tener acceso total.

Para lo cual opta de algunas herramientas para tener acceso al sistema:

- Backdoor (Puertas Traseras),
- Troyanos,
- Shell o Shell Inversa
- RootKits,
- Keyloggers (malware),
- Spyware.

1.8.1.5. Fase 5: Limpiar Huellas

En esta fase el hacker debe ocultar sus huellas evitando que los administradores o auditores puedan encontrar evidencias de los accesos no autorizados que se realizó a cabo en la red.

Existen herramientas y métodos para ocultar las huellas de un hacker:

- Troyanos
- Tunneling
- RootKits
- WinZapper
- Navegación Anónima: Tor, Proxys Anónimos, VPN, etc.
- Alteración de los Log Files
- Eliminar los archivos del IDS (Sistema de Detención de Intrusos).

1.9. Vulnerabilidad

Una vulnerabilidad informática es aquella debilidad tanto en software como en hardware, que permite al invasor exponer la integridad, disponibilidad y confidencialidad de los sistemas (Mediapro, 2018).

Las vulnerabilidades son el resultado de fallos realizados por un mal diseño de software o por error humano, sin embargo, una vulnerabilidad puede ser producida por las limitaciones que tiene la tecnología para la que fue construido. (Informatica T. , s.f.)

Podemos discernir tres tipos de vulnerabilidades que afectan a nuestro sistema:

- **Vulnerabilidades ya conocidas sobre aplicaciones o sistemas instalados:** Son aquellas vulnerabilidades que ya se tiene conocimiento de lo que va efectuar o como se va a comportar al momento de atacar, las empresas que lo elaboran tienen el entendimiento del mismo y para lo cual ya tienen una solución.
- **Vulnerabilidades conocidas sobre aplicaciones no instaladas:** También son conocidas por las empresas desarrolladoras de cómo es su comportamiento y que no más puede ocasionar, pero no se sabe cómo va a actuar la aplicación instalada.
- **Vulnerabilidades aun no conocidas:** Estas vulnerabilidades aún no han sido identificadas por las empresas desarrolladoras, por lo que sí es descubierta por cualquier otra persona puede utilizarla para su beneficio. (Informatica S. , 2013)

En la Tabla 1 se puede observar la clasificación de las vulnerabilidades según su función de gravedad.

Tabla 1.

Clasificación de las vulnerabilidades según su función de gravedad

Tipo	Definición
CRÌTICA	Estas vulnerabilidades permiten la facultad de que las amenazas se propaguen sin que la víctima participe
IMPORTANTE	La vulnerabilidad es capaz de poner en peligro la confidencialidad, integridad o disponibilidad de la información como también los recursos de procesamiento.
MODERADA	Este tipo de vulnerabilidad son más sencillas de controlar, su impacto se puede disminuir a partir de configuraciones predeterminadas.
BAJA	La vulnerabilidad no es aprovecha por el atacante y su impacto es mínimo.

Tomado de (Informatica S. , 2013)

1.10. Amenazas

Una amenaza es la acción que explota una vulnerabilidad para exponer un sistema de información. Las amenazas pueden ser tanto internas como externas y formalizar un ciber ataque.

Para identificar las amenazas que un sistema informático está expuesto en la Tabla 2 se identifica los tipos de atacantes con su respectiva definición.

Tabla 2

Tipos de atacantes

Nombre	Definición

Hacker	Especialista con conocimientos informáticos con curiosidad de encontrar nuevas vulnerabilidades y explotarlas.
Crackers	Hacker con intenciones de dañar o para obtener beneficio económico.
Phreakers	Cracker telefónico con conocimientos de redes de telefónica que sabotean dichas redes para obtener llamadas gratuitas.
Sniffer	Personas competentes en análisis de tráfico de red para la obtención de información.
Lammers	Individuos sin gran conocimiento informático que se hacen llamar hackers y se vanaglorian de hacerlo.
Newbie	Hacker novato
Ciberterrorista	Expertos con intelecto informático e intrusiones en redes que elaboran como espías y revolucionario.
Programadores de Virus	Expertos en programación en producir sistemas dañinos que producen deficiencias en los sistemas y aplicaciones

Tomado de (Informatica S. , 2013)

Se debe conocer que tipos de ataques son los más frecuentes que realiza un hacker como está especificado en la Tabla 3.

Tabla 3.

Tipos de ataques

Nombre del ataque	Definición
Interrupción	Recurso del sistema o infraestructura que deja de estar en función debido al ataque recibido.
Intersección	Un atacante accede al sistema o a la información que se envía por medio de la red
Modificación	Los datos han sido modificados por lo que la integridad de la información ya no es válida.
Fabricación	Se produce un nuevo sistema o programa difícil de distinguir del original y poder obtener información valiosa.

Tomado de (Informatica S. , 2013)

En la Tabla 4, apreciamos los ataques y cómo actúan cada uno de ellos y que consecuencia tienen.

Tabla 4

¿Cómo actúan los ataques?

Ataque	¿Cómo actúan?
Spoofing	Suplantación de la identidad de la victima
Sniffing	Análisis y monitorización de la red para obtener información.

Conexión no autorizada	Indagan en busca de agujeros en la infraestructura, y cuando lo consiguen, se realiza la conexión no autorizada
Keyloggers	Es una herramienta que utilizan los hacker para obtener información sobre lo que se digita con el teclado
Denegación de Servicio	Suspende el servicio que se está dando en servidores o en la red
Ingeniería Social	Accede a la información confidencial de la víctima y los usa con fines maliciosos.
Phishing	Se engatusa al usuario y así obtener información, reemplazando la identidad de un sistema o página web

Tomado de (Informatica S. , 2013)

1.11. Norma INEN-ISO 27005

Esta norma proporciona instrucciones para realizar la gestión del riesgo de la seguridad de la información en una entidad u organización, brindando fundamentos necesarios a los requerimientos de un sistema de gestión de seguridad de la información de acuerdo a lo establecido con la NTE INEN-ISO/IEC 27001. (INEN, 2012, pág. v)

2. CAPITULO II. ANÁLISIS DE HERRAMIENTAS DE SOFTWARE LIBRE Y PROPIETARIO

En la actualidad toda persona u organización utiliza equipos inteligentes, ordenadores, redes inalámbricas, etc.; estos dispositivos se encuentran propensos a un sin número de amenazas cibernéticas mediante la utilización de correos electrónicos, páginas web, aplicaciones, redes sociales, etc.

En este capítulo se analizará las herramientas de software libre y propietario que actualmente se encuentran en el mercado para el control de vulnerabilidades y para la implementación de un centro de monitoreo:

2.1. Herramientas de software libre para el control de vulnerabilidades

2.1.1. Acunetix

Acunetix es una herramienta Open Source que proporciona seguridad a las aplicaciones web, permite analizar las posibles entradas que los hackers puedan tener en el sitio web y así poder cerrarlas. (GREENETICS, 2018)

Entre las características descritas en (Acunetix, 2019); para que los administradores web puedan detectar las vulnerabilidades son:

- Acusensor permite el sondeo de vulnerabilidades
- Efectuar test de inyección SQL y XSS
- Examina los lugares y formularios que se encuentran salvaguardados por contraseñas pocas seguras.
- Examina la seguridad al iniciar sesión en las páginas web con CAPTCHA
- Simplicidad en generación de informes
- Herramientas de penetración, como HTTP Editor y HTTTP Fuzzer

- Análisis y escaneo de sitios web incluyendo contenido flash, Soap y Ajax
- Indagación de puertos de red del servidor web para un mayor control de seguridad

2.1.1.1. Como funciona Acunetix Web Vulnerability:

(Acunetix, 2019), muestra el funcionamiento del software detallado a continuación:

- **Crawling (rastreador):**

  El rastreador examina los webs site desde la URL para detectar los directorios y archivos, luego procederá a la revisión y análisis de la estructura de los directorios del sitio web

- **Escaneo de Vulnerabilidades**

  Acunetix arroja una serie de ataques de vulnerabilidades, a continuación, realiza pruebas de control en cada página, similar a los que los hackers realizan para atacar un web site.

- **Resultados**

  Una vez encontrado las vulnerabilidades se detallará la información en una interfaz gráfica del software. Las alertas abarcan información de cada vulnerabilidad encontrada.

- **Creación de informes**

  El software posee una variedad de informes que permite verificar los escaneos para poder así fijar y probar las vulnerabilidades de forma individual y volver a ejecutar un escaneo completo.

  Para comprender mejor el funcionamiento del software se presenta la Figura 2 como un diagrama de bloques.

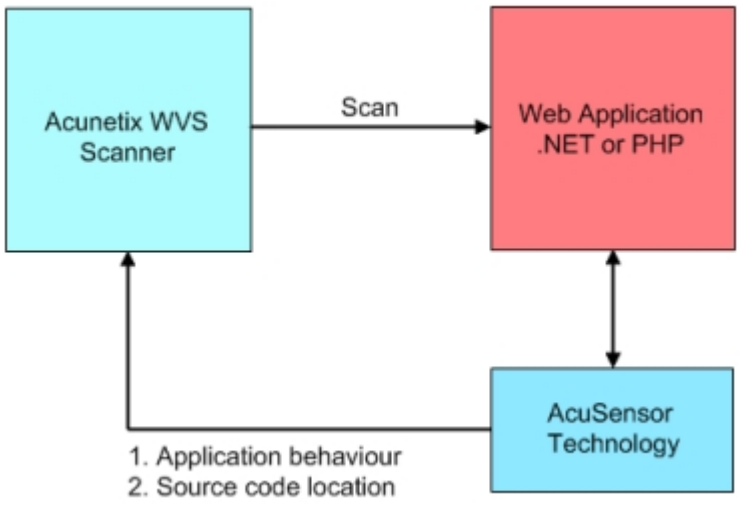


Figura 2. Funcionamiento Acunetix

Tomado de (*Multisystem*, 2014)

2.1.1.2. Empresas que han implementado el software

Existen varias empresas a nivel mundial que utilizan el sistema acunetix vulnerability, las mismas que son detalladas en la tabla 5.

Tabla 5.

Listado de empresas de acunetix vulnerability

CLIENTES		
NASA	Hewlett Packard	State of North Carolina
US Army	AmSouth Bank	US Geological Service
US Air Force	US Department of Energy	France Telecom

KPMG	California Department of Justice	ActionAid UK
Bank of China	Wescom Credit Union	University of Reading
Fujitsu	Trend Micro	Disney
Panasonic Asia Pacific	The Armed Forces of Norway	Credit Suisse

Tomado de (Acunetix, 2019)

2.1.2. OpenVas

Como lo afirma (OpenVAS, s,f), Openvas (Open Vulnerability Assessment System) es una herramienta que proporciona efectuar un escaneo y gestión de vulnerabilidades en la red y este es una distribución Open Source.

2.1.2.1. Características

(ESET, 2014), entre las características de las herramientas podemos mencionar las siguientes:

- Posee un framework que posee servicios y herramientas de apreciación para realizar una evaluación de vulnerabilidades que se realizan de forma individual o en grupo, con la ayuda de la herramienta OSSIM que se encuentra incluida en el mismo.
- La distribución Kali Linux ya cuenta con estas herramientas las cuales se pueden utilizar con dos clientes por medio de comandos y la otra utilizando una interfaz gráfica y con el uso de la herramienta metasploit, se puede realizar la explotación de vulnerabilidades.

- Cuenta con un gestor de servicio que ejecuta tareas de filtrado y clasificación de los resultados de los análisis.

2.1.2.2. Requerimientos mínimos para instalar en una máquina virtual

Según (INFOSEC RESOURCES , 2020), para tener un óptimo rendimiento al momento de realizar la instalación en una máquina virtual se debe considerar lo siguiente:

- 2 GB Memoria RAM
- 10 GB de disco duro
- 2 procesadores

2.1.2.3. Casos de estudio

La herramienta Open Vas según (Greenbone Networks, 2019), ha proporcionado a sus clientes soluciones que encajan en sus necesidades y presentan los siguientes casos de uso:

- Gestión de vulnerabilidades, Universidad de las Fuerzas Armadas de Múnich
- Gestión de vulnerabilidades, TU Dresden

2.2. Herramientas de software propietario para el control de vulnerabilidades

2.2.1. InsightVM

Como lo afirma (Rapid7, 2019); InsightVM es un sistema de seguridad de gestión de vulnerabilidades y pruebas de intrusión. Este ofrece visibilidad en vivo de la infraestructura que está en la nube virtual y remota, para que así se pueda tener monitoreo toda la infraestructura.

2.2.1.1. Características

Entre las características más importantes tenemos las siguientes:

- **Agente de punto final:**

  Agente de punto final reúne todos los datos de sus puntos finales, también aquellas terminales remotas y que se encuentran activas de manera confidencial, o que rara vez se unen a la red, como se puede visualizar en la Figura 3, se valida todos los sistemas operativos que se encentran en la infraestructura.

Figura 3. Agente de Punto Final
Tomado de (RAPID 7, s.f)

- **Paneles en vivo**

  Los paneles que posee InsightVM son en vivo e interactivos con el administrador, se puede crear paneles personalizados para cualquier tipo de persona, como se puede apreciar en la Figura 4, los administradores pueden realizar el monitoreo del comportamiento de la red en los diferentes paneles.

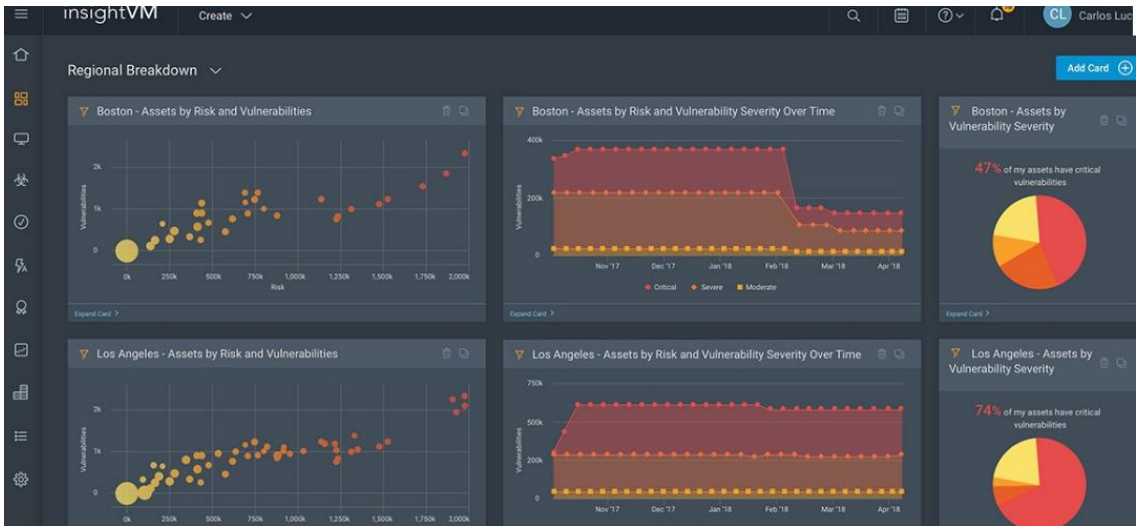


Figura 4. Paneles en vivo

Tomado de (RAPID 7, s.f)

- **Priorización de Riesgo**

  InsightVM proporciona una escala de 1-1000 basada en la probabilidad de que un atacante explote la vulnerabilidad en un ataque real. Como se indica en la Figura 5, se da prioridad a una o ciertas vulnerabilidades para que estas sean monitoreadas como lo que haría un hacker.

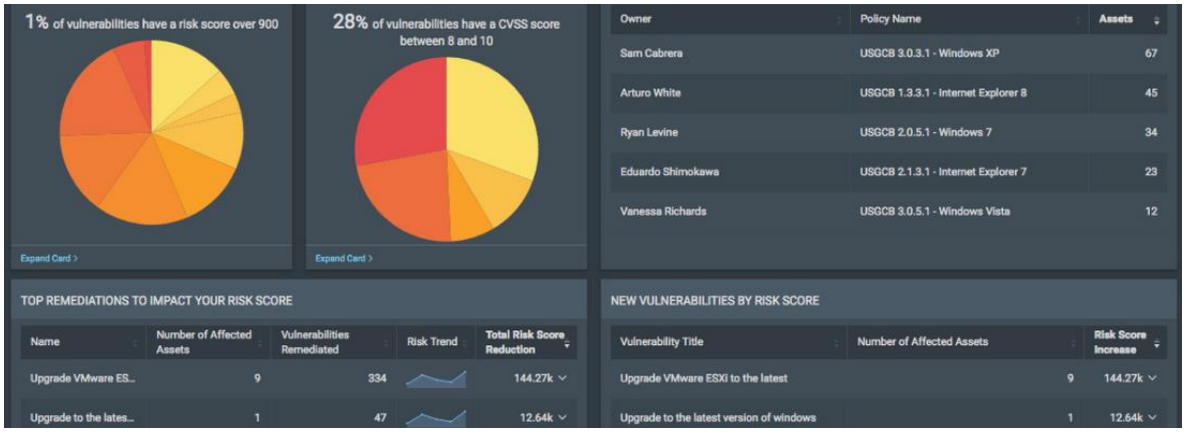


Figura 5. Priorización de riesgo

Tomado de (RAPID 7, s.f)

- **Evaluación de infraestructura virtual y en la nube:**

  El sistema permite integrar y garantizar que todos los servicios que se encuentran en la nube virtualizada o que están en una infraestructura física se puedan visualizar y poder tener el control de las mismas para un mejor control de la red.

En la Figura 6 se puede apreciar la integración de las diferentes infraestructuras que se pude tener en la nube como en una infraestructura física.

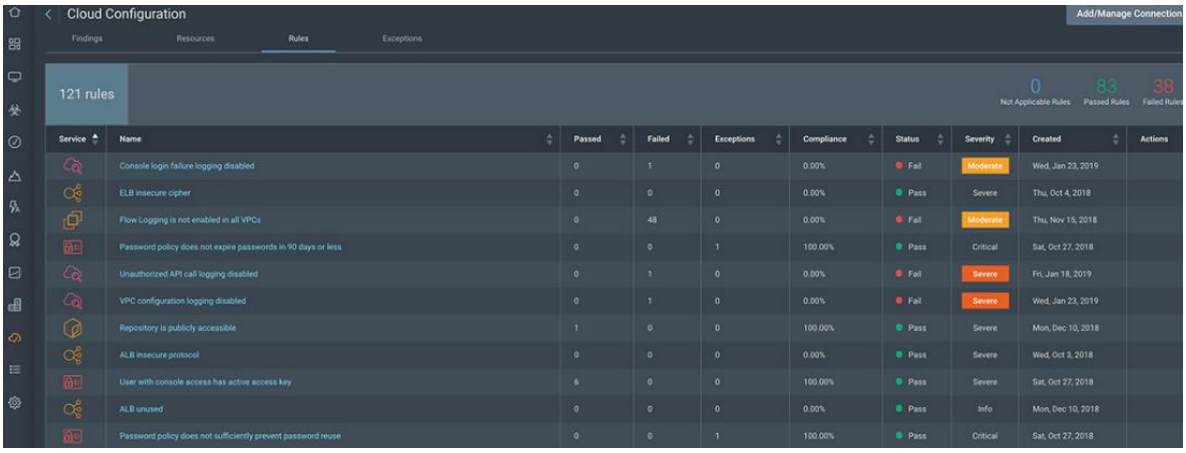


Figura 6. Evaluación de infraestructura virtual y en la nube
Tomado de (RAPID 7, s.f)

2.2.1.2. Empresas que han implementado el software

Existen varias empresas a nivel mundial que utilizan el sistema de control de vulnerabilidades InsightVM, las mismas que son detalladas en la tabla 6.

Tabla 6.

Listado de empresas de InsightVM

CLIENTES

Avnet, Inc.	Cognitive Scale	Energie Sudbayern
Evercore	Harley-Davidson, Inc.	Landmark Health
Liberty Wines	Manchester Metropolitan University	New Mexico Department of Game and Fish
Northern Bank and Trust	Pioneer Telephone Cooperative, Inc.	Rackspace
Rackspace	Revlon, Inc.	Security Finance
Sierra View Medical Center	Univision Comunications Inc.	The Washington Post

Tomado de (rapid7, s.f)

2.2.2. Nessus

Es un sistema que realiza la identificación y escaneo de vulnerabilidades en distintos sistemas operativos, descubriendo los problemas de configuración que emplean los hackers en la red, es el más usado a nivel mundial, consiguiendo el primer lugar en ranking mundial en los años 2000, 2003 y 2006 como el mejor sistema de seguridad de red. (Advisors, s.f)

2.2.2.1. Características

(Martin, 2015), entre las características principales podemos mencionar las siguientes:

- Permite entender que brecha de seguridad se encuentra abierta y que servicios se encuentran susceptibles a ataques de hackers.
- Su ejecución es mediante un proceso de alta velocidad que permite encontrar datos sensibles y realiza auditorias de configuraciones con el perfil activo.
- El servidor es el encargado de realizar todas las tareas de escaneo que sea especificado por el administrador.
- Reconoce las vulnerabilidades existentes e indica cómo interactúa la amenaza y como se debe proceder para proteger el equipo de la misma.

2.2.2.2. Ventajas de usar Nessus

Se describe cuáles son las ventajas según (Tenable, 2018)

- Fácil de usar: la implementación de políticas es sencilla y requiere pasos sencillos para proceder a escanear la red.
- Completo: Acepta todo tipo de tecnologías e identifica más vulnerabilidades que otros sistemas.
- Bajo costo: su sistema de escaneo es de bajo costo comparado a otros sistemas.
- Rápido y preciso: rapidez en el escaneo de vulnerabilidades con una tasa baja de falsos positivos.
- Protección oportuna: se indaga rápidamente sobre nuevas vulnerabilidades que se presenten
- Escalable: Migrar entre las versiones del sistema según la necesidad de vulnerabilidades.

2.2.2.3. Empresas que han implementado el software

Existen varias empresas a nivel mundial que utilizan el sistema Nessus, las mismas que son detalladas en la tabla 7.

Tabla 7.

Listado de empresas de Nessus

CLIENTES		
SIEMENS	Splunk	CYBERARK
Infoblox	Servicenow	Amazon web services
ForeScout	McAfee	Vmware
PayPal	Twiter	Dole
STARBUCKS COFFEE	DocuSign	Capgemini

Tomado de (*tenable*, 2019)

2.2.2.4. Costo del sistema

Para la adquisición de una licencia tiene los siguientes planes como nos indica la siguiente Tabla 8:

Tabla 8.

Listado de precios del sistema

AÑOS	SOPORTE AVANZADO	PRECIO	SLA
1	NO	$ 2.390,00	P1-Crítico: < 2 h P2-Alto: < 4 h
1	SI	$ 2.790,00	
2	NO	$ 4.660,00	

2	SI	$ 5.460,00	P3-Medio: < 12 h P4-Informativo: < 24 h
3	NO	$ 6.811,50	
3	SI	$ 8.011,50	

Tomado de (*tenable*, 2019)

2.3. Herramientas de software libre para el monitoreo de amenazas

2.3.1. Security Onion

(Github, 2019), Security Onion es una distribución Open Source que permite realizar la detección de intrusos y monitoreo de la red, cuenta con una variedad de herramientas que ayuda a controlar y monitorear la infraestructura.

Security Onion cuenta con una variedad de herramientas para auditar la seguridad a nivel de redes entre las más principales son:

- **Snort:** Es un sistema de prevención y detección de intrusos de red (IDS / IPS), como se pude apreciar en la Figura 7, las alertas de Snort.

IP	DPort	Pr	Event Message
10.6.11	1134	6	Snort Alert [1:1000001:0]
10.6.11	1135	6	Snort Alert [1:1000001:0]
10.6.11	1143	6	Snort Alert [1:1000001:0]
10.6.11	1144	6	Snort Alert [1:1000001:0]
10.6.11	1145	6	Snort Alert [1:1000001:0]
10.6.11	1153	6	Snort Alert [1:1000001:0]
10.6.11	1155	6	Snort Alert [1:1000001:0]
10.6.11	3306	6	ET POLICY Suspicious inbound to mySQL port 3306
.16.1.10		1	GPL SHELLCODE x86 inc ebx NOOP
10.6.11	36840	17	GPL SHELLCODE x86 inc ebx NOOP
10.6.11	36840	17	ET SCAN NMAP OS Detection Probe
10.6.11	1210	6	ET POLICY PE EXE or DLL Windows file download
10.6.11	1211	6	ET WEB_CLIENT MS10-090 IE CSS Exploit Metasplo...
10.6.11	1210	6	ET POLICY PE EXE or DLL Windows file download

Figura 7. Alertas Snort

Tomado de (Snort.org, 2019)

- **Suricata:** Es un motor de alto rendimiento para redes IDS, IPS y monitoreo de seguridad en la red como se puede observar en la figura 8 el rendimiento de la aplicación suricata.

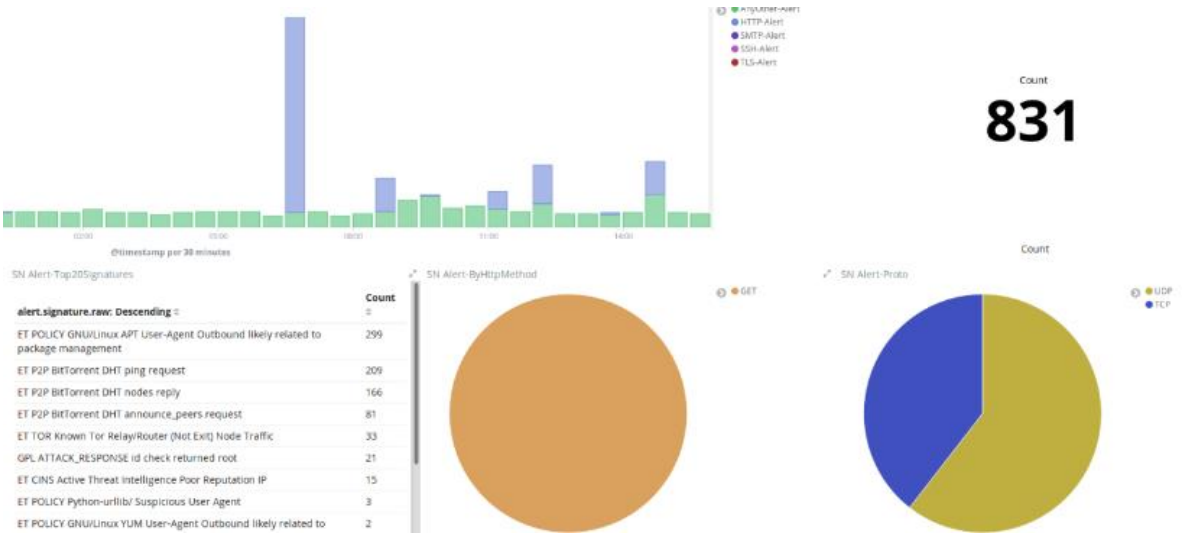


Figura 8. Rendimiento de Suricata

Tomado de (suricata-ids.org, s.f)

- **Squert:** Es una aplicación web que permite examinar y ver datos de eventos almacenados en una base de datos en la figura 9, se verifica la cola de alertas en la pestaña de eventos.

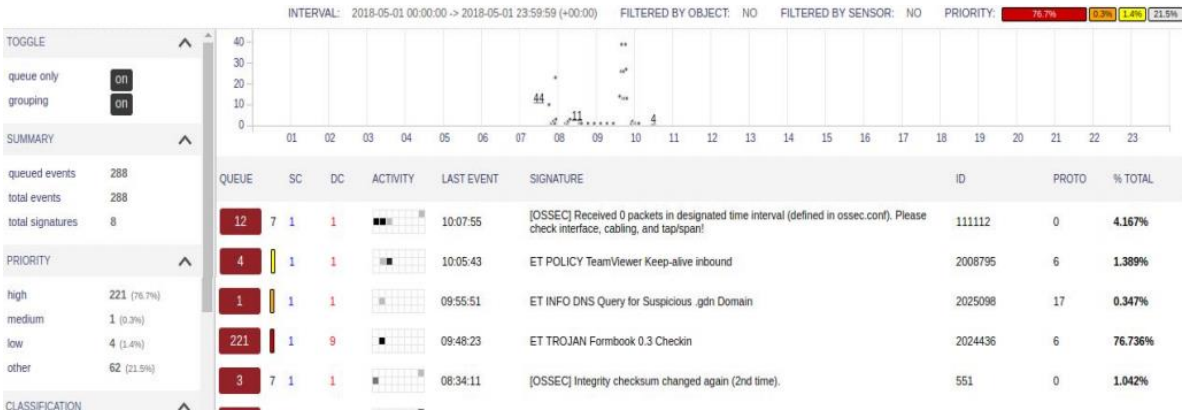


Figura 9. Cola de alertas en la pestaña de eventos
Tomado de (squertproject.org, s.f)

- **Sguil:** Proporciona el paso a eventos en tiempo real, datos de sesión y capturas de paquetes sin procesar también favorece a la práctica el Monitoreo de seguridad de red. y el análisis basado en eventos, como se aprecia en la figura 10, los paquetes que se envían de una ip especifica.

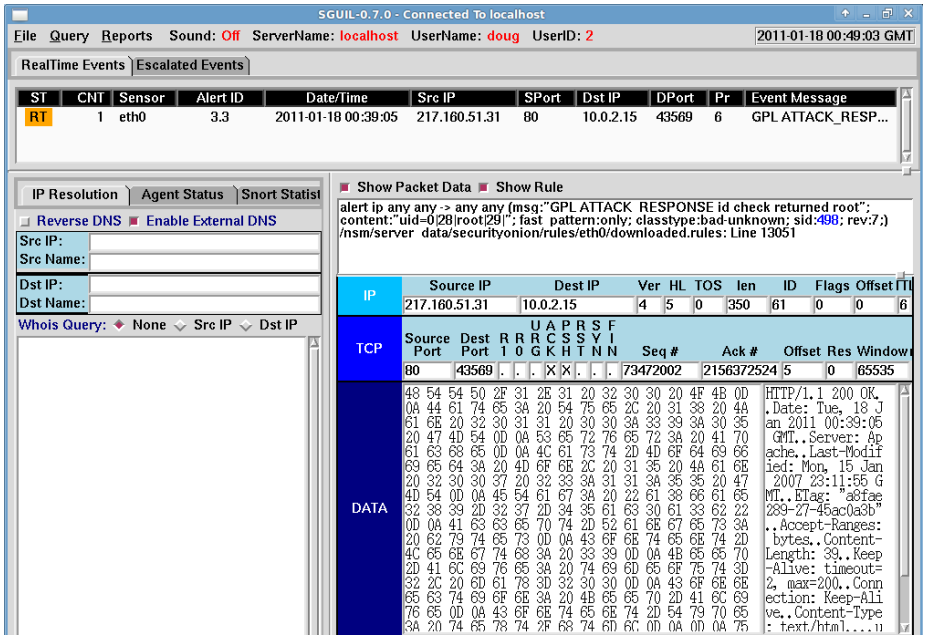


Figura 10. Verificación de paquetes de una IP

Tomado de (*Kustas*, 2017)

- **Wireshark:** Es un comprobador de protocolos de red GUI, su principal característica es explorar interactivamente datos de paquetes desde una red y es multiplataforma, en la figura 11 se puede verificar el tráfico de la red.

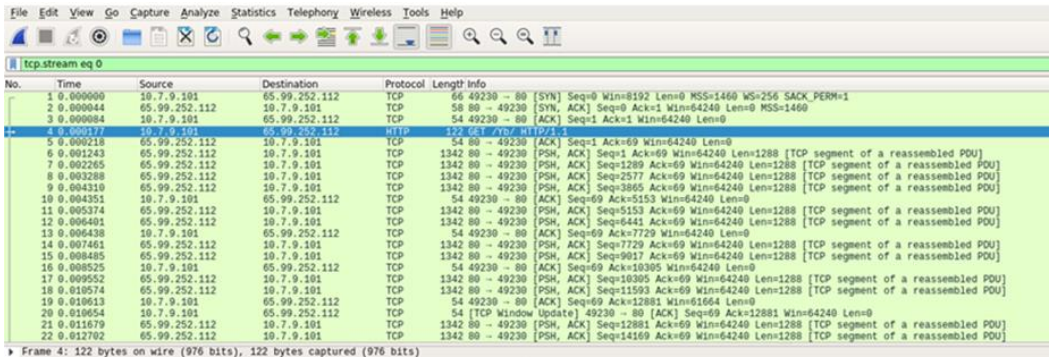


Figura 11. Tráfico de la red

Tomado de (*Onion*, 2019)

- **NetworkMiner:** Es un instrumento de análisis forense de red (NFAT) para Windows. Permite realizar capturas de paquetes y Sniffer dentro de la red para así detectar sistemas operativos, sesiones abiertas, nombres de host, puertos abiertos, etc. En la figura 12 nos indica el tráfico de la red.

Figura 12. Trafico de la red con NetworkMiner
Tomado de (*Onion*, 2019)

2.3.1.1. Funciones Principales

Entre las funciones principales se destacan las siguientes:

- Captura de tráfico: Para la obtención del tráfico de red se realiza a través de netsniff el cual captura el tráfico que aborda a los sensores de Security Onion y se puede almacenar todos los datos que se encuentran configurados y pueda soportar. Security onion tiene la capacidad de purgar datos antiguos antes que se llenen los discos a su máxima capacidad. (Onion, 2019)
- Sistema de detección de intrusos (HIDS/NIDS): Los procedimientos para la detección de intrusos

2.3.1.2. Requerimientos mínimos del sistema

Según (Security Onion Solutions, 2019), para tener un óptimo rendimiento es necesario considerar lo siguiente:

- **Memoria RAM:**
  - Para evaluar rápidamente Security Onion en una máquina virtual, la cantidad mínima de memoria RAM necesaria es de 8 GB o más.
  - Para implementar Security Onion en producción en redes pequeñas (50Mbps o menos) se sugiere 8 GB de RAM o más.
  - Para implementar Security Onion en producción en redes medianas (50Mbps - 500Mbps) se sugiere 16 GB a 128 GB de RAM o más
  - Para implementar Security Onion en producción en redes grandes (500Mbps - 1000Mbps) se sugiere 128 GB a 256 de RAM o más.

- **Tarjeta de red:** Se necesita al menos dos interfaces de red; una para la administración se recomienda ip estática y la otra para la detección.

2.3.1.3. Ventajas y Desventajas

En la Tabla 9 se puede apreciar las ventajas y desventajas que nos ofrece la herramienta Security Onion.

Tabla 9.

Ventajas y desventajas Security Onion

Ventajas	Desventajas
La interfaz es sencilla y muy amigable y fácil de usar	NO es posible elegir las herramientas que se vaya a ocupar, es necesario instalar toda la distribución

La instalación es simple es más automatizada	Alta demanda de recursos

Tomado de (Acosta & Muñoz, 2015)

2.3.2. OSSIM

Sus siglas Open Source Security Information Management (Herramienta de Código abierto para la gestión de Seguridad de la información), es una distribución Open Source que comenzó en el año 2003. OSSIM está empleado a ofrecer a los analistas y al personal de TI a tener una visión más clara de todos los aspectos relacionados con la seguridad de la información (Bravo, s.f).

2.3.2.1. Requerimientos mínimos del sistema

Según (Property, 2019) para realizar la instalación del sistema OSSIM, los requisitos mínimos del sistema son los siguientes:

- 2 núcleos de CPU
- 4-8 GB de RAM
- Disco duro de 250 GB
- Tarjetas de red compatibles con E1000

2.3.2.2. Tipos de Implementación

- **Implementación simple:** el hardware que contenga el sistema se lo implementara atrás del firewall como lo muestra la figura 13.

  Este componente inspecciona y recopila información de las siguientes redes:

  - Red de oficinas
  - Red inalámbrica
  - DMZ
  - Firewall

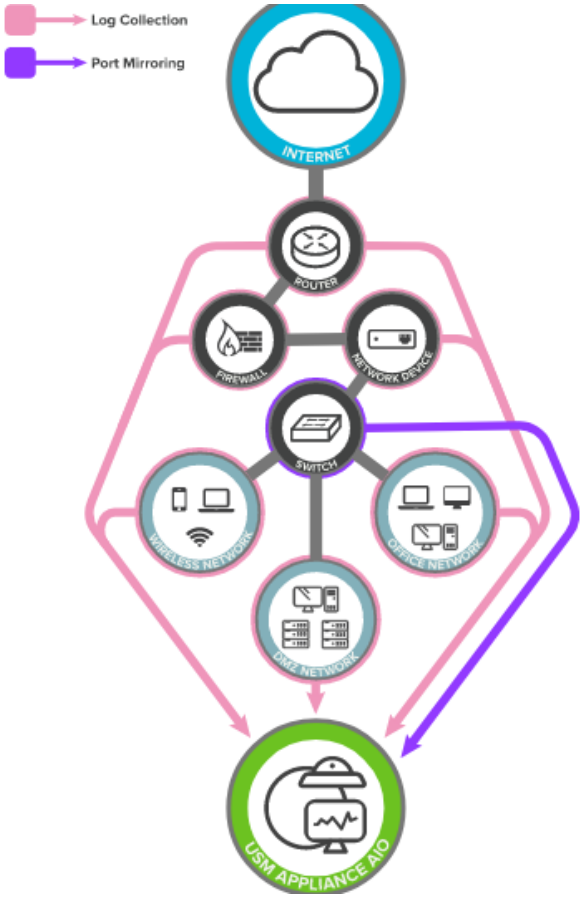


Figura 13. Dispositivo todo en uno
Tomado de (*AT&T Cybersecurity*, 2019)

El dispositivo todo en uno realiza la monitorización de todo el tráfico de la red a través de los conmutadores conectados (Cybersecurity AT&T, 2019)

- **Implementación Simple Extendida:** Esta implementación se diferencia del primero ya que incluye un sensor remoto que permite realizar el monitoreo de forma remota, recopilando datos y monitorea una subred específica para luego enviar al sistema de la red principal para el diagnóstico y evaluación de los riesgos encontrados como lo indica en la figura 14.

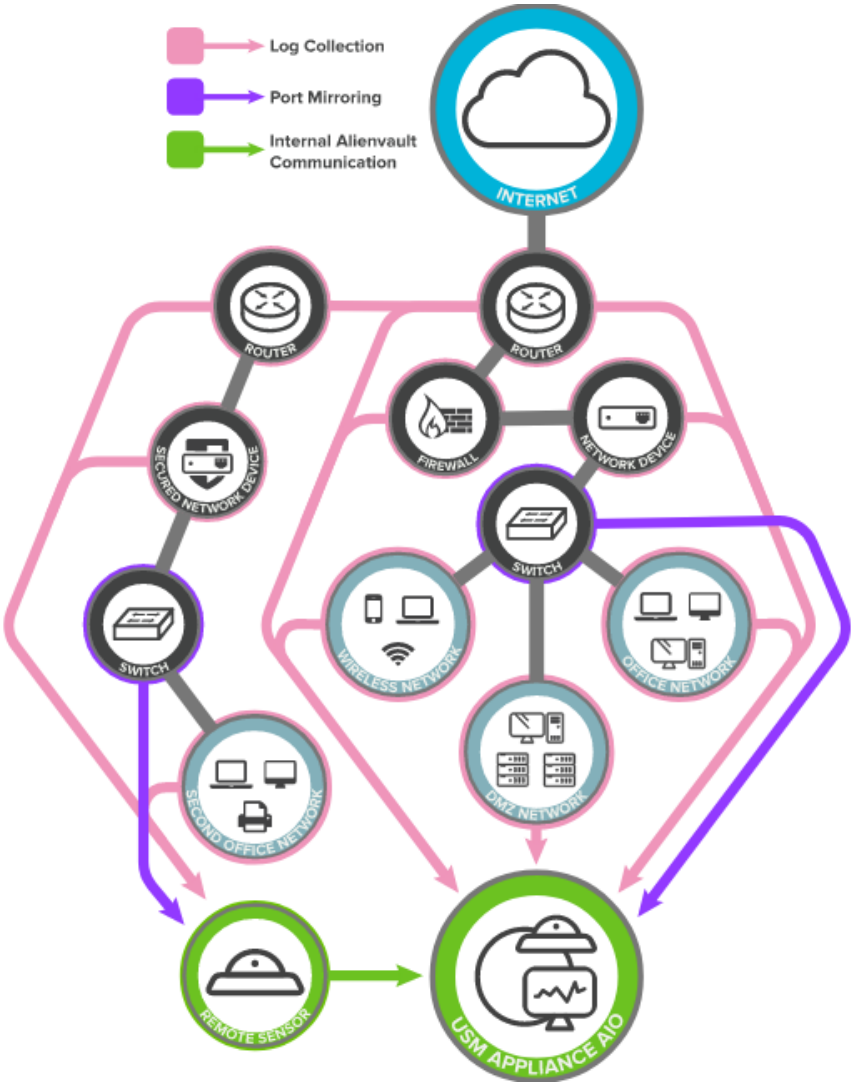


Figura 14. Dispositivo todo en uno y sensor remoto
Tomado de (*AT&T Cybersecurity*, 2019)

- **Despliegue Completo:** Cada oficina posee una subred donde se realiza la implementación con el sensor remoto para la recopilación de información y realizar su monitoreo respectivo. En la red core se debe realizar la instalación del servidor con el sistema, un registrado y un sensor en dispositivos individuales para facilitar la escalabilidad y el rendimiento como nos indica (Cybersecurity AT&T, 2019). En la figura 15 se muestra la implementación compleja con sus componentes individuales en sus dispositivos.

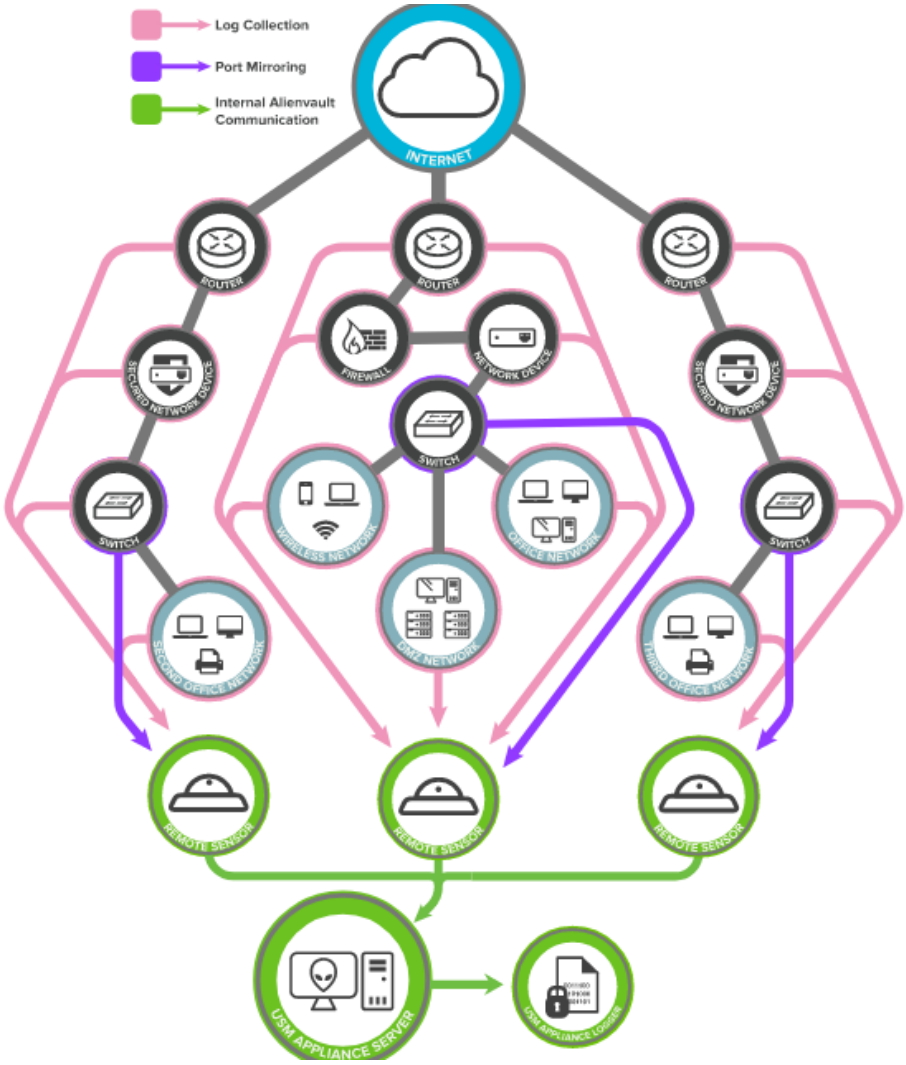


Figura 15. Diseño complejo con sus componentes
Tomado de (*AT&T Cybersecurity*, 2019)

2.3.2.3. Empresas que han implementado el software

Existen varias empresas a nivel mundial que utilizan el sistema Ossim, las mismas que son detalladas en la Tabla 10.

Tabla 10

Listado de empresas de Ossim

CLIENTES		
AVERTIUM	AGIO	DEKTA RISK
BINARY DEFENSE	Abacode Cybersecurity Experts	RoundTower
TriskeleLabs	REDSCAN	NORTHHWAVE
Loop SECURE	CNS 6	Sefisa

Tomado de (*Business, AT&T*, 2019)

2.4. Herramientas de software propietario para el monitoreo de amenazas

2.4.1. AlienVault

AlienVault es una plataforma de seguridad que se encuentra en la nube, nube hibrida y locales, que nos permite la detección de amenazas, una respuesta inmediata sobre incidentes que se presenten en la red. (Cibersecurity, 2019)

2.4.1.1. Características

(Accsys, s.f), AlienVault proporciona una visión completa de seguridad, facilitando las cinco capacidades esenciales de seguridad en una plataforma unificada y controlada.

En la figura 16 se representa las capacidades esenciales de la seguridad en AlienVault.

- **Descubrimiento de activos:** descubrimiento activo y pasivo de la red
- **Evaluación de vulnerabilidades:** Permite realizar escaneos activos de toda la red, monitorización de vulnerabilidades.
- **Detección de intrusiones:** IDS (Detección de intrusión en red) en red y host, monitorización de integridad de archivos
- **Monitoreo de comportamiento:** análisis del comportamiento de la red, monitorización de disponibilidad del servicio
- **SIEM:** gestión de registros, correlación de eventos, análisis e informes.

Figura 16. Capacidades esenciales de AlienVault
Tomado de (*accsys*, s.f)

2.4.1.2. Empresas que han implementado el software

Existen varias empresas a nivel mundial que utilizan el sistema AlienVault para el monitoreo de las redes e infraestructura en la nube, las mismas que son detalladas en la tabla 11.

Tabla 11

Listado de empresas de AlienVault

CLIENTES		
Foot Locker	Soulcycle	SHAKE SHACK
Dart NeuroScience	MOLLIE STONE'S	IRA SERVICES TRUST COMPANY
LUCKY SHOES	BOSTON MUTUAL LIFE INSURANCE COMPANY	CROSSKEY
KLEINER PERKINS CAUFIELD BYERS	Breckenridge INSURANCE GROUP	Carroll College
FOCUSBRANDS	TELENAV	TOWN SQUARE BANK
FRANKLIN DATA	LAVAN	PASC COUNTY FLORIDA
BOG FISH Games	FOSTER FARMS	

Tomado de (*Business*, 2019)

2.4.1.3. Requerimientos mínimos para instalar AlienVault

En la tabla 12, se especifica los requerimientos mínimos del hardware que se debe considerar para la instalación del sistema AlienVault.

Tabla 12

Requerimientos de hardware

Nombre	Valor

Tipo de CPU	Intel® Xeon E5620
Tipo de RAM	DDR3 1333 MHz
Tipo de disco	SAS 10000 RPM (204 MB / s)
Rendimiento de la memoria (MEMCPY)	3310.32 MiB / s
Rendimiento del disco (lectura / escritura aleatoria)	15.97 MB / s (120 Mb / s)

Tomado de (*Cybersecurity*, s.f)

En la tabla 13, se indica los requerimientos mínimos que se debe tener para instalar el sistema AlienVault en máquinas virtuales.

Tabla 13

Requerimientos mínimos para máquinas virtuales

Descripción	**Dispositivo USM**		**Sensor remoto**		**USM Appliance Standard**		
	1 TB	**500 GB**	**1 TB**	**250 GB**	**Servidor**	**Registrador**	**Sensor**
Núcleos totales	8		4 4		8		
RAM (GB)	16		8		24		
Almacenamiento (TB)	1	0.5 0.5	1	0.25	1,2	1,8	1,2
	VMware virtual hardware versión 10						

Entorno de virtualización	Hyper-V 3.0+ (Windows Server 2008 SP2 y posterior)

Tomado de (*Cybersecurity*, s.f)

AlienVault es compatible con los siguientes navegadores, como se describe en la tabla 14.

Tabla 14

Navegadores soportados para AlienVault

Navegador / Plataforma	Ventanas	Mac OS X	Linux
Cromo	si	Si	si
Borde	si	N / A	N / A
Firefox	si	Si	si
Internet Explorer 11	si	N / A	N / A
Safari	N / A	Si	N / A

Tomado de (*Cybersecurity*, s.f)

2.4.2. SolarWinds

Es un software open source de monitoreo de red potente que posibilita la detección, diagnosticar y resolver rápidamente los problemas de rendimiento de la red y las interrupciones que se presenten. (SOLARWINDS , 2017)

2.4.2.1. Características

Entre las características más importantes tenemos las siguientes:

- **Monitoreo de disponibilidad de red**

  Permite realizar una evaluación de la red que está monitoreando constantemente y evalúa el rendimiento y disponibilidad de los equipos que se encuentran en la red (SolarWinds Worldwide, LLC, 2020).

  Con estas alertas inteligentes esta herramienta permite conocer las métricas de rendimiento se encuentran en sus umbrales predefinidos e informar primero al personal encargado cuando ocurren estos problemas como se visualiza en la figura 17.

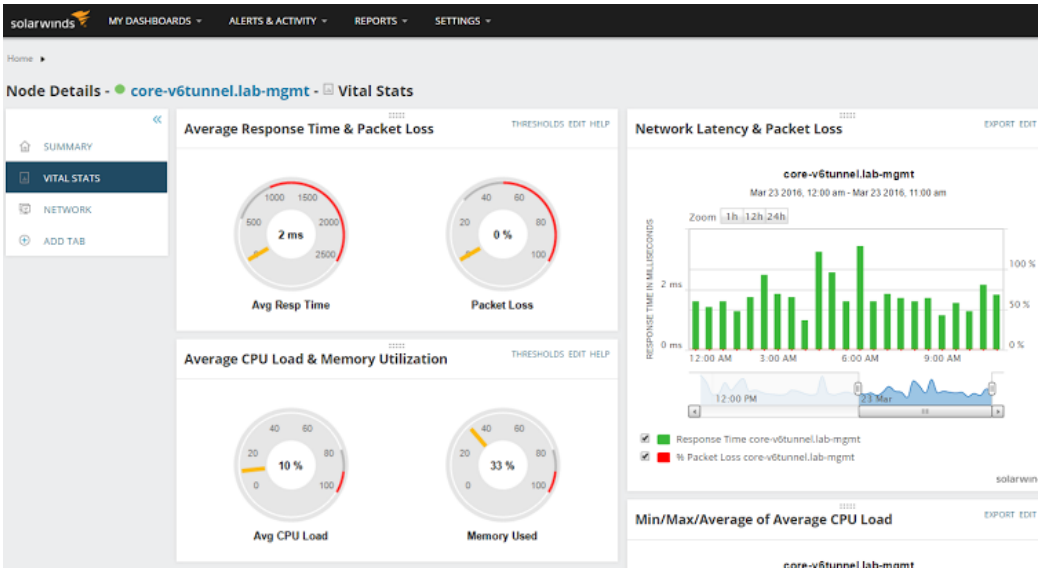


Figura 17. Monitoreo de red

Tomado de (*SolarWinds Worldwide, LLC*, 2020)

- **Análisis de ruta de red de NetPath**

  Según (SolarWinds Worldwide, LLC., 2020), esta herramienta permite visualizar el trazado de las rutas críticas para obtener información contundente y efectuar las correcciones de una forma más rápida. También se tiene el control de los

dispositivos, aplicaciones y redes permite realizar el rastreo de cada salto y latencia que se presenta en los mismos como se visualiza en la figura 18

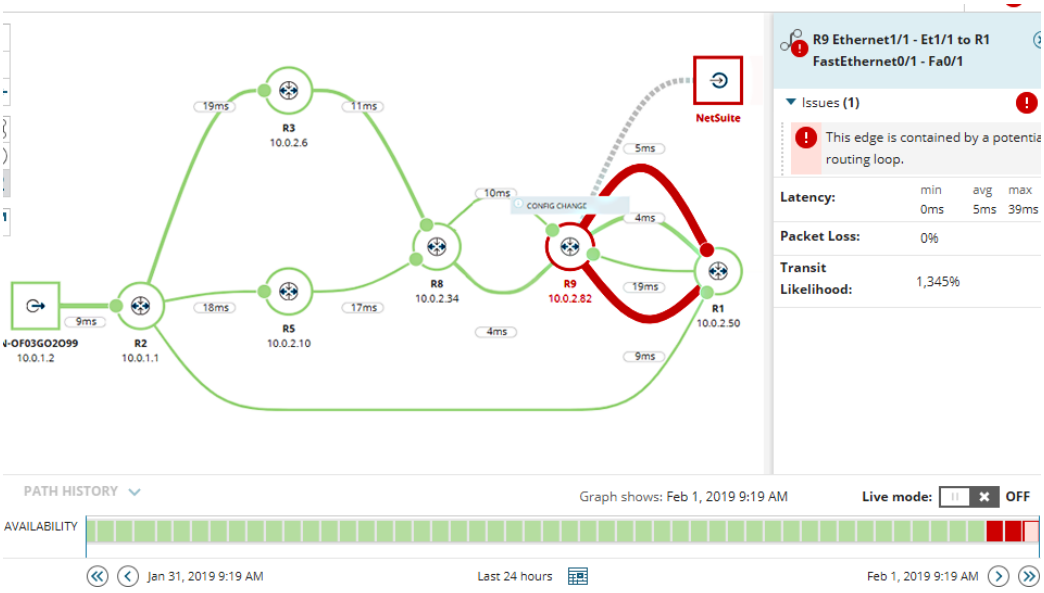


Figura 18. Análisis de ruta.

Tomado de (*SolarWinds Worldwide, LLC*, 2020)

- **Herramienta de mapeo de red**

  Proporciona ver los enlaces físicos y lógicos que se actualizan automáticamente entre dispositivos que se localizan en la red como enrutadores, conmutadores y servidores como se indica en la figura 19 (SolarWinds Worldwide, LLC, 2020).

Figura 19. Herramienta de mapeo de red

Tomado de (*SolarWinds Worldwide, LLC*, 2020)

- **Construye mapas de calor inalámbricos**

  Se observa que la cobertura inalámbrica facilita la ubicación de las zonas muertas que se encuentran y así poder realizar ajustes y mejorar la cobertura inalámbrica. Para la construcción de este mapa se toma la información de los puntos inalámbricos, usuario y clientes conectados y sus intensidades de la señal como se muestra en la figura 20.

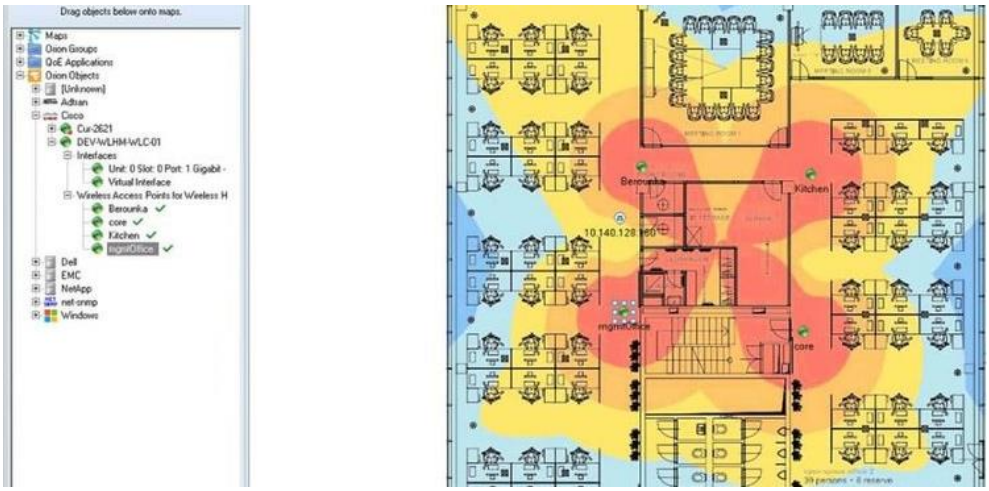


Figura 20. Mapas de calor inalámbricos

Tomado de (*SolarWinds Worldwide, LLC*, 2020)

- **Alertas de monitoreo de red**

  Según (SolarWinds Worldwide, LLC, 2020), se proporciona observar de una manera más rápida la información y así tomar medidas lo más pronto posible, por medio de la creación de las alertas permite verificar el estado de la red como se muestra en la figura 21.

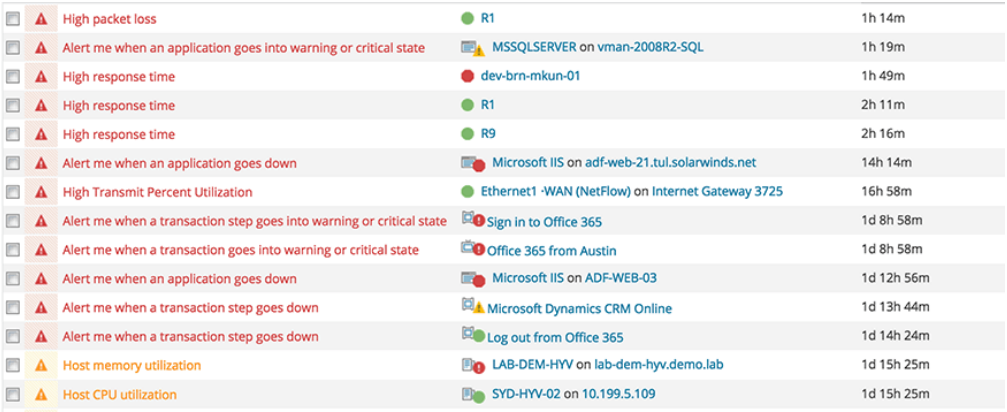


Figura 21. Alertas de monitoreo

Tomado de (*SolarWinds Worldwide, LLC*, 2020)

2.4.2.2. Requerimientos del sistema

Según (SOLARWINDS , 2017), para tener un óptimo rendimiento es necesario considerar lo siguiente como se describe en la tabla 15:

Tabla 15

Requisitos del sistema máquina virtual

Hardware	**Requerimientos Mínimos**
CPU	Procesador Dual, 3.0 GHz
Memoria	3 GB

Disco Duro	20 GB de espacio libre (recomendado)
Software	Requerimientos Mínimos
Sistema Operativo	Windows Server 2008 R2 SP1 Windows Server 2012 Windows Server 2012 R2
Base de Datos	SolarWinds admite las versions Express, Standar o Enterprie -SQL Server 2008 R2, 2008 R2 SP1, 2008 R2 SP3 -SQL Server 2012, 2012 SP1, 2012 SP2, 2012 SP3 -SQL Server 2014, 2014 SP1 -SQL Server 2016
NET Framework	Versión 4.5 (recomendado)

Tomado de (*SOLARWINDS* , 2017)

2.4.2.3. Costo del sistema

El sistema de monitoreo solarwinds se lo puede adquirir por la suma de **$2995,00**, este precio se encuentra oficial en su página web oficial (SolarWinds Worldwide, LLC, 2020)

2.5. Determinación de la herramienta a utilizar

En base a la investigación realizada para este proyecto de los diferentes sistemas de monitoreo tanto propietarios y open source se recalca sus principales funcionalidades, características, ventajas y desventajas; como se visualiza en la tabla 16 las comparaciones de sus funcionalidades para una toma de decisión.

Tabla 16

Comparación de los sistemas Open Source para monitoreo

FABRICANTE /FUNCIONALIDAD	**OSSIM**	**ALIENVAULT**	**SECURITY ONION**
Tipo de Licencia	GPL	Comercial - GPL	GPL
Interfaz Web	SI	SI	SI
Almacenamiento de Logs	SI	SI	SI
Correlación de Logs	SI	SI	SI
Gestión de Incidentes	SI	SI	SI
Módulo de Reportería	SI ILIMITADO	SI	SI
Sistema IDS incluido	SI Snort	SI Snort	SI Snort/Suricata
Arquitectura modular y escalable	NO	SI	SI
Sistema de administración multiusuario	NO	SI	SI

Analizador de Vulnerabilidades	SI OpenVAS	SI OpenVAS	SI
Monitor de tráfico de Red	SI Ntop	SI Ntop	SI Sguil, Squert
Host IDS	SI Osiris	SI Osiris	SI Ossec
Sistema Antivirus incorporado	ClamAV	ClamAV	NO

Tomado de (Pazmiño, J; Pazmiño, C, 2018)

Basándonos en la figura 22 que representa el cuadrante mágico de Gartner 2018 para SIEM (LogRhythm, 2019), se puede apreciar las empresas que por hoy se encuentran liderando el mercado para la seguridad de la información y gestión de eventos.

Figura 22. Cuadrante Mágico para información de seguridad y gestión de eventos.

Tomado de (*LogRhythm*, 2019).

Después de realizar un análisis minucioso en base a la tabla 16 descrita anteriormente y verificar que empresas se encuentran líderes en el mercado tomando como referencia el cuadrante mágico de gartner como se muestra en la figura 22, adicional a las conversaciones mantenidas con los gerentes y el departamento de sistemas de la Empresa Bagant Ecuatoriana Cía. Ltda.; se determina que por los beneficios y la necesidad de la empresa se procederá a utilizar la herramienta SECURITY ONION para el sistema de monitoreo.

3. CAPÍTULO III: ANÁLISIS DE VULNERABILIDADES Y BRECHAS DE SEGURIDAD

Las vulnerabilidades dentro de una red se pueden presentar por varios factores los cuales se encuentran descritos en este capítulo. Además, se definen los procedimientos a seguir para detectar y realizar el tratamiento respectivo a una posible amenaza tomando en cuenta la norma técnica ISO27005.

3.1. Causas de las vulnerabilidades

3.1.1. Diseño de los protocolos utilizados en las redes

Existen empresas que utilizan protocolos para ofrecer ciertos servicios en redes como internet sin prever cómo reaccionar frente una situación anómala; entre los errores más conocidos que se dan en el diseño es el intercambio de información sensible sin cifrar a través de telnet, FTP o SMTP. (Gómez, 2013, pág. 16)

3.1.2. Programación

En varias ocasiones los parches y actualizaciones de seguridad no arreglan del todo los problemas dentro de los sistemas TPe incluso pueden generarse nuevas vulnerabilidades, otra causa frecuente se debe al buffer overflow que es cuando un programa intenta escribir en la memoria de un ordenador por encima de los límites, esto posibilita generar un código arbitrario con los privilegios del usuario actual. (Gómez, 2013, pág. 17)

3.1.3. Políticas de seguridad deficientes

Entre las distintas situaciones se tiene política de contraseñas poco robustas, deficiente control de intentos de acceso al sistema, escaso rigor en el control de acceso a los recursos, escaso control de las copias generadas en papel con información sensible, etc. (Gómez, 2013, pág. 19)

3.2. Proceso de gestión de riesgos de seguridad

La figura 23 muestra el proceso de gestión de riesgos definido por la norma ISO 27005.

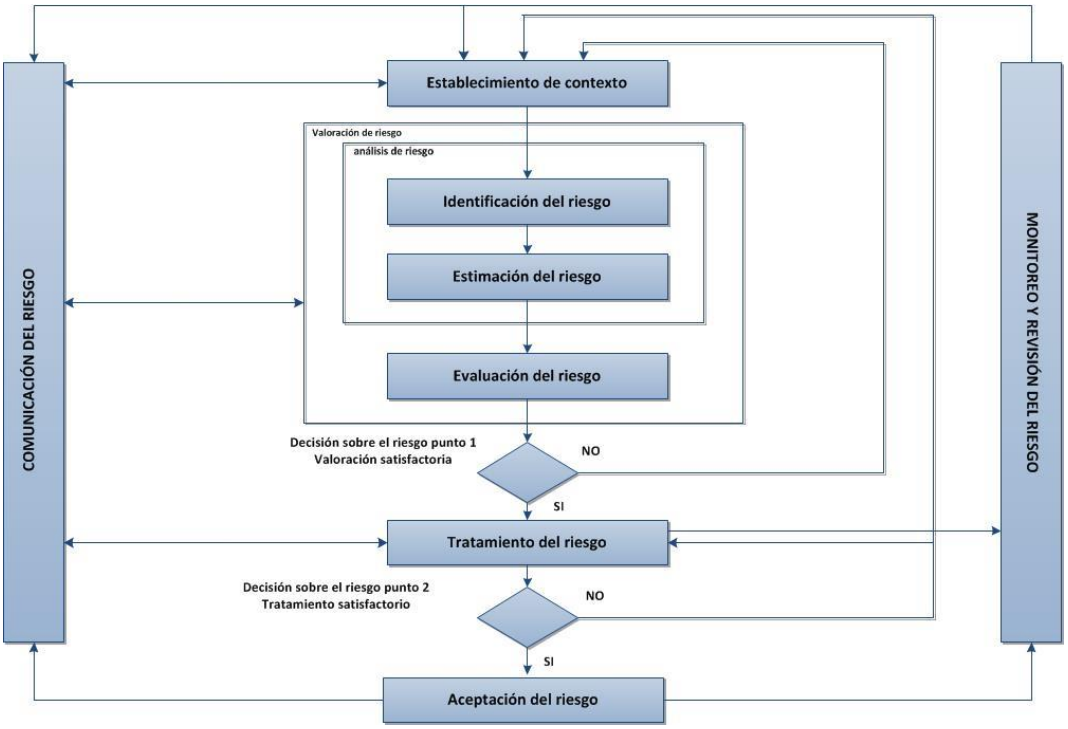


Figura 23. Proceso de gestión del riesgo de la seguridad de la información

Tomado de (INEN, 2012)

De acuerdo esta figura se puede evidenciar que el proceso de gestión de riesgo de seguridad puede ser de manera repetitiva para la valoración y el tratamiento de riesgo, el contexto es establecido primero para luego realizar la valoración de riesgo para verificar si esta suministra la información suficiente para determinar las acciones que se deben tomar para minimizar el riesgo y continuar con el tratamiento del riesgo; si esta información no es suficiente se llevará a cabo otra valoración de riesgo. (INEN, 2012, págs. 5-6)

3.2.1. Establecimiento del contexto

Aquí consta de ciertas consideraciones generales:

- Entrada: Información de la organización pertinente para establecer el contexto.
- Acción: Implica establecer criterios básicos que son necesarios, definir el alcance y los límites y establecer una organización adecuada que opere la gestión de riesgos.
- Guía para la implementación: Determinar el propósito de la gestión del riesgo ya que esto afecta el establecimiento del contexto. Esto puede ser; dar soporte al sistema de gestión de seguridad de la información, preparación de un plan para la continuidad del negocio, plan de respuesta a incidentes, etc.

3.2.1.1. Criterios de evaluación de riesgo

Se sugiere fomentar criterios para fomentar el riesgo con el fin de establecer el riesgo de la seguridad de la información, tomando en cuenta los siguientes puntos como lo indica (INEN, 2012, págs. 7-8):

- Valor estratégico del desarrollo de la información
- Requerimientos legales y reglamentarios, así como sus obligaciones.
- Considerar la disponibilidad, confidencialidad e integridad del flujo de negocio.

3.2.1.2. Criterios de la aceptación del riesgo

Es admisible desarrollar y precisar criterios de aceptación del riesgo considerando políticas, metas, objetivos de la organización por las partes involucradas.

Se debe considerar los siguientes aspectos:

- Los criterios de aceptación se pueden incluir a diferentes clases de riesgos.

- Para los criterios de aceptación se influenciar requisitos de tratamiento adicional en el futuro.

Los criterios de aceptación del riesgo se pueden distinguir de las expectativas de duración que posea del riesgo. (INEN, 2012, pág. 8)

3.2.2. Valoración del riesgo

Aquí se describe ciertas consideraciones generales de acuerdo a (INEN, 2012, pág. 10):

- Entrada: Conceptos básicos, alcance, límites, y la estructura establecida para el proceso de gestión de riesgo en la seguridad de la información.
- Acción: Todo tipo de riesgo debe ser identificado, especificar sus atributos y priorizar frente a os criterios de evaluación de riesgo sus objetivos más relevantes.
- Guía para la implementación: El riesgo es una mezcla de las consecuencias que se presentaron después de la ocurrencia de un acontecimiento indeseado y de su probabilidad de ocurrencia, permitiendo así que el personal capacitado tome cartas en el asunto sobre la gravedad de estos.
- Salida: Poseer una lista de riesgos con su respectiva prioridad con criterios de evaluación de riesgos.

3.2.3. Análisis del riesgo

3.2.3.1. Introducción a la identificación del riesgo

La finalidad de la identificación del riesgo es de establecer lo que puede suceder con una perdida potencial, y poder determinar el cómo, dónde y porque podría ocurrir.

Se debe recolectar los datos sobre los movimientos de estas actividades de la estimación del riesgo los mismos que son detallados en (INEN, 2012, págs. 11-14):

- Identificación de los activos: Se debe tener en consideración el nivel de identificación adecuado que proporcione la suficiente información de la valorización del riesgo. El nivel a utilizar en la identificación influenciara en la cantidad total de información obtenida durante la valoración del riesgo.
- Identificación de las amenazas: Las amenazas tienen las capacidades de ocasionar daños en los activos tales como la información, procedimientos, etc. Las mismas pueden ser ocasiónales o provocadas, se recomienda conocer estas vulnerabilidades desde su origen hasta que es lo que pueden provocar hacer.
- Identificación de los controles existentes: Los controles se programan para que sean proyectados de acuerdo a los planes de implementación del tratamiento del riesgo. Los controles que ya se encuentren implementados podemos conocer si son ineficaces, insuficientes. Si se llegara a determinar si el control no cumple con los requerimientos establecidos se procederá a eliminar, reemplazar por otro más adecuado.
- Identificación de las vulnerabilidades: Las vulnerabilidades no originan daño por si solas, dado que necesitan una amenaza, si la vulnerabilidad no tiene amenaza no es necesario implementar un control, pero se recomienda conocerla y monitorear para determinar qué cambios puede producir. Un control para que sea eficiente o ineficaz depende donde se implementar.
- Identificación de las consecuencias: Trata de determinar qué consecuencias y daños pueden producir a la organización, tomando en consideración los criterios de impacto ya que una consecuencia puede causar eficiencia de los procesos, perdida de negocio, reputación, daño, etc.

3.2.4. Estimación del riesgo

3.2.4.1. Metodologías para la estimación del riesgo

Para una metodología de estimación del riesgo se puede realizar de dos maneras las cuales son de acuerdo a (INEN, 2012, pág. 14)

- Estimación Cualitativa: Emplea una escala de atributos calificativos para conocer las dimensiones de las consecuencias que se dan y saber que probabilidad puedan darse nuevamente por lo cual se puede dar en:
  - Una actividad de evaluación inicial.
  - Toma de decisiones.
  - Cuando los datos no son suficientes para una estimación cuantitativa.
- Estimación cuantitativa: Emplea una escala de valores para las consecuencias o las probabilidades ya que utiliza varias fuentes para su análisis. Para la expresión de las consecuencias y de las probabilidades son consideradas en el análisis transmitirse de una forma clara.

3.2.4.2. Valoración de las consecuencias

Aquí se describe ciertas consideraciones de acuerdo con (INEN, 2012, págs. 15-16):

- Entrada: Registro de escenarios de los incidentes presentados, se define la identificación de las vulnerabilidades y amenazas consecuencias y procesos del negocio
- Acción: Se determina el impacto para el negocio de la organización el cual puede tener incidentes potenciales o reales en la seguridad e integridad de la información.
- Guías para la implementación: Comienza con la implementación de cualquier tipo de metodología de estimación del riesgo para conocer así la importancia de los activos que tiene la organización y cumplir con los objetivos establecidos.

3.2.4.3. Valoración de los incidentes

Se considera todos los incidentes presentados que sean identificados como amenazas y todo tipo de vulnerabilidad que sea explotada y afecten al negocio, evaluando todos los escenarios posibles, una vez identificado se debe utilizar técnicas de cualificación o cuantificación para tener consideraciones de la frecuencia que ocurren las amenazas. (INEN, 2012, págs. 16-17)

3.2.5. Evaluación del riesgo

Según (INEN, 2012, págs. 17-18), los criterios de evaluación de riesgos son dispensables para la toma de decisiones en la organización. Las decisiones se toman en cuenta con un nivel de aceptabilidad del riesgo y cuáles pueden ser sus consecuencias.

Las consideraciones deben incluir:

- Propiedades de la seguridad de la información
- La importancia de los procesos del negocio

3.2.6. Tratamiento del riesgo

La figura 24 muestra el proceso de tratamiento del riesgo de la seguridad de la información.

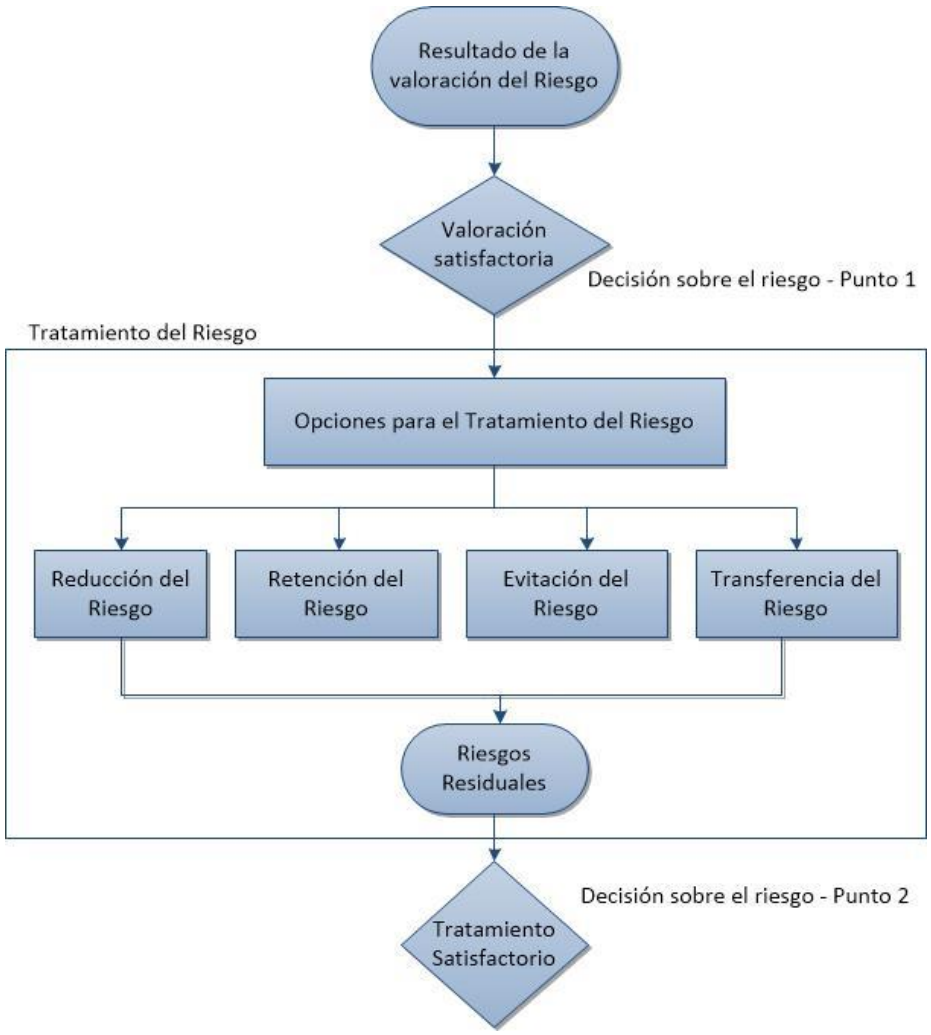


Figura 24. Actividad para el tratamiento del riesgo

Tomado de (INEN, 2012)

De acuerdo a la figura 24, podemos evidenciar el tratamiento del riesgo el cual tiene diferentes fases (INEN, 2012, págs. 20-22):

- Reducción del riesgo: Se debe proceder a la reducción mediante los diferentes controles de manera residual para que los riesgos se puedan reevaluar.
- Retención del riesgo: Es efectuado dependiendo de la evaluación del riesgo y verificar cuáles son sus definiciones y consecuencias.

- Evitación del riesgo: Los riesgos que potencialmente sean peligrosos o los costos de implementación sean demasiados altos se puede tomar la decisión del retiro de la actividad de donde se está realizando y tomar otras consideraciones.
- Transferencia del riesgo: Para realizar la transferencia se debe tener las seguridades de soporte a las consecuencias y su función es monitorear el sistema de información y ejecutar acciones inmediatas antes de que se produzca un daño indefinido.

3.2.7. Aceptación del riesgo

Aquí se describe ciertas consideraciones de acuerdo a (INEN, 2012, pág. 22)

- Entrada: Se debe tener un plan de tratamiento del riesgo y valoración del riesgo.
- Acción: Se debe aceptar los riesgos y con sus responsabilidades que lo con llevan y registrarla de forma normal.
- Guía para la implementación: Los riegos deben tener un plan de tratamiento describiendo en que forma están valorados, con el propósito de satisfacer los criterios de aceptación de riesgo. Es fundamental que los directivos o personas responsables verifiquen y garanticen los planes propuestos para realizar el tratamiento del riesgo.

3.2.8. Comunicación del riesgo

La (INEN, 2012, pág. 23) nos indica que se recopila la información obtenida sobre el riesgo adquirido a través de las actividades de gestión del riesgo, la misma que se debe intercambiar entre las personas involucradas para la toma de decisiones.

Se debe realizar las siguientes actividades con el fin de lograr lo siguiente a la comunicación del riesgo:

- Facilitar la seguridad de la solución de la gestión del riesgo
- Agrupar toda la información del riesgo
- Ofrecer soporte para la toma de decisiones
- Adquirir nuevos conocimientos de seguridad de la información
- Otorgar un sentido de responsabilidad a las personas involucradas en la toma de decisiones.

3.2.9. Monitoreo y revisión del riesgo

Aquí se describe ciertas consideraciones de acuerdo a (INEN, 2012, pág. 24)

- Entrada: La información de los riesgos es obtenida por los procesos de la gestión del riesgo.
- Acción: Las amenazas, los riesgos deben ser monitoreados con la finalidad de identificarlos para tener una visión completa de las perspectivas y como estar listos si se produjera un ataque.
- Guía para la implementación: Todo riesgo, vulnerabilidad o amenaza tiene la adversidad de cambiar sin ninguna notificación, por lo que es importante realizar un monitoreo perseverante para identificar estos cambios.
- Salida: La gestión de riesgo debe alinearse con los objetivos de la organización y tener criterios de aceptación del riesgo.

Las entidades deben garantizar el monitoreo constante de los siguientes aspectos:

- Activos recién adquiridos estén contemplados en la gestión del riesgo.
- Evaluar nuevas amenazas que se puedan presentar dentro y fuera de la organización.
- Vulnerabilidades nuevas o existentes puedan ser explotadas por nuevas amenazas.

4. CAPÍTULO IV: IMPLEMENTACIÓN DEL CENTRO DE MONITOREO

Después de haber realizado un análisis profundo acerca de la importancia de tener un plan de contingencia en caso de presentarse una amenaza o vulnerabilidad que pueda afectar tanto a nivel económico o de integridad de la información de la empresa, se procede a la implementación del centro de monitoreo en la red de negocios.

4.1. Topología de la red

Se trabaja en conjunto con el personal de sistemas de la empresa Bagant Ecuatoriana, con el fin de realizar el levantamiento de la red física y lógica que al momento se encuentra desempeñando en la compañía, como se puede apreciar en la figura 25.

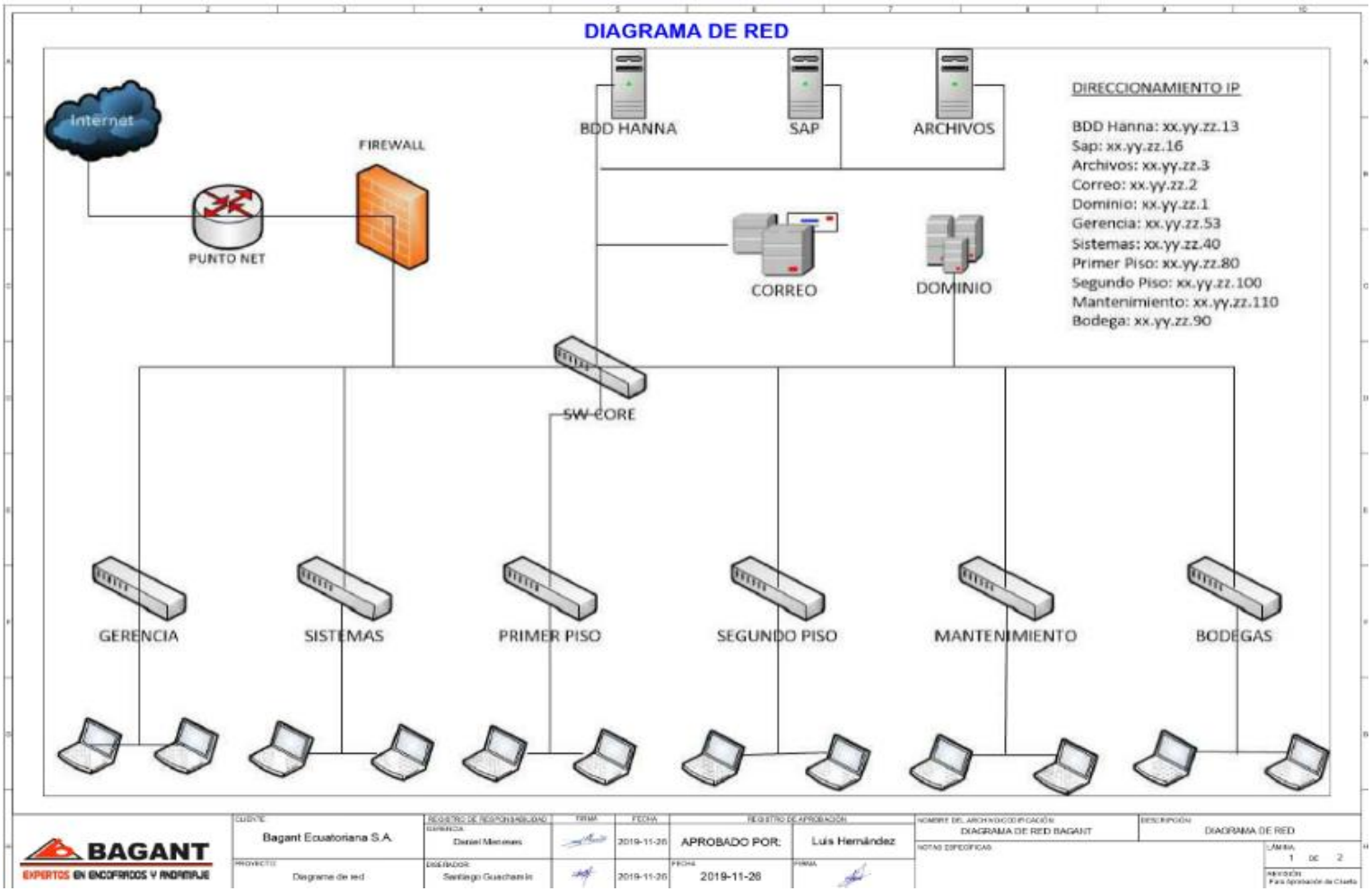


Figura 25. Diagrama de red Bagant Ecuatoriana

4.2. Diagrama de Implementación

Como se valida en el capítulo 2, la herramienta a implementar es Security Onion por todas las funcionalidades antes expuestas. En la figura 26 se describe el diseño de la red con la herramienta mencionada; ésta se conecta entre el firewall y el switch de core seguido de la red LAN de la empresa Bagant Ecuatoriana.

Además, en el firewall se encuentran concentradas todas las reglas y políticas definidas por el administrador de sistemas de la empresa para el control de tráfico de red que proviene desde la nube hacia la LAN y viceversa. Este sistema permite o deniega el flujo de datos en base al análisis que realiza el mismo de manera automática.

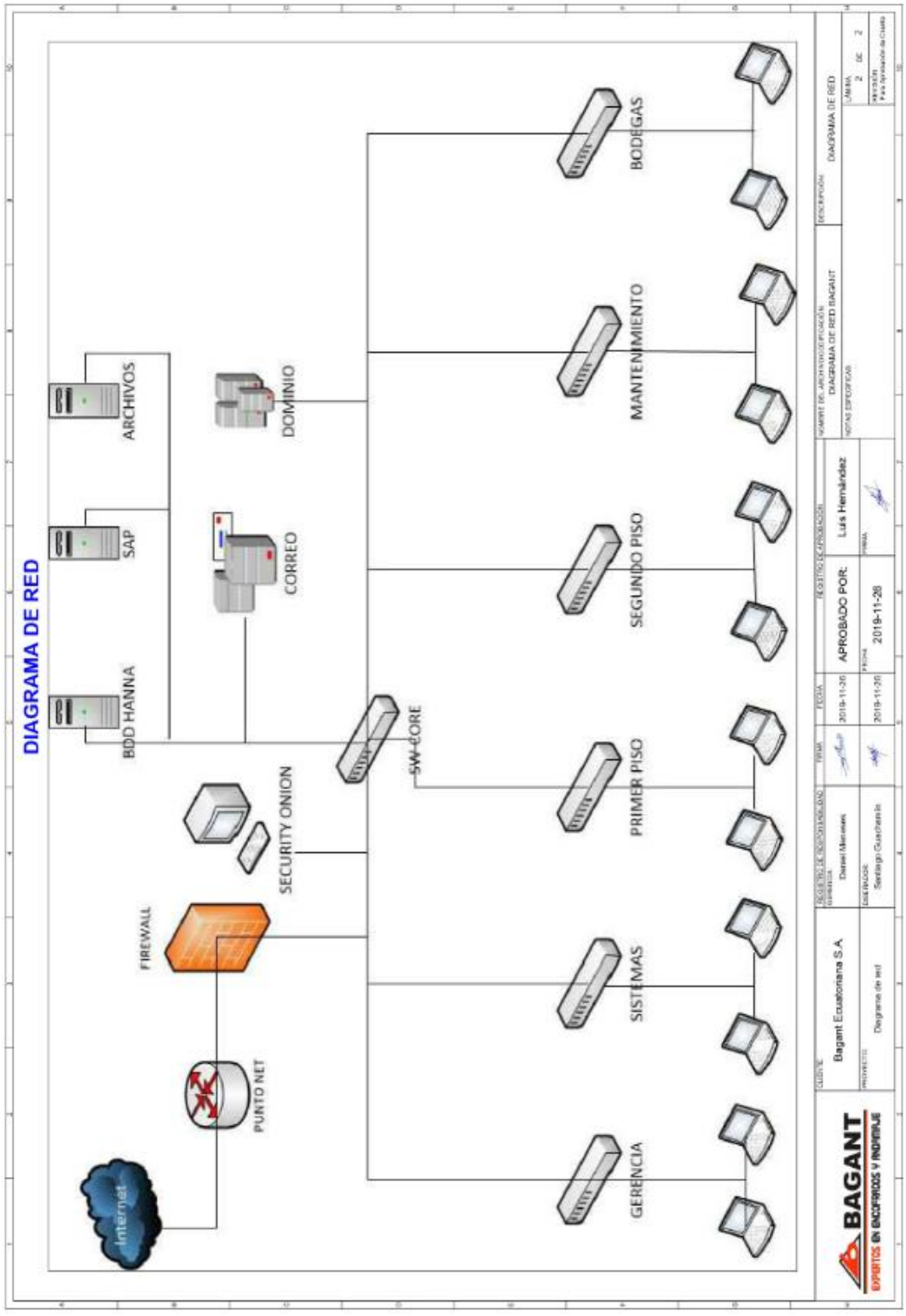


Figura 26. Diseño de red con Security Onion

En la tabla 17 se realiza la descripción de hardware que conforma la topología de red de la empresa Bagant Ecuatoriana. Cabe recalcar que, por temas de derechos de propiedad y seguridad de información de la empresa, en la columna de IP se describe el primer octeto con (xx), el segundo octeto con (yy) y el tercero con (zz).

Tabla 17.

Descripción de hardware de la empresa Bagant Ecuatoriana

Descripción	Conexión de Red	Características	IP
Servidor Security Onion	Red Interna Servidores	Sony Vaio Windows 10 Pro 2 interfaces virtuales	xx.yy.zz.47/24
Swicth de Core	Red Interna Servidores	D-Link DES-1210-28 12.8 Gbps Posee 24 puertos 10/100 BASE-TX	xx.yy.zz.1/24
Servidor Sap	Red Interna Servidores	HP ProLiant DL360 G9 Windows Server 2012 R2	xx.yy.zz.16/24
Servidor Hanna	Red Interna Servidores	Suse Linux Enterprise 11	xx.yy.zz.13/24
Servidor Archivos	Red Interna Servidores	HP ProLiant ML110 G6 Windows Server Enterprise	xx.yy.zz.3/24

Servidor de Dominio	Red Interna Servidores	HP ProLiant ML350 G9 Windows Server 2012 R2	xx.yy.zz.1/24
Servidor de Correo	Red Interna Servidores	Linux Centos 6.6	xx.yy.zz.2/24

4.3. Implementación

Para la implementación del sistema Security Onion, se procederá a utilizar la versión 16.04.6.2, la misma que se encuentra disponible en el siguiente link: https://github.com/Security-Onion-Solutions/security-onion/releases/download/v16.04.6.2_20190826/securityonion-16.04.6.2.iso

Para la ejecución se utiliza dos interfaces virtuales, las mismas que serán configuradas según la tabla 18, por motivos de seguridad y confidencialidad de la información no se podrá especificar la dirección IP.

Tabla 18

Direccionamiento IP de las interfaces

Interfaz	Descripción	IP
Eth0	Interfaz de administración, IP estática	xx.yy.zz.48
Eth1	Configuración SPAN, con el propósito de clonar la interfaz de la WAN y obtener la mayor cantidad de tráfico de la red	Sin IP

Para un mejor detalle sobre la instalación de Security Onion se puede guiar desde el siguiente link https://www.youtube.com/watch?v=jRoQUVY-2Ic, la misma que especifica que aspectos no mas se debe tener en cuenta al momento de la instalación.

4.3.1. Sistema Operativo

Se realiza el boot desde la unidad que contenga la imagen ISO de Security Onion, se presentara un cuadro de instalación como se muestra en la figura 27, simplemente damos enter y continuamos con la instalación.

Figura 27. Pantalla de Arranque

En la figura 28, nos presenta los diferentes idiomas para la configuración del sistema operativo.

Figura 28. Selección de Idioma

En la figura 29, se indica cómo se va a realizar la instalación del sistema operativo por lo cual se tiene cuatro opciones, si no está relacionado con la instalación, simplemente de clic en instalar.

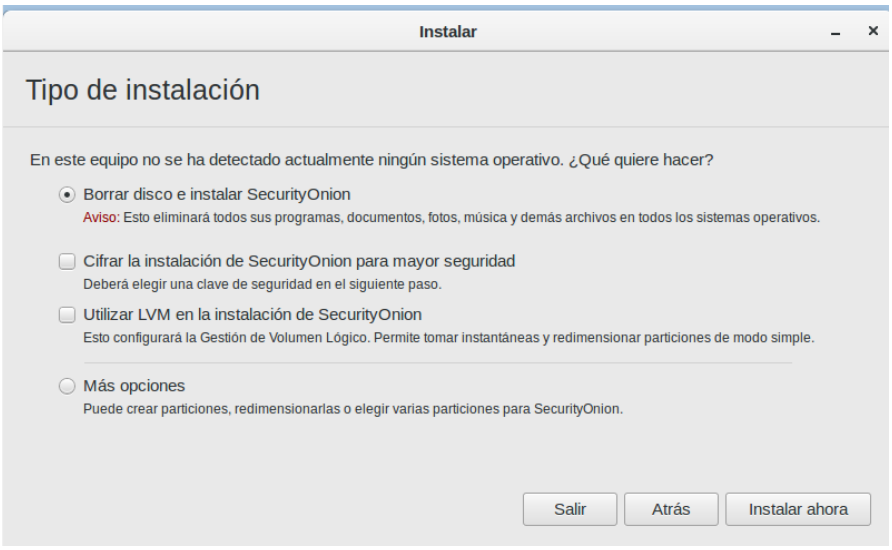


Figura 29. Tipo de Instalación

Es importante precisar la zona horaria respectiva como lo muestra la figura 30, este se empleará para el sensor.

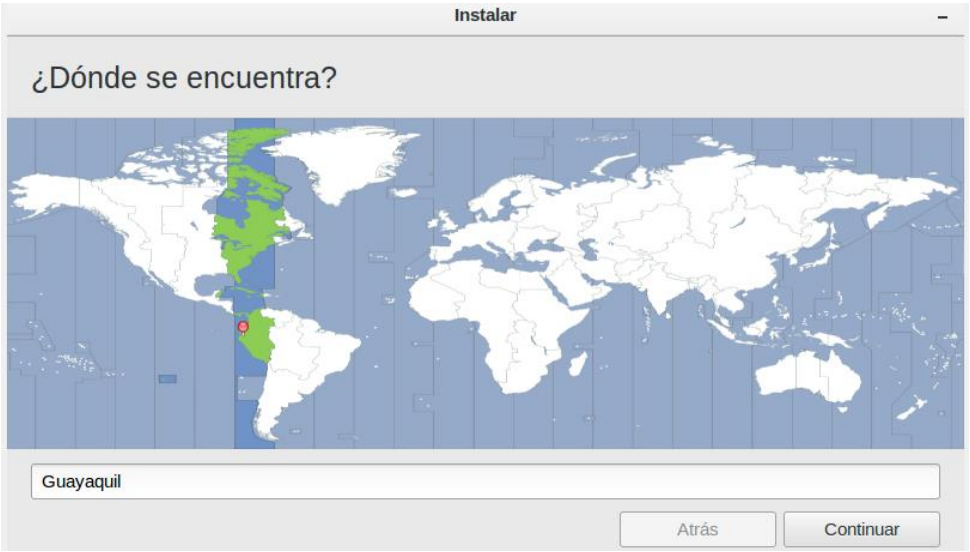


Figura 30. Configuración Zona Horaria.

Como indica la figura 31, se debe especificar los siguientes datos:

- Nombre
- Nombre del equipo
- Nombre de usuario
- Contraseña
- Confirmar contraseña
- Configurar que al inicio de sesión solicite la clave de acceso

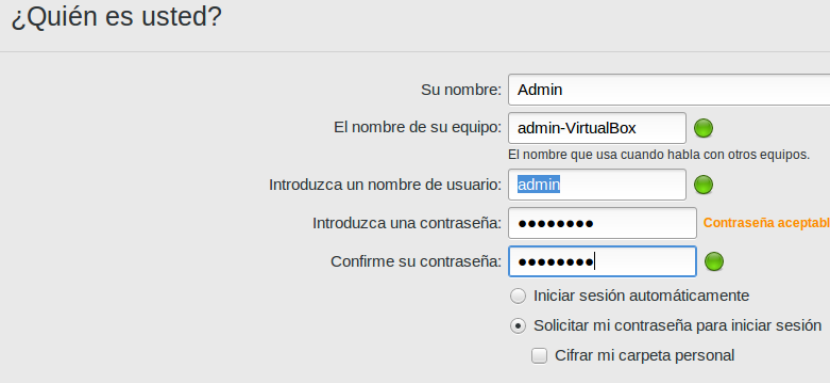


Figura 31. Registro de usuario y contraseña

4.3.2. Red

Después que el sistema se reinicie se procede con la configuración de la red como se puede ver en la figura 32.

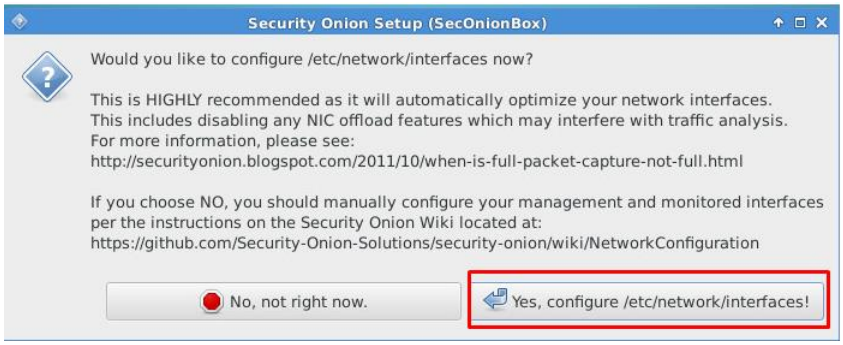


Figura 32. Configuración de la red

De tal manera, como se visualiza en la figura 33 Ingresamos la IP estática para el servidor Security Onion y en la figura 34 detallamos la sub mascara.

Figura 33. Dirección ip

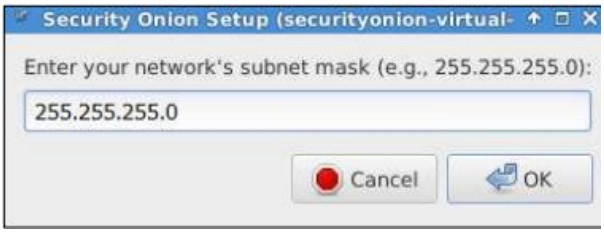


Figura 34. Sub mascara de Red

4.3.3. Sensores y Servidores

Como nos indica la figura 35, se puede elegir en qué modo de producción vamos a utilizar Security Onion.

Figura 35. Modo de configuración

Se debe establecer un usuario para ingresar a las interfaces Squil, Elsa, Squert como indica la figura 36.

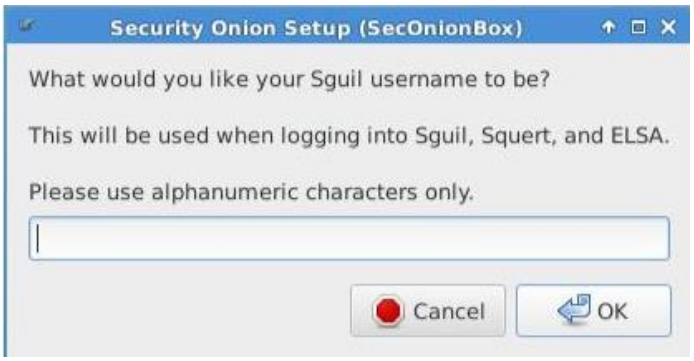


Figura 36. Nombre de Usuario a interfaces

Definidos una contraseña para las interfaces Squil, Elsa, Squert como se indica en la figura 37.

Figura 37. Contraseña a interfaces

4.4. Pruebas y Resultados

Para realizar la validación del sistema Security Onion se ejecutan pruebas de funcionamiento previo a la implementación en la compañía, esto se lo realiza en el data center de la Universidad de las Américas.

En las figuras 38, 39 y 40 se detallan los requerimientos necesarios para el levantamiento de las maquina virtuales.

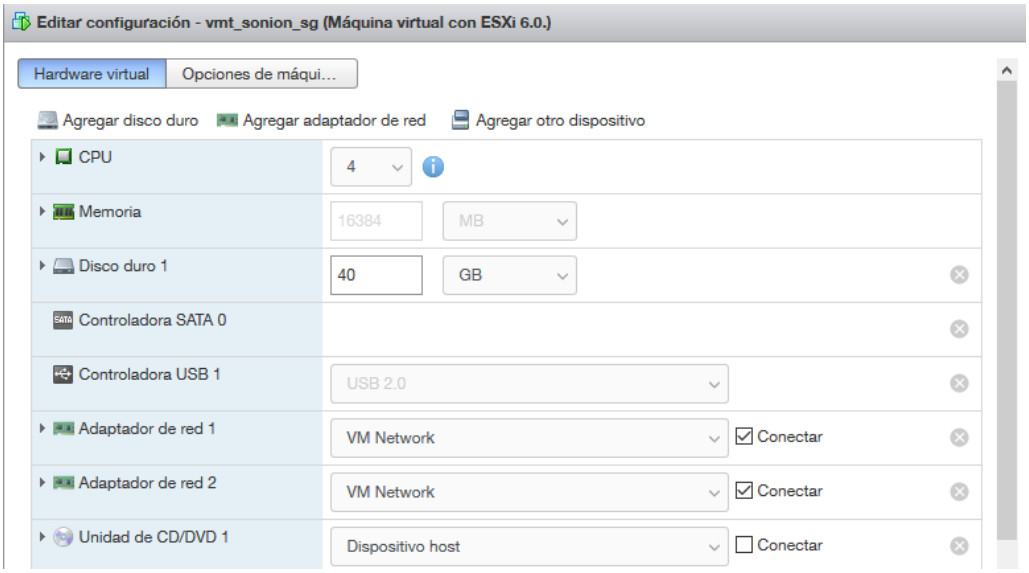


Figura 38. Máquina virtual Security Onion

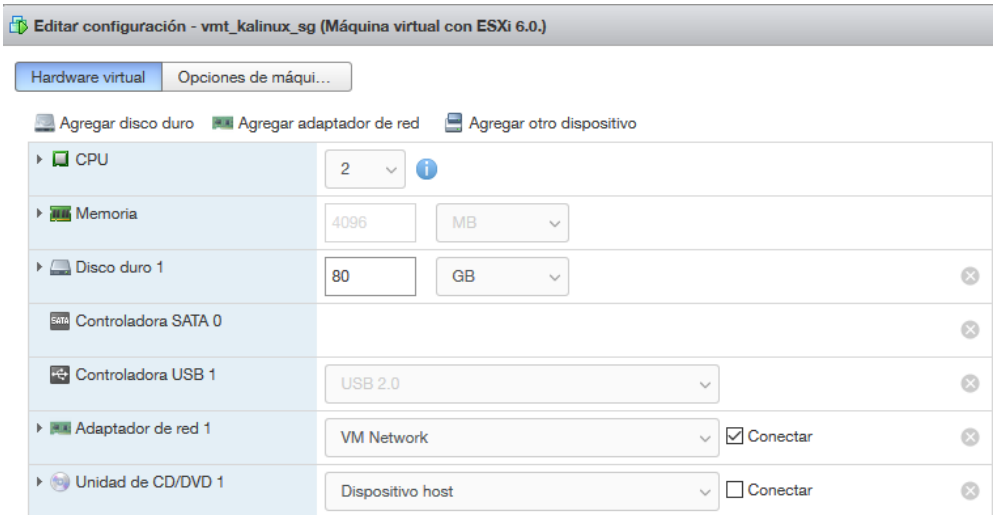


Figura 39. Máquina virtual kali linux

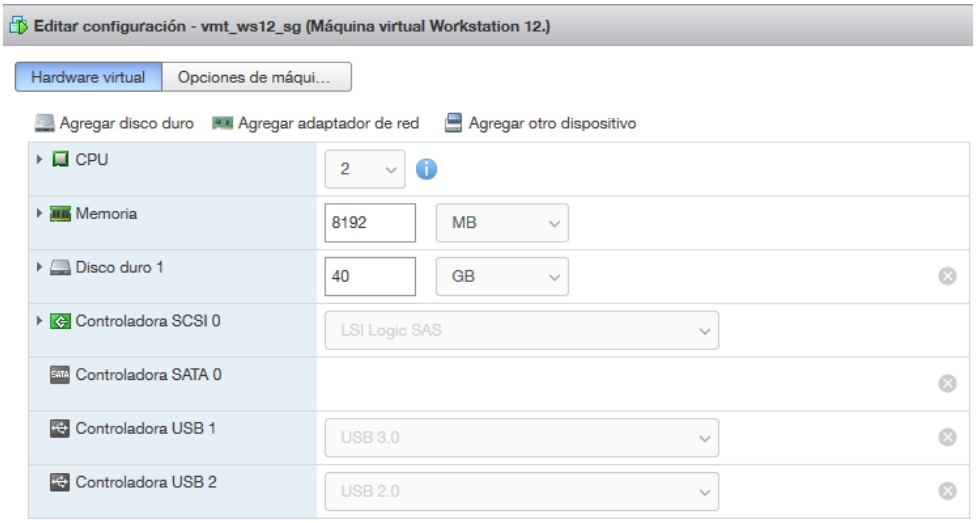


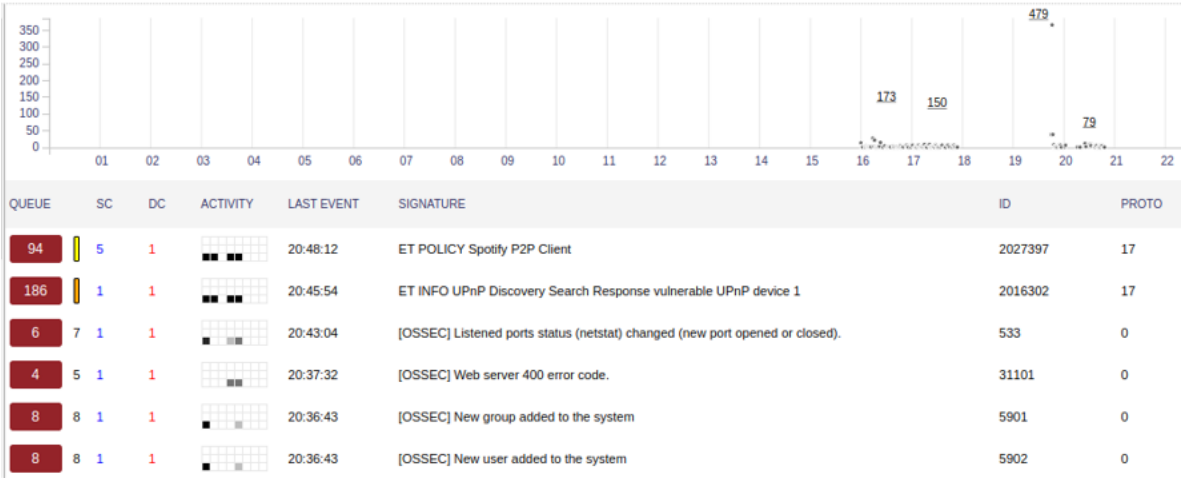
Figura 40. Máquina virtual Windows Server 2012

Una vez realizada la implementación y configuración del sistema Security Onion se procede a realizar el monitoreo con la herramienta Squert como se visualiza en la figura 41.

Figura 41. Herramienta Squert

4.4.1. Violación de alerta

Como se visualiza en la figura 42, encontramos las alertas que han sido detectadas en la red de la empresa Bagant Ecuatoriana.



QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO
94	5	1		20:48:12	ET POLICY Spotify P2P Client	2027397	17
186	1	1		20:45:54	ET INFO UPnP Discovery Search Response vulnerable UPnP device 1	2016302	17
6	7 1	1		20:43:04	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).	533	0
4	5 1	1		20:37:32	[OSSEC] Web server 400 error code.	31101	0
8	8 1	1		20:36:43	[OSSEC] New group added to the system	5901	0
8	8 1	1		20:36:43	[OSSEC] New user added to the system	5902	0

Figura 42. Alertas encontradas

Como se muestra en la figura 42 existe una violación en la política de acceso a la aplicación spotify. En el firewall empresarial se encuentra establecida una regla que indica que ningún personal activo de la empresa pueda acceder a la aplicación como se visualiza en la figura 43.

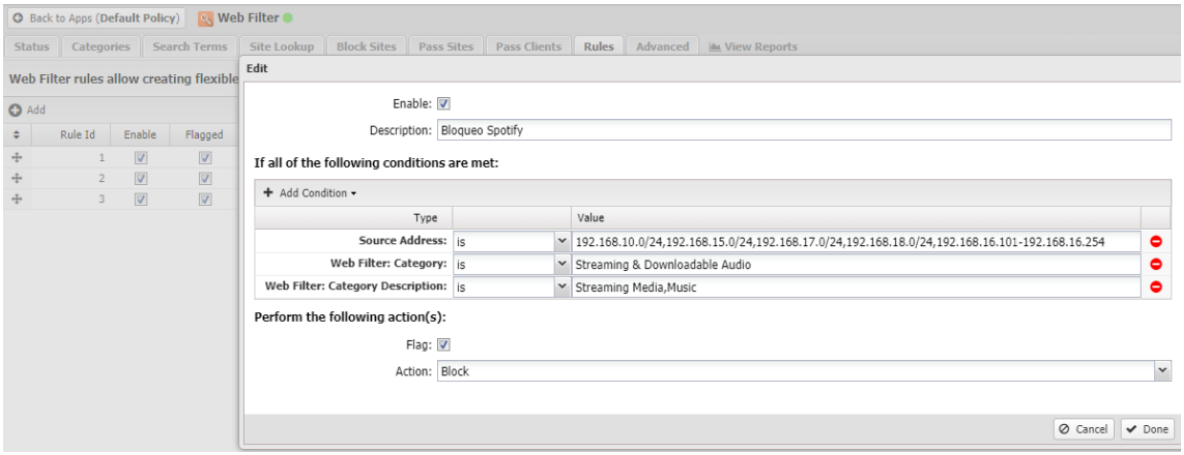


Figura 43. Regla de acceso en el firewall

La figura 44 muestra que el sistema genera una alerta de spotify; adicionalmente se pueden visualizar las IP de origen que se encuentran tratando de ingresar a la aplicación.

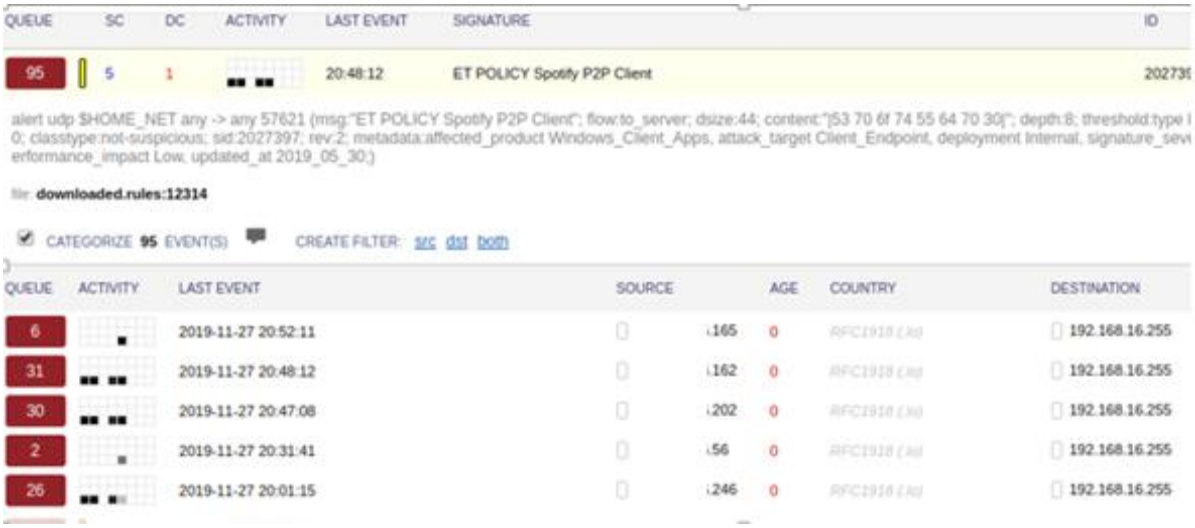


Figura 44. IP intentando ingresar a spotify

4.4.2. Virus

Para verificar el sistema de monitoreo se procede a ejecutar un virus troyano llamado Zeus el cual realiza un envío de paquetes para congestionar la red. Para realizar este ataque controlado se ejecuta el siguiente comando como lo indica la figura 45.

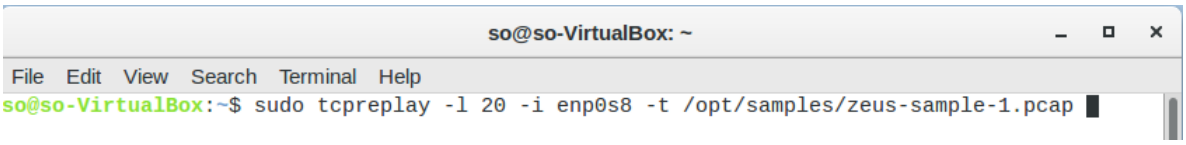


Figura 45. Comando para ejecutar el virus zeus

En la figura 46, el virus empieza a enviar una cadena de paquetes de forma masiva.

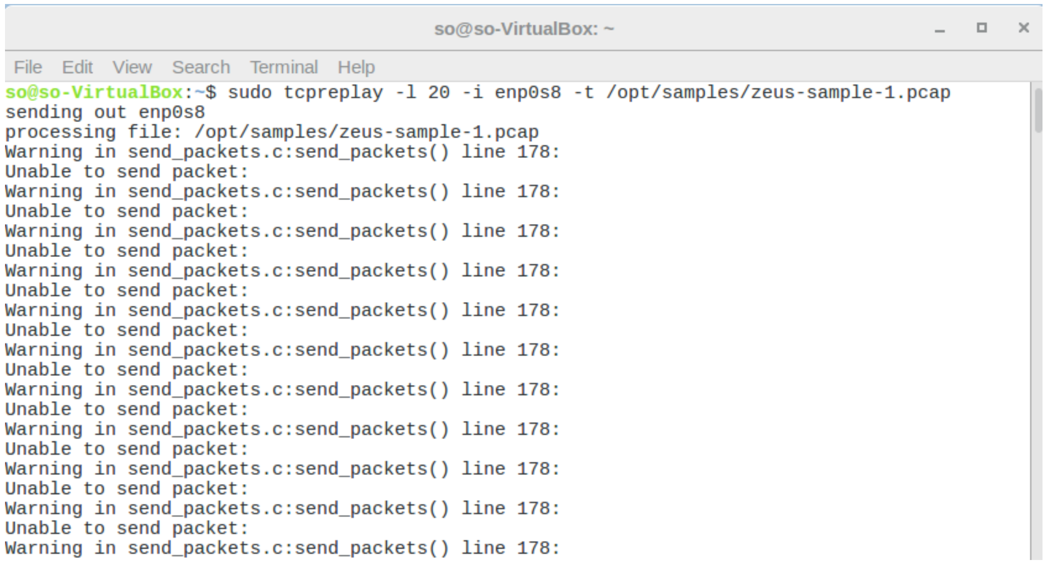


Figura 46. Envió de paquetes de forma masiva

En la figura 47, Security Onion genera una alerta al momento de detectar el virus en la red.

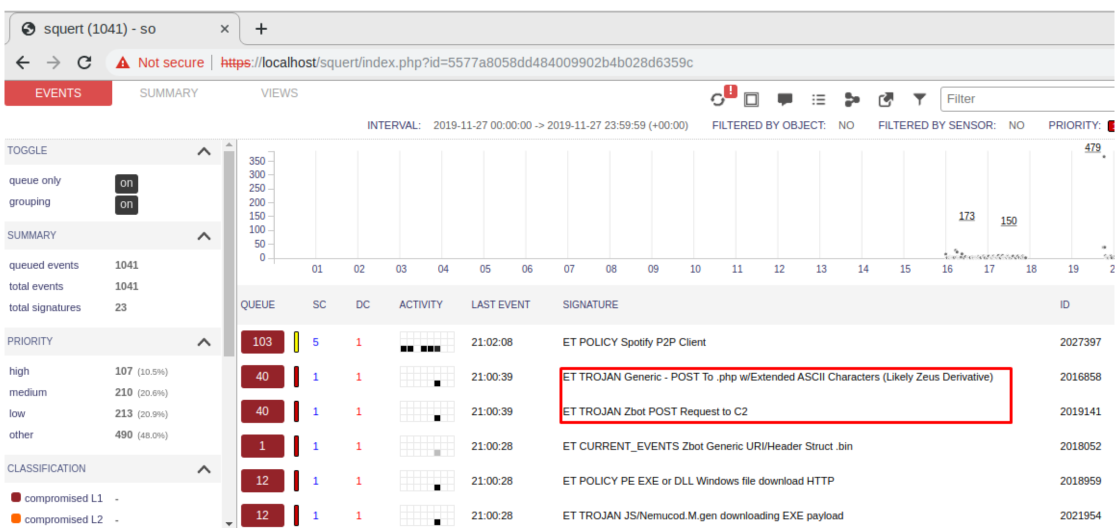


Figura 47. Alerta de virus en Security Onion

Se verifica los eventos de la alerta que se generó y como se puede ver en la figura 48 todos los envíos de paquetes a una dirección IP para que el mismo congestione.

ST	TIMESTAMP	EVENT ID	SOURCE	PORT	DESTINATION	PORT	SIGNATURE
RT	2019-11-27 21:00:39	3.525	35	1034	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
RT	2019-11-27 21:00:39	3.527	35	1033	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
RT	2019-11-27 21:00:38	3.521	35	1034	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
RT	2019-11-27 21:00:38	3.523	35	1033	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
RT	2019-11-27 21:00:37	3.517	35	1034	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
RT	2019-11-27 21:00:37	3.519	35	1033	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
RT	2019-11-27 21:00:36	3.513	35	1034	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
RT	2019-11-27 21:00:36	3.515	35	1033	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
RT	2019-11-27 21:00:35	3.497	35	1034	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
RT	2019-11-27 21:00:35	3.499	35	1033	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
RT	2019-11-27 21:00:35	3.501	35	1034	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)
RT	2019-11-27 21:00:35	3.503	35	1033	.100	80	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)

Figura 48. Eventos de alerta de virus

4.4.3. Ataque de fuerza bruta

Para el ataque de fuerza bruta se utilizará un diccionario de datos, se los puede conseguir en la siguiente dirección: https://wiki.skullsecurity.org/Passwords.

En la figura 44 se puede observar el archivo con el diccionario de datos el cual se está ejecutando sobre un sistema operativo de intrusión con la versión 16.04.6.2 de Kali Linux.

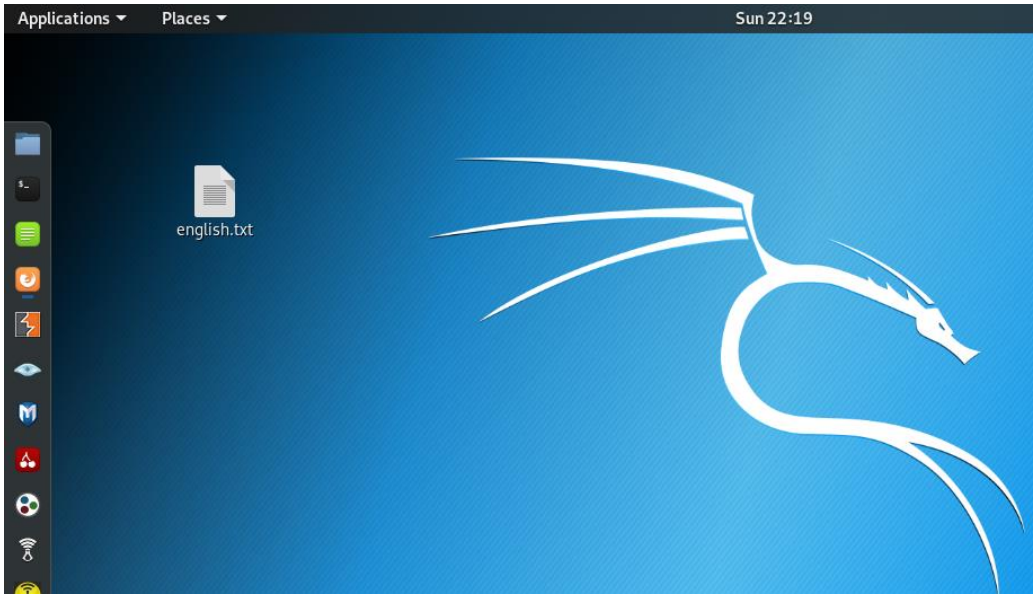


Figura 49. Archivo Diccionario de datos

Se ejecuta el comando nmap para comprobar que puertos del servidor se encuentran abiertos como lo indica la figura 45, por motivos de seguridad y confidencialidad de la información no se podrá especificar la dirección IP; como se valida en la figura 50 para el primer octeto se especifica con (xx), el segundo octeto con (yy) y el tercero con (zz).

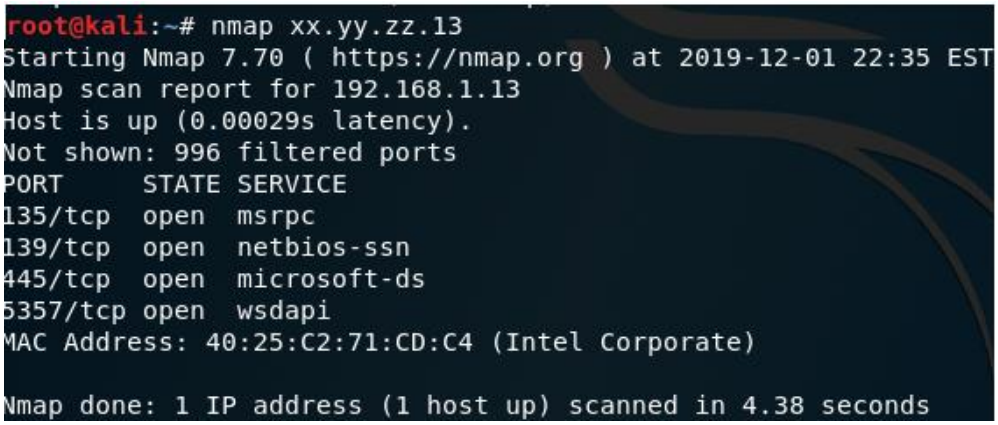


Figura 50. nmap a la ip de servidor

En la figura 50 visualizamos los puertos y servicios que se encuentran abiertos en el servidor de Windows, los mismos realizan las siguientes funciones:

- msrpc: Es un protocolo utilizado en el modelo cliente-servidor; para acceder a un programa que llama al servicio de un programa en otra computadora sin tener que involucrar los detalles de esa computadora en red (ExtraHop Networks, 2019).
- wsdapi: El puerto 5357 es frágil en problemas de pérdidas de información, lo que permitiría el acceso remoto a personas maliciosas (IT-Swarm.Net, 2019).

4.4.3.1. Diagrama de Simulación de ataque

En la figura 51 se observa el diagrama de ataque que se procede desde kali linux hacia el servidor Windows server 2012, el sistema de monitoreo detectara la vulnerabilidad que se esté presentando e inmediatamente lo informara.

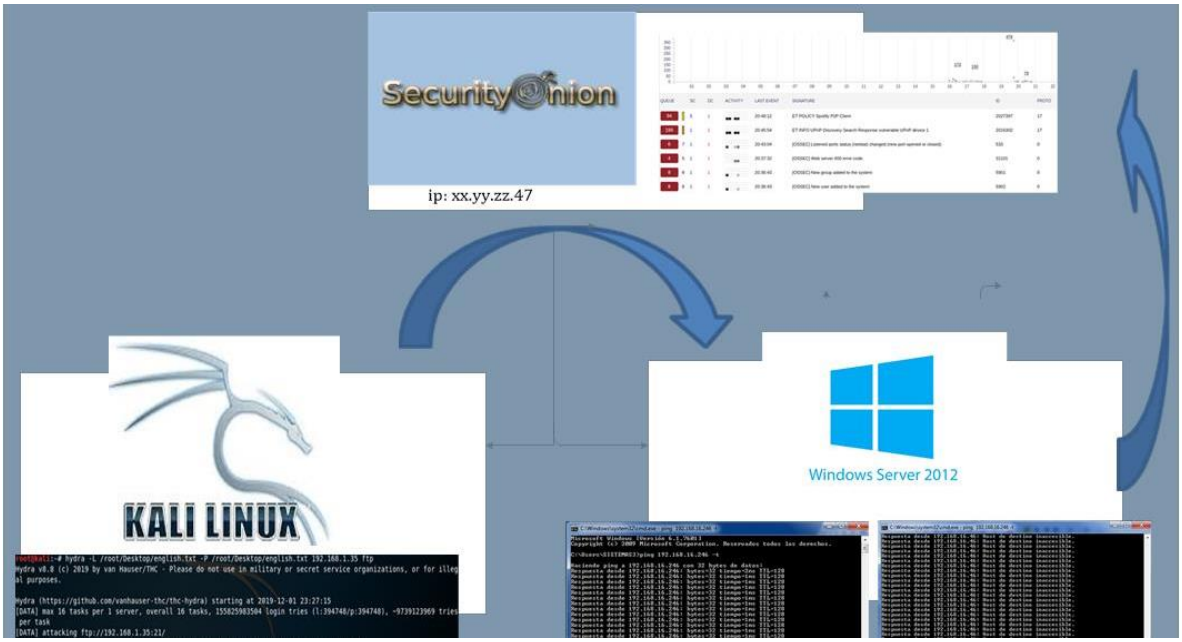


Figura 51. Diagrama de ataque

Se utiliza la herramienta medusa para realizar el ataque, usando el comando que se detalla en la figura 52. Lo que intenta esta funcionalidad es hackear la contraseña del servidor buscando los puertos que se encuentran abiertos en el equipo que va a ser atacado.

```
root@kali:~# medusa -h [redacted]37 -u Administrator -P /root/Desktop/english.tx
t -M http
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.n
et>

ACCOUNT CHECK: [http] Host: 192.168.0.37 (1 of 1, 0 complete) User: Administrato
r (1 of 1, 0 complete) Password: i (1 of 394748 complete)
ACCOUNT FOUND: [http] Host: 192.168.0.37 User: Administrator Password: i [SUCCES
S]
```

Figura 52. Herramienta medusa

En la figura 53, se encuentra la alerta generada por el sistema al momento de generar el ataque con medusa.

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
5	1	1		20:45:28	[OSSEC] Web server 400 error code.	31101	0	0.208%
10	1	1		20:45:00	[OSSEC] Listened ports status (netstat) changed (new port opened or closed).	533	0	0.415%
89	3	3		20:10:53	ET TROJAN Generic - POST To .php w/Extended ASCII Characters (Likely Zeus Derivative)	2016858	6	3.698%
89	3	3		20:10:53	ET TROJAN Zbot POST Request to C2	2019141	6	3.698%
10	2	4		20:10:52	GPL ICMP_INFO PING *NIX	2100366	1	0.415%
4	2	2		20:10:40	ET CURRENT_EVENTS Zbot Generic URI/Header Struct .bin	2018052	6	0.166%
182	10	9		20:10:40	ET POLICY PE EXE or DLL Windows file download HTTP	2018959	6	7.561%

Figura 53. Alerta de fuerza Bruta

4.4.4. Ping de la Muerte

El ataque consiste en enviar una gran cantidad de paquetes icmp mayores a 65500 para colapsar el servidor que se desea atacar.

En la figura 54, se está enviando un ping hacia la IP del servidor (xx.yy.zz corresponden al primer, segundo y tercer octeto) con paquetes de tamaño 65500, el mismo se guardará como un archivo bat y se ejecutará desde la máquina atacante.

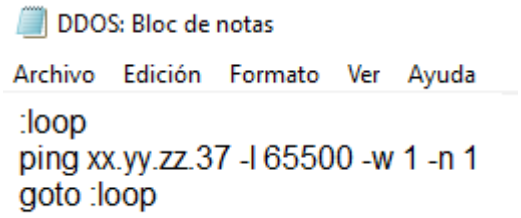


Figura 54. Descripción ddos.bat

La figura 55 muestra el archivo .bat ejecutándose en la máquina atacante y en la figura 56 se encuentra la alerta que muestra que se están enviando grandes cantidades de paquetes hacia uno de los servidores de la red.

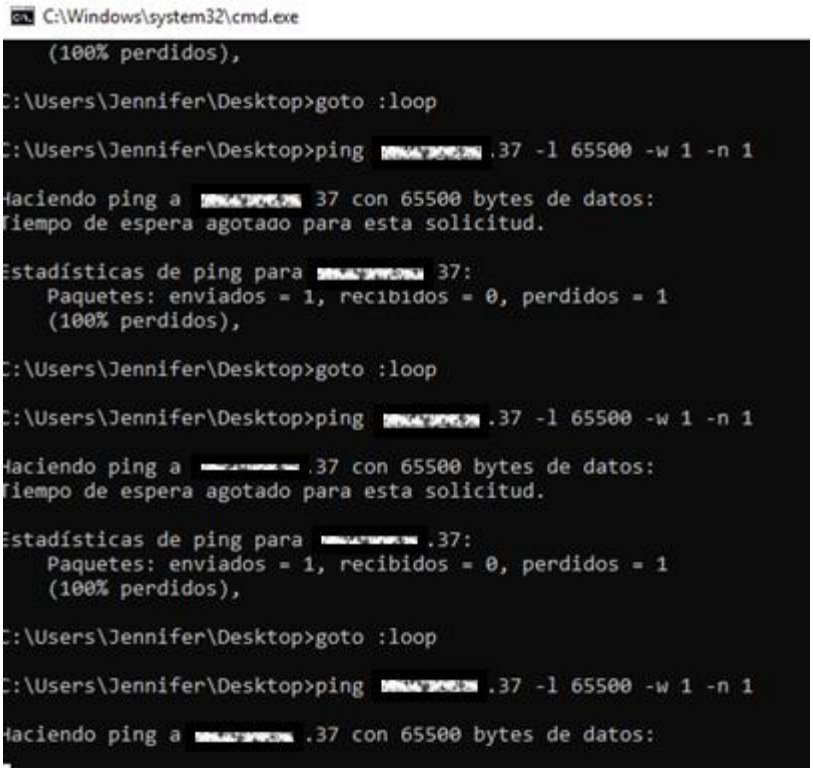
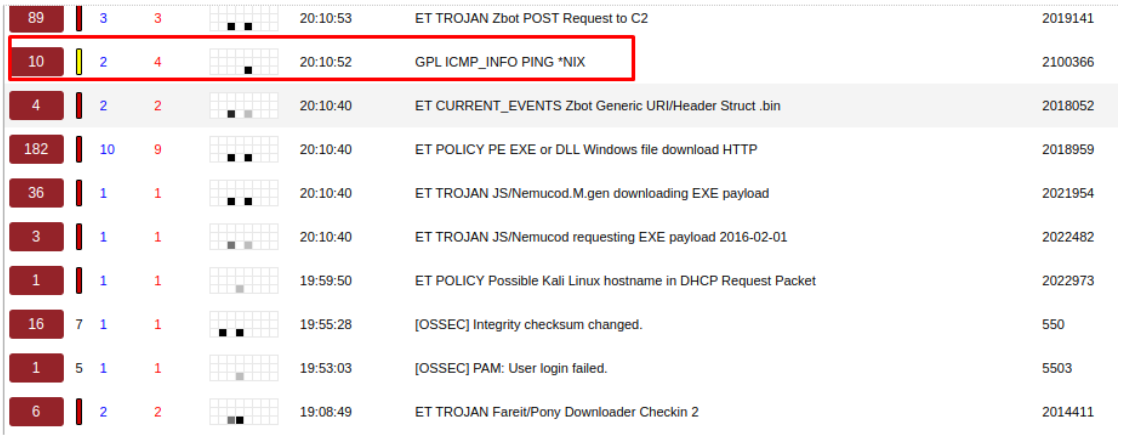


Figura 55. Ejecución del archivo .bat



89	3	3		20:10:53	ET TROJAN Zbot POST Request to C2	2019141
10	2	4		20:10:52	GPL ICMP_INFO PING *NIX	2100366
4	2	2		20:10:40	ET CURRENT_EVENTS Zbot Generic URI/Header Struct .bin	2018052
182	10	9		20:10:40	ET POLICY PE EXE or DLL Windows file download HTTP	2018959
36	1	1		20:10:40	ET TROJAN JS/Nemucod.M.gen downloading EXE payload	2021954
3	1	1		20:10:40	ET TROJAN JS/Nemucod requesting EXE payload 2016-02-01	2022482
1	1	1		19:59:50	ET POLICY Possible Kali Linux hostname in DHCP Request Packet	2022973
16	7 1	1		19:55:28	[OSSEC] Integrity checksum changed.	550
1	5 1	1		19:53:03	[OSSEC] PAM: User login failed.	5503
6	2	2		19:08:49	ET TROJAN Fareit/Pony Downloader Checkin 2	2014411

Figura 56. Alerta generada por ping de la muerte.

4.4.5. Owasp

Se realizó un pentest mediante la herramienta Owasp, la cual sirve para detectar vulnerabilidades en las páginas web, en este caso se hizo un ataque controlado a un servidor de pruebas para verificar el funcionamiento de Security Onion. Esto se puede ver en la figura 57.

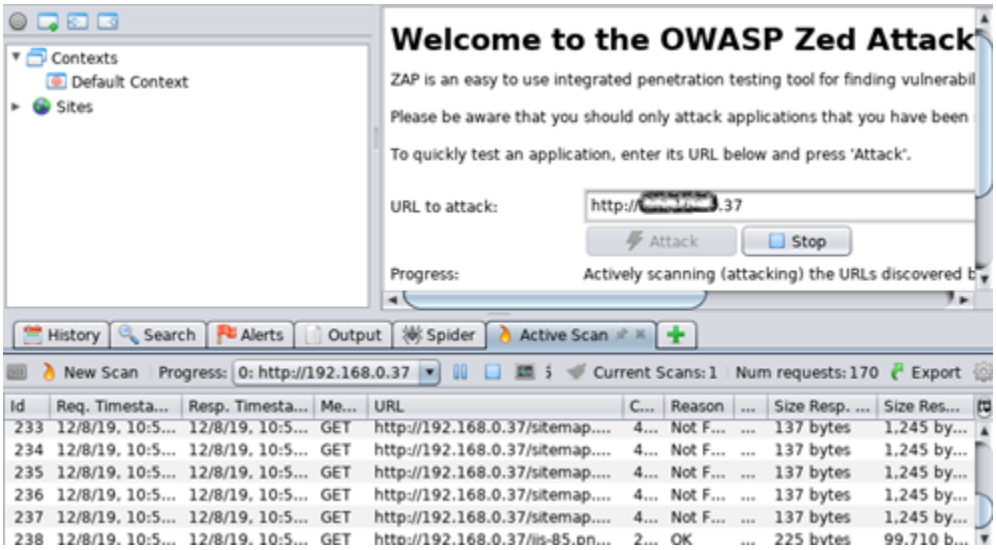


Figura 57. Pentesting owasp

Debido a que este servidor es de pruebas y no contiene un web server, lo que muestra la alerta es un código de error pues no detecta al mismo, por lo cual no es posible realizar el pentesting tal como se muestra en la figura 58.

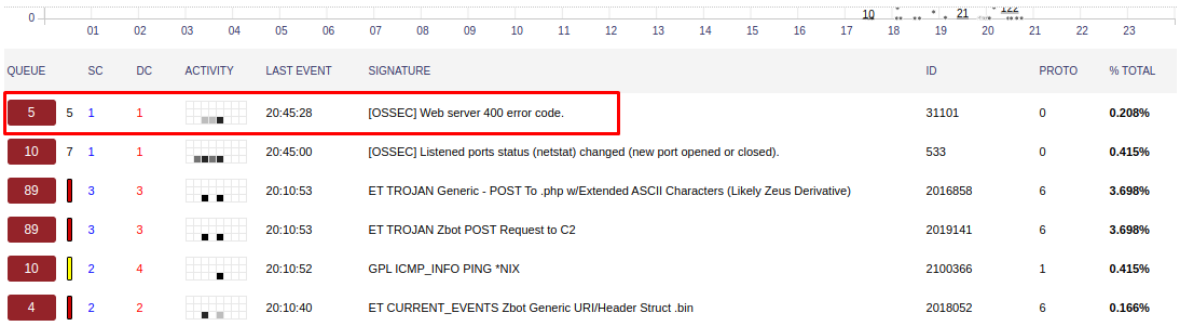


Figura 58. Alerta pentesting owasp

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Se concluye que al implementar una solución para el control de vulnerabilidades en una empresa de construcción utilizando herramientas Open Source Security Onion se pudo notar que existen ciertos errores en las políticas de seguridad del firewall ya que se detectó que ciertos equipos lograron acceder a aplicaciones no permitidas o que estaban bloqueados los accesos y existían puertos que se encontraban abiertos sin tener ninguna utilidad.

Es importante conocer claramente todos los conceptos relacionados con la seguridad de la información, especialmente cuando se trabaja en el área de TI, ya que de esta manera se pueden tratar las vulnerabilidades y amenazas con mayor eficacia.

Se concluye que cada herramienta analizada en este proyecto posee sus propias características, las mismas que las empresas deben tomar en cuenta al momento de adquirir un software de monitoreo dependiendo del tamaño de la empresa, de su presupuesto y de la compatibilidad con el resto de sus sistemas.

Las vulnerabilidades se van presentando día a día, lo que dificulta un control a tiempo o control previo, pero al contar con un software de monitoreo se reduce el índice de riesgo de que se presenten brechas de seguridad y robo de información.

Contar con este tipo de herramientas permitirá a las organizaciones llevar un mayor control de los equipos designados al personal y así monitorear el uso que le dan a los mismos, de esta manera se podrá implementar políticas de seguridad más estrictas como por ejemplo bloqueo de dispositivos USB, prohibición de descargas multimedia (música, videos, imágenes, etc.) que podrían contener virus como troyanos, o la instalación de software ajeno al flujo de negocio de la empresa.

Es primordial tener en consideración que la función de monitorear la red no consiste solamente en implementar un nuevo software, sino que es un trabajo contaste en el cual el personal de TI debe especializarse para tener el conocimiento necesario en el tratamiento de las brechas de seguridad.

Se tomó como referencia INEN 27005 debido que proporciona detalles, formatos y escalas que permite realizar la evaluación e identificación de vulnerabilidad y amenazas.

De acuerdo con el estudio realizado en este proyecto, los softwares propietarios contienen un mayor número de funcionalidades y herramientas que contribuyen con el análisis de las redes empresariales, si la compañía desea contar adicionalmente con este tipo de sistema, debe tomar en cuenta precios y compatibilidad con la infraestructura que posee la misma.

El software operó al 100% al momento de realizar las pruebas de pentesting ya que notificó que los equipos de la empresa estaban siendo vulnerados, además alertó que ciertas políticas de seguridad no estaban bien aplicadas por lo que el personal de TI pudo actuar a tiempo para evitar una caída o una infiltración de información.

5.2. Recomendaciones

Es recomendable realizar la migración de los servidores a una red DMZ, de esta manera se podrá proteger los sistemas importantes y la integridad de la información de un posible ataque que se pueda dar en la infraestructura interna y pueda retrasar el flujo del negocio.

Se debe tener un plan de acción a seguir en el caso de que exista un ataque a los sistemas de la empresa, tomando como base las normas y estándares tanto locales como internaciones.

Los sistemas de monitoreo Open Source o propietarios deben orientarse también como una herramienta para la toma de decisiones y así poder planificar las normas y estándares para la gestión de seguridad de la información.

De acuerdo con los resultados recolectados en este proyecto se recomienda a la empresa realizar un pentesting trimestralmente con el fin de identificar nuevas vulnerabilidades y poder actuar sobre las mismas.

Se recomienda ser más minucioso en el análisis de las políticas y reglas que se encuentran en el firewall, ya que como se pudo comprobar en la herramienta Security Onion, existieron equipos que lograron acceder a aplicaciones que en teoría se encuentran restringidas dentro de la organización.

REFERENCIAS

Accsys. (s.f). Gestión Unificada de Seguridad USM AlienVault. Recuperado el 01 de septiembre de 2019 de https://www.accsys.com.ar/copia-de-mcaffe-intel-security

Acosta, E., & Muñoz, J. (2015). Análisis e implementación de un DIDS para generación de firmas de comportamientos anómalos en la red del edificio matriz de la Empresa Eléctrica Quito. Recuperado el 05 de septiembre de 2019 de https://dspace.ups.edu.ec/handle/123456789/10097

Acunetix. (2019). ¿Està su sitio web a salvo de hackers? Barcelona: Satinfo.

Acunetix. (2019). Acunetix Web Vulnerability Scanner es una herramienta automatizada de seguridad para aplicaciones Web. Recuperado el 08 de septiembre de 2019 de https://www.seaq.co/acunetix.html

Advisors, G. (s.f). Nessus Escáner de Vulnerabilidad. Recuperado el 11 de septiembre de 2019 de https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/

Alejandro. (2016). Como realizar un Ping of Death usando el CMD. Recuperado el 14 de septiembre de 2019 de https://protegermipc.net/2016/06/23/ping-of-death-usando-el-cmd/

Andres, G. (2015). Hydra- Ataque Fuerza Bruta Kali linux. Recuperado el 14 de octubre de 2019 de https://www.youtube.com/watch?v=B65iAhYoi2Y

Antivirus, M. (2018). Sumérgete en la Deep Web. ¿Qué es? ¿Cómo funciona? Recuperado de 15 de Septiembre de 2019 de http://www.mejor-antivirus.es/programas-pc/sumergete-en-la-deep-web-que-es-como-funciona.html

APNIC. (2019). Cómo: analizar capturas de paquetes con Security Onion. Recuperado el 01 de octubre de 2019 de https://blog.apnic.net/2019/07/09/how-to-analysing-packet-captures-with-security-onion/

Arturo, A. T. (2019). LA CIBERSEGURIDAD EN EL ECUADOR, UNA PROPUESTA DE ORGANIZACION. En L. R. Carlos Arturo Tates Almeida. Quito: Primera Edicion.

Bagant Ecuatoriana Cía. Ltda. (2019). Bagant. Recuperado el 19 de noviembre de 2019 de http://www.bagant.com/568_la-empresa/

Bravo, V. P. (s.f). Implantación De Una Herramienta Ossim Para El Monitoreo Y Gestión De La Seguridad De La Red Y Plataformas Windows Y Linux Aplicado A Empresas Medianas. Guayquil: Primera Edicion.

Business, A. (2019). Nuestros clientes son el centro de nuestro universo. Recuperado el 17 de octubre de 2019 de https://www.alienvault.com/who-we-are/customers#customer-logos-2

Business, AT&T. (2019). Cientos de MSSPs confían en AlienVault. Recuperado el 02 de diciembre de 2019 de https://www.alienvault.com/products/usm-for-mssp

bytelearning. (2016). Cómo evitar el "ping de la muerte" en Linux. Recuperado el 11 de noviembre de 2019 de https://bytelearning.blogspot.com/2016/06/como-evitar-el-ping-de-la-muerte-en.html

Cibersecurity, A. (2019). Productos AlienVault. Recuperado el 15 de octubre de 2019 de https://www.alienvault.com/products

Cybersecurity AT&T. (2019). Tipos de implementación de dispositivos USM. Recuperado el 27 de noviembre de 2019 de https://www.alienvault.com/documentation/usm-appliance/deployment-plan/about-usm-deployment-types.htm?tocpath=Documentation%7CAlienVault%C2%AE%20USM%20Appliance%E2%84%A2%7CDeployment%20Guide%7CUSM%C2%A0Appliance%20Deployments%7C_____1

Cybersecurity, A. (s.f). Requisitos de implementación de dispositivos USM. Recuperado el 22 de diciembre de 2019 de

https://www.alienvault.com/documentation/usm-appliance/sys-reqs/hardware-spec.htm

DHacker Tutorials. (2019). Installing OWASP ZAP on Kali Linux. Recuperado el 14 de diciembre de 2019 de https://www.youtube.com/watch?v=9-jcs7Cm-iE

ESET. (2014). Cómo utilizar OpenVAS para la evaluación de vulnerabilidades. Recuperado el 19 de octubre de 2019 de https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/,

Eset. (2019). Ciberataques: una de las amenazas con más probabilidades de ocurrir en 2019. Recuperado el 27 de Noviembre de 2019 de https://www.welivesecurity.com/la-es/2019/02/19/ciberataques-amenazas-mas-probabilidades-sufrir-2019/

ExtraHop Networks. (2019). Llamada a procedimiento remoto de Microsoft (MSRPC). Recuperado el 27 de Noviembre de 2019 de https://www.extrahop.com/resources/protocols/msrpc/

Github. (2019). Security-Onion-Solutions/security-onion. Recuperado el 29 de diciembre de 2019 de https://github.com/Security-Onion-Solutions/security-onion

Gómez, Á. (2013). Auditoría de seguridad informática. Bogotá: Ediciones de la U.

Greenbone Networks. (2019). Cómo los clientes de Greenbone manejan la vulnerabilidad. Recuperado el 18 de noviembre de 2019 de https://www.greenbone.net/en/case-studies/

GREENETICS. (2018). Audita la seguridad de su sitio web con Acunetix Web Vulnerability Scanner. Recuperado el 08 de diciembre de 2019 de https://www.greenetics.com.ec/acunetix

Hector, P. (2014). FASES DEL HACKING ETICO. Recuperado de 28 de noviembre de 2019 de https://hectorpedraza10.wordpress.com/2014/11/21/fases-del-haking-etico/

INEN. (2012). Norma Técnica Ecuatoriana NTE INEN ISO/IEC 27005:2012. Quito: Primera Edicion.

Informatica, S. (2013). Amenazas y fraudes en los sistemas de la información. Recuperado el 23 de diciembre de 2019 de https://infosegur.wordpress.com/2013/11/10/amenazas-y-fraudes-en-los-sistemas-de-la-informacion/

Informatica, T. (s.f.). Vulnerabilidades informáticas. Recuperado el 20 de diiembre de 2019 de https://tecnologia-informatica.com/vulnerabilidades-informaticas/#Vulnerabilidad_Seguridad_informatica

INFOSEC RESOURCES . (2020). A Brief Introduction to the OpenVAS Vulnerability Scanner. Recuperado el 18 de diciembre de 2019 de

https://resources.infosecinstitute.com/a-brief-introduction-to-the-openvas-vulnerability-scanner/#gref

IT-Swarm.Net. (2019). ¿Puerto 5357 TCP en Windows 7 professional 64 bit? Recuperado el 09 de diciembre de 2019 de https://www.it-swarm.net/es/port/puerto-5357-tcp-en-windows-7-professional-64-bit/957462561/

Juniper Research. (2018). Soluciones contra la vulnerabilidad empresarial latente. Computerworld, 28.

K, J. (2017). Security Onion with Elasticsearch, Logstash, and Kibana (ELK). Recuperado el 16 de diciembre de 2019 de https://www.youtube.com/watch?v=cUP_ZRn5rro

k, J. (2018). Security Onion Lab: How to Install/Configure/Troubleshoot *NEW*. Recuperado el 11 de noviembre de 2019 de https://www.youtube.com/watch?v=jRoQUVY-2Ic

Kali Linux. (2013). Tutorial de medusa para Kali Linux. Recuperado el 28 de noviembre de 2019 de https://kalilinux.foroactivo.com/t64-tutorial-de-medusa-para-kali-linux

Kaspersky. (2018). What is ZeuS Virus? Recuperdo el 14 de diciembre de 2019 de https://www.youtube.com/watch?v=mWtlc7mfA2I

La Red. (2018). TUTORIAL. ATAQUE DE DENEGACIÓN DE SERVICIO (DoS). Recuperado el 13 de diciembre de 2019 de http://cursoslared.com/archivos/1529

Leo, R. (2009). Tutorial - Ataques D.o.S a base de pings. Recuperado el 02 de septiembre de 2019 de https://www.blackploit.com/2009/09/tutorial-ataques-dos-base-de-pings.html

LogRhythm. (2019). Obtenga el Cuadrante mágico para SIEM de Gartner 2018. Recuperado el 19 de noviembre de 2019 de https://es.logrhythm.com/gartner-magic-quadrant-siem-report-2018/

Martin, J. (2015). Nessus- Que es, como se usa. Recuperado el 19 de enero de 2019 de https://prezi.com/e351d0eg5hsx/nessus-que-es-como-se-usa/

Mediapro. (2018). Vulnerabilidad informática: ¿cómo protegerse? Recuperado el 23 de noviembre de 2019 de https://blog.mdcloud.es/vulnerabilidad-informatica-como-protegerse/

Multisystem. (2014). LOS BENEFICIOS DE ACUSENSOR DE ACUNETIX. Recuperado el 12 de octubre de 2019 de http://www.multisystem.cl/productos/acunetix-2/los-beneficios-de-acusensor-de-acunetix/

MUNDOHACKERS. (s.f). ATAQUE DDOS EN CMD – PING DE LA MUERTE. Recuperado el 14 de diciembre de 2019 de https://mundo-hackers.weebly.com/ping-de-la-muerte.html

Onion, S. (2019). netsniff-ng . Recuperado el 18 de noviembre de 2019 de https://securityonion.readthedocs.io/en/latest/netsniff-ng.html

OpenVAS. (s,f). About OpenVAS. Recuperado el 15 de octubre de 2019 de https://www.openvas.org/about.html

Property, A. I. (2019). AlienVault OSSIM® Installation Process. Recuperado el 16 de noviembre de 2019 de https://www.alienvault.com/documentation/usm-appliance/initial-setup/ossim-installation.htm

Rapid7. (2019). insight VM. Recuperado el 16 de noviembre de 2019 de https://www.rapid7.com/products/insightvm/

rapid7. (s.f). Features. Recuperado el 17 de noviembre de 2019 de https://www.rapid7.com/products/insightvm/features/

rapid7. (s.f). Our Customers. Recuperado el 11 de noviembre de 2019 de https://www.rapid7.com/about/customers/

Sanchez, G. (2019). Hacking etico. Recuperado el 28 de noviembre de 2019 de https://cronicaseguridad.com/2019/02/05/hacking-etico-1/

Sanchez, R. C. (2019). Las fases del Hacking Ético. Recuperado el 18 de octubre de 2019 de https://ehack.info/las-fases-del-hacking-etico/

Security Onion Solutions. (2019). Security Onion Documentation. Recuperado el 17 de noviembre de 2019 de https://buildmedia.readthedocs.org/media/pdf/securityonion/latest/securityonion.pdf

SoftDoit. (s.f). MÁS INFORMACIÓN SOBRE SAP ERP CARACTERÍSTICAS Y FUNCIONALIDADES. Recuperado el 19 de octubre de 2019 de https://www.softwaredoit.es/sap-erp-caracteristicas-y-funcionalidades/sap-erp-caracteristicas-y-funcionalidades.html

SOLARWINDS . (2017). SOLARWINDS NETWORK PERFORMANCE MONITOR. Recuperado el 26 de noviembre de 2019 de https://www.solarwinds.com/-/media/solarwinds/swdc/pdf/npm/1702_npm_datasheet.ashx

SolarWinds Worldwide, LLC. (2020). Alertas de monitoreo de red. Recuperado el 28 de noviembre de 2019 de https://www.solarwinds.com/network-performance-monitor/use-cases/network-alert

SolarWinds Worldwide, LLC. (2020). Herramienta de mapeo de red. Recuperado el 28 de noviembre de 2019 de https://www.solarwinds.com/network-performance-monitor/use-cases/network-mapping-tool

SolarWinds Worldwide, LLC. (2020). Monitoreo de disponibilidad de red. Recuperado el 28 de noviembre de 2019 de https://www.solarwinds.com/network-performance-monitor/use-cases/network-availability-monitoring

SolarWinds Worldwide, LLC. (2020). Network Availability Monitoring. Recuperado el 28 de noviembre de 2019 de https://www.solarwinds.com/network-performance-monitor/use-cases/network-availability-monitoring

SolarWinds Worldwide, LLC. (2020). Análisis de ruta de red de NetPath. Recuperado el 28 de noviembre de 2019 de https://www.solarwinds.com/network-performance-monitor/use-cases/netpath

Sphinx. (2019). PCAPs for Testing. Recuperado el 19 de octubre de 2019 de https://securityonion.readthedocs.io/en/latest/pcaps.html

Sqearl, S. (31 de Enero de 2019). Intrusion Detection System Tutorial: Setup Security Onion 2019. Recuperado el 29 de noviembre de 2019 de https://www.youtube.com/watch?v=vTLt7dl5IYI

Suarez, D. (2017). Malware, Ransonware, Estrategias de protección. Computerworld, 22.

Tenable. (2018). DataSheet. Hoja de datos de Tenable.sc Recuperado de 16 de enero de 2019 de https://es-la.tenable.com/data-sheets/tenable-sc

tenable. (2019). tenable assure. Recuperado el 22 de diciembre de 2019 de https://es-la.tenable.com/partners