UNIVERSIDAD DE PIURA

FACULTAD DE INGENIERÍA

Implementación de un sistema de Gestión de Eventos e Información de Seguridad para la Marina de Guerra del Perú

Trabajo de Suficiencia Profesional para optar el Título de
Ingeniero Industrial con mención en Gestión Logística

Luis Rodrigo López Torres Herrera

Revisor:
Dr. Ing. Ronald Alejandro Ruiz Robles

Piura, julio de 2019

UNIVERSITAS • STUDIORUM • PIURENSIS

Dedicatoria

A mi familia por su ardua labor, comprensión en momentos difíciles y apoyo incondicional.

UNIVERSITAS • STUDIORUM • PIURENSIS

Resumen Analítico – Informativo

“Implementación de un sistema de Gestión de Eventos e Información de Seguridad para la Marina de Guerra del Perú”
Luis Rodrigo López Torres Herrera
Asesor: Dr. Ing. Ronald Alejandro Ruiz Robles
Trabajo de Suficiencia Profesional.
Título de Ingeniero Industrial con mención en Gestión Logística
Universidad de Piura. Facultad de Ingeniería.
Piura, julio de 2019

Palabras claves: SIEM / herramientas de seguridad / correlación.

Introducción: Hoy en día los ataques a la infraestructura de la red de cualquier institución son cada vez más elaborados y poseen distintas herramientas y/o métodos que amenazan los activos críticos. La Marina de Guerra del Perú, no está exenta de estos tipos de ataque, por tal motivo el alto mando naval designó la tarea de implementar un sistema que permite correlacionar toda información pertinente de las herramientas de seguridad, que antes se monitoreaban de manera independiente que no permitía ver en macro las operaciones. Esto con la finalidad de monitorear el flujo de información y mitigar y/o mitigar cualquier tipo de amenaza que pueda penetrar la red institucional naval.

Metodología: Recopilación de información, elaboración de informes, trabajo en equipo, elaboración de diagrama Gantt, ejecución de tareas programadas.

Resultados: Utilizando el sistema de gestión de eventos e información de seguridad (SIEM) se ha logrado discernir la información sensible y útil para disminuir el porcentaje de intentos de ataque a los servicios que ofrece la institución y datos relevantes de cada trabajador que puede afectar su integridad.

Conclusiones: Es un sistema seguro que permite visualizar el flujo de la información del intento de ataque que permitirá al analista de seguridad de guardia tomar la medida pertinente de cada tipo de amenaza utilizando los casos de uso previamente establecidos.

Fecha de elaboración del resumen: 23 de junio de 2019

Analytical-Informative Summary

"Implementación de un sistema de Gestión de Eventos e Información de Seguridad para la Marina de Guerra del Perú"
Luis Rodrigo López Torres Herrera
Advisor: Dr. Ing. Ronald Alejandro Ruiz Robles
Sufficiency Professional Work
Industrial Engineer degree with a mention in Logistics Management
Universidad de Piura. Facultad de Ingeniería.
Piura, july 2019

Keywords: SIEM / security tools / correlation.

Introduction: Nowadays, attacks on network's infrastructure of any institution are more elaborates and use different tools or methods which threaten critical assets. The Peruvian Navy, is not exempt from these types of attack, for this reason the naval high command appointed the task of implementing a system that allows correlate all relevant information of the security tools, which were previously monitored independently, it did not allow us to see the operations in macro. This us for the purpose of monitoring the flow of information and mitigating or decrease any type of threat that the network's institución can penétrate.
Methodology: Compilation of information, preparation of reports, team work, Gantt's diagram, execution of scheduled tasks.

Methodology: Using the system of security information and event management (SIEM), it has been posible to discern sentive and useful information to reduce the percentage of attempts to attack the offered's services by the institución and relevant data of each worker that may affect their integrity.

Results: It is a secure system that allows visualizing the information flow of the attack attempt that will allow the security analyst on duty to take the relevant measure of each type of threat using previously established use cases.

Conclusions: It is a secure system that allows visualizing the information flow of the attack attempt that will allow the security analyst on duty to take the relevant measure of each type of threat using previously established use cases.

Summary date: june, 23th,2019

Tabla de contenido

Figuras

Anexos

Introducción

Hoy en día los ataques a organizaciones privadas, como a una planta industrial automatizada de ensamblaje de misiles, y a entidades públicas, como la alteración de los resultados en un proceso electoral en el sistema de base de datos de la Oficina Nacional de Procesos Electorales (ONPE), generan gran impacto. Estas intrusiones, que los agresores utilizan, son cada vez más sofisticadas, organizadas e ingeniosas. Los indicios de posibles actividades maliciosas pueden ser difíciles de observar y pueden llegar a pasar desapercibidas. Se hace necesario por tanto revisar los eventos en varias herramientas de seguridad correlacionadas entre sí que monitoreen la red para encadenar y entender una serie de acciones que conlleven a la posibilidad real de detectar una intrusión en los sistemas.

La Marina de Guerra del Perú, no es inmune a los intentos de penetración a los sistemas críticos que componen la red institucional, es por ello que hace algunos años se monitoreaba el ciberespacio naval a través de sensores independientes que por el nivel de tecnología que se usaba era suficiente para mantener el control del mismo. Sin embargo, el mundo de la tecnología crece a pasos agigantados, es por ese motivo que existen nuevos métodos de ataque y se necesita por lo tanto software y hardware acorde a estos. La solución para estos inconvenientes, diseñada y ya en uso, es la implementación de un SIEM (Security Information and Event Management) capaz de centralizar y correlacionar los sensores independientes para una eficaz detección de patrones para un óptimo método que alerta al analista de seguridad para tomar una medida correctiva, en ese momento, y preventiva, estudiando las acciones realizadas por el potencial atacante.

En el capítulo 1, se explica el organigrama de la institución, así mismo se describe las funciones de la Comandancia de Ciberdefensa, y las funciones que yo realizo en mi área de trabajo para llevar a cabo un desempeño óptimo en conjunto con el resto de departamentos y los resultados propuestos del proyecto desarrollado para mejorar la seguridad informática en la red de la Marina de Guerra del Perú.

En el capítulo 2, se describe la fundamentación del tema elegido mediante una problemática a nivel mundial de los incidentes más graves a nivel mundial y los impactos que estos repercutieron, la identificación del problema preliminar de la institución. También se describe la relación de lo desarrollado en este ámbito y la formación naval e ingenieril obtenida a lo largo de los años de estudios a este momento.

En el capítulo 3, se relata los aportes y decisiones que tomé junto con mi equipo de trabajo para llevar adelante el proyecto de un sistema de gestión y seguridad SIEM (Security Information and Event Management) capaz de centralizar y correlacionar los sensores independientes, y las herramientas de seguridad que se integraron.

Capítulo 1

Aspectos generales

1.1. Organigrama, misión y visión

1.1.1. Organigrama

La estructura organizacional de la Marina de Guerra del Perú posee distintos órganos en los cuales se desempeñan diversas funciones específicas según el alcance establecido para el correcto desempeño de este órgano de ejecución de las Fuerzas Armadas nacionales. Dentro de los órganos de línea, se encuentra la Comandancia de Ciberdefensa, la cual es la responsable del alistamiento y entrenamiento de sus medios operativos, así como del planeamiento y conducción de operaciones de Ciberdefensa, con la finalidad de asegurar el empleo del ciberespacio por fuerzas propias en cualquier condición.

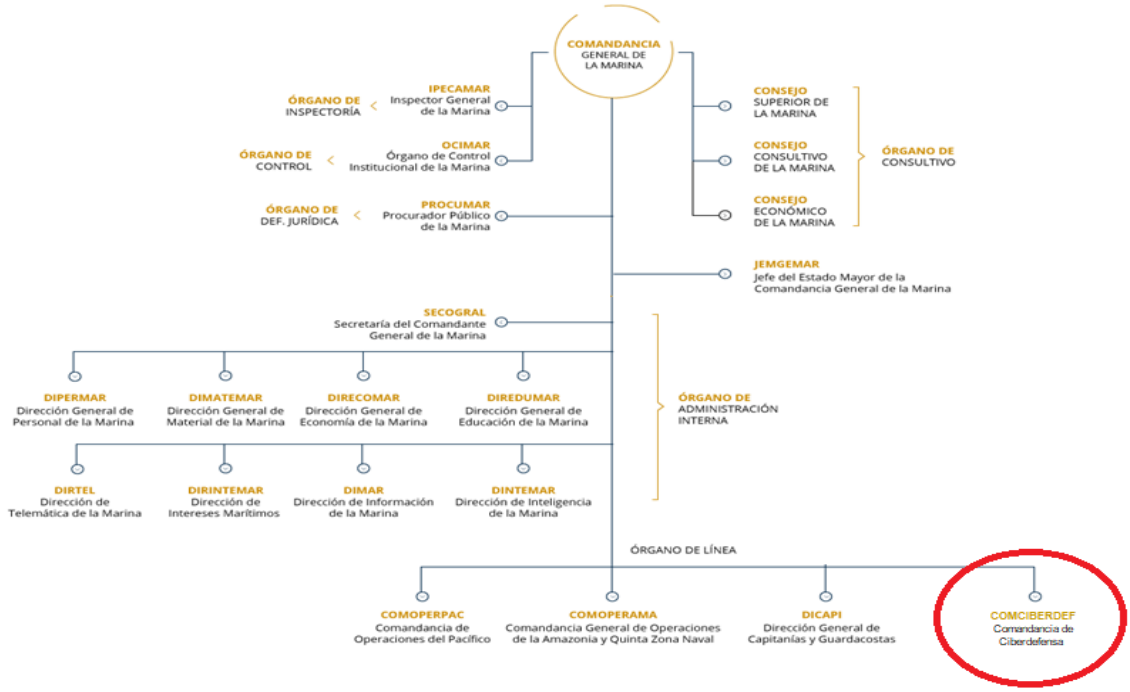

Figura 1 Organigrama de la Marina de Guerra del Perú
Fuente: Marina de Guerra del Perú

1.1.2. Misión

Ejercer la vigilancia y protección de los intereses nacionales en el ámbito marítimo, fluvial y lacustre, y apoyar la política exterior del Estado a través del Poder Naval; asumir el control del orden interno, coadyuvar en el desarrollo económico y social del país y participar en la Defensa Civil de acuerdo a ley; con el fin de contribuir a garantizar la independencia, soberanía e integridad territorial de la República y el bienestar general de la población.

1.1.3. Visión

Poder Naval capaz de actuar con éxito donde lo requieran los intereses nacionales

En la Figura 2, se aprecia el escenario donde La Marina de Guerra del Perú actúa como país marítimo, amazónico, bioceánico y posee presencia en la Antártida para realizar con satisfacción las acciones designadas por el Jefe Supremo de las Fuerzas Armadas.

Figura 2 Situación actual nacional
Fuente: Marina de Guerra del Perú

1.2. Comando de Ciberdefensa

La misión del comando de Ciberdefensa es ejercer el comando de las operaciones en el ciberespacio verificando que los organismos institucionales y extrainstitucionales se encuentren en óptimo estado de alistamiento para el desarrollo de las operaciones asignadas; y otras, que le asigne el Comandante General de la Marina.

Su principal función planear y conducir operaciones en el ciberespacio para asegurar su empleo efectivo con la finalidad de alcanzar los objetivos Institucionales

El alcance de las funciones se resume en formular el planeamiento operativo del comando de Ciberdefensa en el ámbito de responsabilidad en concordancia con las directivas del Comandante General de la Marina y ejecutar las operaciones y acciones necesarias para garantizar la seguridad digital de la Institución y del Estado.

1.3. Descripción de cargo ocupado

En el año 2017 con el grado de Alférez de Fragata, presté servicios en el B.A.P "Sánchez Carrión" ocupando el cargo de "Oficial de Comunicaciones y Navegación" del Departamento de Operaciones realizando el trabajo de operador y mantenimiento del equipamiento de comunicaciones, meteorología y navegación, adicionalmente ejercía el cargo de "Oficial de Telemática" encargado de tramitar la correspondencia interna y externa con las diversas Unidades Navales y Dependencias de la Marina de Guerra del Perú.

En la Comandancia de Ciberdensa ocupó el cargo de jefe de la división de sensores, análisis y correlación de información en el departamento de defensa, como mi función principal es efectuar operaciones de defensa en detección, análisis y correlación de incidentes, para garantizar el libre uso del ciberespacio de las unidades navales y dependencias de la Institución, así como realizar actividades necesarias para la ejecución de las operaciones y tareas asignadas a la comandancia por el comandante general de la Marina. Enfocado en el sistema de "Gestión de Eventos e Información de Seguridad" desarrollo tareas como efectuar operaciones de correlación en los sensores de seguridad, en otras palabras, es monitorear las distintas herramientas de seguridad para buscar algún patrón que no haya sido detectado por las reglas propuestas y asignadas al SIEM, en caso de detectar algún patrón se informa al jefe inmediato superior sobre el ciberataques en proceso u ocurridos con la finalidad de que tomen las acciones respectivas para mitigarlo. Finalmente, efectúo el análisis correspondiente estableciendo una matriz adecuada asignándole un peso

específico para tomar una decisión basándome en un promedio ponderado para la incorporación de sensores de seguridad al sistema de correlación de eventos.

1.4. Descripción del problema

Hace muchos años el monitoreo de las herramientas de seguridad era de forma individualizada y dificultaba trazar un ruta relacionada de los posibles incidentes que han acontecidos en el transcurso del tiempo, usualmente por tal motivo pasaba desapercibido la denegación de servicio de los principales servicios que ofrece la institución a la comunidad en la zona desmilitarizada como son las páginas de: personal superior y personal subalterno de la Marina de Guerra, admisión a la ESNA (Escuela Naval del Perú) y CITEN (Centro Instituto de Educación Superior Tecnológico Público Naval) y servicio de citas en el CEMENA (Centro Medico Naval) y en el policlínico naval de San Borja.

En el caso del antivirus institucional, bloquea y eliminaba los distintos virus como son los troyanos, spyware's, gusanos, etc. en el cual nos mostraba a que área pertenecía, pero al no estar interconectada con el directorio activo de la institución, la tarea de identificar la dependencia, de la cual provenía la alerta, se volvía engorrosa y a veces imposible de determinar el origen. Otro problema que se identificó fue realizar las actualizaciones o corrección de errores de forma remota, a través del ente técnico encargado, se convirtió en una misión titánica en las dependencias más alejadas de la capital y por las cuales su geografía no lo permitía, por dos motivos: el ancho de banda no era el adecuado y dichas dependencias no contaba con el personal técnico especializado en realizar dichas tareas.

En la Figura 3 se visualizará como es el procedimiento de un ataque sin un SIEM y los pasos que se realizan para que este ataque sea evasivo y efectivo en una arquitectura de seguridad estándar.

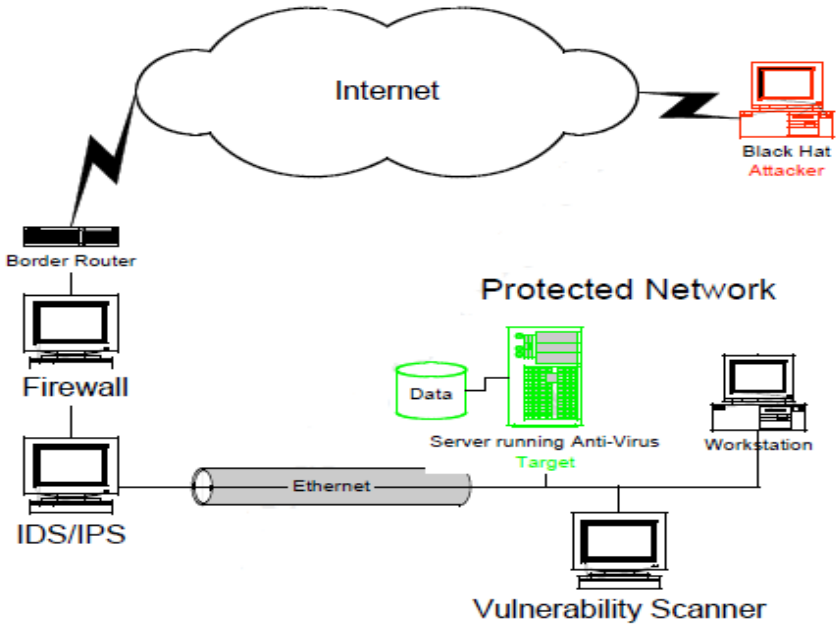

Figura 3 Taxonomía de un ataque informático sin un SIEM
Fuente: Marina de Guerra del Perú

Pasos básicos de un ataque evasivo

- El atacante escanea el firewall utilizando herramientas para escaneo intrusivo de firewalls, para determinar a qué direcciones IP's responde, A qué servicio y cuáles puertos están abiertos, de una forma sigilosa para evitar ser detectado por sistemas de detección/prevención de intrusos.
- Utilizando técnicas de finger printing contra blancos encontrados, para determinar que sistemas operativos se encuentran en los hosts descubiertos, Que aplicaciones están ejecutándose en los hosts.
- Se envían ataques de vulnerabilidades conocidas tales como buffer overflow, paquetes fragmentados (fragroute, nemesis) con patrones de evasión de firmas (admutate, metasploit). Comprometimiento del sistema.

En este punto ya se ha penetrado el sistema operativo y se posee el control de la maquina ocasionando dificultades al usuario y en el peor de los casos robar información sensible.

1.5. Resultados propuestos

Cuando recién se estaba formulando el plan para la implementación de un SIEM se poseía una idea muy superficial de todas las capacidades reales que este aportaba en la

arquitectura de seguridad de cualquier institución. Se pensaba que simplemente centralizaba la información obtenida de los equipos críticos que enviaba la data y se podía intuir de dónde provenía la amenaza y que se podía contrarrestar únicamente generando una alerta para que el analista del sistema de Gestión de Eventos e Información de Seguridad tome una medida correctiva de acuerdo a la severidad.

En la Figura 4, plasmé la idea que teníamos con mi grupo de trabajo del funcionamiento y operatividad del SIEM antes de un estudio a profundidad y describirlo brevemente.

Figura 4 Esquema básico de un SIEM
Fuente: Elaboración propia

- Generación de evento de seguridad: Este provenía de un equipo crítico que presentaba una anomalía, es decir que su funcionamiento no era transparente ni continuo. Un ejemplo básico de esto es que, al introducir un usuario y contraseña equivocada, genera error el cual es enviada al SIEM.
- Generación de una alerta: La información que se obtuvo del error antes mencionado, hace que se disparen las alertas para que el analista correspondiente tome acción pertinente.

- Revisa, analiza y registra: La alerta generada hace que el analista ponga énfasis en el evento que se ha producido. El analista revisa y analiza los motivos por la cual finalmente, toma una decisión de acuerdo a la información recabada, asimismo registra el evento para llevar un control de las posibles intrusiones.
- Atención y notificación: La alerta es enviada a las distintas herramientas de seguridad que se posee para que estas verifiquen el incidente de los equipos críticos.

UNIVERSITAS • STUDIORUM • PIURENSIS

Capítulo 2

Fundamentación del tema elegido

2.1. Problemática a nivel mundial

En este punto hare referencia a los ataques que han tenido mayor relevancia, evidenciando las vulnerabilidades tanto en el factor humano como en las deficiencias en el software.

2.1.1. Ciberataques en las elecciones de Estados Unidos

Los servicios de inteligencia estadounidenses concluyeron que Vladímir Putin, presidente de Rusia, ordenó una campaña de influencia para desprestigiar a Hillary Clinton y ayudar a Donald Trump en las elecciones presidenciales de 2016.

El informe, indica que consistió en hackear a grupos e individuos demócratas y publicar esa información a través de sitios web de terceros para minar el orden democrático liberal que lidera Estados Unidos.

El Gobierno norteamericano atribuye los ciberataques a dos grupos de espionaje ruso. El primero de ellos es el responsable de los ataques realizados en el año 2016, mientras que el segundo operaba desde el verano del año anterior a las elecciones.

La actividad maliciosa, apodada por el gobierno estadounidense como GRIZZLY STEPPE, tenía como objetivo comprometer y explotar las redes y los servidores asociados a las elecciones de Estados Unidos. Todo empezaba en lo que la inteligencia (CIA) describe como espacio adversario, desde el que los piratas informáticos conectaban con la infraestructura de Internet considerada como espacio neutral. Desde estos servidores, los hackers enviaban códigos maliciosos para conectarse con el espacio de la víctima, como eran, por ejemplo, los sistemas informáticos del Partido Demócrata.

Además del código malicioso insertado en la infraestructura informática de sus objetivos, los hackers también enviaron en 2016 una serie de correos electrónicos a

más de 1000 víctimas potenciales. Esos mensajes contenían un enlace a una página creada por los piratas informáticos, que parecía perfectamente legítima y que pedía al usuario que cambiara la contraseña. Una vez dado este acceso, los espías lograban el acceso a las redes que contenían, entre otros, los correos internos del Partido Demócrata y de miembros de la campaña de Hillary Clinton. Esa información era después reenviada a las bases de datos controladas por los hackers a través de "túneles" seguros creados por ellos mismos y difundida en Internet por agentes como Wikileaks o en diferentes páginas web.

Las agencias de inteligencia estadounidenses recomiendan a todos los departamentos que revisen sus sistemas operativos para detectar los puntos de entrada más vulnerables, así como restringir el número de personas que cuentan con las credenciales necesarias para acceder a información sensible. El FBI asegura en su informe que "los atacantes están cada vez más centrados en lograr acceso a las credenciales de las cuentas con mayores privilegios" y recomienda que se reduzcan a los únicos permisos necesarios para realizar el trabajo asignado a cada empleado.

Como se puede apreciar en este caso sobre las elecciones presidenciales, llevadas a cabo en el 2016, tuvieron gran incidencia sobre las preferencias de los electores de Estados Unidos debido a que la excandidata presidencial Hillary Clinton poseía una ventaja importante en las encuestas, sin embargo, perdió las votaciones por el desprestigio llevado a cabo por los ataques perpetrados por hackers rusos.

Una herramienta de seguridad adecuada para mitigar este tipo de ataque, correo malicioso, es el Anti-Spam que en colaboración con un eficaz Anti-Malware correlacionada con un SIEM que centralice la información recolectada para bloquear el malware y no cumpla su propósito.

2.1.2. Stuxnet, el malware más ingenioso de la historia

Probablemente el ataque más famoso fue el malware completo y polifacético que inutilizó las centrifugadoras de enriquecimiento de uranio en Irán, ralentizando varios años el programa nuclear del país. Fue Stuxnet el que incitó que se hablara de las ciberarmas contra los sistemas industriales.

Por aquel entonces, nada podía igualar la complejidad y la astucia del ciberataque Stuxnet, el gusano era capaz de expandirse en oculto a través de memorias

USB y penetrar incluso en ordenadores que no estuvieran conectados a Internet o a una red local.

Según la firma de seguridad cibernética Symantec, Stuxnet probablemente llegó al programa nuclear de Irán en una memoria USB infectada. Alguien habría tenido que insertar físicamente el USB a una computadora conectada a la red. El gusano penetró así en el sistema informático de la planta.

Este gusano sin control se expandió rápidamente por todo el mundo, infectando cientos de miles de ordenadores, pero no podía dañarlos, ya que este malware había sido creado para una tarea muy específica. Se manifestó exclusivamente en ordenadores con controladores programables y software de SIEMENS.

Una vez dentro del sistema informático, Stuxnet buscó el software que controla las máquinas llamadas centrifugadoras. El gusano encontró el software que controla estas y se insertó en ellas, tomando el control de las máquinas. Las centrífugas giran a altas velocidades para separar componentes, para aislar el uranio enriquecido que es fundamental tanto para la energía como para las armas nucleares. Entonces, Stuxnet, reprogramó estos controladores y elevó la velocidad de rotación de las centrifugadoras de enriquecimiento de uranio hasta que las destruyó físicamente.

En este caso se observa como un simple error, de introducir un dispositivo de almacenamiento (USB) ajeno a la central nuclear pudo reproducir un gusano que infecto todo el sistema. Una alternativa de solución al error antes mencionado es brindar políticas de seguridad asignándole autorización específica a un rango de USB’s. Al poseer un sistema de correlación de eventos se pudo identificar inmediatamente en qué lugar de las instalaciones fue introducido la memoria de almacenamiento y bloquear cualquier intento de transferencia de archivos.

2.1.3. WannaCry: Una auténtica epidemia

El ataque WannaCry (Quiero llorar, por su traducción del inglés) dio a conocer el ransomware y el malware en general, incluso para aquellos que no tienen conocimiento de informática.

Usando los exploits del grupo de hackers Equation Group, que fueron publicados por el grupo Shadow Brokers, los atacantes consiguieron crear al monstruo, un ransomware cifrador capaz de expandirse rápidamente por Internet y las redes locales.

En general, WannaCry viene en dos piezas. La primera es un exploit que se encarga de la infección y de la propagación. La segunda se trata de un cifrador que se descarga en un ordenador después de ser infectado.

La primera supone la gran diferencia entre WannaCry y la mayoría de cifradores. Para infectar un ordenador con un cifrador normal, el usuario debe cometer un error, como, por ejemplo, haciendo clic en un enlace sospechoso, permitiendo que Word ejecute macros maliciosas o descargando un adjunto malicioso de un correo electrónico. Un sistema puede ser infectado con WannaCry sin que el usuario haga nada.

Durante 4 días, WannaCry consiguió inutilizar más de 200.000 ordenadores en 150 países, entre ellos infraestructuras críticas. En algunos hospitales, WannaCry cifró todos los dispositivos, incluido el equipo médico, y algunas fábricas se vieron obligadas a detener su producción por culpa de este ransomware. De los ciberataques más recientes, WannaCry es el más trascendental.

En los tres ataques narrados en este capítulo se detecta un factor en común, que es la falta de planificación en la arquitectura de seguridad. Esto se debe a la carencia de sensores relacionados entre sí para la detección oportuna de posibles intentos de intrusión en la red institucional que permita la pronta mitigación de ataques que deterioran y, en el peor de lo casos, neutralizan el sistema por completo, ocasionando grandes pérdidas no solo materiales sino en infraestructura crítica, también.

2.2. Técnicas

Las técnicas que empleé para el desarrollo de la implementación del SIEM y cumplir con las metras propuestas.

- Recopilación de información: Cada integrante del equipo indagó en foros de internet y se realizó consultas a expertos del tema.
- Elaboración de informes: Al término del proyecto realice un informe detallado sobre los resultados obtenidos y los pasos que se realizar para el despliegue del proyecto.
- Trabajo en equipo: Designé las tareas al personal a mi cargo por las capacidades y habilidades de cada uno de ellos.
- Elaboración de diagrama Gantt: A través del juicio de los expertos sobre del tema, pude estimar el tiempo de duración de cada actividad para elaborar un cronograma adecuado.

- Ejecución de tareas programadas

2.3. Cursos de carrera involucrados

A continuación, señalare los cursos de carrera involucrados que me ayudaron en desenvolvimiento y desarrollo de mis actividades.

- Sistema operativo en Linux I y II: Al ser un sistema operativo open source permite una mayor estabilidad en la ejecución de procesos en los servidores.
- Lenguaje de programación Python: Es un lenguaje simple y estructurado que permite la ejecución de los scripts necesarios para el despliegue del software necesario.
- Gestión de proyectos: Identificación de las actividades críticas para el uso adecuado de los recursos
- Arquitectura de redes: Identificar los puntos importantes en la red institucional para determinar el formato de eventos que obtendré.

UNIVERSITAS • STUDIORUM • PIURENSIS

Capítulo 3

Aportes y desarrollo de la experiencia

3.1. Security Information and Event Management (SIEM)

SIEM o Gestión de Eventos e Información de Seguridad (Security Information and Event Management) es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de las redes críticas de su infraestructura, a través de la estandarización de datos y priorización de potencial amenazas. Esto es posible, mediante un análisis centralizado de datos de seguridad, obtenidos desde múltiples sistemas que conforman, incluyendo las siguientes aplicaciones: antivirus, firewall perimetral y soluciones de prevención de intrusiones, firewall de base de datos, anti-DDoS, antimalware.

El software SIEM trabaja con inteligencia artificial para que usted pueda gestionar de forma proactiva las potenciales vulnerabilidades, protegiendo a su organización y a sus componentes de devastadoras filtraciones de datos. Enfoca los esfuerzos de sus analistas hacia donde puedan tener mayor resultado

El término reúne los conceptos de Gestión de Eventos de Seguridad (SEM) con el de Gestión de Información de Seguridad (SIM), para obtener lo mejor de ambos mundos. SEM cubre la monitorización y correlación de eventos en tiempo real, al mismo tiempo que alerta la configuración y vistas de consola relacionadas con esas actividades. Por su parte, SIM lleva estos datos a una siguiente fase que incluye el almacenamiento, análisis y generación de reportes de los resultados.

No es un secreto que las amenazas de seguridad aumentan continuamente, y que pueden provenir tanto de fuentes internas como externas. Una preocupación que crece es la posibilidad de que, accidentalmente, los empleados configuren erróneamente los ajustes de seguridad, dejando los datos vulnerables a un ataque. Para prevenir estos problemas, las

organizaciones de IT han incorporado varios sistemas para protegerse de intrusiones y de una gran cantidad de amenazas diversas.

La desventaja de estos sistemas de protección es que generan tanta información para monitorizar, que los equipos de tecnología de la información se enfrentan al problema de tener que interpretarla en su totalidad para poder reconocer los problemas reales. De hecho, el volumen de datos de seguridad que fluyen hacia los equipos de Seguridad de IT con poco personal, es más que nada inútil, a menos que pueda ser rápidamente analizado y filtrado en alertas procesables. Teniendo en cuenta la cantidad de datos que pueden llegar a ser, para las organizaciones ya no es posible hacer este análisis en forma manual. Es aquí donde aparece el software SIEM.

Con un SIEM, los profesionales de IT cuentan con un método efectivo para automatizar sus procesos y centralizar la gestión de Seguridad de una forma que ayude a simplificar la difícil tarea de proteger información sensible. Un SIEM proporciona a los expertos una ventaja para comprender la diferencia entre una amenaza de bajo riesgo y una que puede ser determinante para su negocio.

Con el concepto ya explicado en los párrafos predecesores, en la Figura 5 se detallará cómo es el procedimiento de un ataque con un SIEM y los pasos que se realizan para que esta ofensiva sea neutralizada con las acciones establecidas en el sistema.

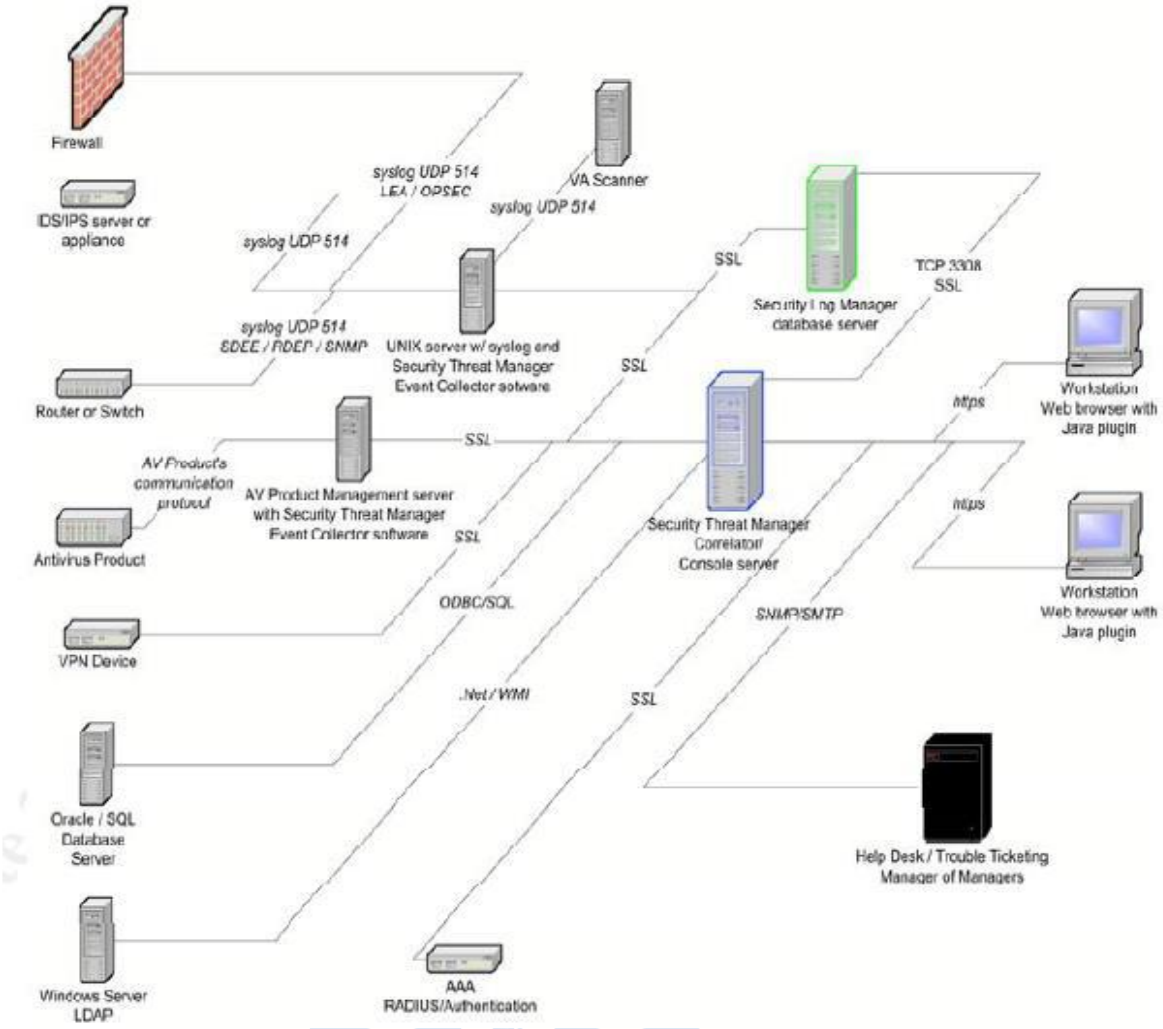

Figura 5 Taxonomía de un ataque informático con un SIEM

- Las herramientas de seguridad envían los eventos al SIEM, indicando que se está realizando una petición de conexión y/o un escaneo de puertos, ésta genera una alerta menor o de advertencia.
- El sensor que se encuentra en primer nivel, reporta el tipo de consulta, si este ataque es conocido, la alerta es elevada a un nivel superior y el equipo de seguridad es notificado.
- Finalmente, se generan las respuestas automáticas escritas con anterioridad como son los casos de uso, bloqueo de las direcciones IP, agregar el dominio a la lista negra, etc.

3.2. Planificación de requerimientos

La Marina de Guerra del Perú designó un comité técnico encargado de investigar, comparar, determinar y decidir las características necesarias para adquirir los servidores con las capacidades necesarias de hardware y software para un despliegue eficiente en rendimiento.

Al comienzo asumí el cargo con un poco de dudas por la falta de experiencia, sin embargo, a medida que iba profundizando en el tema tanto en lo práctico como teórico tuve la certeza de que estaba tomando un proyecto que iba a dar grandes satisfacciones para la institución y para mí en lo profesional. A continuación, mostraré el listado de preguntas que se necesitó para desarrollar el proyecto y posteriormente las actividades realizadas con mayor detalle para el despliegue del SIEM.

- Cantidad de tiempo que almacenaré los eventos
- En donde almacenaré los eventos, en la nube o locamente
- Cantidad de herramientas de seguridad y equipos críticos que realizarán el envío de eventos para determinar los EPS (Eventos por segundo)
- Determinar características del procesador, memoria RAM y la cantidad de almacenamiento en discos duros necesarios para obtener una buena performance en el procesamiento de los eventos.
- Determinar el tipo de configuración de RAID en discos con la finalidad de garantizar la alta disponibilidad del sistema.
- Formato de eventos que obtendré (SYSLOG, CEF, JSON, etc)
- Contar con el personal adecuado para el despliegue
- Determinar qué sistema operativo en relación al beneficio que este nos brinda
- Determinar qué servicios estarán almacenados en que servidor

Una vez definidos los requerimientos y la adquisición de los mismos, se procede a la fase del despliegue.

3.3. Despliegue de servicios

Esta etapa es la más importante y crucial porque si se realiza un comando erróneo o no se siguen en orden los pasos, determinar el error por omisión o equivocación, es una tarea muy complicada de realizar. A continuación, describiré las actividades realizadas.

Paso 1. Instalación del sistema operativo en todos los servidores, CentOs en Linux: Estuve encargado de la descarga de un repositorio en la nube e instalación en los servidores adquiridos, el cual fue el pilar fundamental para que los servicios sean utilizados. Cabe resaltar, que esta actividad fue de prueba y error porque las versiones más recientes no son estables tampoco el performance es el adecuado, es por ello, que se realizaron pruebas hasta encontrar el óptimo.

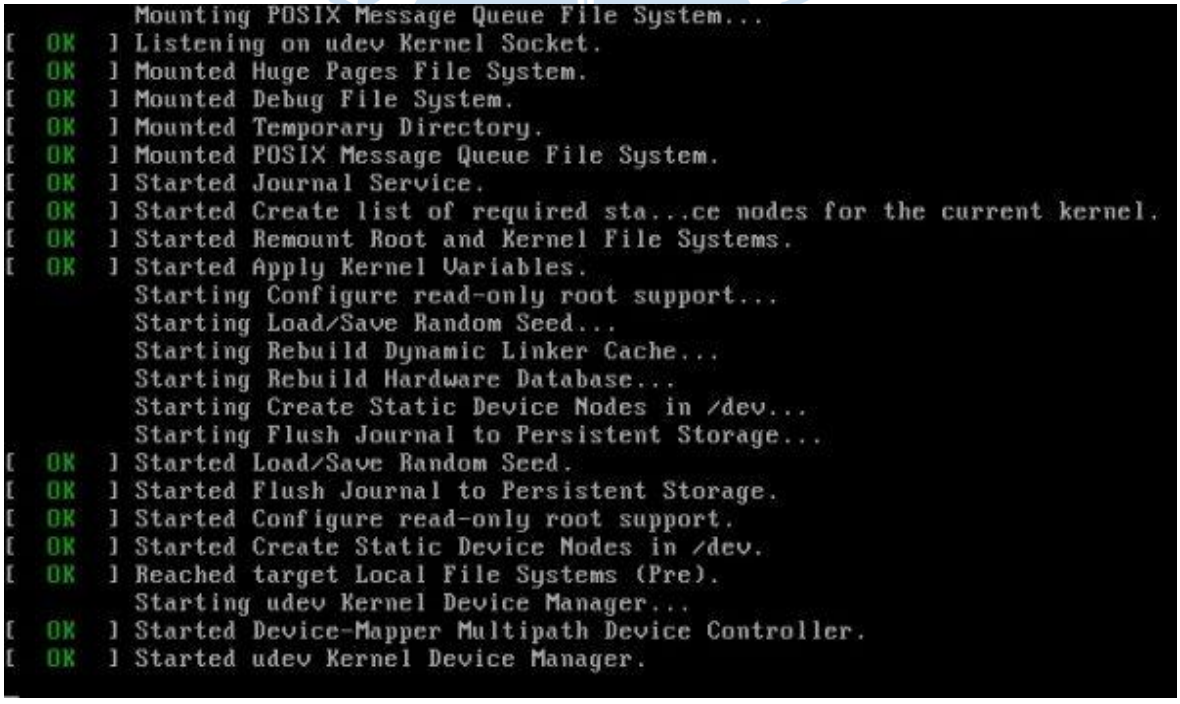

Figura 6 Instalación del sistema operativo CentOs

Paso 2. Instalación de las actualizaciones: En esta actividad estuve encargado de monitorear la descarga de las actualizaciones del sistema operativo seleccionado. Así mismo sugerí la instalación de herramientas como htop, tcpdump con la finalidad de realizar pruebas unitarias

```
---> Paquete httpd.x86_64 0:2.4.6-67.el7.centos.6 debe ser una actualización
--> Procesando dependencias: httpd-tools = 2.4.6-67.el7.centos.6 para el paquete
: httpd-2.4.6-67.el7.centos.6.x86_64
--> Ejecutando prueba de transacción
---> Paquete httpd-tools.x86_64 0:2.4.6-45.el7.centos.4 debe ser actualizado
---> Paquete httpd-tools.x86_64 0:2.4.6-67.el7.centos.6 debe ser una actualizaci
ón
--> Resolución de dependencias finalizada

Dependencias resueltas

================================================================================
 Package           Arquitectura Versión                     Repositorio   Tamaño
================================================================================
Actualizando:
 httpd             x86_64       2.4.6-67.el7.centos.6       updates       2.7 M
Actualizando para las dependencias:
 httpd-tools       x86_64       2.4.6-67.el7.centos.6       updates        88 k

Resumen de la transacción
================================================================================
Actualizar  1 Paquete (+1 Paquete dependiente)

Tamaño total de la descarga: 2.8 M
Is this ok [y/d/N]: _
```

Figura 7 Línea de comando para las actualizaciones

Paso 3. Instalación y configuración del servicio de Ambari: Una vez obtenido el agente de Ambari, procedí a la configuración del entorno gráfico mediante el cual se realiza la verificación del estado de salud de los servicios más importantes.

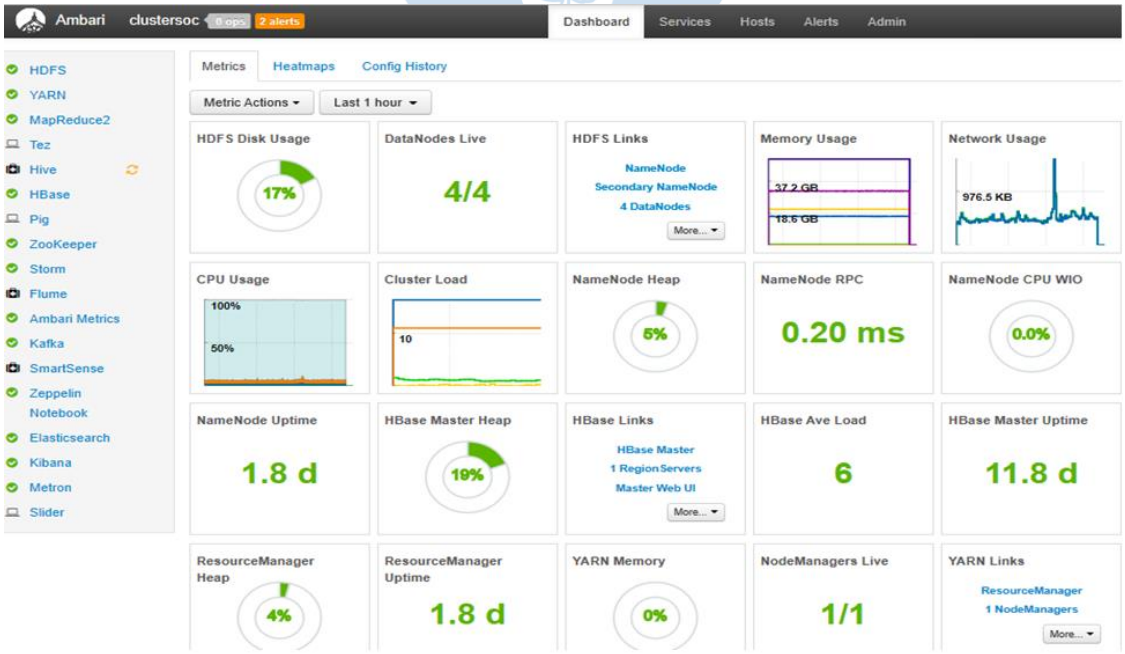

Figura 8 Entorno gráfico Ambari

Paso 4. Integración de las herramientas de seguridad: Programé una reunión con las empresas que proveen las distintas herramientas de seguridad: Anti-Malware, Anti-Virus, Firewall, IPS, etc. A raíz de los input's de las empresas pude conocer y establecer las bases para la creación de los parsers que más adelante explicaré.

Paso 5. Integración de los equipos críticos: Me conecté en forma remota con la autorización de los encargados para realizar la instalación del agente necesario para el envío de los eventos hacia el SIEM. Analizando los datos de los servidores, determiné que el formato en la cual se envía la información es JSON, es decir que no se necesitará realizar el parser.

Paso 6. Creación de parsers en Java: En conjunto con mi equipo de trabajo y utilizando la herramienta online freeformatter.com/java-regex-tester, se realizó los parsers en Java que es de suma importancia para recibir los eventos de las herramientas de seguridad para agregar este al servidor correspondiente para realizar la compilación de los mismos.

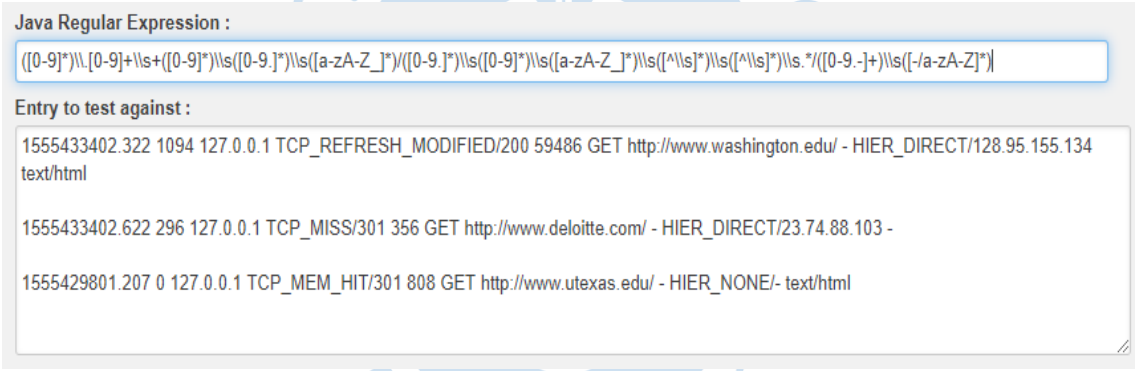

Figura 9 Creación de parsers en Java con freeformatter

```
public class KSquid extends BasicParser {
  private static final Charset UTF_8 = Charset.forName("UTF-8");
  private Pattern p;

  public void init()
  {
    String myRegex = "([0-9]*)\\.[0-9]+\\s+([0-9]*)\\s([0-9.]*)\\s([a-zA-Z_]*)/([0-9.]*)\\s([0-9]*)\\s([a-zA-Z_]*)\\s([^\\s]*)\\s([^\\s]*)\\s.*/([0-9.-]+)\
\s([-/a-zA-Z]*)";
    StringBuilder sb = new StringBuilder("");
    sb.append(myRegex);

    String pattern = sb.toString();
    p = Pattern.compile(pattern);
  }

  @SuppressWarnings("unchecked")
  public List<JSONObject> parse(byte[] rawMessage)
  {
    Matcher matcher;
    List<JSONObject> messages = new ArrayList<>();
    boolean parsed = false;

    String syslogString = new String(rawMessage, UTF_8);
    syslogString = syslogString.replace("\n","");
    matcher = p.matcher(syslogString);

    //if the log entry matches the regex
    if (matcher.matches())
    {
      parsed = true;
      JSONObject obj = new JSONObject();
      System.out.println("\n[PARSER]NEW MATCH!");

      obj.put("elapsed", matcher.group(2));
      obj.put("ip_src_addr", matcher.group(3));
      obj.put("code", matcher.group(4));
      obj.put("status", matcher.group(5));
      obj.put("bytes", matcher.group(6));
```

Figura 10 Integración del parser en el servidor

Paso 7. Creación de dashboard para la visualización grafica de los datos: Realicé la creación y el diseño de los dashboard de cada herramienta de seguridad para extraer los datos de mayor relevancia. Esta acción es el equivalente a un resumen ejecutivo para observar de manera gráfica los datos por el comandante de Ciberdefensa.

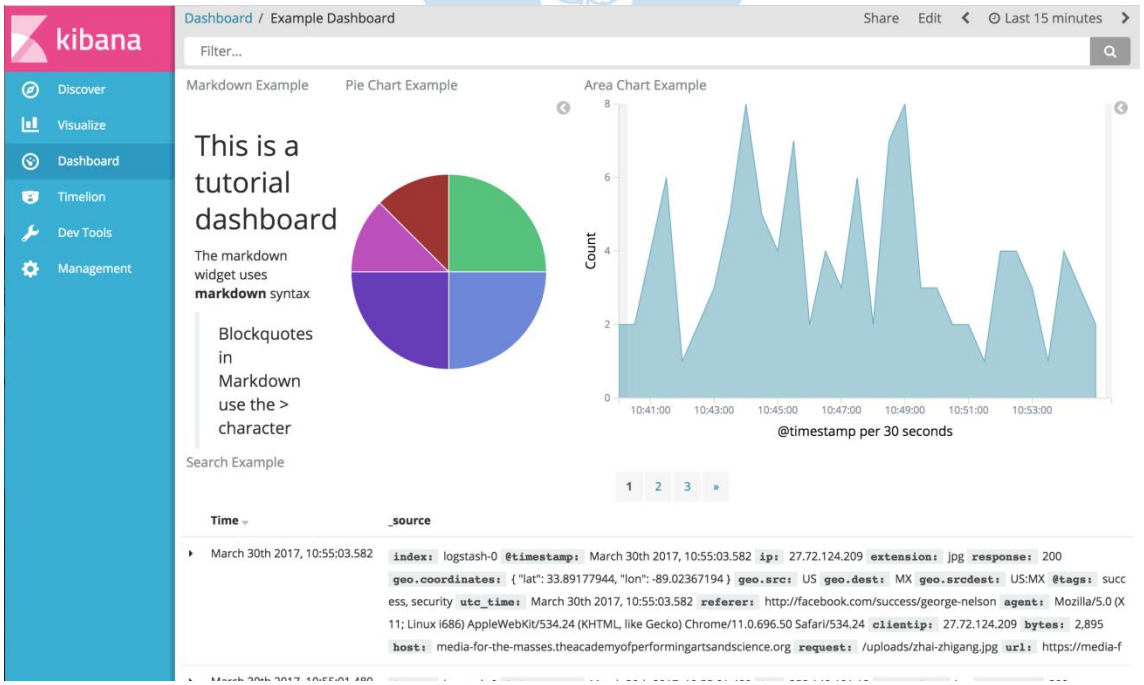

Figura 11 Creación de dashboard

Con estos requerimientos definidos y actividades realizados se pudo efectuar el informe final en cuanto a la documentación hacia el comando respectivo y el despliegue del sistema de Gestión de Eventos e Información de Seguridad para la Marina de Guerra del Perú que servirá para correlacionar los eventos de las distintas herramientas de seguridad que lo alimentan para la detección temprana de incidentes y tomar las medidas correctivas necesarias.

UNIVERSITAS • STUDIORUM • PIURENSIS

Conclusiones

Las amenazas de hoy en día representan una gran vulnerabilidad en la infraestructura de red de cualquier institución siendo innegable el uso de una herramienta que permita correlacionar los eventos y enriquecer los eventos a través de su software.

El SIEM permite acoplar los logs de diferentes herramientas de seguridad de manera segura y correlacionarlos extrayendo información trascendente que podría pasar desapercibida si se examinan los distintos orígenes de información por separado.

Respecto al desempeño del sistema mencionado en el presente trabajo, ha detectado un 27% adicional de potenciales ataques especificando el contexto de la amenaza en la arquitectura de red.

El SIEM permitió mitigar a través de la correlación de eventos de las herramientas de seguridad un 52% más de eventos que monitorear los eventos por sensores de manera independiente.

Bajo hasta un 13% la identificación de los eventos catalogados como falsos positivos permitiéndonos optimizar los recursos horas-hombre de la Comandancia de Ciberdefensa.

El personal del Comando de Ciberdefensa de la Marina de Guerra del Perú se encuentra a la vanguardia de las capacidades de tecnología de la información resguardando la información crítica por un sistema capaz de reaccionar ante las amenazas.

UNIVERSITAS • STUDIORUM • PIURENSIS

Recomendaciones

Capacitar al personal de la Comandancia de Ciberdefensa constantemente en las nuevas tecnologías en seguridad de la información para un desempeño superior en la realización de sus actividades.

Actualizar la capacidad de procesamiento y almacenamiento de los servidores adquiridos para minimizar el tope límite de eventos por segundo (EPS) capaz de soportar el SIEM.

Informarse sobre las capacidades de las herramientas de seguridad utilizando como referencia el cuadrante de Gartner, conociendo sus capacidades, ventajas y desventajas de cada uno.

Replicar el SIEM en toda institución tanto pública y privada que desee proteger la información crítica de su infraestructura centralizando la información para el análisis respectivo.

UNIVERSITAS • STUDIORUM • PIURENSIS

Bibliografía

¿Qué es un SIEM? (2019). Recuperado el junio de 2019, de Help Systems: https://www.helpsystems.com/es/blog/que-es-un-siem

Marvin. (2014). *El origen de Stuxnet*. Recuperado el junio de 2019, de Kaspersky: https://www.kaspersky.es/blog/el-origen-de-stuxnet/4887/

Organigrama, misión y vision. (2018). Recuperado el junio de 2019, de Marina de Guerra del Perú: https://www.marina.mil.pe/es/nosotros/acerca-de/

Pereda, C. (2016). *Así se produjo el ciberataque ruso en la campaña electoral de EE.UU. según el FBI*. Recuperado el junio de 2019, de El país: https://elpais.com/internacional/2016/12/30/estados_unidos/1483119060_863004.html

Perekalin, A. (2017). *¿Estás a salvo?* Recuperado el junio de 2019, de Kaspersky: https://www.kaspersky.es/blog/wannacry-ransomware/10503/

UNIVERSITAS • STUDIORUM • PIURENSIS

Anexos

Anexo 1 Diagrama de Gantt de actividades para el despliegue del SIEM

N°	ACTIVIDADES	ENERO				FEBRERO				MARZO				ABRIL				MAYO			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	DETERMINACIÓN DE REQUERIMIENTOS EN BASE A REUNIONES DEL COMITÉ TÉCNICO	X	X																		
2	ADQUISICIÓN DE HARDWARE Y FIRMWARE			X																	
3	INSTALACIÓN Y PUESTA EN SERVICIO DEL SIEM (UNICAMENTE HARWARE Y FIRWARE)				X																
4	INSTALACIÓN DE LOS SISTEMAS OPERATIVOS EN LOS SERVIDORES (CENTOS)					X															
5	INSTALACIÓN DE ACTUALIZACIONES						X														
6	INSTALACIÓN Y CONFIGURACIÓN DEL AMBARI							X	X												
7	INTEGRACIÓN DE HERRAMIENTAS DE SEGURIDAD									X	X	X									
8	INTEGRACIÓN DE SERVIDORES CRÍTICOS												X	X							
9	CREACIÓN DE PARSERS CON JAVA														X	X					
10	CREACIÓN DE DASHBOARDS																X	X			
11	USO DE KIBANA																		X		
12	OPERACIÓN DEL SIEM Y SENSORES DE SEGURIDAD																			X	X

Anexo 2 Glosario

Ambari:

Es una infraestructura abierta para suministro, gestión y supervisión de servidores que integran el SIEM. Desde esta interfaz web se puede visualizar el estado de los nodos y servicios del SIEM.

Evento de seguridad:

Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de los controles o una situación desconocida hasta el momento y que puede ser relevante para la seguridad. (UNE-ISO/IEC 27000:2014)

Gusano:

Programa desarrollado que permite copiarse y propagarse mediante mecanismos de red.

IDS:

Sistema de detección de intrusos (Intrusion Prevention System, por sus siglas en ingles). Previene la intrusión de los atacantes.

JSON:

Java script object notation. Formato de texto ligero para intercambiar datos.

Kibana:

Es una plataforma de análisis y visualización de código abierto diseñada para trabajar con la base de datos. Se utiliza para buscar, ver e interactuar con los datos almacenados en los índices de la base de datos. Puede realizar fácilmente análisis de datos avanzados y visualizar sus datos en una variedad de tablas y mapas.

Log:

Es un registro de los eventos que suceden en los sistemas de la organización.

Malware:

Programa malicioso que tiene como objetivo dañar el sistema.

Spam:

Correo electrónico con publicidad no deseada.

Troyano:

Código malicioso escondido en un programa inofensivo que brinda acceso directo instalando una puerta trasera.

Vulnerabilidad:

Deficiencia del sistema que puede ser aprovechada por el atacante.