FACULTAD DE INGENIERÍAS Y CIENCIAS AGROPECUARIAS

ANALISIS E IMPLEMENTACION DE UN SISTEMA DE CIBERDEFENSA VIRTUAL PARA DATACENTER ACADEMICO DE LA UNIVERSIDAD DE LAS AMERICAS.

Profesor guía

MSc. William Villegas

Autor

Santiago Andrés Medranda Morejón

Año

2017

DECLARACIÓN PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, 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”.

_____

William Eduardo Villegas Chiliquinga

Magister en Redes de Comunicaciones

C.I. 1715338263

DECLARACIÓN PROFESOR CORRECTOR

“Declaro haber revisado este trabajo dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Luis Santiago Criollo Caizaguano

Máster en Redes de Comunicaciones

C.I. 1717112955

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

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

_____

Santiago Andrés Medranda Morejón

C.I. 1722247572

AGRADECIMIENTOS

Gracias a todas las personas que estuvieron durante el desarrollo de este largo proceso, en el que pude sentir su incondicional apoyo y ánimos para culminar de la mejor manera esta faceta.

DEDICATORIA

A mis padres por su amor, trabajo y apoyo en todos estos años de estudio. A mi hermana por ser una ayuda dentro de mi formación y en mi diario vivir. A mi familia en general le doy las gracias por impulsarme a seguir adelante y no rendirme nunca. Gracias por ser mi guía y ejemplo a seguir.

RESUMEN

En la actualidad, los sistemas de datos a nivel mundial son la plataforma que mueve al mundo en áreas como finanzas, tecnología, compras, ventas e incluso en el hogar de una familia. La interconexión que brinda la internet permite la comunicación entre personas sin distinguir fronteras o distancias. A la par de este esfuerzo por crear una conexión general que provea de contenidos a cada ser humano en el mundo se han ido presentando problemas de seguridades y vulnerabilidades en sistemas cuyos ataques dejan millones en recompensas para las empresas y personas que se dedican a realizar esta actividad ilegal sin mencionar un lugar de importancia en el mundo de la ciberseguridad y un logro más a las filas del cibercrimen.

En un esfuerzo global por evitar el robo de información y por la protección de las infraestructuras tecnológicas, las empresas buscan de manera desesperada un sistema que permita mitigar las amenazas de atacantes y combatirlas de la manera más eficaz evitando que estos ataques se propaguen por redes locales empresariales afectando a toda la corporación y no solo a un par de individuos.

El presente trabajo de titulación tiene como objetivo analizar y encontrar las herramientas y complementos que permitan que una infraestructura de red empresarial cuente con una protección ante amenazas internas y externas al tiempo de alinear esta implementación a las normativas internacionales vigentes, consolidando de esta manera una arquitectura de red con diversos niveles de protección evitando que el usuario final tenga un riesgo mínimo de recepción de virus.

La seguridad empresarial en materia informática es un pilar fundamental a la hora de considerar su aseguramiento y políticas de divulgación puesto que el contar con una solución multiplataforma evita en un caso hipotético tener un acceso no autorizado al core del negocio y por ende a información flexible que en las manos incorrectas podría afectar los planes de la empresa a largo plazo.

Palabras clave: ciberseguridad, *BYOD*, ISP, Redes, Seguridad

ABSTRACT

Currently, data systems world-wide platform are moving the world in the areas of finance, technology, shopping, sales and even in the home of a family. The interconnection provided by the Internet allows communication between people without distinction of borders or distances. At the same time this effort to create a connection in general that to test the contents of human being in the world have been presented security problems and vulnerabilities in systems. The attacks leave millions in rewards for the companies and people who dedicate to perform this illegal activity with a place in the world of cybersecurity and a further achievement in the ranks of cybercrime.

In a global effort to prevent information theft and protection of technological infrastructures, companies desperately seek a system that allows them to mitigate threats from attackers and combat them in the most effective tool, preventing these attacks from spreading over local networks Affecting the entire corporation and not just a couple of individuals.

The present work aims to analyze and find the tools and complements that allow the corporate network infrastructure have a protection against internal and external threats while aligning this implementation to the current international regulations, thus consolidating an architecture of network with different levels of protection that prevent to user about risks of receiving viruses.

Business security in information technology is a fundamental point when considering its assurance and disclosure policies with the multiplatform solution prevents in a hypothetical case having unauthorized access to the core of the business and therefore flexible information that In the wrong hands affecting the plans of the company a long term.

Keywords: cyber security, *BYOD*, ISP, Networks, Security

ÍNDICE

Introducción 1

Alcance 2

Justificación 3

Objetivos 4

Objetivo General 4

Objetivos Específicos 4

1. Capítulo I. Marco Teórico 5

1.1 Ciberespacio 5

1.2 Ciberguerreros 6

1.3 Ataque Informático 6

1.3.1 Reconocimiento (Reconnaissance) 7
1.3.2 Exploración (Scanning) 7
1.3.3 Obtener Acceso (Gaining Access) 8
1.3.4 Mantener el acceso (Maintaining Access) 8
1.3.5 Borrar huellas (Covering Tracks) 8

Ataques Informáticos 9

1.4 DDoS 9

1.5 Botnets 9

1.6 Zeus 10

1.7 Ransomware 10

1.8 Middleware 10

Parámetros de garantía de funcionamiento y disponibilidad de red 11

1.9 Seguridad 11

1.9.1 Autenticación 11
1.9.2 Confidencialidad 11
1.9.3 Integridad 11
1.9.4 Disponibilidad 12

1.9.5 Política de Seguridad 12
Normativa 12
1.10 ISO 27000 12
1.11 SGSI 13
1.12 ISO 27002 15
Herramientas de Supervisión 15
1.13 SIEM (Security Information and Event Management) 15
1.14 OSSIM 16
1.15 HYPERIC HQ 17
1.16 SECURIA 17
1.17 IP HOST 17
1.18 Net IQ 18
2. Capítulo II. Requerimientos de Escenario y Elección de Herramienta 18
2.1 Esquematización de la red de datos 18
2.1.1. Monitoreo de funciones de transmisión de red 20
2.1.2. Monitoreo de funciones de sistemas 21
2.1.3. Análisis de Heurística, Data Minining y Correlación 23
2.1.4. Identificación de equipamiento 24
2.1.5. Elección de la herramienta 25
2.2 Definición de OSSIM 26
2.2.1 Características 28
2.2.2 Ventajas 28
2.2.3 Desventajas 29
2.2.4 Compatibilidad 30
2.3 Componentes y Arquitectura 31
2.3.1 OSSIM Server 31
2.3.2 OSSIM Framework 32
2.3.3 Agente OSSIM 34
2.3.4 Arquitectura OSSIM 36
2.3.5 Diagrama de Arquitectura 37
2.4 Tipos de Monitoreo 38
2.4.1 Arpwatch 38

2.4.2 PADS 39
2.4.3 OpenVas 39
2.4.4 Spade 40
2.4.5 TCPTrack 40
2.4.6 NTop 40
2.4.7 NfSen 41
2.4.8 NfDump 41
2.4.9 Osiris 42
2.5 Costo 43
3. Capítulo III. Implementación del Sistema de Ciberdefensa 44
3.1 Requerimientos de hardware y software 44
3.2 Guía de Implementación 47
4. Capítulo IV. Fase de Pruebas y Verificación de la Solución 65
5. Conclusiones y Recomendaciones 81
5.1 Conclusiones 81
5.2 Recomendaciones 83
Referencias 85
Anexos 89

Introducción

Los datos a nivel mundial sobre encuestas y estudios en el ámbito informático arrojan cada día reportes de crecimiento exponencial en el uso de internet y por ende el acceso a esta plataforma global desde poblaciones que hace algún tiempo tan solo soñaban con tener un enlace al mundo mediante esta red.

Los proveedores de servicio, cada vez más robustos, establecen sus proyecciones de crecimiento en infraestructura y capacidad en base a los abonados, que en la actualidad no cuentan con un solo dispositivo en sus hogares, sino redes que comprenden smartphones, computadores e incluso electrodomésticos.

La pregunta concreta es ¿En que afecta a los usuarios el crecimiento del acceso a Internet?, Los usuarios domésticos y empresariales cambian sus preferencias de acceso a Internet de acuerdo a las nuevas tendencias del mercado, esto incluye para usuarios locales grandes capacidades de transmisión de datos principalmente para video y descargas desde la web y por otro lado para empresas que cuentan cada vez con mayores enlaces y equipos más robustos que permitan una convergencia de datos a fin de entregar a los usuarios diferentes tipos de servicios con el menor retraso posible y la mejor calidad, al mismo tiempo que en sus centros de datos y oficinas locales se mantenga una red robusta.

Concretamente en el caso empresarial, cada año se evalúan las necesidades de infraestructura tecnológica que esta pueda tener, a fin de adquirir servidores robustos con sistemas operativos multiplataforma capaces de soportar este flujo de datos y entregar al usuario (interno o externo) la información al tiempo requerido o incluso soluciones en la nube que evitan desechar recursos después del período de vida para el que fueron adquiridos, prolongando así la inversión en áreas de TI dentro de la empresa. Sin embargo, al crecer la cantidad de equipos de este tipo de redes también crece la complejidad en su administración, que pese a estar centralizada y monitoreada constantemente, es víctima de

ataques informáticos realizados por hackers y delincuentes informáticos, que encuentran un modo de ingresar a estas infraestructuras y atacarlas a fin de suspender los servicios que estas brindan.

En la actualidad la seguridad informática ha adquirido gran importancia, dadas las cambiantes formas de comunicación, la posibilidad de conectarse remotamente a infraestructuras empresariales así como también la interacción natural de usuarios con servicios centralizados en las empresas muestra cada día la importancia de contar con una herramienta de visualización del funcionamiento de las redes y verificar las actividades que un usuario o un posible atacante esté realizando en los equipos que procesan estas solicitudes.

El apartado de seguridad informática necesita una herramienta que permita gestionar la toma de decisiones para mitigar ataques a servidores críticos dentro de la organización, así como también restringir el paso de atacantes a servicios críticos para lo cual al interno de las empresas muchas veces se aplican normas ISO 27000 y sus apartados relacionados con seguridad de la información.

Las actividades que los oficiales de información puedan establecer para controlar ataques o vulnerabilidades deviene de un conjunto de herramientas que para el análisis de este documento se unifican en la solución llamada OSSIM.

Alcance

La investigación del proyecto se realizará basado en información de manuales, tesis doctorales, y artículos científicos indexados. Su diseño e implementación se desglosa en 3 etapas:

La primera etapa contará con la esquematización y reconocimiento de la infraestructura física del Datacenter Académico de la Universidad de las Américas, que durante los procesos de investigación e implementación se modificará en sus configuraciones a fin de receptar los sensores y configuración del servidor de seguridad de manera óptima.

La segunda etapa contará con el despliegue de una solución virtualizada que contará con una distribución de la solución OSSIM para la implementación en los equipos a fin de realizar el monitoreo de vulnerabilidades y tráfico en tiempo real, utilizando sensores virtuales de acuerdo al sistema operativo.

La fase 3 denominada como “despliegue beta”, presentará la solución OSSIM en su interfaz web configurados todos los sensores y contando con la información consolidada de vulnerabilidades mostrando estadísticas de riesgo y describiendo cada fallo a fin de ser corregido para la puesta a punto y salida a producción de la solución.

Para validar el óptimo desempeño de la solución, se realizará ataques internos y externos a la infraestructura supervisada con OSSIM que se encuentra en el Datacenter Académico de la Universidad de las Américas.

Justificación

Un ataque informático puede llegar a perjudicar severamente la infraestructura tecnológica de una empresa que en general actualmente es considerada crítica para el negocio. Como resultado surge la necesidad de conocer y llevar una estadística de los posibles ataques y vulnerabilidades de los sistemas.

Por esta razón se requiere de una solución como OSSIM, equipada con una serie de sensores que facilitan información compacta fácil de interpretar y con la cual se puede tomar una decisión sobre el mejor camino para anular amenazas informáticas.

El proyecto será un aporte a la Universidad de las Américas, contribuyendo con información técnica y un despliegue de la solución a fin de que se pueda tomar como referencia para futuras implementaciones de proyectos similares, la información que este documento contiene.

Objetivos

Objetivo General

- Establecer un sistema de ciberdefensa adjunto a la infraestructura del datacenter académico de la Universidad de las Américas en sus enlaces internos como externos a fin de mitigar la mayoría de ataques informáticos que puedan provenir de miembros internos como externos a la red.

Objetivos Específicos

- Proveer de una herramienta virtual de control de tráfico que permita identificar los posibles ataques a la red.
- Establecer un esquema de ciberdefensa basado en las políticas vigentes sobre seguridad de la información derivadas del estándar ISO 27000.
- Permitir a los estudiantes de las carreras de Ingeniería en Sistemas como de Ingeniería Electrónica y Redes, así como también Ingeniería en Redes y Telecomunicaciones observar diferentes tipos de ataques a una infraestructura de red y los procesos que se utiliza en general para evitar que los atacantes logren su cometido.
- Demostrar la aplicación de herramientas de mitigación de ciberataques de manera virtual evitando el adquirir equipos físicos adicionales, evitando un costo excesivo en herramientas que controlen estos aspectos vulnerables de las redes.

1. Capítulo I. Marco Teórico

Teoría General

1.1 Ciberespacio

La Unión Internacional de Telecomunicaciones (UIT) define al ciberespacio como "ciberentorno" y menciona que "La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos, quiere decir amenazas, de seguridad correspondientes en el ciberentorno." (UIT, s.f.).

El ciberespacio lo conforman todas las redes informáticas del mundo y todo lo que ellas conectan y controlan. No se trata solo de internet. Es importante dejar en claro la diferencia. Internet es una red de redes abierta. Desde cualquier red de internet, se puede establecer comunicación con cualquier ordenador conectado con cualquiera otra de las redes de internet. El ciberespacio es Internet más millones de otras redes de ordenadores a las que, se supone, no es posible acceder desde internet. Algunas de esas redes privadas son muy semejantes a internet, pero, al menos teóricamente, se encuentran separadas de ella (Clarke y Knake, 2011, p. 104).

Tomando en cuenta los conceptos antes descritos se puede concluir que el ciberespacio es la puerta de entrada a la información global que se almacena en inmensos centros de datos convirtiéndose en la ventana para que cada ser humano pueda acceder a diversos tipos de contenidos. Internet por tanto se convierte en el canal de comunicación que dentro del ciberespacio es generador de sesiones a todos los usuarios que buscan datos en este "mundo virtual".

Tras el análisis del ciberespacio en su conjunto y sus niveles de afectación se identifican dos grandes grupos de ataque, por un lado existen aquellos de alta intensidad cuyo objetivo es la estructura del estado central de un país y por tanto los equipamientos militares e infraestructuras críticas que los soportan; por otro

lado y haciendo hincapié en el ciudadano de común se tiene el ataque de baja intensidad pero en sí más perjudicial a la población civil ya que se tratan de estafas, robo de identidad, ataques a páginas web e información bancaria incluyendo diversos tipos de transacciones electrónicas.

1.2 Ciberguerreros

Los ciberguerreros son personas que con su conocimiento técnico informático se dedican a diseñar, construir e implementar programas, códigos o esquemas capaces de determinar el mejor camino para infiltrar un sistema ya sea este de una organización o entidad o como también de usuarios comunes para secuestro de información sensible y la futura amenaza de pago para liberar estos datos. Sin embargo, este tipo de ataques son la punta del iceberg debido a que su profundidad en ámbitos empresariales no tiene un final concreto; para eliminar la huella de ataque un intruso entendido en materia de infraestructura podría colocar bombas lógicas para encubrir su ataque e incluso mediante este tipo de intromisión vulnerar sistemas críticos como redes eléctricas o sistemas telefónicos. (Morelli A., sf, p. 2)

Los tipos de atacantes se clasifican en (Caro M., 2011, p. 72):

- Atacantes patrocinados por estados
- Servicios de inteligencia y contrainteligencia
- Terrorismo, extremismo político e ideológico
- Ataques de delincuencia organizada
- Ataques de perfil bajo

Generalidadea de los Ataques Informáticos

1.3 Ataque Informático

Un ataque informático es cuando se aprovecha de alguna falla o debilidad en un producto de hardware o software, o incluso, en las personas que forman parte de una red privada de información a fin de obtener datos privados que generen

un beneficio de carácter económico, de esta manera se causa un perjuicio que repercute directamente en los activos de la empresa y genera un efecto negativo en la seguridad informática de la misma. En la siguiente ilustración (Figura 1), se muestra los pasos para un ataque bajo un esquema piramidal, empezando por la fase de reconocimiento, y finalizando con la eliminación de nexos con el atacante. (Mieres J., 2009, p. 5)

Figura 1. Proceso típico de ataque informático.
Tomado de Mieres, J. 2009

1.3.1 Reconocimiento (Reconnaissance)

Es la fase inicial del ataque en donde se recopila la información pública de la posible víctima ya sea esta una persona u organización. (Mieres J., 2009, p. 5)

1.3.2 Exploración (Scanning)

En esta etapa el atacante usa la información consolidada en la fase previa a fin de obtener datos sobre los sistemas e infraestructura de la víctima, dentro de estos datos pueden estar direcciones IP, nombres de hosts, datos de autenticación como credenciales VPN, administrador local o Active Directory, entre otros.

En esta fase el atacante ya empieza a usar herramientas propias de la industria para la exploración de estos datos como network mappers, port mappers, network scanners, port scanners, y por último vulnerability scanners. (Mieres J., 2009, p. 5)

1.3.3 Obtener Acceso (Gaining Access)

En esta fase intermedia empieza a generarse el ataque, ya que el atacante empieza a explorar vulnerabilidades y defectos en el sistema en base a la información del apartado de exploración.

Por lo general se utilizan técnica de Buffer Overflow, DoS, DDoS, Password Filtering, y Session hijacking; herramientas que se corren desde computadores de la misma red local, dificultando así la detección de dispositivos periféricos orientados a las conexiones entrantes desde internet. (Mieres J., 2009, p. 6)

1.3.4 Mantener el acceso (Maintaining Access)

Una vez obtenido el acceso del atacante a la red o los hosts es necesario implantar herramientas que permitan controlar la máquina en el futuro desde cualquier lugar, para este tipo de máquinas secuestradas, comúnmente se usan backdoors, rootkits, y troyanos, que permitan agregar a los hosts a bootnets. (Mieres J., 2009, p. 6)

1.3.5 Borrar huellas (Covering Tracks)

Una vez alcanzado el objetivo de la víctima en un solo host o incluso en una red secuestrada, el atacante tratará de disminuir al máximo los indicios que apunten a su ubicación, evitando ser rastreado. Para esto se utilizan herramientas para borrar registros (logs), o incluso evitar alarmas de sistemas y registros en sistemas de detección de intrusos (IDS). (Mieres J., 2009, p. 6)

Ataques Informáticos

1.4 DDoS

Los ataques del tipo DDoS (Distributed Denial of Service) son los más comunes a sitios web, su procedimiento es simple ya que el principal fin que tienen este tipo de amenazas son saturar servidores web de una institución y con ellos posibles aplicaciones que estén siendo ejecutadas en este entorno haciendo imposible el funcionamiento en el corto plazo posterior al ataque de estos dispositivos, para este fin se utilizan computadoras que se encuentren infectadas por virus (botnets) haciendo posible el crear una red paralela de equipos infectados; el sigilo es una herramienta primordial en ataques de DDoS, es por ello que los usuarios infectados nunca tienen conocimiento o indicio de formar parte de la amenaza. (Mirkovic, J., 2002, p.10)

1.5 Botnets

Los botnets o robots en red vienen a constituir un conglomerado de equipos de computación utilizados para dirigir ataques de diferente impacto, principalmente aquellos de tipo DDoS. El ordenador o dispositivo se convierte en parte de la botnet al momento de que el usuario promedio abre un correo basura o Spam, dicho correo electrónico esta previamente cargado por un virus imperceptible a simple vista. Tras la infección la máquina atacada queda a disposición del atacante que a distancia puede ejecutar comandos y comprometer el funcionamiento normal de ese equipo u otros en la red. Este tipo de ataque es utilizado con el fin de espiar corporaciones e instituciones gubernamentales (Joyanes, 2011).

1.6 Zeus

Zeus es el término asociado al conjunto de virus comunes, su distribución ha sabido evolucionar de manera exponencial a lo largo de tiempo; conocido también como troyano este se encarga de ingresar a las computadoras de los usuarios con el fin de obtener sus contraseñas de servicios bancarios, redes sociales, correo electrónico e incluso en algunos casos de intranets de una empresa, los datos obtenidos en estas exploraciones sirven para elaborar planes de suplantación o simplemente ejecutar robos de cuentas bancarias. (So-In, C., Mongkonchai, N., Aimtongkham, P., Wijitsopon, K., & Rujirakul, K., 2014, p90-94)

1.7 Ransomware

Acrónimo de “software de rescate”, genera un comportamiento totalmente opuesto, concretamente un Ransomware es un programa informático que secuestra la información de un ordenador; documentos confidenciales, software crítico o incluso bases de datos son muchos de los datos que al ser encriptados son imposibles de recuperar a menos que el usuario tenga el hash de autenticación que permita des-encriptar la misma. Los primeros intentos de ransomware surgieron en 2013, lo más alarmante en este tipo de ataque es que pese a su corta duración en el medio ya ha encontrado más réditos que cualquiera de los 3 tipos antes descritos. Es el único de todos los ataques que solicita recompensa instantánea y cuyo pago de ser efectuado tiene dos maneras de procesarse, la primera por tarjeta de crédito o depósito en una cuenta determinada y la segunda por bitcoins, lo cual prácticamente deja sin restricción o excusa de pago. (O'Gorman, G., & McDonald, G, 2012, sp)

1.8 Middleware

El término middleware hace referencia a un módulo conductor de sistemas, programas y redes, permitiendo al usuario final acceder a la información

almacenada en diversas fuentes dentro de la LAN o VPN; en sí middleware tiene el objeto concreto de conectar varios tipos de productos sin necesidad de que coincidan los proveedores, esto permite una flexibilidad de implementación y adquisición de equipos manteniendo siempre una interconexión supervisada. (Bernstein,P.A, 1996, sp)

Parámetros de garantía de funcionamiento y disponibilidad de red

1.9 Seguridad

En los sistemas de información y comunicación, se entiende por seguridad al conjunto de funciones, servicios y métodos que permitan garantizar los siguientes postulados

1.9.1 Autenticación

Se define como la capacidad de reconocer la veracidad de cierta información de dominio o identidad de usuarios del sistema, así también valida las autorizaciones de acceso a servicios, en este apartado se verifican permisos de cada usuario.

1.9.2 Confidencialidad

Establece la condición primaria de restricción a la información, asegurando que los datos no se encuentren disponibles o puedan ser ubicados por personal o aplicaciones no autorizadas.

1.9.3 Integridad

La integridad se define como la regla que dentro de la red o en un sistema garantiza la modificación, eliminación o generación de información únicamente al personal autorizado, adicionalmente evita la alteración de información de forma accidental o fraudulenta.

1.9.4 Disponibilidad

Se define como el tiempo medible en el cual una herramienta se encuentra disponible para un usuario autorizado, sin embargo, es necesario considerar un intervalo considerable de tiempo para su medición debido a que en muestras cortas no se identifica un error de conexión recurrente. Adicionalmente se asocia con la tasa de fallos en varios componentes del sistema, por lo general esta tasa genera reportes mensuales sobre un porcentaje definido. Por último, ante el aspecto de seguridad, se asocia la disponibilidad con recuperación en caso de desastre (Recuperabilidad).

1.9.5 Política de Seguridad

Una política de seguridad, es una declaración explícita, legal y formal, del compendio de normas a las cuales se alinea cualquier usuario al que se le conceda el acceso a la infraestructura tecnológica de la organización por cualquier medio.

El objetivo principal de estas políticas es informar y concientizar a los usuarios sobre la protección de los datos contenidos en los activos de una red de datos dentro de la organización. De igual manera es un manual efectivo en el cual establecer el punto de partida para una auditoría informática, verificando el cumplimiento de estos postulados.

Normativa

1.10 ISO 27000

Establecida su primera publicación el 1 de Mayo de 2009, y con una segunda y tercera revisión en 2012 y 2014 respectivamente, es la nomenclatura que la ISO (International Organization for Standardization) brinda a la normativa general de Sistemas de Gestión de Seguridad de la Información (SGSI), dentro de su apartado encontramos diferentes derivaciones, que juntas generan un compendio de pasos para la implementación de procesos que crean, mantienen

y monitorean a un SGSI, si bien es cierto el estándar fue creado como marco de referencia se debe considerar aplicarlo conforme el requerimiento del negocio con su derivación pertinente, ya que incluso muestra maneras de control físico y accesos a datos en sitio; estos apartados no son parte del análisis de este documento pero se define a esta normativa en su totalidad para futuras referencias. (Disterer, G., 2013)

1.11 SGSI

El SGSI, es el término asignado a un sistema integro de control de la información; con el creciente índice de amenazas empresariales, se debe buscar la manera de mitigar cualquier tipo de ataque externo, pero aún bajo esta consideración es importante aplicar la normativa a los usuarios empresariales internos, facilitando así un control de la migración de información entre comunidades y departamentos de la organización, y detectando posibles errores o fugas de información. (Alemán-Novoa, H. C. I., 2015)

En la figura a continuación (Figura 2), se visualiza los 4 pilares que son la base de la creación de controles de un sistema de gestión de seguridad de la información (SGSI) aplicado a una infraestructura de red, sistema, equipo o arquitectura óptima en la rama de IT.

Figura 2. Aspectos que cubre un SGSI.

Si bien es cierto las herramientas de control técnico de una amenaza tanto interna como externa son robustas y aportan en gran mayoría al control de cualquier tipo de ataque, es necesario que cada usuario dentro de la red empresarial concientice los posibles problemas que la red puede sufrir al ser víctima de ataques por medio de SPAM, PHISHING, o cualquier otro tipo de ataque en el que la información pueda ser comprometida y raptada por el lado del atacante.

En la Figura 3, se observa un diagrama con los objetivos de cada elemento perteneciente a un SGSI, tomando como punto de convergencia el riesgo o la amenaza generada por la mala aplicación de estos puntos.

Figura 3. Diagrama de objetivos SGSI
Tomado de ISO27000.es, s.f.

1.12 ISO 27002

Esta normativa partió en sus orígenes bajo el acrónimo de 17799:2005, siendo 2005 el año de su edición. En sus páginas alberga un sinnúmero de recomendaciones sobre buenas prácticas de seguridad de la información y a la par muestra ejemplos de controles que se pueden implementar para verificar estos puntos en cualquier empresa. (Disterer, G., 2013)

Herramientas de Supervisión

1.13 SIEM (Security Information and Event Management)

El concepto SIEM comprende la fusión de dos campos de seguridad de redes primordiales en la toma de decisiones sobre incidentes e intrusiones a las redes de datos, bajo la combinación de security information management (SIM) y security event management (SEM), se recopila datos relevantes sobre el estado de cada uno de los dispositivos en red. Bajo estos conceptos unificados se determina el mejor camino para evitar o combatir una amenaza en su inicio. Cabe

destacar que SIM y SEM son un concepto de manejo de información de seguridades en redes de datos, por lo que su aplicación en diferentes soluciones de software viene dada por el fabricante de la solución y la finalidad concreta de la misma. (ÁNGEL, A., & GALO, J., 2016)

El diagrama del concepto SIEM expuesto en la Figura 4, indica la agrupación de 3 grandes etapas de su núcleo, el manejo de la seguridad de la información, el tratamiento de eventos del mismo tipo y finalmente el apartado del registro o logs, que se genera al realizar una acción dentro del sistema.

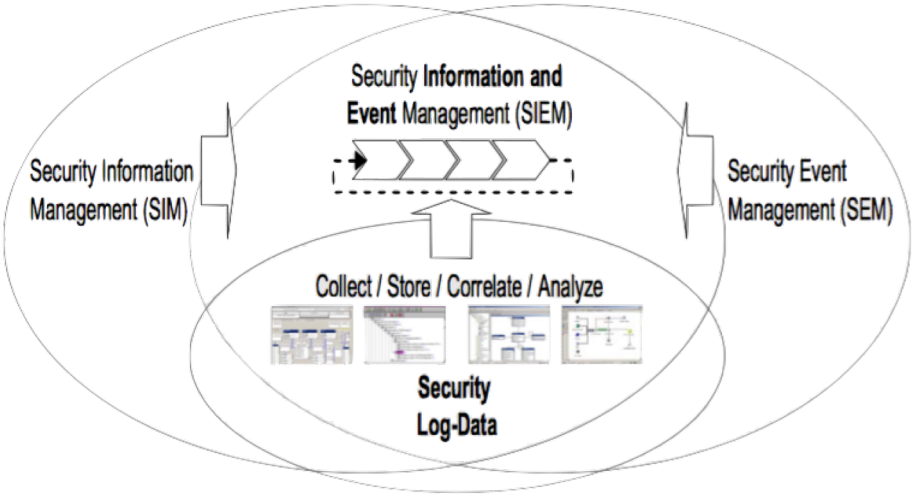


Figura 4. Diagrama de concepto SIEM
Tomado de Gabriel, R., Hoppe, T., Pastwa, A., & Sowa, S. 2009

1.14 OSSIM

Conjunto de herramientas de licencia GPL que recopilan datos correlacionados del tráfico circulante en la red, y mediante el análisis de esta información brindan pistas sobre posibles ataques de seguridad al mismo tiempo que identifican vulnerabilidades comunes de los sistemas. (ÁNGEL, A., & GALO, J., 2016)

1.15 HYPERIC HQ

HYPERIC HQ actualmente es un software de la empresa VMWare considerado como un add-on para las plataformas más robustas como VSphere; entre las funcionalidades de este potente motor de análisis de datos está el monitoreo de aplicaciones y sistemas informáticos, donde se incluyen sistemas operativos de implementación en entornos datacenter. Adicionalmente cuenta con la posibilidad de administrar ciertas aplicaciones o entornos virtuales, de ahí la idea de VMWare de agregar el software a la suite de VSphere. Está herramienta es indispensable a la hora de controlar el rendimiento de los sistemas al ejecutar aplicaciones de alto rendimiento críticas y de alta convergencia. Su plataforma está desarrollada en Java. (Pantaleone, F. M., & Silva, M. N., 2012)

1.16 SECURIA

SECURIA SGSI, es una herramienta completa que supervisa el despliegue de la norma ISO 27001 en la red local cubriendo aspectos como:

- Mantenimiento de equipos
- Funcionamiento de seguridades
- Mejora continua y planes a largo plazo
- Auditorías de Gestión de Seguridad de la Información

Mediante una plataforma de licencia GNU cuenta con desarrollo tanto para plataformas Linux como Windows.

Actualmente el código de esta plataforma se encuentra libre y existen diversos grupos independientes que han adaptado la solución a sus requerimientos específicos, sin embargo, cabe destacar que el desarrollo base de la plataforma se realizó por la empresa SECURIA IDN (España). (Pantaleone, F. M., & Silva, M. N., 2012)

1.17 IP HOST

Anteriormente conocido como RSI, IP Host es un monitor de red y servidores; de manera adicional brinda servicios de monitoreo de intranet web, aplicaciones,

correo empresarial y bases de datos de los proveedores más reconocidos (Oracle, MySQL, Ms SQL). IP Host es pagado y su período de prueba dura 30 días sin pago alguno, es importante destacar que todos los servicios que brinda están soportados bajo la plataforma SNMP, es decir que los dispositivos incluidos en este software deben contar con soporte de SNMP para ser supervisados.

1.18 Net IQ

Net IQ es una solución de monitoreo por concepto SIEM, que permite establecer un control de registro y huellas de atacantes posterior a un evento de este tipo, si bien es cierto es una solución que cubre diferentes aspectos de seguridad, monitoreo, y administración de una red, cada una de estas funcionalidades es pagada y se instala a partir de una plataforma base creada por MICRO FOCUS. Se considera una de las mejores herramientas de auditoría de red y la más rápida de su clase; su funcionalidad más destacada es el monitoreo en tiempo real de inconsistencias de red a nivel de capa 2 y capa 3, sin embargo, su desarrollo es limitado en el nivel de aplicación (capa 7). (Pantaleone, F. M., & Silva, M. N., 2012)

2. Capítulo II. Requerimientos de Escenario y Elección de Herramienta

2.1 Esquematización de la red de datos

Para que la solución de seguridad a elegir se adapte al entorno del negocio y no interfiera con el tráfico regular dentro de la red de datos es necesario establecer un escenario que brinde las pautas de implementación y despliegue de la herramienta, para este requerimiento previo es necesario tener en cuenta algunos parámetros estándar de tráfico y tipos de equipamiento con el que se cuenta dentro del negocio.

En la figura 5, se muestra un esquema tipo de red en la cual se implementa la solución de seguridad de ataques hacia la red empresarial, a simple vista se

observa una topología de red de una sola sucursal, pero con varios enlaces con distintos medios de transmisión. Para una mayor claridad ver Anexo 1.

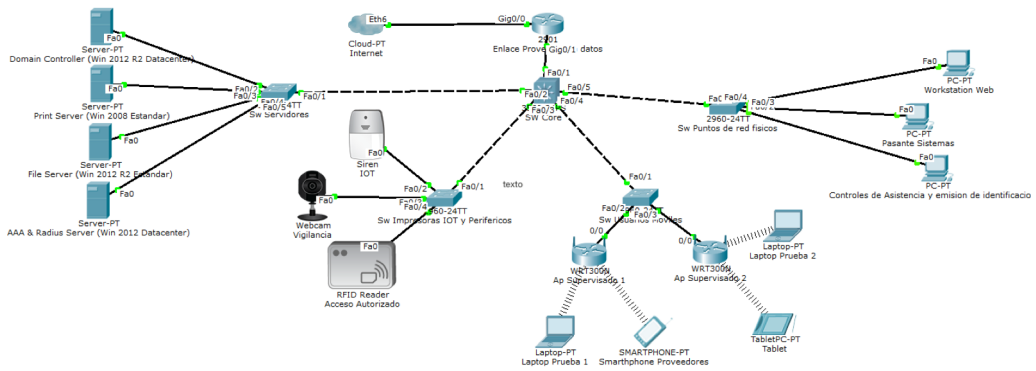


Figura 5. Diagrama de concepto SIEM

Tras analizar el escenario propuesto es necesario tomar ciertas consideraciones para establecer el diseño adecuado para la red de monitoreo de ataques. Como se observa en la figura 5, existen diversos equipos de red y servidores interconectados, sin embargo, muchas veces la conexión de estos dispositivos no solo es por medio de cable de datos sino también por wifi, en este apartado en concreto, es necesario determinar la fidelidad de la conexión y la tasa de transmisión de bits, puesto que en este caso, el monitoreo constante del sensor puede llegar a saturar el canal de transmisión, privando al usuario del uso de otros servicios dentro de la WLan.

Es necesario determinar de acuerdo al tipo de dispositivo y al sensor que características se pueden monitorear del equipo, estás se especifican de acuerdo a los siguientes puntos.

2.1.1. Monitoreo de funciones de transmisión de red

Los equipos de red que se encuentran supervisados por el sistema y sensores de la herramienta a elegir deben contar con parámetros básicos de monitoreo, un ejemplo de este requerimiento es la función de ping, este comando permite establecer una relación sobre el equipo supervisado y el sistema que detecta al sensor como disponible para monitorear otros campos, incluso si el equipo no tuviera un sensor SNMP, la función de ping al dispositivo da una pauta básica de su estado.

Posteriormente a establecer un canal de comunicación por cable o inalámbrico es necesario contar con funciones extra que ayuden a determinar valores adicionales de cada equipo, estos parámetros no solo muestran el funcionamiento del mismo sino también en caso de ataque estos datos ayudan a visualizar el tipo de tráfico circulante y las posibles vulnerabilidades. Por tanto, en el apartado de protocolos SNMP, el sensor puede llegar a recolectar información de la velocidad de transmisión, latencia en el canal, estado de saturación, tipo de paquetes circulantes (Voz, Datos, Video), tipo de enrutamiento (IPv4, IPv6), estos campos generan una correlación con informes anteriores del sistema comparando así tráfico inusual y que no necesariamente llega a ser un ataque a la red.

En la figura 6, se observa en base al protocolo, los diferentes parámetros que se obtienen partiendo de un sensor bajo comunidades SNMP. Es aconsejable en este apartado contar con el software de supervisión compatible con SNMP y múltiples comunidades debido a que esta es la forma para diferenciar sucursales y encontrar de manera más rápida el problema dentro de la red de datos concentrándose en la parte del negocio afectada

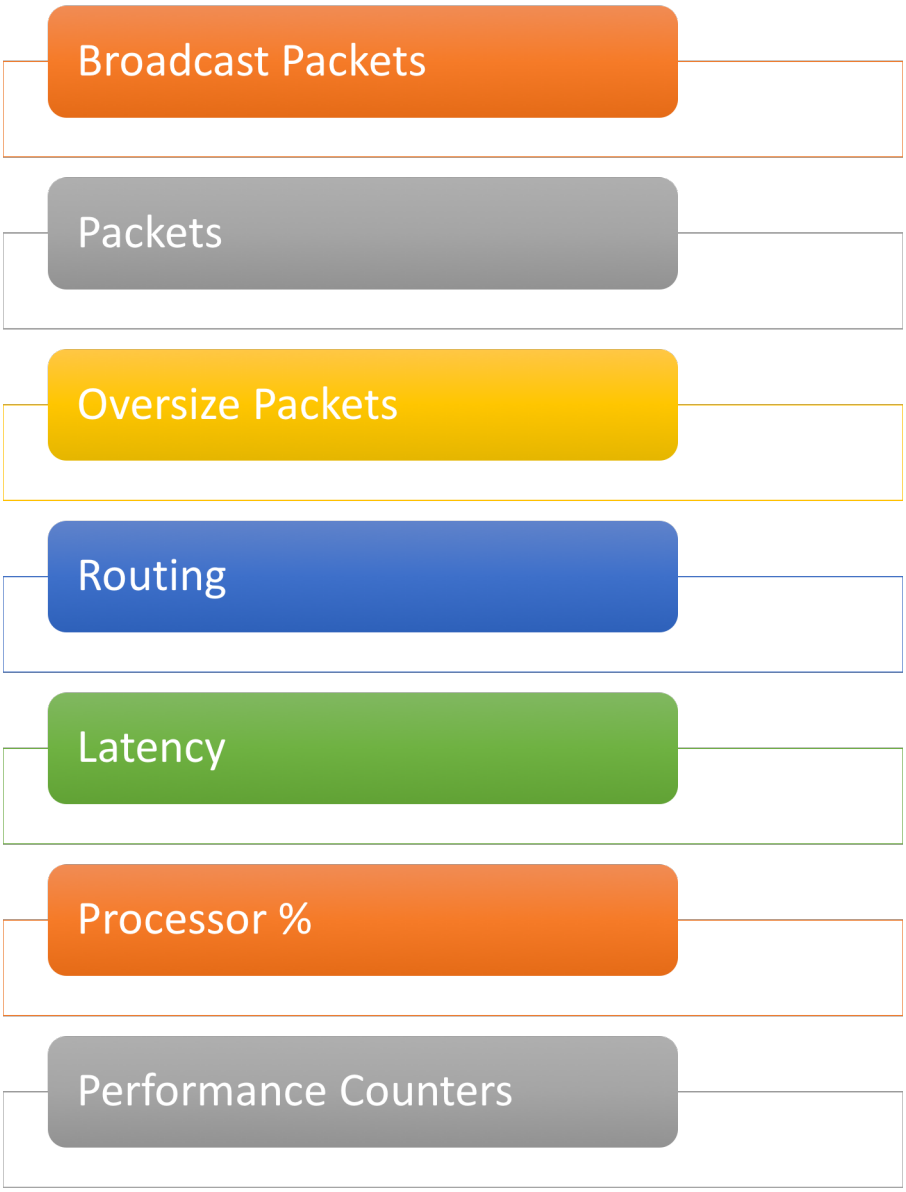


Figura 6. Parámetros SNMP

2.1.2. Monitoreo de funciones de sistemas

Los sensores SNMP fueron diseñados originalmente con capacidades de monitoreo de red, sin embargo, en la actualidad contienen sentencias para el control del equipo en su núcleo y funciones de procesamiento; similar a un sistema scada, el sensor toma valores de lectura de componentes del sistema como su nivel de procesamiento, su temperatura de funcionamiento, el espacio

de almacenamiento, entre otros. El analizar los parámetros de hardware de cada equipo permite determinar si el ataque es físico, o si se lo realiza por software, mediante estas lecturas precisas y en tiempo real, el supervisor del sistema de seguridad empresarial puede determinar si el nodo se desconectó o si está sufriendo un ataque desde algún punto interno o punto virtual (VPN) como se analiza en el punto anterior.

En la figura 7, se observa los datos frecuentes recopilados por un sensor SNMP, de esta manera no solo se supervisan los ataques de penetración de red, sino que adicionalmente se obtiene datos sobre la salud general del equipo.

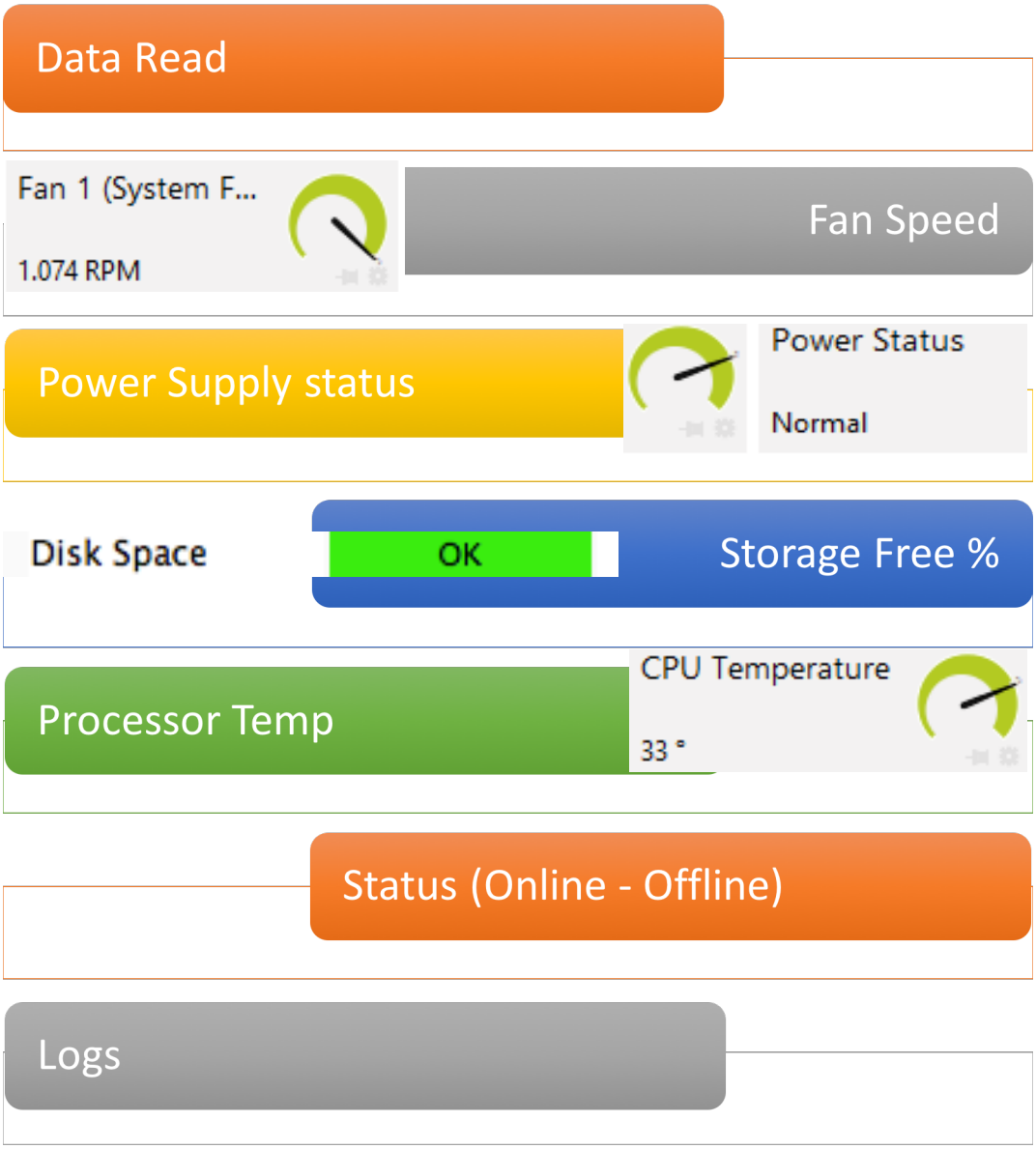


Figura 7. Parámetros Sistemas

2.1.3. Análisis de Heurística, Data Minining y Correlación

Cuando se habla de sistemas de antivirus el término heurística toma importancia debido a su inteligencia automatizada. La heurística dentro de sistemas informáticos se relaciona a la creación de algoritmos óptimos de procesamiento de datos, pero adicionalmente a este apartado, se relaciona a la inteligencia artificial y la capacidad de un sistema de en base a la información recopilada

empezar a conocer el comportamiento de un equipo para que de esta manera se pueda determinar de manera más ágil cualquier anomalía o variación no considerada.

La Heurística aprende datos de la red pero necesita almacenar la información para analizarla incluso meses después de que se haya generado, por tanto los sistemas de seguridad perimetral deben contar con el apartado de data mining, mediante esta función grandes almacenes de datos guardan la información generada de cada uno de los sensores, creando una bitácora organizada para su posterior consulta; el apartado de almacenamiento de información en los sistemas de seguridad empresarial actualmente cuenta con un concepto de big data y empresas como Alien Vault cuentan con una comunidad global que intercambia esta información a fin de replicar cualquier amenaza a cualquier sistema que use su plataforma, por tanto el entorno empresarial está siempre consiente de los riesgos y de posibles ataques con diferente comportamiento en cada equipo de la red de datos.

Como último punto existe la correlación entre datos generados y toda la información almacenada y aprendida por el sistema de seguridad, en este punto debe existir generación de informes de primera mano sobre cualquier tipo de comportamiento fuera de los parámetros definidos, de igual manera es importante considerar que no cualquier tipo de comportamiento fuera de lo común se convierte en un ataque, puede que exista alguna concurrencia de usuarios por un motivo específico, sin embargo el sistema y sus reglas configuradas deben contar con la capacidad de supervisar y entregar estos informes bajo las condiciones descritas anteriormente.

2.1.4. Identificación de equipamiento

Para recolectar información útil al sistema de seguridad informática, es necesario contar con una plataforma robusta de supervisión que permita identificar cada equipo con sus características tanto de hardware como de software, como se encuentra descrito anteriormente el sistema debe ser autónomo en su

aprendizaje sobre el hardware de un sensor supervisado, sin embargo, en el apartado de software es necesario definir estos parámetros:

- Distribución de Sistema Operativo
- Descripción de funcionalidad del equipo
- Localización
- Administradores autorizados a su acceso
- Definición de la comunidad SNMP a la cual pertenece

Estos datos son indispensables para determinar la criticidad de la amenaza a la cual se somete un sistema, e incluso algunas compañías de software de seguridad informática cuentan con funciones desarrolladas para discriminar cierto volumen de tráfico como una congestión de red y no como un ataque, destacando así la importancia de identificar adecuadamente cada sistema y su entorno de funcionamiento.

2.1.5. Elección de la herramienta

Analizando los puntos anteriores y tomando en cuenta la relación de la presente investigación con normas de seguridad de la información (ISO 27000), se procede al análisis y posterior implementación de la herramienta de seguridad de la información basado en SIEM y SNMP conocida como OSSIM, en base a los requerimientos necesarios se determina como la solución de seguridad específica para este escenario propuesto y las normativas aplicadas al compararlo con otras herramientas del mercado y su ventaja al contar con una versión gratuita y pagada que difieren en aspectos mínimos. A continuación, se explica la herramienta, su funcionamiento y la comparativa con otras herramientas del mercado demostrando su confiabilidad.

Las 22 herramientas embebidas en esta solución permiten mantener el control eficaz de una red, al tiempo de contar con previsiones futuras a fin de mitigar algunos tipos de ataques.

A continuación (Tabla 1), se presenta una comparativa que justifica el uso de OSSIM para la presente investigación, y en donde se compara a este sistema con soluciones gratuitas y pagadas que constan de capacidades similares.

Tabla 1.

Comparación de OSSIM con otro Software

	OSSIM	Hyperic HQ	Securia SGSI	IP HOST	NET IQ
Tipo de Licencia	Gratuita (Freeware)	Gratuita (Freeware)	Gratis / Pagada	Pagada	Pagada
Exploración de Redes	✓	X	✓	✓	✓
Detección de Intrusos	✓	✓	✓	✓	✓
Detección de Vulnerabilidades	✓	X	✓	X	X
Monitorización de Equipos	✓	✓	X	✓	✓
Complementos Gratuitos (Plugins)	✓	✓	✓	X	X
Notificaciones Automáticas	✓	✓	X	✓	✓
IDS para la Red	✓	X	X	X	X
GUI Web	✓	✓	✓	X	X

2.2 Definición de OSSIM

La herramienta de la empresa AlienVault llamada OSSIM, lleva su nombre debido a las siglas de Open Source Security Information Management; OSSIM no es una sola herramienta, en el mundo informático es considerada una suite que comprende diversos aplicativos y complementos que unificados realizan tareas de análisis, visualización y gestión de redes en forma centralizada a un solo servidor supervisor de toda la red. De esta manera el software permite una rápida detección de amenazas, así como también permite analizar las vulnerabilidades de equipos anteriores o posteriores a su despliegue.

Aplicando las normativas ISO27000 y sus controles en OSSIM, se observa que la herramienta responde con el mismo efecto a situaciones comunes como

bloqueo de usuarios y logs, como también ataques complejos a toda una infraestructura empresarial.

En su programación cuenta con 22 funcionalidades que por su naturaleza open source, pueden interactuar y generar informes de cada uno de los sensores en conjunto manteniendo al administrador de la infraestructura al tanto de sucesos imprevistos en la red.

En la figura 8 se observa la agrupación de las plataformas, correlación de datos y posterior generación de alarmas del sistema.

La colección de datos permite en esta plataforma correlacionar parámetros antiguos y por medio de la herramienta de supervisión web, es decir el cuadro de mandos se envía la alarma a los administradores del sistema, dependiendo del ataque y de a configuración establecida, esta alarma viene adjunta a un informe del estado del sistema.

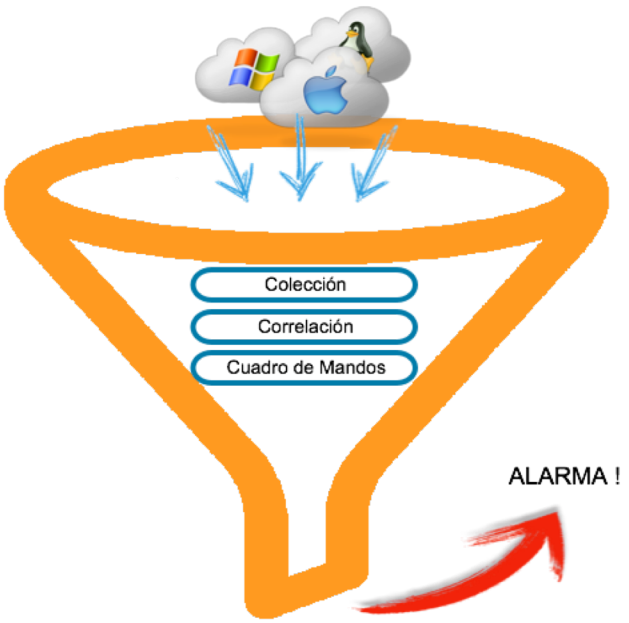


Figura 8. Modelo de OSSIM

2.2.1 Características

OSSIM agrupa un conjunto de útiles funcionalidades para centralizar el control de servidores, red de datos y voz, por tanto, al adquirir una solución de este tipo tenemos:

- Gratuidad (Licencia Open Source).
- Supervisión centralizada a la red.
- Análisis de comportamiento de la infraestructura.
- Informes técnicos sintetizados.
- Evaluación de posibles riesgos actuales y futuros.
- Alarmas sobre anomalías en red.
- Control sobre ataques o intrusiones al sistema.
- Alarmas sobre tráfico inusual.
- Interfaz web amigable al usuario administrador.
- Informes y logs de cualquier sistema operativo (Windows o Linux).
- Implementación semi-automática en Windows.
- Tests de vulnerabilidades.
- Notificaciones automáticas vía correo electrónico.
- Biblioteca con plugins gratuitos disponible.
- Notificaciones catalogadas en subclases.

2.2.2 Ventajas

La principal ventaja de OSSIM radica en el entorno en el cual se presenta la información, al ser centralizado y permitir al usuario acceder en un GUI web, se observa la versatilidad de acceso que puede tener el sistema desde cualquier lugar, no solo dentro de la empresa, en empresas con un núcleo de negocio basado en la infraestructura de TI, el monitoreo constante por parte del oficial de seguridad se vuelve crítico, por tanto una solución que permita generar planes de mejora constante a la red, así como también mitigar cualquier ataque agrega un factor de confiabilidad sobre la estructura implementada.

Los 22 componentes de OSSIM establecen su comportamiento en función de:

- **Correlación**

Reúne todos los eventos y registros generados en la red, de esta manera permite visualizar esta información en una sola pantalla indistintamente de la plataforma que maneje el hardware. Mediante este procesamiento, OSSIM permite organizar la data en función de su prioridad, otorgando niveles bajo, medio o alto dependiendo del tipo de tráfico que se observa.

- **Evaluación de amenaza**

Este proceso brinda al oficial encargado del sistema la posibilidad de evaluar el riesgo en función de la información arrojada por OSSIM, en este punto la clasificación de registros juega un papel trascendente, puesto que permite encontrar el punto más crítico de un supuesto ataque. Para realizar esta tarea OSSIM realiza 4 pasos.

- Costo para la red (performance).
- Verificación de amenaza comparando con su base de datos.
- Alerta a personal de seguridad informática.
- Notificaciones por correo electrónico si se estuviera desconectado del sistema principal de OSSIM.

2.2.3 Desventajas

Como se muestra en la Tabla 1, OSSIM no carece de funciones para un control general de la red, pese a esto es necesario reconocer las limitaciones de OSSIM al actuar como herramienta para bloqueo inmediato de cualquier ataque; se considera a OSSIM un software de recopilación de registros y amenazas como complemento a herramientas de mitigación y control de tráfico (IPS, IDS).

Adicionalmente es necesario conocer que cada complemento de OSSIM dificulta su administración puesto que agrega más funcionalidades y carga al S.O, por tanto, si se encuentra en proceso de pruebas de la herramienta en una infraestructura es mejor mantener la imagen base hasta que exista un dominio considerable sobre la herramienta que permita manejar estos complementos orientándolos únicamente hacia los equipos que lo requieran.

2.2.4 Compatibilidad

La solución de seguridad OSSIM está desarrollada en código debían, si bien es cierto anteriormente era utilizada como un complemento de Linux en todas sus versiones, actualmente maneja su propia imagen, de cierta manera esto permite virtualizar totalmente su plataforma al tiempo que consigue una independencia de cualquier otro sistema operativo, evitando así un ataque al host anfitrión y por ende al complemento OSSIM.

Su arquitectura es x32 o x64, sin embargo, el fabricante recomienda equipos que cuenten con capacidades para datacenter, debido a que el despliegue de sensores y supervisión, así como también procesamiento de datos demanda gran esfuerzo a un procesador común, en equipos empresariales, este procesamiento se puede virtualizar o incluso balancear entre diversos equipos.

Un requerimiento primordial para soportar esta distribución de Linux es la tarjeta de red, se conoce que las distribuciones de Linux son amigables con componentes de red Intel ®, por lo que la empresa AlienVault sugiere desplegar la solución con adaptadores de red Intel ®.

En lo que respecta al resto de componentes del host anfitrión ya sea para la virtualización como para su implementación directo a hardware, se necesita características compatibles con Linux; en caso de discos duros sean estos sata o IDE, requieren tener las especificaciones de partición: “/boot 100mb ext3 / 1 GB ext3 con lvm /var 4GB ext3 con lvm /usr 2 GB ext3 con lvm /home 140 GB ext3 con lvm swap 1 GB. El sistema ya soporta discos sólidos para su instalación.

2.3 Componentes y Arquitectura

2.3.1 OSSIM Server

Como cualquier otra aplicación de core robusto para monitoreo de seguridad, OSSIM funciona con una arquitectura cliente servidor, por tanto y para fines de optimización del monitoreo, la solución permite instalar un solo servidor OSSIM para toda la red incluida sucursales remotas que utilicen la misma salida de internet en la cual OSSIM está operando. El perfil servidor que se instala con la distribución de Linux adecuada a esta función, procesa todos los datos y almacena logs de todos los nodos del sistema, así como también elementos críticos como servidores.

En la figura 9, se visualiza un diagrama del agente de OSSIM (Dionaea), cuya función es la generación de logs enviados posteriormente al servidor.

Figura 9. Arquitectura OSSIM Server

Toda la información adicional a su almacenamiento, se procesa y arroja resultados clave para que el administrador de red pueda tomar decisiones sobre los procedimientos a seguir en caso de ataque.

El servidor ocupa recursos dentro de la infraestructura de red tales como:

- Por defecto tiene configurado los puertos 40001 y 40002 TCP para escucha del servidor, es decir los sensores colocados en los equipos se comunican a través de estos puertos identificándolos por medio de su Id.
- Almacena los datos en una base MYSQL, la cual puede estar en el mismo servidor o en una locación externa, para esta conexión se asigna el puerto 3306 en tráfico de salida
- Cuenta con la opción de administración remota por línea de comando, para el efecto usa el puerto 22 (SSH).
- La consola web está disponible únicamente bajo el puerto de HTTPS (443).

Adicional a las condiciones descritas anteriormente los puertos necesarios para el funcionamiento de todos los complementos de OSSIM se resumen en la siguiente tabla (Tabla 2):

Tabla 2.

Puertos de comunicación requeridos en estado abierto.

Puertos	Tipo	Estado Requerido	Servicio
40001 - 40002	TCP	Abierto	OSSIM COM
3306	TCP	Abierto	MYSQL
22	TCP	Abierto	SSH
443	TCP	Abierto	HTTPS
25	TCP	Abierto	SMTP
80	TCP	Abierto	HTTP
8080	TCP - UDP	Abierto	HTTP-PROXY

2.3.2 OSSIM Framework

Como todo Framework, esta capa intermedia en OSSIM nos permite evitar el uso de recursos de hardware al evitar una conexión en segundo plano a la plataforma por parte del aplicativo web, de esta manera se optimiza la funcionalidad y se destina procesamiento a otras tareas de mayor importancia. De igual manera el Framework tiene vital importancia a la hora de acceder a la base de conocimiento de amenazas de OSSIM, así como también a la base de datos de logs.

Los objetivos de esta capa en el procesamiento y funcionalidad de OSSIM radican en:

- Recolectar los datos tanto de agentes como servidores.
- Priorizar eventos de acuerdo a la configuración e impacto.
- Interconectar eventos de diversas fuentes a fin de interrelacionarlos.
- Realizar evaluaciones de riesgo y disparar alarmas.
- Almacenar logs en la base de datos.
- Reenviar logs o alarmas de ataque a otros servidores dentro del esquema de supervisión.

En la figura 10, se observan las capas del Framework de OSSIM, considerando la capa de acceso a usuario, el motor de correlación de datos actuales y de bitácora, y posteriormente el motor de recolección de datos multiplataforma.

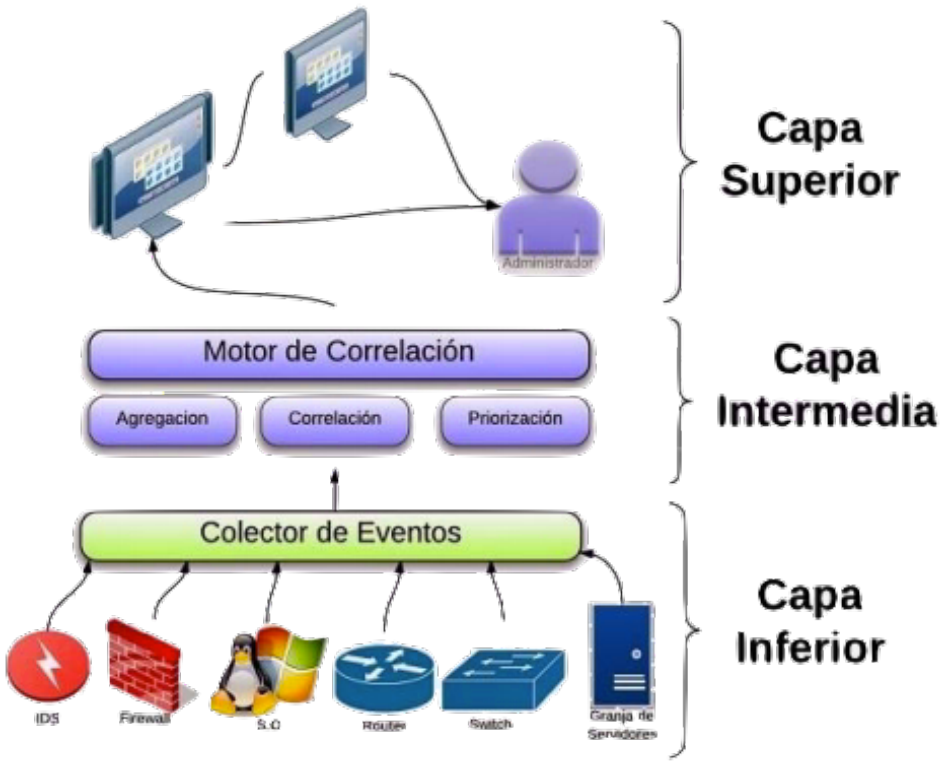


Figura 10. Modelo OSSIM Framework

Tomado de Bravo Bravo, A. H., & Villafuerte Quiroz, A. L. (2015).

2.3.3 Agente OSSIM

El nombre de Agente en la solución OSSIM, hace referencia al conjunto de plugins y aplicaciones que permiten recopilar toda la información de seguridad de una red. El agente consta de 2 grandes grupos, por un lado, aquellos dirigidos a la infraestructura de core como servidores y dispositivos de frontera, y por otra parte sensores de clientes (para topologías basadas en Windows y AD).

En la figura 11, se muestra únicamente el apartado del colector de eventos, esta capa es importante debido a la compatibilidad multi-dispositivo que ofrece la plataforma y que permite generar la recolección de información de diversos tipos de equipos en la red y su desempeño.

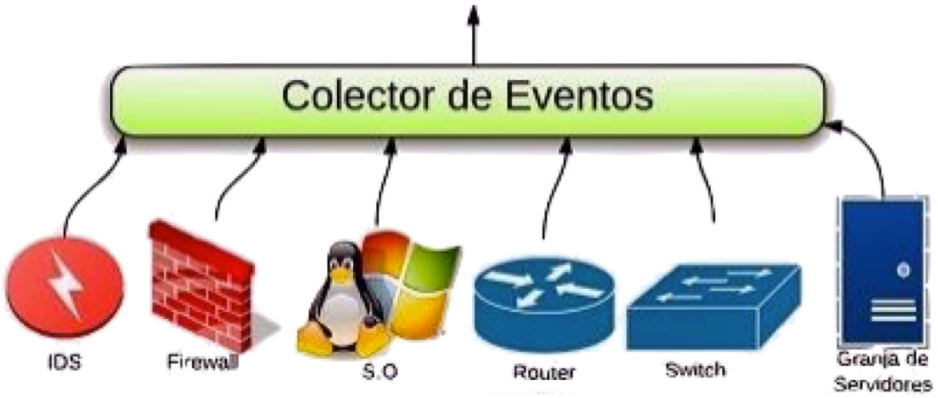


Figura 11. Modelo OSSIM Framework
Tomado de Bravo Bravo, A. H., & Villafuerte Quiroz, A. L. (2015).

En el caso de empresas implementadas con servicios de Windows se tiene disponible el agente HIDS, el cuál al ser desarrollado nativo para esta plataforma recopila un sinnúmero de información de forma centralizada y con una comunicación hacia el servidor mediante protocolos SSL, un mecanismo similar existe para Linux, por lo que este tipo de sensores de host cubren a estos gigantes usados en la mayoría de empresas.

OSSIM fue diseñado para funcionar en la DMZ o en el punto extremo de contacto con la WAN, por tanto necesariamente existe un desarrollo de sensores para equipos perimetrales su nombre es (OSSEC-Client), para aplicar adecuadamente estos aplicativos es necesario definir la arquitectura de la red empresarial con OSSIM de manera implícita debido a que estos complementos son diseñados específicamente por marca y modelo de equipo; esto como medida de control y transparencia del sensor sobre el procesamiento e incluso levantar los parámetros exclusivos que el equipo anfitrión puede ofrecer, sin exigir datos que se encuentran fuera del control de esa máquina. Dentro de este conjunto tenemos software disponible para versiones poco comunes de Linux, así como también MacOS, Solaris, HP-UX, AIX, Checkpoint, Cisco IOS, etc.

La solución de seguridad OSSIM en su entorno cuenta con varios complementos que permiten extraer información de casi cualquier equipo de configuración empresarial, sin embargo hay funcionalidades que necesitan de permisos especiales y procesamiento en los equipos de manera independiente al servidor OSSIM, en este caso en particular y para plataformas Linux existe una conexión al Syslog nativo de la distribución a fin de obtener cada registro que la máquina genere, estos paquetes con el software de registros están disponibles en los repositorios oficiales Linux y en las librerías en general agregadas a estos sistemas; dentro de este apartado se detacan los paquetes RSyslog y Syslog-ng, siendo los más utilizados y soportados por casi toda distribución basada en UNIX.

Dentro del Framework encontramos plugins, estos complementos a los sensores base permiten que la información que se recopila se gestione de tal manera que el administrador pueda contar con una visión global de la red que se está gestionando.

Algunos complementos necesariamente requeridos son:

- **Snort:** Permite tener una actualización de certificación diaria de cada uno de los Agentes OSSIM instalados.
- **Arpwatch:** Controla el monitoreo en capa 2 de la red, y por consiguiente problemas con MAC address.
- **Ocs-NG:** Esta funcionalidad levanta un inventario de equipos dentro de la red y bajo la supervisión de OSSIM, a diferencia de otros sistemas esta utilidad levanta este listado en tiempo real, obviando equipos que no se encuentren en la red al momento del análisis. Este inventario puede ser distribuido a equipos o en su defecto ser únicamente almacenado.

2.3.4 Arquitectura OSSIM

OSSIM desde el principio de este documento ha sido considerado una solución de código abierto sin licencia, por lo que el compendio de sus subsistemas y plugins desarrollados es amplio; el centro de este desarrollo como core de negocio ha sido OSSIM Server ya que cuenta con el soporte para albergar todas las soluciones que actualmente existen y las que desarrolladores propios o externos continúan agregando a la plataforma. La instalación de la herramienta tiene un particular de ubicación; los creadores y equipo de soporte recomiendan colocar el servidor de OSSIM en el centro de la operación a fin de mantener toda la red supervisada en una cantidad de saltos mínima, evitando saturación en la LAN, así como también agilizando el proceso de detección de intrusiones.

La arquitectura en el núcleo se divide en 3 componentes fundamentales:

- **EDB:** Base de datos de logs en la cual se almacenan todo tipo de eventos incluso los no maliciosos, por tanto, resulta de vital importancia para el administrador ya sea para obtener escenarios futuros de amenazas como también levantar planes de acción ante una intrusión en tiempo real.

- **KDB:** Base de datos en donde confluyen todos los elementos del framework, permite de manera más ágil identificar a los hosts supervisados por la herramienta, y de manera simultánea verificar las políticas de seguridad asignados a cada uno de ellos.

- **UDB:** Base de datos de perfiles o de usuarios, en esta base de conocimiento se almacenan los comportamientos del host durante el monitoreo constante de los mismos, por lo general se aprenden datos que confluyan en medidas para mitigar futuros ataques.

2.3.5 Diagrama de Arquitectura

Como se observa en la figura 12, las bases de datos más representativas del sistema interactúan entre sí para recibir y presentar la información obtenida de manera eficiente.

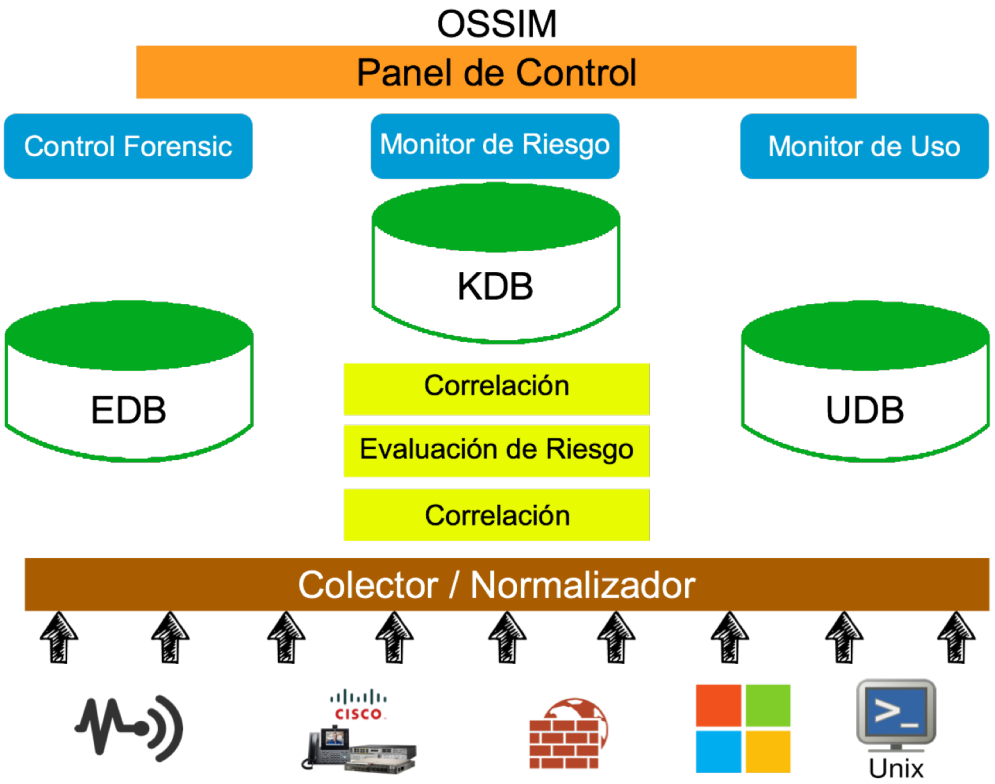


Figura 12. Arquitectura OSSIM.

2.4 Tipos de Monitoreo

2.4.1 Arpwatch

Este espía de solicitudes ARP, se usa en la mayoría de casos en problemas con direcciones MAC,es únicamente soportado por plataformas Linux y su capacidad se restringe a subredes debido a que los paquetes ARP, no saltan de vlan a vlan, como sugerencia de la empresa para el despliegue de OSSIM se recomienda utilizar este proceso únicamente en secciones críticas de la red.

Al ser complemento de un sensor estándar de OSSIM, se encuentra en las librerías de complementos de Linux, y de no encontrarlo, es necesaria la instalación manual del paquete. Esta herramienta genera una correlación entre las IP y direcciones MAC evitando la suplantación de ambos campos incluyendo

una funcionalidad opcional de notificación por correo electrónico de estas intrusiones al sistema.

2.4.2 PADS

Los Passive Asset Detection Systems, sirve efectivamente en el control conjuntos con sistemas IDS, que arrojan detalles de nuevos host o servicios circulantes por la red. Utilizando la dirección MAC, se traducen campos para determinar nombre de fabricante, parámetro básico para almacenar datos en la bitácora de log.

2.4.3 OpenVas

Originalmente conocido como GNessUs proveniente de una variante para escaneos de seguridades NessUs, OpenVas es un plugin integrado a OSSIM para levantar un mapa de red que permita gestionar las vulnerabilidades en los sistemas informáticos presentes; Por tanto, el concepto para su desarrollo fue el delimitar dos grandes áreas, el software y la red donde se considera:

- Escaneo de redes

El análisis de la red obtiene datos a partir de la interacción con todos los subsistemas en ejecución y sus respectivos servicios, de esta manera se visualiza a este escenario escalable desde el punto que admite cambios en la topología y vuelve a escanear únicamente si existe algún cambio de estos campos.

- Escaneo de hosts

Este proceso no es de mucha efectividad debido a que únicamente se ejecuta en entornos donde los sensores se encuentran instalados (Linux, Windows), su principal estrategia es enviar virus controlados a estos hosts determinando puertos vulnerables y generando informes para consideraciones futuras.

2.4.4 Spade

Spade, poderoso motor de estadística, permite la detección de anomalías en paquetes comunes; es una herramienta fundamental a la hora de determinar ataques sin firmas, que simplemente no son otra cosa que tramas enviadas a servidores sin ningún certificado válido, evitando de esta manera poder comprobar su integridad, estos paquetes pueden contener diversos tipos de malware, ransomware, etc.

2.4.5 TCPTrack

TCPTrack es una eficiente herramienta para analizar el “TOP” de una conexión TCP, mediante un modo de operación tipo sniffer, visualiza todas las conexiones y el ancho de banda correspondiente a fin de entregar un informe detallado sobre el estado de una interfaz; recopilando el origen y destino de las conexiones podemos determinar pérdida de paquetes, tiempo de inactividad en el enlace, y por último uso eficaz del ancho de banda asignado.

2.4.6 NTop

Complemento externo que no necesariamente acompaña a OSSIM, esta herramienta de análisis del tráfico de red está disponible para plataformas Windows y Linux. Con una licencia freeware su desarrollo aumenta con cada versión y su proactividad permite diferenciar entre tráfico normal y tramas maliciosas. Es una herramienta en tiempo real, por consiguiente, permite establecer controles de usuarios visitantes e incluso nuevos usuarios considerando para el efecto equipos empresariales (servidores) y de usuario normal (hosts).

- Protocolos soportados
    - TCP
    - UDP
    - ICMP

- ARP
- DLC
- AppleTalk
- Netbios

- Paquetes soportados

  - TCP
  - UDP
  - FTP
  - HTTP
  - DNS
  - Telnet
  - SMTP
  - POP
  - IMAP

2.4.7 NfSen

A partir de dos herramientas de control de flujos de red Netflow y NFdump, NfSen proporciona una interfaz amigable en un entorno web con ciertas modificaciones para el acoplamiento transparente con OSSIM. Mediante comandos de DOS o Bash en plataformas Windows y Linux respectivamente se obtiene:

- Datos de Netflow
- Procesamiento de datos Netflow en una ventana de tiempo determinada
- Creación de históricos de datos y perfiles de amenzas
- Definición de alertas en base a la configuración del administrador

2.4.8 NfDump

En el apartado anterior de NfSen, se determina que la base para su procesamiento es NfDump. A detalle, NfDump es un conjunto de plugins y herramientas comprimidas en una solución que recolecta y procesa flujos en la red donde se encuentra configurada.

Estos complementos mantienen a su core bien provisto de todos los datos necesarios para alarmar sobre un posible comportamiento anormal, las herramientas más notables que se destacan son:

- NfCapd

Script que lee datos que fluyen por la red al tiempo que los almacena en archivos.

- NfDump

Visualizador de datos almacenados por NfCapd y generador de estadísticas a partir de esta información.

- NfProfile

En este complemento se leen los datos de NfCapd y se filtra cierta información a fin de almacenar el contenido vital en archivos de respaldo.

- NfReplay

Plugin que reenvía la información almacenada hacia los demás hosts de la red.

- NfClean

Complemento que permite destruir la información histórica poco relevante que aún se almacena en el sistema.

2.4.9 Osiris

Osiris es un complemento que usando sensores recopila logs del sistema Windows y facilita una visión global de una intrusión. Adicionalmente al monitoreo rutinario en sistemas Windows, la plataforma permite hacer un seguimiento de la red sobre una posible amenaza y su evolución. Su arquitectura consta de tres componentes:

- OsirisImd (Consola de administrador)

Se recomienda la ubicación de esta consola en un equipo confiable dentro de la red ya que es el centro de información con componentes como bases de datos, logs generales y configuraciones de equipos.

- OsirisSd (Agente escáner)

Proceso en segundo plano que corre en los hosts permitiendo obtener la información y monitorear constantemente el equipo, de igual manera gestiona la conexión y envía los logs al servidor centralizado.

- Osiris (GUI)

Aplicación web que gestiona todos los complementos antes descritos y la información que estos generan.

2.5 Costo

OSSIM es una herramienta open source con licencia freeware, sin embargo, la empresa que gestiona su desarrollo (AlienVault), cuenta con una opción que permite obtener soporte con personal capacitado e incluso contar con una auditoría de seguridad.

A continuación, la tabla 3 muestra una comparativa de versiones de OSSIM, siendo la versión gratuita considerada para Pymes y la versión pagada para grandes corporaciones. Las principipales diferencias radican en el nivel de soporte que existe para la aplicación y en general la versión Premium no limita la generación de reportes o sensores.

Tabla 3.

Comparación de versiones OSSIM

	OSSIM (Versión Gratuita)	OSSIM Profesional (SIEM)
Soporte	Comunitario (Foros)	7x24
Garantía de Funcionamiento	Comunitario (Foros)	Q&A Profesional
Seguridad	Sin Auditoría	Con Auditoría
Rendimiento	Moderado	30x más rápido
Inteligencia SIEM	Correlación Lógica	Correlación Cruzada
	Jerarquía Simple	Jerarquía Compleja
Logger	No Incluye	Almacenamiento Ilimitado de Forensic
Reportes	<25	>200 con Asistente de Generación Web
Escalabilidad	No Incluye	Modelo Distribuído, Múltiples Usuarios, Crecimiento Ilimitado
Nivel de Confianza	Reportes de Alto Nivel	Jerarquía Alta y Baja
Actualizaciones	No incluye	Reglas y Reportes Diarios
Manejo de Usuarios	Individual (Controles Simples)	Plantillas de Creación con Control Específico

3. Capítulo III. Implementación del Sistema de Ciberdefensa

3.1 Requerimientos de hardware y software

Alien Vault provee una imagen .ISO para la instalación de OSSIM, este sistema operativo adaptado por el equipo desarrollador de OSSIM es un Linux Debian. Por lo que se debe considerar ciertos requisitos de hardware y software para virtualizar un entorno óptimo en el que la herramienta pueda funcionar con normalidad y fluidez. En general los requerimientos mínimos para este despliegue son:

- Procesador a 1.8 Ghz doble núcleo o superior.
- Memoria RAM mínima de 2 GB.
- Espacio mínimo en el disco duro de 50 GB.
- Tarjeta de Red a 1Gbps o superior.

- Conexión a red de internet (Actualización base de datos de amenazas).

3.1.1 Requerimientos implementación en la nube (Azure)

Para la implementación de OSSIM como solución externa a la empresa alojada en una plataforma en nube se ha seleccionado Azure por el costo y flexibilidad de aprovisionamiento de recursos. Azure es la plataforma en nube de Windows, lanzada oficialmente el 1 de enero de 2010, consta de un portal web que permite acceder a la creación de máquinas virtuales para diferentes sistemas operativos como también aplicaciones. Dentro de las principales ventajas al usar este servicio tenemos:

- Sin costo por adelantado.
- Sin penalidad por cancelación del servicio.
- Se paga por el tiempo que se utiliza el servicio.
- Facturación por minuto.

Su costo varía de acuerdo a las necesidades del cliente por lo que se detalla a continuación las configuraciones básicas para OSSIM y el costo del despliegue en base a esta solución como se observa en el presupuesto de la tabla 4.

Tabla 4.

Costo de aprovisionamiento en Azure

Your estimate

Service type	Custom name	Region	Description	Estimated Cost
Virtual Machines	Máquinas virtuales	West US	1 Basic máquinas virtuales, tamaño A2 (2 núcleos, 3.5 GB de RAM, 60 GB en disco, $0.081/h): 744 hours	$60,26
Support			**Support**	$0,00
			Monthly Total	**$60,26**
			Annual Total	**$723,17**
Disclaimer				
All prices shown are in US Dollar ($). This is a summary estimate, not a quote. For up to date pricing information please visit https://azure.microsoft.com/pricing/calculator/				
This estimate was created at 11/20/2016 5:58:32 PM UTC.				

Cabe destacar que el acceso a estas máquinas virtuales se realiza por medio de RDC (Remote Desktop Conection) o VNC. Adicionalmente para la implementación dentro de la red empresarial es recomendable por seguridad conectar por VPN la máquina virtual, asignando una dirección local (LAN) al recurso, evitando que la información de cada uno de los sensores viaje por internet a la dirección asignada remotamente sin protección, esto como medida de prevención ante ataques al sitio remoto (máquina virtual en Azure).

3.1.2 Requisitos implementación virtualización (Entorno Local)

Actualmente los servicios de aprovisionamiento en la nube han limitado la adquisición de equipos de red, así como también el problema de renovación de infraestructuras, es por este motivo que muchas veces es necesario implementar ciertas soluciones al interior del negocio. Para esta implementación de OSSIM se deben tomar diferentes precauciones en el entorno de red y en el servidor anfitrión, así como también costos necesarios descritos en la tabla 5:

Tabla 5.

Costo de aprovisionamiento en entornos locales

	VMWare Vshere	Windows Hyper-V
Implementación Local de OSSIM	Discos SAS no soportados	Todos los discos soportados
	Aprovisionamiento de disco con tamaño fijo, evitando asignación dinámica	Aprovisionamiento de disco con tamaño fijo, evitando asignación dinámica
	Memoria asignada superior a 2GB (2.5 GB o superior)	Memoria asignada superior a 2GB (2.5 GB o superior)
	Licencia Vsphere para virtualizar 2 núcleos como mínimo	Licencia Hyper-V para máquinas virtuales para 1 procesador como mínimo
	Interfaz de red física dedicada	Interfaz compartida a 10Gbps o superior
Parámetros de Red	Políticas de QoS para puertos OSSIM	Políticas de calidad de servicio para los puertos OSSIM
Costo Estimado de Licencias	$ 995 - $4395	$ 2999 - $3999

En el parámetro de costo de las licencias, la variación de demasiada debido a los tipos de sistemas, a continuación, se enlistan algunos ejemplos de los mismos.

- Windows 2012 R2 Estandar Edition ($2999)
- Windows 2012 R2 DataCenter Edition ($3500)
- Windows 2012 R2 virtualization capabilities ($4000)
- VMWare Vsphere ($995)
- VMWare VSpere plus ($3395)

3.2 Guía de Implementación

Una vez comprobados todos los requisitos de hardware y software anfitrión, es necesario considerar 3 pasos previos al inicio de la instalación de la solución.

- Obtener la versión más reciente de OSSIM desde la página de AlienVault.
- Configurar la Máquina virtual con los parámetros necesarios.
- Iniciar la máquina seleccionando el archivo ISO para el arranque.

Al cargar la imagen en la máquina virtual, un asistente de instalación se desplegará, estas pantallas permiten configurar parámetros básicos del sistema antes de su instalación, a continuación, se muestran los pasos a seguir para la instalación de la suite OSSIM.

- Selección de la distribución de OSSIM necesaria (Figura 13)

En el primer menú existen dos opciones, la primera genera una instalación de OSSIM Server en la MV (Máquina Virtual), y la segunda opción es un sensor que puede ser instalado en cualquier distribución Linux. Es importante tener en cuenta que antes de instalar cualquier sensor es necesario contar con una instalación del servidor que recopila los datos.

Figura 13. Selección de distribución OSSIM

- Selección del idioma de la interfaz del sistema (Figura 14)

Figura 14. Selección de idioma en la solución

- Selección de la ubicación geográfica del equipo (Figura 15)

Figura 15. Selección de ubicación del equipo

- Selección de la distribución de teclado (Figura 16)

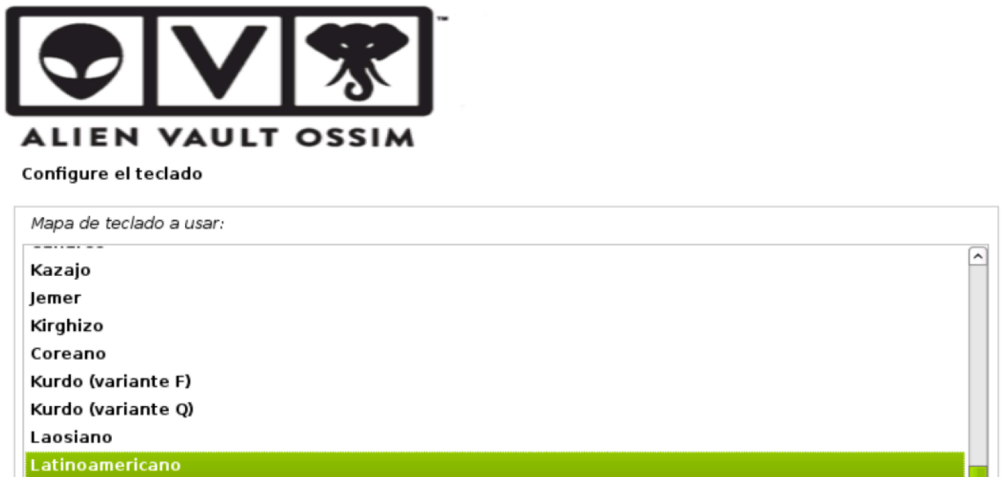


Figura 16. Selección de distribución del teclado

- Configuración básica de parámetros generales (Figura 17)

Figura 17. Progreso de configuración inicial

- Configuración de la dirección IP (Figura 18)

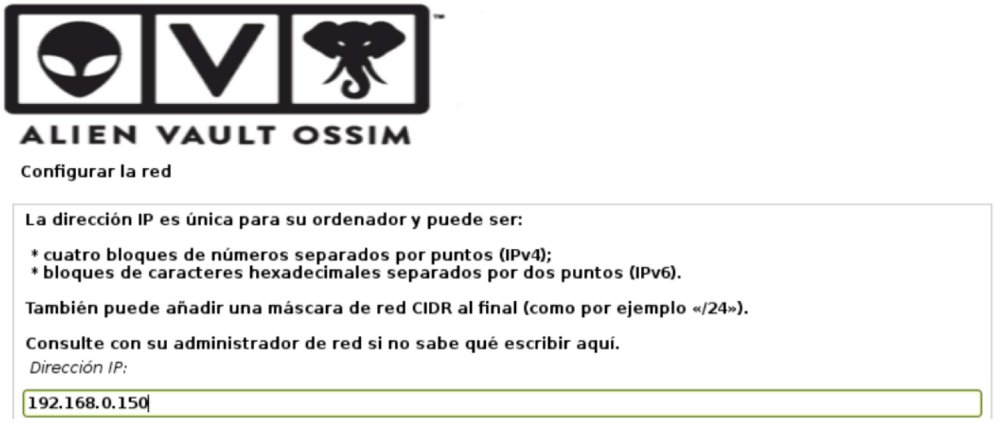


Figura 18. Configuración IP estática

En el apartado de dirección IP, es necesario determinar y reservar una IP fija de la LAN tanto para el despliegue en la nube como en un entorno local, debido a que es necesario que los equipos apunten a una sola dirección evitando conflictos en el futuro.

A continuación, se muestra la reservación de la dirección IP por medio de la MAC obtenida de la máquina virtual (Figura 20) y configurada en un router Huawei dentro del entorno de prueba (Figura 19).

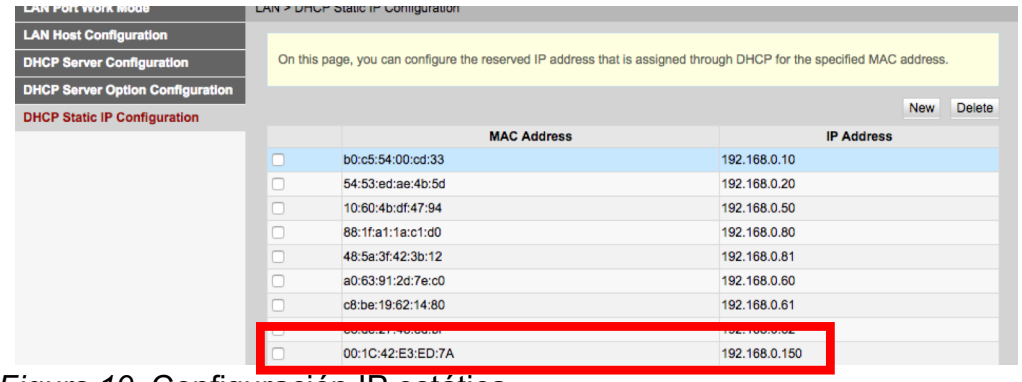


Figura 19. Configuración IP estática

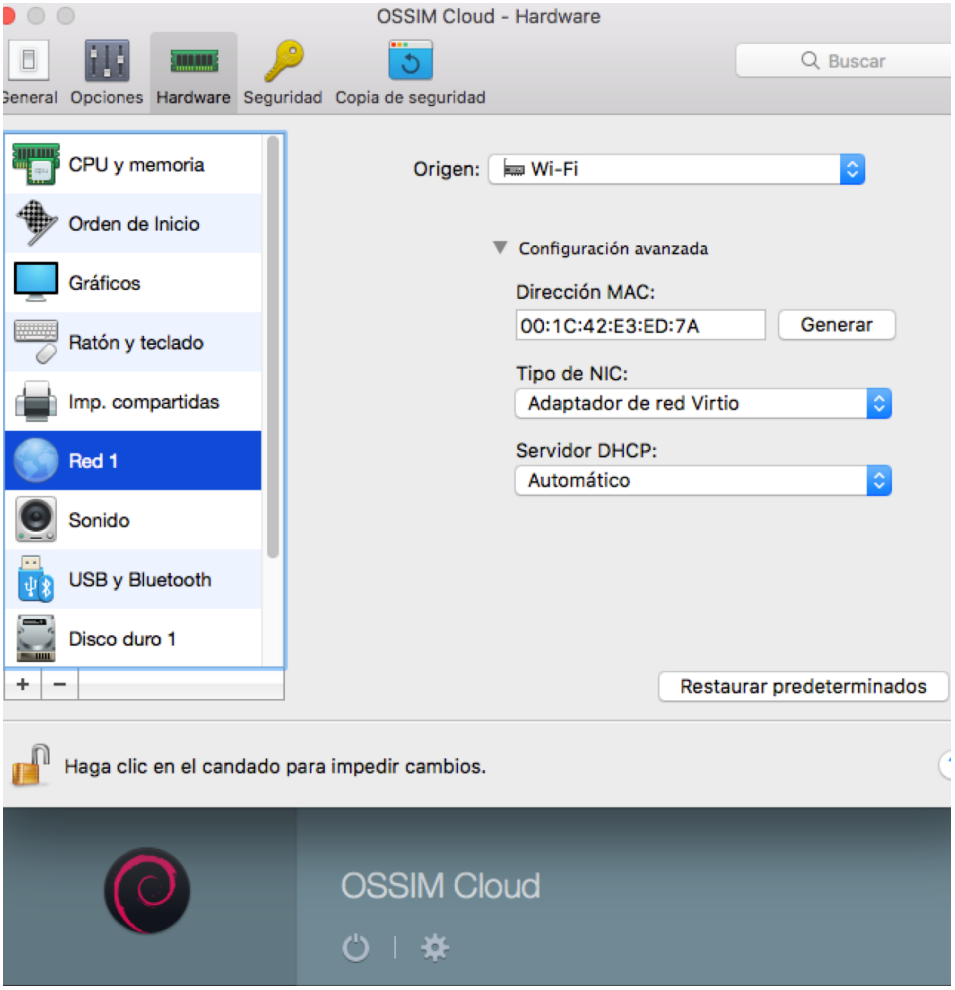


Figura 20. Configuración dirección estática VM

- Configuración de máscara de subred (Figura 21)

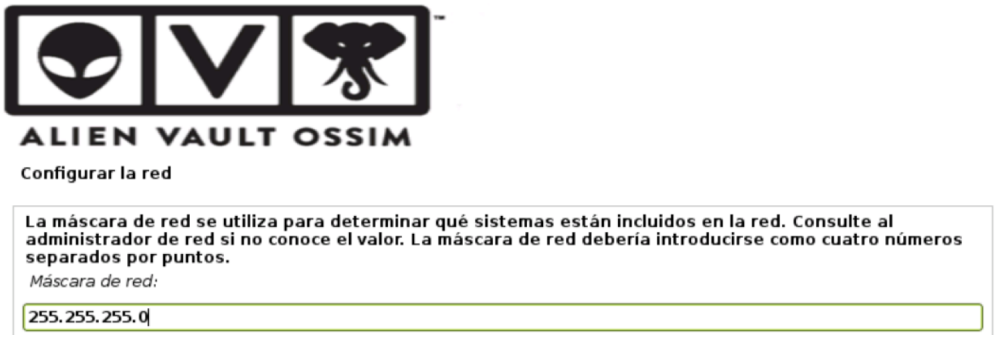


Figura 21. Configuración de máscara de subred

- Configuración de puerta de enlace (Figura 22)

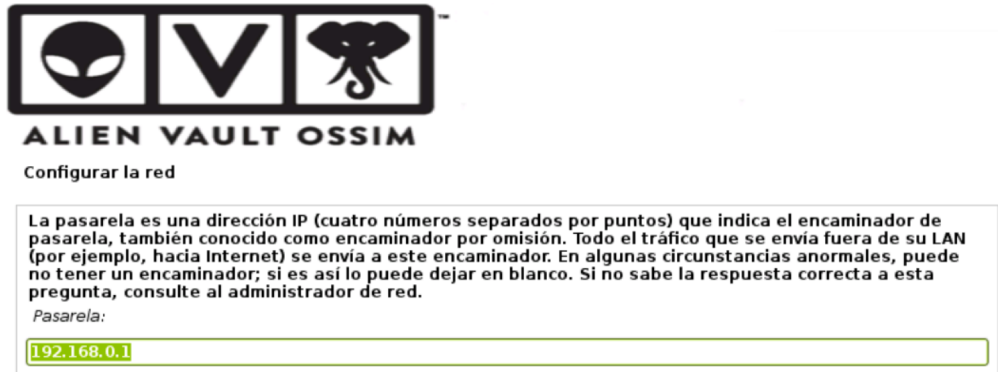


Figura 22. Configuración de la puerta de enlace

- Configuración de DNS (Figura 23)

En entornos empresariales, el servidor DNS (Figura 23), se encuentra configurado generalmente en una distribución de Windows Server, de igual manera este servidor se encuentra atado a un proxy, sin embargo, para la presente implementación solo se tomó en cuenta el servidor DNS. A continuación, se muestra en la figura 24 el servidor DNS configurado para el escenario propuesto.

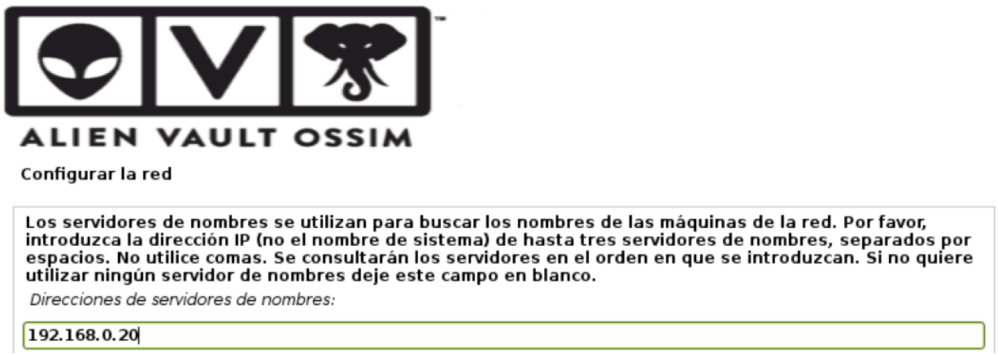


Figura 23. Configuración de servidor de nombres (DNS)

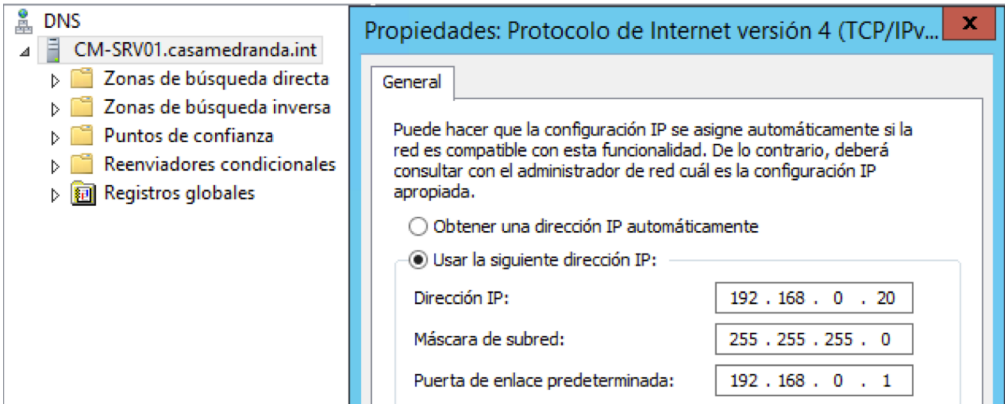


Figura 24. Servidor DNS

- Configuración de clave usuario root (Figura 25)

Figura 25. Configuración de clave superusuario

- Configuración de zona horaria (Figura 26)

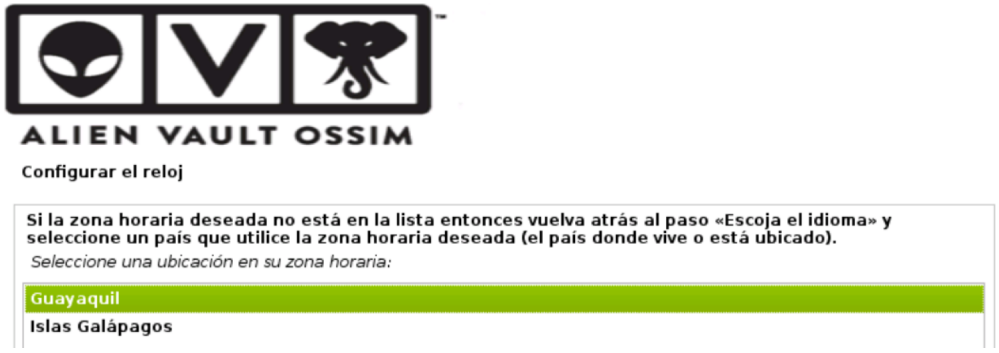


Figura 26. Zona horaria

- Primer inicio de sistema (Figura 27)

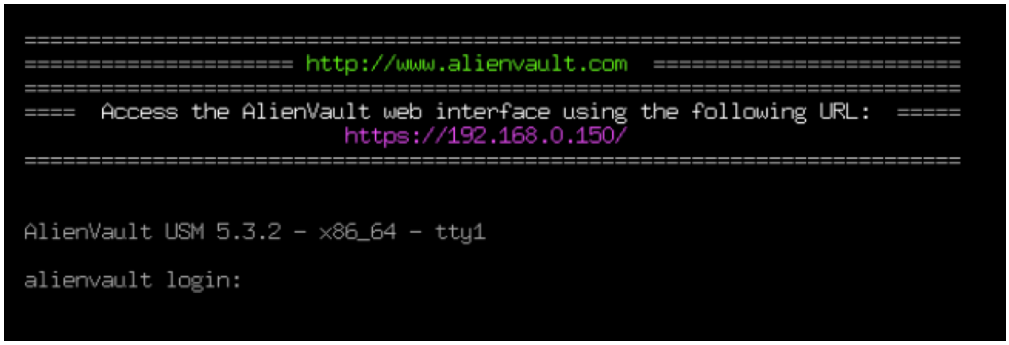


Figura 27. Inicio del sistema

- Acceso a configuración privilegiada (Figura 28)

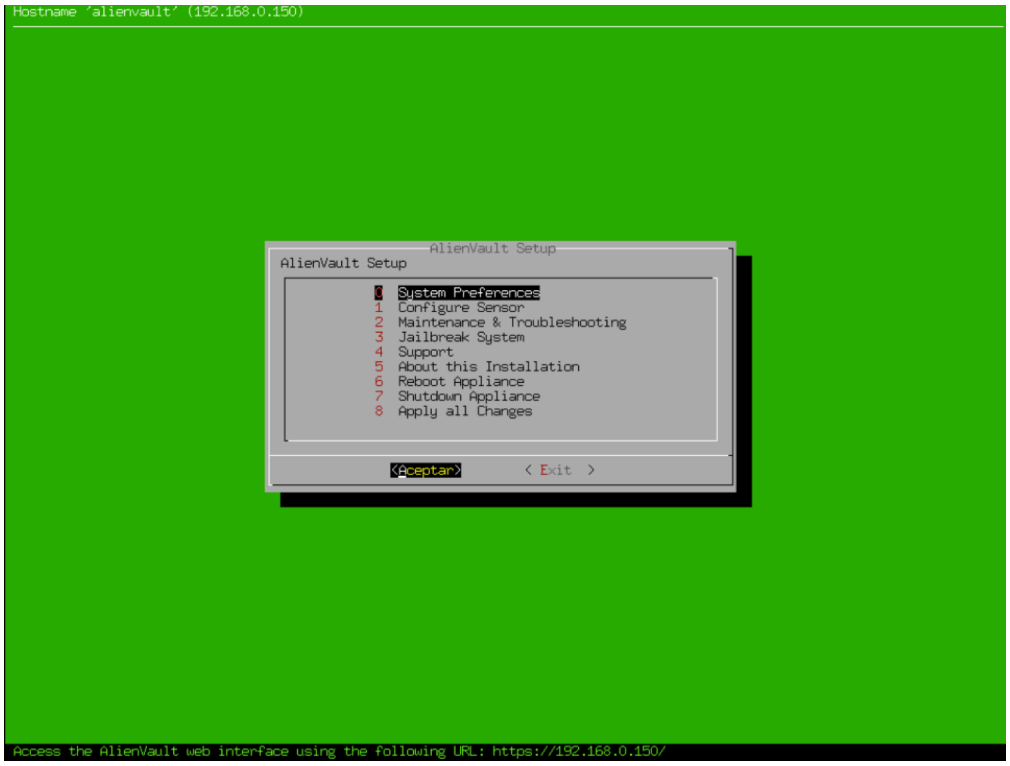


Figura 28. Menú configuración privilegiada

- Configuración de la herramienta web (Figura 29)

Una vez instalado el sistema operativo OSSIM, es necesario configurar el complemento web que permite visualizar los datos recopilados por el aplicativo, para realizar este proceso es necesario llenar los datos que se muestra a continuación (Figura 29).

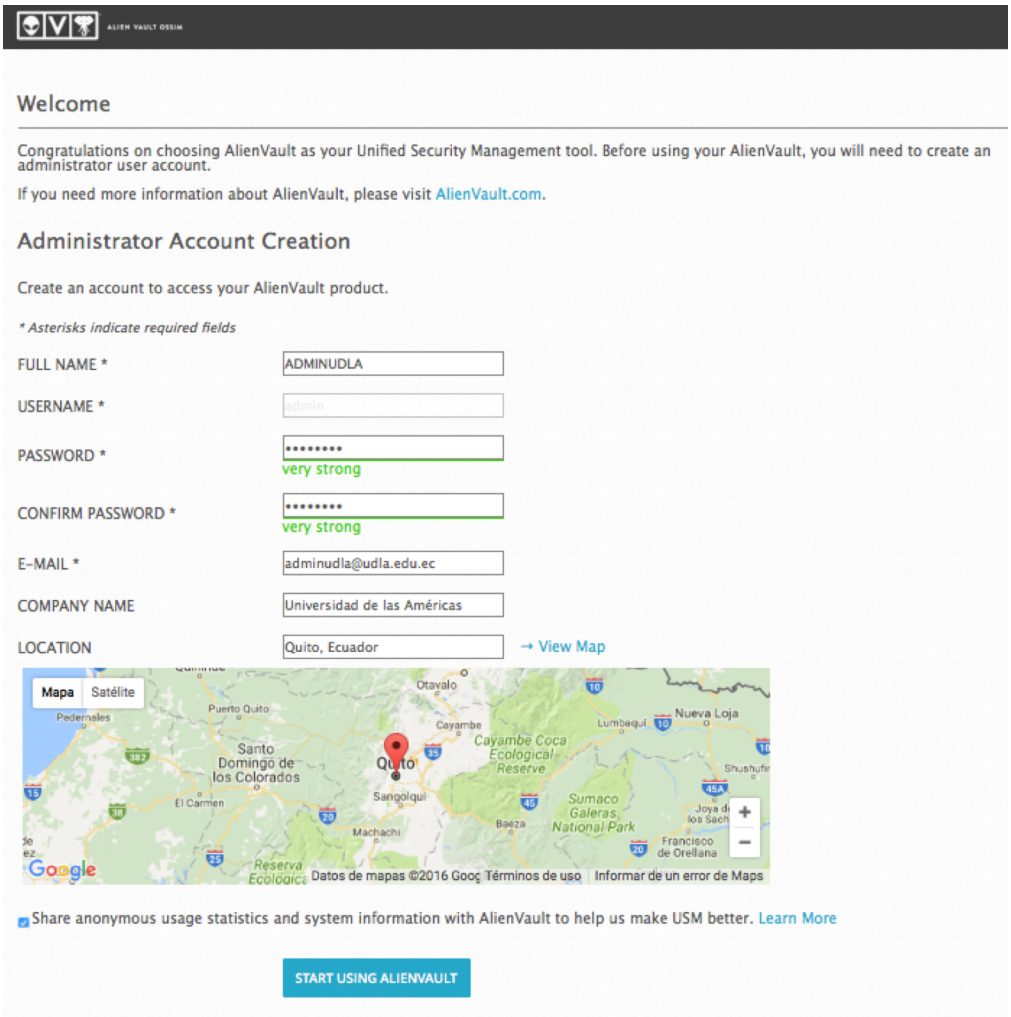


Figura 29. Configuración complemento web

- Ingreso al sitio web de administración (Figura 30)

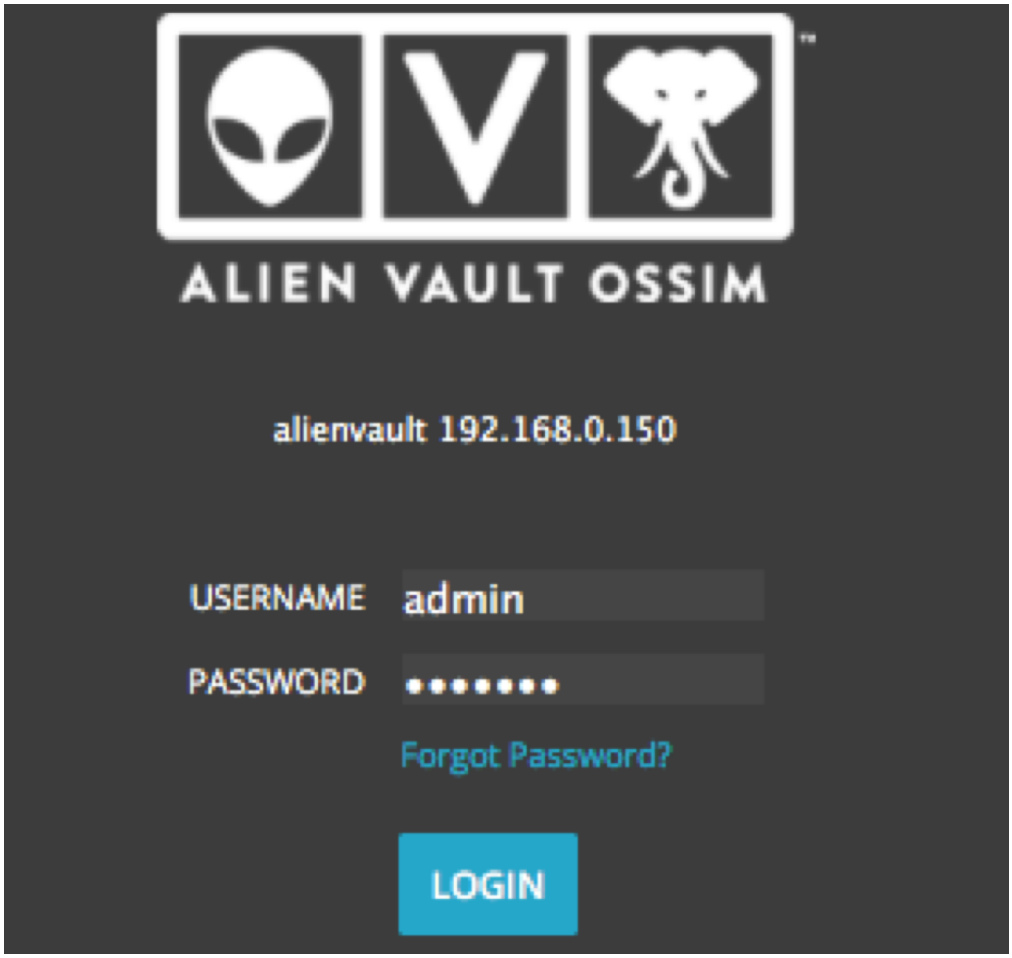


Figura 30. Pantalla de acceso al aplicativo web

- Asistente de identificación de elementos de red (Figura 31)

Una vez el usuario administrador accede al sitio de control de la solución, OSSIM inicia un asistente (Figura 31) que permite añadir todos los dispositivos de la red a fin de facilitar el ingreso manual de todos los elementos de la red local.

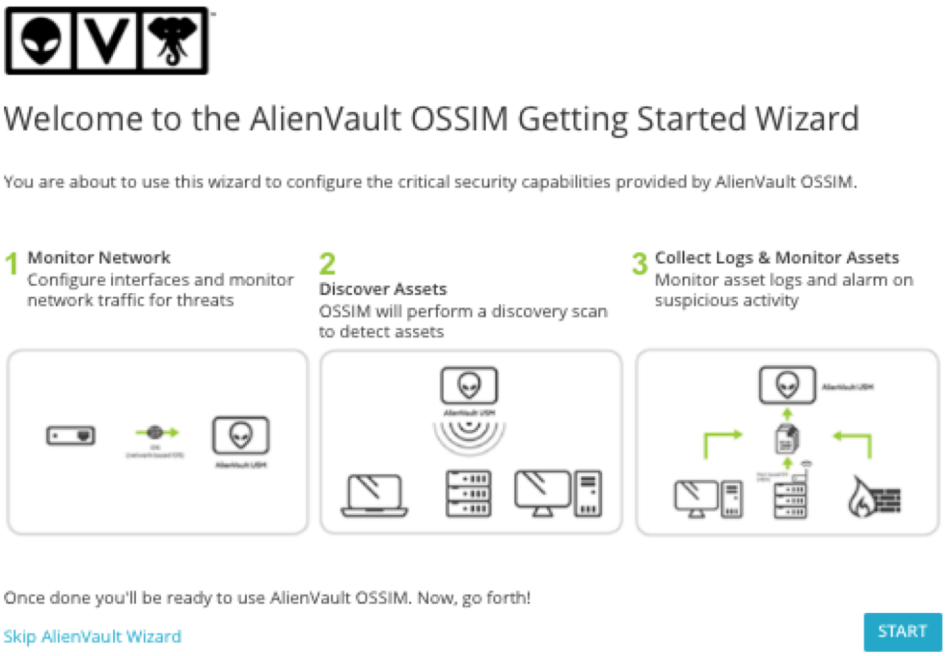


Figura 31. OSSIM asistente

- Selección de interfaz de escucha de sensores (Figura 32)

En este apartado se configura la interfaz (Figura 32), por la cual el sistema va a recibir actualizaciones de los sensores instalados en otros equipos.

Figura 32. Selección de interfaz de escucha

- Proceso de descubrimiento de clientes a supervisar (Figura 33)

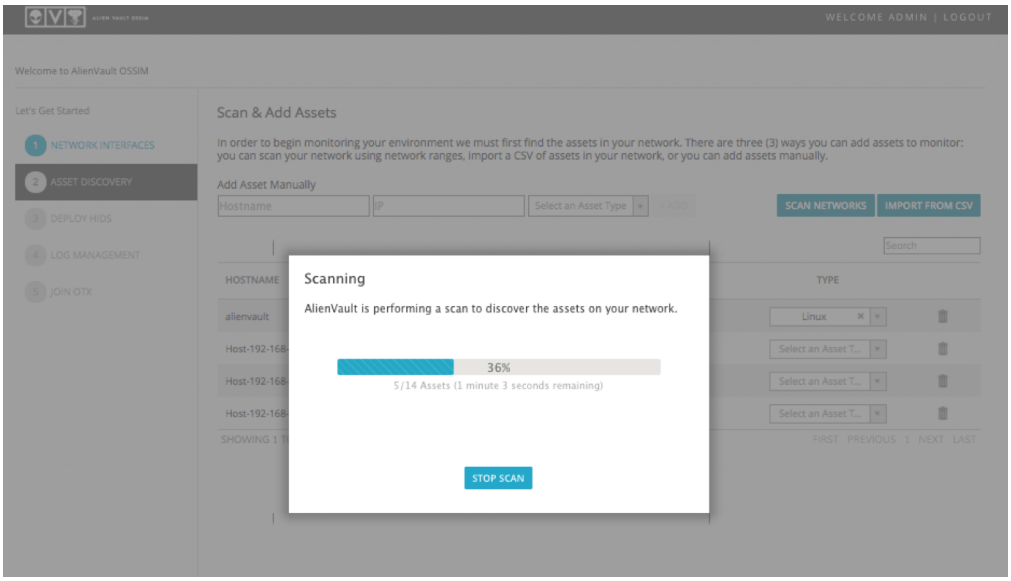


Figura 33. Menú configuración privilegiada

- Lista de hosts disponibles para supervisión (Figura 34)

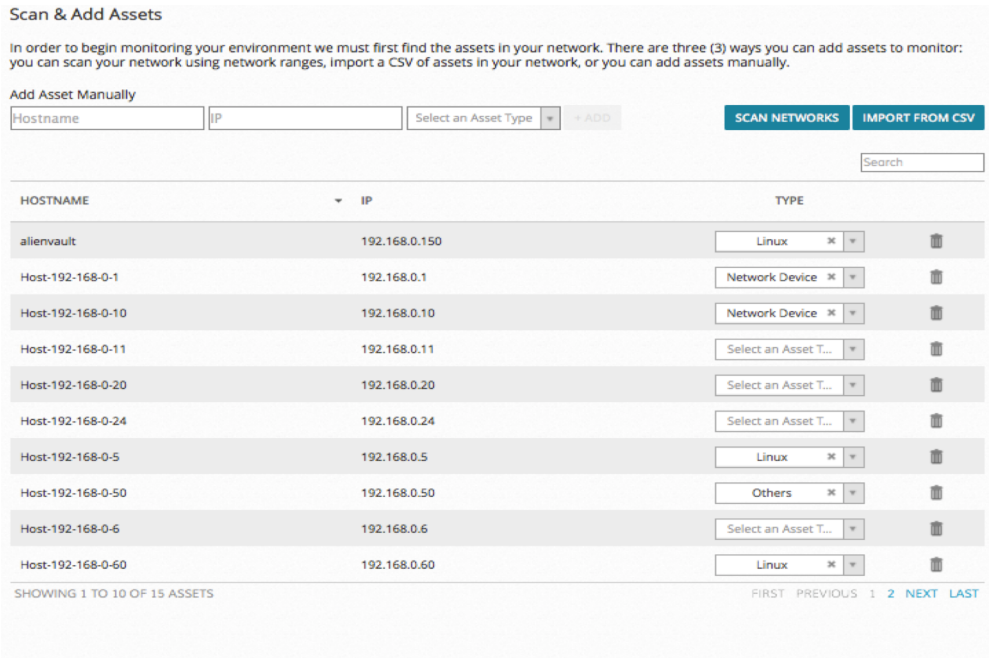


Figura 34. Lista de hosts disponibles

- Despliegue de sensores para Linux (Figura 35)

En el caso de plataformas Linux, el despliegue de estos sensores se realiza mediante un complemento de la plataforma que se conecta con las distribuciones Linux más conocidas mediante el usuario y contraseña a fin de instalar como servicio y por comando, el sensor OSSIM (Figura 35). Cabe destacar que para este proceso todos los servidores Linux deben contar con un usuario y una contraseña coincidente.

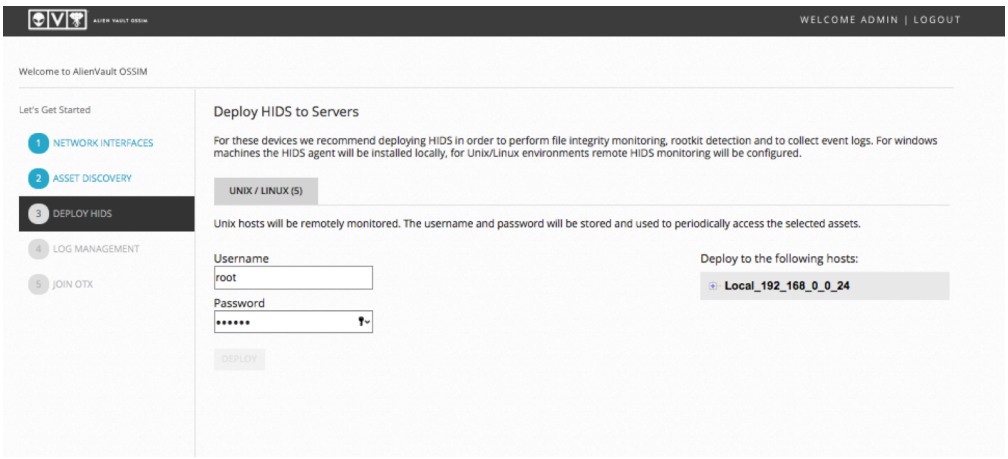


Figura 35. Despliegue sensores Linux

- Registro de logs en dispositivos de red (Figura 36)

En la infraestructura empresarial es necesario mantener un correcto orden de los registros en cada equipo, como un complemento a su función base (Figura 36), OSSIM ofrece la posibilidad de monitorear este registro y analizarlo a fin de encontrar alguna alternativa para combatir ataques en base a lo registrado en esta bitácora.

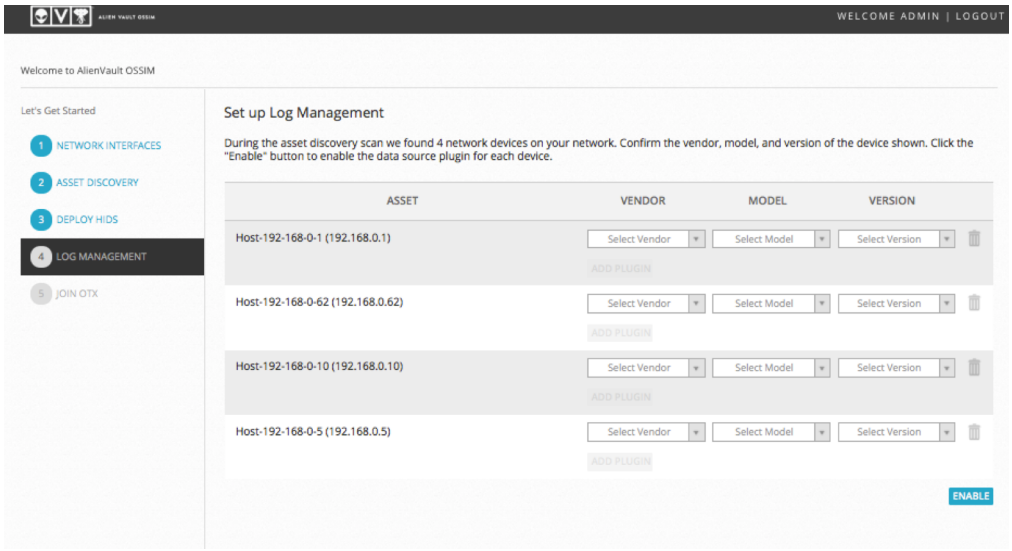


Figura 36. Configuración de logs

- Registro en la plataforma OTX (OSSIM Threat Exchange) (opcional) (Figura 37)

Tras centralizar las operaciones de identificación de amenazas sin un gran éxito, en 2010 OSSIM abre una comunidad en la que diversas empresas y entusiastas de la seguridad informática registran incidentes de violación de redes a fin de contar con una base de datos de conocimiento (Figura 37) que aporte tanto a detectar nuevas amenazas, así como también permitir mitigar un ataque dentro de la infraestructura empresarial.

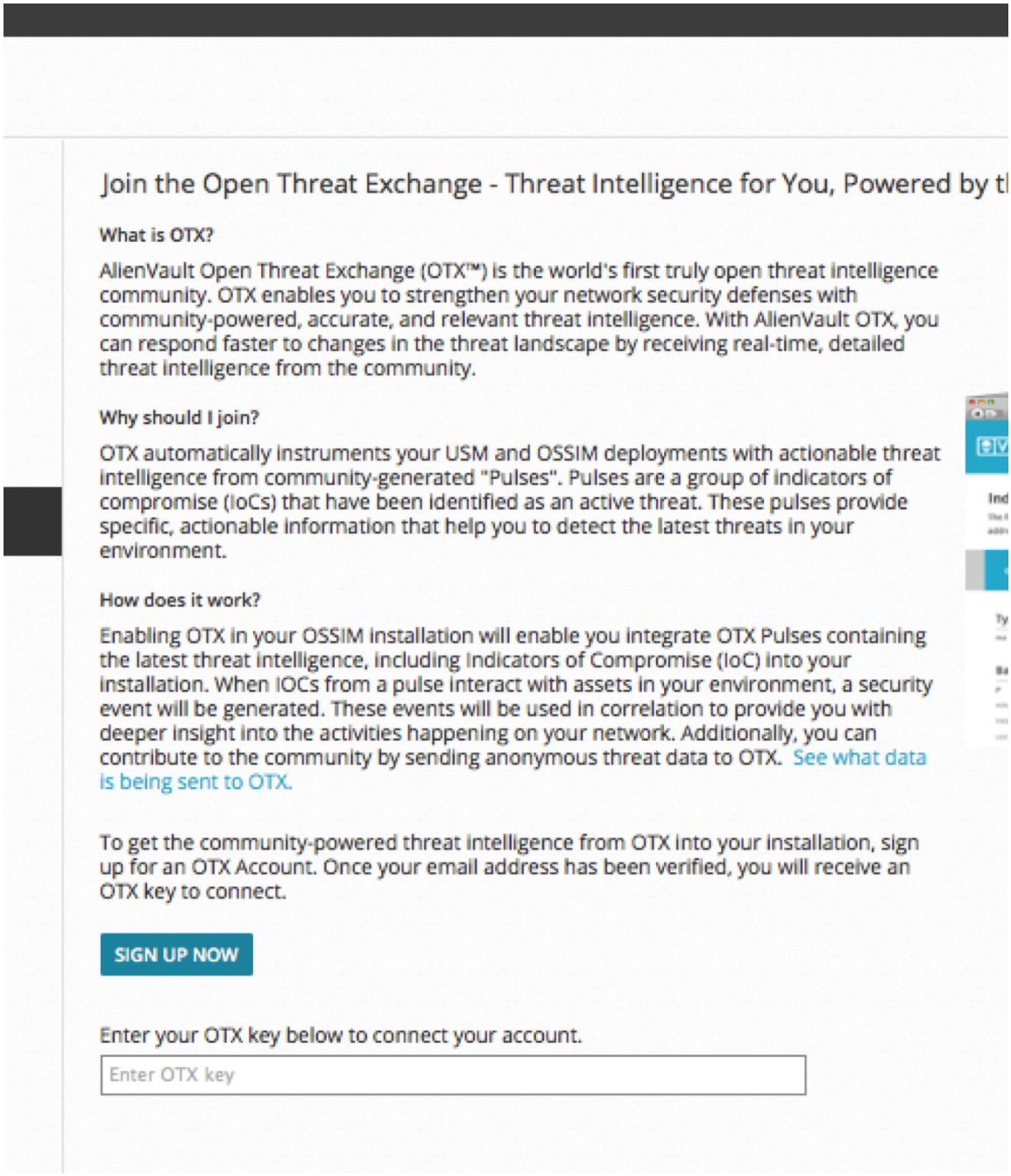


Figura 37. Registro OTX

- Consola de administración OSSIM (Figura 38)

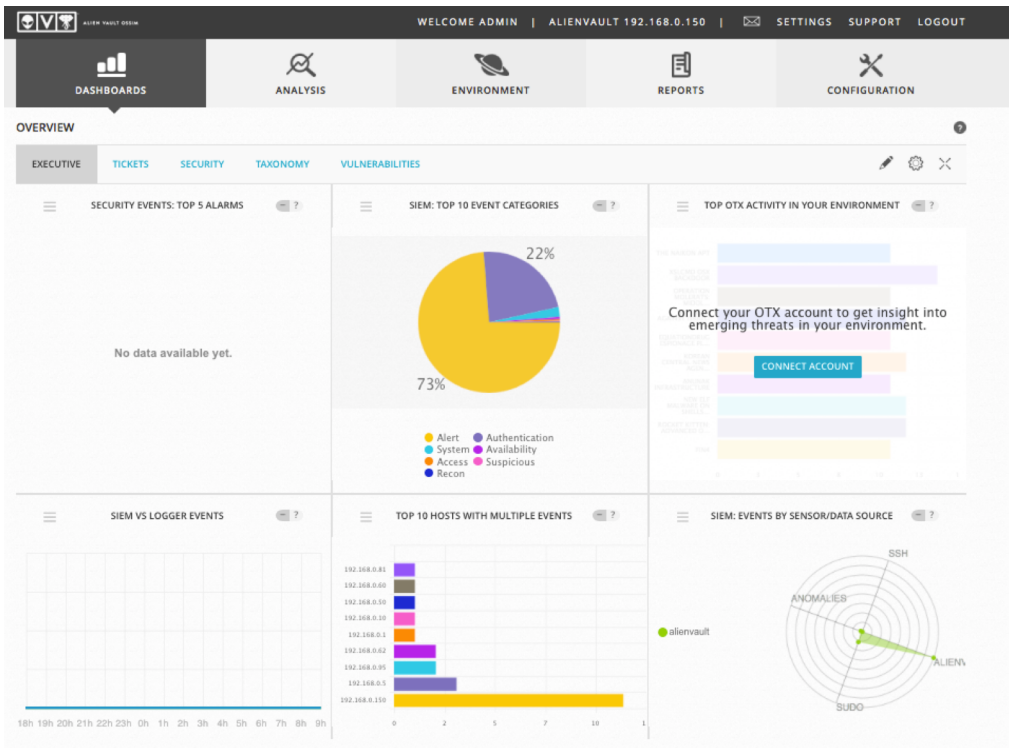


Figura 38. Sitio de administración OSSIM

- Instalación de sensor Windows (Figura 40)

El sensor Windows se descarga en formato .exe desde la plataforma web, cada sensor generado en Windows se crea bajo una clave específica (Figura 40), razón por la cual no se pueden intercambiar sensores, peor aún instalar algún archivo .exe genérico y conectarse al servidor OSSIM.

Para desplegar los sensores es necesario las credenciales de administrador de los clientes Windows (Figura 39).

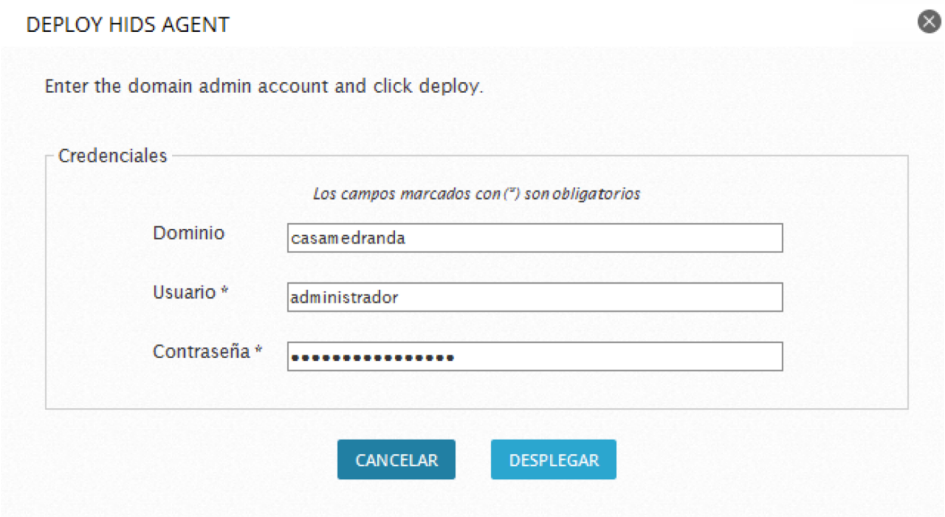


Figura 39. Credenciales para creación de sensor

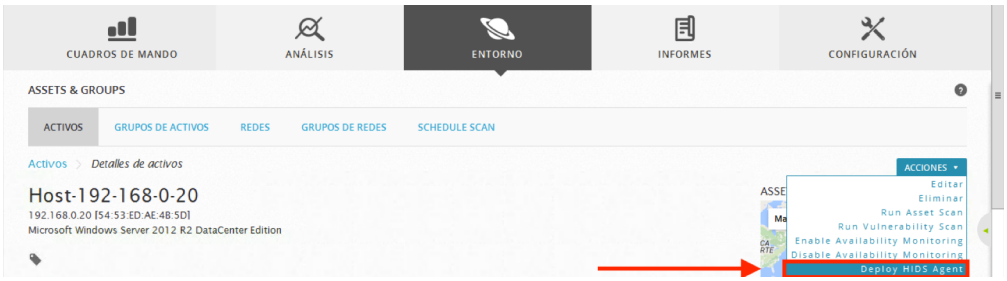


Figura 40. Apartado de instalación de sensores Windows

Posteriormente al despliegue de los sensores, OSSIM nos permite obtener un informe sobre el estado de los servicios, así como también las vulnerabilidades del host examinado (Figura 41).

Para esta implementación se ha considerado un solo análisis a un servidor con distribución Windows Server 2012 R2 Datacenter Edition, que distribuye los servicios de DNS y tiene capacidades para ser configurado como VPN, sin embargo, restricciones de la red de acceso impiden probar esta funcionalidad. Adicionalmente se cuenta con un servidor de autenticación Wireless bajo el protocolo 802.1X, y por último cuenta con despliegue de active directory y acceso a RDP (Remote Desktop Protocol) activado.

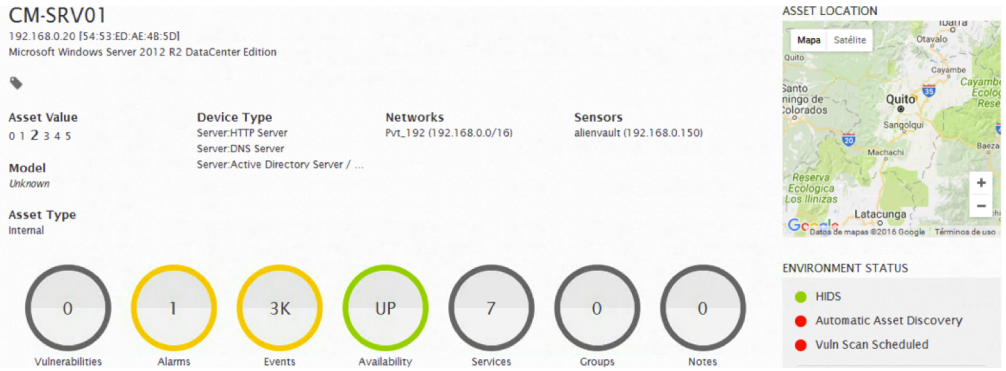


Figura 41. Informe resumido estado servidor

4. Capítulo IV. Fase de Pruebas y Verificación de la Solución

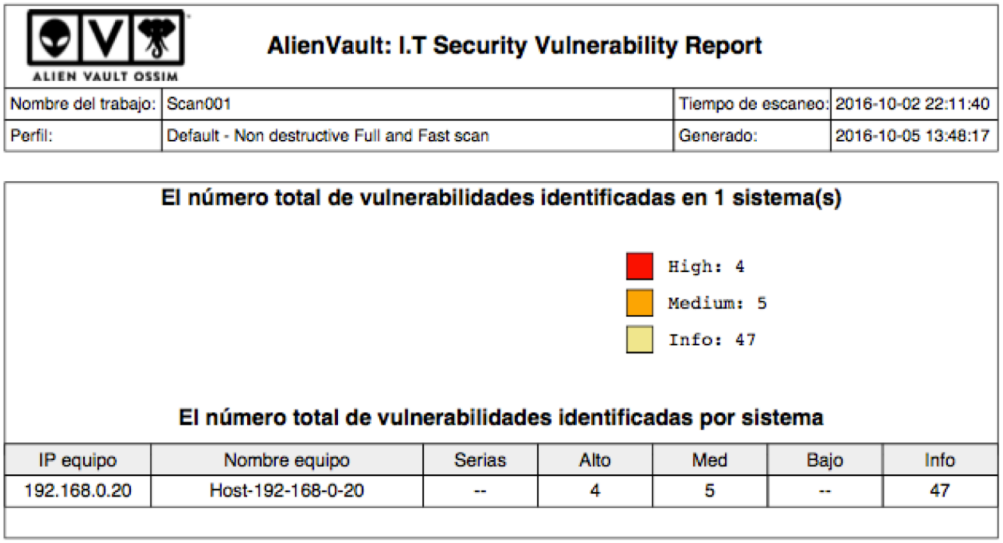
4.1 Preámbulo

Tras el despliegue de una solución de monitoreo de red, es necesario establecer una fase de pruebas que someta al sistema a un “test” real de ciertas amenazas que ocurren a diario en empresas. OSSIM ejecuta procesos de ataque a los servidores para demostrar las posibles vulnerabilidades, es recomendable por medio de software independiente realizar pruebas de penetración en red para medir la eficiencia de sus sensores.

4.1.1 Análisis de amenazas

Ossim cuenta con una función de análisis de amenazas en base a las vulnerabilidades encontradas en un sistema (Figura 42), por tanto es el primer filtro para tomar decisiones sobre qué hacer ante un ataque y tomar en consideración las posibles puertas o protocolos que el atacante está explotando para conseguir la intrusión; pese a esta herramienta es claro que existen ataques nuevos cada día para los cuales el sistema base puede no estar preparado, por esta razón Alien Vault (Creador de OSSIM) cuenta con una plataforma de colaboración en donde usuarios empresariales suben sus últimos registros sobre ataques, de esta manera mantienen enterada a la herramienta y al personal de

TI de todas las nuevas amenazas encontradas, sin embargo y pese a toda esta colaboración se debe tomar en cuenta la categorización de amenazas tanto externas como internas a fin de esquematizar un plan de acción previo que complementado con los datos de OSSIM brinde un escenario claro para la toma de desiciones.



AlienVault: I.T Security Vulnerability Report

Nombre del trabajo:	Scan001	Tiempo de escaneo:	2016-10-02 22:11:40
Perfil:	Default - Non destructive Full and Fast scan	Generado:	2016-10-05 13:48:17

El número total de vulnerabilidades identificadas en 1 sistema(s)

High: 4
Medium: 5
Info: 47

El número total de vulnerabilidades identificadas por sistema

IP equipo	Nombre equipo	Serias	Alto	Med	Bajo	Info
192.168.0.20	Host-192-168-0-20	--	4	5	--	47

Figura 42. Servicios abiertos en servidor de destino

4.1.2 Ataques a Hogares

En entornos de hogares por ejemplo, el atacante se concentra en el consumidor promedio que cuenta con un computador regular con características básicas y cuyo uso se limita a ciertas aplicaciones de ofimática y navegación por internet, adicionalmente este usuario promedio cuenta actualmente con dispositivos móviles dentro de su red así como también otros periféricos controlados por su LAN como equipos IOT; en este primer escenario el atacante debe tomar en cuenta las seguridades que el ISP coloca en el enlace previo al acceso a una red local de usuario que por lo general cuenta con todo tipo de acceso sin restricciones a recursos contenidos en internet. Por tanto, el ciberatacante procede a enviar solicitudes a equipos en el usuario final, eliminando así la complejidad de atacar al ISP directamente.

4.1.3 Ataques a Empresas

En el caso de un cliente empresarial, el escenario varía dependiendo de la complejidad de su red, para el escenario propuesto en el presente trabajo de titulación, se considera la presencia de un firewall y políticas de usuario centralizadas, las cuales impiden que servicios, así como también puertos se encuentren disponibles para todos los usuarios, mitigando de esta manera la utilización de servicios de terceros o aplicaciones no autorizadas. Considerando que el tráfico de la LAN se encuentra protegido por toda la infraestructura del lado de la empresa, la única preocupación proviene de internet. (WEGNER, H., 2014).

Como se menciona anteriormente el entorno empresarial genera un desafío de seguridad a nivel de su conexión WAN comparado con el entorno LAN. Las transacciones financieras, sistemas de reportes y gestión, así como servidores de correo electrónico o colaboración empresarial son alquilados en la nube para evitar la adquisición de hardware que debe ser renovado cada cierto tiempo generando un costo que no siempre retorna como ganancia a la empresa. Por tanto, el enlace empresarial a internet es un pilar fundamental de interacción entre los miembros del entorno laboral y sus colaboradores externos. Se debe tomar en cuenta en el apartado las configuraciones básicas que se cuentan actualmente configuradas en un entorno empresarial básico tales como:

- VPN
- Mail Cloud
- Cloud Apps
- VoIP
- Colaboración Móvil (Skype Empresarial)
- Plataformas SGD (Sistemas de Gestión Documental)

tras mencionar estas maneras de conexión dentro y fuera de la empresa queda claro que el desafío se concentra en restringir aquellos servicios innecesarios, así como también supervisar los mencionados garantizando que su integridad

no quede comprometida, así como también las conexiones externas no tengan la posibilidad alguna de ejecutar ataques a causa de un usuario inexperto en seguridad de la información (SERT Quarterly Threat Report Q2. 2016).

A continuación (Figura 43), se describen los ataques más importantes que provienen de internet al entorno colaborativo empresarial causando daños a nivel de comunidad de usuarios por su alcance y fuerza de penetración en los sistemas.

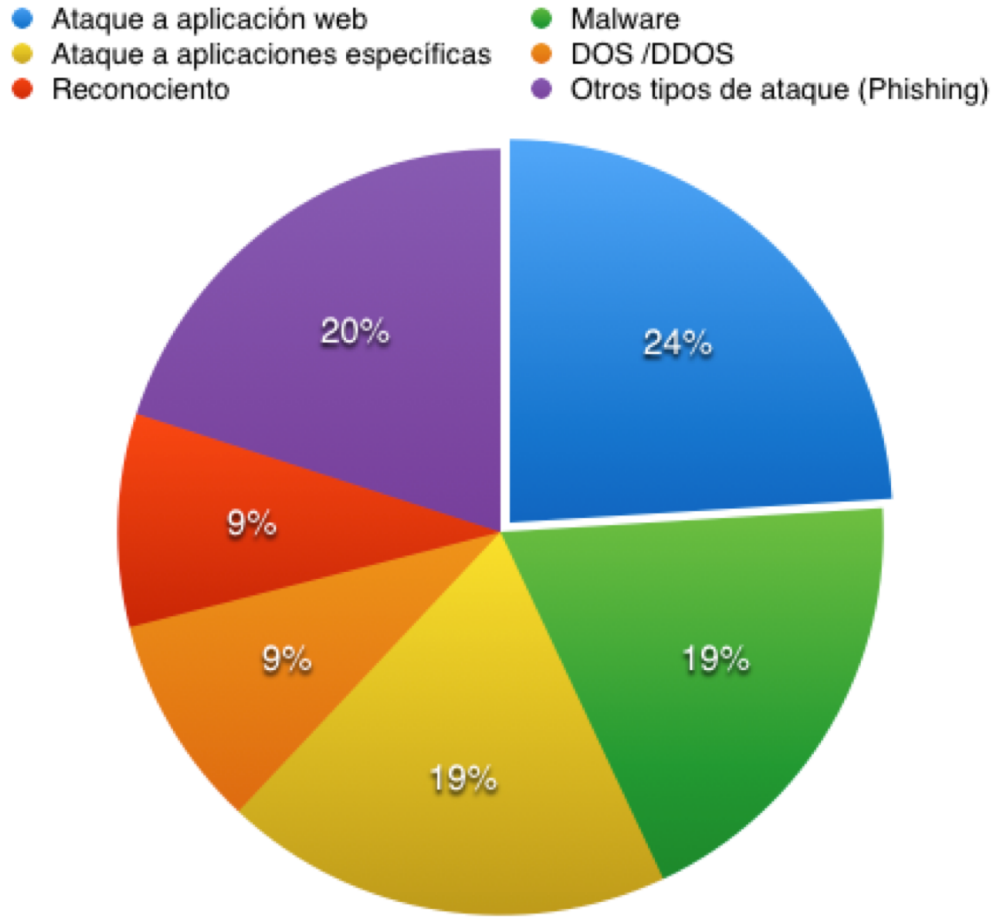


Figura 43. Índices de frecuencia de ataques por tipo
Tomado de SERT Quarterly Threat Report Q2, 2016

De igual manera las industrias más afectadas por estos ataques son las de salud con un 17%, ventas (18 %) y educación (14%) por la vulnerabilidad que pueden existir en este tipo de sistemas debido a la convivencia de equipos de diferente

clase y que requieren un configuración flexible carente de estabilidad y por tanto con puertas de ataque simples para un usuario con gran conocimiento de estas plataformas, sin embargo incluso en estos entornos variables es necesario la colaboración de herramientas de planeación que permitan generar datos tipo de posibles ataques y alertar de los mismos en un tiempo prudencial para los operadores de TI (SERT Quarterly Threat Report Q2. 2016, p. 6).

4.1.4 Ataques Ejemplo

- Ataque de aplicación web

Origen de Ataque: Via WAN y LAN
Rama de Impacto: Servicios al usuario
Plataforma: Web
Negocios más afectados: Ventas, Aplicaciones de colaboración, Finanzas

Las variaciones comunes de este ataque es la inyección SQL o SQLi (45% del total de la categoría), adicionalmente se encuentran comandos de tipo XSS generados entre sitios web.
SQLi se produce cuando el ciberatacante inyecta una instrucción o sentencia maliciosa en un formulario web destinado a ser almacenado en una plataforma con estructura de base de datos, al lograr acertar en alguna sentencia SQL, el atacante tiene la posibilidad de extraer información de la empresa incluyendo datos sensibles como nombres de clientes, teléfonos o tarjetas de crédito registradas. (Boyd, S. W., & Keromytis, A. D., 2004, sp)

En el apartado de XSS y comandos de interacción de datos entre sitios web son una vulnerabilidad común que los hackers pueden explotar a fin de alterar secuencias de conexión entre aplicativos web e información personal que se encuentra en transacción al momento del ataque.

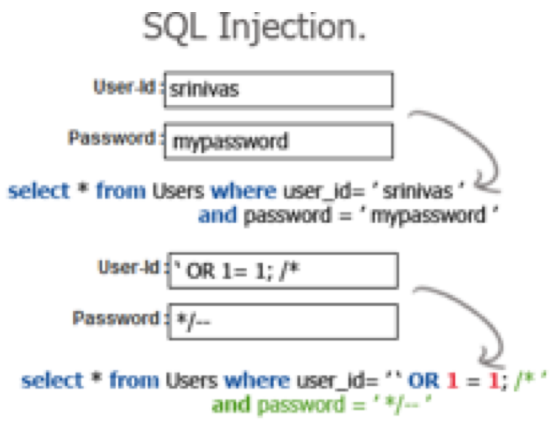


Figura 44. Ejemplo ataque de aplicación web con SQLi
Tomado de 9lessons. 2016

A manera de prevención y como medida de verificación ante un ataque se puede comprobar si el sistema cuenta con API (Identificador de aplicación para el usuario), lo cual permite identificar el ataque de manera más específica por medio del número de esta clave.

Para poder comprobar este ataque se realiza una ejecución de la herramienta de OSSIM para análisis autónomo de vulnerabilidades (Figura 45) identificando una intrusión Cold Fusion relacionada con el servidor web y su base de datos tal y como se menciona en el procedimiento de este ataque

DATE	EVENT NAME	RISK	DATA SOURCE	SENSOR	OTX	SOURCE IP	DEST IP
2016-11-20 18:31:57	AlienVault NIDS: "ET WEB_SERVER ColdFusion administrator access"	0	AlienVault NIDS	alienvault	N/A	Host-192-168-0-80:49211	CM-SRV01:32469
2016-11-20 18:31:57	AlienVault NIDS: "ET WEB_SERVER ColdFusion administrator access"	0	AlienVault NIDS	alienvault	N/A	Host-192-168-0-80:49204	CM-SRV01:80

Figura 45. Ejemplo ataque de aplicación web con SQLi en Ossim

En la imagen anterior (Figura 45), se muestra la secuencia registrada por Ossim al momento de identificar un ataque cold fusion, lo que muestra un panorama más claro a la hora de tomar una decisión desde el momento de preparación del servidor previo a la entrada en producción del mismo.

- Malware

Origen de Ataque: WAN
Rama de Impacto: Equipo final del usuario
Plataforma: Sistema Operativo Anfitrión
Negocios más afectados: Entorno empresarial, Educación, Manufactura, Ventas

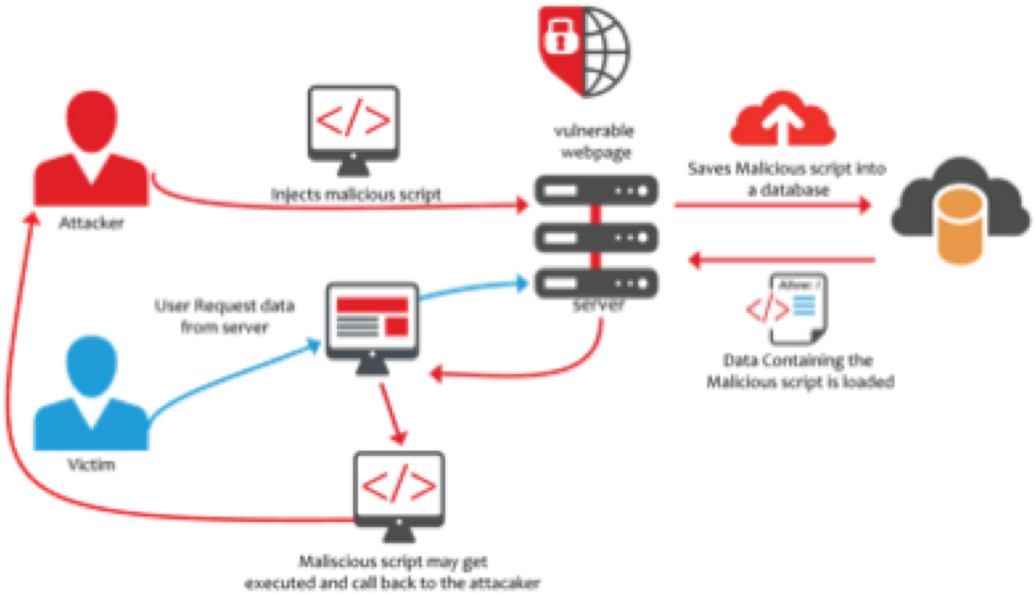


Figura 46. Estructura genérica de malware
Tomado de SecPoint, 2016.

El ataque de malware (Figura 46), viene dado en diferentes formas y grados de penetración, desde un simple virus o gusanos hasta ataques más complejos como spyware o ransomware. Es necesario manifestar que ninguna infraestructura está libre de malware.

En este tipo de ataque el papel del usuario final es vital para mantener la arquitectura empresarial a salvo puesto que este individuo es en último caso el rector de su entorno laborar informático y la persona que toma decisiones sobre que sitios web o documentos se pueden visualizar en su máquina. Actualmente las grandes empresas emplean las capacitaciones como herramienta de

mitigación educando a los usuarios de manera efectiva sobre las normas básicas para evitar una intrusión a la plataforma empresarial. (Chen, Z., & Ji, C., 2009, p. 532)

Para comprobar este ataque en la plataforma OSSIM, se toma un enfoque de pentesting, o ataque de penetración, en el cual por medio de la herramienta NESSUS (Figura 47), se muestran las brechas de seguridad, e identificando las mismas se puede incluso llegar a tener el control del equipo dentro de una botnet. Adicionalmente se muestra en la figura 48 cuáles son los ataques más propensos dentro de la rama del Malware.

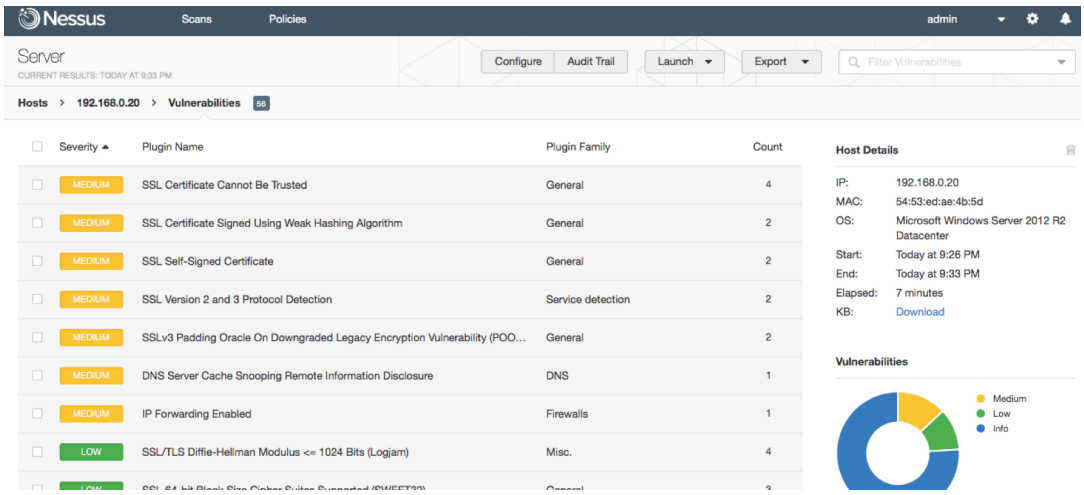


Figura 47. Detección de vulnerabilidades con Nessus (simulación Malware)

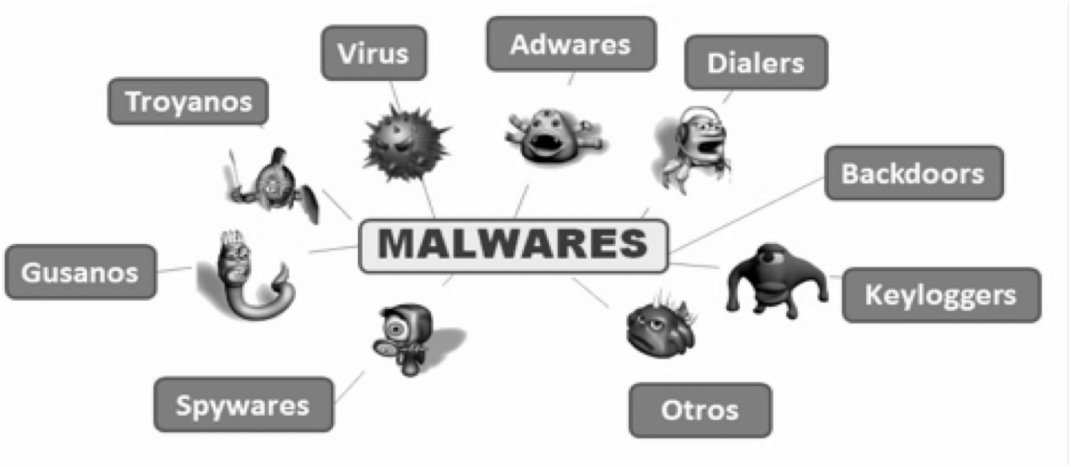


Figura 48. Malwares
Tomado de MalwareTips. 2016.

- Ataques específicos de aplicación

Origen de Ataque: WAN y LAN
Rama de Impacto: Equipo de usuario, Plataformas Cliente-Servidor
Plataforma: Sistema Operativo Anfitrión, Infraestructura de procesamiento de datos
Negocios más afectados: Educación, Salud, Tecnología, Manufactura

En la infraestructura de colaboración en línea de carácter empresarial los ataques específicos de aplicaciones propias del negocio son un factor a considerar puesto que son blancos fáciles para ciberatacantes, debido a su arquitectura cliente servidor, el tráfico de paquetes en este caso puede ser monitoreado por el atacante a fin de obtener información del usuario. (Chen, Z., & Ji, C., 2009, p. 45)

La técnica de sniffer por medio de uso de monitores de paquetes como por ejemplo wireshark (Figura 49), que por lo general se usa para estos ataques, permite obtener datos de sistemas operativos, tráfico de red promedio, así como también información de otras aplicaciones o programas en uso. Para este tipo de ataque es necesario tener en cuenta las principales vulnerabilidades de la

configuración típica del usuario final, puesto que el atacante al encontrar un punto de entrada por medio de una vulnerabilidad específica puede aumentar la tasa de éxito del ataque.

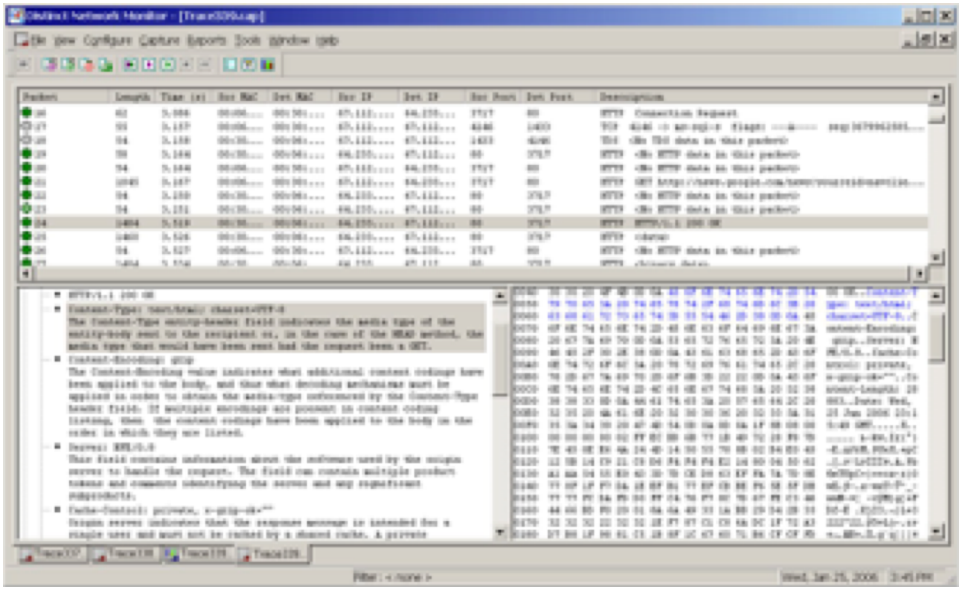


Figura 49. Uso de Wireshark
Tomado de Wireshark ORG, 2016

- Ataques DDoS

Origen de Ataque: WAN y LAN (LAN casi inexistente)
Rama de Impacto: Servidores
Plataforma: S.O Servidor
Negocios más afectados: Tecnología (Servicios de cloud y plataformas colaborativas)

El ataque DDoS se genera por una sobrecarga de peticiones hacia el servidor, se usa botnets (Figura 50) para generar este tráfico a diferencia de DoS que se genera en un solo cliente. Por lo general este ataque es mitigado por elementos de infraestructura de red como routers o switches, evitando colapsar el enlace de datos. (Feinstein, L., Schnackenberg, D., Balupari, R., & Kindred, D., 2003, p. 307)

De igual manera la herramienta de supervisión de ataques detecta por protocolo y por aplicación el tipo de tráfico en la red, y en base a su AKDB puede determinar un tráfico inusual identificado como ataque.

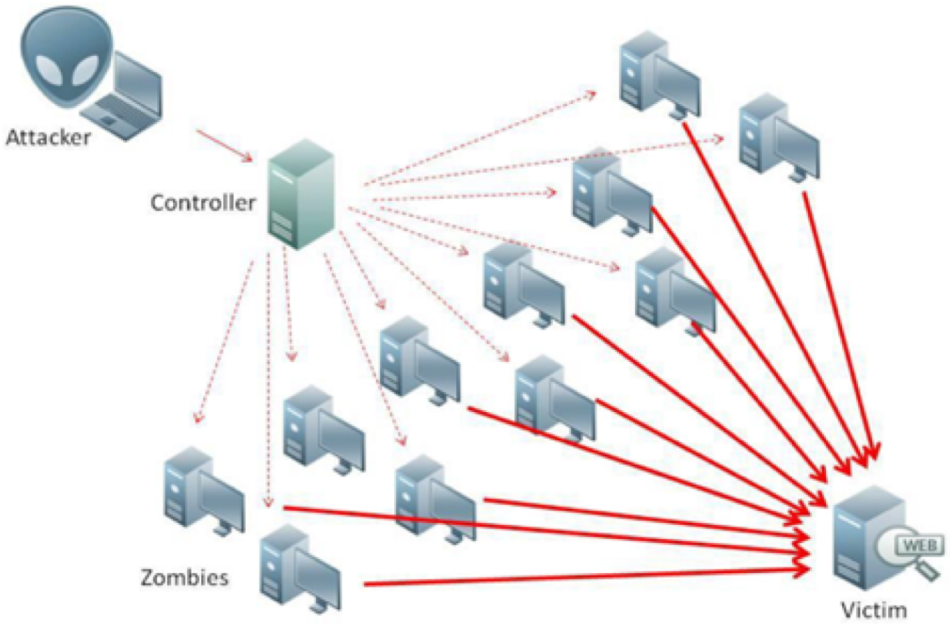


Figura 50. Estructura DDoS por medio de botnet
Adaptado de Invalid Expresion, 2016

Para demostrar este ataque se usa en el escenario propuesto la herramienta LOIC (Figura 51), un ejecutable de libre descarga que genera tráfico http, ftp, y telnet al servidor a ser atacado tratando de que este sature sus peticiones y el servicio quede dado de baja.

- Reconocimiento

Origen de Ataque: WAN y LAN
Rama de Impacto: Equipo de usuario
Plataforma: Sistema Operativo Anfitrión
Negocios más afectados: Ventas, Tecnología, Educación, Finanzas, Plataformas de juegos

El ataque de reconocimiento permite una visión general de un escenario a atacar y es considerado uno de los peores ataques que puede sufrir una red ya que es silencioso al tiempo que causa gran efectividad (Figura 52).

Dentro de su aplicación se encuentra el tipo activo y pasivo.

En el caso del ataque pasivo, el atacante busca información privada sin comprometer un sistema de la víctima, por otro lado, el ataque activo si afecta a la infraestructura base del usuario, sin embargo, ambos tipos de ataques se consideran preparativos para una intrusión mayor. (Uma, M., & Padmavathi, G., 2013).

La prevención por medio de la herramienta de supervisión es asociada a la configuración simultánea de un firewall o IPS para filtrar el tráfico al tiempo que se genera un informe sobre posibles intrusiones de este tipo por parte de OSSIM.

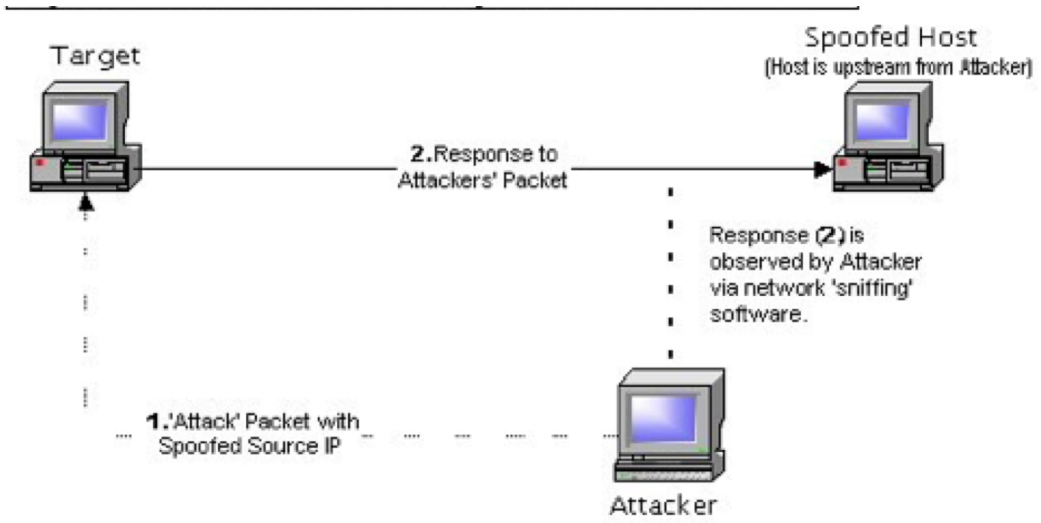


Figura 51. Ataque de reconocimiento (Genérico)
Tomado de: SANS ORG. 2016

Para lograr demostrar este ataque necesitamos de un conjunto de exploits que analizan el equipo infectado generando así datos que se puedan usar para alterar el libre funcionamiento, con la herramienta metaexploit (Figura 53), tras

una intrusión por medio de técnicas de hacking ético, podemos determinar qué tipo de vulnerabilidades el atacante puede obtener de un sistema.

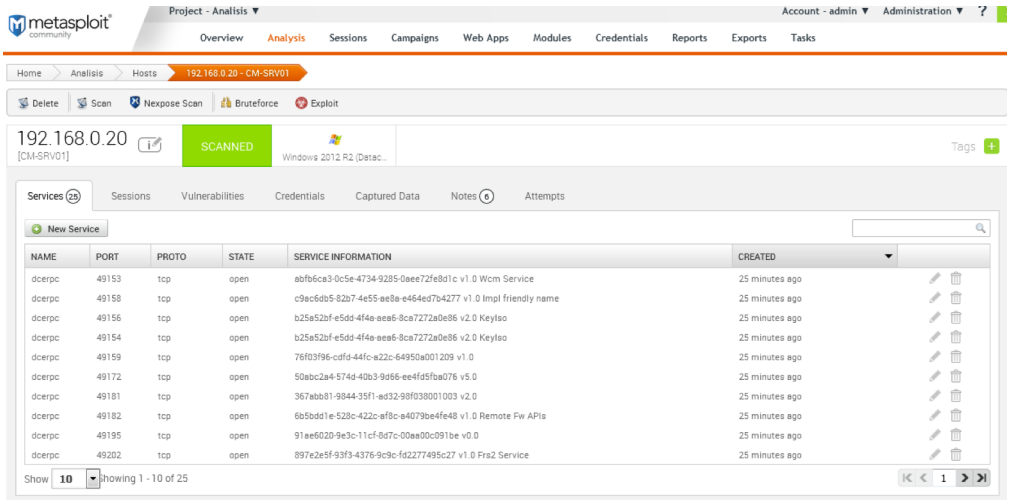


Figura 52. Ataque con Metasploit

Por último y como comprobación a cada uno de estos ataques tras el análisis de los mismos se tiene un aumento considerable de tráfico en la plataforma que diferencia mucho del promedio regular, este a su vez es otro indicativo de primera mano sobre la saturación de la red, sin embargo, no siempre se debe a un ataque de cualquier tipo descrito anteriormente de ahí la conformación por informes de ataques y por otros parámetros dentro de OSSIM.

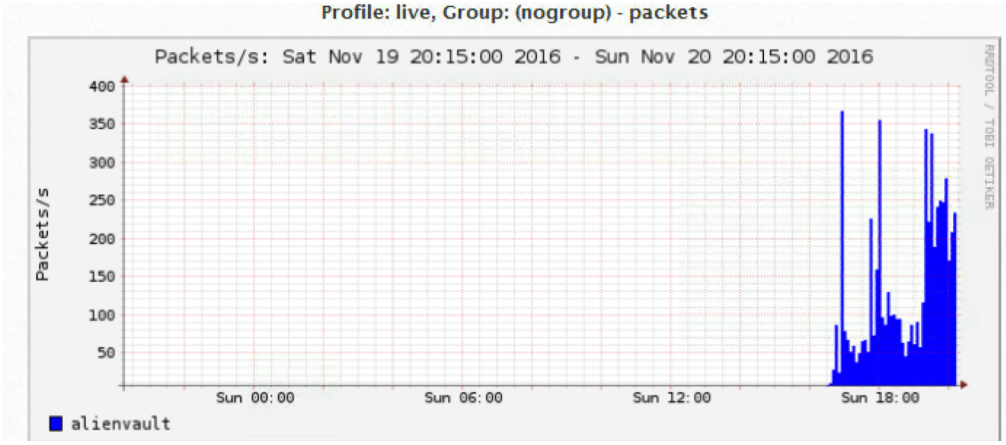


Figura 53. Tráfico de paquetes durante los ataques (Promedio)

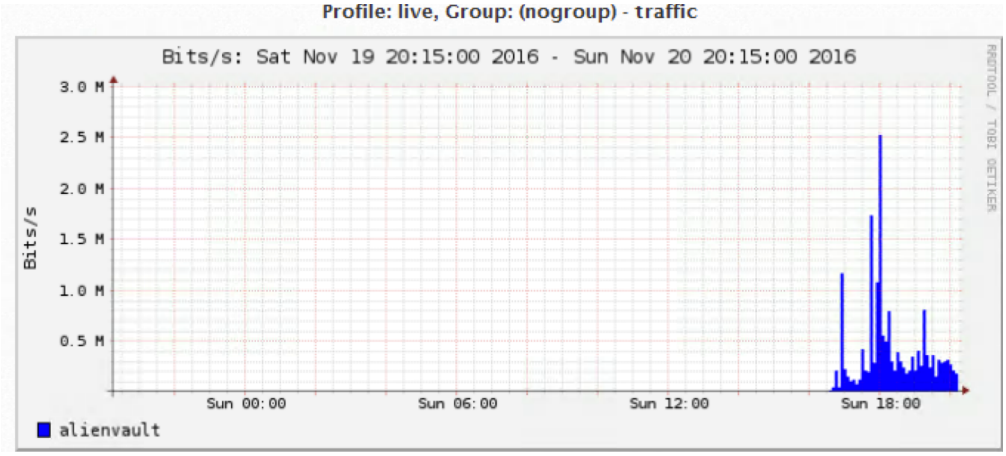


Figura 54. Tráfico Mbps durante el ataque

4.1.5 Vulnerabilidades ISO27000

Tras los ataques realizados por software de terceros, operando bajo el mismo paradigma de SIEM, se debe identificar el comportamiento de la solución ante este tráfico imprevisto, adicionalmente se considerar las vulnerabilidades de usuario en base a la normativa ISO27000 (ver anexo 6).

Según la normativa ISO27000 y su apartado correspondiente al presente análisis, ISO 27002:2013 en general para este tipo de implementaciones se consideran aplicables los siguientes puntos:

- Control 5
  - Directrices de seguridad de la Información.
  - Conjunto de políticas de seguridad de la información.
  - Revisión de políticas de seguridad de la información.
- Control 6
  - Política de uso de dispositivos para movilidad.
- Control 9
  - Política de control de accesos.
  - Control de acceso a redes y servicios asociados.
  - Gestión de los derechos de acceso.
  - Uso de información confidencial para autenticación y registro (usuario).
  - Control de acceso a soluciones empresariales.
  - Uso de herramientas de administración de sistemas.
- Control 10
  - Cifrado y gestión de claves.
- Control 12
  - Responsabilidades y procesos de operación.
  - Separación de entornos de desarrollo, prueba y producción.
  - Protección contra código malicioso.
  - Copias de seguridad de logs.
  - Registros de actividad de administradores y operadores del sistema.
  - Controles de auditoría de los sistemas de información.
- Control 13
  - Control de seguridad de red.
  - Segregación de redes.
  - Mensajería Electrónica.

    - Acuerdos de confidencialidad.
- Control 14
    - Análisis de requisitos de seguridad.
    - Seguridad en comunicaciones sobre plataformas públicas.
    - Protección de transacciones por redes telemáticas.
    - Pruebas de aceptacón.
- Control 16
    - Gestión adecuada de incidentes.
    - Notificación oportuna de eventos de seguridad de la información.
    - Notificación de vulnerabilidades.
    - Respuesta ante incidentes de seguridad.
    - Recopilación de evidencias y registros.
- Control 18
    - Protección de registros de la organización.
    - Revisión independiente de las políticas de seguridad de la información.
    - Cumplimiento de normas de seguridad.

4.2 Comportamiento de OSSIM, e identificación de riesgos (alarmas)

OSSIM, por su creación orientada a la recopilación de datos e información para toma de decisiones críticas en la seguridad de la red cuenta con un desempeño fluido en sus tareas, puesto que en caso de un ataque es necesario tener un registro de alertas e informes que permitan decidir sobre los procedimientos destinados para estas contingencias.

Ossim y su informe ejecutivo previo a los ataques se lo encuentra en el anexo 2, este documento muestra las vulnerabilidades que con los ataques se demuestran como ejemplos de penetración en los sistemas del escenario planteado.

Los informes generados por la herramienta OSSIM tras los ataques se los puede observar en los anexos 3, 4 y 5 de acuerdo al orden de los ataques ejecutados.

5. Conclusiones y Recomendaciones

5.1 Conclusiones

Las redes de datos actuales manejan una alta convergencia a nivel de servicios y aplicaciones críticas para el negocio, el contar con políticas de seguridad basadas en normas internacionales permite mantener el control de usuarios y de trafico circulante por la red por medio de complementos de monitoreo basados en software.

La implementación de una solución de seguridad en la nube está ligada a la empresa por dos amplios frentes; por un lado el costo de la renta de infraestructura cloud, y a la par la velocidad de conexión a internet que se pueda establecer entre el punto remoto y las oficinas centrales que requieren del servicio, por tanto es necesario diferenciar e identificar el tipo de red que se requiere en el entorno laboral de manera que la implementación en nube o en entorno local de la solución de supervisión (Máquina Virtual o Servidor) se encuentre optimizada para el correcto funcionamiento la solución OSSIM o cualquier otro tipo de tráfico.

En el entorno empresarial es necesario contar con una base de conocimientos sobre las incidencias de ataques no solo a la infraestructura de red local, sino también contar con un marco de referencia global; en este apartado y bajo el desarrollo de la plataforma de AlienVault conocida como OTX, la solución OSSIM, puede extraer datos de ataques e informes que fusionando el proceso de detección local con casos similares logran descubrir una interrelación de ataques e incluso detectarlos antes de que ocurran y suspendan los servicios del negocio.

Si bien es cierto el despliegue de la solución de seguridad basada en SIEM no es complejo, requiere de pasos previos de evaluación de compatibilidad con los equipos de hardware de la empresa y a la par con las políticas descritas en los reglamentos de manejo de la información a fin de adaptar el

sistema a los requerimientos particulares de cada grupo de usuarios, evitando alarmas falsas sobre tráfico y accesos que se encuentran aprobados dentro de la infraestructura de red local.

OSSIM es una herramienta de colaboración global y sus funciones actuales se encuentran en desarrollo, si bien es cierto en instancias básicas puede bloquear ciertas peticiones a los equipos supervisados por sus agentes, en un ataque masivo sirve como herramienta de toma de decisiones, no como un sistema IPS o IDS, debido a que su programación se limita a la supervisión de red con tareas puntuales.

La suite de herramientas de OSSIM está diseñada para generar distintos tipos de ataques a la topología de red, sin embargo la versión community o gratuita de este sistema cuenta con limitantes como la generación de alarmas y riesgos en tiempo real; por tanto en un mediana o gran empresa es necesario diferenciar las versiones y considerar adquirir una licencia de servicio, de manera que la supervisión se encuentre respaldada por el proveedor y se puedan ejecutar todos los complementos para el correcto funcionamiento de la herramienta durante un incidente de violación de seguridad.

Al seleccionar OSSIM como la herramienta de supervisión no solo se obtiene el monitoreo de ataques sino también el monitoreo de red, por tanto, el costo de un sistema adicional para monitoreo centralizado de los equipos se anula disminuyendo el consumo de recursos de hardware y económicos.

El retardo que puede llegar a experimentar la red de datos ya configurada políticas de servicio es mínimo debido a que el protocolo SNMP tuvo un desarrollo sobre redes de baja transferencia de datos lo cual ha mantenido el flujo de los mismos en una pequeña porción de información

Al generar los ataques a la solución de seguridad, se destaca la rapidez con la que el sistema elabora un informe sobre el ataque y su nivel de penetración dentro del sistema incluidos lineamientos para la contención del mismo.

Al implementar la solución en una máquina virtual local (Sede Central, no cloud), se nota que el tiempo de latencia de conexión es menor a 3ms, lo que evita enviar paquetes de sensores por el enlace de internet y reducir distancias al servidor de OSSIM.

La compatibilidad de plataforma permite que el usuario registre infinidad de dispositivos y cuente con una lectura de cada uno de ellos incluso si no soportan el protocolo SNMP, lo cual permite contar con una base actualizada y en tiempo real de dispositivos conectados a la red en caso de detectar algún equipo no autorizado.

Pese a no existir necesidad de explorar el canal de conexión con el ISP, la herramienta genera de igual manera logs e incluso actúa en casos básicos como un sistema de firewall bloqueando peticiones que no son autorizadas dentro de la red o incluso mitigando posibles intrusiones del lado del proveedor de servicios.

5.2 Recomendaciones

Es necesario evaluar de manera adecuada los requerimientos de software descritos en la presente investigación, debido a que el impacto de una mala configuración en una distribución de Linux ligada completamente al funcionamiento de la red de datos puede perjudicar la ejecución de diversos procesos tanto en el host anfitrión como en la red local en general.

Al desplegar la solución en una red con diferentes elementos de red, se sugiere implementar grupos de acción dentro de OSSIM, de esta manera las tareas de análisis sobre servicios de red no se mezclan con equipos que solo

ejecutan escaneo de estado de enlace, con lo que se reduce considerablemente la carga de la red con un tráfico innecesario.

Si bien es cierto OSSIM cuenta con un asistente al inicio para configurar a cada uno de los hosts que el sistema encuentra dentro de la subred que se va a configurar para supervisar, es importante por medidas de seguridad obviar esta configuración, debido a que en el proceso de levantamiento de información OSSIM puede agregar dispositivos temporales o equipos que no soportan el despliegue de SIEM, por eso es necesario primero recabar la información del equipamiento destino a la supervisión y posteriormente hacer un despliegue manual sobre la infraestructura garantizando la documentación y registro en el sistema de los elementos que necesitan del servicio OSSIM y no de cualquier tipo de máquina.

La gerencia, mantenimiento y acceso al sistema por parte del equipo de IT debe ser controlado bajo las políticas ISO27000 de acceso a usuarios definidas en el presente documento puesto que la información que maneja el servidor es altamente sensible y recopila la data de cada uno de los equipos del core de negocio.

Se recomienda la adquisición de la versión Premium de la herramienta, debido a que para un primer despliegue es importante que el usuario administrador cuente con una guía a manera de entrenamiento con todas las funciones que puede realizar la plataforma, de esta manera su funcionamiento se puede optimizar evitando falsas alarmas o la identificación incorrecta de sensores de monitoreo y dispositivos del usuario.

Referencias

Alemán-Novoa, H. C. I. (2015). *Metodología para la implementación de un sgsi en la fundación universitaria Juan de Castellanos, bajo la norma ISO 27001: 2005.*

Ángel, A., & Galo, J. (2016). *Análisis de la plataforma ossim para la administración de red en la seguridad de computadoras, detección y prevención de intrusos* (Doctoral dissertation, Universidad de Guayaquil Facultad de Ciencias Matemáticas y Físicas Carrera de Ingeniería en Networking y Telecomunicaciones).

Balarezo Chávez, A. F., & Poveda Pilatasig, D. X. (2015). *Propuesta de mejoramiento de la herramienta ossim siem (Open Source), para obtener los niveles óptimos de gestión en la administración de la seguridad, en una red implementada en cloud computing.*

Bravo Bravo, A. H., & Villafuerte Quiroz, A. L. (2015). *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.*

Bernstein, P. A. (1996). *Middleware: a model for distributed system services.* Communications of the ACM

Bowling, J. (2010). *Alienvault: the future of security information management.* Linux Journal, 2010

Boyd, S. W., & Keromytis, A. D. (2004, June). *SQLrand: Preventing SQL injection attacks. In International Conference on Applied Cryptography and Network Security* Springer Berlin Heidelberg.

Chen, Z., & Ji, C. (2009). *An information-theoretic view of network-aware malware attacks*. IEEE Transactions on Information Forensics and Security.

Córdoba Suárez, A. E. (2015). *Diseño e implementación de un GGSI para el área de informática de la curaduría urbana segunda de pasto bajo la norma ISO/IEC 27001.*

Disterer, G. (2013). *ISO/IEC 27000, 27001 and 27002 for information security management.*

Feinstein, L., Schnackenberg, D., Balupari, R., & Kindred, D. (2003, April). *Statistical approaches to DDoS attack detection and response. In DARPA Information Survivability Conference and Exposition, 2003. Proceedings* IEEE.

Hermanowski, D. (2015, June). *Open Source Security Information Management System Supporting IT Security Audit. In Cybernetics (CYBCONF)*, 2015 IEEE 2nd International Conference on IEEE.

Madrid Molina, J. M., Múnera Salazar, L. E., Montoya González, C. A., Osorio Betancur, J. D., Cárdenas, L. E., Bedoya, R., & Latorre, C. (2016). *Implementación y mejora de la consola de seguridad informática OSSIM: una experiencia de colaboración universidad-empresa.*

Marino, R. A. (2010). *Conectados en el ciberespacio. Editorial UNED*.

Meyer, C. O. *El factor Gente y Seguridad de la Información.*

Mieres, J. (2009). *Ataques informáticos. Debilidades de seguridad comúnmente explotadas)*. Recuperado el 24 de Noviembre del 2016 de http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf.

Miller, D., Harris, S., Harper, A., VanDyke, S., & Blask, C. (2010). *Security information and event management (SIEM) implementation*. McGraw Hill Professional.

Mirkovic, J., Prier, G., & Reiher, P. (2002, November). *Attacking DDoS at the source. In Network Protocols, 2002. Proceedings. 10th IEEE International Conference on* IEEE.

Morelli, A. *Apuntes para una charla sobre la administración del conflicto internacional en el ciberespacio.*

NTTSecurity. (2016). *SERT Quarterly Threat Report Q2 2016.*

Northia, A., & Javier, A. (2016). *Implementación de un servidor para la gestión de seguridad de la información y de eventos, integrado con la infraestructura de una empresa importadora y comercializadora de suministros eléctricos y servicios especializados, como salvaguarda del plan de riesgos informáticos (Master's thesis, Espol).*

O'Gorman, G., & McDonald, G. (2012). *Ransomware: A growing menace*. Symantec Corporation.

Pantaleone, F. M., & Silva, M. N. (2012). *Impacto de la ISO 27.000 en organizaciones: Estudio comparativo de herramientas para la implementación de un SGSI (Doctoral dissertation, Facultad de Informática).*

Párrizas, A. (2005). *Propuesta de una arquitectura de sistemas de detección de intrusos con correlación* (Doctoral dissertation, Ph. D. dissertation, Universidad de Valencia, Escola Técnica Superior de Enginyeria, Valencia).

Pavlik, J., Komarek, A., & Sobeslav, V. (2014, November). *Security information and event management in the cloud computing infrastructure. In Computational Intelligence and Informatics* (CINTI), 2014 IEEE 15th International Symposium on IEEE.

Rodríguez, J. M. R., & Campillo, M. J. D. (2003). *Sistemas de información: aspectos técnicos y legales. Universidad de Almería.*

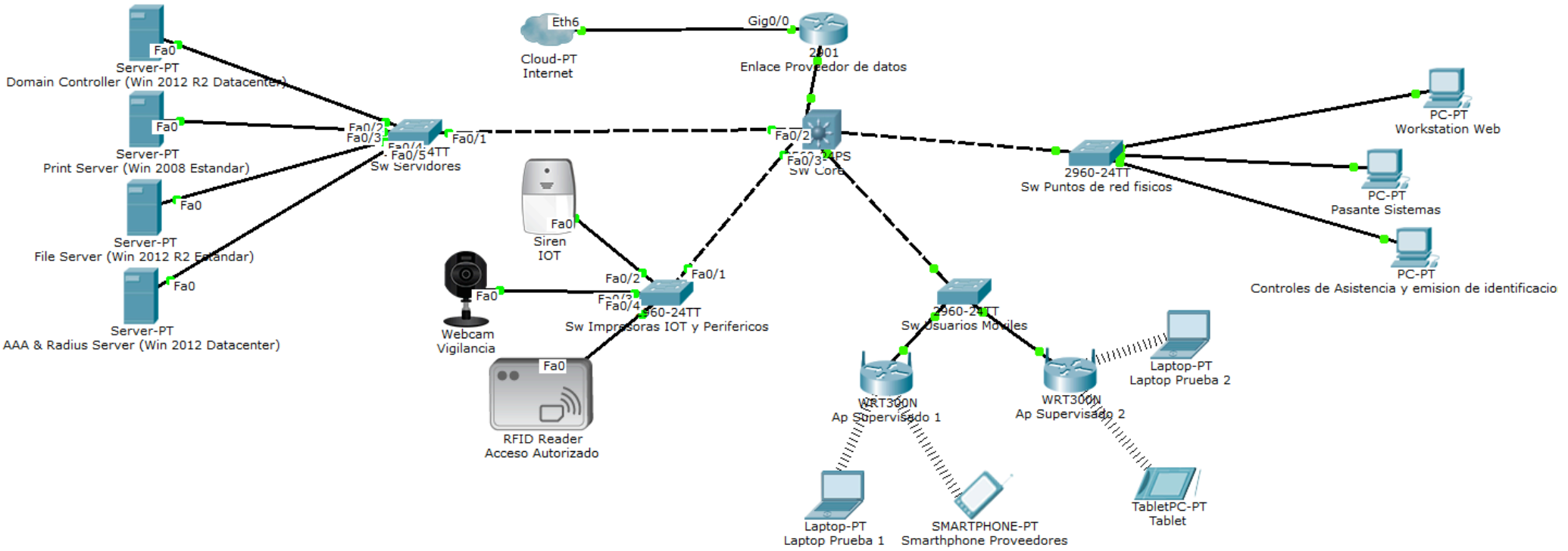
So-In, C., Mongkonchai, N., Aimtongkham, P., Wijitsopon, K., & Rujirakul, K. (2014, May). *An evaluation of data mining classification models for network intrusion detection. In Digital Information and Communication Technology and it's Applications (DICTAP), 2014 Fourth International Conference on*. IEEE.

Uma, M., & Padmavathi, G. (2013). *A Survey on Various Cyber Attacks and their Classification*. *IJ Network Security*.

Wegner, H. (2014). *La ciberseguridad en la Unión Europea*. Boletín Electrónico del Instituto español de Estudios Estratégicos.

ANEXOS

ANEXO 1


Server-PT
Domain Controller (Win 2012 R2 Datacenter)
Server-PT
Print Server (Win 2008 Estandar)
Server-PT
File Server (Win 2012 R2 Estandar)
Server-PT
AAA & Radius Server (Win 2012 Datacenter)
Fa0
Fa0/1
Fa0/2
Fa0/3
Fa0/5
Sw Servidores
Cloud-PT
Internet
Eth6
Gig0/0
2901
Enlace Proveedor de datos
Fa0/2
Fa0/3
Sw Core
Siren
IOT
Webcam
Vigilancia
RFID Reader
Acceso Autorizado
Fa0/4
Sw Impresoras IOT y Perifericos
2960-24TT
Sw Usuarios Moviles
WRT300N
Ap Supervisado 1
WRT300N
Ap Supervisado 2
Laptop-PT
Laptop Prueba 1
SMARTPHONE-PT
Smarthphone Proveedores
Laptop-PT
Laptop Prueba 2
TabletPC-PT
Tablet
2960-24TT
Sw Puntos de red fisicos
PC-PT
Workstation Web
PC-PT
Pasante Sistemas
PC-PT
Controles de Asistencia y emision de identificacio

ANEXO 2

SIEM Events

I.T. Security

Address

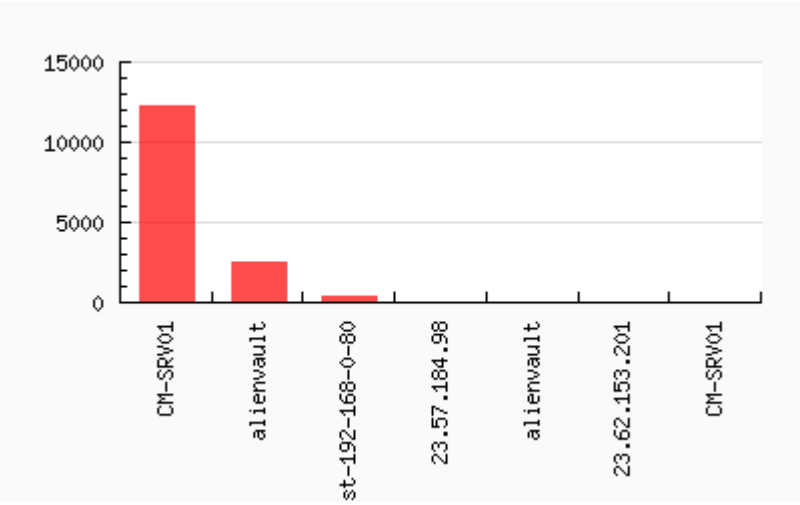
Tel. **Report Date** 2016-11-20 20:56:35

Report Filter Date from: 2016-10-22 Date to: 2016-11-21

Assets Selected: All Assets

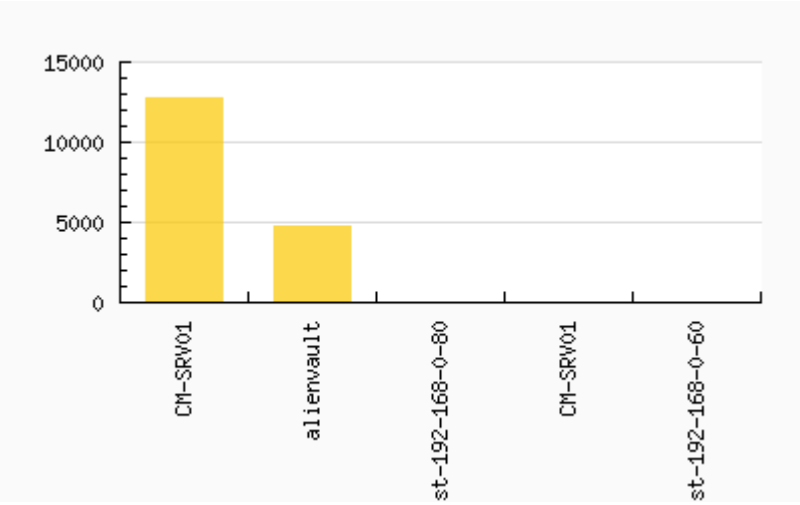
SIEM Events - Top 10 Attacker Host from: 2016-10-22 to: 2016-11-21

Host	Occurrences
CM-SRV01	12.241
alienvault	2.550
Host-192-168-0-80	377
23.57.184.98	23
alienvault	4
23.62.153.201	4
CM-SRV01	2



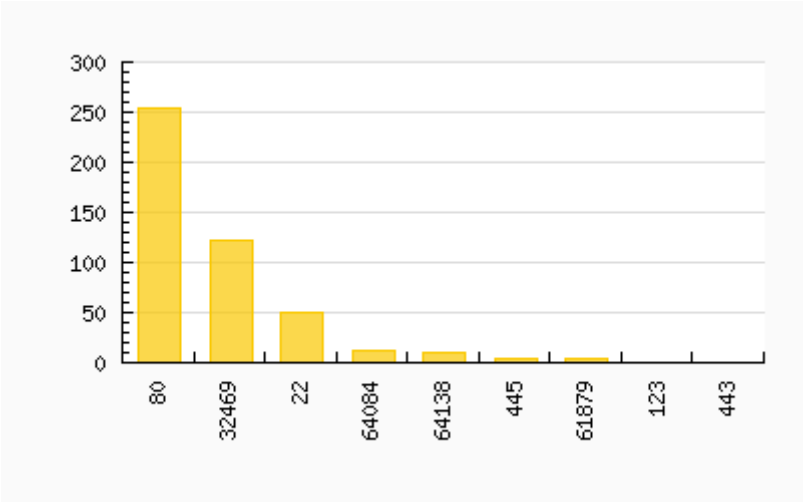
SIEM Events - Top 10 Attacked Host from: 2016-10-22 to: 2016-11-21

Host	Occurrences
CM-SRV01	12.709
alienvault	4.759
Host-192-168-0-80	28
CM-SRV01	6
Host-192-168-0-60	1



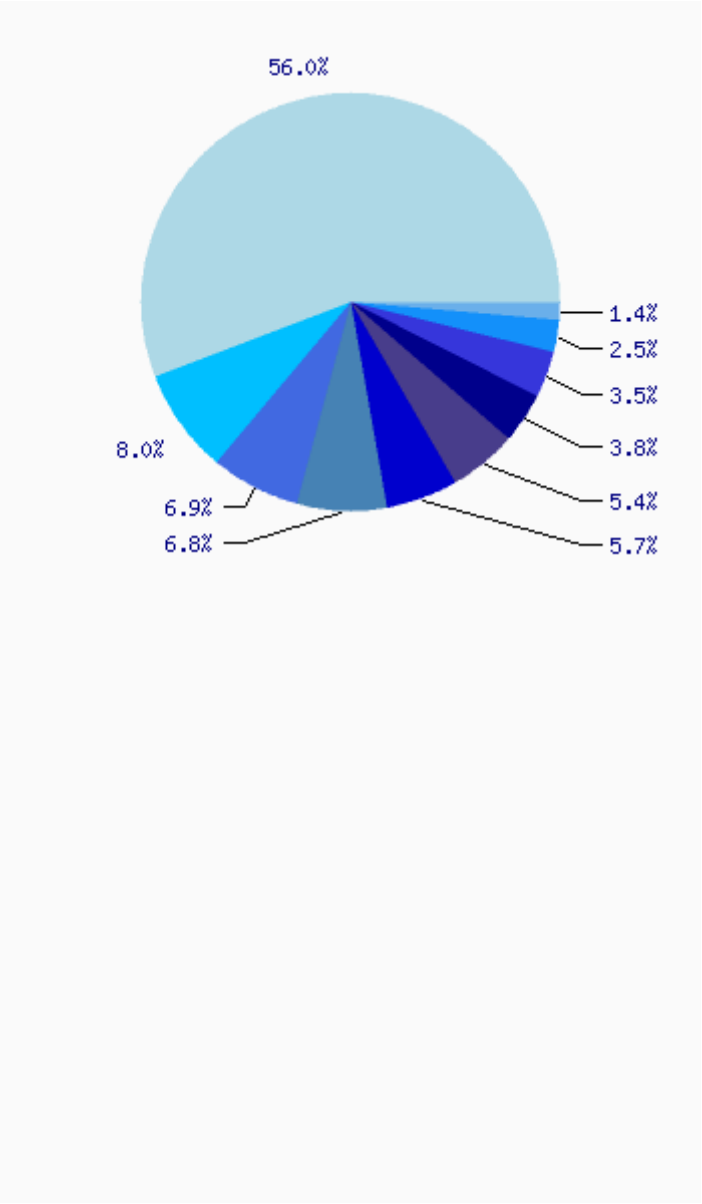
SIEM Events - Top 10 Used Ports from: 2016-10-22 to: 2016-11-21

Port	Service	Occurrences
80	http	255
32469	unknown	122
22	ssh	50
64084	unknown	12
64138	unknown	11
445	microsoft-ds	5
61879	unknown	4
123	ntp	1
443	https	1



SIEM Events - Top 15 Events from: 2016-10-22 to: 2016-11-21

Event	Occurrences
AlienVault HIDS: Windows error event.	9.494
AlienVault HIDS: Multiple Windows error events.	1.352
sudo: Session opened	1.166
sudo: Session closed	1.160
AlienVault HIDS: Login session opened.	969
AlienVault HIDS: Login session closed.	912
AlienVault HIDS: Windows machine logon.	646
AlienVault HIDS: Windows machine logoff.	598
AlienVault HIDS: Integrity checksum changed.	425
AlienVault NIDS: "ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers"	241
AlienVault HIDS: Logon Failure - Unknown user or bad password.	150
AlienVault NIDS: "ET WEB_SERVER Possible CVE-2014-6271 Attempt"	120
AlienVault HIDS: Windows User Logoff.	57
AlienVault HIDS: Successful sudo to ROOT executed	52
sudo: Command executed	52



SIEM Events - Top 15 Events by Risk from: 2016-10-22 to: 2016-11-21

Event	Risk
AlienVault HIDS: New HIDS agent connected.	
AlienVault NIDS: "ET WEB_SERVER Possible IIS Integer Overflow DoS (CVE-2015-1635)"	
Host operating system change	
AlienVault HIDS: Windows machine logon.	
AlienVault HIDS: Windows Logon Success.	
Host service change	
AlienVault HIDS: Windows machine logoff.	
AlienVault NIDS: "ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers"	
AV-FREE-FEED Bruteforce attack, Windows authentication attack against DST_IP	
AlienVault HIDS: Windows Audit event.	
AlienVault NIDS: "ET POLICY PE EXE or DLL Windows file download"	
SSHd: Connection closed	
AlienVault NIDS: "ET POLICY Http Client Body contains pass= in cleartext"	
AlienVault NIDS: "ET WORM UPX compressed file download - possible worm"	
sudo: Session opened	

ANEXO 3

Nessus Report

Nessus Scan Report

Sun, 20 Nov 2016 21:33:49 EST

Table Of Contents

Hosts Summary (Executive)....3
- 192.168.0.20....4

Hosts Summary (Executive)

192.168.0.20

Summary

Critical	High	Medium	Low	Info	Total
0	0	7	6	43	56

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.8)	50686	IP Forwarding Enabled
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Low (3.3)	94046	UPnP File Share Detection
Low (3.3)	94047	UPnP API Listing
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low (2.6)	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
Low (2.6)	94437	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10386	Web Server No 404 Error Code Check
Info	10394	Microsoft Windows SMB Log In Possible
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	10884	Network Time Protocol (NTP) Server Detection
Info	10940	Windows Terminal Services Enabled
Info	11002	DNS Server Detection

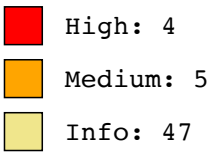
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11935	IPSEC Internet Key Exchange (IKE) Version 1 Detection
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20301	VMware ESX/GSX Server detection
Info	20870	LDAP Server Detection
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	25701	LDAP Crafted Search Request Server Information Disclosure
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35297	SSL Service Requests Client Certificate
Info	35711	Universal Plug and Play (UPnP) Protocol Detection
Info	35712	Web Server UPnP Detection
Info	35716	Ethernet Card Manufacturer Detection
Info	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
Info	43829	Kerberos Information Disclosure
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	62695	IPSEC Internet Key Exchange (IKE) Version 2 Detection
Info	64814	Terminal Services Use SSL/TLS
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	84502	HSTS Missing From HTTPS Server

ANEXO 4

AlienVault: I.T Security Vulnerability Report

Nombre del trabajo:	Scan001	Tiempo de escaneo:	2016-10-02 22:11:40
Perfil:	Default - Non destructive Full and Fast scan	Generado:	2016-10-05 13:48:17

El número total de vulnerabilidades identificadas en 1 sistema(s)



El número total de vulnerabilidades identificadas por sistema

IP equipo	Nombre equipo	Serias	Alto	Med	Bajo	Info
192.168.0.20	Host-192-168-0-20	--	4	5	--	47

192.168.0.20	Host-192-168-0-20

High:

DCE Services Enumeration
Risk: High
Application: msrpc
Port: 135
Protocol: tcp
ScriptID: 10736
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:P
Solution:
filter incoming traffic to this port.
Summary:
Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge
about the remote host.
CVSS Base Score: 5.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2001 Dave Aitel (ported to NASL by rd and Pavel Kankovsky)
Summary: Enumerates the remote DCE services
Version: $Revision: 2837 $

High:

DCE Services Enumeration
Risk: High
Application: msrpc
Port: 135
Protocol: tcp
ScriptID: 10736
Vulnerability Detection Result:
Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge
about the remote host.
Here is the list of DCE services running on this host:
Port: 49152/tcp
UUID: d95afe70-a6d5-4259-822e-2c84da1ddb0d, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49152]
Port: 49153/tcp
UUID: f6beaff7-1e19-4fbb-9f8f-b89e2018337c, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49153]
Annotation: Event log TCPIP
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49153]
Annotation: DHCP Client LRPC Endpoint
UUID: 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49153]
Annotation: DHCPv6 Client LRPC Endpoint
UUID: abfb6ca3-0c5e-4734-9285-0aee72fe8d1c, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49153]
Annotation: Wcm Service
UUID: 30adc50c-5cbc-46ce-9a0e-91914789e23c, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49153]
Annotation: NRP server endpoint
Port: 49154/tcp
UUID: 86d35949-83c9-4044-b424-db363231fd0c, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49154]
UUID: 3a9ef155-691d-4449-8d05-09ad57031823, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49154]
UUID: 98716d03-89ac-44c7-bb8c-285824e51c4a, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49154]
Annotation: XactSrv service
UUID: 1a0d010f-1c33-432c-b0f5-8cf4e8053099, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49154]
Annotation: IdSegSrv service
UUID: a398e520-d59a-4bdd-aa7a-3c1e0303a511, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49154]
Annotation: IKE/Authip API
UUID: 552d076a-cb29-4e44-8b6a-d15e59e2c0af, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49154]
Annotation: IP Transition Configuration endpoint
UUID: 2e6035b2-e8f1-41a7-a044-656b439c4c34, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49154]
Annotation: Proxy Manager provider server endpoint

UUID: c36be077-e14b-4fe9-8abc-e856ef4f048b, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49154]
Annotation: Proxy Manager client server endpoint
UUID: c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49154]
Annotation: Adh APIs
UUID: c9ac6db5-82b7-4e55-ae8a-e464ed7b4277, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49154]
Annotation: Impl friendly name
UUID: 30b044a5-a225-43f0-b3a4-e060df91f9c1, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49154]
Port: 49156/tcp
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49156]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
Endpoint: ncacn_ip_tcp:192.168.0.20[49156]
Annotation: MS NT Directory DRS Interface
UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
Endpoint: ncacn_ip_tcp:192.168.0.20[49156]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : LSA access
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
Endpoint: ncacn_ip_tcp:192.168.0.20[49156]
Annotation: RemoteAccessCheck
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
Endpoint: ncacn_ip_tcp:192.168.0.20[49156]
Annotation: RemoteAccessCheck
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49156]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
Endpoint: ncacn_ip_tcp:192.168.0.20[49156]
Annotation: KeyIso
Port: 49157/tcp
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
Endpoint: ncacn_http:192.168.0.20[49157]
Annotation: MS NT Directory DRS Interface
UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
Endpoint: ncacn_http:192.168.0.20[49157]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : LSA access
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
Endpoint: ncacn_http:192.168.0.20[49157]
Annotation: RemoteAccessCheck
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
Endpoint: ncacn_http:192.168.0.20[49157]

Annotation: RemoteAccessCheck
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncacn_http:192.168.0.20[49157]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
Endpoint: ncacn_http:192.168.0.20[49157]
Annotation: KeyIso
Port: 49158/tcp
UUID: 12345778-1234-abcd-ef00-0123456789ac, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49158]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : SAM access
UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2, version 4
Endpoint: ncacn_ip_tcp:192.168.0.20[49158]
Annotation: MS NT Directory DRS Interface
UUID: 12345778-1234-abcd-ef00-0123456789ab, version 0
Endpoint: ncacn_ip_tcp:192.168.0.20[49158]
Named pipe : lsass
Win32 service or process : lsass.exe
Description : LSA access
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
Endpoint: ncacn_ip_tcp:192.168.0.20[49158]
Annotation: RemoteAccessCheck
UUID: 0b1c2170-5732-4e0e-8cd3-d9b16f3b84d7, version 0
Endpoint: ncacn_ip_tcp:192.168.0.20[49158]
Annotation: RemoteAccessCheck
UUID: 12345678-1234-abcd-ef00-01234567cffb, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49158]
Named pipe : lsass
Win32 service or process : Netlogon
Description : Net Logon service
UUID: b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86, version 2
Endpoint: ncacn_ip_tcp:192.168.0.20[49158]
Annotation: KeyIso
Port: 49159/tcp
UUID: 12345678-1234-abcd-ef00-0123456789ab, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49159]
Named pipe : spoolss
Win32 service or process : spoolsv.exe
Description : Spooler service
UUID: 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49159]
UUID: ae33069b-a2a8-46ee-a235-ddfd339be281, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49159]
UUID: 4a452661-8290-4b36-8fbe-7f4093a94978, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49159]
UUID: 76f03f96-cdfd-44fc-a22c-64950a001209, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49159]
Port: 49167/tcp
UUID: 50abc2a4-574d-40b3-9d66-ee4fd5fba076, version 5

Endpoint: ncacn_ip_tcp:192.168.0.20[49167]
Named pipe : dnsserver
Win32 service or process : dns.exe
Description : DNS Server
Port: 49174/tcp
UUID: 367abb81-9844-35f1-ad32-98f038001003, version 2
Endpoint: ncacn_ip_tcp:192.168.0.20[49174]
Port: 49195/tcp
UUID: 897e2e5f-93f3-4376-9c9c-fd2277495c27, version 1
Endpoint: ncacn_ip_tcp:192.168.0.20[49195]
Annotation: Frs2 Service
Solution : filter incoming traffic to this port(s).
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:P
Solution:
filter incoming traffic to this port.
Summary:
Distributed Computing Environment (DCE) services running on the remote host
can be enumerated by connecting on port 135 and doing the appropriate queries.
An attacker may use this fact to gain more knowledge
about the remote host.
CVSS Base Score: 5.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2001 Dave Aitel (ported to NASL by rd and Pavel Kankovsky)
Summary: Enumerates the remote DCE services
Version: $Revision: 2837 $

High:

Use LDAP search request to retrieve information from NT Directory Services
Risk: High
Application: ldap
Port: 389
Protocol: tcp
ScriptID: 12105
Vulnerability Detection Result:
The following information was pulled from the server via a LDAP request:
NTDS
Settings,CN=CM-SRV01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=casamedranda,DC=int
Solution:
If pre-Windows 2000 compatibility is not required, remove
pre-Windows 2000 compatibility as follows :
- start cmd.exe
- execute the command :
net localgroup 'Pre-Windows 2000 Compatible Access' everyone /delete
- restart the remote host
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:N/A:N
Summary:
It is possible to disclose LDAP information.
Description :
The directory base of the remote server is set to NULL. This allows information
to be enumerated without any prior knowledge of the directory structure.
CVSS Base Score: 5.0
Family name: Remote file access
Category: infos
Copyright: This script is Copyright (C) 2004 David Kyger
Summary: Use LDAP search request to retrieve information from NT Directory Services
Version: $Revision: 3398 $

High:

Use LDAP search request to retrieve information from NT Directory Services
Risk: High
Application: globalcatLDAP
Port: 3268
Protocol: tcp
ScriptID: 12105
Vulnerability Detection Result:
The following information was pulled from the server via a LDAP request:
NTDS
Settings,CN=CM-SRV01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=casamedranda,DC=int
CVSS Base Vector:
AV:N/AC:L/Au:N/C:P/I:N/A:N
Solution:
If pre-Windows 2000 compatibility is not required, remove
pre-Windows 2000 compatibility as follows :
- start cmd.exe
- execute the command :
net localgroup 'Pre-Windows 2000 Compatible Access' everyone /delete
- restart the remote host
Summary:
It is possible to disclose LDAP information.
Description :
The directory base of the remote server is set to NULL. This allows information
to be enumerated without any prior knowledge of the directory structure.
CVSS Base Score: 5.0
Family name: Remote file access
Category: infos
Copyright: This script is Copyright (C) 2004 David Kyger
Summary: Use LDAP search request to retrieve information from NT Directory Services
Version: $Revision: 3398 $

Medium:

Check for SSL Weak Ciphers
Risk: Medium
Application: https
Port: 443
Protocol: tcp
ScriptID: 103440
Vulnerability Detection Result:
Weak ciphers offered by this service:
SSL3_RSA_RC4_128_MD5
SSL3_RSA_RC4_128_SHA
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS_1_2_RSA_WITH_RC4_128_MD5
TLS_1_2_RSA_WITH_RC4_128_SHA
Insight:
These rules are applied for the evaluation of the cryptographic strength:
- Any SSL/TLS using no cipher is considered weak.
- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.
- RC4 is considered to be weak.
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods
and therefore considered as weak.
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong
Summary:
This routine search for weak SSL ciphers offered by a service.
Solution:
The configuration of this services should be changed so
that it does not support the listed weak ciphers anymore.
CVSS Base Vector:
AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Base Score: 4.3
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH
Summary: Checks for the presence of SSL Weak Ciphers
Version: $Revision: 3061 $

Medium:

Deprecated SSLv2 and SSLv3 Protocol Detection
Risk: Medium
Application: https
Port: 443
Protocol: tcp
ScriptID: 111012
Vulnerability Detection Result:
In addition to TLSv1+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'Check SSL Weak Ciphers and Supported Ciphers' NVT.
Insight:
The SSLv2 and SSLv3 protocols containing
known cryptographic flaws.
Affected Software/OS:
All services providing an encrypted communication
using the SSLv2 and/or SSLv3 protocols.
Summary:
It was possible to detect the usage of the
deprecated SSLv2 and/or SSLv3 protocol on this system.
Impact:
An attacker might be able to use the known
cryptographic flaws to eavesdrop the connection between clients and the service
to get access to sensitive data transferred within the secured connection.
Vulnerability Detection Method:
Check the used protocols of the services
provided by this system.
CVSS Base Vector:
AV:N/AC:M/Au:N/C:P/I:N/A:N
Solution:
It is recommended to disable the deprecated
SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the
references for more information.
References:
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report
https://bettercrypto.org/
CVSS Base Score: 4.3
Family name: General
Category: infos
Copyright: Copyright (C) 2015 SCHUTZWERK GmbH
Summary: NOSUMMARY
Version: $Revision: 2699 $

Medium:

POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability
Risk: Medium
Application: https
Port: 443
Protocol: tcp
ScriptID: 802087
Affected Software/OS:
OpenSSL through 1.0.1i
Insight:
The flaw is due to the block cipher
padding not being deterministic and not covered by the Message
Authentication Code
CVSS Base Vector:
AV:N/AC:M/Au:N/C:P/I:N/A:N
Solution:
Vendor released a patch to address this
vulnerabiliy, For updates contact vendor or refer to https://www.openssl.org
NOTE: The only correct way to fix POODLE is to disable SSL v3.0
Vulnerability Detection Method:
Send a SSLv3 request and check the
response.
Impact:
Successful exploitation will allow a
man-in-the-middle attackers gain access to the plain text data stream.
Impact Level: Application
Summary:
This host is installed with OpenSSL
and is prone to information disclosure vulnerability.
References:
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html
http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html
CVSS Base Score: 4.3
Family name: General
Category: infos

Summary: NOSUMMARY
Version: $Revision: 3580 $

Medium:

Check for SSL Weak Ciphers
Risk: Medium
Application: ms-term-serv
Port: 3389
Protocol: tcp
ScriptID: 103440
Vulnerability Detection Result:
Weak ciphers offered by this service:
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS_1_2_RSA_WITH_RC4_128_MD5
TLS_1_2_RSA_WITH_RC4_128_SHA
Insight:
These rules are applied for the evaluation of the cryptographic strength:
- Any SSL/TLS using no cipher is considered weak.
- All SSLv2 ciphers are considered weak due to a design flaw within the SSLv2 protocol.
- RC4 is considered to be weak.
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods
and therefore considered as weak.
- 1024 bit RSA authentication is considered to be insecure and therefore as weak.
- CBC ciphers in TLS < 1.2 are considered to be vulnerable to the BEAST or Lucky 13 attacks
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong
Solution:
The configuration of this services should be changed so
that it does not support the listed weak ciphers anymore.
CVSS Base Vector:
AV:N/AC:M/Au:N/C:P/I:N/A:N
Summary:
This routine search for weak SSL ciphers offered by a service.
CVSS Base Score: 4.3
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2012 Greenbone Networks GmbH
Summary: Checks for the presence of SSL Weak Ciphers
Version: $Revision: 3061 $

Medium:

TCP timestamps
Risk: Medium
Application: general
Port: 0
Protocol: tcp
ScriptID: 80091
Vulnerability Detection Result:
It was detected that the host implements RFC1323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Paket 1: 54904618
Paket 2: 54904730
Summary:
The remote host implements TCP timestamps and therefore allows to compute
the uptime.
Impact:
A side effect of this feature is that the uptime of the remote
host can sometimes be computed.
Vulnerability Detection Method:
Special IP packets are forged and sent with a little delay in between to the
target IP. The responses are searched for a timestamps. If found, the
timestamps are reported.
Solution:
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to
/etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is, to not use the
Timestamp options when initiating TCP connections, but use them if the TCP peer
that is initiating communication includes them in their synchronize (SYN) segment.
See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152
CVSS Base Vector:
AV:N/AC:H/Au:N/C:P/I:N/A:N
Insight:
The remote host implements TCP timestamps, as defined by RFC1323.
Affected Software/OS:
TCP/IPv4 implementations that implement RFC1323.
References:
http://www.ietf.org/rfc/rfc1323.txt
CVSS Base Score: 2.6
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2007 Michel Arboi
Summary: Look at RFC1323 TCP timestamps
Version: $Revision: 3351 $

Info:

DIRB (NASL wrapper)
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 103079
Vulnerability Detection Result:
DIRB could not be found in your system path.
OpenVAS was unable to execute DIRB and to perform the scan you
requested.
Please make sure that DIRB is installed and is
available in the PATH variable defined for your environment.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This script uses DIRB to find directories and files on web
applications via brute forcing.
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos
Copyright: Copyright (C) 2011 Greenbone Networks GmbH
Summary: Brute force web app directories/files
Version: $Revision: 3117 $

Info:

OS Detection
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 105937
Vulnerability Detection Result:
Best matching OS:
cpe:/o:microsoft:windows
Found by NVT 1.3.6.1.4.1.25623.1.0.111067 (HTTP OS Identification)
Other OS detections (in order of reliability):
OS: cpe:/o:microsoft:windows found by 1.3.6.1.4.1.25623.1.0.102011 (SMB NativeLanMan)
OS: cpe:/h:hp:jetdirect found by 1.3.6.1.4.1.25623.1.0.102002 (Detects remote operating system version)
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This script consolidates the OS information detected by several NVTs and tries to find the best matching OS.
CVSS Base Score: 0.0
Family name: Service detection
Category: end
Copyright: This script is Copyright (C) 2016 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 3694 $

Info:

Hostname discovery from server certificate
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 111010
Vulnerability Detection Result:
The following additional hostnames were detected:
CM-SRV01.casamedranda.int
Summary:
It was possible to discover an additional hostname
of this server from its certificate Common or Subject Alt Name.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH
Summary: NOSUMMARY
Version: $Revision: 3690 $

Info:

Traceroute
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 51662
Vulnerability Detection Result:
Here is the route from 192.168.0.90 to 192.168.0.20:
192.168.0.90
192.168.0.20
Summary:
A traceroute from the scanning server to the target system was
conducted. This traceroute is provided primarily for informational
value only. In the vast majority of cases, it does not represent a
vulnerability. However, if the displayed traceroute contains any
private addresses that should not have been publicly visible, then you
have an issue you need to correct.
Solution:
Block unwanted packets from escaping your network.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: General
Category: infos
Copyright: Copyright (c) 2005 E-Soft Inc. http://www.securityspace.com
Summary: Traceroute
Version: $Revision: 2837 $

Info:

SMB Remote Version Detection
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 807830
Vulnerability Detection Result:
SMBv1, SMBv2 and SMBv3 are enabled on remote target
Summary:
Detection of Server Message Block(SMB).
This script sends SMB Negotiation request and try to get the version from the response.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Product detection
Category: infos
Copyright: Copyright (C) 2016 Greenbone Networks GmbH
Summary: NOSUMMARY
Version: $Revision: 3467 $

Info:

CPE Inventory
Risk: Info
Application: general
Port: 0
Protocol: CPE-T
ScriptID: 810002
Vulnerability Detection Result:
192.168.0.20|cpe:/a:microsoft:iis:8.5
192.168.0.20|cpe:/o:microsoft:windows
Summary:
This routine uses information collected by other routines about
CPE identities (http://cpe.mitre.org/) of operating systems, services and applications detected during the scan.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: end
Copyright: Copyright (c) 2009 Greenbone Networks GmbH
Summary: CPE Inventory
Version: $Revision: 2837 $

Info:

SMB Test
Risk: Info
Application: general
Port: 0
Protocol: SMBCl
ScriptID: 90011
Vulnerability Detection Result:
OS Version = WINDOWS SERVER 2012 R2 DATACENTER 9600
Domain = CASAMEDRANDA
SMB Serverversion = WINDOWS SERVER 2012 R2 DATACENTER 6.3
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Test remote host SMB Functions
CVSS Base Score: 0.0
Family name: Windows
Category: infos
Copyright: Copyright (C) 2008 Greenbone Networks GmbH
Summary: Determines the OS and SMB Version of Host
Version: $Revision: 3376 $

Info:

DNS Server Detection
Risk: Info
Application: domain
Port: 53
Protocol: tcp
ScriptID: 100069
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
A DNS Server is running at this Host.
A Name Server translates domain names into IP addresses. This makes it possible for a user to access a website by typing in the domain name instead of the website's actual IP address.
CVSS Base Score: 0.0
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH
Summary: Detect DNS Servers
Version: $Revision: 3492 $

Info:

Windows SharePoint Services detection
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 101018
Vulnerability Detection Result:
Server: Microsoft-IIS/8.5
Summary:
The remote host is running Windows SharePoint Services.
Microsoft SharePoint products and technologies include browser-based collaboration and a document-management platform.
These can be used to host web sites that access shared workspaces and documents from a browser.
Solution:
It's recommended to allow connection to this host only from trusted hosts or networks.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Christian Eric Edjenguele <christian.edjenguele@owasp.org>
Summary: Windows SharePoint Services Information Gathering
Version: $Revision: 3467 $

Info:

HTTP Server type and version
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 10107
Vulnerability Detection Result:
The remote web server type is :
Microsoft-IIS/8.5
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Solution:
Configure your server to use an alternate name like
'Wintendo httpD w/Dotmatrix display'
Be sure to remove common logos like apache_pb.gif.
With Apache, you can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
Summary:
This detects the HTTP Server's type and version.
CVSS Base Score: 0.0
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2000 H. Scholz & Contributors
Summary: HTTP Server type and version
Version: $Revision: 3564 $

Info:

Services
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A web server is running on this port
Summary:
This routine attempts to guess which
service is running on the remote ports. For instance,
it searches for a web server which could listen on
another port than 80 or 443 and makes this information
available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: Find what is listening on which port
Version: $Revision: 3210 $

Info:

No 404 check
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 10386
Vulnerability Detection Result:
CGI scanning will be disabled for this host.
Insight:
This web server is [mis]configured in that it does not return
'404 Not Found' error codes when a non-existent file is requested, perhaps returning a site map,
search page or authentication page instead.

OpenVAS enabled some counter measures for that, however they might be insufficient. If a great
number of security holes are produced for this port, they might not all be accurate
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
Remote web server does not reply with 404 error code.
CVSS Base Score: 0.0
Family name: Web Servers
Category: infos
Copyright: This script is Copyright (C) 2000 RD / H D Moore
Summary: Checks if the remote webserver issues 404 errors
Version: $Revision: 3485 $

Info:

Directories used for CGI Scanning
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 111038
Vulnerability Detection Result:
The following directories are used for CGI scanning:
http://192.168.0.20/scripts
http://192.168.0.20/cgi-bin
http://192.168.0.20/
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
The script prints out the directories which
are used when CGI scanning is enabled.
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2015 SCHUTZWERK GmbH
Summary: NOSUMMARY
Version: $Revision: 3092 $

Info:

Nikto (NASL wrapper)
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 14260
Vulnerability Detection Result:
The target server did not return 404 on requests for non-existent pages.
This scan has not been executed since Nikto is prone to reporting many false positives in this case.
If you wish to force this scan, you can enable it in the Nikto preferences in your client.
Summary:
This plugin uses nikto(1) to find weak CGI scripts
and other known issues regarding web server security.
See the preferences section for configuration options.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2004 Michel Arboi
Summary: Assess web server security with Nikto
Version: $Revision: 3673 $

Info:

Microsoft IIS Webserver Version Detection
Risk: Info
Application: http
Port: 80
Protocol: tcp
ScriptID: 900710
Vulnerability Detection Result:
Detected Microsoft IIS Webserver
Version: 8.5
Location: 80/tcp
CPE: cpe:/a:microsoft:iis:8.5
Concluded from version identification result:
IIS/8.5
Summary:
This script detects the installed MS IIS Webserver and sets the
result in KB
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (C) 2009 SecPod
Summary: Set the Version of Microsoft IIS in KB
Version: $Revision: 2711 $

Info:

Kerberos Detection
Risk: Info
Application: kerberos-sec
Port: 88
Protocol: tcp
ScriptID: 103854
Vulnerability Detection Result:
A Kerberos Server is running at this port.
Realm: CASAMEDRANDA.INT
Server time: 2016-10-03 03:01:46
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
The script sends a connection request to detect a running kerberos server.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 2013 Greenbone Networks GmbH
Summary: Check for Kerberos
Version: $Revision: 2836 $

Info:

Identify unknown services with nmap
Risk: Info
Application: kerberos-sec
Port: 88
Protocol: tcp
ScriptID: 66286
Vulnerability Detection Result:
Nmap service detection result for this port: kerberos-sec
Summary:
This plugin performs service detection by launching nmap's
service probe against ports running unidentified services.
Description :
This plugin is a complement of find_service.nasl. It launches
nmap -sV (probe requests) against ports that are running
unidentified services.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (c) 2009 E-Soft Inc. http://www.securityspace.com
Summary: Launches nmap -sV against ports running unidentified services
Version: $Revision: 2752 $

Info:

SMB on port 445
Risk: Info
Application: netbios-ssn
Port: 139
Protocol: tcp
ScriptID: 11011
Vulnerability Detection Result:
An SMB server is running on this port
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This script detects wether port 445 and 139 are open and
if thet are running SMB servers.
CVSS Base Score: 0.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2002 Renaud Deraison
Summary: Checks for openness of port 445
Version: $Revision: 2837 $

Info:

LDAP Detection
Risk: Info
Application: ldap
Port: 389
Protocol: tcp
ScriptID: 100082
Summary:
A LDAP Server is running at this host.
The Lightweight Directory Access Protocol, or LDAP is an application
protocol for querying and modifying directory services running over
TCP/IP.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH
Summary: Check for LDAP
Version: $Revision: 2837 $

Info:

HTTP Server type and version
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 10107
Vulnerability Detection Result:
The remote web server type is :
Microsoft-HTTPAPI/2.0
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Solution:
Configure your server to use an alternate name like
'Wintendo httpD w/Dotmatrix display'
Be sure to remove common logos like apache_pb.gif.
With Apache, you can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
Summary:
This detects the HTTP Server's type and version.
CVSS Base Score: 0.0
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2000 H. Scholz & Contributors
Summary: HTTP Server type and version
Version: $Revision: 3564 $

Info:

SSL Certificate - Self-Signed Certificate Detection
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 103140
Summary:
The SSL certificate on this port is self-signed.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
http://en.wikipedia.org/wiki/Self-signed_certificate
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH
Summary: Checks for Self-Signed Certificates
Version: $Revision: 2603 $

Info:

Services
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A TLScustom server answered on this port
Summary:
This routine attempts to guess which
service is running on the remote ports. For instance,
it searches for a web server which could listen on
another port than 80 or 443 and makes this information
available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: Find what is listening on which port
Version: $Revision: 3210 $

Info:

Services
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A web server is running on this port through SSL
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This routine attempts to guess which
service is running on the remote ports. For instance,
it searches for a web server which could listen on
another port than 80 or 443 and makes this information
available for other check routines.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: Find what is listening on which port
Version: $Revision: 3210 $

Info:

SSL Certification Too Long Valid
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 103958
Vulnerability Detection Result:
Certificates which are valid for more than 15years from now:
The SSL certificate of the remote service will expire on 2036-09-26 15:01:04
Certificate details:
subject ...: CN=NVIDIA GameStream Server
issued by .: CN=NVIDIA GameStream Server
serial ....: 00F397673A5039A302
valid from : 2016-09-26 15:01:04 UTC
valid until: 2036-09-26 15:01:04 UTC
fingerprint: 91D14C5F849034B2C26A6B1322518222BDBFE6C1
Solution:
Replace the SSL certificate by a new one.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
The remote server's SSL certificate expiration date is too far
in the future.
Insight:
This script checks expiry dates of certificates associated with
SSL-enabled services on the target and reports whether any do not have a
reasonable expiration date.
CVSS Base Score: 0.0
Family name: General
Category: infos

Summary: SSL certificate too long valid
Version: $Revision: 2937 $

Info:

Directories used for CGI Scanning
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 111038
Vulnerability Detection Result:
The following directories are used for CGI scanning:
https://192.168.0.20/scripts
https://192.168.0.20/cgi-bin
https://192.168.0.20/
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
The script prints out the directories which
are used when CGI scanning is enabled.
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos

Summary: NOSUMMARY
Version: $Revision: 3092 $

Info:

Nikto (NASL wrapper)
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 14260
Vulnerability Detection Result:
Here is the Nikto report:
- Nikto v2.1.5

+ Target IP: 192.168.0.20
+ Target Hostname: 192.168.0.20
+ Target Port: 443

+ SSL Info: Subject: /CN=NVIDIA GameStream Server
Ciphers: ECDHE-RSA-AES256-SHA384
Issuer: /CN=NVIDIA GameStream Server
+ Start Time: 2016-10-03 02:57:23 (GMT0)

+ Server: Microsoft-HTTPAPI/2.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Hostname '192.168.0.20' does not match certificate's CN 'NVIDIA'
+ 6544 items checked: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2016-10-03 02:58:52 (GMT0) (89 seconds)

+ 1 host(s) tested
Summary:
This plugin uses nikto(1) to find weak CGI scripts
and other known issues regarding web server security.
See the preferences section for configuration options.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2004 Michel Arboi
Summary: Assess web server security with Nikto
Version: $Revision: 3673 $

Info:

Check for SSL Ciphers
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 802067
Vulnerability Detection Result:
Service does not support SSLv2 ciphers.
Service supports SSLv3 ciphers.
Service supports TLSv1 ciphers.
Service supports TLSv1.1 ciphers.
Service supports TLSv1.2 ciphers.
Medium ciphers offered by this service:
SSL3_RSA_DES_192_CBC3_SHA
TLS1_RSA_DES_192_CBC3_SHA
TLS1_DHE_RSA_WITH_AES_128_SHA
TLS1_RSA_WITH_AES_128_SHA
TLS1_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS1_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS1_RSA_DES_192_CBC3_SHA
TLS1_DHE_RSA_WITH_AES_128_SHA
TLS1_RSA_WITH_AES_128_SHA
TLS1_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS1_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_1_2_RSA_WITH_AES_128_GCM_SHA256
TLS_1_2_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_1_2_RSA_WITH_AES_256_CBC_SHA256
TLS_1_2_RSA_WITH_AES_128_CBC_SHA256
TLS_1_2_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_1_2_RSA_WITH_AES_256_GCM_SHA384
TLS_1_2_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_1_2_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_1_2_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_RSA_WITH_AES_256_CBC_SHA
TLS_1_2_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA
Weak ciphers offered by this service:
SSL3_RSA_RC4_128_MD5
SSL3_RSA_RC4_128_SHA
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS_1_2_RSA_WITH_RC4_128_MD5
TLS_1_2_RSA_WITH_RC4_128_SHA
No non-ciphers are supported by this service
Summary:
This routine search for SSL ciphers offered by a service.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS Base Score: 0.0
Family name: General
Category: infos
Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: Checks for the SSL Ciphers
Version: $Revision: 2827 $

Info:

Check for SSL Medium Ciphers
Risk: Info
Application: https
Port: 443
Protocol: tcp
ScriptID: 902816
Vulnerability Detection Result:
Medium ciphers offered by this service:
SSL3_RSA_DES_192_CBC3_SHA
TLS1_RSA_DES_192_CBC3_SHA
TLS1_DHE_RSA_WITH_AES_128_SHA
TLS1_RSA_WITH_AES_128_SHA
TLS1_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS1_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS1_RSA_DES_192_CBC3_SHA
TLS1_DHE_RSA_WITH_AES_128_SHA
TLS1_RSA_WITH_AES_128_SHA
TLS1_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS1_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_1_2_RSA_WITH_AES_128_GCM_SHA256
TLS_1_2_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_1_2_RSA_WITH_AES_256_CBC_SHA256
TLS_1_2_RSA_WITH_AES_128_CBC_SHA256
TLS_1_2_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_1_2_RSA_WITH_AES_256_GCM_SHA384
TLS_1_2_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_1_2_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_1_2_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_RSA_WITH_AES_256_CBC_SHA
TLS_1_2_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This Plugin reports about SSL Medium Ciphers.
CVSS Base Score: 0.0
Family name: General
Category: infos

Summary: Checks for the presence of SSL Medium Ciphers
Version: $Revision: 3060 $

Info:

SMB NativeLanMan
Risk: Info
Application: microsoft-ds
Port: 445
Protocol: tcp
ScriptID: 102011
Vulnerability Detection Result:
Detected SMB workgroup: CASAMEDRANDA
Detected SMB server: Windows Server 2012 R2 Datacenter 6.3
Detected OS: Windows Server 2012 R2 Datacenter 9600
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
It is possible to extract OS, domain
and SMB server information from the Session Setup AndX Response packet
which is generatedduring NTLM authentication.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (C) 2009 LSS
Summary: Extracts info about the OS through NTLM authentication packets
Version: $Revision: 3637 $

Info:

SMB on port 445
Risk: Info
Application: microsoft-ds
Port: 445
Protocol: tcp
ScriptID: 11011
Vulnerability Detection Result:
A CIFS server is running on this port
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This script detects wether port 445 and 139 are open and
if thet are running SMB servers.
CVSS Base Score: 0.0
Family name: Windows
Category: infos
Copyright: This script is Copyright (C) 2002 Renaud Deraison
Summary: Checks for openness of port 445
Version: $Revision: 2837 $

Info:

Identify unknown services with nmap
Risk: Info
Application: kpasswd5
Port: 464
Protocol: tcp
ScriptID: 66286
Vulnerability Detection Result:
Nmap service detection result for this port: kpasswd5
This is a guess. A confident identification of the service was not possible.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This plugin performs service detection by launching nmap's
service probe against ports running unidentified services.
Description :
This plugin is a complement of find_service.nasl. It launches
nmap -sV (probe requests) against ports that are running
unidentified services.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (c) 2009 E-Soft Inc. http://www.securityspace.com
Summary: Launches nmap -sV against ports running unidentified services
Version: $Revision: 2752 $

Info:

Identify unknown services with nmap
Risk: Info
Application: ldapssl
Port: 636
Protocol: tcp
ScriptID: 66286
Vulnerability Detection Result:
Nmap service detection result for this port: tcpwrapped
Summary:
This plugin performs service detection by launching nmap's
service probe against ports running unidentified services.
Description :
This plugin is a complement of find_service.nasl. It launches
nmap -sV (probe requests) against ports that are running
unidentified services.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (c) 2009 E-Soft Inc. http://www.securityspace.com
Summary: Launches nmap -sV against ports running unidentified services
Version: $Revision: 2752 $

Info:

Services
Risk: Info
Application: unknown
Port: 902
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A VMWare authentication daemon is running on this port:
220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , , NFCSSL supported/t
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This routine attempts to guess which
service is running on the remote ports. For instance,
it searches for a web server which could listen on
another port than 80 or 443 and makes this information
available for other check routines.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: Find what is listening on which port
Version: $Revision: 3210 $

Info:

Services
Risk: Info
Application: unknown
Port: 912
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A VMWare authentication daemon is running on this port:
220 VMware Authentication Daemon Version 1.0, ServerDaemonProtocol:SOAP, MKSDisplayProtocol:VNC , ,
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This routine attempts to guess which
service is running on the remote ports. For instance,
it searches for a web server which could listen on
another port than 80 or 443 and makes this information
available for other check routines.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: Find what is listening on which port
Version: $Revision: 3210 $

Info:

HTTP Server type and version
Risk: Info
Application: unknown
Port: 1560
Protocol: tcp
ScriptID: 10107
Vulnerability Detection Result:
The remote web server type is :
UPnP/1.0 DLNADOC/1.50 Platinum/1.0.5.13
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Solution:
Configure your server to use an alternate name like
'Wintendo httpD w/Dotmatrix display'
Be sure to remove common logos like apache_pb.gif.
With Apache, you can set the directive 'ServerTokens Prod' to limit
the information emanating from the server in its response headers.
Summary:
This detects the HTTP Server's type and version.
CVSS Base Score: 0.0
Family name: General
Category: infos
Copyright: This script is Copyright (C) 2000 H. Scholz & Contributors
Summary: HTTP Server type and version
Version: $Revision: 3564 $

Info:

Services
Risk: Info
Application: unknown
Port: 1560
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A web server is running on this port
Summary:
This routine attempts to guess which
service is running on the remote ports. For instance,
it searches for a web server which could listen on
another port than 80 or 443 and makes this information
available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: Find what is listening on which port
Version: $Revision: 3210 $

Info:

Directories used for CGI Scanning
Risk: Info
Application: unknown
Port: 1560
Protocol: tcp
ScriptID: 111038
Vulnerability Detection Result:
The following directories are used for CGI scanning:
http://192.168.0.20:1560/scripts
http://192.168.0.20:1560/cgi-bin
http://192.168.0.20:1560/
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
The script prints out the directories which
are used when CGI scanning is enabled.
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos

Summary: NOSUMMARY
Version: $Revision: 3092 $

Info:

Nikto (NASL wrapper)
Risk: Info
Application: unknown
Port: 1560
Protocol: tcp
ScriptID: 14260
Vulnerability Detection Result:
Here is the Nikto report:
- Nikto v2.1.5

+ Target IP: 192.168.0.20
+ Target Hostname: 192.168.0.20
+ Target Port: 1560
+ Start Time: 2016-10-03 02:57:01 (GMT0)

+ Server: UPnP/1.0 DLNADOC/1.50 Platinum/1.0.5.13
+ IP address found in the 'server' header. The IP is "1.0.5.13".
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 6544 items checked: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2016-10-03 02:57:21 (GMT0) (20 seconds)

+ 1 host(s) tested
Summary:
This plugin uses nikto(1) to find weak CGI scripts
and other known issues regarding web server security.
See the preferences section for configuration options.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Web application abuses
Category: infos
Copyright: This script is Copyright (C) 2004 Michel Arboi
Summary: Assess web server security with Nikto
Version: $Revision: 3673 $

Info:

PPTP detection and versioning
Risk: Info
Application: pptp
Port: 1723
Protocol: tcp
ScriptID: 10622
Vulnerability Detection Result:
A PPTP server is running on this port
Firmware Revision:0
Host name:
Vendor string:Microsoft
Summary:
The remote host seems to be running a PPTP (VPN) service, this service allows remote users to connect to the internal network and play a trusted rule in it. This service should be protect with encrypted username & password combinations, and should be accessible only to trusted individuals. By default the service leaks out such information as Server version (PPTP version), Hostname and Vendor string this could help an attacker better prepare her next attack.
Also note that PPTP is not configured as being cryptographically secure, and you should use another VPN method if you can
Solution:
Restrict access to this port from untrusted networks. Make sure only encrypt channels are allowed through the PPTP (VPN) connection.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
http://www.counterpane.com/pptp-faq.html
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 2001 SecuriTeam
Summary: Determine if a remote host is running a PPTP (VPN) service
Version: $Revision: 2837 $

Info:

Identify unknown services with nmap
Risk: Info
Application: globalcatLDAP
Port: 3268
Protocol: tcp
ScriptID: 66286
Vulnerability Detection Result:
Nmap service detection result for this port: ldap
Summary:
This plugin performs service detection by launching nmap's
service probe against ports running unidentified services.
Description :
This plugin is a complement of find_service.nasl. It launches
nmap -sV (probe requests) against ports that are running
unidentified services.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (c) 2009 E-Soft Inc. http://www.securityspace.com
Summary: Launches nmap -sV against ports running unidentified services
Version: $Revision: 2752 $

Info:

Identify unknown services with nmap
Risk: Info
Application: globalcatLDAPssl
Port: 3269
Protocol: tcp
ScriptID: 66286
Vulnerability Detection Result:
Nmap service detection result for this port: tcpwrapped
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This plugin performs service detection by launching nmap's
service probe against ports running unidentified services.
Description :
This plugin is a complement of find_service.nasl. It launches
nmap -sV (probe requests) against ports that are running
unidentified services.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (c) 2009 E-Soft Inc. http://www.securityspace.com
Summary: Launches nmap -sV against ports running unidentified services
Version: $Revision: 2752 $

Info:

SSL Certificate - Self-Signed Certificate Detection
Risk: Info
Application: ms-term-serv
Port: 3389
Protocol: tcp
ScriptID: 103140
Summary:
The SSL certificate on this port is self-signed.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
References:
http://en.wikipedia.org/wiki/Self-signed_certificate
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: This script is Copyright (C) 2011 Greenbone Networks GmbH
Summary: Checks for Self-Signed Certificates
Version: $Revision: 2603 $

Info:

Services
Risk: Info
Application: ms-term-serv
Port: 3389
Protocol: tcp
ScriptID: 10330
Vulnerability Detection Result:
A TLScustom server answered on this port
Summary:
This routine attempts to guess which
service is running on the remote ports. For instance,
it searches for a web server which could listen on
another port than 80 or 443 and makes this information
available for other check routines.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Written by Renaud Deraison <deraison@cvs.nessus.org>
Summary: Find what is listening on which port
Version: $Revision: 3210 $

Info:

Identify unknown services with nmap
Risk: Info
Application: ms-term-serv
Port: 3389
Protocol: tcp
ScriptID: 66286
Vulnerability Detection Result:
Nmap service detection result for this port: ms-wbt-server
This is a guess. A confident identification of the service was not possible.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This plugin performs service detection by launching nmap's
service probe against ports running unidentified services.
Description :
This plugin is a complement of find_service.nasl. It launches
nmap -sV (probe requests) against ports that are running
unidentified services.
CVSS Base Score: 0.0
Family name: Service detection
Category: infos
Copyright: Copyright (c) 2009 E-Soft Inc. http://www.securityspace.com
Summary: Launches nmap -sV against ports running unidentified services
Version: $Revision: 2752 $

Info:

Check for SSL Ciphers
Risk: Info
Application: ms-term-serv
Port: 3389
Protocol: tcp
ScriptID: 802067
Vulnerability Detection Result:
Service does not support SSLv2 ciphers.
Service does not support SSLv3 ciphers.
Service supports TLSv1 ciphers.
Service supports TLSv1.1 ciphers.
Service supports TLSv1.2 ciphers.
Medium ciphers offered by this service:
TLS1_RSA_DES_192_CBC3_SHA
TLS1_DHE_RSA_WITH_AES_128_SHA
TLS1_RSA_WITH_AES_128_SHA
TLS1_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS1_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS1_RSA_DES_192_CBC3_SHA
TLS1_DHE_RSA_WITH_AES_128_SHA
TLS1_RSA_WITH_AES_128_SHA
TLS1_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS1_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_1_2_RSA_WITH_AES_128_GCM_SHA256
TLS_1_2_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_1_2_RSA_WITH_AES_256_CBC_SHA256
TLS_1_2_RSA_WITH_AES_128_CBC_SHA256
TLS_1_2_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_1_2_RSA_WITH_AES_256_GCM_SHA384
TLS_1_2_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_1_2_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_1_2_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_RSA_WITH_AES_256_CBC_SHA
TLS_1_2_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA
Weak ciphers offered by this service:
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS1_RSA_RC4_128_MD5
TLS1_RSA_RC4_128_SHA
TLS_1_2_RSA_WITH_RC4_128_MD5
TLS_1_2_RSA_WITH_RC4_128_SHA
No non-ciphers are supported by this service
Summary:
This routine search for SSL ciphers offered by a service.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
CVSS Base Score: 0.0
Family name: General
Category: infos

Copyright: Copyright (C) 2014 Greenbone Networks GmbH
Summary: Checks for the SSL Ciphers
Version: $Revision: 2827 $

Info:

Check for SSL Medium Ciphers
Risk: Info
Application: ms-term-serv
Port: 3389
Protocol: tcp
ScriptID: 902816
Vulnerability Detection Result:
Medium ciphers offered by this service:
TLS1_RSA_DES_192_CBC3_SHA
TLS1_DHE_RSA_WITH_AES_128_SHA
TLS1_RSA_WITH_AES_128_SHA
TLS1_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS1_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS1_RSA_DES_192_CBC3_SHA
TLS1_DHE_RSA_WITH_AES_128_SHA
TLS1_RSA_WITH_AES_128_SHA
TLS1_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS1_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_1_2_RSA_WITH_AES_128_GCM_SHA256
TLS_1_2_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_1_2_RSA_WITH_AES_256_CBC_SHA256
TLS_1_2_RSA_WITH_AES_128_CBC_SHA256
TLS_1_2_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_1_2_RSA_WITH_AES_256_GCM_SHA384
TLS_1_2_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_1_2_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_1_2_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_RSA_WITH_AES_256_CBC_SHA
TLS_1_2_RSA_WITH_AES_128_CBC_SHA
TLS_1_2_RSA_WITH_3DES_EDE_CBC_SHA
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Summary:
This Plugin reports about SSL Medium Ciphers.
CVSS Base Score: 0.0
Family name: General
Category: infos
Copyright: Copyright (C) 2012 SecPod
Summary: Checks for the presence of SSL Medium Ciphers
Version: $Revision: 3060 $

Info:

Ping Host
Risk: Info
Application: general
Port: 0
Protocol: tcp
ScriptID: 100315
Vulnerability Detection Result:
The alive test was not launched because no method was selected.
CVSS Base Vector:
AV:N/AC:L/Au:N/C:N/I:N/A:N
Vulnerability Detection Method:
Whether a host is up can be detected in 3 different ways:
- A ICMP message is sent to the host and a response is taken as alive sign.
- An ARP request is sent and a response is taken as alive sign.
- A number of typical TCP services (namely the 20 top ports of nmap)
are tried and their presence is taken as alive sign.
None of the methods is failsafe. It depends on network and/or host configurations
whether they succeed or not. Both, false positives and false negatives can occur.
Therefore the methods are configurable.
If you select to not mark unreachable hosts as dead, no alive detections are
executed and the host is assumed to be available for scanning.
Summary:
This check tries to determine whether a remote host is up (alive).
Several methods are used for this depending on configuration of this check.
Insight:
The available methods might fail for the following reasons:
- ICMP: This might be disabled for a environment and would then cause false
negatives as hosts are believed to be dead that actually are alive.
In case it is configured that hosts are never marked as dead, this can cause
considerable timeouts and therefore a long scan duration in case the hosts
are in fact not available.
CVSS Base Score: 0.0
Family name: Port scanners
Category: scanner
Copyright: This script is Copyright (C) 2009 Greenbone Networks GmbH
Summary: Ping the remote host
Version: $Revision: 3316 $

ANEXO 5

Alarms Report

I.T. Security

Address

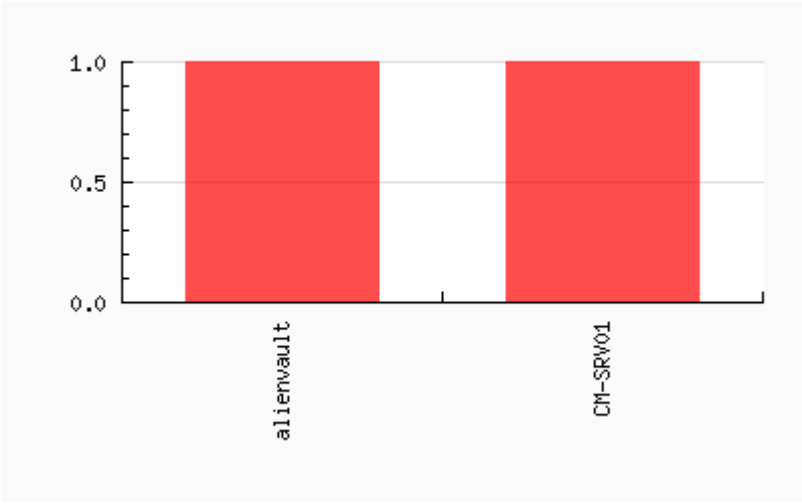
Tel. **Report Date** 2016-11-20 20:55:21

Report Filter Date from: 2016-10-22 Date to: 2016-11-21

Assets Selected: All Assets

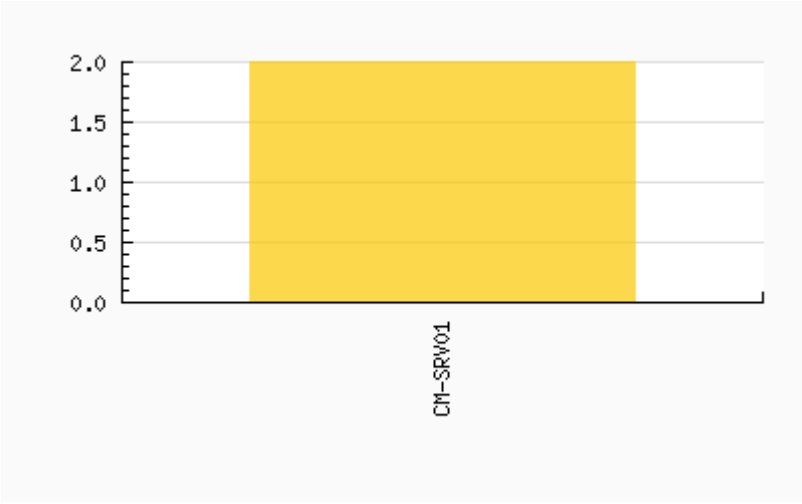
Alarms Report - Top 10 Attacker Host from: 2016-10-22 to: 2016-11-21

Host	Occurrences
alienvault	1
CM-SRV01	1



Alarms Report - Top 10 Attacked Host from: 2016-10-22 to: 2016-11-21

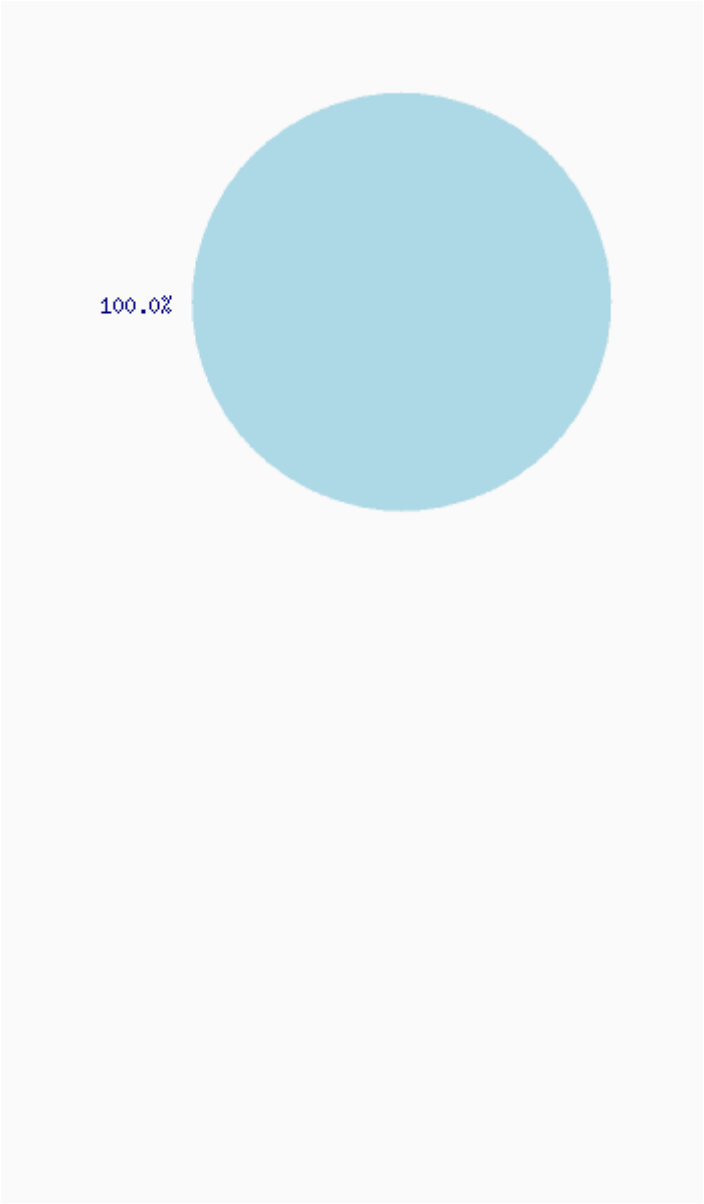
Host	Occurrences
CM-SRV01	2



Alarms Report - Top 10 Used Ports from: 2016-10-22 to: 2016-11-21

No data available

Alarms Report - Top 15 Alarms from: 2016-10-22 to: 2016-11-21



Alarm	Occurrences
Delivery & Attack — Bruteforce Authentication — Windows Login	2

ALIEN VAULT OSSIM

Alarms Report - Top 15 Alarms by Risk from: 2016-10-22 to: 2016-11-21

Alarm	Risk
Delivery & Attack — Bruteforce Authentication — Windows Login	

ANEXO 6

5. POLÍTICA DE SEGURIDAD.

5.1 Política de seguridad de la información.

- 5.1.1 Documento de política de seguridad de la información.
- 5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.

- 6.1.1 Compromiso de la Dirección con la seguridad de la información.
- 6.1.2 Coordinación de la seguridad de la información.
- 6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
- 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
- 6.1.5 Acuerdos de confidencialidad.
- 6.1.6 Contacto con las autoridades.
- 6.1.7 Contacto con grupos de especial interés.
- 6.1.8 Revisión independiente de la seguridad de la información.

6.2 Terceros.

- 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
- 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
- 6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.

7.1 Responsabilidad sobre los activos.

- 7.1.1 Inventario de activos.
- 7.1.2 Propiedad de los activos.
- 7.1.3 Uso aceptable de los activos.

7.2 Clasificación de la información.

- 7.2.1 Directrices de clasificación.
- 7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

8.1 Antes del empleo.

- 8.1.1 Funciones y responsabilidades.
- 8.1.2 Investigación de antecedentes.
- 8.1.3 Términos y condiciones de contratación.

8.2 Durante el empleo.

- 8.2.1 Responsabilidades de la Dirección.
- 8.2.2 Concienciación, formación y capacitación en seg. de la informac.
- 8.2.3 Proceso disciplinario.

8.3 Cese del empleo o cambio de puesto de trabajo.

- 8.3.1 Responsabilidad del cese o cambio.
- 8.3.2 Devolución de activos.
- 8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.

9.1 Áreas seguras.

- 9.1.1 Perímetro de seguridad física.
- 9.1.2 Controles físicos de entrada.
- 9.1.3 Seguridad de oficinas, despachos e instalaciones.
- 9.1.4 Protección contra las amenazas externas y de origen ambiental.
- 9.1.5 Trabajo en áreas seguras.
- 9.1.6 Áreas de acceso público y de carga y descarga.

9.2 Seguridad de los equipos.

- 9.2.1 Emplazamiento y protección de equipos.
- 9.2.2 Instalaciones de suministro.
- 9.2.3 Seguridad del cableado.
- 9.2.4 Mantenimiento de los equipos.
- 9.2.5 Seguridad de los equipos fuera de las instalaciones.
- 9.2.6 Reutilización o retirada segura de equipos.
- 9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.

10.1 Responsabilidades y procedimientos de operación.

- 10.1.1 Documentación de los procedimientos de operación.
- 10.1.2 Gestión de cambios.
- 10.1.3 Segregación de tareas.
- 10.1.4 Separación de los recursos de desarrollo, prueba y operación.

10.2 Gestión de la provisión de servicios por terceros.

- 10.2.1 Provisión de servicios.
- 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
- 10.2.3 Gestión del cambio en los servicios prestados por terceros.

10.3 Planificación y aceptación del sistema.

- 10.3.1 Gestión de capacidades.
- 10.3.2 Aceptación del sistema.

10.4 Protección contra el código malicioso y descargable.

- 10.4.1 Controles contra el código malicioso.
- 10.4.2 Controles contra el código descargado en el cliente.

10.5 Copias de seguridad.

- 10.5.1 Copias de seguridad de la información.

10.6 Gestión de la seguridad de las redes.

- 10.6.1 Controles de red.
- 10.6.2 Seguridad de los servicios de red.

10.7 Manipulación de los soportes.

- 10.7.1 Gestión de soportes extraíbles.
- 10.7.2 Retirada de soportes.
- 10.7.3 Procedimientos de manipulación de la información.
- 10.7.4 Seguridad de la documentación del sistema.

10.8 Intercambio de información.

- 10.8.1 Políticas y procedimientos de intercambio de información.
- 10.8.2 Acuerdos de intercambio.
- 10.8.3 Soportes físicos en tránsito.
- 10.8.4 Mensajería electrónica.
- 10.8.5 Sistemas de información empresariales.

10.9 Servicios de comercio electrónico.

- 10.9.1 Comercio electrónico.
- 10.9.2 Transacciones en línea.
- 10.9.3 Información públicamente disponible.

10.10 Supervisión.

- 10.10.1 Registros de auditoría.
- 10.10.2 Supervisión del uso del sistema.
- 10.10.3 Protección de la información de los registros.
- 10.10.4 Registros de administración y operación.
- 10.10.5 Registro de fallos.
- 10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.

11.1 Requisitos de negocio para el control de acceso.

- 11.1.1 Política de control de acceso.

11.2 Gestión de acceso de usuario.

- 11.2.1 Registro de usuario.
- 11.2.2 Gestión de privilegios.
- 11.2.3 Gestión de contraseñas de usuario.
- 11.2.4 Revisión de los derechos de acceso de usuario.

11.3 Responsabilidades de usuario.

- 11.3.1 Uso de contraseñas.
- 11.3.2 Equipo de usuario desatendido.
- 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.

11.4 Control de acceso a la red.

- 11.4.1 Política de uso de los servicios en red.
- 11.4.2 Autenticación de usuario para conexiones externas.
- 11.4.3 Identificación de los equipos en las redes.
- 11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
- 11.4.5 Segregación de las redes.
- 11.4.6 Control de la conexión a la red.
- 11.4.7 Control de encaminamiento (routing) de red.

11.5 Control de acceso al sistema operativo.

- 11.5.1 Procedimientos seguros de inicio de sesión.
- 11.5.2 Identificación y autenticación de usuario.
- 11.5.3 Sistema de gestión de contraseñas.
- 11.5.4 Uso de los recursos del sistema.
- 11.5.5 Desconexión automática de sesión.
- 11.5.6 Limitación del tiempo de conexión.

11.6 Control de acceso a las aplicaciones y a la información.

- 11.6.1 Restricción del acceso a la información.
- 11.6.2 Aislamiento de sistemas sensibles.

11.7 Ordenadores portátiles y teletrabajo.

- 11.7.1 Ordenadores portátiles y comunicaciones móviles.
- 11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

12.1 Requisitos de seguridad de los sistemas de información.

- 12.1.1 Análisis y especificación de los requisitos de seguridad.

12.2 Tratamiento correcto de las aplicaciones.

- 12.2.1 Validación de los datos de entrada.
- 12.2.2 Control del procesamiento interno.
- 12.2.3 Integridad de los mensajes.
- 12.2.4 Validación de los datos de salida.

12.3 Controles criptográficos.

- 12.3.1 Política de uso de los controles criptográficos.
- 12.3.2 Gestión de claves.

12.4 Seguridad de los archivos de sistema.

- 12.4.1 Control del software en explotación.
- 12.4.2 Protección de los datos de prueba del sistema.
- 12.4.3 Control de acceso al código fuente de los programas.

12.5 Seguridad en los procesos de desarrollo y soporte.

- 12.5.1 Procedimientos de control de cambios.
- 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 12.5.3 Restricciones a los cambios en los paquetes de software.
- 12.5.4 Fugas de información.
- 12.5.5 Externalización del desarrollo de software.

12.6 Gestión de la vulnerabilidad técnica.

- 12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

13.1 Notificación de eventos y puntos débiles de seguridad de la información.

- 13.1.1 Notificación de los eventos de seguridad de la información.
- 13.1.2 Notificación de puntos débiles de seguridad.

13.2 Gestión de incidentes y mejoras de seguridad de la información.

- 13.2.1 Responsabilidades y procedimientos.
- 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
- 13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

- 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
- 14.1.2 Continuidad del negocio y evaluación de riesgos.
- 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
- 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
- 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.

15.1 Cumplimiento de los requisitos legales.

- 15.1.1 Identificación de la legislación aplicable.
- 15.1.2 Derechos de propiedad intelectual (DPI).
- 15.1.3 Protección de los documentos de la organización.
- 15.1.4 Protección de datos y privacidad de la información de carácter personal.
- 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
- 15.1.6 Regulación de los controles criptográficos.

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.

- 15.2.1 Cumplimiento de las políticas y normas de seguridad.
- 15.2.2 Comprobación del cumplimiento técnico.

15.3 Consideraciones sobre las auditorías de los sistem. de información.

- 15.3.1 Controles de auditoría de los sistemas de información.
- 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.