Escuela Politécnica Superior de Linares

Grado en Ingeniería telemática

UNIVERSIDAD DE JAÉN
Escuela Politécnica Superior de Linares

Trabajo Fin de Grado

SISTEMA DE MONITORIZACIÓN Y DETECCIÓN DE RED – OSSEC

Alumno: María Isabel Pinilla Medina

Tutor: Prof. D. Juan Carlos Cuevas Martínez
Depto.: Ingeniería de Telecomunicación

Septiembre, 2018

Resumen

En el presente Trabajo Fin de Grado se presenta una herramienta de seguridad en las redes de ordenadores que permite la detección de actos maliciosos y no deseados en dichas redes. Así, el objetivo fundamental del presente trabajo es la instalación, configuración y puesta en marcha de la herramienta OSSEC, destinada a la monitorización de intrusiones en los sistemas. Esta herramienta detectará posibles ataques o amenazas a la integridad, completitud y confidencialidad de la información que contienen los sistemas. Se ha planificado y llevado a cabo un plan de pruebas específico para ciertas situaciones, identificadas como un riesgo para los sistemas del esquema de red propuesto. Además, para poder comprender el problema de la seguridad en las redes, se presentará en primer lugar un análisis con los riesgos más relevantes que presentan los sistemas y equipos de las redes de ordenadores actuales, concretamente se dedicará especial interés a las vulnerabilidades de los sistemas operativos, en concreto *Windows* y *Ubuntu*.

Palabras clave: Security, OSSEC, auditoria, amenaza, vulnerabilidad, mecanismos de protección, detección de intrusos.

Abstract

In the present Final Degree Project it is presented a networking security tool that allows the detection of malicious and unwanted activities. Thus, the fundamental aim of the present work is the installation, setting and start-up of the OSSEC tool, which is designed to detect and analyses intrusions in computer systems. This tool will detect attacks or threatening events to the integrity and confidentiality of the information stored in the systems. A specific test plan has been planned and carried out for certain situations identified as a risk for the systems in the proposed network scheme. Furthermore, in order to understand the network security problems, an analysis of the most relevant risks will be performed with special attention to the vulnerabilities of operating systems, specifically Windows and Ubuntu.

Keywords: Security, OSSEC, audit, threat, vulnerability, protection mechanisms, intrusion detection.

CONTENIDO

FIGURAS

TABLAS

1 INTRODUCCIÓN

El principal objetivo de este trabajo es la implementación de un sistema de detección de intrusos en una red y dar a conocer sus características, además de justificar el porqué de su necesidad y qué es la defensa de ataques telemáticos. En principio, para llevar a cabo un ataque se tienen que dar tres circunstancias: que exista o que se descubra una vulnerabilidad, el empleo de algún mecanismo de amenaza y que haya una motivación. Estos son tres de los objetivos a desarrollar en este proyecto. Serán de especial interés aquellos que puedan afectar a los sistemas operativos *Windows* y *Linux*.

El punto de partida del proyecto, consiste en analizar el estado actual de vulnerabilidades y amenazas a las que están expuestas las redes de ordenadores y sistemas informáticos. Son de especial interés las debilidades de los sistemas operativos, en concreto *Linux* y *Windows*. Como guía, se utilizan estándares de seguridad de gestión de la información, como la ISO27001/2:2013 [1] y guías de buenas prácticas como COBIT versión 5 [2] y las guías STIC [3] del CNN-CERT [4] o los boletines de seguridad de los propios proveedores de sistemas informáticos, como los de *Microsoft* [5].

A través, de los diferentes apartados contenidos en este trabajo se pretende mostrar en qué consiste y cómo funcionan la monitorización de sistemas y equipos informáticos, así como su papel cada vez más solicitado y necesario por las organizaciones, e incluso los particulares

Las amenazas a los sistemas de información están a la orden del día y crecen exponencialmente, algunos ejemplos recientes más destacados sufridos por las grandes compañías han sido los denominados *WannaCry* [6] y *Petya* [7] que se trata de dos códigos maliciosos con el objetivo el robo o secuestro de información para el lucro de los atacantes. Es por ello que en este trabajo se presenta la importancia de implantar sistemas de seguridad y demostrar la necesidad de mantener un nivel de seguridad óptimo. En detalle se define que es un ataque, amenaza o vulnerabilidad, y que tipos hay y cuales son característicos de los sistemas operativos y redes.

Se dedica un punto completo para desarrollar qué es y cómo funciona un sistema de detección de intrusiones. Además, se realiza un planteamiento de los beneficios y ventajas, así como de los inconvenientes de su uso.

Para comprender de forma práctica que es un sistema de detección de intrusiones se propone una herramienta para tratar la detección y monitorización de

intrusiones en host[1], en adelante HIDS (del inglés *host intrusión detection system*). Para ello se hace uso de una herramienta código abierto, concretamente OSSEC (del inglés *open source HIDS security*). Esta herramienta se va a instalar y configurar para evaluar su funcionalidad y eficacia. El despliegue se realizará en sistemas operativos distintos, como *Linux* y *Windows*. Para este despliegue se propone un sencillo esquema de red con máquinas que simularan el comportamiento de un usuario o empleado al uso, una máquina desde la que realizar los ataques y una máquina que llevará la gestión centralizada.

Para facilitar la revisión, teniendo en cuenta un personal sin cualificación técnica avanzada, OSSEC ofrece una interfaz de usuario de seguimiento de los sistemas monitorizados, la cual se ha instalado, configurado e incluido en el plan de pruebas.

1.1 Motivación

Este proyecto surge por la necesidad de protección informática, en la que cada vez más se ve envuelta la sociedad actual. Los posibles ataques, robos de información, manipulación, fraude, intentos de accesos o accesos exitosos no autorizados han incrementado de forma exponencial en lo últimos tiempos, y además, el tamaño y complejidad de las redes es cada vez mayor, lo que establece un alto grado de complejidad para mantener las redes y sistemas protegidos, manteniendo además la información sensible de una forma íntegra, completa, disponible, eficiente y correcta.

Siempre que pensamos en ciberseguridad[2] o seguridad de la información lo asociamos solamente con herramientas criptográficas, cifrado, claves o autenticación pero también son indispensables herramientas con la capacidad de vigilar y alertar en caso de ocurrir una actividad no deseada.

Los ataques o intentos de ataque que cada vez preocupan y tienen una mayor relevancia en las empresas. A continuación, se hace referencia a los ataques informáticos de mayor relevancia en el último año a empresas [8].

Comenzando el año 2017 se alertó de un particular caso de timo denominado “estafa del *CEO*”. Podía ser víctima cualquier empleado con permisos de pagos. El empleado recibiría un supuesto mensaje de urgencia de su superior con carácter de urgencia para realizar alguna operación financiera. En el caso de no identificar el fraude podrían revelarse datos confidenciales. En general a este tipo de estafas se les conoce como “*whaling*” [9]. La elevación de privilegios sin autorización es un ataque habitual

[1] *host* o anfitrión: ordenador, estación de trabajo o equipo simular con capacidad de proceso que aloja servicios o es un puesto de trabajo

[2] Ciberseguridad: Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados

que preocupa a las empresas. En enero de 2016, se produjo un ataque de este tipo llamado "*hot potato*" [10] en sistemas *Windows*, del cual ha escrito sobre en *Elevenpath* [11][3].

Uno de los casos más sonados y difícil de olvidar para muchas empresas fue el incidente del 12 de mayo de 2017, el conocido *WannaCry*, el cual es un ataque de tipo *malware*, concretamente denominado *ransomware*[4] [12]. Afectaba a todos los sistemas *Windows* desde *Windows XP* hasta *Windows Server* 2016. Consintió en una infección a nivel mundial a multitud de organizaciones, en la que se pedía un rescate por devolver el acceso a información que previamente se había bloqueado.

No se hizo esperar mucho el siguiente ataque, el conocido como *Petya*. Es similar al anterior, pero se considera mucho más dañino, puesto que además de limitar el acceso era capaz de inutilizar el equipo. La primera detección de este ataque de alcance mundial fue el 27 de junio de 2017.

En el último trimestre del año 2017 se identificó uno de los riesgos más preocupantes de los últimos tiempos y se trata de un fallo del protocolo WPA2 elevando la inseguridad de las redes *wifi*. La vulnerabilidad está en la comunicación entre el dispositivo y el *router*, pudiendo un atacante interceptar todo el tráfico que sale de cada dispositivo. Se viola la privacidad de los usuarios y permite realizar ataques como inserción de código malicioso, manipulación de DNS o ataque del hombre de en medio (del inglés, *man in the middle attack*) [13].

1.2 Objetivos

En este punto se van a desarrollar los objetivos a obtener en el presente trabajo, los cuales son:

1. Realizar un estudio sobre las amenazas y brechas de seguridad más importantes en la actualidad en los sistemas *Linux* y *Windows*.
2. Realizar un estudio de las soluciones de seguridad más importantes a la intrusión de sistemas.
3. Desplegar y documentar el sistema OSSEC tanto para sistemas *Linux* como *Windows*. Opcional: comprobar la viabilidad de su integración en los laboratorios docentes.
4. Probar la eficacia de la protección que ofrece OSSEC a través de un banco de pruebas comparativo de sistemas *Linux* y *Windows*.

[3] *Elevenpath*: unidad de ciber-seguridad del grupo telefónica

[4] *Ransomware*: es un software malicioso que bloquea el acceso a los sistemas y exige un pago a la víctima para devolver los permisos.

5. Implementar un portal de seguimiento personalizado de los sistemas monitorizados con OSSEC dado que esta información debe llegar a personal sin conocimientos técnicos avanzados.

1.3 Metodología

En este punto, se van a describir las tareas planificadas para la realización del presente proyecto y así alcanzar los objetivos establecidos.

En primer lugar, se procederá a buscar información bibliográfica sobre amenazas y brechas de seguridad en sistemas. Se complementará esta información aportando soluciones de seguridad en redes y sistemas.

Se va a realizar un estudio del sistema OSSEC desde su procedimiento de instalación, configuración inicial, programación de las alertas y análisis de los resultados de las pruebas.

Previo al banco de pruebas, se realizará una evaluación de los riesgos y posibles vulnerabilidades de los sistemas del esquema de red propuesto, basado en el estándar ISO/IEC 27001 [1] y en la metodología de análisis de riesgos margerit [14]. En base a esta evolución, se aplicará la y la ISO/IEC 27002:2013 [1], objetivos de control de COBIT versión 5 [2] y de las recomendaciones de ITIL versión 3 [15], además se ha tenido en cuenta el marco operacional definido por el CNN-CERT en la guía CCN-STIC 804 [16].

Para la realización de las pruebas de eficacia de la herramienta se desplegará el sistema OSSEC en dos entornos distintos, ya que se trata de una aplicación multiplataforma, se implementarán los agentes en dos sistemas operativos, *Linux* y *Windows*, para realizar comparativas. En los agentes se generarán alarmas que serán enviadas y gestionadas por el servidor. OSSEC soporta interfaces web para la visualización de las alarmas. Se plantearan situaciones de riesgo y vulnerabilidades para las que se propondrán medidas de control para mitigarlas con los recursos disponibles de OSSEC.

El análisis de los experimentos tendrá en cuenta parámetros de evaluación como: fidelidad de la alerta con la situación detectada, tiempo de reacción de la alerta y alertas fallidas o inexistentes.

Para facilitar la accesibilidad de las alarmas al usuario se dispondrá un portal de recepción y monitorización de notificaciones.

Finalmente, se obtendrán conclusiones.

1.4 Estructura del proyecto

El presente proyecto describe las aportaciones y características de los Sistemas de Detección de Intrusos, en adelante IDS, en una organización. En este punto, se hace una breve descripción de los que se contiene cada apartado del presente proyecto.

En el estado del arte se aportan otras herramientas de funcionamiento similar a la que se propone en el proyecto. Además, contiene los aspectos más relevantes para hacer comprender mejor la materia sobre la que se va a trabajar.

En el siguiente punto, se aporta la información necesaria para entender de donde surgen las necesidades de herramientas como las que conciernen al presente trabajo, siendo de gran importancia y sirviendo de punto de partida para comprender perfectamente el objetivo y la función de este tipo de herramientas. En el punto, siguiente se da la respuesta a la problemática planteada en el punto anterior, la cual sirve como introducción de la herramienta de estudio.

A continuación, se entra más en detalle en los sistemas de detección de intrusiones. Se describe el tipo de herramienta, su comportamiento, arquitectura y las principales características para hacer un uso apropiado y una buena aplicación de este tipo de sistemas. Posteriormente, se describe de forma precisa la herramienta OSSEC y sus principales características. Se evalúa la efectividad de la herramienta y se pone en práctica toda la teoría planteada en los puntos anteriores. Se planifica un mecanismo de evaluación y se realizan pruebas de implementación y de eficacia de las configuraciones planteadas. Por último, en los anexos se puede encontrar información sobre la instalación y configuración de la herramienta de estudio.

2 ESTADO DEL ARTE

En este punto se define el entorno de la herramienta que abarca este proyecto. Se refieren múltiples estudios e informes relacionados directamente con la herramienta o con sistemas similares. Se muestran situaciones de la vida cotidiana en las que queda palpable la necesidad de emplear herramientas de monitorización de seguridad, presentándose además una comparativa de este tipo de herramientas.

2.1 Estudios y artículos relacionados

Se aportan en este punto, publicaciones y noticias de actualidad relacionadas con el tema que se aborda en este proyecto.

Según indica el *Sans Institute*[5] [17] en una de sus publicaciones, la detección y gestión de intrusiones ha evolucionado de forma exponencial en los últimos años. En su artículo "*Logging and Monitoring to Detect Network Intrusions and Compliance Violations in the Environment*" [18] propone una solución de detección basada en registros. La solución es similar a la aportada en el proyecto actual salvo que en el proyecto que el estudio de *Sans Institute* está enfocado a sistemas de detección en redes y el proyecto actual está destinado a sistemas operativos.

El instituto nacional de ciberseguridad o CERTSI, ha publicado un estudio sobre los sistemas de detección y prevención de intrusos. Incluyen detalles sobre la instalación y consejos de algunas aplicaciones. Entre otras, la herramienta OSSEC, que es la que se trata en este proyecto, y una similar llamada *Snort* [19] o *Suricata* [20]. También, define otras herramientas de monitorización como IPS, sistemas para detectar y responder de forma activa ante un ataque; o SIEM, que es una herramienta capaz de realizar un análisis a tiempo real de las alertas generadas por *hardware* o el *software* para gestionar la información de seguridad y posteriormente elaborar informes [21]. En el proyecto actual se da una visión más precisa de la instalación y configuración del sistema OSSEC y sobre el plan de pruebas para revisar su eficacia.

El CNN-CERT[6] [4] aporta entre las guías de seguridad de las STIC [22] la guía CNN-STIC 817 [23] no clasificada[7], forma parte del esquema nacional de seguridad de gestión de ciberincidentes. En dicha guía, en el punto 6.2 se hace referencia al uso de sistemas de monitorización y detección de intrusiones.

[5] *Sans Institute*: organización cooperativa de investigación y formación de seguridad. Se considera una fuente de información y certificación de seguridad confiable y de las más grandes del mundo, según ellos mismos.

[6] CCN-CERT: organismo dedicado a alertar y responder de forma rápida y eficiente ante ciberataques a cualquier organismo o empresa pública.

[7] No clasificada: información que puede ser leído por cualquier público.

2.2 Herramientas de monitorización de tráfico disponibles en el mercado

En este punto se hará un breve resumen de algunas herramientas de monitorización disponibles en el mercado actual. Se ofertan multitud de herramientas que permiten monitorizar los eventos[8] [24] y alertas en caso de actividades no deseadas.

Los mecanismos de monitorización [25] surgen de la necesidad del mantenimiento y de garantizar la continuidad del funcionamiento de los sistemas. Aunque una red presente un correcto funcionamiento al principio con el paso del tiempo puede sufrir ataques, deterioro o disminución del rendimiento, lo que incrementa el riesgo de fallo de la seguridad de los sistemas.

A continuación, se describen las características más importantes de las herramientas más destacables de monitorización:

Wireshark [26]: se incluye entre las herramientas de análisis de tráfico más conocidas y usadas del mundo. Es multiplataforma (*Windows*, *Linux*, Solaris, etc.). Ofrece lectura en profundidad de cientos de protocolos, entre ellos: *Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI*. Permite una revisión de los eventos de red hasta el nivel más profundo de los mensajes.

Snort [19]: herramienta de prevención de intrusión de redes de código fuente abierto[9]. Analiza protocolos, búsquedas de contenidos y detección de ataques, como escaneos de puertos o desbordamientos de búfer. Puede funcionar de tres modos distintos. Como sistema que captura tráfico o en inglés s*niffer*, registro de paquetes o como sistema de detección de intrusión de red (NIDS). Es una herramienta de fácil manejo aun disponiendo de muchas opciones y configuraciones.

Suricata [20]: solución de código fuente abierto, desarrollado por OISF (del inglés, *Open Information Security Foundation*). Se encarga de monitorizar el tráfico realizado funciones tanto de IDS (del inglés, *intrusion detection system*) como IPS (del inglés, *Intrusion Prevention System*) y alertar en caso de eventos sospechosos. Se basa en reglas y firmas.

Tripwire [27]: herramienta diseña para monitorizar, al detalle, cualquier cambio de la integridad de los archivos directorios, registros, parámetros de configuración, DLL, puertos, servicios, protocolos, etc. Ofrece una solución denominada “entorno de aislamiento” o más conocido por su traducción en inglés como *sandbox* [28] que consiste

[8] Evento: hecho o acontecimiento que puede ocurrir en un momento determinado y generalmente de imprevisto.

[9] Código abierto: software que se basa en la aportación colaboradores, es decir, permite que los usuarios puedan modificar y mejorar su diseño.

en un espacio cerrado donde se puede ejecutar cualquier aplicación sospechosa sin riesgo de propagación o daño.

Nagios [29]: Permite monitorizar las infraestructuras de TI al completo para garantizar que funcionan de forma correcta. Detecta situaciones no deseadas que pueden afectar al funcionamiento de procesos de negocio y alerta a tiempo para aplicar un plan de actuación. Puede analizar aplicaciones, servicios, sistemas operativos, protocolos y sistemas internos. Ofrece información detallada de a través de su interfaz web. Entre los servicios de red que puede monitorizar están: SMTP[10] (del inglés *Simple Mail Transfer Protocol*), POP3[11] (del inglés *Post Office Protocol*), HTTP[12] (del inglés *Hypertext Transfer Protocol*), ICMP[13](del inglés *Hypertext Transfer Protocol*), SNMP[14](del inglés *Simple Network Management Protocol*). Realiza monitorización remota mediante SSL[15] (del inglés *Secure Sockets Layer*) o SSH[16] (del inglés *Secure Shell*). Además, permite visualizar el estado de la red en tiempo real, aportando informes y gráficas sobre los resultados obtenidos del análisis.

PandoraFMS [30]: se considera una de las herramientas de código abierto del mercado que más fácil se adapta a cada negocio, para monitorizar: dispositivos, infraestructuras aplicación, servicio y proceso de negocio. Analiza la información que los agentes recolectan y envían hacia un servidor. Puede funcionar en multitud de sistemas operativos como *DNU*/*Linux*, *Solaris*, *Windows*, etc.

Zabbix [31]: solución de código abierto para monitorizar y registrar el estado de redes, servidores, la nube y aplicaciones. Es multiplataforma, pudiendo utilizarse tanto en *Linux* como en *Windows*. Tiene una gran capacidad de alcance de monitoreo (más de mil elementos). Ofrece un potente interfaz gráfico y es de fácil configuración.

[10] SMTP: protocolo de red para recibir y enviar correos electrónicos.

[11] POP3: protocolo para recibir y descargar mensajes de correo electrónico que están alojados en un servidor remoto.

[12] HTTP: protocolo de intercambio de información en la *world wide web*.

[13] ICMP: protocolo para la administración de la información relacionada con errores en equipos de una red.

[14] SNMP: protocolo de intercambio de información de gestión de los equipos de red.

[15] SSL: protocolo para una trasferencia de información segura entre un usuario y la web.

[16] SSH: protocolo que permite mantener conexiones remotas de forma segura.

3 Vulnerabilidades de los sistemas informáticos

En el punto anterior se ha definido que un ataque o intrusión aprovecha una vulnerabilidad para materializarse. Es por esto que es necesario entender qué es una vulnerabilidad para saber dónde poner el foco de vigilancia. Así, una vulnerabilidad, en el mundo de la seguridad informática, es cuando una capacidad o una característica de un activo [32] de un sistema de información es susceptible de ser atacada. También, se define como la probabilidad de que una amenaza se haga realidad y se convierta en un ataque [33]. Se clasifican en tres tipos:

Vulnerabilidad intrínseca o inherente: lo contiene el activo y es propio de la amenaza.

Vulnerabilidad efectiva: se ha generado tras la implantación de una defensa.

Vulnerabilidad residual: es la que todavía queda tras la aplicación de salvaguardas implantadas siguiendo el resultado del proceso de análisis y gestión de riesgos.

3.1 Vulnerabilidades generales en sistemas operativos y aplicaciones

En este punto, se verán las principales vulnerabilidades [33] [34] de los sistemas operativos en general que pueden desembocar en un fallo de seguridad informática. Entre otras, se describen a continuación, las más comunes a cualquier sistema operativo:

Contraseñas: El problema que se suele dar en las contraseñas es que sean demasiado débiles: muy cortas, poco robustas y no demasiado complejas. Por lo que cualquier atacante no encontrará demasiadas dificultades en descubrir las contraseñas de los usuarios del sistema.

Vulnerabilidades de configuración: Se dan cuando no se gestiona de forma adecuada el *software*. Se debe fundamentalmente a un fallo humano, ya sea por desconocimiento, o por malintencionado.

Accesos indebidos: Cuando no se realiza una adecuada administración de los parámetros para la validación de entrada en el sistema.

Asignación de permisos y roles no apropiados: Se da cuando desde el exterior se puede acceder a la raíz del sistema, ya que no existe un nivel adecuado de protección.

Inyección de comandos: Cuando se inyecta un código en otro sistema. Existen de varios tipos:

- Inyección SQL**:** Debilidad a nivel de base de datos. Se da cuando no hay un filtrado de información a través del código SQL. Esto da la oportunidad

a los atacantes de modificar y obtener información sensible o inyectar código malicioso.

Error de búfer: Se da cuando el almacenamiento de datos en el sistema se realiza sin una correcta gestión del espacio del disco.

Fallo de autenticación: No se realiza, o se realiza de forma incorrecta, la autenticación de un usuario en un sistema.

Error en la gestión de recursos: No se gestionan de forma equilibrada los recursos del sistema. Llevaría a una interrupción del correcto funcionamiento del sistema.

Error de diseño: Cuando se realiza un incorrecto diseño de las aplicaciones y programas, lo que dejaría puertas abiertas a los atacantes.

Ventanas engañosas (*windows spoofing*): Anuncios de sorteos engañosos para obtener información del usuario o del equipo.

3.1.1 Análisis de vulnerabilidades

Una forma de evaluar una vulnerabilidad [33] [34] es teniendo en cuenta el tiempo trascurrido entre que es una amenaza potencial hasta que se materializa. Otro factor a tener en cuenta es la frecuencia con la que se materializa la amenaza. Algunos métodos para encontrar vulnerabilidades en un sistema son:

Análisis local para la detección de vulnerabilidades: consiste en realizar pruebas sobre el *software* para valorar la calidad de las aplicaciones, con pruebas como:

Pruebas estáticas: se realiza un análisis del pero no es necesaria la ejecución de código.

Pruebas dinámicas: se requiere ejecución de la aplicación para evaluar efectos y resultados. Se consideran más precisos que las pruebas estáticas.

Análisis de caja blanca: este tipo de análisis se da cuando se realiza un examen del cuerpo interno de las aplicaciones y de los sistemas. Previamente, se recoge información sobre el equipo: archivos de configuración, código de las aplicaciones, etc. Los resultados son más acertados que en el caso del análisis local pero su vez requiere de más consumo de recursos para realizarlo.

Análisis de caja negra: se trata de una revisión exhaustiva de las entradas y salidas del sistema. El método que se aplica consiste en simular el posible comportamiento de un atacante.

3.2 Principales vulnerabilidades de *Windows* y *Linux*

Tras la introducción del punto anterior sobre las principales vulnerabilidades, donde se ha explicado desde un punto de vista más general independientemente del sistema que sea, en este apartado se van a mostrar algunas vulnerabilidades que suelen

ser aprovechadas por los atacantes de sistemas operativos *Windows* y *Linux*. En CVE *details*[17] [35], se han seleccionado las estadísticas que se han considerado más representativas de todo el conjunto de vulnerabilidades detectadas en los distintos sistemas operativos. Para *Windows,* las versiones que se han seleccionado son: *Windows Server* 2008 y *Windows* 7, ya que son las que más número de vulnerabilidades se han detectado en total, y, además la versión 7 es una de las que se han realizado las pruebas de eficiencia de la herramienta OSSEC:

Para *Windows Server* 2008 [36]

Número de vulnerabilidades por año (desde 2007 hasta la actualidad). Se comentará más adelante, comparando con el resto de sistemas operativos.

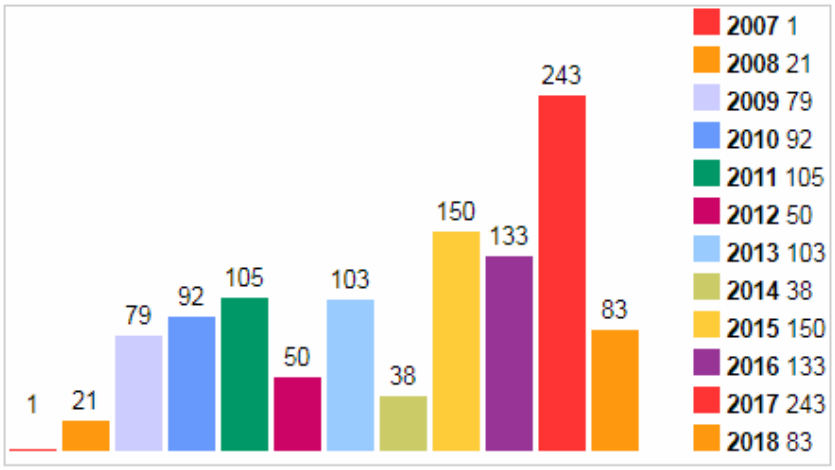


Figura 1 Vulnerabilidades detectadas por CVE Details desde 2007 a 2018 para Windows Server 2008

En la siguiente figura se detecta identifican todas las vulnerabilidades detectadas en *Windows* server 2008. Destacan: elevación de privilegios no autorizada, ejecución de código malicioso y obtención de información sensible. Se seguirá comentando más adelante.

[17] CVE *details:* web que recoge información sobre las vulnerabilidades detectadas.

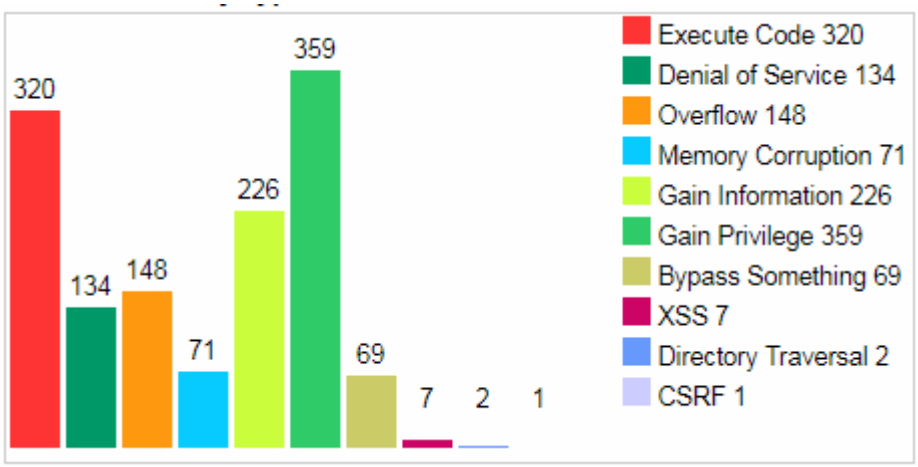


Figura 2 Tipos de vulnerabilidades detectadas por CVE details desde 2007 a 2018 para Windows Server 2008

Distrución los valores de la Figura 2 de las vulenrabilidades detectadas en Windws Server 2008.

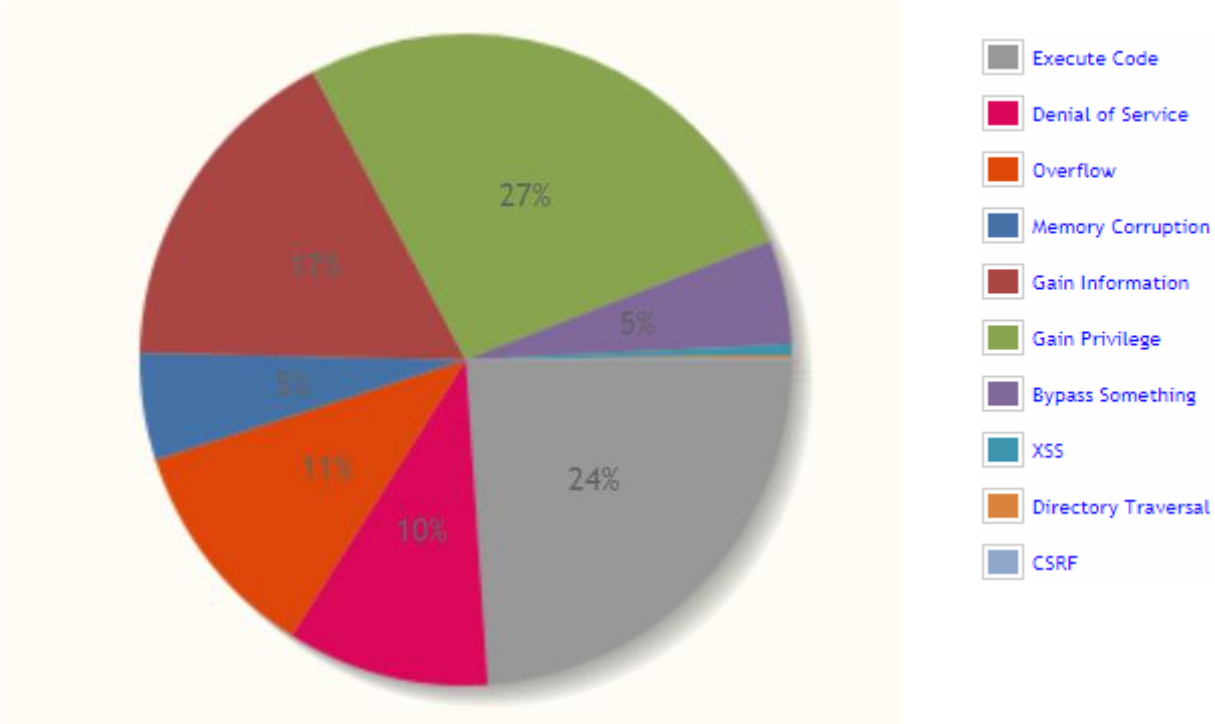


Figura 3 Reparto de las vulnerabilidades detectadas por CVE details desde 2007 a 2018 para Windows Server 2008

Para *Windows* 7 [37]

Número de vulnerabilidades por año (desde 2009 hasta la actualidad). Se comentará más adelante, comparando con el resto de sistemas operativos.

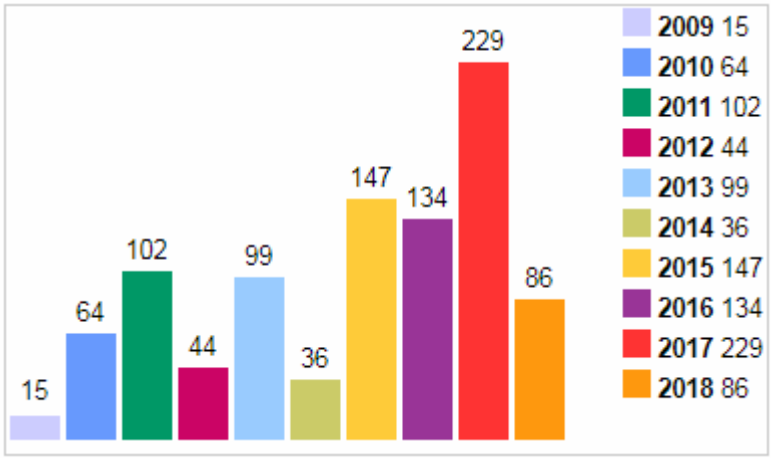


Figura 4 Número de vulnerabilidades detectadas por CVE Details desde 2009 a 2018 para Windows 7

Similar a la versión de *Windows,* mostrada anteriormente, donde las principales vulnerabilidades detectadas para *Windows* 7 son elevación de privilegios, obtención de información y ejecución de código.

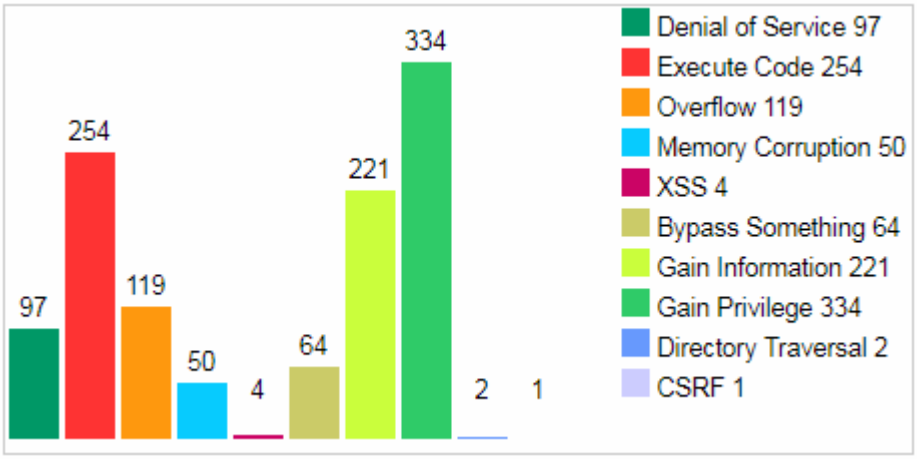


Figura 5 Tipos de vulnerabilidades detectadas por CVE Details desde 2009 a 2018 para Windows 7

A continuación, se muestra la distribución de la anterior Figura 5 en porcentajes de las vulnerabilidades detectadas.

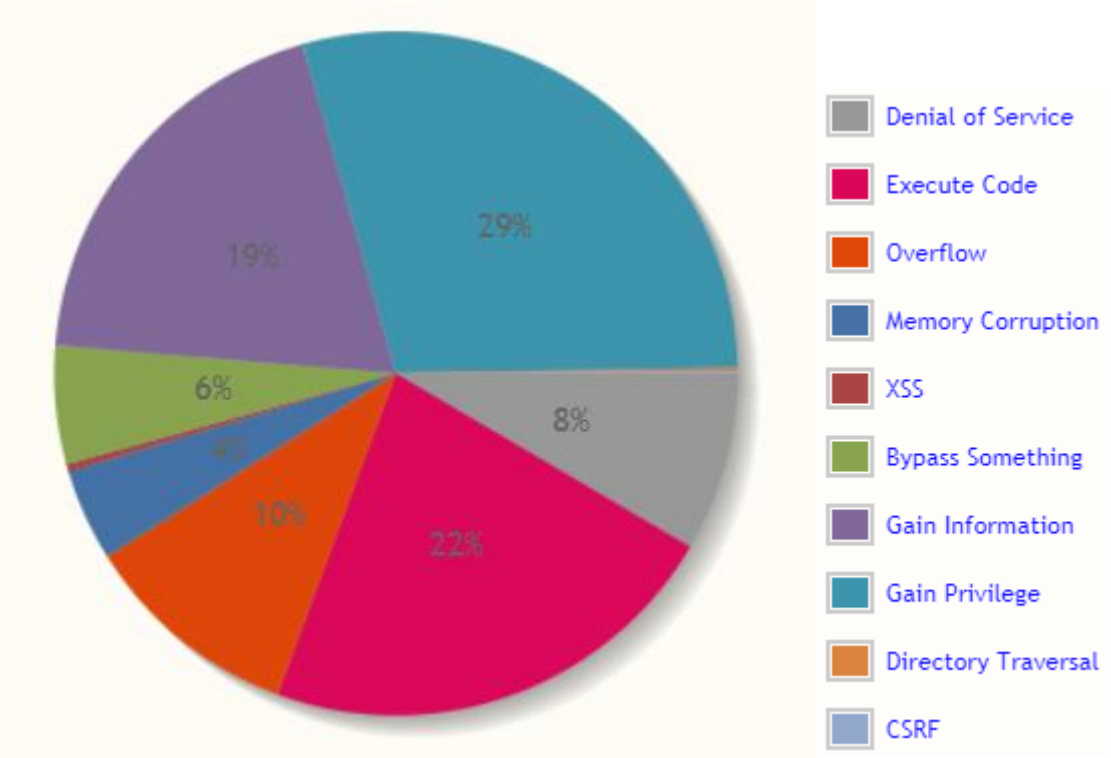


Figura 6 Reparto de las vulnerabilidades detectadas por CVE Details desde 2009 a 2018 para Windows 7

Para *Linux Debian* [38]**:**

Número de vulnerabilidades por año (desde 1999 hasta la actualidad). Se comentará más adelante, comparando con el resto de sistemas operativos.

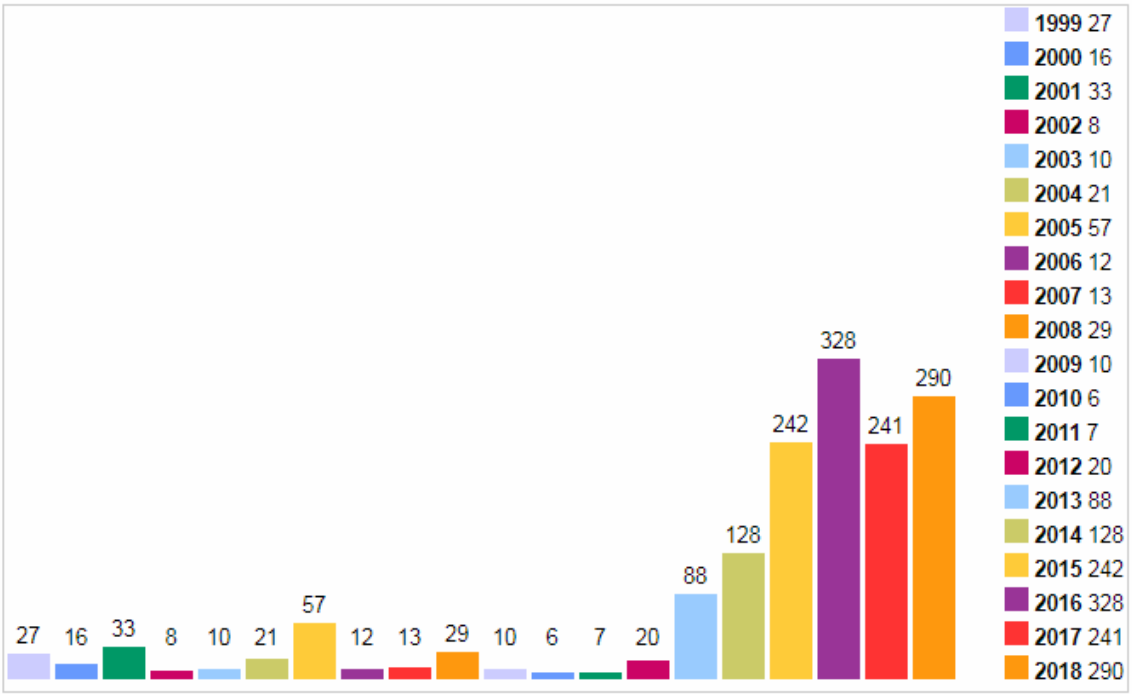


Figura 7 Número de vulnerabilidades detectadas por CVE Details desde 1999 a 2018 para Linux Debian

En esta versión de *Linux* las vulnerabilidades que más se han detectado son: denegación de servicio, ejecución de código malicioso

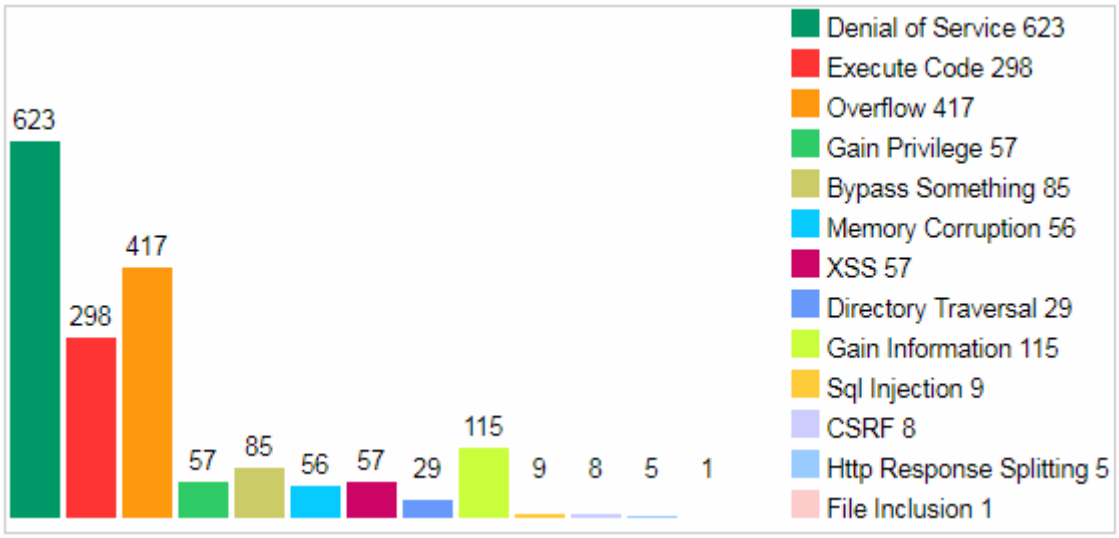


Figura 8 Tipos de vulnerabilidades detectadas por CVE Details desde 1999 a 2018 para Linux Debian

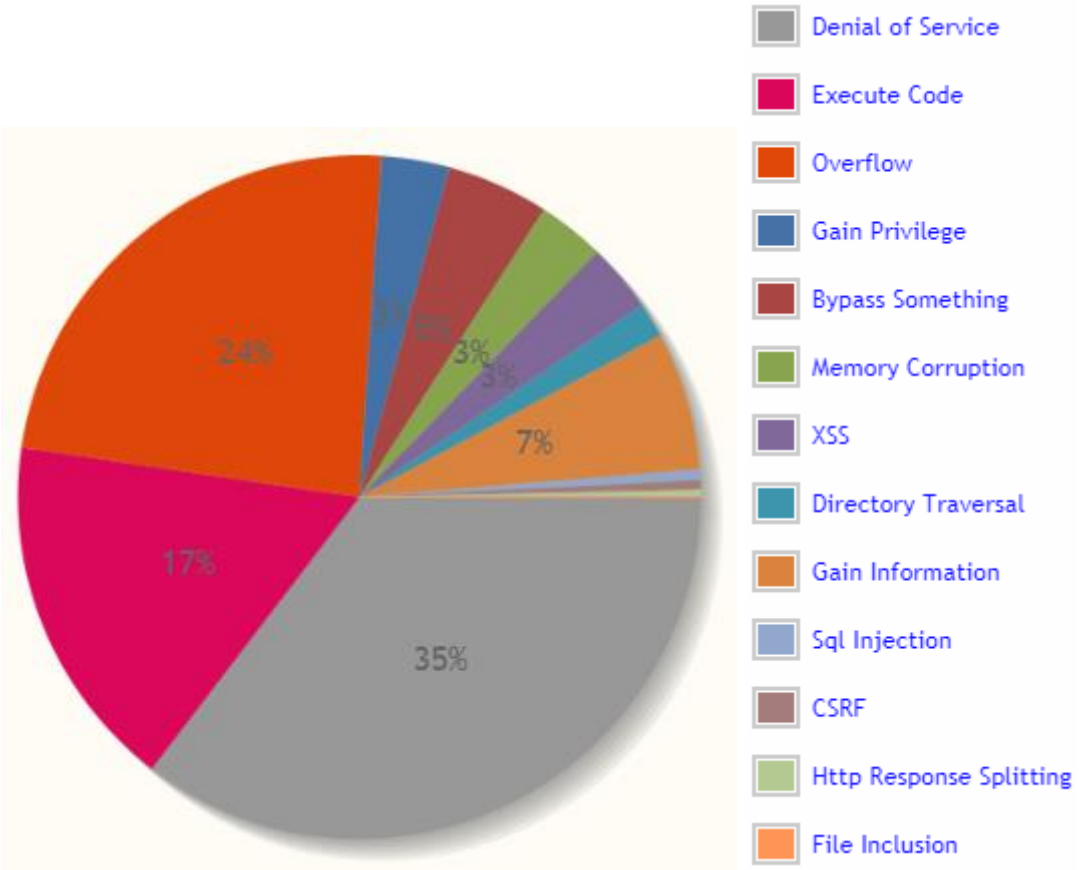


Figura 9 Reparto de las vulnerabilidades detectadas por CVE details desde 1999 a 2018 para Linux Debian

Para *Linux Ubuntu* [39]

Número de vulnerabilidades por año (desde 2004 hasta la actualidad). Se comentará más adelante, comparando con el resto de sistemas operativos.

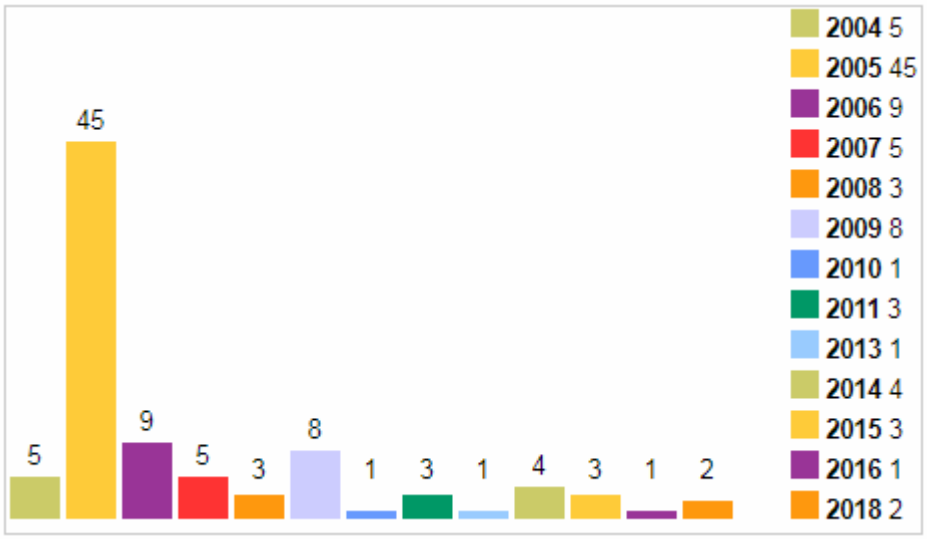


Figura 10 Número de vulnerabilidades detectadas por CVE Details desde 2004 a 2018 para Linux Ubuntu

Coinciden con el sistema operativo anterior *Linux Debian*: denegación de servicio, ejecución de código malicioso

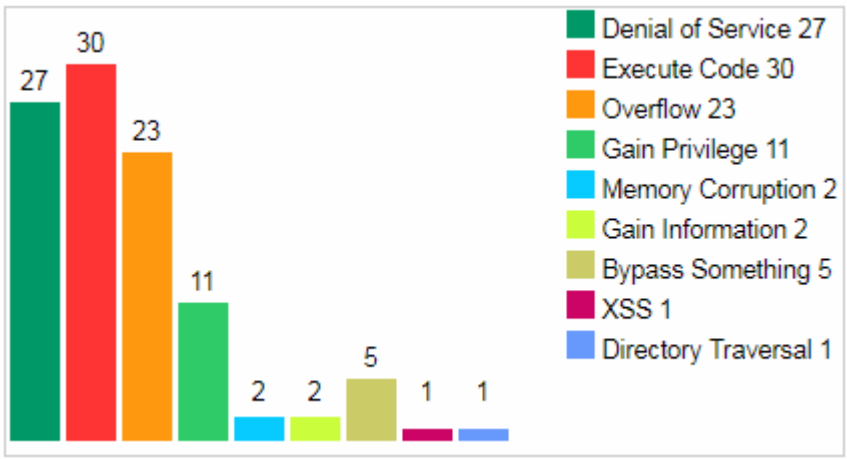


Figura 11Tipo de vulnerabilidades detectadas por CVE Details desde 2004 a 2018 para Linux Ubuntu

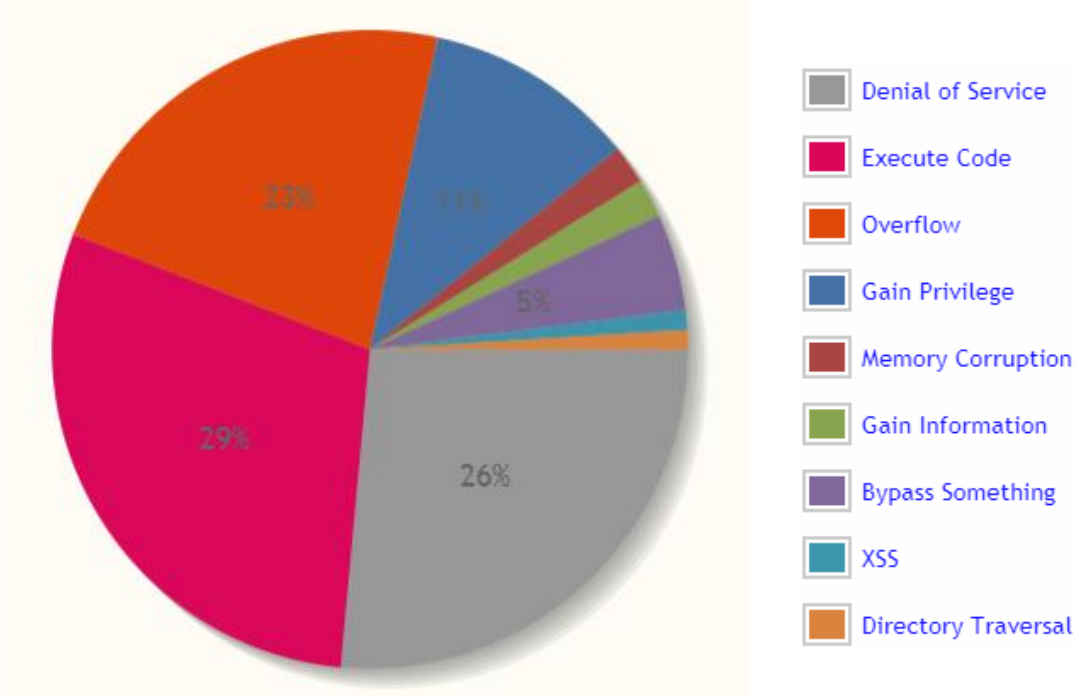


Figura 12 Reparto de las vulnerabilidades detectadas por CVE Details desde 2004 a 2018 para Linux Ubuntu

Si comparamos entre sistemas operativos, se observa en las primeras gráficas que las versiones de *Windows* coincidieron en picos de mayor número de vulnerabilidades en los años 2015 y 2017, este hecho se asemeja con *Linux Debian* aunque tuvo su pico en 2016 y todavía está por valorar el año 2018, ya que viendo su evolución (en 6 meses casi alcanza el 90% de lo que se detectó en 2016) quizá podría superarlo. Por el contrario, *Ubuntu* apenas tienes vulnerabilidades en estos años, incluso en 2017 no tuvo. En cuanto al tipo, las vulnerabilidades detectadas en las versiones *Windows* coinciden, en orden de mayor a menor número: elevación de privilegios, obtención de información y ejecución de código. Sin embargo, para las versiones de *Linux* las principales son: elevación de privilegios, obtención de información y ejecución de código. La única similitud entre ambos sistemas operativos es la vulnerabilidad de ejecución de código malicioso.

3.3 Vulnerabilidades detectadas para *Windows* y *Linux*

A continuación, se van a detallar y a dar ejemplos reales de en qué consisten las principales vulnerabilidades que afectan a los sistemas operativos [40] y el origen por lo que se pueden dar. En CVE *Details* se observa, desde una visión a alto nivel, el total de vulnerabilidades detectadas para los distintos proveedores de *software* desde 1999 [41].

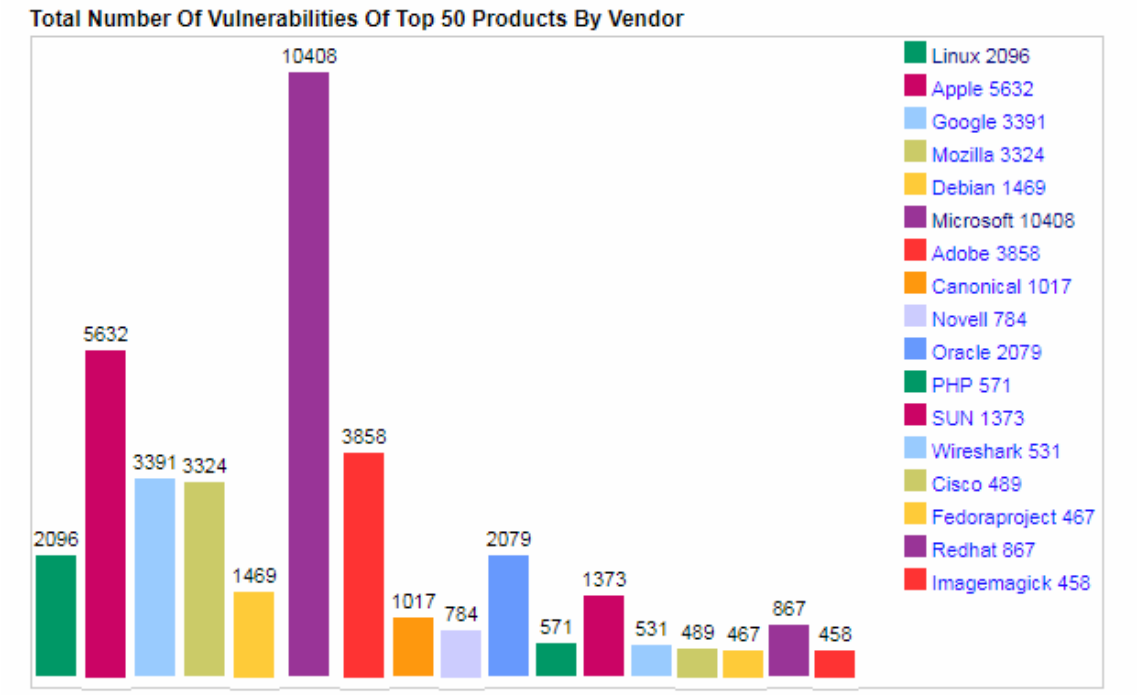


Figura 13 Total de vulnerabilidades detectadas por proveedor

El criterio utilizado para determinar las principales vulnerabilidades está basado en resultados recientes aportados por el Instituto Nacional de Normas y Tecnología o NIST (del inglés, *National Institute of Standards and Technology*), en su base de datos de vulnerabilidades, llamado el *NVD* (del inglés *national vulnerability database*) que a su vez está conformado por el listado de identificadores comunes para las vulnerabilidades de ciberseguridad detectadas, llamado CVE[18] (del inglés *common vulnerabilities and exposures*). Además, se darán algunos ejemplos reales evaluados y de publicados por el NIST o en la propia página de *Microsoft*. La clasificación de las vulnerabilidades se ha tomado de referencia la evaluación del NIST.

Desde CVE *Details* [42], se obtienen las principales vulnerabilidades y se seleccionan, a continuación, la Tabla 1 muestra las vulnerabilidades con mayor ocurrencia. Las vulnerabilidades se identifican mediante un código único y pertenecen al CWE[19] (del inglés, *common weakness enumeration)* [43].

Identificador CWE	Nombre vulnerabilidad	Número de vulnerabilidades
94	Error al controlar la generación de código ('Inyección de código')	2209
284	Problemas de control de acceso (autorización)	2373

[18] CVE: listado de vulnerabilidades de seguridad de la información, identificadas por un código único.

[19] CWE: listado de tipos de vulnerabilidades de software dirigido a desarrolladores y profesionales de la seguridad. Fue creada, al igual que CVE para unificar la descripción de las debilidades de seguridad de software en cuanto a arquitectura, diseño y código se refiere.

22	Limitación incorrecta de un nombre de ruta a un directorio restringido ('Trayectoria de ruta')	2390
89	Desinfección inadecuada de elementos especiales utilizados en un comando SQL ('Inyección SQL')	4986
200	Exposición a la información	5028
20	Validación de entrada incorrecta	5770
79	Falla en preservar la estructura de la página web (*'Cross-site Scripting'*)	9107
119	Error al restringir las operaciones dentro de los límites de un búfer de memoria	10844

Tabla 1 Principales vulnerabilidades. Fuente: CVE Details.

Y se obtiene el siguiente gráfico:

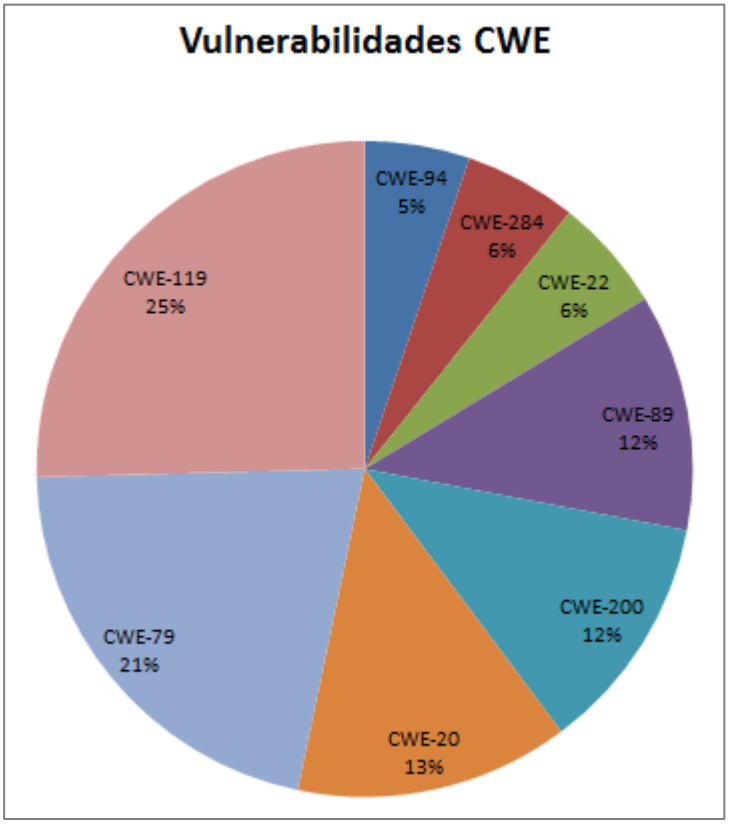


Figura 14 Vulnerabilidad CWE detectadas. Fuente: CVE Details.

Otra fuente de información, *Securelist*[20] [44] publica una lista con las principales vulnerabilidades [45]. Comparando con la anterior no hay muchas discrepancias, coinciden en du mayoría con fallos por búfer *overflow*, problemas de control de acceso o autenticaciones no apropiadas e inyecciones de código malicioso.

[20] *Securelist:* oficina central de los expertos de seguridad de *Kaspersky Lab*.donde se realizan publicaciones de informes y resultados de seguridad.

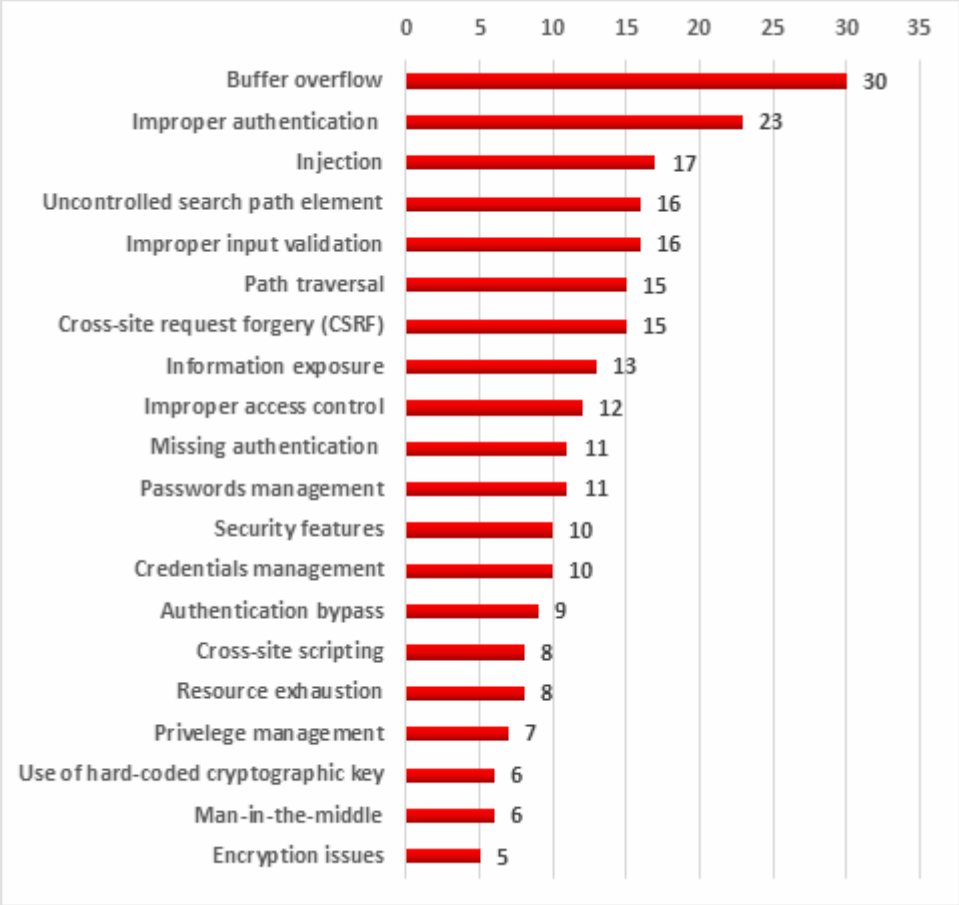


Figura 15 Principales vulnerabilidades: Fuente: Securelist.

Es importante tener en cuenta que la denominación de las vulnerabilidades en las gráficas anteriores del punto 3.1.1 no corresponde en exactitud con las vulnerabilidades descritas en los puntos siguientes, ya que las gráficas corresponden con CVE *Details* y los siguientes puntos son a partir de la valoración del CWE y del NVD. No obstante, para no perder trazabilidad se facilita en cada punto el código CWE que corresponde con cada vulnerabilidad y se explicará de forma detallada las distintas definiciones. Además, *Mitre* también ofrece en la web del *itsecdb* [46] más datos para completar información sobre vulnerabilidad, parches y cumplimiento en *Windows* y *Linux*.

3.3.1 Error de búfer

Esta vulnerabilidad, puede dar pie a que un usuario aproveche para ejecutar un código malicioso para acceder a un espacio de memoria fuera del límite previsto del búfer, haciéndose con el control del sistema. Para saber más sobre esta vulnerabilidad, acceda a la página de CWE, que se identifica como CWE-787 [47], CWE-125 [48], CWE-119 [49] y CWE-123 [50].

Windows:

- Vulnerabilidad CVE-2018-0935: *Internet Explorer* en *Microsoft Windows* 7 *SP1, Windows Server* 2008 y R2 SP1, *Windows* 8.1 y *Windows RT* 8.1, *Windows Server* 2012 y R2, *Windows* 10 *Gold*, 1511, 1607, 1703, 1709 y *Windows Server* 2016 permiten la ejecución remota de código, debido a cómo el motor de scripts maneja los objetos en la memoria, también conocido como "vulnerabilidad de daños en la memoria del motor de secuencias de comandos". Este ID de CVE es exclusivo de CVE-2018-0876, CVE-2018-0889, CVE-2018-0893 y CVE-2018-0925. La última actualización sobre esta vulnerabilidad se encuentra disponible en la página del NIST [51], del CVE [52] y CVE *Details* [53]. El centro tecnológico de seguridad de *Microsoft* [54] incluye también información sobre esta vulnerabilidad.
- Vulnerabilidad CVE-2018-0778: *Microsoft Edge* en *Windows* 10 1709 permite a un atacante ejecutar código arbitrario en el contexto del usuario actual, debido a la forma en que el motor de scripts maneja los objetos en la memoria, también conocido como "vulnerabilidad de daños en la memoria del motor de *scripting*". Este ID de CVE es exclusivo de CVE-2018-0758, CVE-2018-0762, CVE-2018-0768, CVE-2018-0769, CVE-2018-0770, CVE-2018-0772, CVE-2018-0773, CVE- 2018-0774, CVE-2018-0775, CVE-2018-0776, CVE-2018-0777 y CVE-2018-0781. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [55] y del CVE [56].

Linux:

- Vulnerabilidad CVE-2018-1125: *procps-ng*[21] [57] antes de la versión 3.3.15 es vulnerable a un desbordamiento de búfer de pila tras ejecutar un *pgrep*[22]. La última actualización en la página del NIST [58] y CVE [59].
- Vulnerabilidad CVE-2018-10689: *blktrace*[23] [60] (también conocido como *Block IO Tracing*) 1.2.0, que se usa con el núcleo de *Linux* y *Android,* tiene un desbordamiento de búfer en la función *dev_map_read*[24] en *btt*/*devmap*.*c*[25] porque las matrices del dispositivo son demasiado pequeñas, como se demuestra cuando salta el error *invalid_free*[26] cuando se utiliza el programa

[21] *procps-ng:* paquete generado dinámicamente por el núcleo para proporcionar información sobre el estado de las entradas en su tabla de procesos.

[22] *Pgrep:* comando que busca una expresión regular dada en la línea de comandos, y muestra los ID de los procesos que coincidan con dicha expresión.

[23] *Blktrace:* paquete de herramientas que aporta información sobre el tiempo que gasta en el subsistema de E/S de disco.

[24] *dev_map_read:* función para leer la información del fichero de mapas de desarrollo, *devmap*.c.

[25] *btt*/*devmap*.c: fichero generado como salida de *blktrace*. Crea una línea de tiempo y recopilar estadísticas.

[26] *invalid_free*: error que indica espacio libre inválido.

btt[27] [61] en un archivo modificado. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [62] y CVE [63].

3.3.2 Fuga de información/divulgación

Esta vulnerabilidad, se da cuando información sensible se expone a una persona o personas que no están autorizadas para ello, ya sea de forma intencionada o no. Para saber más sobre esta vulnerabilidad que se identifica como CWE-200 acceda a la página del CWE [64].

***Windows*:**

- Vulnerabilidad CVE-2018-1234: El agente de autenticación *RSA*[28] (*Rivest scureidShamir Adleman*) versión 8.0.1 y anterior para el servidor *Web IIS*[29] [65] *de Windows* se ve afectado por un problema donde los permisos de la lista de control de acceso o *ACL (*del *inglés, Access Control List)* de *Windows* no eran suficientes para evitar el acceso de usuarios no autorizados. El atacante con acceso local al sistema puede aprovechar esta vulnerabilidad para leer las propiedades de configuración del agente de autenticación. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [66], del CVE [67] y Aviso de seguridad (boletín de seguridad de *Microsoft*) 180012 [68].
- Vulnerabilidad CVE-2018-0887: Existe una vulnerabilidad de divulgación de información, cuando el núcleo de *Windows* no puede inicializar correctamente una dirección de memoria, también conocida como "vulnerabilidad de divulgación de información del núcleo de *Windows*". Esto afecta a *Windows* 7, *Windows Server* 2012 R2, *Windows* RT 8.1, *Windows Server* 2008, *Windows Server* 2012, *Windows* 8.1, *Windows Server* 2016, *Windows Server* 2008 R2, *Windows* 10, *Windows* 10 *Server*. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [69] y del CVE [70].

Linux:

- Vulnerabilidad CVE-2018-3639: Los sistemas con microprocesadores que utilizan ejecución especulativa y ejecución especulativa de lecturas de memoria antes de conocer las direcciones de todas las escrituras anteriores pueden permitir la revelación no autorizada de información a un atacante con

[27] *Btt:* programa que analiza las trazas de bloque de E/S producidas por *blktrace*[16].

[28] Autenticación *RSA:* mecanismo para la autenticación administrativa servidor a servidor.

[29] *ISS*: plataforma, de *Microsoft*, para hospedar sitios web, servicios y aplicaciones.

acceso como usuario local a través de un análisis de canal lateral, esta vulnerabilidad es también conocida como *Specultaive Store Bypass* (SSB) versión 4 [71]. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [72] y del CVE [73].

- Vulnerabilidad CVE-2016-0777: La función *resend_bytes*[30] en el cliente en *OpenSSH*[31] [74] 5.x, 6.x y 7.x antes de 7.1p2, permite a los servidores remotos obtener información confidencial de la memoria del proceso, solicitando la transmisión de un búfer completo, como leer una clave privada que se utiliza al establecer la comunicación. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [75] y del CVE [76].

3.3.3 Control de acceso inapropiado

Esta vulnerabilidad, existe porque no se realiza una restricción de acceso adecuada, para la autorización de cada usuario. Para saber más sobre esta vulnerabilidad que se identifica como CWE-284 acceda a la página del CWE [77].

***Windows*:**

- Vulnerabilidad CVE-2018-8225: Existe una vulnerabilidad de ejecución remota de código en *DNSAPI.dll*[32], que pertenece al servicio de nombres de dominio (*DNS*) de *Windows, que implica* no manejar adecuadamente las respuestas *DNS*, y que se conoce como "vulnerabilidad de ejecución remota de código *DNSAPI* de *Windows*". Esto afecta a *Windows* 7, *Windows Server* 2012 R2, *Windows* RT 8.1, *Windows Server* 2008, *Windows Server* 2012, *Windows* 8.1, *Windows Server* 2016, *Windows Server* 2008 R2, *Windows* 10, *Windows* 10 *Server*. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [78] y del CVE [79].
- Vulnerabilidad CVE-2016-8824: Todas las versiones de *NVIDIA*[33] [80] *Windows GPU Display Driver*[34] contienen una vulnerabilidad en el controlador[35] de capa de modo núcleo (*nvlddmkm.sys*[36]) para

[30] *Resend_bytes:* función *para reenviar datos que no recibió el servidor debido a una desconexión.*

[31] *OpenSSH*: herramienta para realizar conexiones remotas de forma segura.

[32] *DNSAPI.dll:* archivo*, desarrollado por Microsoft,* de biblioteca de vínculos dinámicos de Windows que se utiliza para ejecutar ciertos programas y extensiones del navegador.

[33] NVIDIA: es una empresa dedicada al desarrollo de tecnologías de procesamiento de gráficos y circuitos integrados para equipos como ordenadores o dispositivos móviles.

[34] *NVIDIA Windows GPU Display Driver:* controlador de pantalla*.*

[35] Controlador: es un programa que permite comunicar el software con el hardware de un sistema.

[36] *nvlddmkm.sys:* archivo de configuración de *Windows, relacionado con el controlador de pantalla.*

DxgDdiEscape[37] donde los controles de acceso incorrectos permiten a un usuario escribir una parte del registro destinado únicamente a usuarios con privilegios, lo que lleva a una escalada de privilegios. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [66] y del CVE [81].

Linux:

- Vulnerabilidad CVE-2017-17807: El subsistema de claves en el núcleo de *Linux* anterior a 4.14.6 omite una comprobación de control de acceso al agregar una clave al "conjunto de solicitud de claves" a través de la llamada al sistema "*request_key*[38]", permitiendo a un usuario local claves al "conjunto de claves", con solamente permiso de búsqueda (sin permiso de escritura) para ese "conjunto de claves". La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [82] y del CVE [83].
- Vulnerabilidad CVE-2015-9006: En *RPM*[39] (del inglés, *Resource Power Manager*) para todas las versiones de *Android* de *CAF*[40] que utilizan el núcleo de *Linux*, podría existir una vulnerabilidad de control de acceso incorrecto. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [84] y del CVE [85].

3.3.4 Permisos y privilegios

Esta vulnerabilidad, se produce porque no se realiza una adecuada asignación de permisos y roles en la gestión de accesos. Para saber más sobre esta vulnerabilidad, acceda a la página del CWE, se identifica como CWE-264 [86]. También *Microsoft* [87], publica un artículo sobre qué cuentas son más atractivas para el robo de credenciales, normalmente son las de administradores o con más privilegios altos. Algunos ejemplos reales registrados en la página del NIST son:

***Windows*:**

- Vulnerabilidad CVE-2017-15302: En *CPUID CPU-Z*[41] a 1.81, existen derechos de acceso incorrectos a un controlador de modo núcleo (por ejemplo, *cpuz143_x64.sys*[42] para la versión 1.43) que pueden dar como

[37] *DxgDdiEscape:* función que pertenece a la biblioteca *nvlddmkm.sys* del componente Kernel Mode Layer.

[38] *request_key*: función de petición de clave.

[39] *RPM:* es un controlador dedicado para administrar recursos compartidos del centro de operaciones de seguridad.

[40] *CAF:* es un repositorio de código donde *Qualcomm* [236] publica sus códigos, concretamente *Code Aurora* [235].

[41] *CPUID CPU-Z:* programa para recopilar información del sistema como nombre del procesador, placa base, memoria, tamaño o la frecuencia interna del núcleo.

[42] C*puz143_x64.sys*: es un controlador de modo núcleo de *Windows*, informa sobre el estado de la *CPU*.

resultado la divulgación de información o la elevación de privilegios, debido a una lectura arbitraria de cualquier dirección física a través de *ioctl*[43] [88] *0x9C402604*. Cualquier aplicación que se ejecute en el sistema (*Windows*), incluidos los usuarios de espacio aislado, puede emitir un *ioctl* a este controlador sin ninguna validación. Además, el controlador puede asignar cualquier página física en el sistema y devuelve la dirección asignada de la página del mapa al usuario: eso produce una fuga de información. El proveedor indica que la lectura arbitraria en sí misma es un comportamiento intencional (para la funcionalidad de exploración de *ACPI*[44] [89]; el problema de seguridad es la falta de una ACL[45] [90] *(*del inglés*, Access Control List)*. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [91] y del CVE [92].

- Vulnerabilidad CVE-2017-11829: *Microsoft Windows* 10 permite una vulnerabilidad de elevación de privilegios cuando la optimización de entrega de actualizaciones de *Windows* no aplica correctamente los permisos de archivos compartidos. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [93] y del CVE [94].
- Vulnerabilidad CVE-2018-8134: Existe una vulnerabilidad de elevación de privilegios por la forma en que la API[46] *(*del inglés*, Application Programming Interface)* de núcleo de *Windows* impone permisos, también conocida como "vulnerabilidad de *Windows Elevation of Privilege*". Esto afecta a *Windows Server* 2012 R2, *Windows* RT 8.1, *Windows Server* 2016, *Windows* 8.1, *Windows* 10, *Windows* 10 *Server.* La última actualización sobre esta vulnerabilidad está disponible en la página del *NIST* [95] y del CVE [96].

Linux:

- Vulnerabilidad CVE-2017-16939: La implementación de la política de vuelco *XFRM*[47] [97] en *net/xfrm/xfrm_user.c* en el núcleo de *Linux* anterior a 4.13.11 permite a los usuarios locales obtener privilegios o causar una denegación de servicio (*use-after-free*). La última actualización sobre esta vulnerabilidad está disponible en la página del NIST *y* del CVE [98].

[43] *IOCTL*: dispositivo de control de entrada y salida de datos. Es la interfaz a través de la cual una aplicación se puede comunicar directamente con un controlador de dispositivo.

[44] *ACPI*: característica de *Windows* para administración de energía.

[45] *ACL*: lista de control de acceso. Identifica un administrador y especifica los derechos de acceso permitidos y restringidos.

[46] *API*: es un conjunto de funciones y procedimientos que cumplen una o muchas funciones con el fin de ser utilizadas por otro software.

[47] *XFRM:* es la interfaz de configuración y supervisión entre la parte del espacio de usuario de *IPsec* y los componentes del núcleo de *IPsec.*

- Vulnerabilidad CVE-2017-5551: La función *simple_set_acl*[48] en *fs/posix_acl.*c[49] en el núcleo de *Linux* anterior a 4.9.6 preserva el bit *setgid*[50] durante una llamada *setxattr*[51] que involucra un sistema de archivos *tmpfs*[52], que permite a los usuarios locales obtener privilegios de grupo aprovechando la existencia de un programa *setgid* con restricciones en la ejecución permisos. Nota: esta vulnerabilidad existe debido a una solución incompleta para CVE-2016-7097 [99]. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [100] y del CVE [101].

3.3.5 Validación de datos de entrada

Esta vulnerabilidad se encuentra cuando un sistema no realiza una validación correcta del flujo de datos de entrada a un programa o sistemas, por lo que un atacante podría introducir un código malicioso. Para saber más sobre esta vulnerabilidad, acceda a la página del CWE, se identifica como CWE-20 [102]. Algunos ejemplos reales registrados en la página del NIST:

***Windows*:**

- Vulnerabilidad CVE-2018-8997: En *Windows Master* (también conocido como *Windows Optimization Master*) 7.99.13.604, el archivo del controlador *WoptiHWDetect.sys*[53] permite a los usuarios locales provocar una denegación de servicio y como resultado un pantallazo azul (*BSOD,* del inglés *Blue Screen of Death)* o posiblemente otro impacto no especificado debido a que no validan los valores de entrada de *ioctl* 0xf1002004. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [103] y del CVE [104].
- Vulnerabilidad CVE-2017-5092: La validación insuficiente de la entrada no confiable en los complementos de *PPAPI* en *Google Chrome* antes de 60.0.3112.78 para *Windows* permitió que un atacante remoto realizara potencialmente un escape de espacio aislado a través de una página *HTML* diseñada. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [105] y del CVE [106].

***Linux*:**

[48] *simple_set_acl:* función que preserva el *bit setgid,* durante una llamada *setxattr*.

[49] *fs/posix_acl.*c: archivo de sistemas *Linux* que contiene listas de control de acceso a directorios y archivos.

[50] *setgid:* es un *bit,* que al ejecutarse el archivo que lo tiene configurado, lo hace con los permisos del grupo que posee el archivo.

[51] *Setxattr:* función para asignar atributos a un fichero o directorio.

[52] *Tmpfs:* sistema de almacenamiento, en algunos sistemas operativos de tipo Unix

[53] *WoptiHWDetect.sys:* archivo controlador, de sistemas *Windows, para la gestión del hardware.*

- Vulnerabilidad CVE-2018-1000026: La versión 4.8 del núcleo de Linux, y en adelante, contiene una vulnerabilidad de validación de entrada insuficiente, en el controlador de tarjeta de red *bnx2x* que puede dar como resultado denegación del servicio, porque la confirmación de firmware de la tarjeta de red saca la tarjeta fuera de línea. Este ataque parece ser explotable, mediante el envío de un paquete muy grande y especialmente diseñado a la tarjeta *bnx2x*. Esto se puede hacer desde una VM invitada que no es de confianza. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [107] y del CVE [108].
- Vulnerabilidad CVE-2017-18065: En *Android* para *MSM*[54], *Firefox OS* [109] y *QRD Android*, con todas las versiones de *Android* de *CAF* utilizando el núcleo de *Linux*, la validación de entrada que se recibe del *firmware* es incorrecta, lo que conduce a la posibilidad de ejecución de código arbitrario. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [110] y del CVE [111].

3.3.6 Gestión de credenciales

Esta debilidad se da cuando no se realiza una correcta gestión de las credenciales almacenadas o generadas en un sistema. Para saber más sobre esta vulnerabilidad, acceda a la página del CWE [112] que se identifica como CWE-255 [113]. Algunos ejemplos reales registrados en la página del NIST:

***Windows*:**

- Vulnerabilidad CVE-2018-1000041: La versión de *librsvg*[55] de *GNOME* contiene una vulnerabilidad de validación de entrada, que puede provocar que el nombre de usuario de la víctima de *Windows* y el hash de contraseña *NTLM*[56] se filtren a atacantes remotos a través de *SMB*[57] *(*del inglés *Server Message Block)*. Este ataque parece ser explotable a través de que la víctima procese un archivo *SVG*[58] *(*del inglés *Scalable Vector Graphics)*. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [114] y del CVE [115].

[54] *Android* para *MSM:* es un proyecto que permite crear una plataforma basada en *Android.*

[55] *Librsvg:* biblioteca de código abierto para la generación de gráficos vectoriales escalables*.*

[56] *NTLM:* protocolo de autenticación, de usuarios y equipos, para acceder a un servidor o un controlador de dominio*.*

[57] *SMB:* es un protocolo de red para la compartición de archivos e impresoras.

[58] *SVG:* formato de gráficos*.*

- Vulnerabilidad CVE-2018-1217: El administrador de instalación de *Avamar*[59], en *Dell EMC Avamar Server* 7.3.1, 7.4.1 y 7.5.0, y el dispositivo de protección de datos integrado *Dell EMC* 2.0 y 2.1, se ven afectados por una vulnerabilidad de control de control de acceso faltante que podría permitir que un atacante remoto no autenticado lea o cambie las credenciales del servicio de descarga local (*LDLS*). Estas se utilizan para conectarse al soporte en línea de *Dell EMC*. Si la configuración de *LDLS* se cambió a una configuración no válida, es posible que el Administrador de instalación de *Avamar* no pueda conectarse al sitio web de soporte en línea de *Dell EMC* con éxito. El atacante remoto no autenticado también puede leer y usar las credenciales para iniciar sesión en la Asistencia en línea de *Dell EMC*, personificando las acciones del servicio *AVI* utilizando esas credenciales. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [116] y del CVE [117].

***Linux*:**

- Vulnerabilidad CVE-2018-1240: En versiones posteriores a la 3.0.0.38 de *Dell EMC ViPR Controller*, contienen una vulnerabilidad de exposición a la información en el *VRRP*[60] *(*del inglés *Virtual Router Redundancy Protocol). VRRP* se predetermina a una configuración insegura en el componente *keepalived* de *Linux* que envía la contraseña del clúster en texto sin formato a través de multidifusión. Un usuario malintencionado, que tiene acceso a la subred *vCloud* donde se implementa *ViPR*[61], podría detectar la contraseña y usarla para hacerse cargo de la IP virtual del clúster y provocar una denegación de servicio en ese sistema *ViPR Controller***.** La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [118] y del CVE [119].
- Vulnerabilidad CVE-2017-18270: En el núcleo de *Linux* anterior a 4.13.5, un usuario local podría crear llaveros para otros usuarios a través de comandos *keyctl*, configurando valores predeterminados no deseados o causando una denegación de servicio. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [120] y del CVE [121] .

[59] *Avamar:* sistema de recuperación y respaldo de información.

[60] *VRRP:* protocolo de penetración no propietario definido en el RFC 3768. Diseñado para aumentar la disponibilidad de la puerta de enlace por defecto dando servicio a máquinas en la misma subred.

[61] *ViPR*: aplicación para la gestión del almacenamiento en aplicaciones de virtualización, como *VMware* de *Microsoft*.

3.3.7 Errores de canales y rutas de comunicación

Esta vulnerabilidad se genera por canales y rutas debilites de comunicación. Para saber más sobre esta vulnerabilidad que identifica como CWE-417 acceda a la página del CWE [122]. Para *Linux* no se ha encontrado ninguna vulnerabilidad relacionada. Un ejemplo real de *Windows* registrado en la página del NIST es el siguiente:

***Windows*:**

- Vulnerabilidad CVE-2018-7295: *Square Enix Final Fantasy XI*V 4.21 y 4.25 en *Windows* se ve afectado por la gestión incorrecta de la integridad del mensaje durante la transmisión en un canal de comunicación, lo que permite a un "atacante en el medio", o en inglés "*man in the middle*", robar credenciales de usuario. Esto se soluciona en el parche 4.3. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [123] y del CVE [124].

3.3.8 Servidores Web

Este punto contiene lo que se ha determinado como vulnerabilidad de servidores web pero no es una vulnerabilidad como tal para el NIST sino que engloba otras como: CWE-*79* [125], *Cross-Site Scripting (*XSS*);* CWE-*444* [126], *Inconsistent Interpretation of* HTTP *Requests ('*HTTP *Request Smuggling');* CWE-*918* [127], *Server -Side Request Forgery (*SSRF*)*. Al ubicar un servidor web en un sistema operativo se habilitan servicios y funcionalidades que pueden descubrir debilidades como: configuraciones pobres, por defecto o erróneas, cuando se hacen despliegues sin buena planificación de tiempos o desconocimiento del administrador de sistemas; versiones y parches de *software* desactualizados, por descuido o un inadecuado mantenimiento; comunicaciones inseguras entre cliente y servidor, sin cifrar o con protocolos de cifrado inseguros y obsoletos; otras vulnerabilidades que se dan en la propia aplicación, que permiten ataques *Cross-Site Scripting* (XSS) o inyección SQL. Algunos ejemplos, que aún están sin clasificar porque son muy recientes y podrían afectar tanto a *Linux* como a *Windows* son los siguientes:

- Vulnerabilidad CVE-2018-1000556: *WordPress* [128] versión 4.8 + contiene una vulnerabilidad de *Cross Site Scripting (*XSS*).* Puede ocasionar desde el robo de una cookie hasta la inyección del código. Este ataque parece ser explotable a través de un atacante que debe crear una *URL* con carga útil y enviarlo al usuario. La víctima debe abrir el enlace para verse afectado por XSS reflejado. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [129] y del CVE [130].

- Vulnerabilidad CVE-2017-12356: Una vulnerabilidad en la interfaz de administración de una solución web de *Cisco Jabber* [131] *para Windows, Mac, Android* e *iOS* podría permitir que un atacante remoto no autenticado realice un ataque *Cross Site Scripting* (XSS) contra un usuario administrador. La vulnerabilidad se debe a la validación insuficiente de la entrada proporcionada por el usuario por parte de la interfaz de administración basada en la web de un dispositivo afectado. Un atacante podría aprovechar esta vulnerabilidad persuadiendo a un usuario de la interfaz para que haga clic en un enlace diseñado. Un *exploit* exitoso podría permitir al atacante ejecutar código de *script* arbitrario en el contexto de la interfaz o permitir que el atacante acceda a información confidencial basada en el navegador. ID de error de Cisco: CSCvf50378, CSCvg56018 [132]. La última actualización sobre esta vulnerabilidad está disponible en la página del NIST [133] y del CVE [134].

3.4 Vulnerabilidades en la red

Las redes de comunicación, aportan infinidad de ventajas en la vida cotidiana como permitir comunicarnos con personas al otro lado del mundo, realizar cualquier tipo de compra, visualizar en un mapa el punto que deseemos geográfico, etc. pero no debemos perder de vista los riesgos que surgen en cada uno de los procesos [25] [135].

En este punto se muestran vulnerabilidades que se pueden encontrar en cada una de las capas del modelo OSI (del inglés, *Open System Interconnection*) de interconexión de equipos informáticos. La pila OSI se compone de 7 capas o niveles: aplicación, presentación, sesión, transporte, red, enlace y físico. Las vulnerabilidades que presenta cada una de ellas se describen en la tabla 1.

Capas modelo OSI	Vulnerabilidades
Aplicación, presentación y sesión	En esta capa se definen los protocolos de aplicación para el intercambio de datos, se trata de la última capa cuyo cometido es interactuar entre el usuario y la capa de transporte. Aquí se puede ver afectado la integridad, la disponibilidad, no repudio o autenticación [25] [136]. Los ataques que se pueden realzar a este nivel son: Amenazas a la confidencialidad. Suplantación de DNS. Agotamiento de IPs. XSS *(Cross Site Scripting)* Desbordamiento de buffer. Denegación de servicio de redes.

Transporte	Los protocolos más utilizados son TCP y UPD. En este nivel dan riesgos asociados a autenticación, integridad y confidencialidad de la información. Los ataques que se pueden dar son [25]: Ataques de reconocimiento. Impedimento de establecimiento de sesiones TCP. Denegación del servicio.
Red	En este nivel se pueden encontrar vulnerabilidades que afectan a la integridad y confidencialidad de la información. Los ataques que pueden suceder son [25]: Suplantación o IP spoofing. Denegación del servicio.
Enlace	En esta capa se pueden dar complicaciones en el control de acceso y en la confidencialidad. Algunos riesgos que pueden surgir son [25]: Espías en la red. Falsificar direcciones MAC. Envenenamiento ARP.
Físico	Este nivel es el que abarca la conexión desde el equipo final de usuario con la red. En este caso puede surgir el riego de accesos no autorizados [25]. Algunos ejemplos podrían ser: Desconexión del equipo de forma intencionada. Accidentes meteorológicos. Incendios, inundaciones o cualquier otro incidente que impida el correcto funcionamiento del sistema.

Tabla 2 Vulnerabilidades en pila de capas de modelo OSI [25] [136]

4 Amenazas

En el punto actual, se va a definir lo que es una amenaza ya que es la causa que ha propiciado que sea necesario aplicar soluciones de los mecanismos de protección. Según el INCIBE[62] [137], una amenaza [138] es toda aquella acción no deseada que aprovechará una vulnerabilidad (definida esta última en el punto 3 con más detalles), siendo esta es una debilidad propia de las características de un sistema, para afectar a la integridad, confidencialidad o disponibilidad de la información sensible que se quiere proteger porque tiene un valor para una empresa o particular [139] [140].

[62] Incibe: Instituto nacional de ciberseguridad. trabaja para afianzar la confianza digital, elevar la ciberseguridad y la resiliencia y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España.

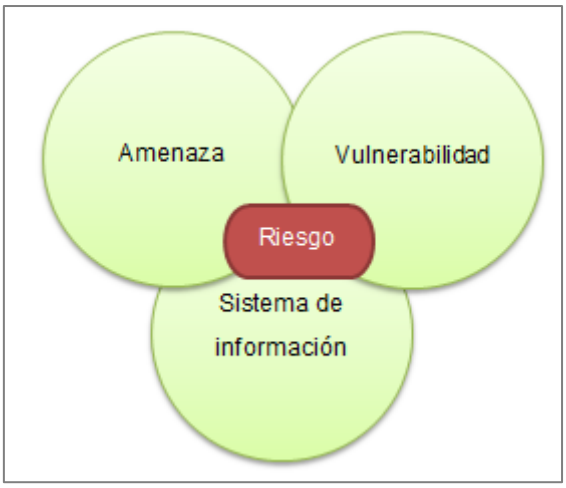


Figura 16 Relación entre ataque, vulnerabilidad y sistema de información y riesgo [138]

El riesgo [138] es la probabilidad de que una amenaza se materialice y el impacto tras producirse. Estas se materializan mediante ataques o intrusiones a los sistemas. Estos conceptos se van a definir en los puntos a continuación.

4.1 Clasificación y tipos de ataques

Es necesario conocer la tipología y el perfil del atacante para optimizar el funcionamiento de la herramienta utilizada.

El usuario que puede originar el ataque puede clasificarse por los permisos y el perfil que tiene:

- Usuario con acceso no autorizado a los sistemas.
- Usuario con acceso autorizado a los sistemas, con privilegios elevados no adecuados.
- Usuario con acceso autorizado a los sistemas, con privilegios elevados o no, pero con mala intención.

Según la intención y el objetivo del atacante puede clasificarse como [141]:

No intencionado: Inundaciones, incendios accidentales, errores/descuidos humanos, fallo en el suministro de energía, mantenimiento deficiente o carencia total de él, accidentes medioambientales, segregación inadecuada de funciones.

Intencionado: Obtención no autorizada de perfiles privilegiados, mal uso de los privilegios, accesos no autorizados exitosos, intentos repetitivos de accesos no autorizados, alteración de la información, empleo de la información para fines no apropiados, vandalismo, borrado de información, robo o fraude.

Por otro lado, según su ejecución los ataques [139] también se clasifican en función de su modo de actuación.

Ataque Pasivo: Es aquél en el que el atacante monitoriza el tráfico en la red para capturar información sensible de la víctima. Son muy difíciles de detectar porque no suelen alterar los sistemas o realizar cambios en los datos.

Ataque Activo: Es aquél en el que el atacante explota la(s) vulnerabilidad(es) descubiertas y obstaculiza el tráfico de datos.

En el ámbito de una organización, la amenaza o la intrusión puede clasificarse dependiendo el origen del que provienen, son:

Externa a la red privada o remota: Los atacantes son externos o ajenos a la Entidad. Los objetivos de ataques son servidores para acceder a información sensible, con motivos como difamación, robo de información por parte de la competencia...

Interna de la organización o corporativa: los atacantes no disponen autorización o no es adecuada. Pueden comprometer la seguridad de la información, servicios de la organización, impedir la correcta continuidad del negocio y producir filtraciones o difamaciones.

Para que un ataque se lleve a cabo se debe contar con material y conocimientos adecuados y con una motivación para realizarlo. Las fases [142] más habituales, por las que suele pasar un ataque son:

1. Descubrimiento del sistema.
2. Localizar vulnerabilidades o puertas abiertas en el sistema.
3. Explotar las vulnerabilidades.
4. Ejecución del ataque o el daño planeado en los sistemas.
5. Eliminar el rastro.

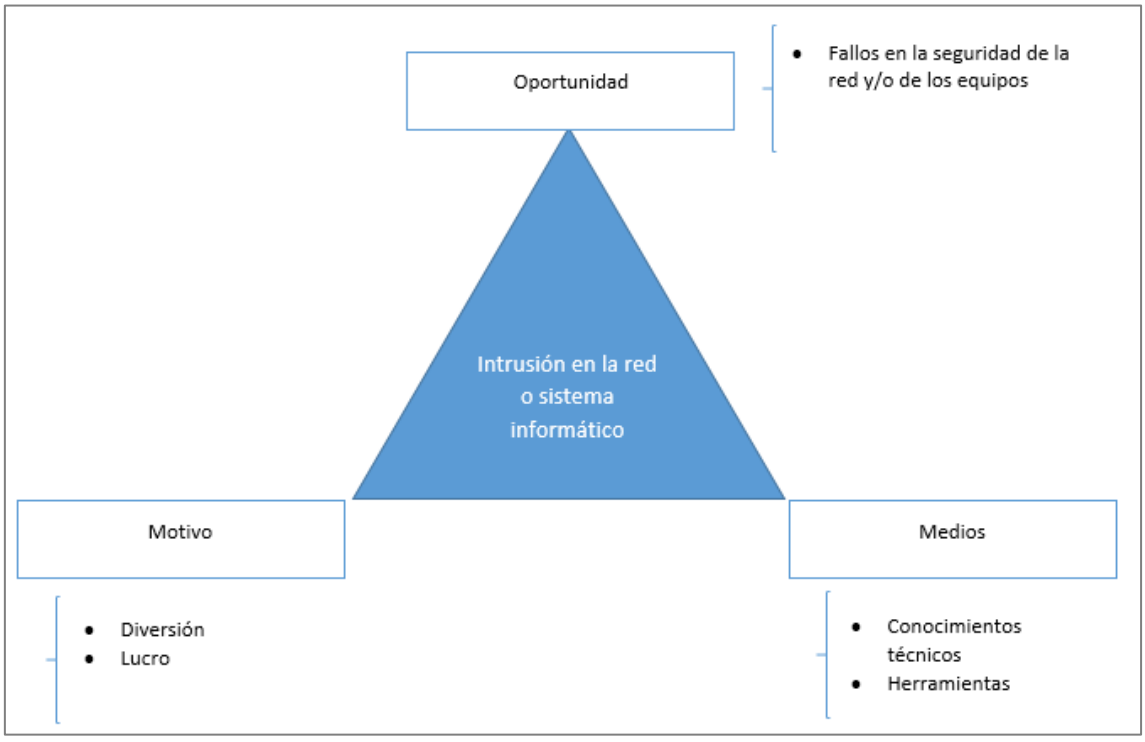


Figura 17 Triángulo explicativo de intrusión [143]

4.2 Identificar amenazas a la seguridad de los sistemas

Para identificar las amenazas [33] [139] se requiere un alto conocimiento del entorno que rodea a los sistemas y a los activos que se desean proteger. Lo ideal es adelantarse a que se materialice el riesgo. Entre otras, las más habituales son:

- Suplantación: Un usuario sin autorización se hace pasar por otro.
- Alteración: Modificación de los datos.
- Repudio: Negar la realización de un hecho delictivo o que atenta a la organización.
- Divulgación de información: Traspaso de información a terceros.
- Denegación del servicio: Servicio inaccesible.
- Elevación de privilegios: Usuarios con unos privilegios no adecuadamente asignados o no autorizado.

Los efectos de las amenazas dependerán del impacto o el daño incidido a los activos. Su valor depende de los siguientes hechos:

- La capacidad que tenga de volver producirse o de expandirse a otros activos.
- Perjuicio causado a los activos.
- El total de usuarios que puedan verse afectados.
- Habilidad para la detección y hallazgo de la amenaza.

También, hay que tener en cuenta la vulnerabilidad del activo, que se verá condicionada por:

- Degradación del activo: Daño sufrido.
- Frecuencia de amenaza: Número de repeticiones en un periodo.

4.3 Intrusos y atacantes de los sistemas y redes

En este punto, se definen los principales tipos de atacantes y ejecutores [142] [144] de las acciones malintencionadas, es decir, se van a definir los tipos de personas que hay detrás de los ataques, su motivación y objetivo hacia los sistemas que se desea proteger:

Hackers [142] [144]: Son sujetos que indagan en los sistemas de una organización en busca de debilidades informáticas para acceder sin autorización. Su motivación es medir su destreza y demostrar su habilidad, pero no con la intención de hacer daño. Aun así, no deja de ser un delito. La palabra hacker deriva del anglosajón, *hack* que su traducción literal sería “Golpear con un hacha”.

Pirata informático o *crackers* [142] [144]: También son conocidos como *blackhats*. Su actividad está fundamentada en el ataque de sistemas para conseguir beneficios por algún tipo de interés (religioso, político económico) o por dañar una entidad. Además, son especialistas en obtener y distribuir programas o elementos de contenido digital, infringido la ley de propiedad intelectual.

Rastreadores o *sniffers* [142] [144]: Se dedican a espiar a recolectar mensajes que transitan en la red.

Expertos en telefonía o *phreakers* [142] [144]: Se dedican a manipular las redes telefónicas para poder hacer uso de la red de forma gratuita.

Emisores de basura informática o s*pammers* [142] [144]: Su objetivo es producir un colapso de los servidores que alojan los buzones de correo mediante el envío masivo de correos no solicitados.

Creadores de virus y programas dañinos [142] [144]: Su objetivo es demostrar y poner en alza su habilidad, creando códigos y programas maliciosos. Son similares a los hackers, aunque a diferencia de estos tienen otras intenciones malintencionadas como el robo de datos sensibles para obtener un beneficio económico.

Persona sin habilidades técnicas o *Lammers* (*wannabes*) [142] [144]**:** Son individuos sin conocimientos técnicos que hacen uso de herramientas maliciosas para realizar ataques.

Personal interno de una organización por mal uso [142] [144]: Aquella persona que pueden dañar a una entidad, que puede darse por falta de conocimientos, por descontento, por desinterés o por algún intento de difamación o divulgación.

Ex empleados [142] [144]: similar al anterior, pueden causar daños perdiendo o borrando información relevante debido al conocimiento que pueden tener de la entidad en la que trabajaban.

Personal interno de una organización - fallo humano [142] [144]: es una agresión al sistema por un mal uso de los mismos, falta de mantenimiento, por falta de conocimiento, descuido, abuso o malas prácticas de los servicios informáticos. El usuario no realiza el mantenimiento adecuado de la información que maneja, provocando daños en los datos o permitiendo que otros accedan a ellos. No suele tener un objetivo o motivación claros, son más habitualmente producidos por descuidos o dejadez.

Intrusos remunerados [142] [144]: son expertos para robar o sabotear una organización bajo sueldo con el objetivo de comprobar las medidas de seguridad implementadas por la empresa.

4.4 Técnicas de amenazas a sistemas

Se pueden dar multitud de eventualidades y situaciones no deseadas, entre otros ataques informáticos a los sistemas. En este apartado se indican métodos con los que los atacantes amenazan la seguridad de los sistemas de sus víctimas. Además, se presentan algunas estadísticas emitidas por entidades del sector sobre las principales amenazas.

En primer lugar, *McAfee*[63], empresa que ofrece servicios y productos de seguridad y habitualmente reconocidos por sus productos antivirus, publicó en diciembre de 2017 un informe sobre amenazas informáticas [145]. El crecimiento de *malware* ha ido incrementando en estos dos últimos años como se ve en la siguiente imagen:

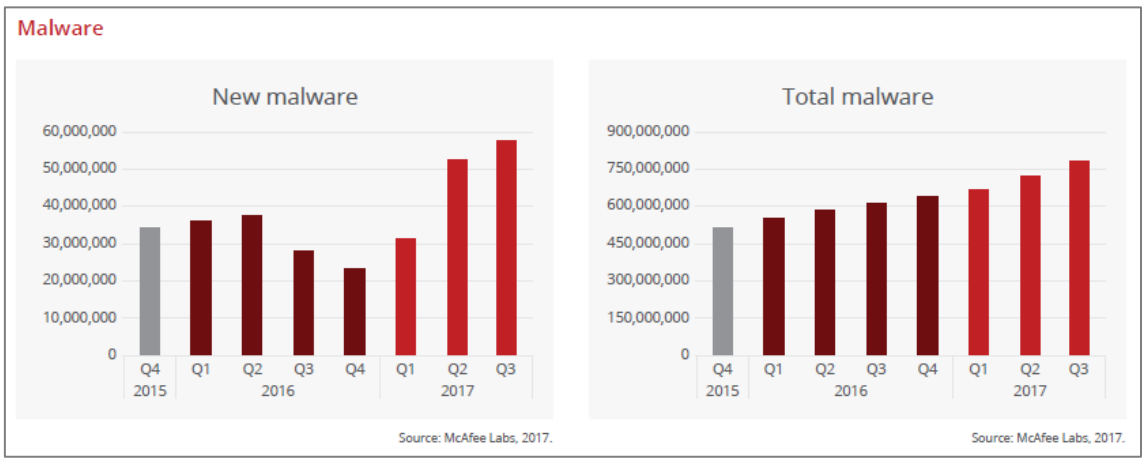


Figura 18 Evolución de ataques malware. Fuente: McAfee.

En la siguiente Figura se muestras los 10 principales ataques de 2016 y 2017, en orden de mayor a menor ocurrencia: Desconocido (no se identifica en el documento en una leyenda que se aporta con este dato exactamente pero se interpreta como que todavía no se ha determinado el tipo de ataque), secuestro de cuentas, fuga de información, *malware*, denegación de servicio, ataque dirigido, inyección código SQL, estafa en los comprobantes de salarios e impuestos (formulario W2, del inglés *Wage and Tax Statement)* y vulnerabilidades propias de los sistemas.

[63] *McAfee: Empresa que provee soluciones de ciberseguridad ofreciendo servicios de protección, detección y neutralización de amenazas a las empresas.*

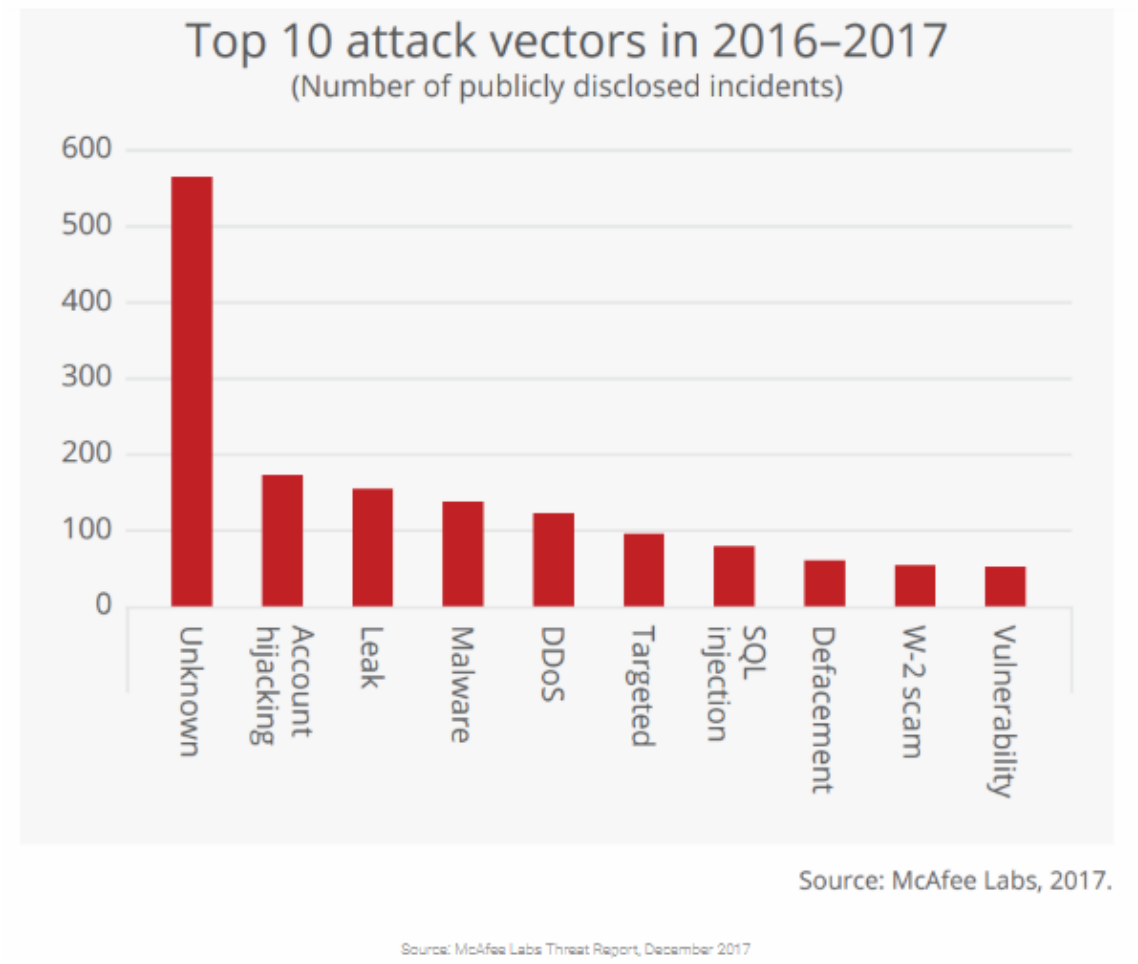


Figura 19 Los 10 principales ataques informáticos durante el 2016-2017. Fuente: McAfee.

Por otro lado, *Calyptix Security* es una empresa del sector que ayuda a aportar soluciones de seguridad a pequeñas y medianas empresas. Publicó el 23 de octubre de 2017, desde otro punto de vista, los principales ataques durante el segundo cuatrimestre del 2017 [146]. En orden de mayor a menor ocurrencia: ataque por fuerza bruta y ataque a través del navegador (al mismo nivel), denegación del servicio, gusanos, *malware*, ataque web, escaneo y otros que se definen en la página web como: ataques físicos, ataques internos y amenazas persistentes avanzadas o ATP (del inglés *Advanced Persistent Threats).* Para saber más sobre cada ataque se puede visitar la página web de la referencia [146].

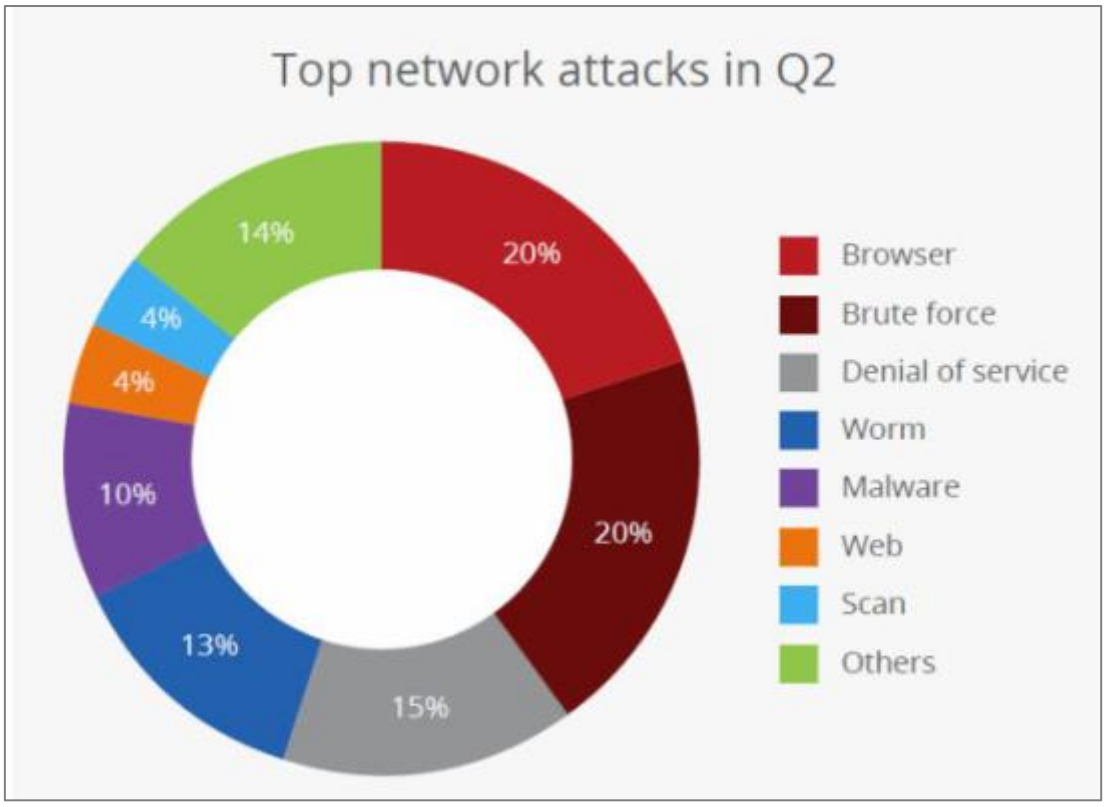


Figura 20 Ataques segundo trimeste 2017. Fuente: Calyptix.

Desde *hackgeddon* [147], *blog* de *Paolo Passeri* especialista en seguridad informática, la última publicación es de mayo de 2018 [148] se muestra en la siguiente Figura 4. En orden de mayor a menor ocurrencia: *Malware*, desconocido (no se ha definido en la web a que se refieren exactamente), secuestro de cuentas, ataque dirigido, alteraciones o desfiguraciones web, vulnerabilidades, denegación del servicio, fuerza bruta, ataques *malware* a puntos de venta y ataque 51% (hace referencia a minería de criptomonedas[64]).

[64] Criptomonedas: Alternativa a las divisivas tradicionales que por su forma de pago es similar al trato que se le da a materias primas como el oro. Una de las más conocidas es el *Bitcoin*.

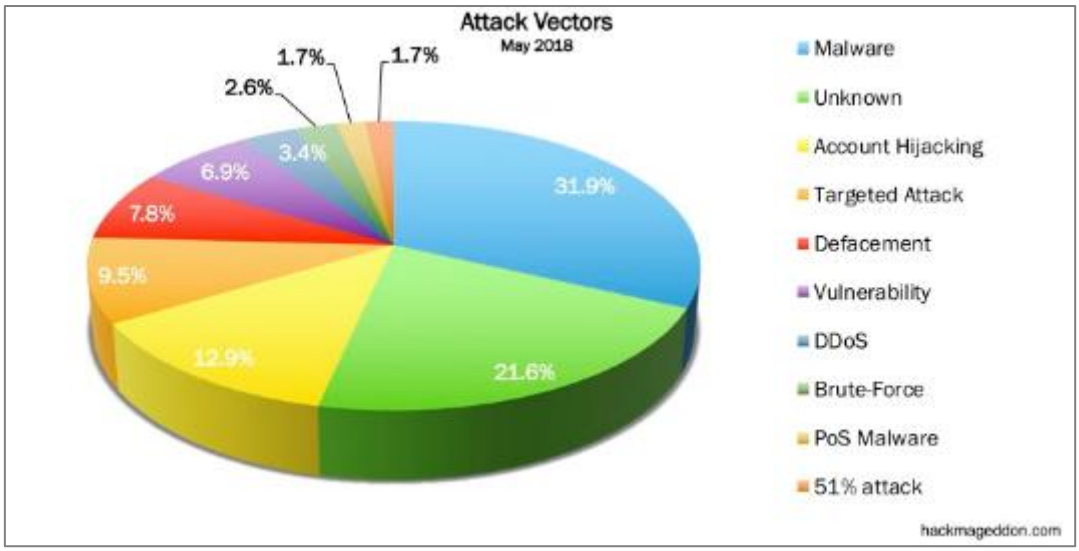


Figura 21 Principales ataques durante mayo de 2018. Fuente: hackgeddon.

En su blog, también publica una comparativa de la evolución de los ataques a lo largo del 2015, 2016 y 2017 [149].

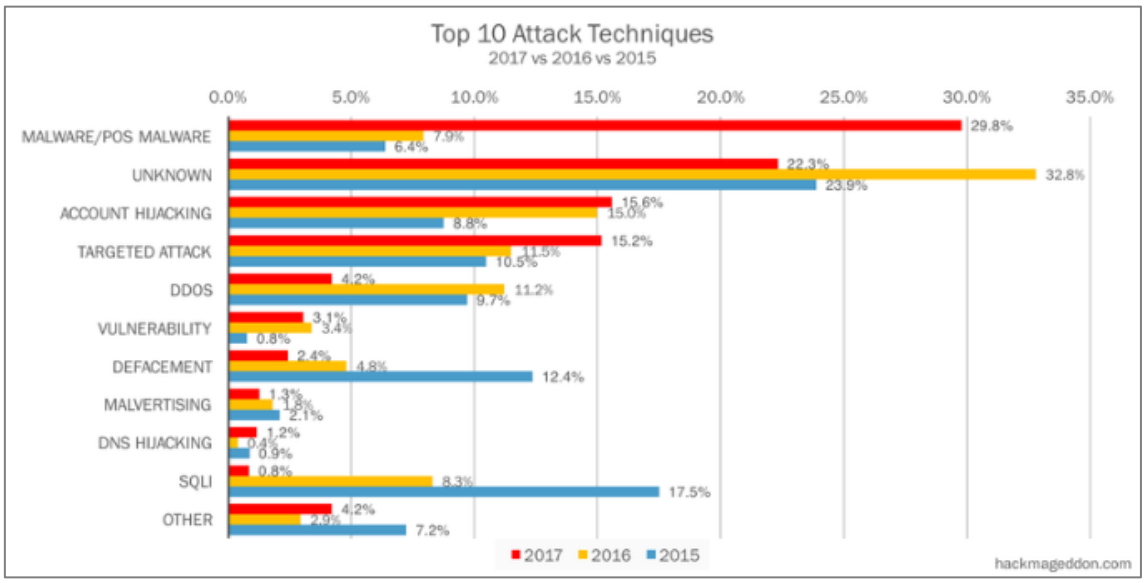


Figura 22 Evolución de los ataques durante 2015, 2016 y 2017. Fuente: hackgeddon.

Como se puede observar, los ataques *malware* se han disparado, lo que concuerda con Figura 16 elaborada por *McAfee*. Los secuestros de cuentas o accesos indebidos también tienen una presencia significativa y coincide en todas las gráficas de las distintas fuentes de este punto, al igual que los ataques dirigidos a un objetivo concreto. Por el contrario, los ataques de denegación del servicio, junto con los de inyección SQL han ido disminuyendo, quizá esto se deba a que es una de las principales preocupaciones para las empresas y son ataques para los que se suele dedicar mucho esfuerzo para defenderse.

Sobre fugas de información, *Infowatch*[65] [150] publicó un informe sobre la evolución de este tipo de ataque a lo largo del 2017 [150]. Los sectores más afectados, según este informe, fueron la industria de alta tecnología, banca y venta al por menor. El mecanismo por el que se ha producido la fuga ha sido analizado y el 11,2% se debe a fraude y solamente un 5,9% es debido a accesos indebidos, el 82,9% restante es debido a fugas sin clasificar. Los principales canales de difusión han sido la red (*web* o nube), correo electrónico o a través de impresión de documentos.

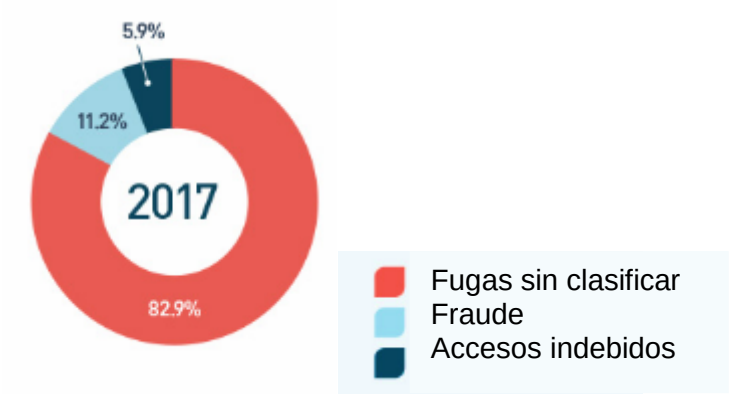


Figura 23 Distribución de las causas de fugas de información. Fuente: Infowatch.

A continuación, se describen algunos de los ataques más representativos basado en las estadísticas anteriores y en mi propio criterio obtenido a través de la experiencia profesional y documentación del presenta trabajo fin de grado. Algunos de los mecanismos de ataque más representativos suelen ser los siguientes [33] [139] [151] [152] :

Acceso ilícito a sistemas o a información sensible [153]**:** Un atacante tiene la capacidad de ingresar en un sistema informático, para el cual no tiene permiso o autorización por el propietario de los sistemas de información, para poder alcanzar un objetivo, como robar o dañar la información. Algunos mecanismos para realizar ataques de este tipo son:

- *Spoofing-Looping* [154] [155]*:* consiste en hacerse pasar por otro robando las credenciales. El método de obtención de credenciales suele ser por ingeniería social, aprovechándose de la confianza o falta de cultura de las víctimas. Se le añade el termino *looping* porque el atacante pasa desapercibido, como si se "evaporara", porque utiliza dos equipos

[65] *Infowatch*: es un grupo formado por varias empresas que desarrollan productos de software y soluciones integradas para garantizar la seguridad de la información de las organizaciones y combatir las amenazas de seguridad externas e internas.

intendentes para el ataque, uno para obtener las credenciales y otro para ingresar.

- *DNS Spoofing* [154] [155]: redirige a la víctima a páginas falsas modificando el sistema de nombre de dominio o *DNS*.
- IP *Spoofing* [154] [155]*:* suplantación de IP. Se sustituye la IP origen de los paquetes TCP/IP (por ejemplo, ICMP, UDP o TCP) por lo que las respuestas del sistema de la víctima llegarán al destino con IP falsa.
- ARP *Spoofing* [154] [155]*:* falsificación de la tabla ARP. Un sistema "A" cuando tiene la necesidad de comunicarse con otro sistema "B", manda una petición ARP para obtener la MAC que corresponde con la IP del sistema "B" con él que se quiere comunicar. El ordenador "B" manda una respuesta ARP indicando su MAC. Toda esta información se irá almacenando en la tabla ARP, pero ésta puede recibir tramas ARP con direcciones falsas. El ataque *Man-In-The-Middle* puede hacer uso de un ARP *Spoofing* para llegar a su fin, y se produce cuando un atacante es capaz de acceder, modificar o añadir información sensible.
- IP *splicing-hijacking* [154] [155]*: s*e trata de un secuestro de una conexión TCP/IP, por ejemplo, de una sesión *Telnet*, una vez que la víctima ya está autenticada.
- Obtención de credenciales por fuerza bruta [154] [155]: mediante programas y diccionarios que realizan miles de posibles claves hasta dar con la buena. Algunos ejemplos de herramientas que se pueden utilizar son: *Cain and Abel, RainbowCrack o Wfuzz*. Para saber más sobre estas herramientas, entre otras, se recomienda visitar la web "Top 10 de las herramientas más populares para *crackear*[66] contraseñas" [156].
- *Physing* [154] [155]: Es un ataque a través del correo electrónico haciéndose pasar por una empresa e confianza para la víctima para obtener datos sensibles y posteriormente cometer algún tipo de actividad fraudulenta.

Código malicioso o *malware*: se trata acontecimientos que se cuelan en un sistema sin autorización del propietario y con dudosas intenciones respecto al interés de la víctima. Algunos podrían ser [142]:

[66] *Crackear* contraseñas: proceso de obtención de contraseñas almacenadas en un equipo.

- Virus informáticos: Programa informático malintencionado con la intención de alterar el correcto funcionamiento del equipo sin que el usuario tenga conocimiento de su existencia.
- Caballos de Troya o Troyanos: Código malicioso que se implanta en el equipo informático como un programa aparentemente legítimo e inofensivo. Una vez que se ha ejecutado permite el acceso y control remoto a usuarios no autorizados. Este nombre proviene del caballo de madera que emplearon los griegos para entrar en la ciudad de Troya, y derrotarla, según se menciona en la Odisea de Homero.
- Gusanos informáticos: Programa malicioso que tras acceder al sistema se va duplicando a sí mismo. Su objetivo no es alterar los archivos, pero reduce y limita la capacidad del sistema.
- *Cookies*: No se consideran una amenaza de seguridad, pero sí que pueden perturbar la privacidad y la confidencialidad de los datos de usuarios. Consiste en detectar y almacenar la información de usuario cuando navega en Internet. Es una poderosa herramienta en el área del marketing.
- Ladrones de claves o *Keyloggers*. Se trata de un componente o funcionalidad que se incluye en los virus, troyanos, gusanos, etc. que recoge información de los usuarios y se la envía al atacante.
- *Software* espía o *Spyware*. Es un *software* malicioso que recopila información de los usuarios para venderla a terceros.
- *Rootkits*: Son programas utilizados por los atacantes para cubrir sus huellas y evitar ser detectado.

Exploits: Un *exploit* [157] [158] se entiende como un código malicioso pero esto no es exactamente así. Se trata de un programa que aprovecha una vulnerabilidad. Cuando se identifica un *exploit,* se detecta una forma de explotar una vulnerabilidad. *Microsoft* publica en su boletín [159] de seguridad más información sobre ellos y cómo prevenirlos. Un ejemplo es el *exploit* que *Windows* registró en la vulnerabilidad CVE-2010-2568 [160] que permitía a los atacantes realizar ataques de denegación del servicio y para enviar *spam*. *Kaspersky*, empresa que ofrece servicios y productos de seguridad de sistemas, realizó un estudio sobre los ataques durante el 2017 [161] y concluyó la siguiente Figura 5, sobre ataques producidos por *exploits* en aplicaciones.

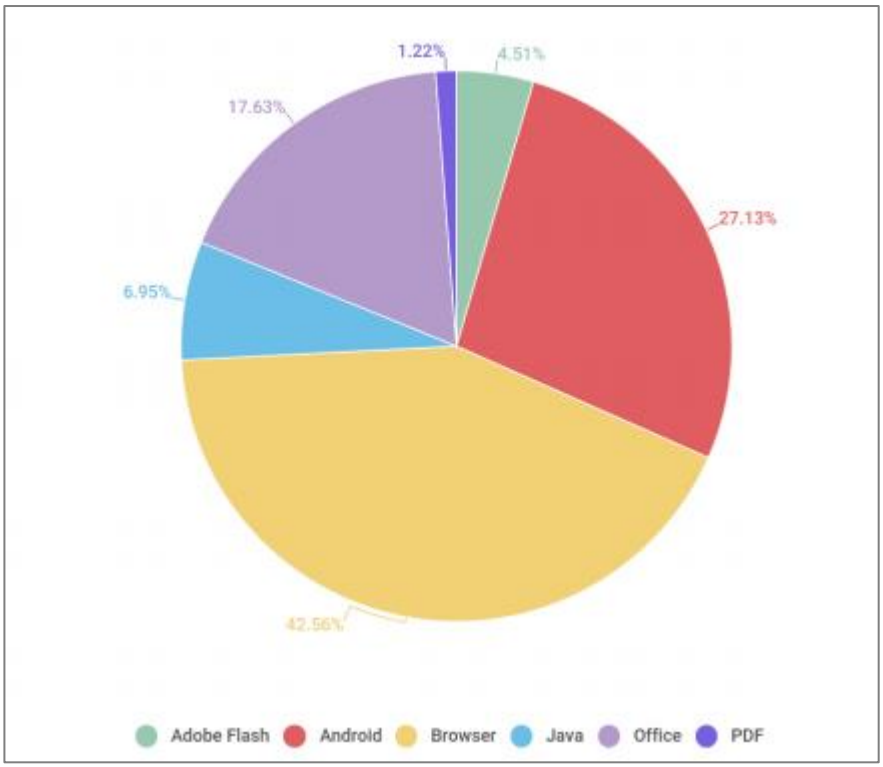


Figura 24 Ataques con exploits según la aplicación atacad (desde noviembre de 2016 a octubre de 2017). Fuente: Kaspersky.

Denegación del servicio: son sucesos que provocan la pérdida del servicio, imposibilitando la correcta ejecución. Se suele detectar cuando los tiempos de respuesta son muy bajos y los servicios inaccesibles, sin motivo aparente [143] [162]:

- Inundación TCP/SYN: Un atacante puede llevar a cabo un ataque de denegación del servicio mediante el envío continuado de paquetes SYN (segmento de petición de conexión de TCP) a todos los puertos disponibles de un servidor con IP*s* falsas. Esto implica la respuesta de ese mensaje, con la consiguiente saturación de la red y el propio sistema.
- Inundación *ICMP*: Se lleva a cabo un ataque de denegación del servicio mediante el envío de una gran cantidad de paquetes *ICMP* que acaparan el ancho de banda provocando una sobrecarga en la red. Otra variante de este tipo de ataque se llama SMURF que consiste en mandar peticiones *ICMP* a la dirección de difusión con dirección origen de la víctima para que el tráfico de vuelta de todos los equipos de la red inunde a la víctima.
- Inundación *HTTP*: Para este ataque se suele hacer uso de *bots* o *zombies,* los cuales se definen en este mismo punto en la página 51*,* para saturar los puertos que dan servicio *HTTP*.

- Inundación *UDP*: Consiste en enviar una gran cantidad de paquetes al sistema víctima, no se requiere que esté iniciada la sesión previamente. Esto provoca que la víctima compruebe para cada petición cada uno de los puertos si un receptor en destino está escuchando. Debido a la gran cantidad de paquetes podría producirse una denegación del servicio.
- Desbordamiento de búfer (*Buffer overflow*): Un atacante es capaz de acceder a una posición de memoria del búfer no permitida, mediante la ejecución de un código malicioso, pudiendo acceder a ubicaciones no permitidas e incluso hacerse con el control del sistema. Una variante sería el ataque conocido como el *ping* de la muerte, en el que un atacante responde con un paquete *ICMP* mayor de lo permitido (mayor de 65536 bytes) en el protocolo IP.
- *Bomba UDP* (UDP *bomb)*: Se envía un datagrama *UDP* con valores inválidos en algunos campos que con seguridad causará un fallo en el equipo receptor.
- Ataque *land*: Se realizan envíos de paquetes TCP/SYN con la misma dirección de origen y destino, en este caso el de la víctima lo que hace que se responda continuamente hacia sí mismo y se produzca un fallo en el servicio.
- *WinNuke*: Es un ataque que afecta a los sistemas *Windows*. Se trata de ataques que reducen el rendimiento de los sistemas *Windows* mediante el envío de paquetes *UDP*.

Karspersky publica en su boletín de seguridad de 2017 [161] la siguiente Figura 25 Distribución de ataques de denegación de servicio por tipo, 1º trimestre 2018, con la distribución de algunos de los ataques de denegación de servicio (están definidos más arriba y para más información se incluyen referencias):

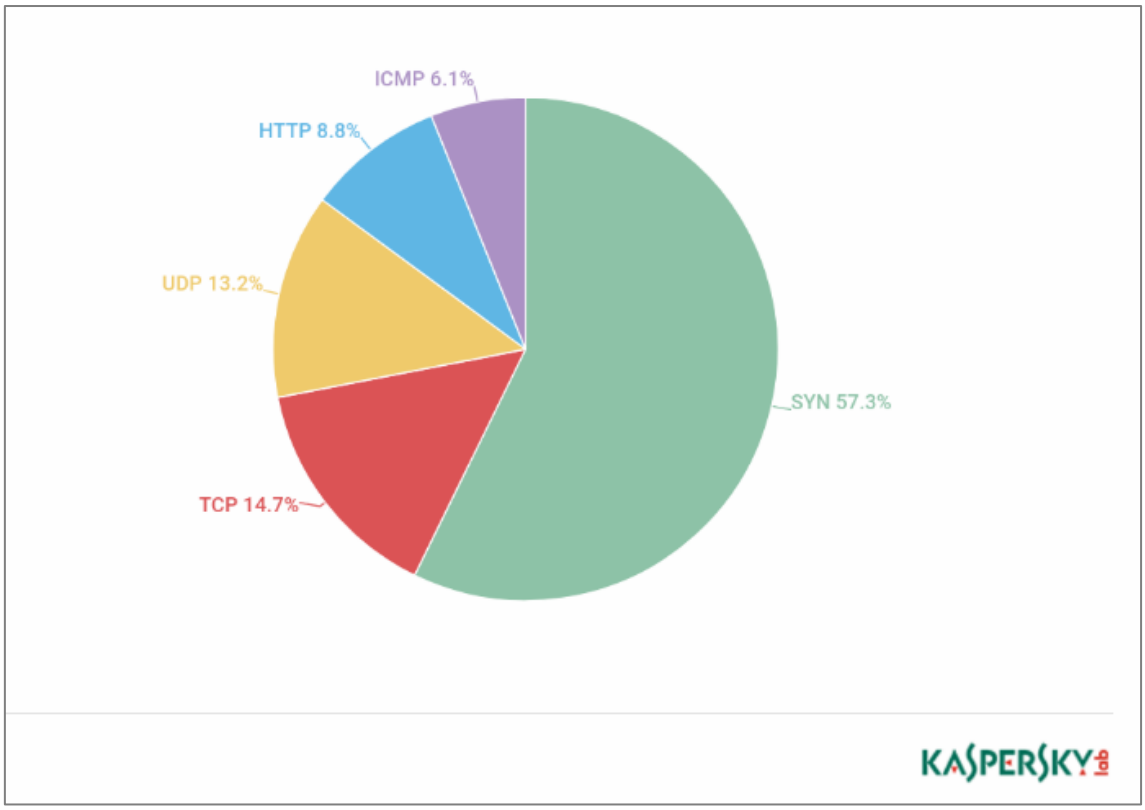


Figura 25 Distribución de ataques de denegación de servicio por tipo, 1º trimestre 2018

Rastreadores o s*niffers*: se utilizan para capturar paquetes y conseguir la información que envían los equipos de una red. Con esto se puede adquirir conocimientos de posibles vulnerabilidades del sistema o de la red.

Red de *bots* (*botnet*): Se trata de un conjunto de equipos "secuestrados", ya que los propietarios no son conscientes de ello, y han sido infectados por algún software malicioso con el objetivo de propagar virus, realizar ataques de denegación de servicios o envío continuo de *spam*[67].

Pruebas, escaneos o intentos de obtención de información de un sistema de información: Se trata de una actividad en la que un atacante intenta acceder a información sobre las actividades y servicios que se usan en un sistema mediante herramientas especializadas *(*como nmap [163] desde *Linux* o zmap [164] desde *Windows*); además realiza intentos de acceder a información sobre las actividades que se usan en un sistema, y es capaz de identificar qué puertos están habilitados y cuales no y qué servicios funcionan a través de cada uno.

Elevación de privilegios no autorizada: Un atacante se hace con permisos de administrador para los cuales no tiene autorización [165] [166].

[67] *Spam:* correo electrónico no solicitado con carácter publicitario.

4.5 Monitorización de ataques en tiempo real

Algunas empresas dedicadas al sector de seguridad ofrecen la posibilidad de ver en tiempo real los ataques que están ocurriendo en todo el mundo.

Ese es el caso de *Karspersy* [167], ofrece una aplicación web para monitorizar ciber-amenzas en tiempo real. Las fuentes de información de la web son:

OAS *(On-Access* Scan), para detección de *malware* durante el escaneo.

ODS *(On Demand Scanner)*, detección de *malware* durante el análisis bajo pedido, cuando el usuario selecciona manualmente la opción "Buscar virus".

MAV *(Mail Anti-Vir),* detección de *malware* durante el escaneo MAV cuando aparecen nuevos objetos en una aplicación de email (*Outlook, The Bat, Thunderbird).*

WAV *(Web Anti-Virus)*, detección de *malware* durante el análisis *Web Anti-Virus* donde la página *HTML* de un sitio web se abre o un archivo es descargado.

IDS, detección de los ataques a las redes.

VUL (Vulnerability Scan), detección de vulnerabilidades.

KAS *(Kaspersky Anti-Spam)*, muestra el tráfico sospechoso y no deseado descubierto por las tecnologías de filtrado de reputación de *Kaspersky Lab.*

BAD *(Botnet Activity Detection)*, muestra estadísticas sobre direcciones IP de víctimas de ataques *DDoS* y servidores *botnet* C&C. El aspecto que tienen las estadísticas de detección a tiempo real es como la imagen siguiente, que muestra el número de detecciones encima de cada herramienta ofrece una visión de los ataques del último mes en una gran cantidad de países.

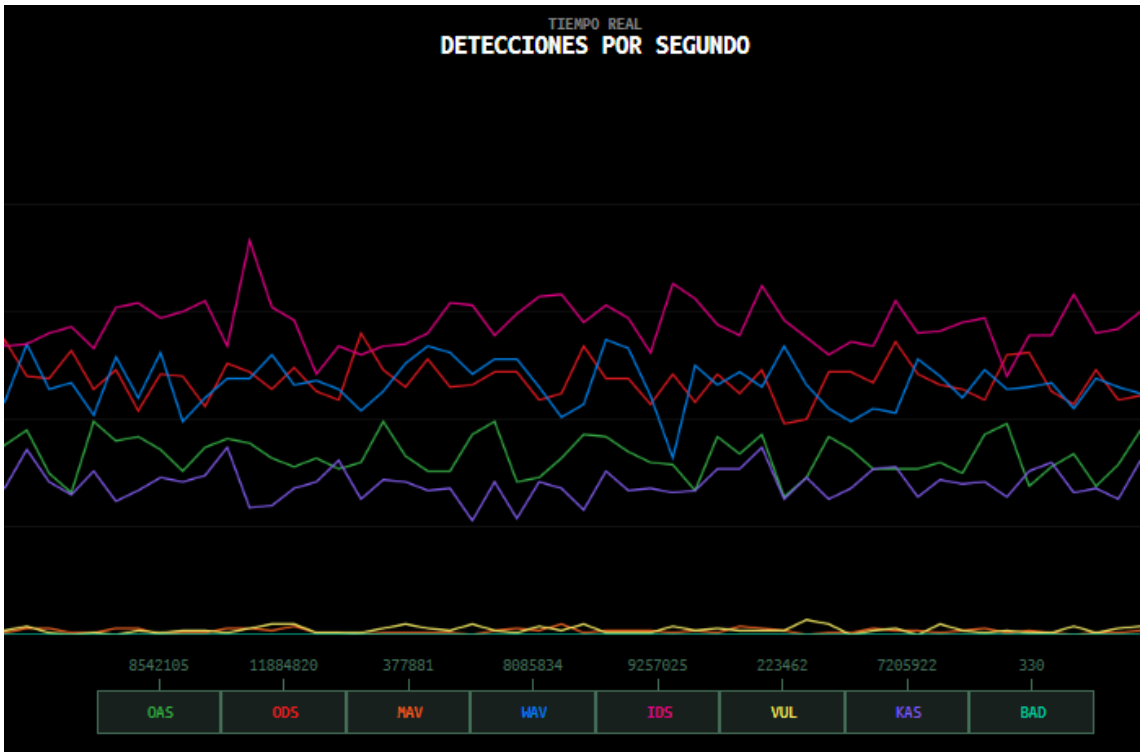


Figura 26 Detecciones a tiempo real. Fuente: Karsperky.

Se muestra a continuación los ataques a redes detectadas durante el último mes (desde el 5 de junio de 2018 al 1 de julio de 2018) en España por *Karspersky*:

Figura 27 Detecciones de ataques a redes del último mes. Fuente: Karsperky.

Desde *Securelist* [168], se puede obtener información de los ataques (a redes, infecciones locales amenazas web) y vulnerabilidades del último mes. El porcentaje de amenazas locales detectadas, durante el mes de junio de 2018, en todo el mundo se puede visualizar de una forma rápida y sencilla con el mapa que facilita *Securelist* con una escala de colores [168].

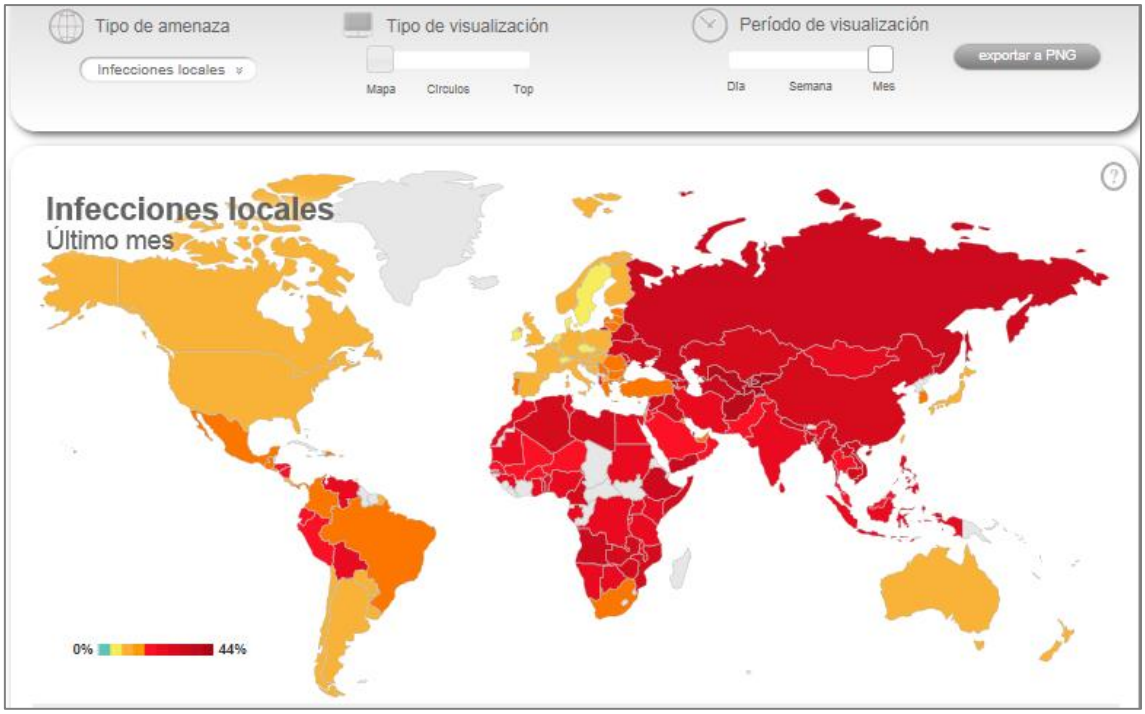


Figura 28 Mapa mundial infecciones locales detectadas durante el mes de junio de 2018. Fuente: Securelist.

Además, se indican el listado de las 10 infecciones locales del último mes con mayor ocurrencia:

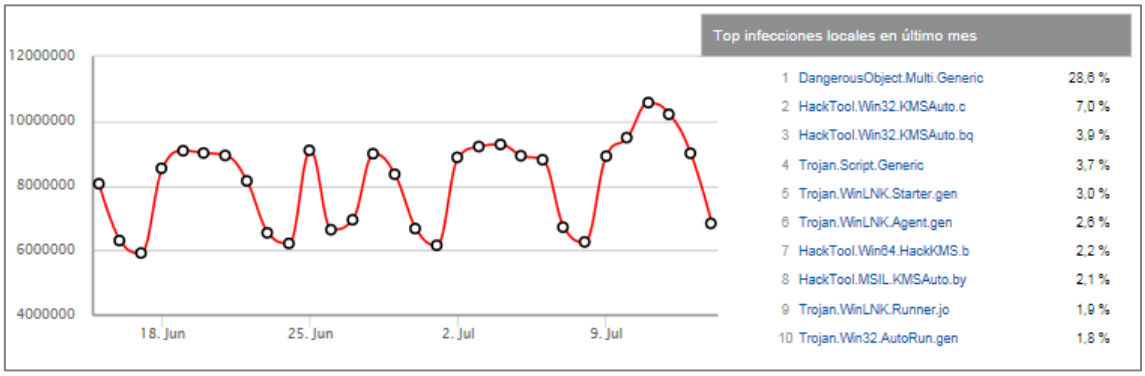


Figura 29 Listado de 10 infecciones locales que más han ocurrido durante el mes de junio de 2018. Fuente: Securelist.

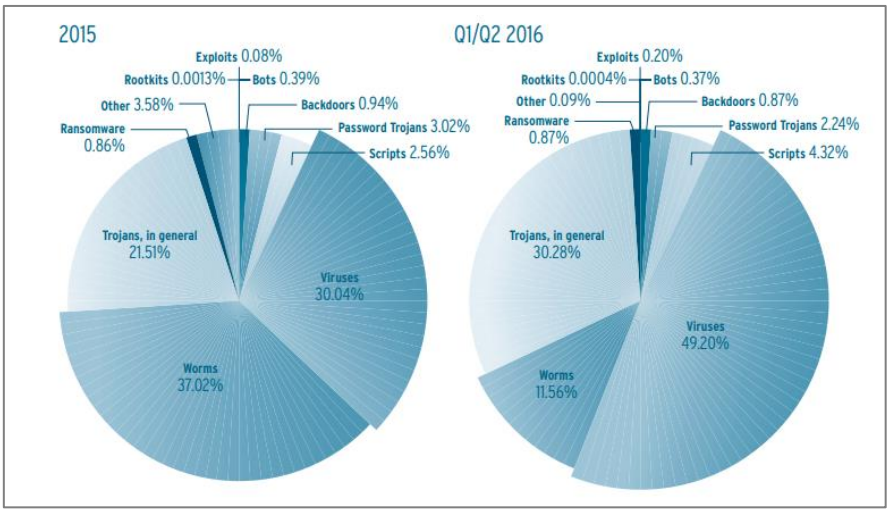
Checkpoint[68] [169], ofrece en su web un mapa con los ataques a tiempo real e identificada origen y destino del ataque y el tipo de ataque [170]. Un ejemplo, es la siguiente captura del día 14 de julio de 2018.

Figura 30 Mapa con ataques en tiempo real. Fuente: Checkpoint

4.6 Ataques a los sistemas operativos: *Windows* y *Linux*

En el punto anterior se ha dado una visión general de los mecanismos de amenazas que los atacantes dirigen hacía los sistemas y las redes. En este punto, se acotarán estas amenazas a los sistemas operativos y se procurarán ejemplos reales.

En primer lugar, una de las amenazas que a las empresas más preocupan son los códigos maliciosos o *malware*, que según los últimos informes de seguridad de 2015-2016 [171] y el 2016-2017 [172] publicado por *AV-test*[69] [173] los resultados de años anteriores de la distribución de *malware* por categorías es la siguiente en sistemas *Windows*.



[68] *Checkpoint*: proveedor de soluciones de seguridad. Es conocido por sus herramientas cortafuegos y VPN.

[69] *AV-test:* instituto alemán de investigación independiente en materia de seguridad.

Figura 31 Distribución malware en sistemas operativos Windows del informe DE AV-test de 2015/16

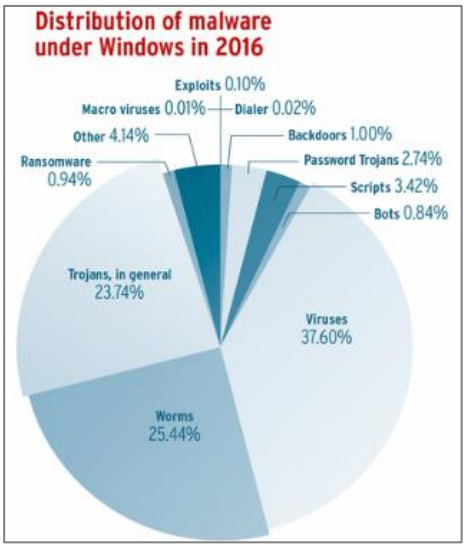


Figura 32 Distribución malware en sistemas operativos Windows del informe DE AV-test de 2016/17

Comparando con la información aportada por *Securelist* se observa que coincide en que los troyanos, gusanos y virus encabezan la lista (en esta fuente no distinguen por sistemas operativos).

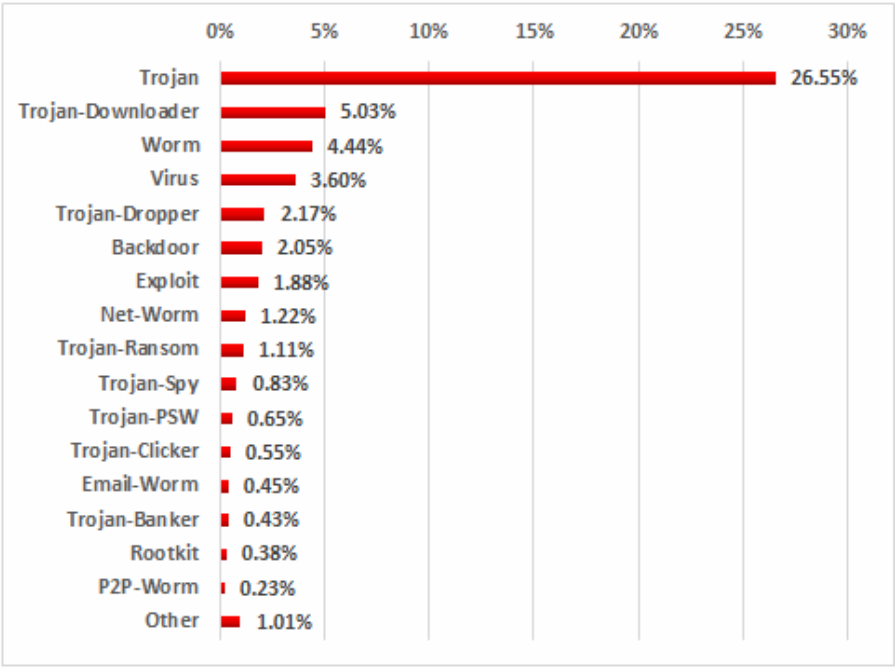


Figura 33 Distribución malware en sistemas operativos por Securelist (2º semestre 2017)

Además, se añade una tercera fuente *Statista*[70] [174] para contrastar que tipos de *malware* son más comunes. En este caso, solo para sistemas operativos *Windows* [175].

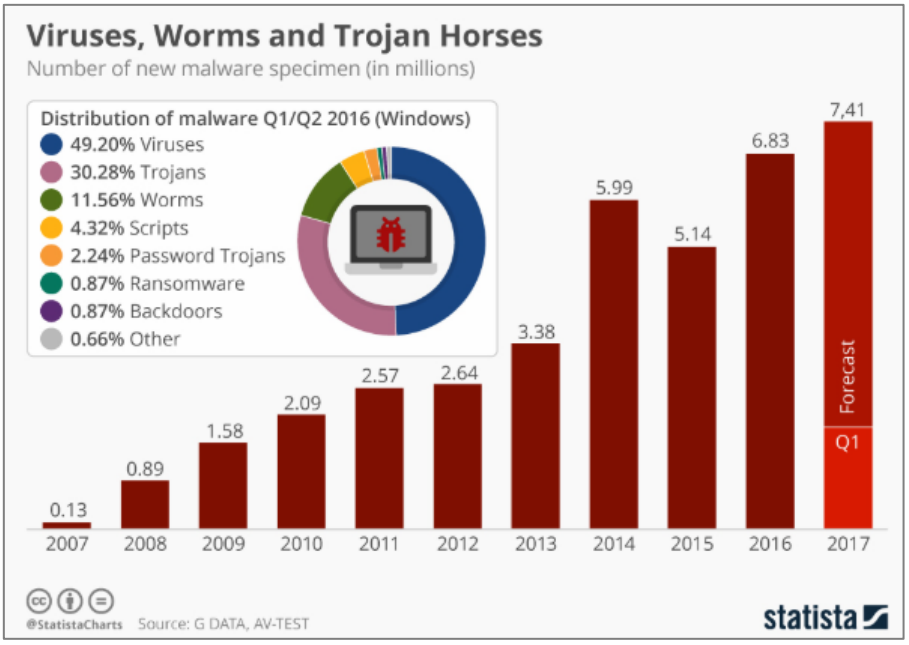


Figura 34 Distribución malware en sistemas operativos Windows del informe de Statista (1º semestre de 2016)

Además, *AV-test* [171] [172] y *Securelist* [44] aportan un estudio de la afectación del *malware* en distintitos sistemas operativos como se puede observar a continuación:

[70] Statista: proveedor de datos de mercado y consumo.

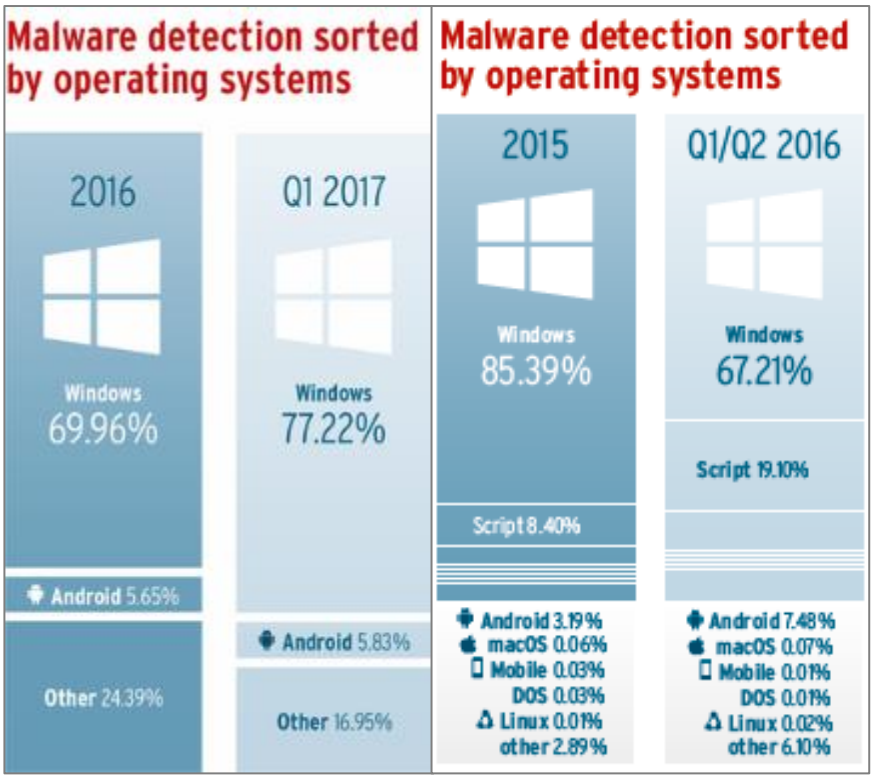


Figura 35 Reparto del malware por sistemas operativos del informe de AV-test de 2016/17

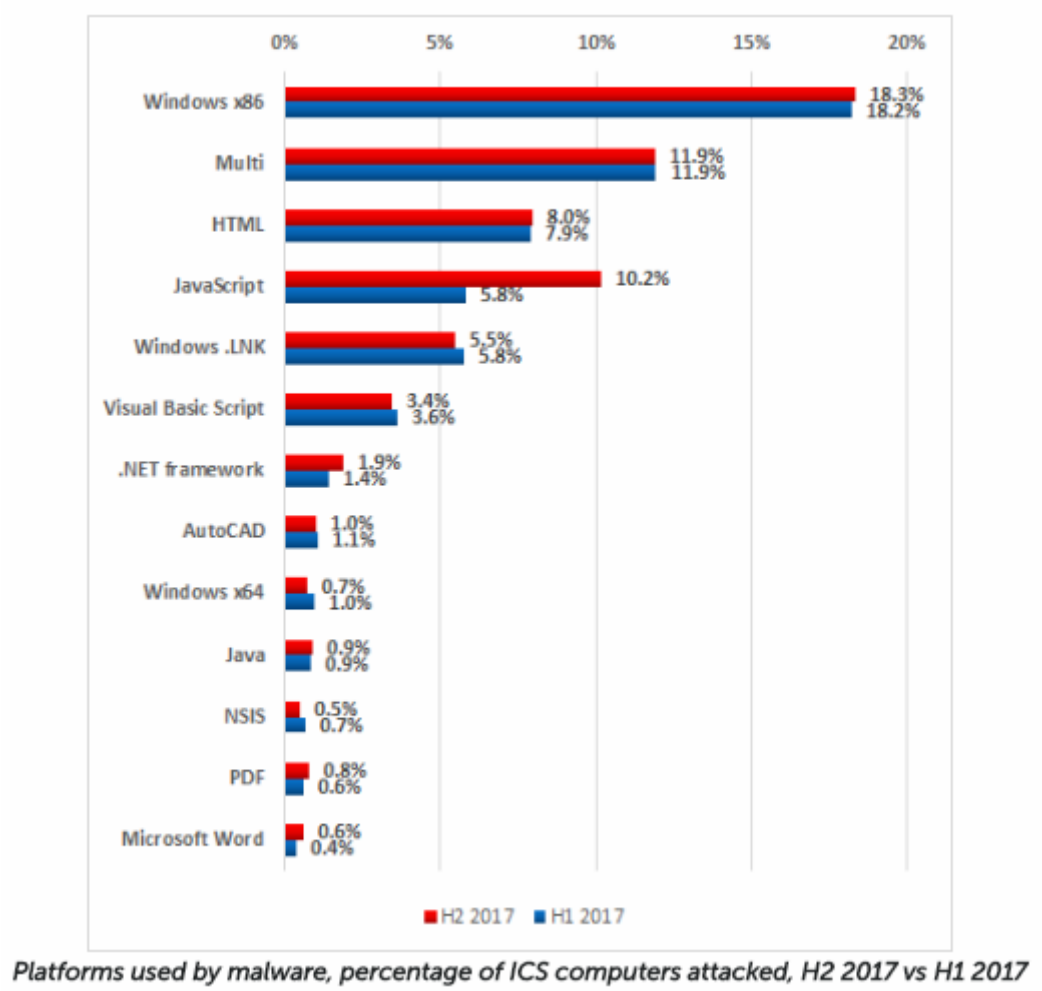


Figura 36 Reparto del malware por tipo de plataformas del informe de Securelist de 2017

Según *Securelist*, durante el primer semestre de 2018 [176] los 10 *malware* más comunes son los siguientes:

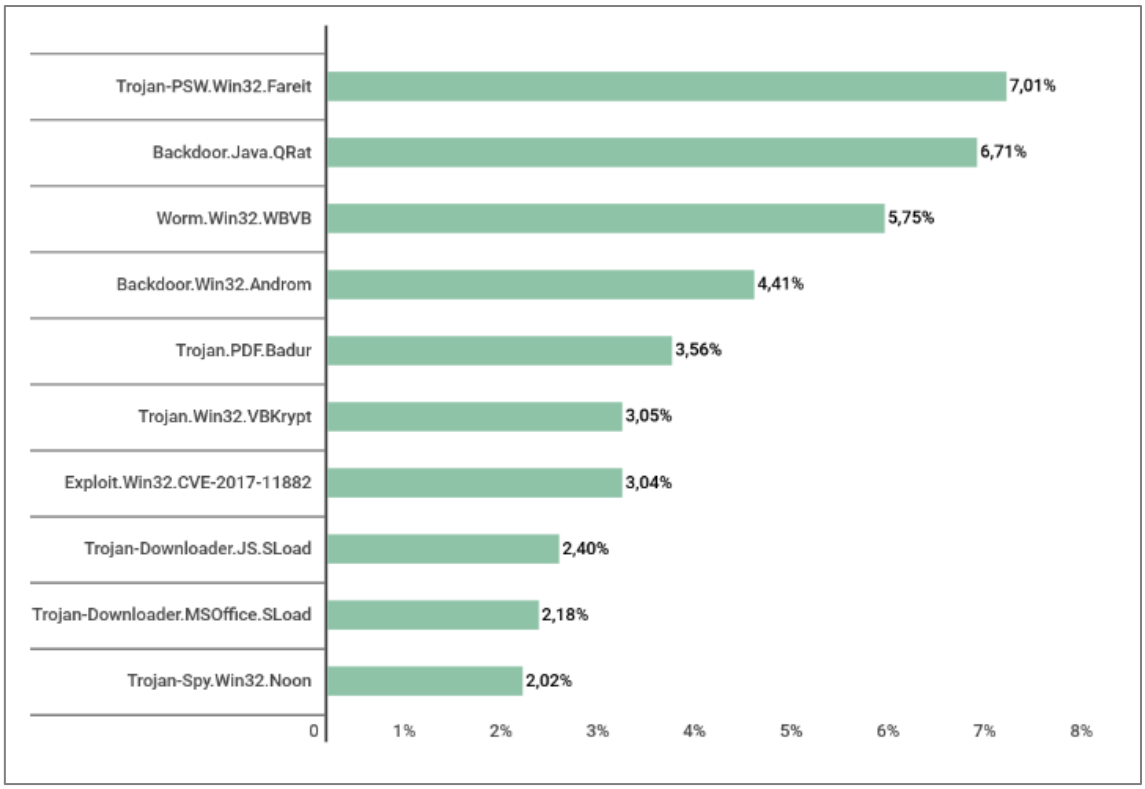


Figura 37 TOP 10 familias maliciosas (1º trimestre de 2018)

El CNN-CERT ha alertado en su página web de los siguientes códigos maliciosos detectados para *Windows*, todos ellos identificados como troyanos: el troyano *koyter* [177], '*TROJ_QUANT'* y '*CrossRat'* [178], *Trojan-Banker.Win32.ChePro* y *Shiotob* [179], *BetaBot* y *Fleercivet* [180].

Además, en 2018 se ha detectado *CrossRAT* que puede infectar a varias plataformas y es indetectable. *CrossRAT* permite espiar a la víctima, desde hacer capturas de pantallas a recopilar cualquier información del sistema operativo [181]. Específico para *Linux*, se detectó en 2016 el troyano *LinuxProxy* 10, utilizado por los atacantes para proteger su identidad [182] [183].

Por otro lado, en cuanto a virus informáticos para *Windows*, se detectó muy recientemente en julio de 2018 el virus *All-Radio 4.27 Portable* [184]. Se trata de un programa para reproducción musical pero unos hacker rusos lo falsificaron y en la máquina de la víctima puede robar información y utilizan el equipo de la víctima para mandar *spam*.

Por último, en cuanto a ataques por denegación de servicio *Securelist* publica en su informe del primer trimestre de 2018 [185] . Es interesante mencionar uno de los mayores ataques de denegación del servicio más recientes que se produjo en marzo de 2018 a la empresa *Github*[71] [186] este ataque se llevó a cabo aprovechando una

[71] Github: Plataforma de desarrollo colaborativa.

vulnerabilidad de los servidores *Memcached*[72], este permite aumentar el tráfico *UDP* hasta 51.000 veces. Se llegaron a generar hasta 1 Tb de información basura que, como curiosidad, contenía demandas de Monero[73]. Según la investigación realizada por *Securelist* el ataque se llevó a cabo instalando en uno de los servidores del cliente un servidor *CentOS Linux* con el servicio *Memcached*, siendo este vulnerable y aprovechando esta vulnerabilidad los atacantes utilizaron este servidor como amplificador, lo que derivó en un ataque de denegación de servicio. A continuación, se adjunta la gráfica que *Securelist* proporciona, en el informe del primer trimestre de 2018 [185], sobre la distribución de redes de *bot* entre sistemas operativos *Linux* y *Windows*.

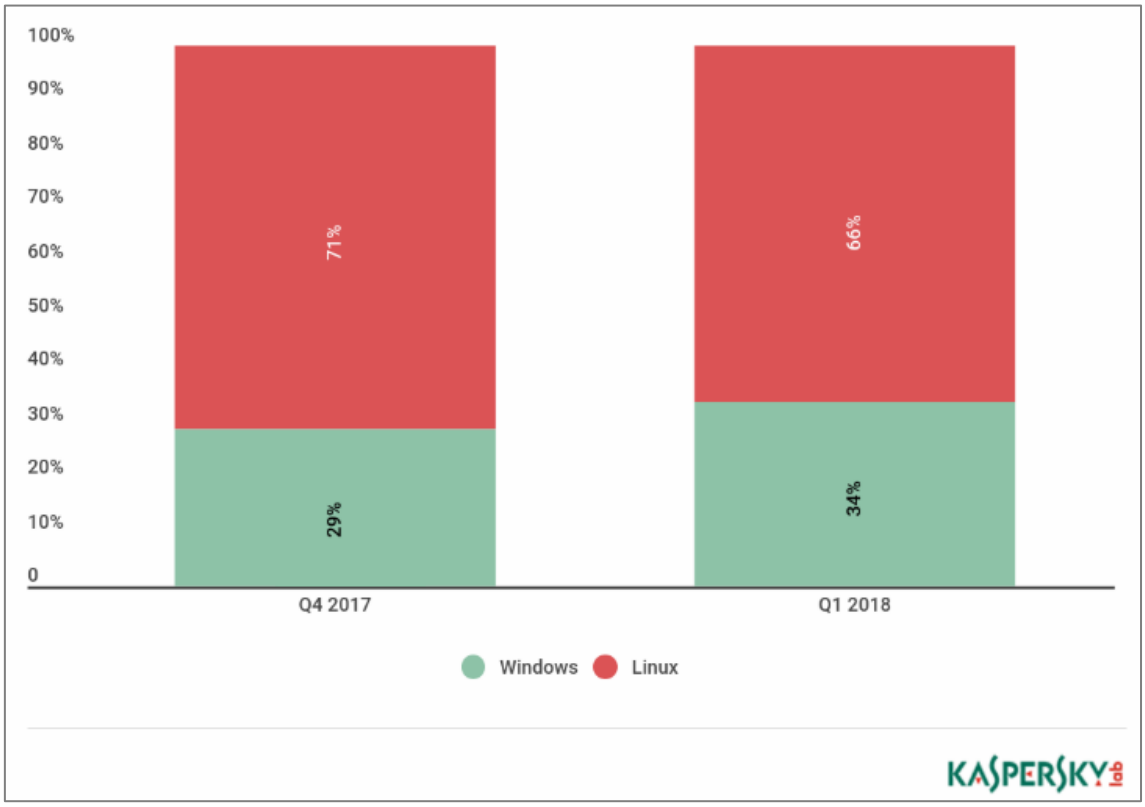


Figura 38 Correlación entre Windows y Linux de ataques por redes botnet (1º trimestre 2018)

[72] *Memcached: Servidores de almacenamiento en caché.*
[73] Monero: Criptomoneda 64.

5 Mecanismos de Protección

En el siguiente punto se van a definir los tipos procedimientos que existen para afrontar un incidente y se especifican los métodos más representativos de protección hasta ahora aplicados. Algunos de los mecanismos más destacables se presentan en los apartados siguientes.

5.1 Gestión de riesgos

El riesgo se define como el resultado de la combinación entre el valor de la probabilidad de ocurrencia de un daño y el impacto de dicho daño sobre los activos de valor. A continuación, en la Tabla 3, se muestra mediante una tabla la evaluación cualitativa del riesgo, se trata de una adaptación basada en *Margerit*[74] [14] [187]:

Riesgo		Probabilidad			
		Improbable	Poco probable	Bastante probable	Muy probable
Impacto	Leve	Trivial	Bajo	Moderado	Significativo
	Moderado	Bajo	Moderado	Significativo	Alto
	Grave	Moderado	Significativo	Alto	Muy alto
	Crítico	Significativo	Alto	Muy alto	Severo

Tabla 3 Evaluación cualitativa del riesgo [187]

El riesgo se compone de los siguientes agentes [188] [189]:

Amenaza: Es el factor que puede ocasionar el daño (persona, actividad o circunstancia ambiental).

- Vulnerabilidad: Característica o capacidad que debilita o hace susceptible a los sistemas frente a las amenazas.

  Los diferentes tipos de riesgos son:

- Riesgo residual: Es resto que queda tras haber aplicado los controles y las medidas de seguridad.
- Riesgo inherente: Es un riesgo propio adherido al sistema y no puede ser eliminado del sistema.

La gestión de riesgo consiste en analizar, evaluar y eliminar o mitigar en la medida de lo posible los riesgos. En el siguiente esquema describe el proceso de gestión de riesgos y relaciona algunos de los conceptos vistos hasta ahora.

[74] *Margerit:* Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, promovida por el Ministerio de Administraciones Públicas de España.

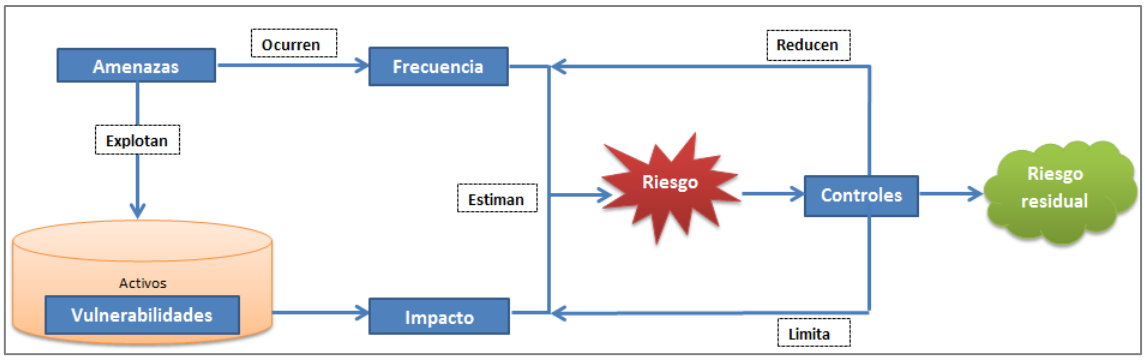


Figura 39 Proceso gestión del riesgo

En función del nivel del riesgo calculado, se pueden aplicar las siguientes alternativas basadas en controles que se definirán en la política de gestión de riesgos. Los controles son normas o procedimientos pensados para garantizar qué eventos no deseados serán detectados o corregidos y mitigarán los riesgos detectados. Tipos de controles [190]:

- Controles disuasorios: Pretenden disuadir a intrusos malintencionados y malhechores.
- Controles preventivos: Se establecen mecanismos para evitar la materialización de un daño o reducir la frecuencia de ocurrencia del daño.
- Controles detectores: Identifican sucesos no deseados una vez que han ocurrido.
- Controles correctivos: Se implementan con el objetivo de corregir un daño tras un incidente.

5.2 Gestión de incidencias

Es fundamental que las empresas dispongan de procedimientos de respuesta ante acontecimientos no deseados. Su principal objetivo es la continuidad del negocio y del funcionamiento normal de los sistemas. El CNN-CERT ha elaborado una guía STIC para la gestión de incidentes de ciberseguridad, concretamente la 817 [191]. Las medidas [139] entre las que se puede optar para afrontar incidencias son:

Medidas preventivas: Se aplican para evitar que ocurran incidentes de seguridad. Por ejemplo: uso de contraseñas, cifrado, implementación de *firewall*s, etc.

Medidas de detección: Sirven para detectar y controlar los incidentes de seguridad. Por ejemplo: auditorías de seguridad, revisiones de seguridad, mecanismos de monitorización, etc.

Medidas correctivas: medidas que aplican tras el suceso o el incidente de seguridad, para evitar que vuelvan a ocurrir y para reanudar a un punto previo al

incidente. Por ejemplo: procedimientos de restauración, eliminación de amenaza y auditoría forense.

Desde una visión a alto nivel los principales pasos [139] a seguir para realizar una correcta gestión de las medidas definidas anteriormente son:

1. Prevención de los incidentes.
2. Detección y reporte de los incidentes.
3. Clasificación del incidente.
4. Análisis del incidente.
5. Respuesta y aplicación de medidas correctivas tras el incidente.
6. Registro de incidentes.
7. Aprendizaje y análisis de los posibles errores causantes de la incidencia para evitar que se vuelvan a producir.

La correcta aplicación de las fases de gestión de incidentes aporta beneficios y mejora continua en la gestión de incidentes así como en su tratamiento con respuestas más eficientes y sistemáticas, favoreciendo una rápida restauración de los sistemas y garantizando la mínima pérdida de tiempo e información posible. Además, ayudar a evitar la reaparición de posibles incidentes, hacer un mejor uso de los recursos y mayor producción.

Por otro lado, una mala gestión de incidentes puede desencadenar en pérdidas de información valiosa y sensible, reducción de productividad y pérdida de calidad y que el rendimiento de los recursos disponibles no fuera el deseado.

5.3 Robustez de los sistemas operativos

Mantener intacta la configuración inicial de los sistemas operativos eleva el nivel de inseguridad. En el caso de los sistemas operativos de *Windows* su premisa es “permitir todo aquello que no esté expresamente prohibido” por lo que habrá muchos agujeros en la seguridad de los equipos [192].

El proceso de endurecimiento de un equipo consiste en la supresión de debilidades y aseguramiento de servicios. A continuación, se sugieren algunas pautas a seguir para fortalecer el nivel de seguridad de los equipos [136]:

Gestión de la seguridad: Configuración de puestos de trabajo y servidores, mantenido al día las últimas actuaciones y parches. Implantación de seguridad Políticas de seguridad.

Gestión de cuentas: Medidas de seguridad en la creación y entrega de contraseñas.

Información confidencial: Se aplican estándares y las medidas adecuadas de seguridad para proteger información confidencial.

Uso de correo electrónico y acceso a internet: Se aplican estándares de buenas prácticas. Se mantiene informado al personal del comportamiento tolerable y se les mantiene en alerta de posibles ataques.

Plan de contingencia: Implantación de pruebas y revisión del correcto funcionamiento de los sistemas ante desastres o fallos.

Acceso lógico: Se aplican mecanismos de control de acceso a la red y a los sistemas. Monitorización de los accesos realizados.

Seguridad física: Control de accesos físicos. Correcto almacenamiento de las copias de seguridad.

5.4 Fortalecimiento y aseguramiento de sistemas *Windows*

En este aparatado se van aportar algunas de las fortalezas que ha ido incorporando *Windows* y algunas medidas que se pueden aplican para reforzar la protección frente a algunas vulnerabilidades vistas en el punto 3.1 y ataques del 4.5. También basado en las recomendaciones de buenas prácticas de *Microsoft* [193].

Protección ante denegación de servicio: El primer paso a realizar, como para la mayoría de las vulnerabilidades, es el mantenimiento de las versiones de software actualizadas. Es fundamental estar al tanto de las mejoras de los fabricantes y desarrolladores ya que ellos están continuamente investigando problemas de seguridad. Por otro lado, otra tarea importante es deshabilitar todos los puertos y eliminar todos los servicios que no se utilicen. Otra solución, recomendada por el CERTSI [194] es configurar *SynAttackProtect* [195]*, TcpMaxPortsExhausted* [196] o *TcpMaxHalfOpen* [197], que son medidas para proteger de posibles ataques de inundación SYN. En la página de *Microsoft* también se aportan algunas pautas de buenas prácticas para prevenir de ataques de este tipo [198] [199] [200] y el CNN-CERT dedicó la guía CCn-STIC-820 completa para la protección contra denegación del servicio [201].

Escaneo de puertos: Para limitar que el ataque de escaneo de puertos encuentre vulnerabilidades en el sistema, algunas acciones a tener en cuenta en la gestión de los sistemas son: abrir solo los puertos necesarios y cerrar los que no se usen, hacer uso de puertos no estándar, asegurar las redes mediante cortafuegos, añadir la protección necesaria puertos y servicios en uso, por ejemplo: SSL, TLS (del inglés *Transport Layer Security*), HTTPS (del inglés *Hyper Text Transfer Protocol Secure*).

Protección contra *malware ransomware*: Tras los acontecimientos de los últimos tiempos y que los ataques de este tipo no han parado de aumentar, el CNN-CERT ha publicado en su página web guías buenas prácticas CCN-CERT BP-04/16 y

medidas de seguridad CCN- CERT IA-11/18, para saber más visitar referencia [202]. Un resumen de las medidas preventivas que aconseja el CNN-CERT:

1. Mantener informado y formado a todo el personal de los riesgos y amenazas.
2. Realizar copias de seguridad y procesos de respaldo.
3. Deshabilitar macros de *Microsoft* Office y aplicaciones similares.
4. Deshabilitar *Windows script host* (evita la ejecución de *scripts*).
5. Utilizar antivirus y cortafuegos, habilitando “bloqueo de ejecución de programas” y “detección y bloqueo de técnicas de *exploits*”.
6. Activar la visualización de extensiones de ficheros.
7. Mantener sistema operativo actualizado.
8. No emplear contraseñas por defecto.

Protección frente a un desbordamiento de búfer: Es fundamental que las aplicaciones se desarrollen con lenguajes de programación avanzados. Para solucionar problemas producidos por desbordamientos de búfer se pueden abordar algunas soluciones como: mantener actualizado el sistema operativo a través de *Windows Update;* elevar la seguridad del navegador web, si el ataque se origina a través de él; por último, habilitar la opción "Activar DEP para todos los programas y servicios excepto los que seleccione" (en *"Sistema y mantenimiento/Configuración avanzada del sistema /Configuración/Performance”*) [203].

Accesos no autorizados: Lo recomendable es crear e implantar contraseñas de un tamaño mínimo recomendado, con un nivel de complejidad elevado, alfanuméricas y con caracteres especiales, fecha de caducidad y es recomendable forzar a un cambio tras la asignación de la primera contraseña a un usuario, para saber más sobre políticas de contraseñas *Microsoft* aporta algunas recomendaciones [204] y el CNN-CERT ha publicado una guía (no clasificada) [205]. También, estos consejos protegen de posibles ataques de fuerza bruta. Los accesos también pueden deberse al robo de contraseñas por lo que la oficina de seguridad del internauta (OSI) [206] recomienda evitar la compartirlas con otros usuarios, el no repetirlas en diferentes sistemas, o el almacenamiento seguro de contraseñas con gestores de contraseñas.

Ataque *Man-In-The-Middle*: Una solución es implantar sistemas basados en autenticación de certificados de las máquinas. El CNN-CERT [207] en su guía CCN-STIC 950, propone como solución la herramienta EMET, que permite la comprobación de certificados SSL para detectar este tipo de ataques.

Protección ante elevación de privilegios no autorizada: Para asegurar que los privilegios asignados a los ficheros y carpetas, y los roles de los usuarios son los correctos, la solución más adecuada es realizar bastionado [208] o en inglés *hardening*.

que quiere decir aseguramiento, en este caso, de los privilegios de los usuarios. Algunas soluciones son la configuración del directorio activo [209] [210] o herramientas de pago como *cyberark* [211] *.* Un ejemplo concreto que publicó la empresa *Elevenpath* para mitigar esta vulnerabilidad de la versión 8.1 de *Windows,* se puede encontrar en la siguiente referencia [212]*. Microsoft* también facilita nociones sobre configuración de cuentas de usuario y asignación de privilegios para *Windows Server 2000* [213]*. Adicionalmente, una* gestión adecuada de contraseñas también puede evitar este posible ataque, siguiendo las pautas anteriormente descritas.

5.5 Fortalecimiento y aseguramiento de sistemas *Linux*

Protección ante denegación de servicio: Al igual que se ha visto en el punto anterior para *Windows*, el primer paso de protección frente a esta vulnerabilidad es realizar un mantenimiento continuo de las versiones de software actualizadas. Además de cerrar puertos y deshabilitar servicios en desuso. El CERSTI, recomienda aplicar soluciones como: SYN-*Cookies,* SYN-*Cache,* SYN-*Proxy* [194] [214].

Protección de escaneo de puertos: Para protección de escaneos, *Jacob Rickerd* ha desarrollado en *Python* un *script*, denominado "*PortScanDetector*", capaz de detectar dicho escaneo. Es capaz de registrar los paquetes TCP transmitidos y bloquea cunado se han escaneado más de diez puertos. Además, se deben tener en cuenta las pautas marcadas en el punto 5.4 para *Windows*.

Accesos indebidos: Para evitar accesos indebidos, además de aplicar los comentarios indicados en el punto anterior sobre *Windows*, en *Linux* también hay que tener en cuenta cómo proteger las contraseñas. Éstas deben esta encriptadas y almacenadas en */etc/shadow*. Asegurarse que en la ubicación */etc/password* no hay contraseñas en texto plano (comando para comprobarlo *$ grep -v ':x:' /etc/passwd*).

Protección de los ficheros: Los ficheros tienen asignado un código binario de 9 *bits* para protegerlos y se divide en tres campos de 3 *bits* cada uno, que corresponden (de izquierda a derecha) el primer bit con el propietario, el segundo con los demás miembros del mismo grupo del propietario, y el tercero con todos los demás miembros. Cada uno de los campos anteriores disponen de 3 *bits*: acceso de lectura, escritura y ejecución. Estos *bits* son conocidos como los *bits rwx*, donde se indica si se puede leer (r), escribir (w), ejecutar (x) o nada (-).

Protección de directorios: En el caso de los directorios es muy similar al anterior, de protección de ficheros salvo que la x sirve para determinar si se tiene permiso de búsqueda y el guion (-) es que no tiene permiso.

Gestión no adecuada del mantenimiento del sistema: En ciertos casos se suele dar que los sistemas *Linux* suelen estar más descuidados en cuanto a la gestión

de parches y actualizaciones, ya que las empresas, algunos casos, no suelen contar con procedimientos para estos sistemas.

6 Detección y monitorización de anomalías

Una vez explicado qué es un ataque y cuáles son los principales mecanismos de protección se concretará qué es la monitorización. Hay que aceptar que, a pesar de aplicar fielmente las medidas de aseguramiento, que recomiendan las guías y los profesionales del sector, jamás se erradicarán las vulnerabilidades, por lo que es necesario apoyarse en alternativas, para detectar y monitorizar los sistemas.

6.1 Sistemas de detección y monitorización de anomalías

El crecimiento exponencial de los sistemas y redes informáticas junto con su inmersión en la vida cotidiana, eleva el riesgo de comprometer la integridad, confidencialidad o disponibilidad de la información contenida y gestionada en dichos sistemas. Esto ha derivado en el fomento de la investigación y el desarrollo de mecanismos de seguridad de prevención y detección de incidentes.

Los ya mencionados sistemas de detección de intrusiones o IDS, son la solución más apropiada para advertir y evitar lo explicado en el punto 4. Estos sistemas de detección de intrusión son herramientas de seguridad que se emplean para monitorizar el tráfico y los eventos que suceden en la red o en los sistemas informáticos, con objeto de identificar situaciones anómalas o intrusiones que puedan pasar desapercibidas y comprometer la seguridad de los activos del negocio y el cometido de los sistemas. Aportan dos funciones significativas: prevención y reacción [140] [215], mediante la escucha del tráfico en la red y el análisis de los eventos del sistema. Los IDS, habitualmente se componen de:

- **Interfaz de usuario o consola**, para visualizar eventos o alarmas y administrar el IDS.
- **Sensor, agente o fuente de recogida de datos**, para analizar información proveniente de log[75], dispositivos de red o el propio sistema.
- **Gestor**, se trata de una centralita que recibe la información de los sensores y dispone de una base de datos como repositorio de esta información.
- **Analizador,** que combinan reglas, filtros y patrones para detectar anomalías de seguridad en los sistemas.

Como mejora, algunos IDS cuentan con la capacidad de envío de alertas, tanto por correo como por mensajería [140] [216].

Los IDS, se pueden clasificar atendiendo a cuatro tipos, como se puede ver en la Figura 40:

[75] *Log*: registro de eventos cronológicamente acontecido en un sistema informático.

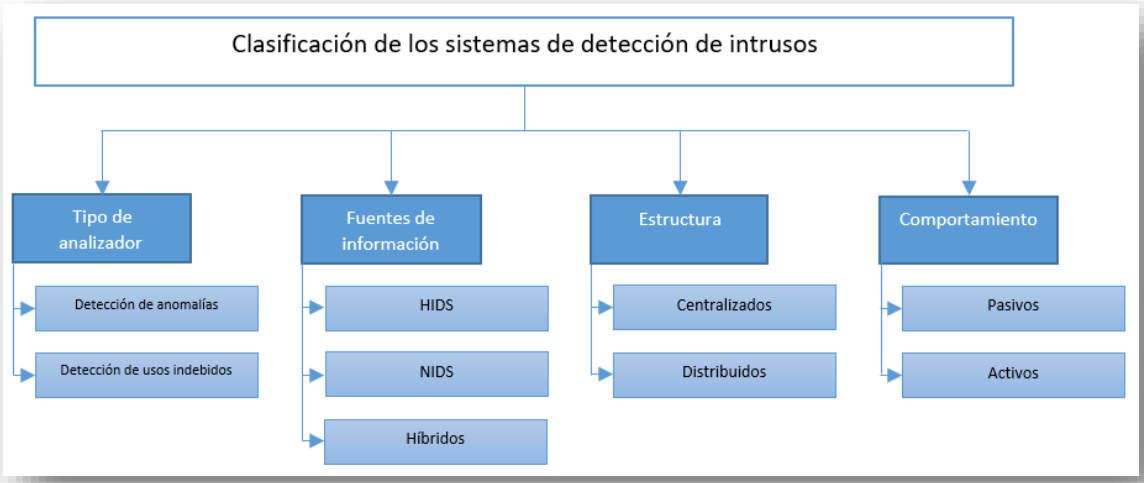


Figura 40 Convenciones de clasificación de los ISD [215]

Tipo de Análisis: Se divide en dos métodos de análisis de amenaza:

- Detección de anomalías: Se emplean métodos estadísticos para comparar patrones de comportamiento. Dentro de este grupo, teniendo en cuenta el tiempo de ejecución del análisis:
  - Análisis por lotes: El análisis se realiza en rango delimitado de tiempo. Tiene como limitación, generar alertas tardías tras producirse los ataques, por no trabajar a tiempo real.
  - Análisis en tiempo real: Se hace un examen de los datos a tiempo real. Facilitan la detección de intrusiones en el momento en el que se están produciendo.
- Detección de usos indebidos: Trabajan comparando firmas almacenadas en una base de datos, las cuales se han ido rellenando y actualizado previamente, a base de eventos anteriores.

Fuente de información: Depende de donde esté situado el IDS en la arquitectura de red:

- NIDS: Se trata de IDS basados en red. Supervisan el tráfico de información de entrada y salida de los dispositivos en búsqueda de posibles amenazas hacia estos. No solo trabajan a nivel TCP/IP, también lo pueden hacer a nivel de aplicación.
- HIDS: Se trata de IDS basados en *host*. Monitorizan eventos y protegen máquinas o dispositivos concretos, además proporcionan salvaguardas a la red general contra amenazas procedentes del exterior**.** Analizan

información como: *logs* o eventos de sistema, recursos, servicios, puertos, etc.

Estructura: Esta clasificación se basa en el modo de funcionamiento del sistema de recolección y gestión de la información, respecto a los agentes.

- Centralizados: Dispone de sensores que envían toda la información al sistema centralizado, desde el cual se gestiona todo.
- Distribuidos: Surgió para paliar las limitaciones de las estructuras centralizadas. La infraestructura consiste en un despliegue de agentes por distintas máquinas y puntos de la red, donde se tomarán decisiones en cada punto concreto. Todos los agentes envían los eventos a un gestor donde se tomarán las decisiones. Se emplea en redes en las que no es necesario o factible monitorizar todo el tráfico.

Comportamiento: En función de si el modo de actuación del IDS es de reacción o de prevención.

- Pasivos: Son aquellos que solo se emplea como procesadores de información para emitir alertas.
- Activos: En este caso además de procesar información como los anteriores sí que tienen capacidad de actuar en la red o en los sistemas cuando se detecta un posible ataque o situación sospechosa.

6.2 Registro *(Log)*

La función principal de un IDS es recabar información de los eventos y funcionamiento de los sistemas, para ello recurre a los registros oficiales de eventos del sistema o *log* [139]. La información básica que puede aportar sobre un evento suele ser la siguiente:

- ¿De qué tipo es?
- ¿Quién lo ha originado?
- ¿Cuándo ha ocurrido?
- ¿Dónde se ha producido?
- ¿Por qué ha pasado?

Implantando un procedimiento organizado de supervisión de *logs* [139] se podrían llegar a detectar, o incluso, evitar situaciones no deseadas o fallos relacionados con:

- Incidentes de seguridad
- Funcionamientos anómalos.
- Cambios de configuración de aplicaciones o dispositivos.
- Utilización y rendimiento de los recursos.

- Intentos fallidos de acceso de usuarios no autorizados.

Por lo tanto, permiten detectar las distintas deficiencias en la gestión de recursos y acontecimientos, para un posterior estudio de dónde provienen, para así establecer una serie de medidas, correctivas o preventivas. De esta manera, se pueden determinar los eventos dañinos para una organización.

A continuación, se hace una breve introducción de las distintas posibilidades que ofrecen los sistemas operativos, concretamente *Linux* y *Windows*, en cuanto a tratamiento y visualización de *logs* y eventos.

6.2.1 Logs en Windows

En el caso de *Windows,* el mecanismo manual para acceder a los *logs* es hacer uso del "Visor de Eventos" [34] [139]. La ruta de acceso es la siguiente: *-> Configuración -> Panel de control -> Herramientas administrativas -> Visor de eventos*:

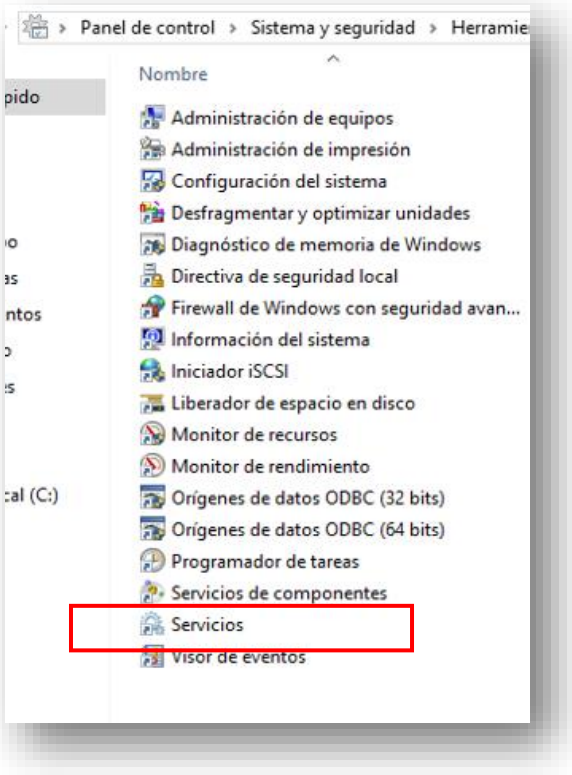


Figura 41 Visor de eventos de Windows

Con el "Visor de Eventos" [139] se puede obtener información básica de eventos ocurridos en el sistema, como:

- Tipo de Evento.
- Fecha y Hora.
- Origen.
- Identificador.

- Usuario que lo ha generado.

Para buscar concretamente un tipo de evento, *Windows* dispone de una clasificación por defecto, que se compone de los siguientes registros [139]:

Registros de aplicación: eventos registrados por aplicaciones o programas.

Registros de seguridad: eventos ocurridos en los accesos del sistema, como los intentos de inicio de sesión (tanto exitosos como fallidos), las introducciones de contraseñas erróneas o la utilización de los recursos.

Registros de instalación: eventos que hacen referencia a la instalación de aplicaciones en el equipo. Se suelen utilizar para comprobar si se ha instalado algún código malicioso en el equipo.

Registros de eventos reenviados: eventos que se han reenviado a este registro desde otros equipos.

En la Figura 42, se destacan donde se encuentran los registros de *Windows*: aplicación, seguridad, instalación, sistema y eventos reenviados. También, los campos de información que se aporta para cada evento, como: Palabras clave, fecha y hora, origen, identificador del evento y categoría de la tarea.

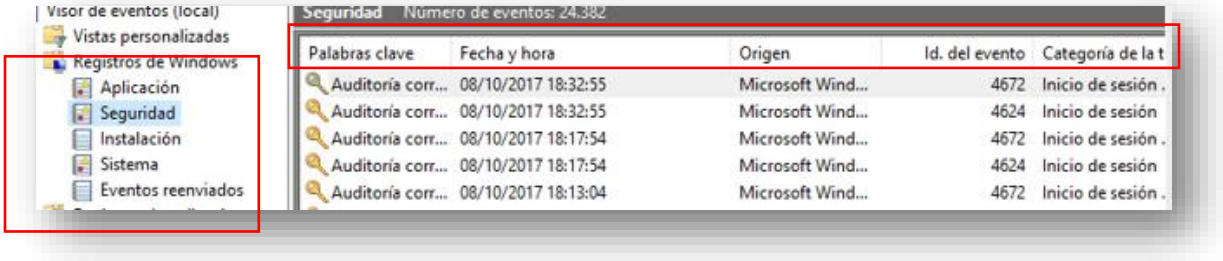


Figura 42 Registros de Windows

6.2.2 Log en Linux

Linux no dispone de una herramienta con interfaz gráfica para visualizar los eventos. Para acceder a los registros de eventos del sistema es requisito necesario iniciar sesión como administrador. Los principales ficheros, y de especial interés para el presente trabajo, ya que aportan información relacionada con el funcionamiento del sistema, serían los siguientes [34] [139]:

Nombre del archivo	Funcionalidad
/var/*log*/auth.*log*	Eventos de autenticación y permisos
/var/*log*/boot.log	Eventos y servicios empezados cuando se inicia el sistema
/var/log/daemon.log	Mensajes sobre permisos o servicios corriendo en el sistema
/var/log/dmesg.log	Mensajes del núcleo *Linux*
/var/log/errors.log	Errores del sistema
/var/log/*HTTP*d.log	Mensajes y errores de apache

/var/log/mail.log	Mensajes del servidor de correo electrónico
/var/log/messages.log	Alertas generales del sistema
/var/log/secure.log	Registro de seguridad
/var/log/syslog.log	Registro del sistema de registro
/var/log/user.log	Muestra información acerca de los procesos usados por el usuario

Tabla 4 Principales ficheros de logs de Ubuntu

Algunos comandos útiles de Linux, para facilitar el manejo de estos ficheros debido a las dimensiones que pueden alcanzar, son los siguientes:

- *tail* – f se ven las últimas líneas de un archivo y sus actualizaciones.
- *less* +F en lugar de acceder a las últimas líneas de un archivo de registro se accede a su totalidad, pudiéndose ver, incluso, las actualizaciones del mismo a tiempo real.

Para finalizar la ejecución de estos comandos se pulsa la combinación de teclas "*Ctrl* + C" y en el caso del comando *less* +F se pulsa además la tecla "Q" [139].

6.3 Características de un sistema de detección de intrusiones

En este punto, se describe qué es un de un sistema con detección de intrusiones o *IDS* [139]. Las características principales que debe ofrecer son: elevada autonomía, capacidad de sortear una caída del sistema, no afectar en el funcionamiento normal los sistemas, alta fiabilidad, imperturbabilidad y fácil adaptación a cambios.

6.3.1 Ventajas de un IDS

Es una de las herramientas más útiles ý completas para apoyar la defensa y seguridad de los equipos. Entre otras, las ventajas [139] más destacables son las siguientes:

Identificación del origen del ataque: puede revelar de donde proviene el ataque, por ejemplo, detectando la IP y puerto de origen.

Tiene un papel disuasorio: un atacante que descubra la presencia de un sistema de detección evitará realizar el ataque o se limitará el impacto del ataque, por miedo a ser descubierto.

Resguarda contra las intrusiones: cualquier intrusión será registrada y controlada en todo momento. Detecta intentos de acceso no autorizados y comportamientos anómalos o no deseados.

Envío de alarmas: se reduce la posibilidad de no detectar ataque.

Almacena toda la información sobre los intrusos: dispone de una pila incremental de información que permite el continuo aprendizaje de patrones de comportamiento de atacantes, lo que refuerza la prevención frente a un posible ataque.

Permite espacio para la reacción y prevenir el daño: cuenta con la capacidad de responder frente a comportamientos sospechoso.

Previenen de daños: alerta de situaciones no deseadas permitiendo en algunos casos el tiempo suficiente para evitar un incidente o un problema mayor.

6.3.2 Debilidades o Inconvenientes de IDS

Hay que tener en cuenta las debilidades [139] que tienen estas herramientas y donde deberemos poner el foco de seguridad para mitigarlo con otro mecanismo:

- Deben ser ejecutados por técnicos especializados y experimentados
- Falsos positivos.
- Sensibilidad mal calibrada de la herramienta.
- Por norma general no disponen de la funcionalidad para luchar contra o eliminar una amenaza.
- Registro erróneo del incidente.
- Ataques durante la fase de aprendizaje, lo que altera la definición del ataque dejando de considerarlo anómalo.
- Aprendizaje continuo de la herramienta, actualizaciones y mejoras.

6.3.3 Arquitectura IDS

En este punto, se aporta la arquitectura [139] de más común que se suele definir al implantar un IDS dentro de una organización. El principal objetivo, de un IDS es ser utilizado como herramienta de auditoria de vulnerabilidades de sistemas y redes. Los elementos que componen un IDS y sus funcionalidades desde el punto de vista más sencillo podrían ser como el del siguiente esquema:

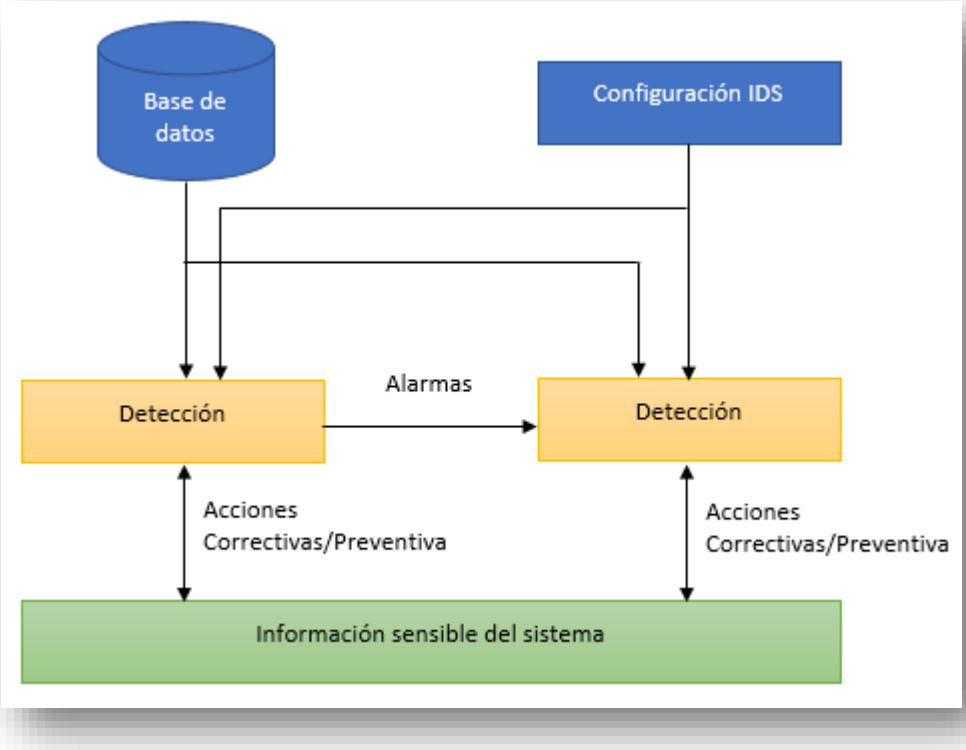


Figura 43 Esquema arquitectura funcional básico de un IDS [139]

Se ha de tener en cuenta que en el mercado actual se pueden encontrar multitud de propuestas, sin existir un estándar para alguna de ellas, lo que complica la interoperabilidad en organizaciones con distintos ID. Aun así, los elementos en común de cualquier IDS son [217] [218]:

Fuente de recogida de Datos: Se trata de un log, sensores en la red o el propio sistema de información.

Reglas: Para la detección de patrones anómalos de comportamiento.

Filtros: Comparación entre los datos de la red o el sistema y las reglas almacenadas.

Sensores de eventos no esperados y anomalías en el tráfico de red.

Generador de informes y alarmas: Sonoras, visuales y alertas vía mail o SMS.

6.3.4 Toma de decisiones: ubicar un IDS en una organización

La implementación, no puede desligarse del nivel de conocimientos de los responsables que lo gestionan ni de las peculiaridades en la arquitectura de cada organización. Es por esto que, una Organización debe realizar un profundo análisis de los elementos y equipos que componen la red para que la efectividad del IDS sea la mayor posible y óptima [139] [140].

Previo a la implantación de un IDS, se plantearán gestiones de planificación, preparación, pruebas y formación especializada del personal responsable. Los principales puntos para decidir dónde se va a implantar y el alcance, son:

- Evaluación de los procesos del negocio para identificar los activos de valor.
- Evaluación de los protocolos de red empleados en la transferencia de información.
- Ajuste de política de costes, protocolos y políticas de seguridad de la organización en la implantación del sistema IDS.
- Análisis de la futura ubicación del IDS en la organización.
- Planificación de servicios que ofrecerá la organización.

6.3.5 Políticas de Gestión de Intrusiones en el Sistema

A continuación, se muestra la necesidad de desarrollar e implantar políticas y procedimientos de gestión de los IDS/IPS, y la respuesta ante incidentes o situaciones de riesgo de ataques. Una política de seguridad [139] contiene el procedimiento y los detalles de lo que se debe permitir y lo que no, de aquí que se pueden aplicar dos tipos de políticas diferentes:

Política permisiva: se define lo que se va a prohibir, lo que no está, se toma como permitido.

Política prohibitiva: se define todo lo que se va a permitir, todo lo demás se considera prohibido.

Por otro lado, según la respuesta de los sistemas ante la detección, se puede clasificar en dos tipos de políticas de corte:

Políticas de respuesta pasiva: El ataque solamente es registrado en un histórico y se envía una alerta al responsable, pero no realiza ninguna acción de defensa ante la intrusión. Algunas propuestas de política de respuesta pasiva son:

- Alerta mediante correo electrónico en caso de detectar una intrusión.
- Histórico del ataque que contenga información, como la fecha del ataque, hora, IP del intruso, IP del destino, protocolo utilizado, etc.
- Guardar los paquetes sospechosos.
- Emitir una notificación visual de alerta por consola.

Políticas de respuesta activa: Además del procedimiento de una política pasiva (registrar y alertar), se desencadena algún mecanismo para evitar que el ataque sea exitoso. Algunos podrían ser:

- Envío de un *ResetKill*[76], lo que implica cerrar la conexión, bloqueando la entrada del atacante al equipo.
- Reconfiguración de dispositivos externos, bloqueando el dispositivo externo impidiendo la entrada.

6.3.6 *Problemática de detectores de intrusión*

Los posibles escenarios que se pueden dar en la detección de intrusiones con un IDS pueden ser las que se ven en la Figura 44.

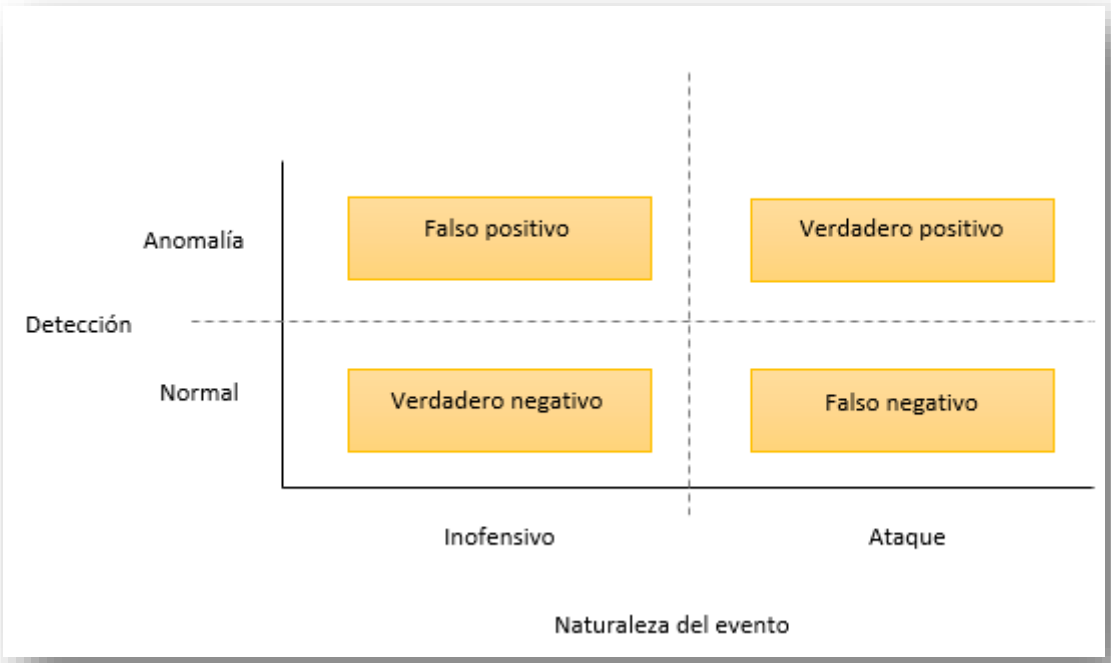


Figura 44 Clasificación de tipo de escenarios de eventos [139]

Detección de falso positivo o falsa alarma: cuando el IDS/IPS detecta como ataque el tráfico de datos que en verdad es inofensivo.

Falso negativo: ataque que no es detectado por el IDS/IPS.

Verdadero positivo: evento inofensivo que el IDS/IPS ha detectado como tráfico de red normal.

Verdadero negativo: ataque detectado correctamente por el IDS/IPS.

El objetivo es reducir el número de falsos negativos y positivos durante la detección y elevar el número de aciertos, porque un número elevado de falsos positivos y negativos puede reducir la efectividad de la herramienta tapando verdaderos positivos y elevando el tiempo y esfuerzo en el procesamiento de los eventos detectados.

[76] *ResetKill: paquete de alerta TCP para forzar la finalización de la conexión.*

Es fundamental equilibrar la sensibilidad del sistema, para generar alertas fiables y facilitar el procesado de la información. Se tendrán en cuenta las siguientes situaciones:

- con más sensibilidad, se eleva la posibilidad de detección de falsos positivos y menos falsos negativos;
- con menor sensibilidad, la posibilidad de una menor detección de falsos positivos y más falsos negativos;
- un número elevado de información procesada, eleva la posibilidad de detectar falsos positivos y menos falsos negativos;
- por último, un número bajo de información procesada, se reduce la posibilidad de detectar falsos positivos y más falsos negativos.

7 HERRAMIENTA DE MONITORIZACIÓN: OSSEC

Es una plataforma para monitorear y controlar sistemas informáticos. Concretamente, un IDS basado en *host* o también llamado HIDS, que además incluye aspectos de correlación de *log*, de SIM (del inglés de *Security Incident Management*) y SIEM (del inglés *Security Information and Event Management*). [219]. Es un sistema muy potente, flexible y robusto. [220]

7.1 Características principales de OSSEC

Requisitos de conformidad: Permite cumplir a los clientes con el cumplimiento de PCI[77] [221] (del inglés *Security Standards Council*) y HIPAA[78] [222] (del inglés *Health Insurance Portability and Accountability Act*). Detecta y alerta sobre modificaciones no autorizadas o comportamientos sospechosos.

Multiplataforma: Implantar un sistema de detección de intrusiones basado en *host* en una amplia variedad de sistemas operativos, como: *Linux*, Solaris, *Windows* y *Mac OS X*.

Alertas a tiempo real y configurable: La recepción de alertas permite centrarse en elevar la prioridad de los incidentes críticos. Al integrar SMPT[79] (del inglés *Simple Mail Transfer Protocol*), SMS[80] (del inglés *Short Message Service*) y *syslog*[81] (se define en el apartado 7.2.3), esta herramienta aportar el mayor conocimiento de la situación en el menor tiempo posible.

Gestión centralizada: Realizar una administración centralizada simplificando el trabajo de gestión de los agentes. Además, permite definir políticas más específicas sobre la infraestructura a monitorizar.

Supervisión con agente/sin agente: Supervisión flexible de los sistemas con o sin agente de los enrutadores y *firewall*.

7.2 Funcionalidad de OSSEC

En este punto se describen las capacidades y las cualidades de OSSEC para procesar y gestionar los eventos.

[77] PCI: estándar de seguridad de datos para la industria de tarjeta de pago.
[78] HIPAA: Ley de transferencia y responsabilidad de seguro médico de 1996 fue creada para proteger a millones de trabajadores y a miembros de sus familias en los Estados Unidos que padecen alguna afección médica.
[79] SMPT: protocolo para el envío de correo electrónico a través de internet.
[80] SMS: servicio de envío de mensajes cortos de texto.
[81] Syslog: protocolo para el envío de mensajes de registro (*log*).

7.2.1 Monitorización de Log

Recopilación, análisis y correlación de los registros del sistema para alertar en caso de una actividad sospechosa en tiempo real. Esta función se llevará a cabo mediante dos procesos:

1. *Logcollector* (se define en el apartado 7.3.2) proceso de OSSEC para recoger y supervisar los *logs* (cualquier tipo de *logs* del sistema, ya sean de *syslog*, ficheros planos, eventos de *Windows*, etc.) y por otro lado
2. *Analysisd* (se define en el apartado 7.3.2), es el proceso principal de análisis de OSSEC, se encargará de analizar los log haciendo uso de reglas[82].

El objetivo de la monitorización, es la detección de posibles ataques o empleo no adecuado de los sistemas basándose en análisis de los registros o LIDS (del inglés *log-based intrusion detection*). La detección de intrusiones basada en log o registro de seguridad es una técnica para actividades no apropiadas, uso indebido o ataques a los sistemas.

La configuración se realizará en cada agente, en el fichero de configuración del agente OSSEC concretamente (*/var/ossec/etc/shared/agent.conf*).

7.2.2 Comprobación de integridad de archivos

El proceso *syscheck* (se define en el apartado 7.3.2*),* se ejecuta de forma periódica para verificar que se mantiene la integridad de los directorios y archivos, alertando cuando se detecta algún cambio. Esta función forma parte de *analysisd*.

La comprobación de la integridad de los archivos, es de una gran utilidad puesto que cualquier ataque los algunos archivos sufren cambios o variaciones, por lo que, este proceso suele ser crucial para la detección de intrusiones. Se realiza mediante los algoritmos MD5/SHA1. El mecanismo de funcionamiento está basado en que el agente realiza revisión en función de la frecuencia definida (por defecto seis horas) y realiza envíos de los resultados de los algoritmos al servidor. El servidor guarda estos resultados y posteriormente los revisa buscando cambios.

7.2.3 Alertas

Consisten en notificaciones de los eventos detectados con las reglas. Todas las aleras se configurarán en el fichero de configuración de OSSEC (ossec.conf). OSSEC ofrece los siguientes mecanismos de alerta mediante:

Syslog: se trata de un mecanismo de envío y colección de log sobre el estado de aplicaciones y el sistema operativo.

[82] Reglas: código que se emplea como motor de búsqueda y revisión de eventos para generar alertas de patrones detectados.

E-mail: se pueden enviar alertas a través a un correo electrónico atendiendo al nivel de criticidad o del tipo de regla. Se puede configurar como reportes diarios o alertas particulares por eventos.

7.2.4 Detección de rootkit:

Mediante el proceso *rootcheck* se puede detectar si se ha utilizado en el sistema algún tipo de *rootkits*[83]. Utilizará como fuente de información el archivo *rootkit_files.txt* que contiene una base de datos de *rootkit* y archivos que suelen utilizar estos. Es muy similar al funcionamiento de un antivirus, debe estar en constante actualización.

También dispone de una base de datos de troyanos en el archivo *rootkit_trojans.txt*. Aunque, hay que tener en cuenta que este tipo de proceso de detección no encontrará *rootkits* desconocidos o a nivel del núcleo del sistema.

Muchos *rootkit*s ocultan archivos en el directorio */dev* (es el que contiene los ficheros de dispositivo del sistema). *Rootcheck* también realiza el escaneo de esta ubicación y en su jerarquía de carpetas.

También realiza escaneo de archivos inusuales y cualquier problema de permisos. Por ejemplo, el caso de los archivos que propiedad del *root,* que tienen permisos de lectura/escritura para cualquier usuario, se considera una situación de riesgo elevado porque cualquier usuario puede hacer modificaciones a su antojo, por lo que, son un objetivo a revisar por *rootcheck*. Otro ejemplo, son archivos y directorios ocultos que también los inspeccionará.

Además, los procesos ocultos también son revisados, mediante la verificación de si algún *PID*[84] está en uso. Si fuera así, pero no se pudiera localizar el proceso que lo ocupa, quiere decir que ocurre alguna inconsistencia en el sistema podría significar que algún *rootkit* está actuando en el núcleo del sistema.

Rootcheck busca la presencia de puertos ocultos, para verificar los puertos del sistema. Si detecta un puerto como ocupado, pero al compararlo con las conexiones activas hay discrepancias, es posible que esté bajo la influencia de un *rootkit*.

Por último, *rootcheck* tiene capacidad de escanear todas las interfaces en modo promiscuo. Se comprueba que la interfaz está configurada como modo promiscuo, si el estado de las interfaces de red no concuerda, es posible que se trate de *rootkit*.

7.2.5 Respuesta activa

Las repuestas activas son acciones inmediatas que se ejecutan en el agente o en el servidor que se activan tras un determinado evento. Se emplean para evitar la propagación de un incidente. Las respuestas activas se componen de dos partes, en

[83] *Rootkit*: herramientas utilizadas por los *hackers* para cubrir sus huellas.
[84] PID: identificador de procesos empleado por el núcleo de algunos sistemas operativos.

primer lugar, del comando que ejecutará la respuesta activa, y en segundo lugar, de la que enlaza los comandos definidos con las reglas.

7.2.5.1 Crear respuestas activa

En la primera fase, se crean los comandos para ser usados como respuestas. Los campos necesarios para crear un comando son:

```
<command>
<name>El nombre (La-Za-Z0-9)</name>
<ejecutable>Comando a ejecutar (La-Za-z0-9.-)</ejecutable>
<expect> (separar argumentos por coma) (La-Za-z0-9)</expect>
<timeout_allowed>si/no</timeout_allowed>
</command>
```

En la segunda fase de ejecución de respuesta activa, es donde se hará la asociación de los comandos entre eventos y las condiciones:

```
<active-response>
  <disabled>si/no</disabled>
  <command>Nombre del comando</command>
  <location>Ubicación del comando</location>
  <agent_id>ID del agente (when using a defined agent)</agent_id>
  <level>Mínimo valor del nivel para su ejecución (0-9)</level>
  <rules_id>(separar argumentos por coma) (0-9)</rules_id>
  <rules_group>(separar lista de grupos por coma) (La-Za-z0-9)</rules_group>
  <timeout>Tiempo de bloqueo</timeout>
</active-response>
```

Nota: En el caso del sistema operativo *Windows* hay que deshabilitar primero la respuesta activa por defecto y después activar la de *Windows*. Se hará mediante la siguiente configuración en el archivo OSSEC.*conf* del agente.

```
<active-response>
<disabled>yes</disabled>
</active-response>
```

7.3 Infraestructura OSSEC

7.3.1 Despliegue OSSEC

Los elementos que forman parte o pueden formar parte de una arquitectura OSSEC, según el Manual de OSSEC, son los siguientes [219]:

Servidor: es el elemento central. Es la ubicación donde se almacenan las bases de datos de comprobación de integridad de archivos, registros, eventos y las entradas de auditoría en el sistema. También es donde se almacenan las reglas, decodificadores y opciones de configuración principales. Un solo servidor es capaz de gestionar un número elevado de agentes, por defecto está limitado a un máximo de 256, pero se puede reconfigurar el tiempo de compilación y dependiendo de la carga del evento se puede aumentar el número de agentes para un mismo servidor, en algún caso se podría llegar hasta 1000. Los agentes se suelen conectar al servidor por el puerto 1514/UDP.

Agente: es un programa que se instala en el sistema que se va a supervisar. Dependiendo el tipo de información se recoge a tiempo real o en diferido. Es un programa que consume pocos recursos de la CPU, por lo que el impacto es bajo en el rendimiento del sistema. El agente se ejecuta con un nivel bajo de privilegios, y además se ejecuta en un *chroot jail*[85] que aísla del sistema. La mayor parte de la configuración del agente se puede realizar desde el servidor.

Sin agente: en sistemas en los que no se puede instalar un agente. Se puede emplear para supervisar cortafuegos, enrutadores o sistemas *Unix*.

Virtualización: OSSEC, puede ser instalado en algunas versiones de *VMWare ESX*[86] [223] , pero hay que tener en cuenta que puede causar falsos positivos, alertas cuando se instala, se elimina, se inicia un huésped, etc. También, supervisa los inicios de sesión, los *logouts* y los errores dentro del servidor *ESX*.

Cortafuegos, *conmutadores* y enrutadores: OSSEC tiene la capacidad de analizar eventos desde distintos cortafuegos, conmutadores y enrutadores. Soporta todos los *routers* de *Cisco, Cisco PIX, Cisco FWSM, Cisco ASA, Juniper Routers*, *firewall Netscreen, Checkpoint* y otros.

7.3.2 Arquitectura funcional OSSEC

Algunos de los principales servicios que conforman el funcionamiento de OSSEC son:

syscheckd: proceso que realiza los análisis de integridad.

logcollector: se encarga de la recogida de todos los *logs* del sistema (syslog, ficheros planos, eventos de *Windows*, etc.).

agentd: envía los registros al servidor.

execd: encargado de ejecutar las respuestas activas.

remoted: se encarga de la recepción de los *logs* de los agentes.

---

[85] *chroot jail:* es un mecanismo para aislar la ejecución de un proceso padre y sus hijos del directorio raíz, y que un atacante no pueda acceder.

[86] *VMware ESX*: hipervisor nativo o plataforma que permite técnicas de virtualización que permite dividir un servidor físico en vario servidores, denominados máquinas virtuales.

analysisd: se trata del proceso principal de OSSEC. Gestiona todos los procesos de análisis.

maild: envío correos electrónicos de las alertas.

El siguiente esquema, muestra como el servidor central recibe eventos de los agentes de los distintos sistemas remotos y cómo funcionan entre si los distintos servicios.

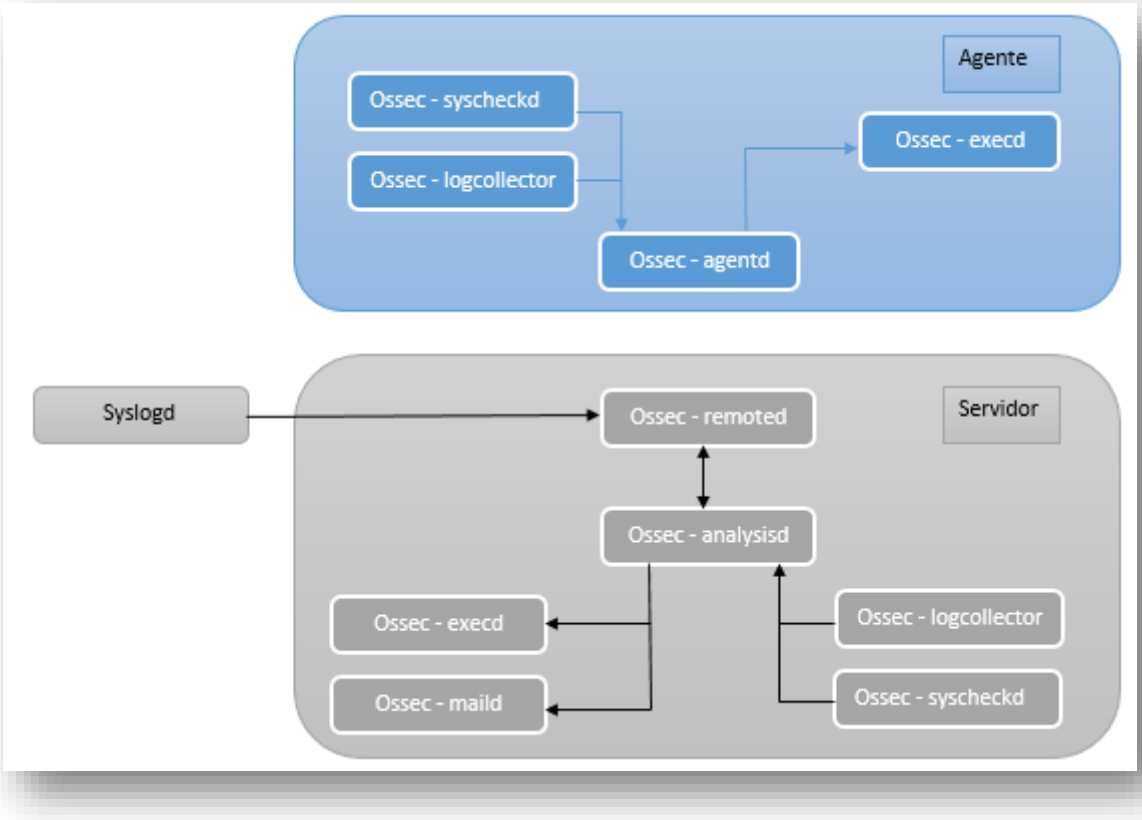


Figura 45 Iteración entre los servicios de la configuración OSSEC [224]

7.4 Reglas en OSSEC

7.4.1 Características de las reglas

Las reglas implementadas en OSSEC definen una política de seguridad para cada sistema o servicio informático. Se crean para implementar controles de seguridad. Las reglas están codificadas en ficheros XML[87] (del inglés *Extensible Markup Language*). Se encuentran en: */var/OSSEC/rules*.

Las reglas se clasifican por niveles, empezando desde el 00, que es el más bajo, hasta el 16, que es el máximo y algunos que todavía no están definidos:

Nivel	Estado	Acción

[87] XML: lenguaje basado en etiquetas. Se utilizan para organizar datos y que estos sean más fáciles de leer para otros programas.

00	Ignorado	Ninguna acción tomada. Se utiliza para evitar falsos positivos. Estas reglas son escaneadas antes que todas las demás. Incluyen eventos sin relevancia de seguridad.
01	Ninguno	
02	Notificación de baja prioridad del sistema	Notificación del sistema o mensajes de estado. No tienen ninguna relevancia de seguridad.
03	Sucesos / Eventos autorizados	Incluyen intentos de inicio de sesión exitosos, eventos de *firewall* permitidos, etc.
04	Errores de baja prioridad del sistema	Errores relacionados con malas configuraciones o dispositivos / aplicaciones no utilizados. No tienen ninguna relevancia de seguridad y normalmente son causados por instalaciones predeterminadas o pruebas de software.
05	Error generado por el usuario	Incluyen contraseñas perdidas, acciones denegadas, etc. Por sí mismas no tienen relevancia de seguridad.
06	Ataque de baja relevancia	Indican un gusano o un virus que no afectan al sistema (como el código rojo para servidores apache, etc). También incluyen frecuentemente eventos IDS y frecuentemente errores.
07	Correspondencia "palabra errónea"	Incluyen palabras como "malo", "error", etc. Estos eventos son la mayoría del tiempo sin clasificar y pueden tener cierta relevancia de seguridad.
08	Primera vez vista	Incluye eventos por primera vez. Primera vez que se dispara un evento IDS o la primera vez que un usuario inicia sesión. Si acaba de empezar a usar OSSEC HIDS, estos mensajes probablemente serán frecuentes. Después de un tiempo deben irse, también incluye medidas de seguridad relevantes (como el inicio de un *sniffer* o algo así).
09	Error de origen no válido	Incluye intentos de inicio de sesión como usuario desconocido o de una fuente no válida. Puede tener relevancia de seguridad (especialmente si se repite). También incluyen errores con respecto a la cuenta "*admin*" (*root*).
10	Errores generados por múltiples usuarios	Incluyen varias contraseñas incorrectas, múltiples inicios de sesión fallidos, etc. Pueden indicar un ataque o simplemente que un usuario acaba de olvidar sus credenciales.
11	Advertencia de verificación de integridad	Incluyen mensajes relativos a la modificación de binarios o la presencia de *rootkit*s (por *rootcheck*). Si acaba de modificar la configuración del sistema, debería estar bien con respecto a los mensajes "syscheck". Pueden indicar un ataque exitoso. También se incluyen eventos IDS que serán ignorados (alto número de repeticiones).

12	Evento de alta importancia	Incluyen mensajes de error o de advertencia del sistema, núcleo, etc. Pueden indicar un ataque contra una aplicación específica.
13	Error inusual (alta importancia)	La mayoría de las veces coincide con un patrón de ataque común.
14	Evento de seguridad de alta importancia	La mayoría de las veces se hace con correlación e indica un ataque.
15	Grave ataque	No hay posibilidades de falsos positivos. Es necesaria una atención inmediata.

Tabla 5 Niveles de las reglas OSSEC

Además, se pueden agrupar para la utilidad de respuesta activa y para la correlación. Los grupos que existen actualmente son: *invalid_login, authentication_success, authentication_failed, connection_attempt, attacks, adduser, sshd,* IDS*, firewall, squid, apache y syslog.*

Un ejemplo, de la estructura mínima básica que tendría una regla sería:

```
<rule id = "numero de regla" level = "Numero del nivel de regla">
  <description> Descripción de la regla </description>
  <group> Grupo al que la regla pertenece</group>
</rule>
```

A continuación, la Tabla 6 Campos para crear reglasTabla 6 contiene todos los campos que puede formar parte de una regla:

Campos que definen la regla		Definición del campo	Valor permitido
Attributes	Level	Especifica el nivel de la regla. Las respuestas activas y las alertas hacen uso de este nivel.	Cualquier número entre 0 y 16 ambos incluidos.
	ID	Identificador de la regla.	cualquier número del 1 al 99999
	Maxsize	Especifica el tamaño máximo del evento	cualquier número del 100 al 9999
	Frequency	Número de veces que una regla debe coincidir antes de ejecutarse.	cualquier número del 100 al 999
	Timeframe	Esta opción está destinada a ser utilizada con la opción de frecuencia.	cualquier número del 1 al 9999
	Ignore	El tiempo (en segundos) para ignorar esta regla después de dispararla (para evitar inundaciones).	cualquier número del 1 al 9999

	Overwrite	Se usa para reemplazar una regla OSSEC con cambios locales.	sí
match	Cualquier cadena que coincida con el evento de registro.		cualquier sintaxis *OS_Match / sregex*
regex	Cualquier expresión regular que coincida con el evento de registro.		Cualquier sintaxis *OR_Regex / regex*
decoded_as	Cualquier nombre de decodificador		cualquier nombre de decodificador
category	La categoría descodificada para que coincida (IDS, *syslog*, *firewall*, web-log, *squid* o *Windows*).		cualquier categoría de categoría
srcip	Cualquier dirección IP o bloque *CIDR* que se comparen con un IP decodificado como *srcip*.		Use "!" Para negarlo. Cualquier *srcip*
dstip	Cualquier dirección IP o bloque CIDR que se comparen con un IP decodificado como *dstip*.		Use "!" Para negarlo. Cualquier dstip
extra_data	Cualquier cadena que se decodifica en el campo extra_data.		Cualquier cadena.
user	Cualquier nombre de usuario		cualquier sintaxis *OS_Match / sregex*
program_name	El nombre del programa se decodifica desde el nombre del proceso *syslog*.		cualquier sintaxis *OS_Match / sregex*
hostname	Cualquier nombre de *host* (decodificado como el nombre de *host syslog*) o archivo de registro.		cualquier sintaxis *OS_Match / sregex*
time	Hora en que se generó el evento		Cualquier intervalo de tiempo (hh: mm-hh: mm)
weekday	Día de la semana en que se generó el evento.		lunes - domingo, día laborable, fin de semana
id	Cualquier ID (decodificada como la ID).		cualquier sintaxis *OS_Match / sregex*
url	Cualquier URL (decodificada como la URL).		cualquier sintaxis OS_Match / sregex
if_sid	Coincide si la ID ha coincidido.		cualquier ID de regla
if_group	Coincide si el grupo ha coincidido antes.		cualquier grupo
if_level	Coincide si el nivel ha coincidido antes.		Cualquier nivel del 1 al 16
if_matched_sid	Coincide si se ha activado una alerta de la ID definida en un número determinado de segundos.		Esta opción se usa junto con la frecuencia y el marco de tiempo.
if_matched_group	Coincide si se ha activado una alerta del grupo definido en un número determinado de segundos.		cualquier grupo
same_id	Especifica que el ID decodificado debe ser el mismo.		Esta opción se usa junto con la frecuencia y el marco de tiempo.
same_source_ip	Especifica que la fuente IP decodificada debe ser la misma.		Esta opción se usa junto con la frecuencia y el marco de tiempo.

same_source_port	Especifica que el puerto de origen decodificado debe ser el mismo.	Esta opción se usa junto con la frecuencia y el marco de tiempo.
same_dst_port	Especifica que el puerto de destino decodificado debe ser el mismo.	Esta opción se usa junto con la frecuencia y el marco de tiempo.
same_location	Especifica que la ubicación debe ser la misma.	Esta opción se usa junto con la frecuencia y el marco de tiempo.
same_user	Especifica que el usuario descodificado debe ser el mismo.	Esta opción se usa junto con la frecuencia y el marco de tiempo.
description	Descripción de la regla	cualquier cadena
check_diff	Se usa para determinar cuándo cambia la salida de un comando.	Uso: <check_diff />
group	Agregue grupos adicionales a la alerta. Los grupos son etiquetas opcionales agregadas a las alertas. Pueden ser utilizados por otras reglas usando *if_group* o *if_matched_group*, o por herramientas de análisis de alerta para categorizar alertas.	Cualquier grupo.

Tabla 6 Campos para crear reglas

7.4.2 Crear reglas

OSSEC, dispone de una base de datos de reglas muy amplia pero no es suficiente para cubrir todas las necesidades de los usuarios, es por esto que permite crear reglas a gusto y modificar reglas que ya existen.

Para modificar una regla se añadirá en la etiqueta de identificación de la regla el comando "*overwrite=yes*".

1. Regla existente, de nivel 5:

```
<rule id="XXX" level="5">
  <match> coincidencia con cadena de texto del log </match>
  <description> despcripción de la regla </description>
  <group> grupo de la regla </group>
</rule>
```

2. Regla actualizada, con nuevo nivel de regla a 10:

```
<rule id="XXX" level="10" overwrite="yes">
  <if_sid>XXX</if_sid>
  <match> coincidencia con cadena de texto del log </match>
  <description> despcripción de la regla </description>
  <group> grupo de la regla </group>
</rule>
```

Por otro lado, para crear una regla nueva desde cero bastará con que incluya los siguientes campos del ejemplo (en el Anexo 12 se detallan todos los campos que puede tener una regla):

```
<rule id="100010" level="0">
  <match> coincidencia con cadena de texto del log </match>
  <description> despcripción de la regla </description>
</rule>
```

Cada vez que se crea y de define una nueva regla, hay que reiniciar OSSEC para que entre en funcionamiento la regla, mediante el comando "*sudo /var/OSSEC/bin/OSSEC-control restart*".

7.4.3 Pruebas con reglas

En versiones anteriores a la 1.6 las pruebas de las reglas o decodificadores implementados había que realizarlas a mano, pero hoy en día es mucho más sencillo con la herramienta: *OSSEC-logtest*, facilita:

- La depuración de las reglas personalizadas.
- Solución de problemas de falsos positivos o falsos negativos.

Se encuentra instalada en la ubicación */var/OSSEC/bin* y la ejecución será de la siguiente forma:

```
sudo /var/OSSEC/bin/OSSEC-logtest
```

Los argumentos que soporta son los siguientes:

Argumento	Función
a	Analiza las líneas de entrada como si fueran eventos en vivo.
-c	Es la ruta y el nombre de archivo a cargar en lugar del */var/OSSEC/etc/OSSEC.conf* predeterminado
-D	Esta es la ruta a la que *OSSEC-logtest* accederá antes de completar todas las reglas, decodificadores y listas y procesar la entrada estándar.
-d	Imprime la salida de depuración en la terminal. Esta opción se puede usar varias veces para aumentar la verbosidad de los mensajes de depuración.
-h	Imprime el mensaje de ayuda en la consola.
-t	Configuración de prueba. Esto imprimirá los detalles del archivo en las reglas, decodificadores y listas de *OSSEC-anaylistd* a medida que se cargan y el orden en que se procesaron.
-U	Esta opción hará que *OSSEC-logtest* regrese con un estado de salida distinto de cero a menos que la última línea probada coincida con los argumentos aprobados.

Tabla 7 Opciones de argumentos de OSSEC-Logtest

8 PRUEBAS

En este proyecto se propone una herramienta de seguridad, concretamente un sistema detector de intrusión, para elevar la confianza en los sistemas y disminuir el riego de ocurrencia de un ataque.

Se han planteado una solución para comprender de forma práctica las capacidades de cada uno de los sistemas, así como tener en cuenta los beneficios y limitaciones de cada uno y sus posibles aplicaciones en un entorno real.

En primer lugar, se ha implementado la Herramienta OSSEC, el cual es un detector de intrusión para *host*.

8.1 Arquitectura de red propuesta

8.1.1 Diagrama de red

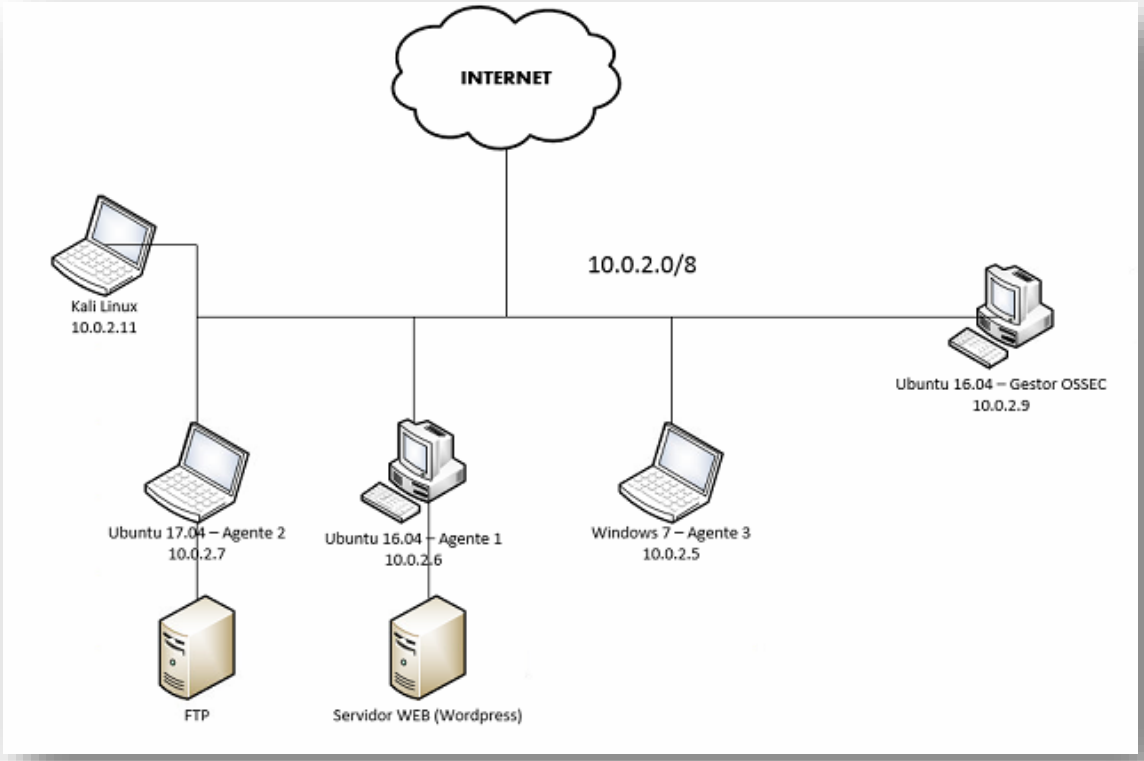


Figura 46 Esquema de red propuesto para las pruebas

8.1.2 Elementos

El despliegue del entorno se ha realizado mediante *Virtualbox*[88] [225], que es una herramienta que permite ejecutar múltiples sistemas operativos a la vez. Las máquinas que forman el entorno son:

- **Gestor OSSEC:** Sistema operativo *Ubuntu*16.04 *Server* de 64 *bits*. Es la máquina que alojará el gestor de OSSEC. IP: 10.0.2.9
- **Agentes:**
  - **Agente 1:** Sistema operativo *Ubuntu*17.04 *Server* de 64 *bits*. IP: 10.0.2.7. Aloja un servidor FTP.
  - **Agente 2:** Sistema operativo *Ubuntu*16.04 *Server* de 64 *bits*. IP: 10.0.2.6. Alojará un servidor web.
  - **Agente 3:** Sistema operativo *Windows* 7 *Server* de 32 *bits*. IP: 10.0.2.5
- **Máquina *kali-Linux*:** Sistema operativo *Debian* de 64 *bits*. Es la máquina empleada para encontrar vulnerabilidades. IP 10.0.2.11.

8.2 Evaluación de riesgos

En este punto se va a realizar una evaluación de supuestos riesgos a los que podrían estar expuestos los sistemas del esquema propuesto. Para ello se proponen situaciones que pueden encontrarse en cualquier momento de la vida cotidiana de las empresas y particulares. Se han elegido estos riesgos por la experiencia obtenida en auditorias de sistemas, basada en la aplicación del estándar ISO/IEC 27001 [1] y en la metodología de análisis de riesgos margerit [14].

Riesgo 1. Acceso de usuarios en horarios restringidos. Posibilidad de ataques o actividades malintencionadas fuera de un horario habitual, por ejemplo, horario laboral, puesto que hay menos vigilancia a estas horas.

Riesgo 2. Múltiples fallos de autenticación en breve periodo de tiempo. Un posible atacante que desconoce la contraseña para acceder podría ejercer un ataque de fuerza bruta para obtener las credenciales de acceso.

Riesgo 3. Realización de acciones no autorizadas o ilícitas por usuarios administradores. Estos usuarios poseen un perfil con permisos de escritura y lectura total en todo el sistema por lo que podrían hacer o deshacer a su parecer.

Riesgo 4. Incidencias en servidores web. Por falta de capacidad o mantenimiento de los sistemas podría dejarse de ofrecer un servicio a un cliente.

[88] *Virtualbox*: es un producto de virtualización x86 y AMD64/Intel64 para uso empresarial y doméstico.

Riesgo 5. Acciones ilícitas servidores web propios. Clientes o empleados podrían realizar acciones ilícitas sobre los servidores web y derivar en una denegación del servicio o robo de información.

Riesgo 6. Múltiples fallos de autenticación en breve periodo de tiempo. Un posible atacante que desconoce la contraseña para acceder podría ejercer un ataque de fuerza bruta para obtener las credenciales de acceso.

Riesgo 7. Acceso de un usuario que no existe en el sistema. Intento de acceso con usuario que no existe para acceder ejerciendo un ataque de fuerza bruta para obtener las credenciales de acceso.

Riesgo 8. Cambios de contraseñas no autorizados. Un atacante que ha conseguido entrar en el sistema podría cambiar las claves de acceso de los usuarios impidiendo su acceso.

Riesgo 9. Elevación de permiso no autorizado. Un atacante o intruso, tras acceder a los sistemas, se otorga a si mismo perfil de administrador, adquiriendo el control total del sistema.

Riesgo 10. Acceso a información en ubicaciones críticas. Usuarios sin permiso para ello aceden a información sensible lo que vulnera la confidencialidad de la información.

Riesgo 11. Conexiones remotas no autorizadas. Posibles intrusos intentan acceder de forma remota.

Riesgo 12. Creación, borrado o modificación de información sensible. Se vulnera la integridad, exactitud, completitud y disponibilidad de datos sensibles.

Riesgo 13. Ataque inyección SQL. Mediante código SQL obtener información que contienen las bases de datos.

Riesgo 14. Acceso remoto no autorizado: Un usuario no autorizado realiza con éxito un acceso no autorizado a los sistemas mediante SSH.

Riesgo 15. Ataque XSS. Ataque web que mediante código *javascript* o similar, se puede obtener información sensible o limitar las capacidades del navegador y del servicio.

Riesgo 16. Evento *rootkit*. Un ataque puede estar pasando desapercibido mediante el uso de estas herramientas.

Riesgo 17. Un grupo/usuario es añadido al sistema. Se pueden otorgar permisos a usuarios no autorizados por error o de forma intencionada.

8.3 Marco de control de seguridad

Para demostrar las funcionalidades de OSSEC y su capacidad en este punto, se indican los controles que se plantean para mitigar los riesgos descritos en el punto anterior con la implementación de OSSEC. Este análisis está basado en la aplicación de objetivos de control de la normativa ISO/IEC 27001 y la ISO/IEC 27002:2013 [1], objetivos de control de COBIT versión 5 [2] y de las recomendaciones de ITIL versión 3 [15], además se ha tenido en cuenta el marco operacional definido por el CNN-CERT en la guía CCN-STIC 804) [16]. A continuación, la Tabla 8 contiene la relación entre los controles definidos en este proyecto y las tres normativas de seguridad referidas anteriormente.

Nombre del control	Objetivo de control ISO 27002:2013	Objetivo de Control COBIT 5	Información de soporte ITIL V3
Detección de accesos en horarios.	7.1.1 Inventario de activos 11.1.1 Políticas de control de acceso	PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	SD 5.2 Gestión de los datos y la información SD 7 Consideraciones tecnológicas
Elevación de privilegios	6.1.5 Acuerdos de confidencialidad 6.2.1 Identificación de riesgos relacionados con terceros 6.2.2 Considerar la seguridad al tratar con los clientes 8.1.1 Roles y responsabilidades 8.3.1 Responsabilidades en el cese 8.3.3 Eliminación de privilegios de acceso 10.1.3 Segregación de funciones 11.1.1 Políticas de control de acceso 11.2.1 Registro de usuarios 11.2.2 Gestión de privilegios 11.2.4 Revisión de derechos de acceso de usuarios 11.3.1 Uso de contraseñas 11.5.1 Procedimientos seguros de inicio de sesión 11.5.3 Sistema de gestión de contraseñas 11.6.1 Restricción de acceso a la información	DS5.4 Gestión de cuentas de usuario	SO 4.5 Gestión de acceso SO 4.5.5.1 Peticiones de acceso SO 4.5.5.2 Verificación SO 4.5.5.3 Habilitar privilegios SO 4.5.5.4 Monitorear el estado de la identidad SO 4.5.5.5 Registro y seguimiento de accesos SO 4.5.5.6 Eliminar o restringir privilegios
Múltiples intentos fallos de inicio de	5.1.1 Documento de la política de seguridad de la información	DS5.3 Gestión de identidad	SO 4.5 Gestión de acceso

sesión en un breve periodo de tiempo.	5.1.2 Revisión de la política de seguridad de la información 6.1.2 Coordinación para la seguridad de la información 6.1.5 Acuerdos de confidencialidad 8.2.2 Educación, entrenamiento y concienciación en seguridad de información 11.1.1 Políticas de control de acceso 11.7.2 Teletrabajo		
Conexión exitosa SSH	5.1.1 Documento de la política de seguridad de la información 5.1.2 Revisión de la política de seguridad de la información 6.1.2 Coordinación para la seguridad de la información 6.1.5 Acuerdos de confidencialidad 8.2.2 Educación, entrenamiento y concienciación en seguridad de información 11.1.1 Políticas de control de acceso 11.7.2 Teletrabajo	DS5.3 Gestión de identidad	SO 4.5 Gestión de acceso
Detectar intento de acceso SSH con un usuario que no existe.	6.1.5 Acuerdos de confidencialidad 6.2.1 Identificación de riesgos relacionados con terceros 6.2.2 Considerar la seguridad al tratar con los clientes 8.1.1 Roles y responsabilidades 8.3.1 Responsabilidades en el cese 8.3.3 Eliminación de privilegios de acceso 10.1.3 Segregación de funciones 11.1.1 Políticas de control de acceso 11.2.1 Registro de usuarios 11.2.2 Gestión de privilegios 11.2.4 Revisión de derechos de acceso de usuarios 11.3.1 Uso de contraseñas 11.5.1 Procedimientos seguros de inicio de sesión 11.5.3 Sistema de gestión de contraseñas 11.6.1 Restricción de acceso a la información	DS5.4 Gestión de cuentas de usuario	SO 4.5 Gestión de acceso SO 4.5.5.1 Peticiones de acceso SO 4.5.5.2 Verificación SO 4.5.5.3 Habilitar privilegios SO 4.5.5.4 Monitorear el estado de la identidad SO 4.5.5.5 Registro y seguimiento de accesos SO 4.5.5.6 Eliminar o restringir privilegios

Intento de ataque por fuerza bruta de SSH.	5.1.1 Documento de la política de seguridad de la información 5.1.2 Revisión de la política de seguridad de la información 6.1.2 Coordinación para la seguridad de la información 6.1.5 Acuerdos de confidencialidad 8.2.2 Educación, entrenamiento y concienciación en seguridad de información 11.1.1 Políticas de control de acceso 11.7.2 Teletrabajo	DS5.3 Gestión de identidad	SO 4.5 Gestión de acceso
Accesos a ubicaciones lógicas determinadas críticas.	6.1.5 Acuerdos de confidencialidad 6.2.1 Identificación de riesgos relacionados con terceros 6.2.2 Considerar la seguridad al tratar con los clientes 8.1.1 Roles y responsabilidades 8.3.1 Responsabilidades en el cese 8.3.3 Eliminación de privilegios de acceso 10.1.3 Segregación de funciones 11.1.1 Políticas de control de acceso 11.2.1 Registro de usuarios 11.2.2 Gestión de privilegios 11.2.4 Revisión de derechos de acceso de usuarios 11.3.1 Uso de contraseñas 11.5.1 Procedimientos seguros de inicio de sesión 11.5.3 Sistema de gestión de contraseñas 11.6.1 Restricción de acceso a la información	DS5.4 Gestión de cuentas de usuario	SO 4.5 Gestión de acceso SO 4.5.5.1 Peticiones de acceso SO 4.5.5.2 Verificación SO 4.5.5.3 Habilitar privilegios SO 4.5.5.4 Monitorear el estado de la identidad SO 4.5.5.5 Registro y seguimiento de accesos SO 4.5.5.6 Eliminar o restringir privilegios
Conexión desde fuera del país.	7.1.1 Inventario de activos 11.1.1 Políticas de control de acceso	PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos	SD 5.2 Gestión de los datos y la información SD 7 Consideraciones tecnológicas
Cambiar permisos de ficheros (permitir lectura/escritura para cualquier usuario).	6.1.5 Acuerdos de confidencialidad 6.2.1 Identificación de riesgos relacionados con terceros 6.2.2 Considerar la seguridad al tratar con los clientes	DS5.4 Gestión de cuentas de usuario	SO 4.5 Gestión de acceso SO 4.5.5.1 Peticiones de acceso SO 4.5.5.2 Verificación SO 4.5.5.3 Habilitar privilegios

	8.1.1 Roles y responsabilidades 8.3.1 Responsabilidades en el cese 8.3.3 Eliminación de privilegios de acceso 10.1.3 Segregación de funciones 11.1.1 Políticas de control de acceso 11.2.1 Registro de usuarios 11.2.2 Gestión de privilegios 11.2.4 Revisión de derechos de acceso de usuarios 11.3.1 Uso de contraseñas 11.5.1 Procedimientos seguros de inicio de sesión 11.5.3 Sistema de gestión de contraseñas 11.6.1 Restricción de acceso a la información		SO 4.5.5.4 Monitorear el estado de la identidad SO 4.5.5.5 Registro y seguimiento de accesos SO 4.5.5.6 Eliminar o restringir privilegios
Habilitar/Deshabilitar puertos.	6.2.1 Identificación de riesgos relacionados con terceros 10.6.1 Controles de red 10.6.2 Seguridad de los servicios de red 11.4.1 Política de uso de los servicios de red 11.4.2 Autenticación de usuarios para conexiones externas 11.4.3 Identificación de equipos en redes 11.4.4 Protección de puertos de configuración y diagnóstico remoto 11.4.5 Segregación en redes 11.4.6 Control de conexiones en la red 11.4.7 Control de enrutamiento de la red 11.6.2 Aislamiento de sistemas sensitivos	DS5.10 Seguridad de la red	SO 5.5 Gestión de redes
Evento producido por rootkit.	10.4.1 Controles contra código malicioso	DS5.9 Prevención, detección y corrección de software malicioso	N/A
Cambio en la integridad de un archivo (tamaño).	N/A	PO2.4 Gestión de integridad	SD 5.2 Gestión de los datos y la información ST 4.7 Gestión del conocimiento
Nuevo grupo añadido al sistema.	6.1.2 Coordinación para la seguridad de la información	PO4.6 Establecer roles y responsabilidades	SS 2.6 Funciones y procesos a través del ciclo de vida SD 6.2 Análisis de actividades

	6.1.3 Asignación de las responsabilidades para la seguridad de la información 6.1.5 Acuerdos de confidencialidad 8.1.1 Roles y responsabilidades 8.1.2 Verificación 8.1.3 Términos y condiciones del empleo 8.2.2 Educación, entrenamiento y concienciación en seguridad de información 15.1.4 Protección de datos y privacidad de la información personal		SD 6.4 Roles y responsabilidades ST 6.3 Modelos organizacionales para apoyar la transición de servicios SO 6.6 Roles y responsabilidades en la operación del servicio CSI 6 Organización para la mejora continua del servicio
Nuevo usuario añadido al sistema.	6.1.2 Coordinación para la seguridad de la información 6.1.3 Asignación de las responsabilidades para la seguridad de la información .1.5 Acuerdos de confidencialidad 8.1.1 Roles y responsabilidades 8.1.2 Verificación 8.1.3 Términos y condiciones del empleo 8.2.2 Educación, entrenamiento y concienciación en seguridad de información 15.1.4 Protección de datos y privacidad de la información personal	PO4.6 Establecer roles y responsabilidades	SS 2.6 Funciones y procesos a través del ciclo de vida SD 6.2 Análisis de actividades SD 6.4 Roles y responsabilidades ST 6.3 Modelos organizacionales para apoyar la transición de servicios SO 6.6 Roles y responsabilidades en la operación del servicio CSI 6 Organización para la mejora continua del servicio
Detección de múltiples intento ataques web: Inyección SQL.	10.4.1 Controles contra código malicioso	DS5.9 Prevención, detección y corrección de software malicioso	N/A
Ataque de fuerza bruta a Wordpress.	10.4.1 Controles contra código malicioso	DS5.9 Prevención, detección y corrección de software malicioso	N/A
Intento de ataque de inyección SQL	10.4.1 Controles contra código malicioso	DS5.9 Prevención, detección y corrección de software malicioso	N/A
Intento de ataque web (XSS).	10.4.1 Controles contra código malicioso	DS5.9 Prevención, detección y	N/A

		corrección de software malicioso	
Fallo del servidor web.	10.10.1 *Logs* de auditoría 10.10.5 *Logs* de fallas 12.2.1 Validación de datos de entrada 12.2.2 Control de procesamiento interno 12.2.3 Integridad de mensajes 12.2.4 Validación de datos de salida 13.2.3 Recolección de evidencia 15.3.1 Controles de auditoría de sistemas de información 15.3.2 Protección de herramientas de auditoría de sistemas	AI2.3 Control y auditoría de aplicaciones	N/A

Tabla 8 Marco de controles y comparativa con ISO27002:2013 [1], Cobit v5 [2] e Itil v3 [15].

8.4 Plan de pruebas

En este punto, se procede a ejecutar el plan de pruebas de las herramientas. Se detallarán los pasos realizados en el test de intrusión para explotar las vulnerabilidades, además se incluye configuraciones necesarias y herramientas utilizadas para las intrusiones.

Se van a evaluar los controles descritos en el punto 8.3, para ello en el sistema OSSEC se realiza un chequeo de su efectividad. Se detalla su implementación en la herramienta OSSEC para cada uno de los controles, ya que se va a asociar a cada control una o varias reglas. Así, OSSEC tiene la posibilidad de detectar cada una de las situaciones de riesgo que se han determinado en el punto 8.2. Algunas reglas, ya están contenidas en la última versión de OSSEC y otras diseñadas o sobrescritas de alguna existente, por lo que se van describir tres tipos de reglas: existentes (ya existen en la base de datos de OSSEC); modificadas (se han modificado para este proyecto, pero se parte de una regla ya existente) y nuevas reglas (se han definido para este proyecto).

Para evidenciar la existencia de la implementación se aportará para cada caso la regla programada en la herramienta y una captura de las alertas en la aplicación web de OSSEC. Las alertas se visualizan en la aplicación web que se explica más adelante en el punto 12

A continuación, se va a detallar punto a punto las pruebas para cada control que incluye el objetivo de control, riesgo que mitiga, implementación de la regla en OSSEC del control y las pruebas de intrusión de vulnerabilidades.

8.4.1 Detección de accesos en horarios no permitidos.

ID Control: 01

Objetivo del control: El objetivo de este control es detectar los accesos que se produzcan fuera de un horario permitido.

Riesgo: Este control mitigaría el Riesgo 1 indicado en el punto 8.2.

Descripción regla en OSSEC: Se ha definido una regla nueva. Esta nueva regla se define en el fichero de reglas locales, donde normalmente definiremos nuevas reglas. La ubicación del fichero de reglas es: */var/ossec/etc/rules.d/local_rules.xml.*

Se define un nuevo ID para la regla, en este caso ID=100070, asegurándose que esté libre o fallará en la compilación. Se establece el nivel de la regla en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 12 (ver niveles definidos en el punto 7.4.1 de este trabajo) para la regla ya que se considera un evento de alta importancia que pueden indicar un ataque contra una aplicación específica. Se definen las condiciones para que se cumpla la regla, en este caso cualquier tipo de acceso (5501, se abre sesión; 5504, intento de *login* con usuario no valido; 40101, autenticación del sistema) y dentro de una franja horaria. La franja horaria se define en función de las necesidades del negocio, por lo que se ha considerado que dentro de este rango no debería acceder ningún usuario o estar justificado.

```
<rule id="100070" level="12">
        <if_sid>5501,5504,40101</if_sid>
        <time>5:00 pm - 8:30 am</time>
        <description>Login fuera de horario permitido.</description>
        <group>Policy_violation</group>
</rule>
```

Las reglas utilizadas como condición son existentes en la base de datos. Las reglas ID= 5501 e ID=5504 se localiza en *etc/rules/pam_rules.xml* .

```
<rule id="5501" level="3">
  <if_sid>5500</if_sid>
  <match>session opened for user </match>
  <description>Login session opened.</description>
  <group>authentication_success,</group>
</rule>
<rule id="5504" level="5">
  <if_sid>5500</if_sid>
  <match>check pass; user unknown</match>
```

```
  <description>Attempt to login with an invalid user.</description>
  <group>invalid_login</group>
</rule>
```

La regla ID= 40101, se encuentra en */etc/rules/attack_rules.xml*.

```
<group name="syslog,attacks,">
<rule id="40101" level="12">
  <if_group>authentication_success</if_group>
  <user>$SYS_USERS</user>
  <description>System user successfully logged to the system.</description>
  <group>invalid_login,</group>
</rule>
```

Test de intrusión: La prueba se va a realizar en dos fases. La primera consiste en iniciar sesión con alguno de los equipos de la red fuera del horario permitido para comprobar que salta la alerta, posteriormente en una segunda fase se va a iniciar sesión dentro del horario permitido y comprobar que no salta la alerta anterior.

Hallazgos: La prueba se ha realizado con el equipo ubuntu17 (IP 10.0.2.7).

Fase 1: Se adjunta una captura (Figura 47) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (12) y la descripción de la alerta (*Login* fuera de tiempo). El ID=100070 identifica unívocamente la regla. El campo *location* , indica el sistema que origina el evento, en este caso desde el agente1 con IP 10.0.2.7. Todos los parámetros observados.

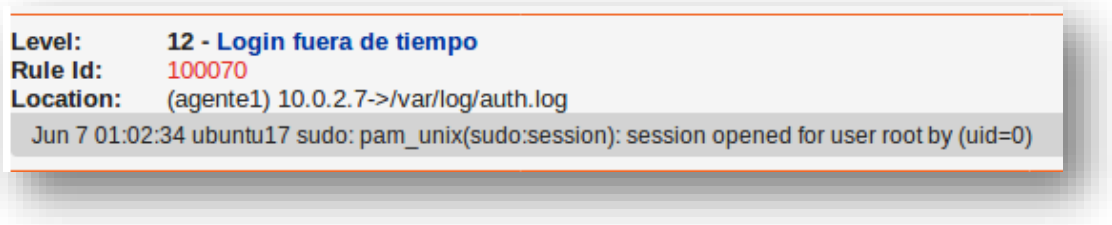


Figura 47 Evidencia alerta de acceso fuera de horario

Fase 2: Para comprobar que esta fase se cumple, se vuelve a realizar el inicio de sesión dentro de una hora permitida y buscamos por el id en el buscador de la web. Se observa que no hay alerta en el momento del acceso.

8.4.2 Elevación de privilegios

ID Control: 02

Objetivo del control: El objetivo de este control es detectar un ataque de elevación de privilegios, para saber sobre este ataque en el punto 4.4.

Riesgo: Este control mitigaría Riesgo 9 el indicado en el punto 8.2.

Descripción regla en OSSEC: La regla ya existe en la base de datos de reglas de OSSEC. Se trata de ID=5404. Esta regla se encuentra definida en el fichero: */etc/rules/syslog_rules.xml.* Se establece el nivel de la regla en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 10 (ver niveles definidos en el punto 7.4.1 de este trabajo) para la regla ya que se considera un evento por errores generados por múltiples usuarios. La primera condición es detectar la regla ID=5401, que se verá más adelante. La cadena de caracteres que espera detectar es "*3 incorrect password attempts*", que significa tres intentos erróneos al introducir las contraseñas. Se mantiene la condición en tres intentos, a pesar de ser un número bajo, por realizar de una manera más sencilla las pruebas. En un entorno real, habría que estudiar que sería un comportamiento anómalo para evitar falso positivos.

```
<rule id="5404" level="10">
  <if_sid>5401</if_sid>
  <match>3 incorrect password attempts</match>
  <description>Three failed attempts to run sudo</description>
</rule>
```

La regla ID=5401, es una regla ya existente. Esta regla tiene la condición de alertar cuando la regla ID=5400 (regla ya existente y que se explicará un poco más adelante) se cumple y cuando en el log se detecte la cadena de caracteres "*incorrect password attempt",* que significa intentos erróneos al introducir contraseña*.* Por otro lado, la regla ID=5400 tiene la funcionalidad de detectar todas las ordenes realizadas en el agente como "sudo", que serían realizadas con el usuario con mayor privilegio. Estas reglas se localizan en *etc/rules/syslog_rules.xml.*

```
<rule id="5401" level="5">
  <if_sid>5400</if_sid>
  <match>incorrect password attempt</match>
  <description>Failed attempt to run sudo</description>
</rule>
<group name="syslog,sudo">
  <rule id="5400" level="0" noalert="1">
  <decoded_as>sudo</decoded_as>
  <description>Initial group for sudo messages</description>
 </rule>
```

Test de intrusión: La prueba se ha realizado con el equipo ubuntu16 (IP 10.0.2.6) Desde el terminal de *Linux* se lanza el comando "sudo su", para elevar privilegios como usuario administrador. Se pide introducir una clave, esta se introducirá erróneamente hasta tres veces, que es el límite máximo de errores aceptado.

Hallazgos: Se adjunta una captura (Figura 47) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (10) y la descripción de la alerta (*Three failed attempsts to run sudo*). El ID=5404 identifica unívocamente la regla. El campo location indica el sistema que origina el evento, en este caso desde el agente1 con IP 10.0.2.7.

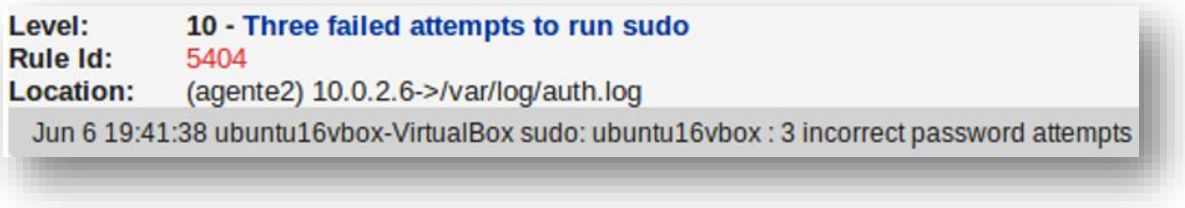


Figura 48 Alerta de tres intentos erróneos de autenticación como sudo

8.4.3 Múltiples intentos fallos de inicio de sesión en un breve periodo de tiempo

ID Control: 03

Objetivo del control: El objetivo de este control es detectar un ataque de intento de acceso de fuerza bruta, para saber sobre este ataque en el punto 4.4.

Riesgo: Este control mitigaría el Riesgo 2 indicado en el punto 8.2.

Descripción regla en OSSEC: Se ha creado una regla nueva. Se define un nuevo ID para la regla, en este caso ID=2510, debe ser un identificador libre o fallará en la compilación. Se establece el nivel de la regla en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 10 (ver niveles definidos en el apartado 7.4.1 de este trabajo) para la regla ya que se consideran errores generados por múltiples usuarios. Los nuevos parámetros (ver 7.4.1) que se han programado son: "*frequency*=3" que quiere decir que la alerta se producirá cuando se detecten 6 eventos de autenticación, esto es así porque por defecto "*frequency*=1" requiere de 2 eventos para saltar; "*timeframe*=120" es el tiempo máximo, 120 segundos, en el que se han de producir los eventos para que salte la regla. La única regla que tiene como condición es que previamente se detecte que se ha lanzado la regla ID=2510, se incluye un poco más adelante en este mismo punto.

```
<rule id="2510" level="10" frequency=”3” timeframe=”120”>
  <if_matched_sid>2501</if_matched _sid>
  <description>6 fallos de autenticación de usuario</description>
```

```
  <group>authentication_failed,</group>
</rule>
```

La regla ID=2501, regla existente en la base de datos de OSSEC, se ubica en *etc/rules/syslog_rules.xml*. Se utiliza como condición en la regla anterior. Se forma de seis condiciones cuyo objetivo es detectar cualquier mensaje en el log que esté relacionado con fallo de autenticación o fallo de acceso al sistema.

```
<rule id="2501" level="5">
  <match>FAILED LOGIN |authentication failure|</match>
  <match>Authentication failed for|invalid password for|</match>
  <match>LOGIN FAILURE|auth failure: |authentication error|</match>
  <match>authinternal failed|Failed to authorize|</match>
  <match>Wrong password given for|login failed|Auth: Login incorrect|</match>
  <match>Failed to authenticate user</match>
  <group>authentication_failed,</group>
  <description>User authentication failure.</description>
</rule>
```

Test de intrusión: La prueba se ha realizado con el equipo ubuntu17 (IP 10.0.2.7). Desde el terminal de *Linux* se lanza el comando “sudo su”, para elevar privilegios como usuario administrador. Se pide introducir una clave, ésta se introducirá erróneamente hasta 3 veces, que es el límite máximo de errores aceptado.

Hallazgos: Se adjunta una captura (Figura 49) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (10) y la descripción de la alerta (6 fallos de autenticación de usuario). El ID= 2510 identifica unívocamente la regla. El campo *location* , indica el sistema que origina el evento, en este caso desde el agente1 con IP 10.0.2.7.

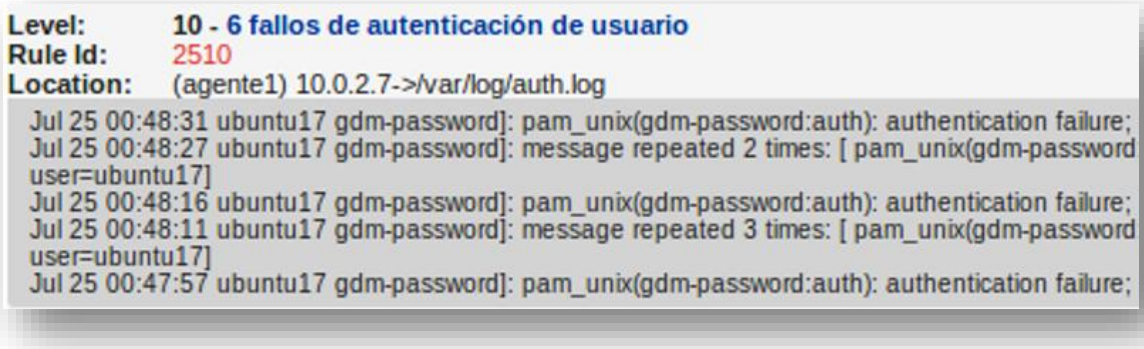


Figura 49 Alerta de detección de 6 intentos fallidos de autenticación

8.4.4 Conexión exitosa SSH no autorizada

ID Control: 04

Objetivo del control: El objetivo de este control es detectar conexiones SSH no autorizadas.

Riesgo: Este control en principio mitigaría el 94Riesgo 11 indicado en el punto 8.2.

Descripción regla en OSSEC: Se trata de una regla modificada, a partir de una ya existente en la base de datos de OSSEC, ubicada en *etc/rules/sshd_rules.xml.* Se establece el nivel de la regla en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 9 (ver niveles definidos en el apartado 7.4.1 de este trabajo) para la regla ya que se ha considera como un error generado por un origen no válido. Como condición se define que se detecte la regla ID=5700, se explicará a continuación de la regla actual. Otra condición, es la detectar si el origen es desde la IP 10.0.2.7, ya que se ha considerado que este sería un origen no autorizado y es lo que se quiere detectar. Como última condición, se busca en el *log* la cadena de caracteres "*Accepted|authenticated*", que significa aceptada la clave pública y autenticación aceptada. El símbolo "^", especifica el inicio del texto, ver punto 7.4.1.

```
<rule id="5715" level="9">
  <if_sid>5700</if_sid>
  <srcip>10.0.2.11</srcip>
  <match>^Accepted|authenticated.$</match>
  <description>SSHD authentication success.</description>
  <group>authentication_success,</group>
</rule>
```

La regla ID=5700, regla existente. Se utiliza como condición en la regla anterior. Su objetivo es detectar todas las órdenes realizadas en el agente relacionadas con el servicio "*sshd*". Se ubica en *etc/rules/sshd_rules.xml.*

```
<group name="syslog,sshd,">
  <rule id="5700" level="0" noalert="1">
  <decoded_as>sshd</decoded_as>
  <description>SSHD messages grouped.</description>
 </rule>
```

Test de intrusión: Se requiere instalar el cliente SSH en la máquina de la víctima y en el atacante.

1. Instalación:

```
sudo apt-get install openssh-server
```

2. Editar fichero de configuración. Los parámetros que se configuran son:

```
sudo gedit /etc/ssh/sshd_config
```

- Puerto: Se puede mantener el puerto por defecto, el 22, o definir otro. En este caso para el equipo *Ubuntu*17 se ha asignado el puerto 3450.
- Versión: Se define la 2.
- Ubicación de almacenamiento de las claves: *hostKey /etc/ssh/ssh_host_rsa_key.*

3. Inicio:

```
sudo /etc/init.d/ssh restart
```

Una vez instalado se realiza la conexión:

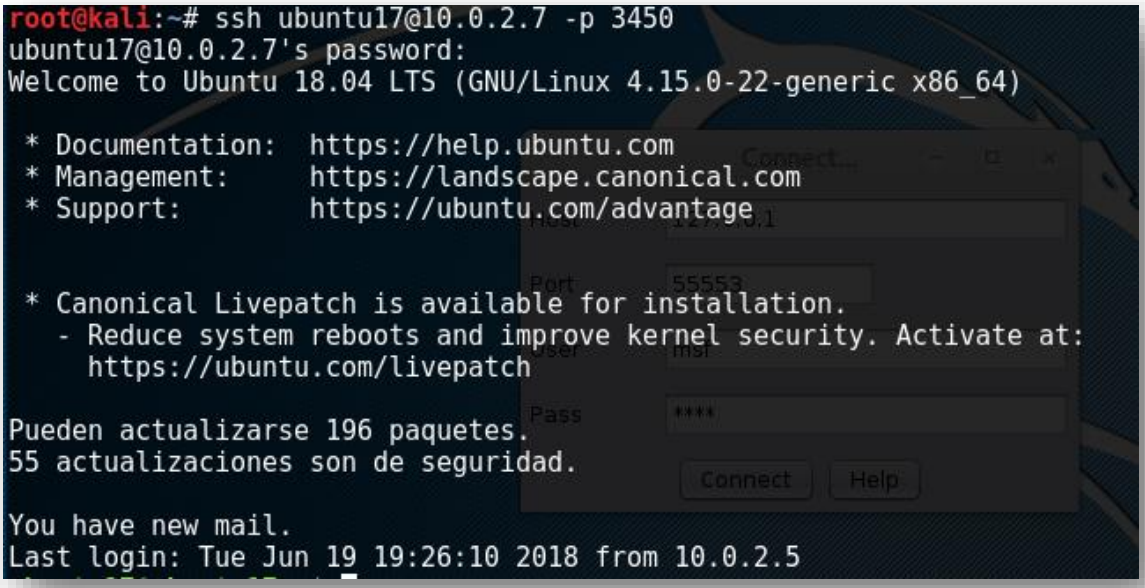


Figura 50 Conexión ssh con éxito

Hallazgos: Se adjunta una captura (Figura 51) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (3) y la descripción de la alerta (SSHD *authentication sucess*). El ID= 2575 identifica unívocamente la regla. El campo *srcip* indica el sistema que origina el evento, es el equipo kali con IP 10.0.2.11, la cual se ha considerado que no está autorizada para conectarse mediante ssh. En este caso, el campo *location es* el destino que es el agente1, maquina ubuntu17 con IP 10.0.2.7.

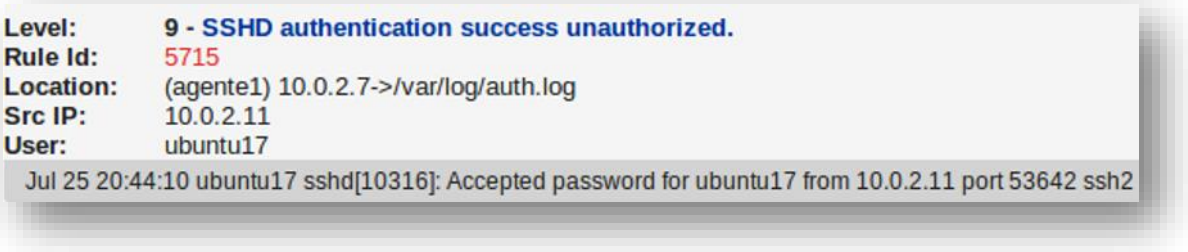


Figura 51 Evidencia de alerta de Conexión ssh con éxito no autorizada

8.4.5 Detectar intento de conexión SSH con un usuario que no existe en el sistema

ID Control: 05

Objetivo del control: El objetivo de este control es

Riesgo: Este control mitigaría el Riesgo 7 indicado en el punto 8.2.

Descripción regla en OSSEC: Se trata de una regla ya existente, ID =5710, en la base de datos de OSSEC, ubicada en *etc/rules/sshd_rules.xml.* Se establece el nivel de la regla en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 5 (ver niveles definidos en el apartado 7.4.1 de este trabajo) para la regla ya que se considera un error generado por el usuario. La primera condición, es que se detecte la alerta ID=5700, ya explicado en el punto 8.4.4. La cadena de caracteres esperada en el log será "*illegal user|invalid user*", que significa que el usuario detectado no es válido o no existe.

```
<rule id="5710" level="5">
  <if_sid>5700</if_sid>
  <match>illegal user|invalid user</match>
  <description>Attempt to login using a non-existent user</description>
  <group>invalid_login,authentication_failed,</group>
</rule>
```

Test de intrusión: Se requiere la instalación y configuración del servicio *SSH*, ya explicado en el punto 8.4.4. Cuando se intenta establecer conexión se indicará un nombre de usuario incorrecto.

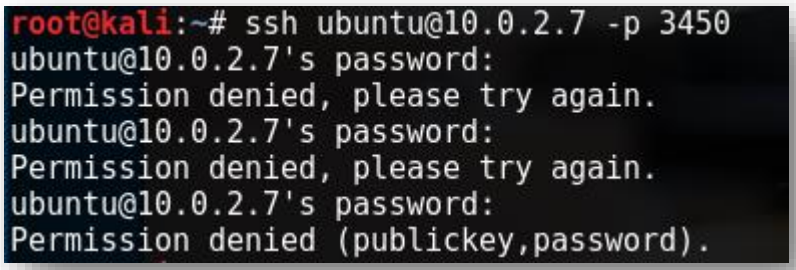


Figura 52 Evidencia intento de conexión SSH con usuario no existente en el sistema

Hallazgos: Se adjunta una captura (Figura 53) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (5) y la descripción de la alerta (*Attempt to login using a non-existent user*). El ID=5710 identifica unívocamente la regla. El campo *location* indica el sistema que origina el evento, en este caso desde el agente1 con IP 10.0.2.7.

Figura 53 Evidencia de alerta de intento de conexión con usuario no existente en el sistema

8.4.6 Intento de ataque por fuerza bruta de SSH

ID Control: 06

Objetivo del control: El objetivo de este control es detectar un ataque de fuerza bruta para obtener credenciales de acceso remoto mediante el servicio SSH.

Riesgo: Este control mitigaría el Riesgo 11 indicado en el punto 8.2.

Descripción regla en OSSEC: Se trata de una regla ya existente, ID =5712, en la base de datos de OSSEC, ubicada en *etc/rules/sshd_rules.xml.* La regla tiene un nivel 5, ya que se considera un error generado por el usuario. La primera condición, es que se detecte la alerta ID=5710, ya explicado en el punto 8.4.5. Se establece el nivel de la regla en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 10 (ver niveles definidos en el apartado 7.4.1 de este trabajo) para la regla ya que se consideran errores generados por múltiples usuarios. Los parámetros (ver 7.4.1) definidos son: "*frequency*=6" que quiere decir que la alerta se producirá cuando se detecten doce intentos de autenticación; "*timeframe=120*" es la ventana de tiempo en el que se han de realizar los intentos para que salte la alerta; "ignore=60" es el tiempo definido para ignorar la regla tras lanzarla.

```
<rule id="5712" level="10" frequency="6" timeframe="120" ignore="60">
  <if_matched_sid>5710</if_matched_sid>
  <description>SSHD brute force trying to get access to </description>
  <description>the system.</description>
  <same_source_ip />
  <group>authentication_failures,</group>
 </rule>
```

Test de intrusión: El test de intrusión será similar al del punto 8.4.4 salvo por la diferencia de introducir de forma incorrecta la contraseña. Se ha considerado que la máquina agente2 con IP 10.0.2.6, desde donde se origina el ataque, intenta acceder mediante fuerza bruta, ya que a priori desconoce la contraseña, a la maquina con IP 10.0.2.7.

Hallazgos: Se adjunta una captura (Figura 54) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (10) y la descripción de la alerta (*Attempt to login using a non-existent user*). El ID=5712 identifica unívocamente la regla. El campo *srcip* , indica el sistema que origina el evento, en este caso desde el IP 10.0.2.7 hacia donde indica el campo *location,* el agente2 con IP 10.0.2.6.

Figura 54 Alerta por ataque de fuerza bruta SSH

8.4.7 Accesos a ubicaciones lógicas determinadas críticas

ID Control: 07

Objetivo del control: El objetivo de este control es detectar accesos no autorizados a ubicaciones críticas y adición, sustracción o modificación de elementos en dichas ubicaciones sensibles.

Riesgo: Este control mitigaría el Riesgo 10 indicado en el punto 8.2.

Descripción regla en OSSEC: Se ha definido una regla nueva. Esta nueva regla se define en el fichero de reglas locales, donde normalmente se definen las nuevas reglas. La ubicación del fichero de reglas es: */var/ossec/rules/local_rules.xml.*

Se define un nuevo ID para la regla, en este caso ID=100200, debe ser un identificador libre o fallará en la compilación. Se establece el nivel de la regla en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 12 (ver niveles definidos en el apartado 7.4.1 de este trabajo) para la regla ya que se considera un evento de alta importancia que pueden indicar un ataque contra una aplicación específica. La cadena de caracteres que espera detectar es "*/home/ubuntu17/Escritorio*", se trata de la ubicación critica que se desea monitorizar.

```
<rule id="100200" level="12">
  <if_matched_group>syscheck</if_matched_group>
  <match>/home/ubuntu17/Escritorio</match>
  <description> Cambios en una ubicación critica.</description>
</rule>
```

Test de intrusión: Se ha definido una ubicación del sistema como critica. En este caso, la ubicación en el equipo ubuntu17 es */home/ubuntu17/Escritorio.* Para comprobar que el usuario ha accedido, se ha creado un fichero en la ubicación crítica.

Hallazgos: Se adjunta una captura (Figura 55) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (12) y la descripción de la alerta (*Changes to Critical directory)*. El ID=100200 identifica unívocamente la regla. El campo *location* , indica el sistema que origina el evento, en este caso desde el IP 10.0.2.7.

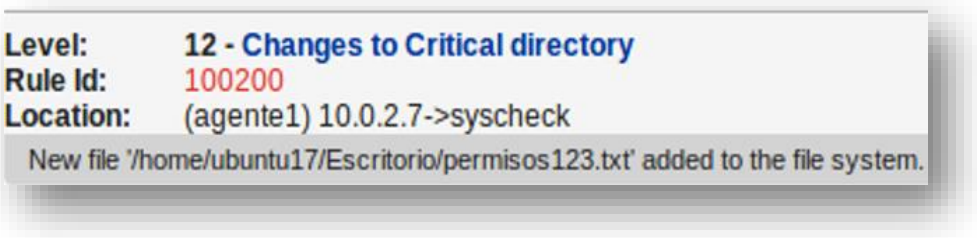


Figura 55 Alerta por acciones realizadas en ubicación crítica

8.4.8 Conexión de un USB

ID Control: 08

Objetivo del control: El objetivo de este control es detectar la conexión de cualquier dispositivo a través del puerto serie.

Riesgo: Este control mitigaría el Riesgo 5 indicado en el punto 8.2.

Se ha definido una regla nueva. Esta nueva regla se define en el fichero de reglas locales, donde normalmente se definen las nuevas reglas. La ubicación del fichero de reglas es: */var/ossec/rules/local_rules.xml.*

Se define un nuevo ID para la regla, en este caso ID=100201, debe ser un identificador libre o fallará en la compilación. Se establece el nivel de la regla, en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 13 (ver niveles definidos en el apartado 7.4.1 de este trabajo) para la regla ya que se considera un evento de alta importancia. La primera condición es que salte la regla ID=530, se incluye un poco más adelante en este mismo punto. La cadena de caracteres que espera detectar es *"|/media|usb|",* se trata de la ubicación critica que se desea monitorizar.

```
<rule id="100201" level="13">
  <if_sid>530</if_ sid >
  <match>|/media|usb|</match>
  <description> Dispositivo USB conectado </description>
</rule>
```

Test de intrusión: La prueba consisten en introducir un dispositivo USB en un puerto serie del equipo, en este caso del sistema Windows con IP 10.0.2.6.

Hallazgos: Se adjunta una captura (Figura 56) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (13) y la descripción de la alerta (*Dispositivo USB conectado).* El ID=100201 identifica unívocamente la regla. El campo *location* , indica el sistema que origina el evento, en este caso desde el agente2 con IP 10.0.2.6.

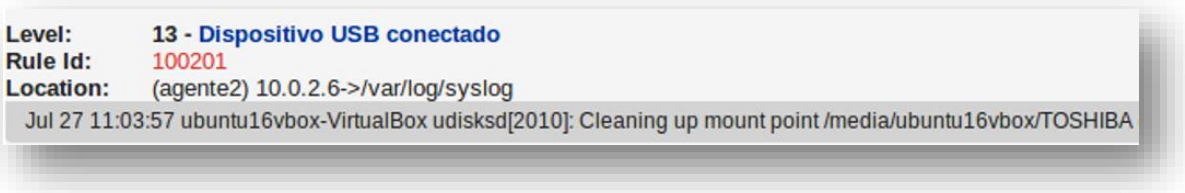


Figura 56 Alerta por conectar un dispositivo USB

8.4.9 Cambiar permisos de ficheros (permitir lectura/escritura para cualquier usuario) o detección de uso de rootkit

ID Control: 09

Objetivo del control: El objetivo de este control es detectar cualquier actividad relacionada con el uso de herramientas *rootkits* (ver nota al pie 27) o gestión sospechosa con los permisos de carpetas/ficheros.

Riesgo: Este control mitigaría el Riesgo 16 indicado en el punto 8.2.

Descripción regla en OSSEC: Se trata de una regla existente en OSSEC. Esta regla tiene como condición que se produzca previamente la regla ID=509, se explicará más adelante. Se ubica en *etc/rules/ossec_rules.xml.* Se establece el nivel de la regla, en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 7 (ver niveles definidos en el apartado 7.4.1 de este trabajo).

```
<rule id="510" level="7">
  <if_sid>509</if_sid>
  <description>Host-based anomaly detection event(rootcheck).</description>
  <group>rootcheck,</group>
  <if_fts />
</rule>
```

La regla ID=509, es una regla existente en la base de datos de reglas de OSSEC. Esta regla, alerta cuando se detecta algún evento relacionado con *rookits*. Se ubica en *etc/rules/ossec_rules.xml.*

```
<rule id="509" level="0">
  <category>ossec</category>
  <decoded_as>rootcheck</decoded_as>
  <description>Rootcheck event.</description>
  <group>rootcheck,</group>
</rule>
```

Test de intrusión: *Rootcheck*, como se indica en el punto 7.2.4, es capaz de detectar un cambio de permisos de permisos sospechoso. Para la esta prueba, a un archivo, en concreto */var/log/apache2/Access.log*, que es propiedad del *root* o usuario administrador, se le reasigna que “cualquier” usuario tiene permiso de escritura. Esto puede ser una situación de riesgo porque es posible que un atacante devalúe los permisos de un fichero para poder sustraer o modificar su contenido.

```
# sudo chmod 111 access.log
```

Hallazgos: Se adjunta una captura (Figura 57) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (7) y la descripción de la alerta (*Host-based anomaly detection event (roorcheck))*. El ID=510 identifica unívocamente la regla. El campo *location*, indica el sistema que origina el evento, en este caso desde el IP 10.0.2.6.

Figura 57 Alerta de evento de asignación de permisos de lectura/escritura a cualquier usuario

8.4.10 Habilitar/Deshabilitar puertos

ID Control: 010

Objetivo del control: El objetivo de este control es monitorizar el estado de los puertos del sistema.

Riesgo: Este control mitigaría el Riesgo 10 indicado en el punto 8.2.

Descripción regla en OSSEC: Se trata de una regla existente en OSSEC, concretamente ID=581. La condición es alertar de nueva información de los puertos del sistema. Se establece el nivel de la regla, en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 8 (ver niveles definidos en el apartado 7.4.1 de este trabajo).

```
<rule id="581" level="8">
  <category>ossec</category>
  <decoded_as>hostinfo_new</decoded_as>
  <description>Host information added.</description>
  <group>hostinfo,</group>
 </rule>
```

Test de intrusión: Se habilitan los puertos 22, 25 y 80 en la máquina del servidor, con IP 10.0.2.9. Los puertos están habilitados por los servicios que están funcionando en el sistema. En este caso, se ha instalado los servicios SSH, SMPT y HTTP, que corresponden con los puertos 22, 25 y 80, respectivamente.

Hallazgos: Se adjunta una captura (Figura 58) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (8) y la descripción de la alerta "*Host information added"*. El ID=581 identifica unívocamente la regla. El campo *location* , indica el sistema que origina el evento, en este caso en el equipo ubuntu16-servidor con IP 10.0.2.9.

Figura 58 Alerta de activación de puertos lógicos

8.4.11 Cambio en la integridad de un archivo (tamaño)

ID Control: 11

Objetivo del control: El objetivo de este control es detectar los cambios de integridad de un archivo.

Riesgo: Este control mitigaría el Riesgo 12 indicado en el punto 8.2.

Descripción regla en OSSEC: Se trata de una regla existente en OSSEC. Esta regla tiene como condición que se produzca previamente la regla ID=550, se explicará más adelante. Se ubica en */var/ossec/rules/local_rules.xml.* Se establece el nivel de la regla, en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 7 (ver niveles definidos en el apartado 7.4.1 de este trabajo).

```
<rule id="550" level="7">
  <category>ossec</category>
  <decoded_as>syscheck_integrity_changed</decoded_as>
  <description>Integrity checksum changed.</description>
  <group>syscheck,</group>
 </rule>
```

Test de intrusión: Abrir un archivo, realizar una modificación y guardar. Este control se aplicaría en ficheros que no deberían alterarse o al menos no hacerlo sin autorización, por lo que requiere de una monitorización exhaustiva.

Hallazgos: Se adjunta una captura (Figura 59) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (7) y la descripción de la alerta (*Integrity checksum changed*). El ID=550 identifica unívocamente la regla. El campo *location* , indica el sistema que origina el evento, en este caso en el equipo ubuntu16-servidor con IP 10.0.2.9.

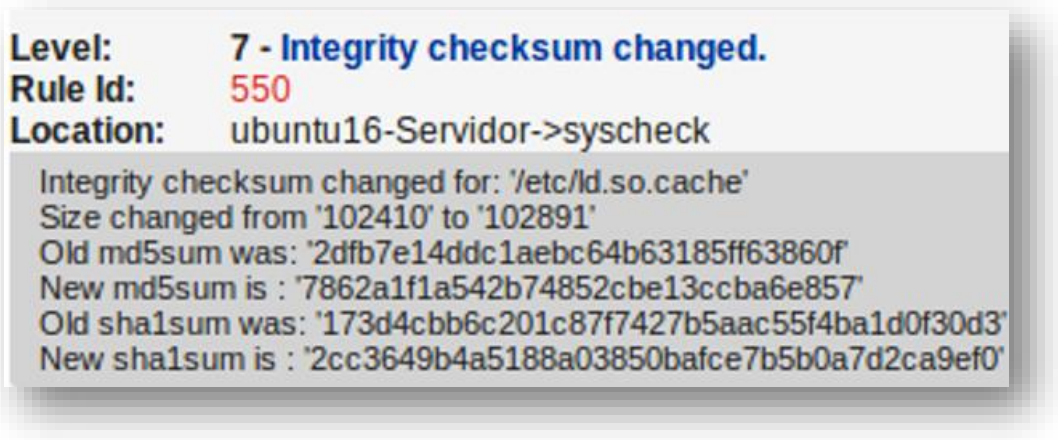


Figura 59 Alerta por modificación de la integridad de un archivo

8.4.12 Detectar la creación de nuevos grupos y usuarios

ID Control: 12

Objetivo del control: El objetivo de este control es detectar la creación de nuevos grupos y usuarios al sistema.

Riesgo: Este control mitigaría el Riesgo 17 indicado en el punto 8.2.

Descripción regla en OSSEC: Son reglas ya existentes en OSSEC, concretamente ID=5901 e ID=5902. Su funcionamiento es similar, comparan los registros de eventos con las cadenas de caracteres: "*new group*" y "*new user|new account added*"**.**

```
<rule id="5901" level="8">
  <match>^new group</match>
  <description>New group added to the system</description>
 </rule>
<rule id="5902" level="8">
  <match>^new user|^new account added</match>
  <description>New user added to the system</description>
 </rule>
```

Test de intrusión: Se crea un usuario (usuarioprueba) y añade un grupo (grupoprueba) en el sistema operativo.

```
# sudo groupadd grupoprueba
# sudo adduser usuarioprueba
```

Hallazgos: Se adjunta una captura (Figura 60 y Figura 61) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (8) y la descripción de la alerta (Integrity

checksum changed). Los ID=5901 e ID= 5902, identifican unívocamente la regla. El campo *location* , indica el sistema que origina el evento, en este caso en el equipo ubuntu16-servidor con IP 10.0.2.6.

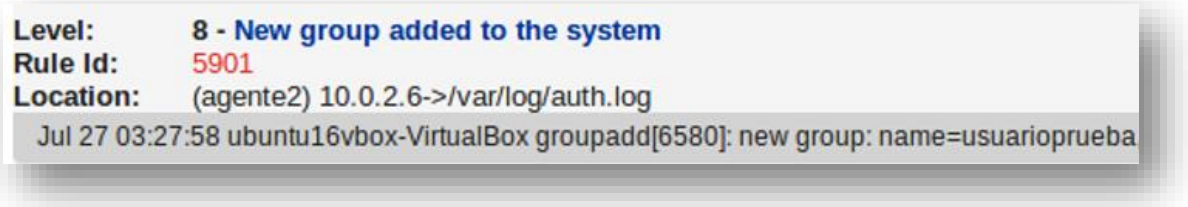


Figura 60 Alerta por creación de nuevo grupo en el sistema

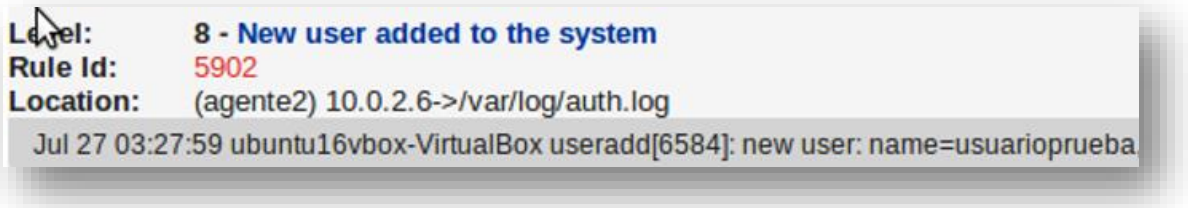


Figura 61 Alerta por creación de nuevo usuario en el sistema

8.4.13 Cambio de contraseña de usuario administrador

ID Control: 13

Objetivo del control: El objetivo de este control es detectar cambios de las contraseñas de acceso al sistema de los usuarios administradores.

Riesgo: Este control mitigaría el Riesgo 8 indicado en el punto 8.2.

Descripción regla en OSSEC: Se trata de una regla existente en OSSEC. Esta regla tiene como condición que se produzca previamente la regla ID=100050, se explicará más adelante. Se ubica en */var/ossec/rules/local_rules.xml.* La condición es que se cumpla la regla ID=5555, ya existente y que se explicará más adelante en este mismo punto. Se establece el nivel de la regla, en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 10 (ver niveles definidos en el apartado 7.4.1 de este trabajo) para la regla ya que se considera un evento que puede tener origen desde múltiples usuarios.

```
<rule id="100050" level="10">
  <if_matched_sid>5555</if_matched_sid>
  <description>Cambio de contraseña de usuario administrador </description>
</rule>
```

La regla ID=5555, es la utilizada como condición en la regla anterior. Buscar en el log la cadena de caracteres "*password changed for*", que se da cuando se realiza un cambio de contraseña.

```
<rule id="5555" level="3">
  <match>: password changed for</match>
  <description>User changed password.</description>
</rule>
```

Test de intrusión: Se crea un usuario (usuarioprueba) en el sistema y se añade al grupo de administrador. Este es el mismo grupo que el del *root*.

```
# sudo adduser -u 0 -o -g 0 usuarioprueba
```

Hallazgos: Se adjunta una captura (Figura 62) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (10) y la descripción de la alerta (Cambio de contraseña de usuario administrador). El ID=100050 identifica unívocamente la regla. El campo *location* , indica el sistema que origina el evento, en este caso en el equipo ubuntu16-servidor con IP 10.0.2.6.

Figura 62 Alerta por cambio de contraseña de usuario administrador

8.4.14 Nuevo usuario o grupo añadido al sistema

ID Control: 14

Objetivo del control: El objetivo de este control es detectar la creación de nuevos usuarios o grupos en el sistema.

Riesgo: Este control mitigaría el Riesgo 17 indicado en el punto 8.2.

Descripción regla en OSSEC: Son reglas ya existentes en OSSEC, concretamente ID=5901 e ID=5902. Su funcionamiento es similar, comparan los registros de eventos con las cadenas de caracteres: "*new group*" y "*new user|new account added*"**.** Se establece el nivel de la regla, en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 8 (ver niveles definidos en el apartado 7.4.1 de este trabajo).

```
<rule id="5901" level="8">
  <match>^new group</match>
```

```
  <description>New group added to the system</description>
 </rule>
<rule id="5902" level="8">
  <match>^new user|^new account added</match>
  <description>New user added to the system</description>
 </rule>
```

Test de intrusión: Se crea un usuario (usuarioprueba) y añade un grupo (grupoprueba) en el sistema operativo.

```
# sudo groupadd grupoprueba
# sudo adduser usuarioprueba
```

Hallazgos: Se adjunta una captura (Figura 60 y Figura 61) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (8) y la descripción de la alerta (Integrity checksum changed). Los ID=5901 e ID= 5902, identifican unívocamente la regla. El campo *location* , indica el sistema que origina el evento, en este caso en el equipo ubuntu16-servidor con IP 10.0.2.6.

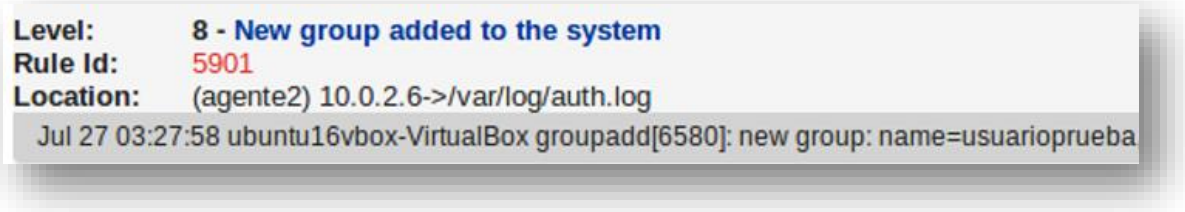


Figura 63 Alerta por creación de nuevo grupo en el sistema

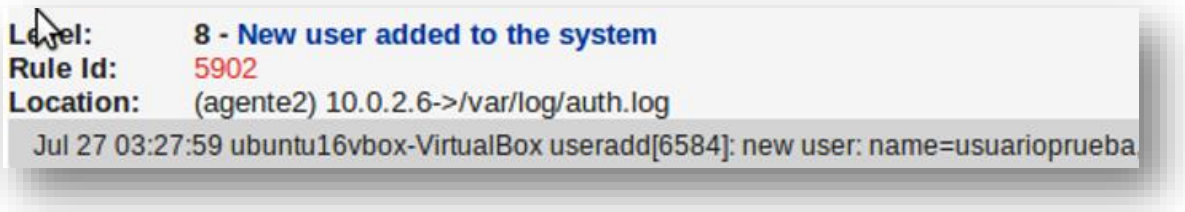


Figura 64 Alerta por creación de nuevo usuario en el sistema

8.4.15 Ataque de fuerza bruta a Wordpress

ID Control: 15

Objetivo del control: El objetivo de este control es detectar intentos de accesos ilícitos a un usuario *Wordpress* mediante ataque de fuerza bruta.

Riesgo: Este control mitigaría el Riesgo 6 indicado en el punto 8.2.

Descripción regla en OSSEC: Se trata de una regla existente en OSSEC. Esta regla tiene como condición que se produzca previamente la regla ID=31510, se incluye más adelante. Se ubica en */var/ossec/rules/local_rules.xml.* La condición es que se cumpla la regla ID=31509, ya existente y que se explicará más adelante en este mismo punto. Se establece el nivel de la regla, en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 8 (ver niveles definidos en el apartado 7.4.1 de este trabajo).

```
<rule id="31510" level="8" frequency="6" timeframe="30">
  <if_matched_sid>31509</if_matched_sid>
  <same_source_ip />
  <description>CMS (WordPress or Joomla) brute force attempt.</description>
</rule>
```

La regla ID=31509, es una regla existente en OSSEC. Alerta cuando un usuario se ha autenticado en *Wordpress*. Se ubica en */var/ossec/rules/local_rules.xml*

```
<rule id="31509" level="3">
  <if_sid>31108</if_sid>
  <url>wp-login.php|/administrator</url>
  <regex>] "POST \S+wp-login.php| "POST /administrator</regex>
  <description>CMS (WordPress or Joomla) login attempt.</description>
</rule>
```

Test de intrusión: Para realizar esta prueba previamente se requiere instalar un servidor web. Para ello, se ha instalado *Wordpress* [226], en la referencia anterior se explica todo el proceso de instalación.

Desde el equipo ubuntu17 con IP 10.0.2.7 se realiza la autenticación, introduciendo una contraseña errónea a través del navegador al agente2 con IP 10.0.2.6, donde se encuentra ubicado *Wordpress.*

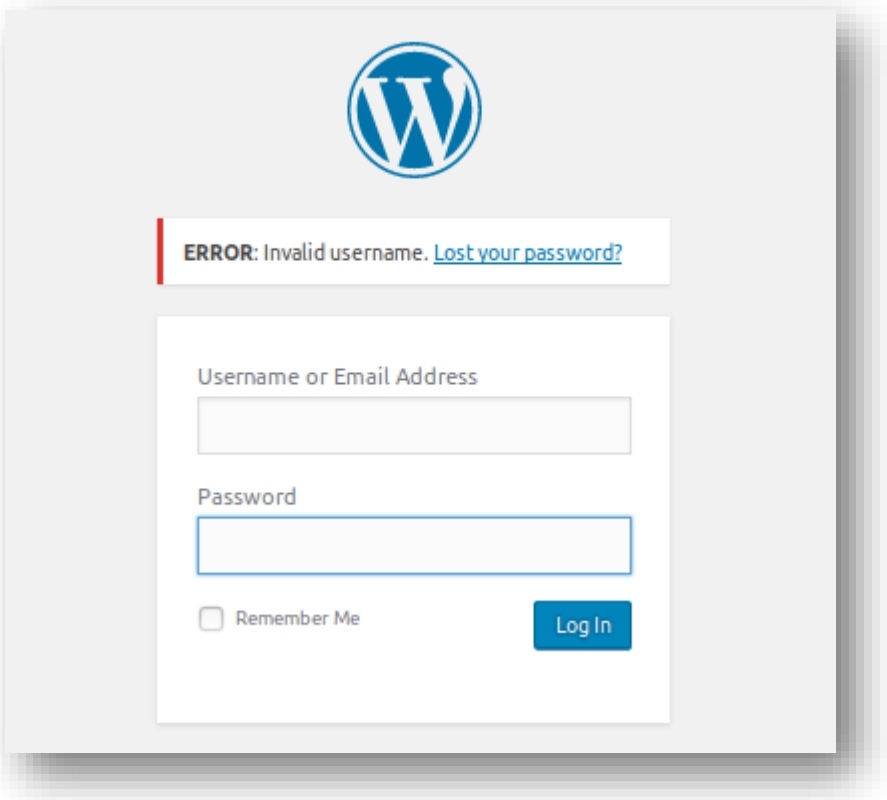


Figura 65 Página de autenticación de usuario de Wordpress

Hallazgos: Se adjunta una captura (Figura 66) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (8) y la descripción de la alerta (C*MS (Wordpress or Joomla) brute forcé attempt*). El ID=31510 identifica unívocamente la regla. El campo *location*, indica el sistema que recibe el ataque, en este caso en el equipo *ubuntu16*-servidor con IP 10.0.2.6. El ataque se origina en el equipo con IP 10.0.2.9, como se indica en el campo *Src IP*

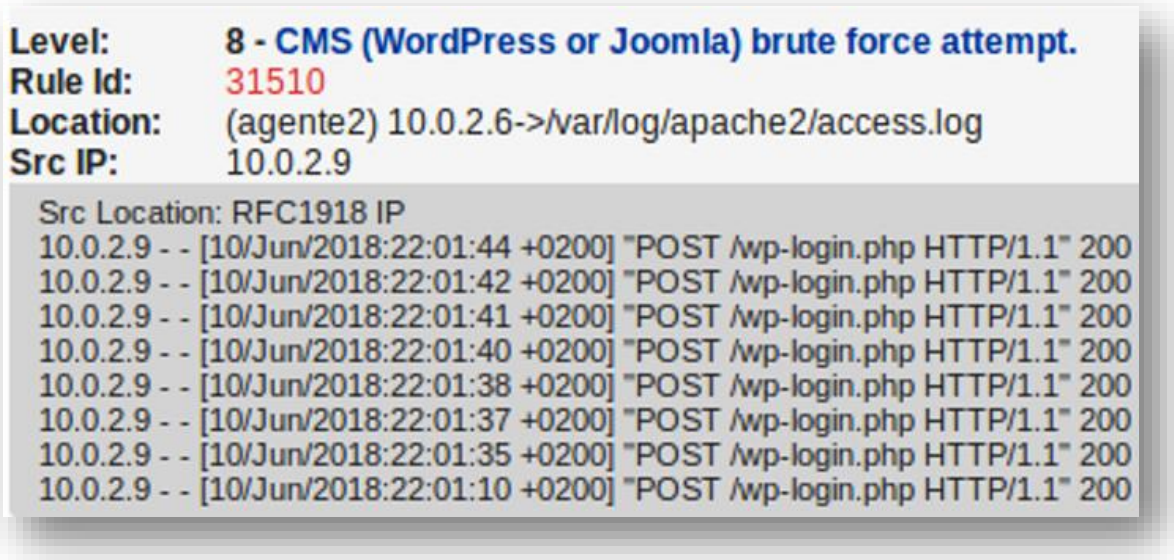


Figura 66 Alerta de ataque de fuerza bruta a Wordpress

8.4.16 Intento de ataque de inyección de código SQL

ID Control: 16

Objetivo del control: El objetivo de este control es detectar un ataque de inyección de código SQL.

Riesgo: Este control mitigaría el Riesgo 13 indicado en el punto 8.2.

Descripción regla en OSSEC: Se trata de una regla existente en la base de datos de OSSEC. La regla se localiza en la ubicación *etc/rules/web_rules.xml*. La primera condición es que se cumpla la regla con ID=31100. La siguiente condición, es que en la *url* se detecte alguno de los siguientes comandos propios del código SQL. Se establece el nivel de la regla, en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 6 (ver niveles definidos en el apartado 7.4.1 de este trabajo).

```
<rule id="31164" level="6">
  <if_sid>31100</if_sid>
  <url>=%27|select%2B|insert%2B|%2Bfrom%2B|%2Bwhere%2B|%2Bunion%2B</url>
  <description>SQL injection attempt.</description>
  <group>attack,sqlinjection,</group>
</rule>
```

La regla ID=31100, se utiliza como condición en la regla anterior. Esta regla es existente en la base de datos de OSSEC, y detecta los eventos Web. La regla se localiza en la ubicación *etc/rules/web_rules.xml*.

```
<rule id="31100" level="0">
  <category>web-log</category>
  <description>Access log messages grouped.</description>
</rule>
```

Test de intrusión: Es necesario un cuadro de texto de la página que haga uso de una base de datos. Por ejemplo, el buscador de la página suele ser víctima habitual de este tipo de ataques. Se inyecta el código SQL “or 1’=1”, su función es completar la sentencia de la petición SQL programada en la *web*, añadiéndole la condición 1=1. En el caso que esta se cumpla, que será siempre ya que 1=1 siempre se cumple, devolverá todos los datos que la petición SQL solicita.

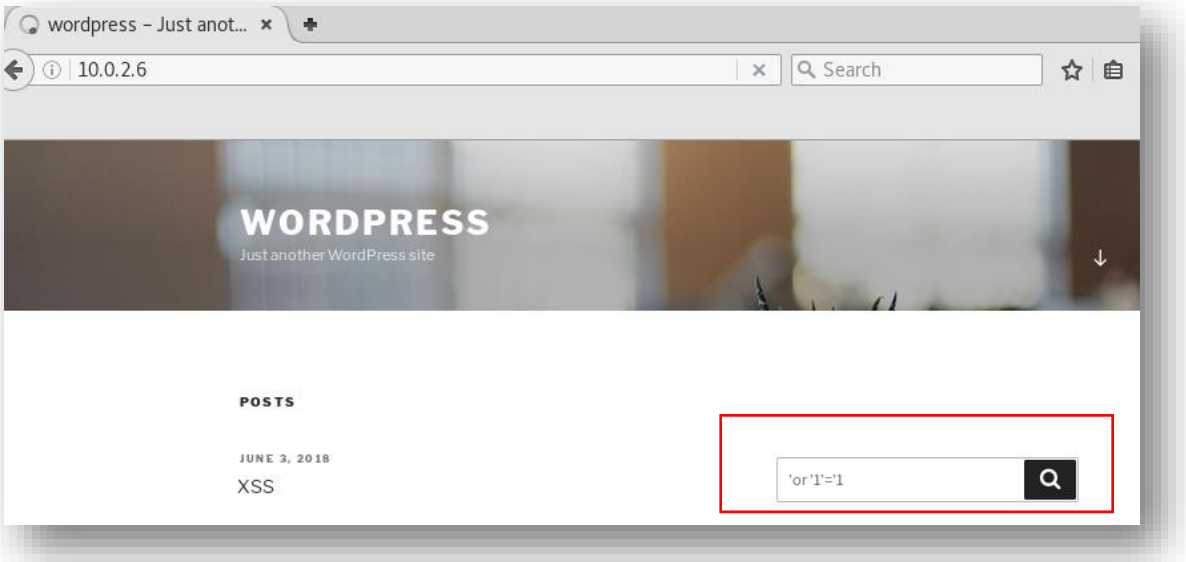


Figura 67 Ataque inyección SQL en el cuadro de buscador de Wordpress

Hallazgos: Se adjunta una captura (Figura 68) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (6) y la descripción de la alerta (SQL *injection attempt*). El ID=31164 identifica unívocamente la regla. El campo *location,* indica el sistema que recibe el ataque, en este caso en el equipo ubuntu16-servidor con IP 10.0.2.6. El ataque se origina en el equipo con IP 10.0.2.7, como se indica en el campo *Src IP*.

Figura 68 Alerta intento de ataque de inyección SQL

8.4.17 Intento de ataque Web (XSS)

ID Control: 17

Objetivo del control: El objetivo de este control es

Riesgo: Este control mitigaría el Riesgo 15 indicado en el punto 8.2.

Descripción regla en OSSEC: Se trata de una regla existente en la base de datos de OSSEC. La regla se localiza en la ubicación *etc/rules/web_rules.xml*. Esta regla tiene como condición que se ejecuten previamente las reglas 31103, 31104, 31105, se incluyen más adelante. Se establece el nivel de la regla, en función de la criticidad del riesgo y las necesidades de la empresa, en este caso se ha definido un nivel 6 (ver

niveles definidos en el apartado 7.4.1 de este trabajo) para la regla ya que se considera un evento que puede tener origen desde múltiples usuarios.

```
<rule id="31106" level="6">
  <if_sid>31103, 31104, 31105</if_sid>
  <id>^200</id>
  <description>A web attack returned code 200 (success).</description>
  <group>attack,</group>
 </rule>
```

Las reglas 31103, 31104,31105 son reglas existentes en OSSEC. Alertan respectivamente, cuando se detectan en la *url* algún comando propio del código SQL, cuando se detecta algún acceso o modificación de algún fichero típico en la configuración de servidores *web* o en el caso detectar el uso de código *javascript*. Se ubica en */var/ossec/rules/local_rules.xml*

```
<rule id="31103" level="6">
  <if_sid>31100,31108</if_sid>
  <url>=select%20|select+|insert%20|%20from%20|%20where%20|union%20|</url>
  <url>union+|where+|null,null|xp_cmdshell</url>
  <description>SQL injection attempt.</description>
  <group>attack,sql_injection,</group>
</rule>

<rule id="31104" level="6">
  <if_sid>31100</if_sid>
  <!-- Attempt to do directory transversal, simple sql injections,
  -  or access to the etc or bin directory (unix). -->
  <url>%027|%00|%01|%7f|%2E%2E|%0A|%0D|../..|..\..|echo;|</url>
  <url>cmd.exe|root.exe|_mem_bin|msadc|/winnt/|/boot.ini|</url>
  <url>/x90/|default.ida|/sumthin|nsiislog.dll|chmod%|wget%|cd%20|</url>
  <url>exec%20|../..//|%5C../%5C|././././|2e%2e%5c%2e|\x5C\x5C</url>
  <description>Common web attack.</description>
  <group>attack,</group>
</rule>
<rule id="31105" level="6">
```

```
  <if_sid>31100</if_sid>
  <url>%3Cscript|%3C%2Fscript|script>|script%3E|SRC=javascript|IMG%20|</url>
  <url>%20ONLOAD=|INPUT%20|iframe%20</url>
  <description>XSS (Cross Site Scripting) attempt.</description>
  <group>attack,</group>
</rule>
<rule id="31110" level="6">
  <if_sid>31100</if_sid>
  <url>?-d|?-s|?-a|?-b|?-w</url>
  <description>PHP CGI-bin vulnerability attempt.</description>
  <group>attack,</group>
</rule>
```

Test de intrusión: Para realizar este ataque, se busca un cuadro de texto, por ejemplo, el campo de comentarios, y se introduce el código "*<script>alert(XSS)</script>.*

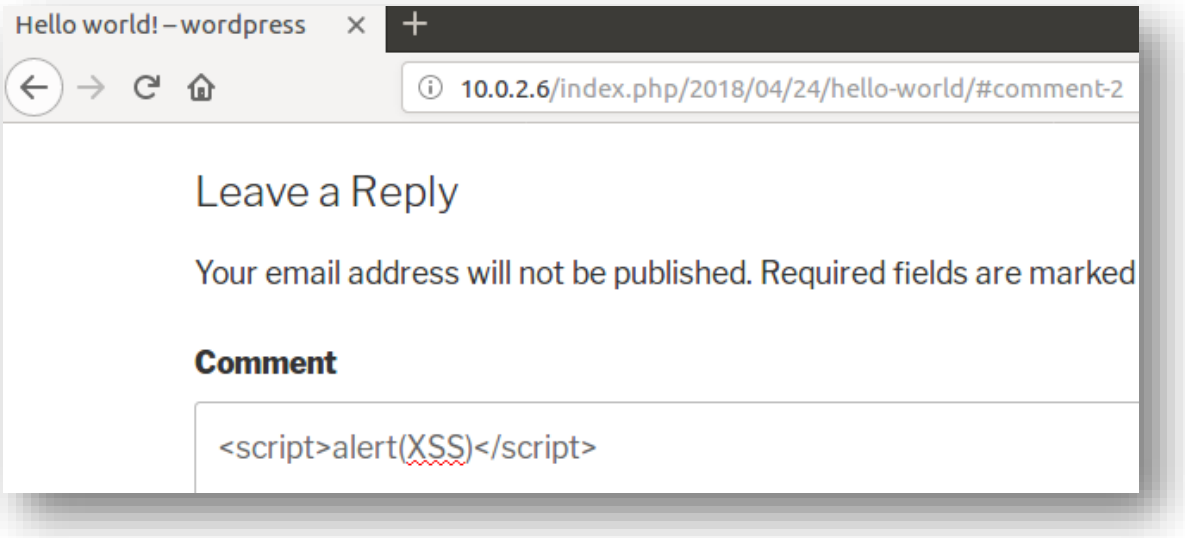


Figura 69 Ataque XSS en cuadro de texto de Wordpress

Nota: En el caso que apareciera un cuadro de alerta con el texto "XSS", significaría que este sitio web es vulnerable a ataques XSS.

Hallazgos: Se adjunta una captura (Figura 70) de la interfaz OSSEC-UI con la alerta recibida. El nivel de la alerta (6) y la descripción de la alerta (*A web attack returned code 200 (success)*). El ID=31106 identifica unívocamente la regla. El campo *location,* indica el sistema que recibe el ataque, en este caso en el equipo ubuntu16-servidor con IP 10.0.2.6. El ataque se origina en el equipo con IP 10.0.2.9, como se indica en el campo *Src IP*.

Figura 70 Alerta ataque XSS

9 ESTUDIO ECONÓMICO

Descripción	Horas.	Coste/Hora	Total
Documentación	120	35,00 €	4.200,00 €
Instalación y preparación del entorno de pruebas	10	30,00 €	300,00 €
Instalación y configuración de OSSEC	30	30,00 €	900,00 €
Realización de las pruebas	140	40,00 €	5.600,00 €
Total	300	**Base imponible**	11.000,00 €
		IVA (21 %)	2.310,00 €
		TOTAL	13.310,00 €

El total del importe por la realización del presente Trabajo Fin de Grado asciende a la cantidad de **trece mil trescientos diez euros** (**13.310,00 €**).

10 CONCLUSIONES Y LINEAS DE FUTURO

La seguridad no solamente se alcanza comprando o instalando un software, como un antivirus o equipos de seguridad, como un cortafuegos, es algo que va más allá, es un trabajo continuo de diseño, implantación y mantenimiento de medidas para controlar que la interacción entre las personas y los sistemas sea de forma responsable y adecuada, para salvaguardar la información sensible, pero sin perjudicar el funcionamiento normal de los sistemas. Por ejemplo, se puede invertir una gran cantidad de dinero en un cortafuegos y en contratar un ingeniero que lo administre y diseñe reglas robustas de control de acceso, sin embargo, para acceder a los sistemas no se ha implementado ninguna contraseña de acceso o la que ha se ha definido es débil. Esta es una situación, en la que se está asegurando limitar la entrada intrusos externos a la red, pero cualquier usuario que tenga acceso desde dentro a los sistemas podría autenticarse como administrador, sin mucha dificultad, y producir daños irreparables.

En cuanto a la comparativa entre sistemas operativos, tras evaluar los parámetros estadísticos la información de las distintas fuentes se puede concluir que, a priori, en los sistemas *Windows* se han identificado mayor número de vulnerabilidades y también es el principal objetivo de los atacantes. Según los datos estadísticos[89] de la Figura 9 del punto 3.3, de los cuales se obtiene el gráfico de la Figura 71 agrupando los productos de cada proveedor, en este caso *Windows* y *Linux*:

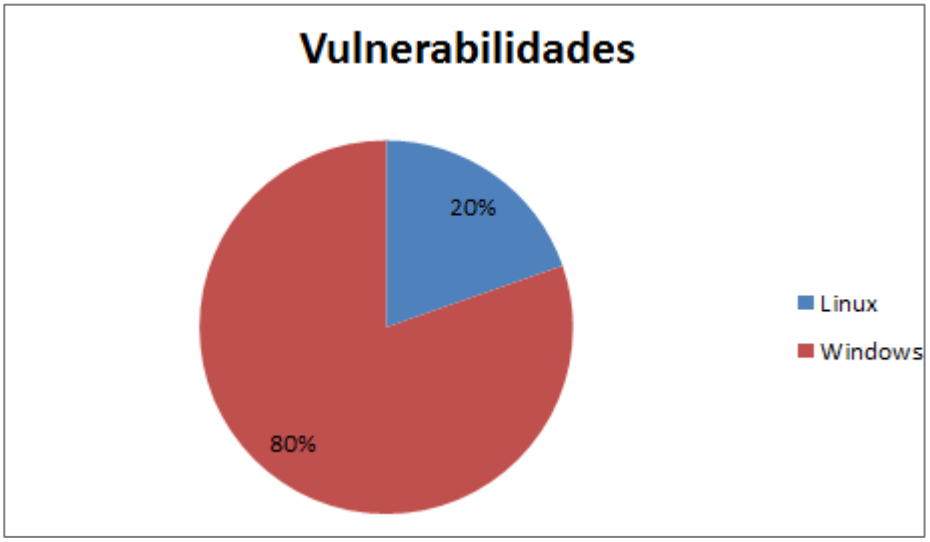


Figura 71 Reparto de vulnerabilidades por sistema operativo

Como se puede observar, el número de vulnerabilidades es cuatro veces mayor en *Linux* que en *Windows*. Se podría argumentar que una de las razones de podría ser que la cuota de mercado de *Linux* es de un 2,24% frente al 88.4 % de *Windows*, según

[89] El origen de los datos viene de la referencia [41].

netmarketshare [227] ya que un objetivo de los hackers podría asumirse como el de hacer daño donde el alcance sea mayor. Pero esto, desde otro punto de vista, no sería exactamente así, ya que *Linux* suele ser el elegido para ubicar servidores web, por ejemplo, *Apache* [228], y su cuota de mercado es mayor que la de *Microsoft ISS* [229], según *w3techs* [230] Apache está en torno al 46% de uso frente al 9,6% de *Microsoft ISS*. Por lo tanto, se puede deducir que, independientemente del sistema operativo que se utilice, la clave para mantener un nivel de seguridad óptimo es estar al tanto de las vulnerabilidades que se detectan, aplicar en la mayor brevedad de tiempo las actualizaciones que se recomiendan y gestionar que los usuarios realicen un uso responsable de los sistemas. Los especialistas suelen concluir que *Linux* es el más seguro y se llega a esto porque al ser de código abierto, está en continua revisión por colaboradores y desarrolladores especialistas alrededor del mundo.

Desde un punto de visto a alto nivel, la implementación de la herramienta OSSEC en este Trabajo Fin de Grado se podría considerar en sí misma dentro de una auditoria como un control compensatorio. Este tipo de controles se suelen implantar en las empresas para mitigar un riesgo que no se puede cubrir según los requisitos establecidos. Por ejemplo, se puede dar el caso en el que se detecte que no se ha aplicado una adecuada segregación de funciones en una empresa y se han otorgado permisos de administrador a un trabajador al que no le corresponden. Esta situación elevaría la probabilidad del riesgo de que este trabajador pudiera realizar cualquier actividad ilícita a su antojo. Se podría mitigar implementando un control que monitorice las actividades realizadas por el usuario. Si tras la auditoria se descubre que no ha realizado ninguna actividad ilícita, la probabilidad de riesgo se reduciría. Otro ejemplo, requisitos mínimos [205] de construcción de contraseñas no es el adecuado, ya sea por un tamaño inferior al recomendado o por uso de contraseñas poco robustas. En este caso, la herramienta de monitorización detectaría cualquier acceso ilícito. Para implantar este tipo de controles se recurre a herramientas similares a la propuesta en el proyecto, se aportan algunas referencias en el punto 2, que facilitan enormemente el trabajo de aseguramiento de los sistemas, además de ahorrar tiempo y rebajar costes, debido a la reducción de personal y disminución en probabilidad de fallo en los sistemas.

Como se puede observar en las figuras del punto 4, la cantidad de ataques han ido aumentando con el paso del tiempo y los atacantes, son tantos, que se podría decir que nunca duermen por lo que las amenazas a los sistemas informáticos están siempre latentes. El papel de un administrador de sistemas o un responsable de seguridad, nunca cesa y el alcance de un sistema operativo puede ser de dimensiones inabarcables, por lo que, para considerar un nivel de seguridad óptimo, sería básico

hacer un análisis de riesgos, identificación y valoración de activos y una adecuada gestión de costes de implementación de seguridad.

Así pues, con todo lo anterior mente expuesto se considera que se han cumplido con los objetivos establecidos para el presente trabajo fin de grado, los cuales son:

1. Realizar un estudio sobre las amenazas y brechas de seguridad más importantes en la actualidad en los sistemas Linux y Windows.
2. Realizar un estudio de las soluciones de seguridad más importantes a la intrusión de sistemas.
3. Desplegar y documentar el sistema OSSEC tanto para sistemas Linux como Windows. Opcional: comprobar la viabilidad de su integración en los laboratorios docentes.
4. Probar la eficacia de la protección que ofrece OSSEC a través de un banco de pruebas comparativo de sistemas Linux y Windows.
5. Implementar un portal de seguimiento personalizado de los sistemas monitorizados con OSSEC dado que esta información debe llegar a personal sin conocimientos técnicos avanzados.

Como propuesta, las nuevas líneas de trabajo en las que podría seguir desarrollándose este proyecto, podrían ser las siguientes:

- Completar la comparativa con otro tipo de sistemas operativos. Por ejemplo, los sistemas operativos *macOS*.
- Extender la monitorización de dispositivos móviles o a otros elementos de red como cortafuegos.
- Comparativa con otros sistemas operativos basados en *Linux*, como *Android*.
- Revisar el análisis de riesgos e identificar nuevos.
- Diseñar e implementar nuevos controles en base a un nuevo análisis de riesgos.

11 ANEXO 1 - FICHEROS DE CONFIGURACIÓN

11.1 Fichero de configuración de gestor OSSEC: OSSEC.conf

A continuación, se adjunta el fichero de configuración completo del gestor OSSEC. El fichero se ubica en /*var*/*ossec*/etc/*ossec*.conf. Se divide por partes para explicar que contiene cada una.

Configuración de alerta por correo:

```
<!-- OSSEC example config -->
<OSSEC_config>
 <global>
 <email_notification>yes</email_notification>
 <email_to>buzonalertatfg@gmail.com</email_to>
 <smtp_Server >127.0.0.1</smtp_Server >
 <email_from>buzonalertatfg@gmail.com</email_from>
<!-- OSSECm@localhost -->
 </global>
```

Configuración de la base de datos de OSSEC:

```
<database_output>
 <hostname>localhost</hostname>
 <username>root</username>
 <password>pass</password>
 <database>OSSEC</database>
 <type>mysql</type>
</database_output>
```

Configuración de *syscheck* para la monitorización de la integridad de los ficheros:

```
 <syscheck>
 <!-- Frequency that syscheck is executed -- default every 20 hours --
>
 <frequency>300</frequency>
 <alert_new_files>yes</alert_new_files>
 <scan_on_start>yes</scan_on_start>
<auto_ignore>no</auto_ignore>
 <!-- Directories to check (perform all possible verifications) -->
 <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
```

```
 <directories check_all="yes">/bin,/sbin,/boot</directories>
 <directories check_all="yes">/var/www/HTML</directories>
 <directories report_changes="yes" realtime="yes"
check_all="yes">/etc/p</directories>

 <!-- Files/directories to ignore -->
 <ignore>/etc/mtab</ignore>
 <ignore>/etc/hosts.deny</ignore>
 <ignore>/etc/mail/statistics</ignore>
 <ignore>/etc/random-seed</ignore>
 <ignore>/etc/adjtime</ignore>
 <ignore>/etc/HTTPd/logs</ignore>

 <!-- Check the file, but never compute the diff -->
 <nodiff>/etc/ssl/private.key</nodiff>
 </syscheck>
```

Definir fichero que contienen las bases de datos de *rootkit*s para su detección:

```
 <rootcheck>

<rootkit_files>/var/OSSEC/etc/shared/rootkit_files.txt</rootkit_files>
<rootkit_trojans>/var/OSSEC/etc/shared/rootkit_trojans.txt</rootkit_tr
ojans>
 </rootcheck>
```

Configuración de las alertas. Nivel mínimo de la alerta para ser almacenada en el log de alertas, el nivel mínimo para alertar por correo:

```
 <alerts>
 <log_alert_level>1</log_alert_level>
 <email_alert_level>5</email_alert_level>
</alerts>
```

Configuración de las respuestas activas definidas por defecto en OSSEC:

```
 <command>
 <name>host-deny</name>
 <executable>host-deny.sh</executable>
```

```
<expect>srcip</expect>
<timeout_allowed>yes</timeout_allowed>
</command>

<command>
<name>firewall-drop</name>
<executable>firewall-drop.sh</executable>
<expect>srcip</expect>
<timeout_allowed>yes</timeout_allowed>
</command>

<command>
<name>disable-account</name>
<executable>disable-account.sh</executable>
<expect>user</expect>
<timeout_allowed>yes</timeout_allowed>
</command>



<!-- Active Response Config -->
<active-response>
<!-- This response is going to execute the host-deny
- command for every event that fires a rule with
- level (severity) >= 6.
- The IP is going to be blocked for 600 seconds.
-->
<command>host-deny</command>
<location>local</location>
<level>6</level>
<timeout>600</timeout>
</active-response>

<active-response>
<!-- Firewall Drop response. Block the IP for
```

```
- 600 seconds on the firewall (iptables,
- ipfilter, etc).
-->
<command>firewall-drop</command>
<location>local</location>
<level>6</level>
<timeout>600</timeout>
</active-response>
```

Ficheros que contienen los *logs* que se van a procesar para revisar los eventos:

```
<!-- Files to monitor (localfiles) -->

<localfile>
<log_format>syslog</log_format>
<location>/var/log/messages</location>
</localfile>
<localfile>
<log_format>nmapg</log_format>
<location>/var/log/nmap-out.log</location>
</localfile>

<localfile>
<log_format>syslog</log_format>
<location>/var/log/authlog</location>
</localfile>

<localfile>
<log_format>syslog</log_format>
<location>/var/log/secure</location>
</localfile>

<localfile>
<log_format>syslog</log_format>
<location>/var/log/xferlog</location>
```

```
 </localfile>


 <localfile>
 <log_format>syslog</log_format>
 <location>/var/log/maillog</location>
 </localfile>


 <localfile>
 <log_format>apache</log_format>
 <location>/var/www/logs/access_log</location>
 </localfile>


 <localfile>
 <log_format>apache</log_format>
 <location>/var/www/logs/error_log</location>
 </localfile>


 <localfile>
 <log_format>syslog</log_format>
 <location>/var/log/wordpress</location>
 </localfile>


</OSSEC_config>
```

Ficheros con las reglas:

```
<OSSEC_config> <!-- rules global entry -->
 <rules>
 <include>rules_config.xml</include>
 <include>pam_rules.xml</include>
 <include>sshd_rules.xml</include>
 <include>telnetd_rules.xml</include>
 <include>syslog_rules.xml</include>
 <include>arpwatch_rules.xml</include>
 <include>symantec-av_rules.xml</include>
```

```
<include>symantec-ws_rules.xml</include>
<include>pix_rules.xml</include>
<include>named_rules.xml</include>
<include>smbd_rules.xml</include>
<include>vsftpd_rules.xml</include>
<include>pure-ftpd_rules.xml</include>
<include>proftpd_rules.xml</include>
<include>ms_ftpd_rules.xml</include>
<include>ftpd_rules.xml</include>
<include>hordeimp_rules.xml</include>
<include>roundcube_rules.xml</include>
<include>wordpress_rules.xml</include>
<include>cim Server _rules.xml</include>
<include>vpopmail_rules.xml</include>
<include>vmpop3d_rules.xml</include>
<include>courier_rules.xml</include>
<include>web_rules.xml</include>
<include>web_appsec_rules.xml</include>
<include>apache_rules.xml</include>
<include>nginx_rules.xml</include>
<include>php_rules.xml</include>
<include>mysql_rules.xml</include>
<include>postgresql_rules.xml</include>
<include>ids_rules.xml</include>
<include>squid_rules.xml</include>
<include>firewall_rules.xml</include>
<include>apparmor_rules.xml</include>
<include>cisco-ios_rules.xml</include>
<include>netscreenfw_rules.xml</include>
<include>sonicwall_rules.xml</include>
<include>postfix_rules.xml</include>
<include>sendmail_rules.xml</include>
<include>imapd_rules.xml</include>
<include>mailscanner_rules.xml</include>
```

```
 <include>dovecot_rules.xml</include>
 <include>ms-exchange_rules.xml</include>
 <include>racoon_rules.xml</include>
 <include>vpn_concentrator_rules.xml</include>
 <include>spamd_rules.xml</include>
 <include>msauth_rules.xml</include>
 <include>McAfee_av_rules.xml</include>
 <include>trend-osce_rules.xml</include>
 <include>ms-se_rules.xml</include>
 <!-- <include>policy_rules.xml</include> -->
 <include>zeus_rules.xml</include>
 <include>solaris_bsm_rules.xml</include>
 <include>vmware_rules.xml</include>
 <include>ms_dhcp_rules.xml</include>
 <include>asterisk_rules.xml</include>
 <include>OSSEC_rules.xml</include>
 <include>attack_rules.xml</include>
 <include>openbsd_rules.xml</include>
 <include>clam_av_rules.xml</include>
 <include>dropbear_rules.xml</include>
 <include>sysmon_rules.xml</include>
 <include>opensmtpd_rules.xml</include>
 <include>exim_rules.xml</include>
 <include>local_rules.xml</include>
 <include>unbound_rules.xml</include>
</rules>
</OSSEC_config> <!-- rules global entry -->
```

11.2 Fichero de configuración de los agentes OSSEC: agent.conf

Se adjunta el resultado final del fichero de configuración del agente OSSEC. El fichero se ubica en /var/OSSEC/etc/shared/agent.conf.

A continuación, Configuración de *syschek* para comprobar la integridad de los archivos. Se determina la frecuencia de ejecución del proceso, habilitar el escáner de integridad y alerta de nuevos ficheros y las ubicaciones que comprobar y las que ignorar (falsos positivos):

```
<agent_config os="Linux">
 <syscheck>
 <!-- Frequency that syscheck is executed - default to every 22 hours
-->
 <frequency>300</frequency>
 <scan_on_start>yes</scan_on_start>
 <alert_new_files>yes</alert_new_files>
 <skip_nfs>yes</skip_nfs>

 <!-- Directories to check (perform all possible verifications) -->
 <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
 <directories report_changes="yes" realtime="yes"
check_all="yes">/home/ubuntu17/Escritorio</directories>
 <directories check_all="yes">/bin,/sbin,/boot</directories>

 <!-- Files/directories to ignore -->
 <ignore>/etc/mtab</ignore>
 <ignore>/etc/mnttab</ignore>
 <ignore>/etc/hosts.deny</ignore>
 <ignore>/etc/mail/statistics</ignore>
 <ignore>/etc/random-seed</ignore>
 <ignore>/etc/adjtime</ignore>
 <ignore>/etc/HTTPd/logs</ignore>
 <ignore>/etc/utmpx</ignore>
 <ignore>/etc/wtmpx</ignore>
 <ignore>/etc/cups/certs</ignore>
 <ignore>/etc/dumpdates</ignore>
 <ignore>/etc/svc/volatile</ignore>

 </syscheck>
```

Fichero que contienen los *logs*:

```
 <!-- Files to monitor (localfiles) -->
 <localfile>
 <log_format>syslog</log_format>
```

```
 <location>/var/log/messages</location>
 </localfile>

 <localfile>
 <log_format>syslog</log_format>
 <location>/var/log/auth.log</location>
 </localfile>

 <localfile>
 <log_format>syslog</log_format>
 <location>/var/log/syslog</location>
 </localfile>

 <localfile>
 <log_format>command</log_format>
 <command>df -P</command>
 <frequency>360</frequency>
 </localfile>

 <localfile>
 <log_format>full_command</log_format>
 <command>netstat -tan |grep LISTEN |grep -v 127.0.0.1 |
sort</command>
 <frequency>360</frequency>
 </localfile>

 <localfile>
 <log_format>full_command</log_format>
 <command>last -n 5</command>
 <frequency>360</frequency>
 </localfile>



 <localfile>
```

```
 <log_format>syslog</log_format>
 <location>/var/log/secure</location>
 </localfile>

 <localfile>
 <log_format>syslog</log_format>
 <location>/var/log/maillog</location>
 </localfile>

 <localfile>
 <log_format>apache</log_format>
 <location>/var/log/HTTPd/error_log</location>
 </localfile>

 <localfile>
 <log_format>apache</log_format>
 <location>/var/log/apache2/error.log</location>
 </localfile>

 <localfile>
 <log_format>syslog</log_format>
 <location>/var/OSSEC/logs/active-responses.log</location>
 </localfile>
```

Configuración de respuesta activa:

```
 <!-- Active response -->
 <active-response>
 <disabled>no</disabled>
 </active-response>

</agent_config>

<!-- Log analysis -->
 <localfile>
```

```
 <location>Application</location>
 <log_format>eventlog</log_format>
 </localfile>

 <localfile>
 <location>Security</location>
 <log_format>eventchannel</log_format>
 <query>Event/System(EventID != 5145 and EventID != 5156 and EventID
!= 5447]</query>
 </localfile>

 <localfile>
 <location>System</location>
 <log_format>eventlog</log_format>
 </localfile>

 <localfile>
 <location>C:\Program Files (x86)\OSSEC-agent\active-response\active-
responses.log</location>
 <log_format>syslog</log_format>
 </localfile>

 <!-- Policy monitoring -->
```

Configuración de ficheros para detectar *rootkit*s:

```
 <rootcheck>
 <disabled>no</disabled>
 <Windows_audit>./shared/win_audit_rcl.txt</Windows_audit>
 <Windows_apps>./shared/win_applications_rcl.txt</Windows_apps>
 <Windows_malware>./shared/win_malware_rcl.txt</Windows_malware>
 </rootcheck>
```

Ficheros por defecto que se comprueba la integridad:

```
 <!-- Active response -->
 <active-response>
 <disabled>no</disabled>
```

```
</active-response>
```

12 ANEXO 2 – INSTALACIÓN Y CONFIGURACIÓN DE OSSEC

En este anexo se describen los pasos de las instalaciones y configuraciones realizadas en cada uno de los equipos.

12.1 Instalar y configurar gestor OSSEC en *Ubuntu* 16.04

En este punto se detalla paso a paso como se realiza la descarga e instalación del gestor OSSEC en un Sistema operativo *Ubuntu*.

1. Requerimientos previos a instalación:
    a. Paquete *build-essential* para compilar e instalar OSSEC.

```
# apt-get install build-essential
```

    b. Paquete *mysql-dev* o *postgresql-dev* ya que se requiere una base de datos.

```
# apt-get install mysql-dev postgresql-dev
```

2. Descargar y comprobación de la integridad del fichero.

```
# wget -U OSSEC
HTTPs://bintray.com/artifact/download/OSSEC/OSSEC-
hids/OSSEC-hids-2.9.3.tar.gz
# wget -U OSSEC
HTTPs://raw.githubusercontent.com/OSSEC/OSSEC-
docs/master/docs/whatsnew/checksums/2.9.3/OSSEC-hids-
2.9.3.tar.gz.sha256
# cat OSSEC-hids-2.9.3.tar.gz.sha256
# sha256sum -c OSSEC-hids-2.9.3.tar.gz.sha256 OSSEC-hids-
2.9.3.tar.gz
(SHA256) OSSEC-hids-2.9.3.tar.gz: OK
```

3. Descomprimir e iniciar instalación en modo gestor:

```
# tar -zxvf OSSEC-hids-2.9.3.tar.gz (or gunzip -d; tar -
xvF)
# cd OSSEC-hids-2.9.3
# ./install.sh
```

Configuración tras ejecutar el instalador.

    a. Selección del idioma.

```
** Para instalação em português, escolha (br].** (cn].**
Fur eine deutsche Installation wohlen Sie (de].** For
installation in English, choose (en].** Para instalar en
Español , eliga (es].** Pour une installation en français,
choisissez (fr].** Per l'installazione in Italiano, scegli
(it].** (jp].

** Aby instalowa w jzyku Polskim, wybierz (pl].** no
установке на русскоМ ,ВВеДите (ru].** Za instalaciju na
srpskom, izaberi (sr].** Türkçe kurulum için seçin
(tr].(en/br/cn/de/es/fr/it/jp/pl/ru/sr/tr) (en]: es
```

b. Indicar "local" para monitorizar el servidor donde está instalado.

```
1- What kind of installation do you want (Server , agent,
local, hybrid or help)? local
```

c. Ubicación de la instalación local.

```
- Server installation chosen.
2- Setting up the installation environment.
- Choose where to install the OSSEC HIDS (/var/OSSEC]:
```

d. Notificaciones por E-mail.

```
- Installation will be made at /var/OSSEC .
3- Configuring the OSSEC HIDS.
3.1- Do you want e-mail notification? (y/n) (y]: y
- What's your e-mail address? root@localhost
- We found your SMTP Server as: 127.0.0.1
- Do you want to use it? (y/n) (y]: y
```

e. Comprobación de integridad.

```
3.2- Do you want to run the integrity check daemon? (y/n)
: y
 - Running syscheck (integrity check daemon).
```

f. Motor de detección de *rootkit*s.

```
3.3- Do you want to run the rootkit detection engine?
(y/n) : y
 - Running rootcheck (rootkit detection).
```

g. Habilitar respuesta activa.

```
- Do you want to enable active response? (y/n) : y
 - Active response enabled.
```

h. Habilitar cortafuegos.

```
- Do you want to enable the firewall-drop response? (y/n):
y
 - firewall-drop enabled (local) for levels >= 6
- Default white list for the active response:
 - 192.168.50.58
- Do you want to add more IPs to the white list? (y/n)?
(n]: n
```

i. Habilitar *Syslog* remoto.

```
3.5- Do you want to enable remote syslog (port 514 UDP)?
(y/n): y
 - Remote syslog enabled.
```

j. *Click* intro y se inicia la instalación.

```
- If you want to monitor any other file, just change the
OSSEC.conf and add a new localfile entry.
Any questions about the configuration can be answered
by visiting us online at HTTP://www.OSSEC.net .
--- Press ENTER to continue ---
- System is Debian (Ubuntu or derivative).
- Init script modified to start OSSEC HIDS during boot.


- Configuration finished properly.
```

k. Una vez completada la instalación, se inicia OSSEC.

```
# /var/OSSEC/bin/OSSEC-control start
```

```
Starting OSSEC HIDS v2.9 (by Trend Micro Inc.)...
Started OSSEC-maild...
Started OSSEC-execd...
Started OSSEC-analysisd...
Started OSSEC-logcollector...
Started OSSEC-syscheckd...
Started OSSEC-monitord...
Started OSSEC-dbd...
Completed.
```

4. El gestor OSSEC escucha a través del puerto 1514 *UDP*. Por lo que habrá que asegurarse que ninguna regla impida el tráfico a través de este puerto entre el agente y el gestor.

```
# iptables -I INPUT -p UDP --dport 1514 -s nuestra-
subred/24 -j ACCEPT
# iptables -I OUTPUT -p UDP --sport 1514 -d nuestra-
subred/24 -j ACCEPT.
```

5. Iniciar OSSEC:

```
# /var/OSSEC/bin/OSSEC-control start
```

12.1.1 Instalar y configurar OSSEC-WUI

En este punto se detalla la instalación de la interfaz web de OSSEC con la que interactuará el usuario.

1. Como prerrequisitos se ha de instalar apache con PHP.

```
sudo apt install apache2 php5
```

2. Descargar y ejecutar.

```
# wget HTTPs://github.com/OSSEC/OSSEC-wui/releases/OSSEC-wui-
0.9.tar.gz
# tar –xvzf OSSEC-wui-0.9.tar.gz
# cd OSSEC-wui-0.9.tar.gz
# OSSEC-wui-0.9.tar.gz
# mv OSSEC-wui-master /var/www/HTML/OSSEC
# cd /var/www/HTML/OSSEC

# ./setup.sh
```

```
trap: SIGHUP: bad trap
Setting up OSSEC ui...

Username: user
New password: ****
Re-type new password: ****
Adding password for user user
Enter your web Server user name (e.g. apache, www, nobody, www-
data, ...)
www-data
You must restart your web Server after this setup is done.
Setup completed successfully.
```

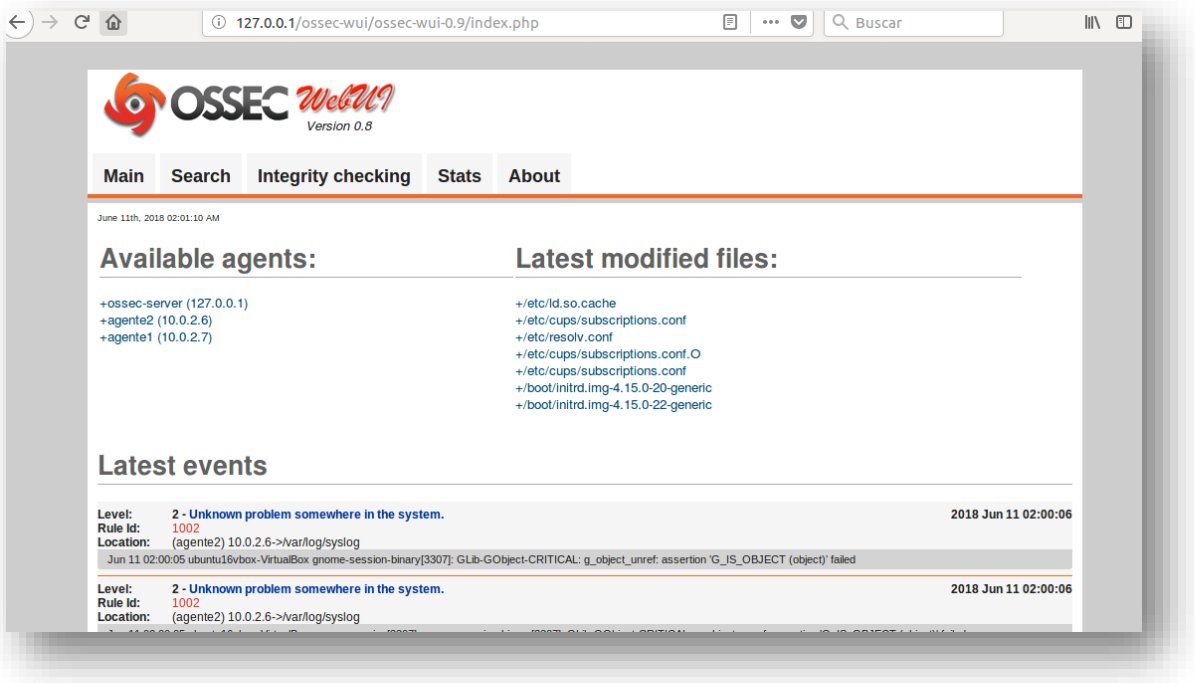
3. Gestión de permisos.

```
chown www-data:www-data /var/www/HTML/OSSEC/tmp/
chmod 666 /var/www/HTML/OSSEC/tmp
```

4. Puesta en marcha.

```
/etc/init.d/apache2 restart
```

5. Aspecto de la interfaz.



12.1.2 Configuración base de datos

1. Crear base de datos y asignación de privilegios.

```
# mysql -u root -p
# mysql> create database OSSEC;
# mysql> grant INSERT,SELECT,UPDATE,CREATE,DELETE,EXECUTE
on OSSEC.* to OSSECuser@<ip_OSSEC_servidor>;
Query OK, 0 rows affected (0.00 sec)
grant INSERT,SELECT,UPDATE,CREATE,DELETE,EXECUTE on OSSEC.* to
OSSEC_u;
Query OK, 0 rows affected (0.00 sec)
set password for OSSEC_u = PASSWORD('Passw0rd');
Query OK, 1 row affected (0.00 sec)
# mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)
mysql> quit
# mysql -u root -p OSSEC < src/os_dbd/mysql.schema
```

2. Configuración en /var/OSSEC/etc/OSSEC.conf.

```
<OSSEC_config>
 <database_output>
 <hostname>127.0.0.1</hostname>
 <username>OSSEC</username>
 <password>Password</password>
 <database>OSSEC</database>
 <type>mysql</type>
 </database_output>
</OSSEC_config>
```

3. Habilitar base de datos en OSSEC.

```
/var/OSSEC/bin/OSSEC-control enable database
/var/OSSEC/bin/OSSEC-control restart
```

12.1.3 Configuración envío de correos de alerta

Para el envío de correos se requiere instalar un servidor de correo en la máquina del gestor OSSEC. Los pasos son los siguientes:

1. Instalación *Postfix*. Se trata de una MTA (del inglés *Mail Transport Agent*).

```
aptitude install postfix
```

2. Configuración del fichero /etc/postfix/main.cf. Se añaden las siguientes líneas:

```
relayhost = (smtp.gmail.com]:587
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl/passwd
smtp_sasl_security_options = noanonymous
smtp_use_tls = yes
smtp_tls_CAfile = /etc/postfix/cacert.pem
```

3. Configuración de la autenticación en /etc/postfix/sasl/passwd:

```
(smtp.gmail.com]:587 (CUENTA]@gmail.com:(CONTRASEÑA]
```

4. Protección del fichero y transformación de tipo hash[90].

```
chmod 600 /etc/postfix/sasl/passwd
postmap /etc/postfix/sasl/passwd
```

5. Instalar certificados SSL (del inglés *Secure Socket Layer*).

```
aptitude install ca-certificates
```

6. Inicio del servidor.

```
/etc/init.d/postfix restart
```

12.1.4 Administrar agentes

12.1.4.1 Añadir agente

1. En el gestor ejecutaremos el comando para gestionar agentes.

```
# /var/OSSEC/bin/manage_agents

****************************************
* OSSEC-hids-2.9.3 - Agent manager. *
* The following options are available: *
****************************************
 (A)dd an agent (A).
 (E)xtract key for an agent (E).
 (L)ist already added agents (L).
 (R)emove an agent (R).
 (Q)uit.
Choose your action: A,E,L,R or Q:A
```

[90] Hash: función criptográfica o de resumen que a partir de una entrada (alfanumérica o archivo) genera una salida fija que representa un resumen de la información dada. Se usa para proteger la integridad y confidencialidad de la información.

2. Nombrar agente.

```
- Adding a new agent (use '\q' to return to the main menu).
 Please provide the following:
 * A name for the new agent: agente1
```

3. Dirección IP[91] (del inglés de *Internet Protocol*) del agente o red en a la que pertenece (en el caso de la red hay que indicar la máscara de red).

```
* The IP Address of the new agent: 10.0.2.6
```

4. Identificamos en agente con un código número de 3 dígitos.

```
* An ID for the new agent(001]: 001

Agent information:
 ID:001
 Name:agent1
 IP Address: 10.0.2.6
Confirm adding it?(y/n): y
Agent added.
```

5. Puesta en marcha el gestor OSSEC.

```
/var/OSSEC/bin/OSSEC-control restart
```

6. Una vez creado el agente se genera una clave (en el gestor) que debe ser copiada en el agente.

```
# /var/OSSEC/bin/manage_agents

Choose your action: A,E,L,R or Q: E

Available agents:
 ID: 001, Name: agent1, IP: 10.0.2.6
Provide the ID of the agent to extract the key (or '\q' to quit):
001

Agent key information for '001' is:
KDOyEWRnZW50MSAxOTIuMTY4LjIuDJ3yNCBlmIY3N2RiMTdmMTJjZGRlZjg5YzA7
ZDk5m
```

[91] Dirección IP: número identificador de una interfaz de red que utiliza el protocolo IP.

```
** Press ENTER to return to the main menu.
```

12.1.4.2 Eliminar agente

```
# /var/OSSEC/bin/manage_agents

Choose your action: A,E,L,R or Q: R
Available agents:
 ID: 001, Name: agent1, IP: 10.0.2.6
Provide the ID of the agent to be removed (or '\q' to quit): 001
Confirm deleting it?(y/n): y
Agent '001' removed.
```

12.2 Instalar y configurar agente OSSEC en *Windows 7*

En el caso del sistema operativo *Windows* solo permite instalar el agente OSSEC.

1. Descargar ejecutable desde la página oficial.
    - Página web: *HTTP*://www.OSSEC.net/downloads.*HTML*
2. Ejecutar el instalador.

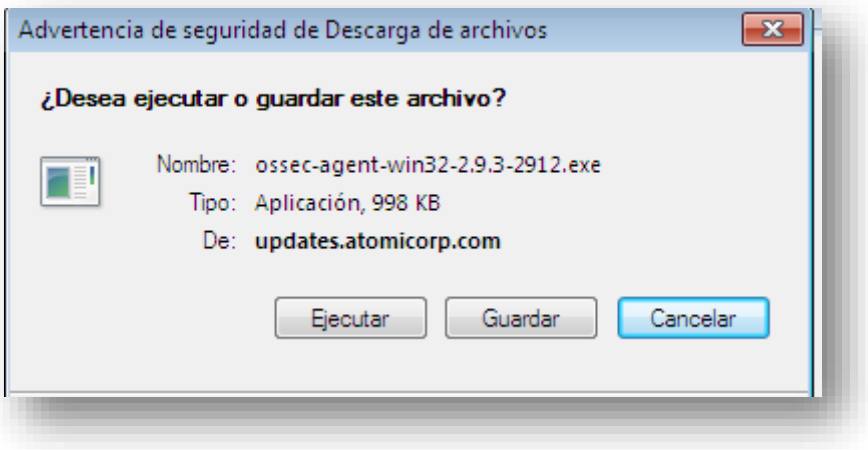


Figura 72 Ejecutar instalación agente OSSEC *Windows*

Figura 73 Siguiente paso en la instalación de agente OSSEC *Windows*

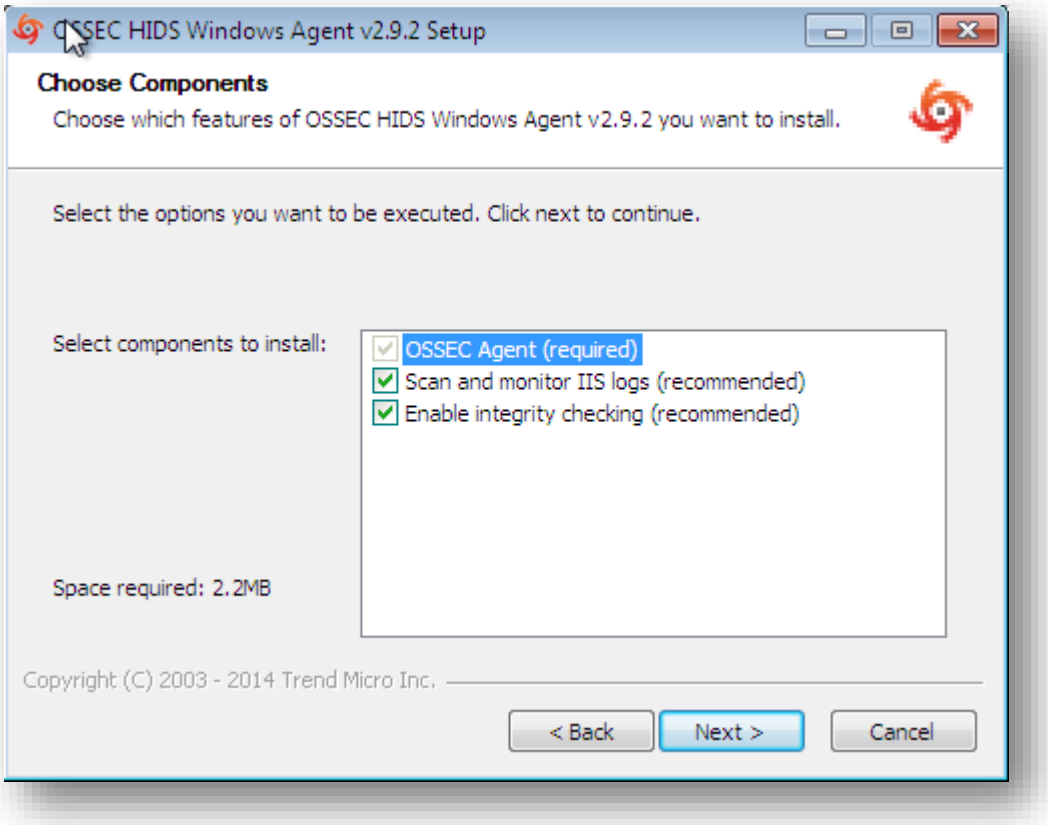


Figura 74 Seleccionar componentes en la instalación del agente OSSEC Windows

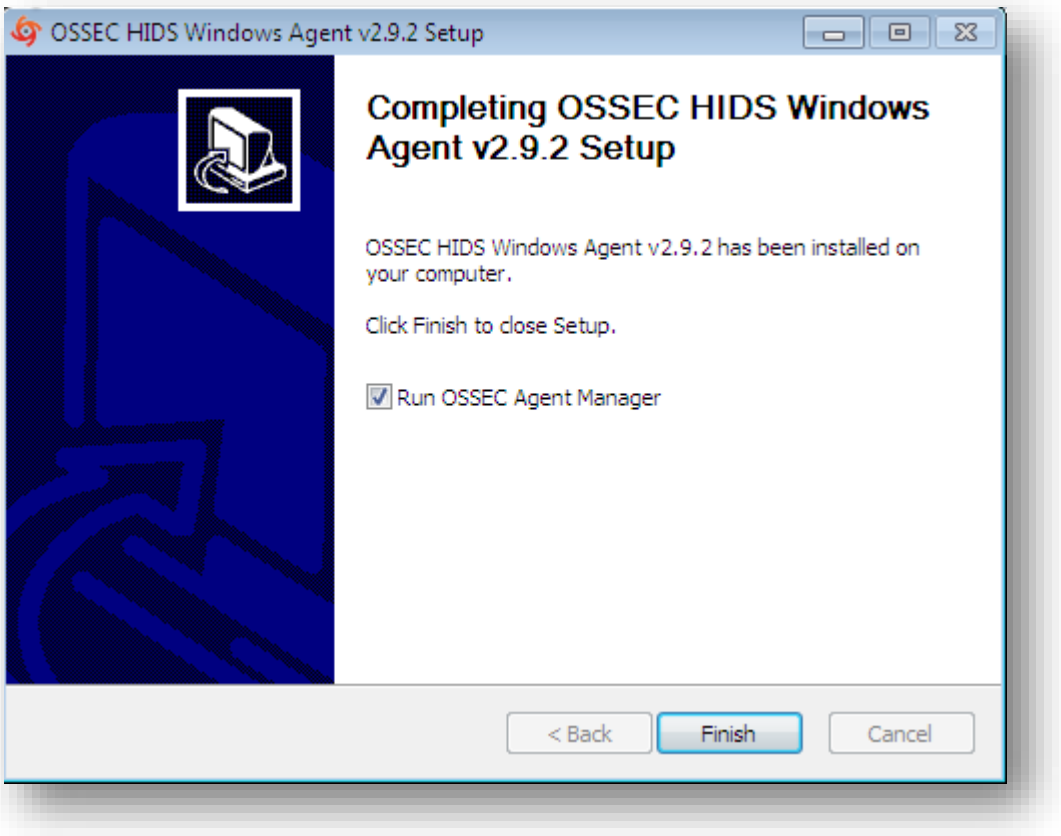


Figura 75 Finalizar instalación agente OSSEC Windows

3. Configurar agente:

Figura 76 Asignar IP del servidor OSSEC y definir clave de autenticación

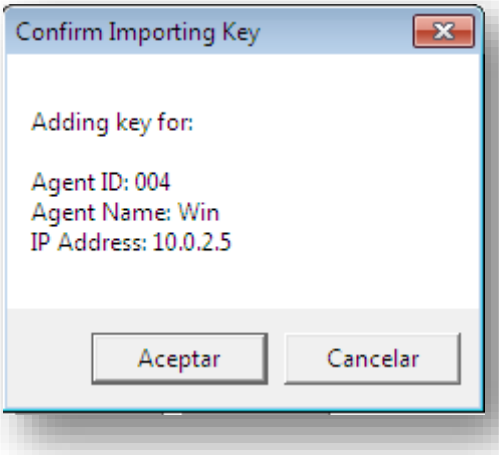


Figura 77 Aceptar parámetros

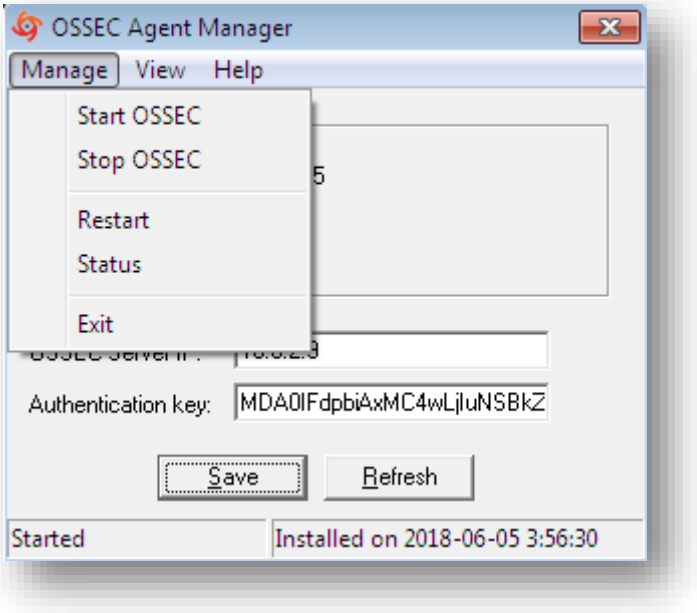


Figura 78 Iniciar agente OSSEC *Windows*

12.3 Instalar y configurar Agente en *Ubuntu* 16.04 LTS y 17.04 LTS

La instalación y configuración inicial de los agentes en el sistema operativo *Ubuntu* se realiza igual independientemente de la versión. La descarga e instalación se realiza exactamente igual que en el gestor por lo que se continuará con los siguientes pasos.

12.3.1 Importar clave al agente

Este paso se tiene que realizar para que el agente se sincronice con el gestor. Se podrá realizar una vez que en el gestor se ha añadido el agente.

```
# /var/OSSEC/bin/manage_agents
```

```
************************************
* OSSEC-hids-2.9.3 Agent manager. *
* The following options are available: *
************************************
 (I)mport key from the Server (I).
 (Q)uit.
Choose your action: I or Q: i

* Provide the Key generated by the Server .
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): (key extracted via
manage_agents on the Server ]

Agent information:
 ID:001
 Name:agent1
 IP Address:10.0.2.6

Confirm adding it?(y/n): y
Added.
** Press ENTER to return to the main menu.
```

13 GLOSARIO DE TÉRMINOS

Amenaza [14] [187] : Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización [UNE 71504:2008] [231].

Intrusión [139]: Cualquier acción no autorizada o no deseada que pueda comprometer la integridad, confidencialidad o disponibilidad de la información.

Auditoria de control de accesos [232]: Revisiones periódicas de los procesos de control de acceso para evaluar la efectividad de dichos controles.

Autenticidad [33]: Garantía de la fuente de la que proceden los datos. La seguridad de la organización debe asegurar que los datos proceden de sitios seguros sin haber sufrido manipulación alguna.

Confidencialidad [232]: Solo las personas, procesos y sistemas autorizados deben tener acceso a la información en función de la necesidad.

Diccionario de datos [233]**:** Repositorio centralizado de elementos que forman parte de un un flujo de datos dentro de un sistema. El diccionario guarda detalles y descripciones de estos elementos.

Disponibilidad [232]: La información debe ser accesible y estar disponible siempre que se la necesite.

Integridad [232]: La información debe mantenerse protegida de cambios fortuitos o deliberados.

Lista de control de acceso [232]: Lista de usuarios o direcciones autorizados a acceder a un sistema.

Riesgo [234]: Es la probabilidad de que ocurra un hecho que produzca ciertos efectos no deseados, la combinación de la probabilidad de la ocurrencia de un evento y la magnitud del impacto que puede causar, así mismo es la incertidumbre frente a la ocurrencia de eventos y situaciones que afecten los beneficios de una actividad

Syslog: Servicio de envío y recepción de registros del sistema.

Trazabilidad [33]: Se debe conocer en todo momento quién y cuándo ha realizado cada acción con la información de la información. Esta característica es muy útil para analizar los incidentes y para detectar a los atacantes.

Vulnerabilidad [234]. Debilidad o grado de exposición de un sujeto, objeto o sistema. También son aquellas fallas, omisiones o deficiencias de seguridad que puedan ser aprovechadas por los delincuentes.

14 BIBLIOGRAFÍA

[1] «ISO27000,» [En línea]. Available: http://iso27000.es/. [Último acceso: 15 06 2018].

[2] «Cobit5,» [En línea]. Available: http://www.isaca.org/cobit/pages/default.aspx. [Último acceso: 08 05 2018].

[3] «Guias STIC,» [En línea]. Available: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html. [Último acceso: 17 07 2018].

[4] «CCN-CERT,» [En línea]. Available: https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html. [Último acceso: 30 06 2018].

[5] «Boletin de seguridad de Microsoft,» [En línea]. Available: https://technet.microsoft.com/es-es/security/bulletins.aspx. [Último acceso: 02 04 2018].

[6] «Repercusión del Wannacry,» [En línea]. Available: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4506-repercusion-en-espana-de-la-campana-wannacry-239-direcciones-ip-en-contacto-con-uno-de-los-dominios-daninos-identificados-y-2-774-direcciones-ip-vulnerables.html. [Último acceso: 18 06 2018].

[7] «Ataque petya,» [En línea]. Available: https://www.incibe.es/protege-tu-empresa/avisos-seguridad/nueva-oleada-ransomware-afectando-multiples-equipos. [Último acceso: 18 06 2018].

[8] «INCIBE,» 28 12 2017. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/2017-el-ano-las-empresas-se-concienciaron-ciberseguridad. [Último acceso: 18 06 2018].

[9] «INCIBE,» 19 01 2017. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/avisos-seguridad/fraude-del-ceo. [Último acceso: 18 06 2018].

[10] «Hot-potato,» 19 01 2016. [En línea]. Available: http://blog.elevenpaths.com/2016/01/hot-potato-mas-que-una-elevacion-en.html. [Último acceso: 18 06 2018].

[11] «Elevenpaths,» [En línea]. Available: https://www.elevenpaths.com/company/index.html. [Último acceso: 09 06 2018].

[12] «INCIBE,» 12 05 2017. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/avisos-seguridad/importante-oleada-ransomware-afecta-multitud-equipos. [Último acceso: 18 06 2018].

[13] «INCIBE,» 16 10 2017. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/avisos-seguridad/importante-fallo-el-protocolo-wpa2-pone-riesgo-seguridad-las. [Último acceso: 19 06 2018].

[14] «Margerit,» [En línea]. Available: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html. [Último acceso: 20 2018 2018].

[15] «Manual ITIL v3,» [En línea]. Available: http://www.biable.es/wp-content/uploads/2014/ManualITIL.pdf. [Último acceso: 22 08 2018].

[16] «Esquema nacional de seguridad,» 03 2013. [En línea]. Available: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/804-Medidas_de_implantacion_del_ENS/804_medidas_de_implantacion_del_ens.pdf. [Último acceso: 30 06 2018].

[17] «SANS Institute,» [En línea]. Available: https://www.sans.org/about/. [Último acceso: 22 06 2018].

[18] «SANS Institute,» 04 07 2012. [En línea]. Available: https://www.sans.org/reading-room/whitepapers/logging/logging-monitoring-detect-network-intrusions-compliance-violations-environment-33985.

[19] C. a. i. Affiliates, «Snort,» 2018. [En línea]. Available: https://www.snort.org/. [Último acceso: 20 06 2018].

[20] «Suricata,» [En línea]. Available: https://suricata-ids.org/. [Último acceso: 02 05 2018].

[21] «CERTSI,» 11 2017. [En línea]. Available: https://www.certsi.es/sites/default/files/contenidos/guias/doc/certsi_design_configuration_ips_ids_siem_in_ics.pdf. [Último acceso: 15 06 2018].

[22] «GUIAS STIC,» [En línea]. Available: https://www.ccn-cert.cni.es/guias.html. [Último acceso: 12 07 2018].

[23] CNN-CERT, «Guía de Seguridad de las TIC CCN-STIC 817,» [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html.

[24] «Ecured,» 2018. [En línea]. Available: https://www.ecured.cu/Eventos. [Último acceso: 03 07 2018].

[25] G. Escrivá Gascó, R. M. Romero Serrano , D. Jorge Ramada y R. Onrubia Pérez , SEGURIDAD INFORMATICA, Macmillan Profesional, 2013.

[26] «Wireshark,» [En línea]. Available: https://www.wireshark.org/. [Último acceso: 06 06 2018].

[27] «Tripwire,» US Headquarters, 2018. [En línea]. Available: https://www.tripwire.com/. [Último acceso: 12 05 2018].

[28] «Sandbox,» 28 05 2016. [En línea]. Available: https://www.redeszone.net/2016/05/28/3-aplicaciones-sandbox-proteger-ordenador-del-malware/. [Último acceso: 12 05 2018].

[29] «Nagios,» Nagios Enterprises, LLC, 2018. [En línea]. Available: https://www.nagios.org.

[30] «Pandorafms,» [En línea]. Available: https://pandorafms.com. [Último acceso: 17 05 2018].

[31] «ZABBIX,» Zabbix LLC, 2018. [En línea]. Available: https://www.zabbix.com/]. [Último acceso: 17 05 2018].

[32] E. Valdés-Solís Iglesias, «LOS DELITOS CONTRA LOS SISTEMAS INFORMÁTICOS: ARTS. 197 BIS Y 197,» 14 07 2017. [En línea]. Available: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Vald%C3%A9s-Sol%C3%ADs%20Iglesias,%20Enrique.pdf?idFile=7fa46cba-15ec-482b-a2dc-2f7a02f29e5b.

[33] E. Chicano Tejada, Auditoría de seguridad informática (MF0487_3), Málaga: IC EDITORIAL, 2014.

[34] J. GÓMEZ LÓPEZ, E. VILLAR FERNANDEZ y A. ALCAYDE GARCIA, Seguridad en sistemas operativos Windows y Linux. 2ª Edición actualizada, RA-MA EDITORIAL, 2011.

[35] «CVE details,» [En línea]. Available: https://www.cvedetails.com/. [Último acceso: 19 06 2018].

[36] «Windows Server 2008: Vulnerability Statistics,» [En línea]. Available: https://www.cvedetails.com/product/11366/Microsoft-Windows-Server-2008.html?vendor_id=26. [Último acceso: 02 07 2018].

[37] «Windows 7: Vulnerability Statistics,» [En línea]. Available: https://www.cvedetails.com/product/17153/Microsoft-Windows-7.html?vendor_id=26. [Último acceso: 12 07 2018].

[38] «Debian : Vulnerability Statistics,» [En línea]. Available: https://www.cvedetails.com/vendor/23/Debian.html. [Último acceso: 06 07 2018].

[39] «Ubuntu : Vulnerability Statistics,» [En línea]. Available: https://www.cvedetails.com/vendor/51/Ubuntu.html. [Último acceso: 12 07 2018].

[40] «NIST,» 06 2018. [En línea]. Available: https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cwe-over-time#vuln-type-total-by-year-desc. [Último acceso: 23 05 2018].

[41] «CVE Details,» [En línea]. Available: https://www.cvedetails.com/top-50-products.php. [Último acceso: 11 07 2018].

[42] «CVE Details,» [En línea]. Available: https://www.cvedetails.com/cwe-definitions/1/orderbyvulnerabilities.html?order=2&trc=668&sha=0427874cc45423ccb6974ee25935fbfceac76fcb. [Último acceso: 15 07 2018].

[43] «CWE,» [En línea]. Available: http://cwe.mitre.org/data/index.html. [Último acceso: 01 06 2018].

[44] «Securelist,» 26 03 2018. [En línea]. Available: https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h2-2017/85053/. [Último acceso: 26 03 2018].

[45] «Securelist,» 26 03 2018. [En línea]. Available: https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h2-2017/85053/. [Último acceso: 26 03 2018].

[46] «itsecdb,» [En línea]. Available: http://www.itsecdb.com/oval/definitions/class-5-Vulnerability/?family=windows.

[47] «CWE-787,» 29 03 2018. [En línea]. Available: https://cwe.mitre.org/data/definitions/787.html. [Último acceso: 22 05 2018].

[48] «CWE-125,» 29 03 2018. [En línea]. Available: https://cwe.mitre.org/data/definitions/125.html. [Último acceso: 22 05 2018].

[49] «CWE-119,» 29 03 2018. [En línea]. Available: http://cwe.mitre.org/data/definitions/119.html. [Último acceso: 22 05 2018].

[50] «CWE-123,» 29 03 2018. [En línea]. Available: https://cwe.mitre.org/data/definitions/123.html. [Último acceso: 22 05 2018].

[51] «CVE-2018-0935,» [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-0935. [Último acceso: 28 05 2018].

[52] «CVE-2018-0935,» 01 12 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0935. [Último acceso: 25 05 2018].

[53] «Vulnerability Details : CVE-2018-0935,» 07 04 2018. [En línea]. Available: https://www.cvedetails.com/cve-details.php?cve_id=CVE-2018-0935. [Último acceso: 18 05 2018].

[54] «CVE-2018-0935 | Scripting Engine Memory Corruption Vulnerability,» 23 03 2018. [En línea]. Available: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0935. [Último acceso: 18 05 2018].

[55] «CVE-2018-0778,» 04 01 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-0778. [Último acceso: 27 05 2018].

[56] «CVE-2018-0778,» 01 12 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0778. [Último acceso: 28 05 2018].

[57] «fedoraproject,» 12 06 2012. [En línea]. Available: https://fedoraproject.org/wiki/Features/procps-ng. [Último acceso: 29 05 2018].

[58] NIST, «CVE-2018-1125,» 23 05 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-1125. [Último acceso: 25 07 2018].

[59] «CVE-2018-1125,» 04 12 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1125. [Último acceso: 21 07 2018].

[60] «Redhat,» [En línea]. Available: https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/html/performance_tuning_guide/ch06s03. [Último acceso: 02 07 2018].

[61] «Debian.org,» [En línea]. Available: https://manpages.debian.org/testing/blktrace/btt.1.en.html. [Último acceso: 16 07 2018].

[62] NIST, «CVE-2018-10689,» 03 05 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-10689. [Último acceso: 02 08 2018].

[63] «CVE-2018-10689,» 03 05 2018. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10689. [Último acceso: 03 08 2018].

[64] «CWE-200,» 29 03 2018. [En línea]. Available: https://cwe.mitre.org/data/definitions/200.html. [Último acceso: 12 05 2018].

[65] «ISS,» [En línea]. Available: https://msdn.microsoft.com/es-es/library/hh831725(v=ws.11).aspx.

[66] «CVE-2018-1234,» 30 03 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-1234. [Último acceso: 21 06 2018].

[67] «CVE-2018-1234,» 12 06 2018. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1234. [Último acceso: 01 07 2018].

[68] Microsoft, «Boletín de seguridad de Microsoft,» [En línea]. Available: https://blogs.technet.microsoft.com/seguridad/2018/06/12/lanzamiento-de-actualizacion-de-seguridad-de-microsoft-de-junio-de-2018/. [Último acceso: 28 07 2018].

[69] «CVE-2018-0887,» 11 04 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-0887. [Último acceso: 02 06 2018].

[70] «CVE-2018-0887,» 01 12 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0887. [Último acceso: 01 07 2018].

[71] «SSB,» 21 05 2018. [En línea]. Available: https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/Variant4.

[72] «CVE-2018-3639,» 22 05 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-3639. [Último acceso: 11 07 2018].

[73] «CVE-2018-3639,» 28 12 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-3639. [Último acceso: 02 07 2018].

[74] «openssh,» [En línea]. Available: https://www.freebsd.org/doc/es/books/handbook/openssh.html.

[75] «NIST,» 14 01 2016. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2016-0777. [Último acceso: 21 07 2018].

[76] «CVE-2016-0777,» [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0777. [Último acceso: 02 06 2018].

[77] CWE, «CWE-284,» 29 03 2018. [En línea]. Available: http://cwe.mitre.org/data/definitions/284.html. [Último acceso: 21 07 2018].

[78] «NVD,» 14 06 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-8225.

[79] «CVE-2018-8225,» 14 03 2018. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8225.

[80] «NVIDIA,» [En línea]. Available: https://www.nvidia.com/en-us/about-nvidia/corporate-timeline/.

[81] «CVE-2016-8824,» 18 10 2016. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8824.

[82] «CVE-2017-17807,» 20 12 2017. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-17807.

[83] «CVE-2017-17807,» 20 12 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17807.

[84] «NVD,» 06 06 2017. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2015-9006.

[85] «CVE-2015-9006,» 28 03 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9006.

[86] «CWE264,» 29 03 2018 . [En línea]. Available: https://cwe.mitre.org/data/definitions/264.html.

[87] «Cuentas atractivas para el robo de credenciales,» 31 05 2017. [En línea]. Available: https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/plan/security-best-practices/attractive-accounts-for-credential-theft.

[88] «IOCTL,» 31 05 2018. [En línea]. Available: https://docs.microsoft.com/en-us/windows/desktop/devio/device-input-and-output-control-ioctl-. [Último acceso: 02 08 2018].

[89] «ACPI,» 01 24 2018. [En línea]. Available: https://docs.microsoft.com/es-es/windows-hardware/drivers/acpi/#in-this-section. [Último acceso: 02 08 2018].

[90] «ACL,» 01 05 2018. [En línea]. Available: https://docs.microsoft.com/en-us/windows/desktop/secauthz/access-control-lists. [Último acceso: 22 07 2018].

[91] NIST, «CVE-2017-15302,» 15 10 2017. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-15302.

[92] «CVE-2017-15302,» 14 10 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15302. [Último acceso: 12 07 2018].

[93] «CVE-2017-11829,» 13 10 2017. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-11829. [Último acceso: 06 06 2018].

[94] «CVE-2017-11829,» 31 07 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11829CVE-2017-11829. [Último acceso: 18 07 2018].

[95] «CVE-2018-8134,» 09 05 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-8134. [Último acceso: 17 07 2018].

[96] «CVE-2018-7500,» 26 02 2018. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7500. [Último acceso: 12 07 2018].

[97] «XFRM,» [En línea]. Available: https://nscpolteksby.ac.id/ebook/files/Ebook/Computer%20Engineering/Linux%20Kernel%20Networking%20-%20Implementation%20(2014)/chapter10%20IPsec.pdf. [Último acceso: 02 08 2018].

[98] «CVE-2017-16939,» 24 11 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-16939. [Último acceso: 12 07 2018].

[99] «CVE-2016-7097,» 16 10 2016. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2016-7097. [Último acceso: 17 06 2018].

[100] «CVE-2017-5551,» 02 06 2017. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-5551. [Último acceso: 23 06 2018].

[101] «CVE-2017-5551,» 20 01 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5551. [Último acceso: 12 07 2018].

[102] «CWE-20: Improper Input Validation,» 29 03 2018. [En línea]. Available: http://cwe.mitre.org/data/definitions/20.html. [Último acceso: 07 06 2018].

[103] «CVE-2018-8997,» 24 03 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-8997.

[104] «CVE-2018-8997,» 24 03 2018. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8997.

[105] «CVE-2017-5092,» 27 10 2017. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-5092.

[106] «CVE-2017-5092,» 02 01 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5092.

[107] «CVE-2018-1000026,» 24 04 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-1000026.

[108] «CVE-2018-1000026,» 29 01 2018. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000026.

[109] «mozilla,» [En línea]. Available: https://support.mozilla.org/es/products/firefox-os.

[110] «CVE-2017-18065,» 16 03 03. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-18065.

[111] «CVE-2017-18065,» 22 01 2018. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18065.

[112] «CWE,» 29 03 2018. [En línea]. Available: http://cwe.mitre.org/data/definitions/264.html. [Último acceso: 25 04 2018].

[113] «CWE CATEGORY: Credentials Management,» 29 03 2018. [En línea]. Available: http://cwe.mitre.org/data/definitions/255.html.

[114] «CVE-2018-1000041,» 09 02 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-1000041.

[115] «CVE-2018-1000041,» 05 02 2018. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000041.

[116] «CVE-2018-1217,» 09 04 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-1217. [Último acceso: 12 08 2018].

[117] «CVE-2018-1217,» 06 12 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1217. [Último acceso: 21 07 2018].

[118] «CVE-2018-1240,» 18 04 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-1240. [Último acceso: 18 07 2018].

[119] «CVE-2018-1240,» 06 12 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1240. [Último acceso: 18 08 2018].

[120] «CVE-2017-18270,» 18 05 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-18270. [Último acceso: 19 08 2018].

[121] «CVE-2017-18270,» 18 05 2018. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18270. [Último acceso: 06 08 2018].

[122] «CWE-417,» 29 03 2018. [En línea]. Available: http://cwe.mitre.org/data/definitions/417.html. [Último acceso: 11 08 2018].

[123] «CVE-2018-7295,» 26 06 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-7295. [Último acceso: 12 08 2018].

[124] «CVE-2018-7295,» 21 02 2018. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7295. [Último acceso: 18 07 2018].

[125] «CWE-79,» 29 03 2018. [En línea]. Available: http://cwe.mitre.org/data/definitions/79.html. [Último acceso: 18 08 2018].

[126] «CWE-444,» 29 03 2018. [En línea]. Available: http://cwe.mitre.org/data/definitions/444.html. [Último acceso: 19 06 2018].

[127] «CWE-918,» 29 03 2018. [En línea]. Available: http://cwe.mitre.org/data/definitions/918.html. [Último acceso: 19 07 2018].

[128] «Wordpress,» [En línea]. Available: https://es.wordpress.com/. [Último acceso: 05 03 2018].

[129] «CVE-2018-1000556,» 26 06 2018. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-1000556.

[130] «CVE-2018-1000556,» 22 06 2018. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000556.

[131] «Cisco Jabber,» [En línea]. Available: https://www.cisco.com/c/en/us/products/unified-communications/jabber/index.html. [Último acceso: 17 08 2018].

[132] «Cisco Security Advisory,» 29 11 2017. [En línea]. Available: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-jabber. [Último acceso: 18 06 2018].

[133] «CVE-2017-12356,» 30 11 2017. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-12356. [Último acceso: 11 08 2018].

[134] «CVE-2017-12356,» 03 08 2017. [En línea]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12356. [Último acceso: 19 08 2018].

[135] Á. L. Calvo García, Gestión de redes telemáticas (UF1880), Madrid: IC Editorial, 2014.

[136] G. Alvarez Marañón y P. P. Perez Garcia, SEGURIDAD INFORMATICA PARA LA EMPRESA Y PARTICULARES, S.A. MCGRAW-HILL / INTERAMERICANA DE ESPAÑA, 2004.

[137] «Incibe,» [En línea]. Available: https://www.incibe.es/que-es-incibe. [Último acceso: 10 07 2018].

[138] INCIBE, «INCIBE,» 20 03 2017. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian. [Último acceso: 10 07 2018].

[139] E. Tejada Chicano, Gestión de incidentes de seguridad informática (MF0488_3), IC Editorial, 2014.

[140] J. Costas Santos, Seguridad y alta disponibilidad, RA-MA Editoria, 2014.

[141] G. B. Urbina, Introducción a la seguridad informática, México: Grupo Editorial Patria, 2016.

[142] Á. Gómez Vieites, Gestión de incidentes de seguridad informática, Starbook Editorial, S.A., 2011.

[143] Á. Gómez Vieites, Enciclopedia de la Seguridad Informática. 2ª edición, Editorial RA-MA, 2014.

[144] «Security Threats,» [En línea]. Available: https://technet.microsoft.com/en-us/library/cc723507.aspx.

[145] «McAfee,» 12 2017. [En línea]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2017.pdf. [Último acceso: 20 06 2018].

[146] «Calyptix security,» 23 10 2017. [En línea]. Available: https://www.calyptix.com/top-threats/top-8-network-attacks-type-2017/. [Último acceso: 29 07 2018].

[147] «Hackmageddon,» [En línea]. Available: https://www.hackmageddon.com/about/. [Último acceso: 18 07 2018].

[148] «Cyber Attacks Statistics,» 28 06 2018. [En línea]. Available: https://www.hackmageddon.com/2018/06/28/may-2018-cyber-attacks-statistics/. [Último acceso: 02 08 2018].

[149] «2017 Cyber Attacks Statistics,» 17 01 2018. [En línea]. Available: https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/.

[150] «Infowatch,» [En línea]. Available: https://infowatch.com/report2017. [Último acceso: 12 08 2018].

[151] «Amenazas de seguridad comunes en la informática moderna,» [En línea]. Available: https://docs.microsoft.com/es-es/skypeforbusiness/plan-your-deployment/security/common-threats.

[152] M. A. Castro Gil, G. Díaz Orueta, I. Alzórriz Armendáriz y E. Sancristobal Ruíz, Procesos y herramientas para la seguridad de redes, Editorial UNED, 2014.

[153] E. Valdés-Solís Iglesias, «Los delitos contra los sistemas informáticos,» 14 07 2017. [En línea]. Available: https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/Ponencia%20Vald%C3%A9s-Sol%C3%ADs%20Iglesias,%20Enrique.pdf?idFile=7fa46cba-15ec-482b-a2dc-2f7a02f29e5b. [Último acceso: 17 04 2018].

[154] «Segu-info,» [En línea]. Available: https://www.segu-info.com.ar/ataques/ataques_autenticacion.htm. [Último acceso: 11 08 2018].

[155] «Ataques de Autenticacion,» 18 02 2010. [En línea]. Available: https://underc0de.org/foro/hacking/ataques-de-autenticacion/. [Último acceso: 27 07 2018].

[156] «Top 10 de las herramientas más populares para crackear contraseñas,» 6 08 2016 . [En línea]. Available: https://www.redeszone.net/2016/08/06/top-10-las-herramientas-mas-populares-crackear-contrasenas/.

[157] «Exploits,» [En línea]. Available: https://www.elhacker.net/exploits.html. [Último acceso: 10 06 2018].

[158] «Exploit-db,» [En línea]. Available: https://www.exploit-db.com/platform/?p=Windows. [Último acceso: 09 06 2018].

[159] «Exploits,» [En línea]. Available: https://www.microsoft.com/en-us/wdsi/threats/exploit-malware. [Último acceso: 18 05 2018].

[160] «CVE-2010-2568 Detail,» 22 07 2010. [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2010-2568. [Último acceso: 17 06 2018].

[161] «Kaspersky: Boletín De Seguridad,» 19 12 2017. [En línea]. Available: https://securelist.lat/ksb-overall-statistics-2017/85873/. [Último acceso: 12 07 2018].

[162] «Microsoft,» 02 2010. [En línea]. Available: https://technet.microsoft.com/es-es/library/dd897047.aspx. [Último acceso: 19 07 2018].

[163] «NMAP,» [En línea]. Available: https://nmap.org/. [Último acceso: 08 06 2018].

[164] «ZMAP,» [En línea]. Available: https://zmap.io/. [Último acceso: 01 07 2018].

[165] D. Dumas, D. Puche, F. Ebel, F. Vicogne, G. Fortunato, J. Hennecart, M. Agé, L. Schalkwijk, R. Rault, R. Crocfer y S. Lasson, Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa (3ª edición), Ediciones ENI, 2015.

[166] «Elevación de privilegios,» 30 03 2017. [En línea]. Available: https://docs.microsoft.com/es-es/dotnet/framework/wcf/feature-details/elevation-of-privilege.

[167] «Mapa de ciberamenazas a tiempo real,» [En línea]. Available: https://cybermap.kaspersky.com/stats/. [Último acceso: 14 07 2018].

[168] «Securelist,» [En línea]. Available: https://securelist.lat/estadisticas/. [Último acceso: 14 07 2018].

[169] «Checkpoint,» [En línea]. Available: https://www.checkpoint.com/. [Último acceso: 18 07 2018].

[170] «Checkpoint,» [En línea]. Available: https://threatmap.checkpoint.com/ThreatPortal/livemap.html. [Último acceso: 16 07 2018].

[171] «Reporte de seguridad15/16,» [En línea]. Available: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2015-2016.pdf. [Último acceso: 04 07 2018].

[172] «Reporte de seguridad 16/17,» [En línea]. Available: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2016-2017.pdf. [Último acceso: 19 07 2018].

[173] «Sobre el instituto AV-TEST,» [En línea]. Available: https://www.av-test.org/es/sobre-el-instituto/.

[174] «Statista,» [En línea]. Available: https://www.statista.com/aboutus/. [Último acceso: 10 07 2018].

[175] «Malware Threat,» 28 06 2017. [En línea]. Available: https://www.statista.com/chart/10045/new-malware-specimen-and-share-of-windows-based-malware/. [Último acceso: 19 08 2018].

[176] «Spam y phishing,» 23 05 2018. [En línea]. Available: https://securelist.lat/spam-and-phishing-in-q1-2018/86992/. [Último acceso: 10 06 2018].

[177] «Códigos maliciosos: troyanos,» [En línea]. Available: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/6477-publicado-un-nuevo-informe-de-codigo-danino-sobre-la-familia-de-troyanos-kovter.html. [Último acceso: 18 06 2018].

[178] «Códigos maliciosos: troyanos,» [En línea]. Available: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/6228-trok-quant-y-crossrat-dos-nuevos-informes-de-codigo-danino-del-ccn-cert.html. [Último acceso: 18 06 2018].

[179] «Códigos maliciosos: troyanos,» [En línea]. Available: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/6126-el-ccn-cert-analiza-la-familia-de-troyanos-trojan-banker-win32-chepro-y-shiotob.html. [Último acceso: 17 06 2018].

[180] «Códigos maliciosos: troyanos,» [En línea]. Available: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/6087-betabot-y-fleercivet-dos-nuevos-informes-de-codigo-danino-del-ccn-cert.html. [Último acceso: 17 07 2018].

[181] «CrossRAT, nuevo troyano que infecta equipos Windows, Mac y Linux,» 26 01 2018. [En línea]. Available: https://computerhoy.com/noticias/software/crossrat-nuevo-troyano-que-infecta-equipos-windows-mac-linux-74981. [Último acceso: 12 06 2018].

[182] «Perfiles de amenazas,» [En línea]. Available: https://www.cyber.nj.gov/threat-profiles/botnet-variants/linuxproxy10. [Último acceso: 18 07 2018].

[183] «Ataques a Windows y Linux,» 26 01 2017. [En línea]. Available: https://www.profesionalreview.com/2017/01/26/hackers-redirigir-ataques-windows-linux/. [Último acceso: 02 07 2018].

[184] «sputniknews,» 02 07 2018. [En línea]. Available: https://mundo.sputniknews.com/tecnologia/201807021080060181-malware-all-radio-portable-windows/. [Último acceso: 09 07 2018].

[185] «DDOS,» 26 04 2018. [En línea]. Available: https://securelist.com/ddos-report-in-q1-2018/85373/. [Último acceso: 10 07 2018].

[186] «Github,» [En línea]. Available: https://github.com/github. [Último acceso: 10 07 2018].

[187] «Margerit,» [En línea]. Available: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Último acceso: 12 08 2018].

[188] Y. K. P. H. Bruce Potter, Mastering FreeBSD and OpenBSD Security, O'Reilly Media, 2005.

[189] I. S. R. Córsico, Trabajo de auditoría normas COBIT., El Cid Editor, 2009.

[190] G. F. Luis y F. R. Pedro Pablo, Cómo implantar un SGSI según UNE-ISO-IEC 27001-2014 y su aplicación en el esquema nacional de seguridad, AENOR Internacional, S.A.U, 2015.

[191] «CCN-STIC 817,» 06 2018. [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html. [Último acceso: 02 07 2018].

[192] E. C. Tejada, Gestión de servicios en el sistema informático (MF_0490), Málaga: IC EDITORIAL, 2014.

[193] «Data Security and Data Availability for End Systems,» [En línea]. Available: https://technet.microsoft.com/en-us/library/cc722919.aspx. [Último acceso: 14 07 2018].

[194] «Medidas de protección frente ataques de denegación de servicio (DoS),» 26 01 2018. [En línea]. Available: https://www.certsi.es/blog/medidas-proteccion-frente-ataques-denegacion-servicio-dos. [Último acceso: 15 07 2018].

[195] «SynAttackProtect,» 09 10 2008. [En línea]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc938202(v=technet.10). [Último acceso: 12 07 2018].

[196] «TcpMaxPortsExhausted,» 09 10 2008. [En línea]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc938214(v=technet.10). [Último acceso: 12 07 2018].

[197] «TcpMaxHalfOpen,» 09 10 2008. [En línea]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc938212(v=technet.10). [Último acceso: 12 07 2018].

[198] «Denegación de servicio,» 30 03 2017. [En línea]. Available: https://docs.microsoft.com/es-es/dotnet/framework/wcf/feature-details/denial-of-service. [Último acceso: 12 07 2018].

[199] «Best Practices for Preventing DoS/Denial of Service Attacks,» [En línea]. Available: https://technet.microsoft.com/en-us/library/cc750213.aspx. [Último acceso: 12 07 2018].

[200] «Planeación para protegerse contra los ataques de tipo “flood” de denegación de servicio,» [En línea]. Available: https://technet.microsoft.com/es-es/library/dd897007.aspx. [Último acceso: 12 07 2018].

[201] «GUÍA DE PROTECCIÓN CONTRA DENEGACIÓN DE SERVICIO,» 06 2013. [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/528-ccn-stic-820-proteccion-contra-denegacion-de-servicio/file.html. [Último acceso: 12 07 2018].

[202] «Cómo enfrentarse a las amenazas del ransomware,» 30 05 2018. [En línea]. Available: https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/6339-como-enfrentarse-a-las-amenazas-del-ransomware.html. [Último acceso: 17 06 2018].

[203] «Seabrookewindows,» 09 01 2018. [En línea]. Available: http://www.seabrookewindows.com/l9W5rAXP0/. [Último acceso: 16 07 2018].

[204] «AD DS: Fine-Grained Password Policies,» 22 10 2012. [En línea]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770394(v=ws.10). [Último acceso: 15 06 2018].

[205] «CCN-STIC 821 APÉNDICE V : NORMAS DE CREACIÓN Y USO DE,» 02 2018. [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/534-ccn-stic-821-normas-de-seguridad-en-el-ens-anexo-v/file.html. [Último acceso: 18 06 2018].

[206] «Aprende a gestionar tus contraseñas,» [En línea]. Available: https://www.osi.es/es/contrasenas. [Último acceso: 18 05 2018].

[207] «CCN-STIC 950,» 04 2017. [En línea]. Available: https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2154-ccn-stic-950-recomendaciones-de-empleo-de-la-herramienta-emet-1/file.html. [Último acceso: 17 07 2018].

[208] «Bastionado de Sistemas y Servidores,» [En línea]. Available: https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-soluciones/bastionado-sistemas-y-servidores. [Último acceso: 18 07 2018].

[209] «Ecured,» [En línea]. Available: https://www.ecured.cu/Directorio_Activo. [Último acceso: 20 07 2018].

[210] «Apéndices,» [En línea]. Available: https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/plan/security-best-practices/appendices. [Último acceso: 18 07 2018].

[211] «Cyberark,» [En línea]. Available: https://www.cyberark.com/products/privileged-account-security-solution/. [Último acceso: 17 07 2018].

[212] «En qué consiste y cómo mitigar la última elevación de privilegios en Windows 8.1,» 12 01 2015. [En línea]. Available: http://blog.elevenpaths.com/2015/01/en-que-consiste-y-como-mitigar-la.html. [Último acceso: 17 04 2018].

[213] «Configuring User Rights,» [En línea]. Available: https://technet.microsoft.com/en-us/library/dd277404.aspx. [Último acceso: 12 04 2018].

[214] «What is the difference between SYN cookie, SYN cache, and SYN proxy?,» 10 12 2013. [En línea]. Available: https://security.stackexchange.com/questions/46756/what-is-the-difference-between-syn-cookie-syn-cache-and-syn-proxy. [Último acceso: 16 07 2018].

[215] C. V. Miranda, Redes telemáticas, Ediciones Paraninfo, S.A., 2014.

[216] K. Scarfone y P. Mell, «NIST National Institute os Standards and Technology,» NIST, Febrero 2007. [En línea]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf. [Último acceso: 02 07 2018].

[217] Platzi, «Maestros de la Web,» 2003. [En línea]. Available: http://www.maestrosdelweb.com/snort/. [Último acceso: 15 06 2018].

[218] M. Á. M. López, «Colección de Tesis Digitales,» 13 Agosto 2010. [En línea]. Available: http://catarina.udlap.mx/u_dl_a/tales/documentos/lem/martinez_l_ma/. [Último acceso: 01 05 2018].

[219] J. Rossi, «OSSEC Documentation,» 12 Mayo 2015. [En línea]. Available: https://media.readthedocs.org/pdf/ossec-docs/latest/ossec-docs.pdf. [Último acceso: 16 03 2018].

[220] D. C. A. H. Rory Bray, OSSEC Host-Based Intrusion Detection Guide, Syngress, 2008.

[221] «PCI Security Standards,» [En línea]. Available: https://www.pcisecuritystandards.org/. [Último acceso: 28 08 2018].

[222] «HIPAA,» [En línea]. Available: https://www.hhs.gov/hipaa/index.html. [Último acceso: 28 08 2018].

[223] «Vmware ESXi,» [En línea]. Available: https://www.vmware.com/es/products/esxi-and-esx.html. [Último acceso: 06 08 2018].

[224] A. Ramos, «Security by default,» 22 Noviembre 2012. [En línea]. Available: http://www.securitybydefault.com/2012/11/ossec-introduccion.html. [Último acceso: 11 05 2018].

[225] «Virtualbox,» [En línea]. Available: https://www.virtualbox.org/. [Último acceso: 11 05 2018].

[226] «wordpress,» [En línea]. Available: https://codex.wordpress.org/Installing_WordPress#Using_the_MySQL_Client. [Último acceso: 19 07 2018].

[227] «Netmarketshare,» [En línea]. Available: https://www.netmarketshare.com/operating-system-market-share.aspx?options=%7B%22filter%22%3A%7B%22%24and%22%3A%5B%7B%22deviceType%22%3A%7B%22%24in%22%3A%5B%22Desktop%2Flaptop%22%5D%7D%7D%5D%7D%2C%22dateLabel%22%3A%22Trend%22%2C%22attributes%22%3A%22share%. [Último acceso: 14 07 2018].

[228] «Apache,» [En línea]. Available: https://www.apache.org/. [Último acceso: 18 07 2018].

[229] «Microsoft ISS,» [En línea]. Available: https://www.iis.net/. [Último acceso: 14 07 2018].

[230] «W3techs,» 15 07 2018. [En línea]. Available: https://w3techs.com/. [Último acceso: 20 07 2018].

[231] «UNE 71504:2008,» [En línea]. Available: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0041430. [Último acceso: 27 08 2018].

[232] M. C. D. G. D. S. James M. Stewart, CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, Wiley, 2016.

[233] I. Corporation, BM Dictionary of Computing.

[234] ISACA, CISA Review Manual, 26th Edition, ISACA, 2018.

[235] «CAF,» [En línea]. Available: https://www.codeaurora.org/.

[236] «Qualcomm,» [En línea]. Available: https://www.qualcomm.com/. [Último acceso: 17 07 2018].