Universidad de Buenos Aires

Facultades de Ciencias Económicas,

Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Tema

Soluciones con Software Open Source para PyMEs orientadas a la Seguridad.

Autor: César R Bourlot

Tutor: Ing. Hugo Pagola

2019

COHORTE 2017

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADA

CÉSAR RUBÉN BOURLOT

Resumen

En muchas oportunidades, como parte de mis largos años en el rubro informático, tanto en el ámbito privado como en el estatal, he realizado implementaciones y relevamientos en PyMEs y diversos organismos donde pude apreciar que la seguridad nunca estuvo en los planes cuando se diseñó la topología de red o los sistemas que dan soporte a la infraestructura tecnológica.

En general esto se evidencia rápidamente al notar que tanto los usuarios como los servidores, sistemas de aplicaciones o bases de datos se encuentran en una misma red sin segmentación, podemos encontrar también routers hogareños dando servicio inalámbrico en esta red única, comprometiendo seriamente la seguridad de la empresa o institución. Por cuestiones presupuestarias o por desconocimiento del tema y de los riesgos a los que se exponen, estas prácticas son muy habituales y también peligrosas desde el punto de vista de la Seguridad Informática.

En este trabajo de investigación descriptivo-explicativo se pretende aportar el conocimiento necesario para ayudar a mejorar la seguridad a un costo reducido por el uso de programas de código abierto o como se lo conoce por su nombre en inglés *open source*. Existe también el software libre con algunas diferencias filosóficas que no son el objeto de este trabajo y que para el caso consideraremos en la misma categoría al referirnos al *open source*, código abierto, fuente abierta o software libre.

Palabras Clave

Seguridad Informática | Riesgos | PyMEs | Infraestructura | Topología | Costos | Open source | Software libre | Código abierto | Fuente abierta.

Ref: [1]

Índice

Declaración Jurada de origen de los contenidos **2**

Resumen **3**
Palabras Clave 3

Índice **4**

Introducción **6**

Capítulo 1 - Seguridad Informática **9**
1.1 Cuestión de principios... 9
1.2 ¿Qué debemos proteger? 9
1.3 Separación de funciones 10
1.4 ¿De qué debemos proteger la información? 12

Capítulo 2 - Red y Selección de Software **14**
Diseño 14
2.1 - Filtrado perimetral - Firewall 16
2.2 Servidor de nombres de dominio - DNS 23
2.3 Proxy 23
2.4 Red privada virtual - VPN 24
2.5 Detección/Prevención de intrusos - IDS/IPS 25
2.6 Virtualización 25
2.7 Suite de Oficina 26
2.8 Servidor de archivos o Fileserver 28
2.9 Servidor Web 29
2.10 Base de Datos BBDD 30
2.11 Servidor de Correo 31
2.12 Monitoreo de logs 32
2.13 Sistema de respaldo - Backups 33
2.14 Manejador de Eventos de Seguridad (SIEM) 35

Capítulo 3 - Cumplimiento de normas **46**
3.1 Gestión de Riesgos 46
3.2 Políticas y Procedimientos de Seguridad 48
3.3 Política de Seguridad 48
3.4 Política de Control de Accesos 49
3.5 Política de dispositivos móviles 52

Capítulo 4. - Seguridad de la plataforma **53**

Conclusiones finales **54**

Anexo 1 - El impacto financiero de la seguridad de IT en las empresas europeas **56**

Anexo 2 - Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina **58**

Anexo 3 - Encuesta Mundial sobre el Estado de la Seguridad de la Información 2018 **59**

Anexo 4 - Configuración segura de servidor Apache **60**

Anexo 5 - Configuración segura de servidor Linux. **62**

Anexo 6 - Configuración segura de Samba **64**

Anexo 7 - Configuración segura de PostgreSQL **65**

Anexo 8 - Configuración segura de Zimbra **67**

Anexo 9 - Configuración segura de OnlyOffice **68**

Glosario de términos **69**

Referencias: **71**

Introducción

Independientemente del tipo de empresa u organismo del que se trate, hay necesidad de software común a casi todos los rubros, por ejemplo la suite de oficina, que habitualmente consta de un procesador de textos, una planilla de cálculos, presentación de diapositivas, agenda, etc. Seguramente todos necesitan de un correo electrónico, un sistema de archivos compartidos, un sistema de impresión de documentos, un servidor web, un motor de base de datos, algún sistema para manejo de proyectos, algún sistema de registro de tickets, un proxy para navegación por internet, en cuanto a la seguridad está culturalmente instalado el uso de antivirus, casi como el único sistema de defensa según mi experiencia profesional, y los más previsores, hasta pensarán en un sistema de backup.

Luego en cuanto a las áreas de trabajo, comúnmente hay un área de administración, un área de ventas, de proveedores, diseño, dirección, desarrollo, informática, etc. todas estas con marcadas diferencias en cuanto a tareas y funciones, así como requisitos de software y de seguridad.

Tomando como base estas premisas vamos a ir construyendo la infraestructura informática que dará soporte a estas necesidades comunes pensando siempre en la seguridad de la información y dando prioridad al software libre como herramienta de bajo costo y excelentes resultados.

Cabe señalar que si bien el sistema operativo más utilizado en las PCs históricamente ha sido un producto de Microsoft®, ya sea Windows10®, Windows8®, Windows7®, etc, en el mundo de los servidores y en la construcción de la mayoría de los sitios de internet la supremacía absoluta la tienen los sistemas operativos Linux y el software libre que opera en los mismos.

Pero ¿qué es esto del Linux se preguntarán?, bueno en forma muy breve, Linux es un sistema operativo de fuente abierta creado por Linus Torvalds, nacido en Finlandia el 28 de diciembre de 1969, quien siendo un estudiante de Ingeniería de Software en la Universidad de Helsinki, por el año 1991

comenzó a escribir las primeras líneas de lo que en principio era un emulador de terminal MINIX (un derivado de UNIX en versión libre para universidades y centros educativos, UNIX es el sistema operativo que por aquellos tiempos daba vida a las enormes computadoras de las empresas y universidades, era un sistema operativo pago).

Torvalds sentía que le faltaban funcionalidades a la terminal MINIX y decidió crear la suya propia, y así sin saberlo comenzó lo que hoy es el Kernel o núcleo del sistema operativo que terminó tomando el nombre de Linux y que luego utilizó la licencia GPL del sistema operativo GNU de la Free Software Foundation que permite liberar y compartir libremente el código fuente. Este código fuente una vez liberado por Linus fue tomado con mucho entusiasmo por la comunidad de programadores y comenzó así su andar sumando desarrolladores de todo el mundo que contribuyen de diversas formas al crecimiento exponencial de este núcleo.

Al ser el núcleo abierto, surgieron muchas versiones de Linux, algunas de las más conocidas son Red Hat, Centos, Debian, Ubuntu, Mint, etc.

Actualmente más del 80% de la web está creada sobre servidores montados en alguna versión de Linux.

Como contraparte, la mayoría de las personas solo ha utilizado Windows® y nunca vio un servidor o no se imagina como es el funcionamiento de un centro de cómputos, datacenter o la famosa nube, ni sabe que casi todo lo que conoce como internet tiene mucho que ver con sistemas operativos Linux y software libre.

Tampoco sabe que ya es un habitual usuario de Linux, ya que el teléfono celular que lleva encima, si tiene sistema operativo Android, no es otra cosa que una versión de Linux, y así también al utilizar su televisión inteligente - *smart tv* - o el sistema multimedia de su automóvil, el enrutador - router - inalámbrico de su casa, junto con el decodificador de televisión también y otros tantos aparatos de la vida diaria que tienen un sistema embebido.

Para una mejor comprensión de la amplia variedad de temas del presente trabajo se ha dividido el mismo en 4 capítulos.

Un primer capítulo con los fundamentos de Seguridad Informática, los principios y buenas prácticas.

Un segundo capítulo que incluye el diseño topológico según esas buenas prácticas y principios, y una selección de software de uso común en empresas o instituciones, pensando siempre en la reducción de costos por medio del software libre, y las herramientas más usadas en seguridad para mitigación de riesgos y monitoreo.

Un tercer capítulo de gestión de riesgos y cumplimiento de normas, y un cuarto y último capítulo de recomendaciones y conclusiones.

Ref: [2] [3]

Capítulo 1 - Seguridad Informática

1.1 Cuestión de principios...

La seguridad informática se basa en tres principios fundamentales: confidencialidad, integridad y disponibilidad, que explicaremos a continuación, y también saber “¿que debemos proteger?”, y “¿de que debemos protegernos?”.

1.2 ¿Qué debemos proteger?

La información debe considerarse como un recurso con el que cuenta la empresa u organización, y por lo tanto tiene valor. Al igual que el resto de los activos, debe estar debidamente protegida y en esta época cada vez dependemos más de los sistemas informáticos que dan soporte a todas las áreas, siendo impensado poder trabajar sin sistemas o sin la información que éstos sustentan.

Hablamos de Seguridad Informática, pero en realidad el concepto es más ámplio y debe tratarse de Seguridad de la Información, ya que no siempre la información reside en un activo informático, y no por eso deja de ser incumbencia del área de Seguridad.

Por ejemplo, un Post-it® pegado en un monitor no tiene nada de informática, pero si el contenido escrito es un usuario y contraseña de acceso al sistema administrativo, productivo, o bancario, se trata de información confidencial, que no debe revelarse a quienes no tienen el derecho de acceso a esa información.

Por esto debemos proteger la información, la seguridad debe ser integral, y no circunscribirse solo a la informática, entendiendo por información a toda aquella documentación o dato, en cualquier tipo de soporte, ya físico, digital, magnético u óptico, que represente un activo importante para la organización.

En adelante cuando hablemos de Seguridad Informática o Seguridad de la Información ya sabemos a qué nos estamos refiriendo.
La Seguridad Informática se basa en tres pilares fundamentales que son:

Confidencialidad

Se garantiza que la información es accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad

Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento. La información debe mantenerse inalterable a efectos de no falsear su sentido.

Disponibilidad

Se garantiza que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma toda vez que se requiera.

A estos tres pilares, podemos agregar los principios de:

1.3 Separación de funciones

Deben separarse las funciones para que una misma persona no concentre el poder o privilegios sobre los datos, equipos o sistemas que contengan la información, o la posibilidad de atentar contra alguno de los pilares de la seguridad y borrar sus rastros o la evidencia de sus actividades.

Mínimo privilegio

Los permisos sobre la información no deben exceder a los estrictamente necesarios para la tarea a desarrollar, esto es por ejemplo, si una persona solo necesita la lectura de un documento, habilitar la escritura o modificación es un exceso que podría permitir al usuario alterar dicho documento o incluso borrarlo.

Necesidad de saber

Incluso cuando un determinado usuario, por sus funciones pueda tener determinado nivel de acceso a la información, hay que analizar la real necesidad de saber y limitar el acceso según este principio.

Defensa por capas

En Seguridad Informática no existe una “bala de plata” que pueda acabar con todas las amenazas, y como estas son de toda índole, siempre deben aplicarse todas las capas de defensa posibles, pensando desde los accesos físicos, hasta las diversas capas lógicas.

1.4 ¿De qué debemos proteger la información?

Las amenazas contra la información pueden ser de diversas índoles, y van desde lo fortuito hasta lo intencional, desde el exterior o interior de la organización.

Amenazas más comunes

- Ingeniería social y phishing

  La ingeniería social es un conjunto de técnicas para obtener información manipulando a los usuarios, abusando de su confianza, descuido o ingenuidad. Una de estas técnicas se llama phishing (pesca) y generalmente se realiza por medio del envío de correos falsos con links a sitios diseñados para robar las contraseñas o descargar código malicioso en la máquina del usuario.
- Denegación de servicio y Denegación de servicio distribuido.

  Este tipo de ataque atenta contra la disponibilidad de la información saturando los enlaces de internet enviando un volumen de conexiones mayores al ancho de banda disponible y haciendo que las consultas o conexiones legítimas no sean posibles, o saturando los recursos de los servidores, obteniendo el mismo efecto.
- Ataques de contraseñas.

  Se le llama ataque de diccionario, cuando precisamente se utilizan estos para probar combinaciones de usuario y contraseña, existen diccionarios temáticos o con las contraseñas estadísticamente más utilizadas, así como las bases de datos que circulan en el mercado negro con las combinaciones de usuario y clave robadas en sitios de uso masivo. También existen los denominados ataques de fuerza bruta, probando todas las combinaciones posibles hasta obtener resultados. Con el poder de cómputo actual y el aumento exponencial del ancho de banda promedio para las conexiones de internet los ataques de contraseñas se hacen muy fáciles y rápidos cuando no

hay protecciones adecuadas o no se diseñan de forma adecuada los login de las aplicaciones.

- Control Remoto de equipos y backdoors

  De la mano del spam y el phishing suelen venir archivos adjuntos o enlaces a páginas donde se descargan archivos maliciosos con algún tipo de virus troyano diseñados para abrir puertas traseras o backdoors y establecer un control remoto del equipo por parte del atacante.

- Escaneo de puertos.

  El escaneo de puertos forma parte del proceso básico de reconocimiento de servicios activos por parte del atacante que tratará de determinar el tipo de sistema operativo que utilizamos y que software corremos , así como su versión, en búsqueda de vulnerabilidades conocidas para intentar explotarlas.

- Exploits.

  Los exploits son porciones de código malicioso diseñado para aprovechar una determinada vulnerabilidad muy específica en un software utilizado por la víctima, por lo general se ataca al navegador, a la suite de oficina, o visor de documentos PDF, entre otros.

- Virus/malware/ransomware

  Son programas maliciosos creados para cumplir con un objetivo en la PC de la víctima y a la vez propagarse o infectar a otras PC que se encuentren en la misma red. Cuando los virus tienen la propiedad de propagarse e infectar otros sistemas sin la intervención del usuario son llamados gusanos, y es la técnica que fue muy utilizada por algunos ransomware últimamente y su propagación es muy rápida y efectiva.

Capítulo 2 - Red y Selección de Software

Diseño

Ahora comencemos por el diseño o topología de red de nuestra infraestructura.

Esto es algo básico ya que de un buen diseño depende en gran medida la eficacia y eficiencia de las protecciones de seguridad que diseñaremos para cubrir nuestras necesidades.

Dividiremos la red interna en varias subredes que llamaremos DMZ o zonas de-militarizadas, donde lo interno o perteneciente a ese grupo se considera confiable o del mismo nivel de incumbencia, y todo lo externo a la DMZ se considera hostil o desconocido. Así surge un área donde alojaremos los servicios que estarán expuestos hacia internet, como por ejemplo nuestro servidor web, el servidor de correo, o el proxy que permite la navegación, que llamaremos DMZ-Externa.

Nuestros servicios internos, por ejemplo donde se aloja la intranet, servicios de impresión, servidor de archivos compartidos, etc, que llamaremos DMZ-Corporativa, podemos colocar en una DMZ separada por ejemplo a nuestro motor de Base de datos, que llamaremos DMZ-BBDD.

Si tuviéramos áreas del tipo de desarrollo por ejemplo podríamos crear una DMZ a este efecto donde tendríamos los servidores de desarrollo para que no se mezclen con los de producción. Para este mismo caso se crearía también una división en testing, y una de producción. Seguramente una DMZ-WiFi donde aislamos los routers inalámbricos. En fin, podemos crear tantas DMZ como sean necesarias basándose en el principio de separación de funciones.

Luego tendremos un área de usuarios que se llama habitualmente LAN, que puede también a su vez subdividirse según sus funciones, por ejemplo, gerencia, administración, RRHH, operaciones, informática, seguridad, etc.

Cada una de las divisiones de redes que hagamos en subredes se verá reflejada en la topología configurada en el Firewall, y la función de este es controlar todas las comunicaciones entre las distintas DMZs o divisiones de LANs. De esta forma tendremos el control de todo el tráfico de paquetes en la red. Se deberán crear reglas en el firewall consignando en la interfaz donde se origina la comunicación cuál es el origen y cual es el destino de la misma, y por qué puertos se establece, además del tipo de protocolo.

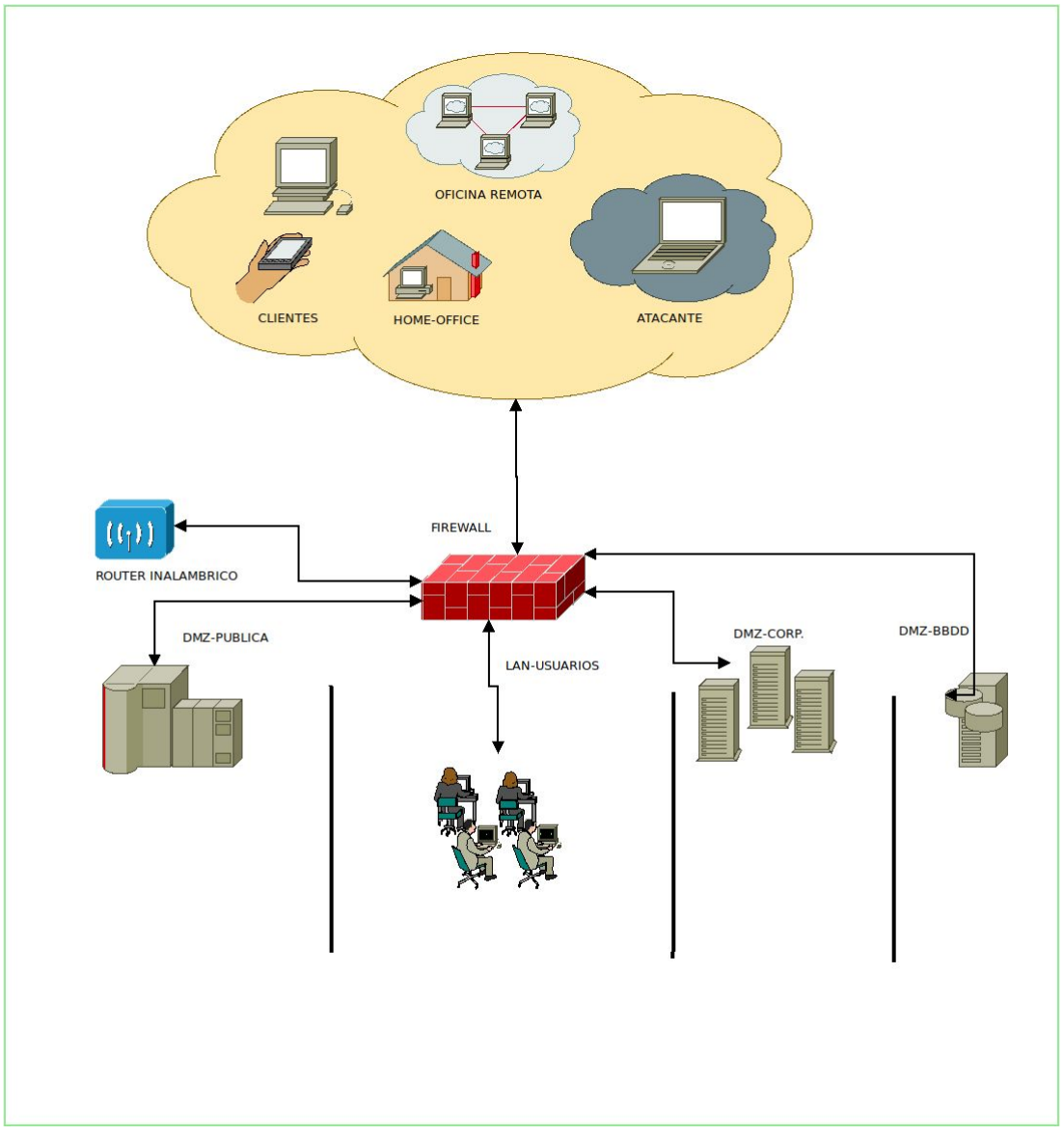


Fig. 1 - Diseño de red - segmentación

2.1 - Filtrado perimetral - Firewall

El Firewall es el corazón de una red pensada bajo principios de seguridad, comenzando por separar las áreas en subredes que necesitan de un permiso específico para interactuar y nos permite de esa forma tener el control de quién puede acceder a qué recurso, cuando, y por que puertos o servicios. Esto es acorde a los principios de necesidad de saber, separación de funciones y confidencialidad.

Como buena práctica debería haber al menos tantas subredes en el firewall como áreas en la empresa, y digo al menos porque seguramente veremos que serán más.

El objetivo de esta segmentación es la separación a nivel informático de las áreas de incumbencia, ya sea para mejor control de los permisos de accesos como de la contención de daños en caso de producirse algún tipo de intrusión. Con esto quiero decir por ejemplo una persona del área de diseño no tendría necesidad de acceder al sistema de liquidación de sueldos, y por el contrario, todas las personas del área contable si necesitan ese acceso. Si alguien del área de desarrollo tuviera un virus del tipo gusano en su PC, este quedaría contenido en ese sector, disminuyendo la posibilidad de propagarse a las otras áreas. Es muy importante configurar el firewall en modo restrictivo, para tener control de las conexiones entrantes y salientes.

Para el caso, y por mi experiencia personal, encuentro particularmente adecuada la solución que brinda PFSense, por su facilidad de instalación, uso y cantidad de funciones disponibles y flexibilidad. Este firewall cuenta con una comunidad de usuarios grande y activa donde puede encontrarse mucha ayuda a todo tipo de situaciones o problemas. Tiene la ventaja de poder integrar varios de los sistemas necesarios, por ejemplo DNS, Proxy, IPS, VPN,etc. Trabajo con este firewall desde hace más de 6 años, con una carga intensa y miles de reglas y objetos de filtrado. Está construído sobre FreeBSD, que es el sistema operativo de opensource con la más alta

reputación, estabilidad y confiabilidad en lo que respecta a seguridad. Está preparado para ser escalable, y puede ser configurado en clusters para alta disponibilidad, lo que hace posible por ejemplo realizar actualizaciones completas de software y sistema operativo en caliente, actualizando un nodo a la vez.

PFSense cuenta con una amplia gama de paquetes de software que pueden integrarse en una misma consola administrativa y manejar desde ahí buena parte de la infraestructura informática de base y que da soporte al resto de los sistemas.

Entre otros sistemas, integra LDAP y Radius como módulos para autenticación, Bind como servidor DNS, Squid como Proxy, SquidGuard para filtrar por sitios, categorías y reglas, soporta IPSec y Openvpn precisamente para hacer Redes Privadas Virtuales, puede incorporar ClamAV como antivirus para sumarse al Proxy, Suricata y Snort se pueden agregar para hacer inspección de tráfico y funcionar como IDS/IPS. Estos son solo algunos de los muchos paquetes que se pueden integrar y están disponibles en forma totalmente gratuita y se instalan sencillamente seleccionandolos de un listado.

Prueba de concepto:

www.PFSense.org

Instalando PFSense sobre una máquina virtual creada en Virtual Box de Oracle®, con 4 interfaces de red, 2 GB de memoria Ram, 120 mb de memoria de video, y 8GB de disco para reproducir el entorno que recomendamos a modo de ejemplo en el diseño.

Ref: [4]

Montamos la imágen de disco de PFSense (.iso) descargada para este ejercicio desde:

https://nyifiles.PFSense.org/mirror/downloads/PFSense-CE-2.4.4-RELEASE-p3-amd64.iso.gz

y al bootear nos encontramos con este menú de opciones:

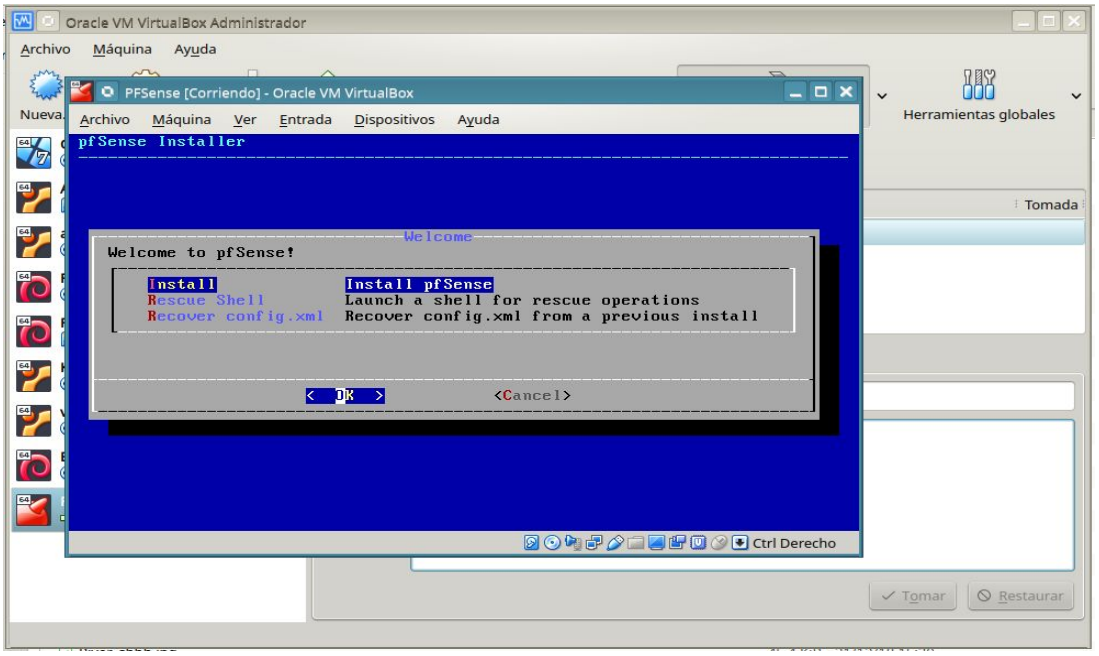


Fig.2 Boot desde la unidad de CD de la máquina virtual.

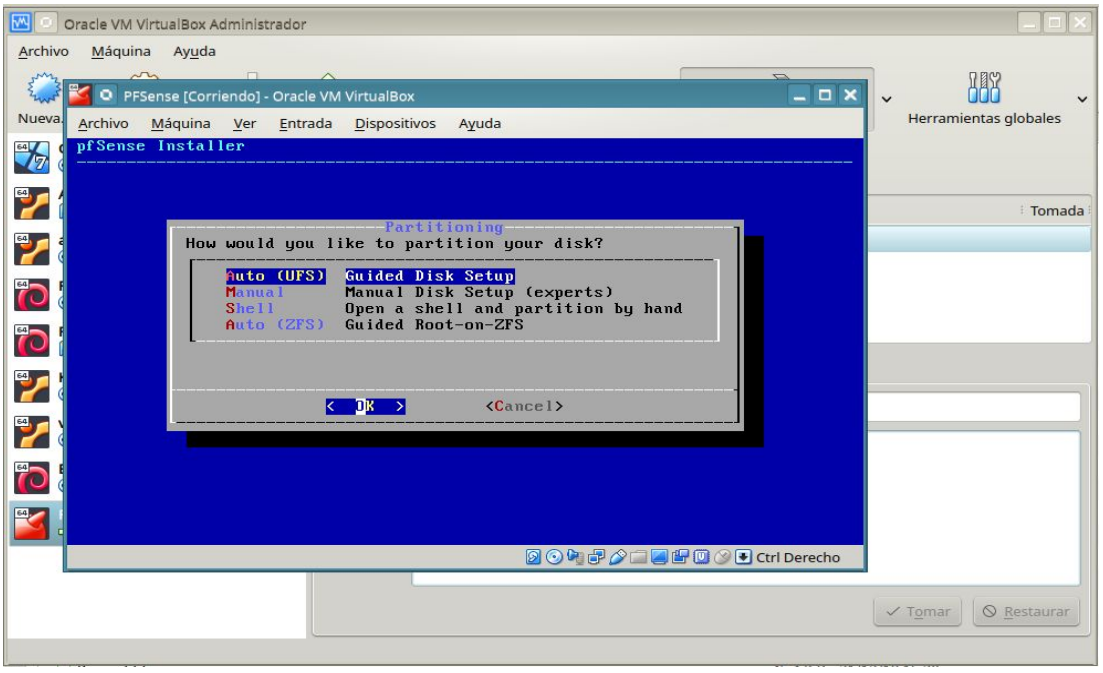


Fig.3 Selección setup de disco guiado

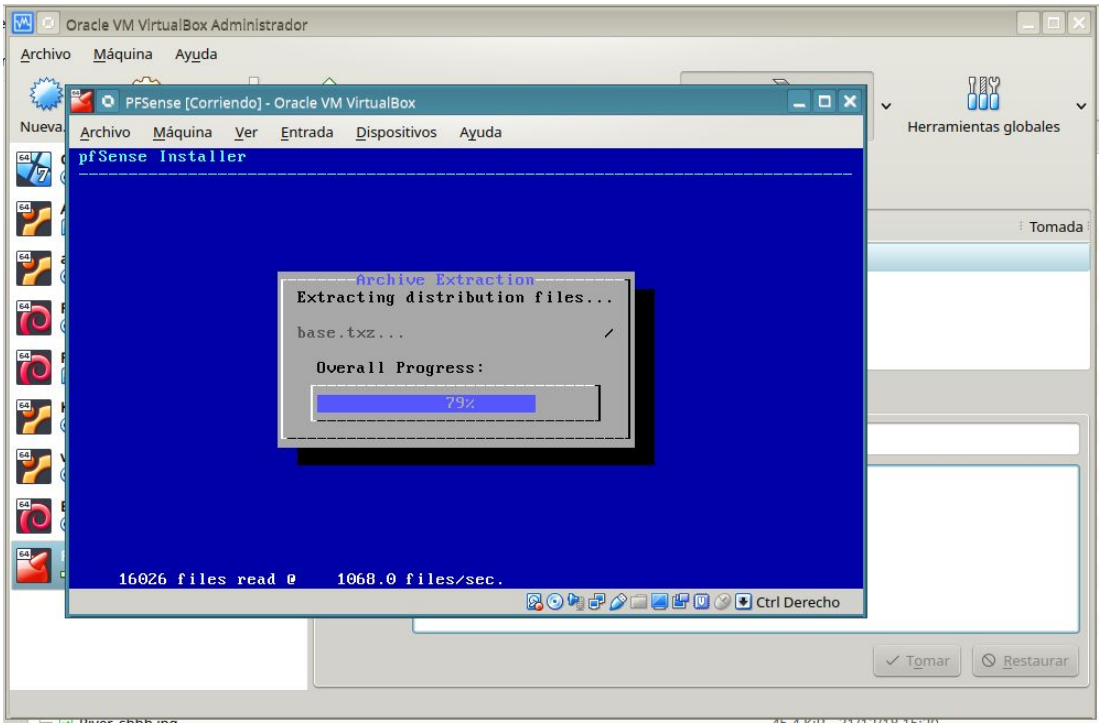


Fig.4 Progreso de la instalación.

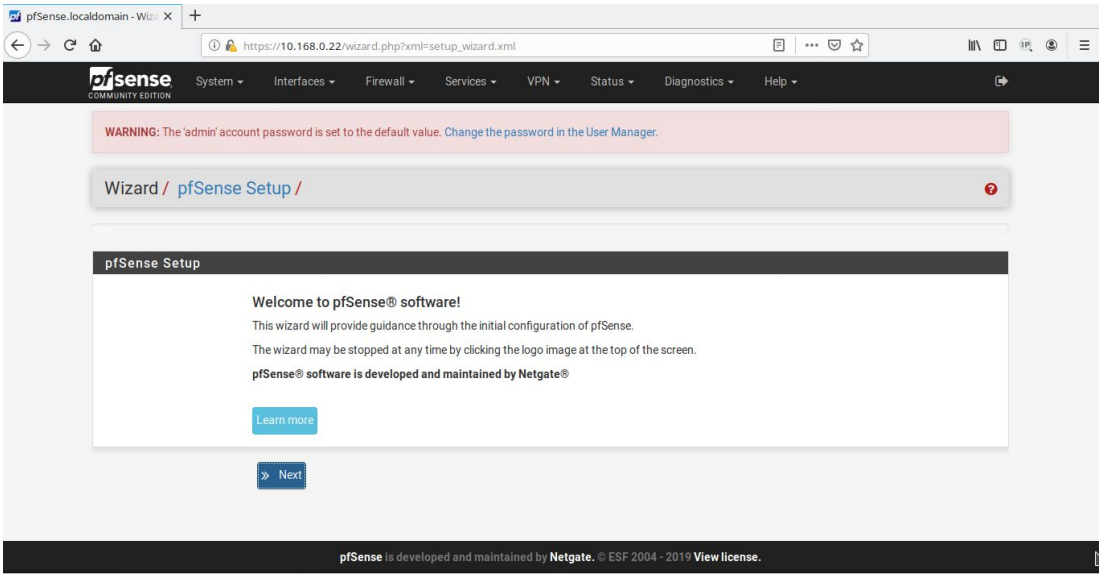


Fig.5 Finalizando la instalación.

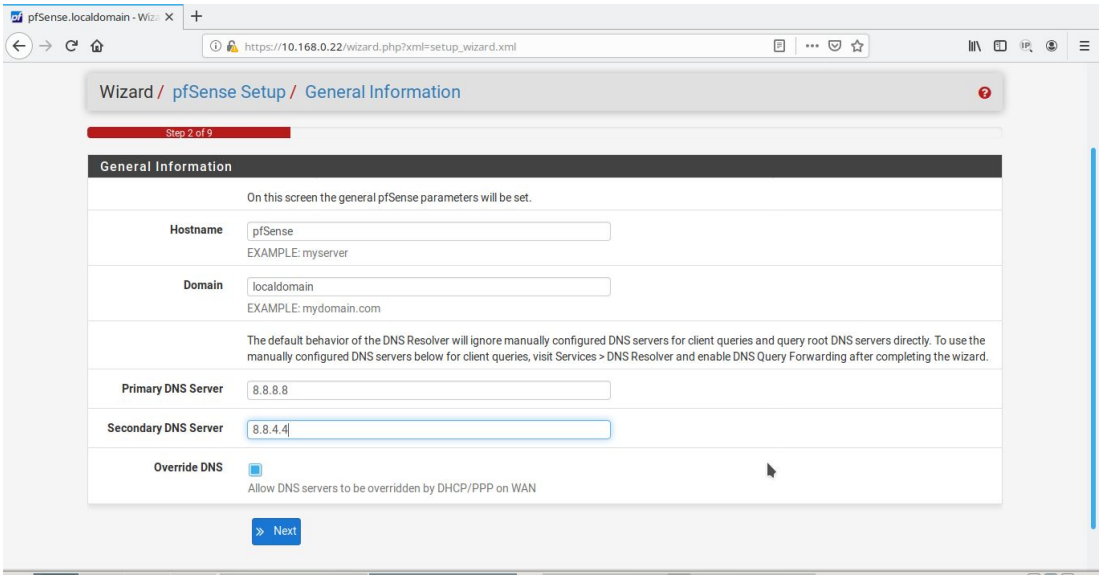


Fig.6 configurando DNS públicos.

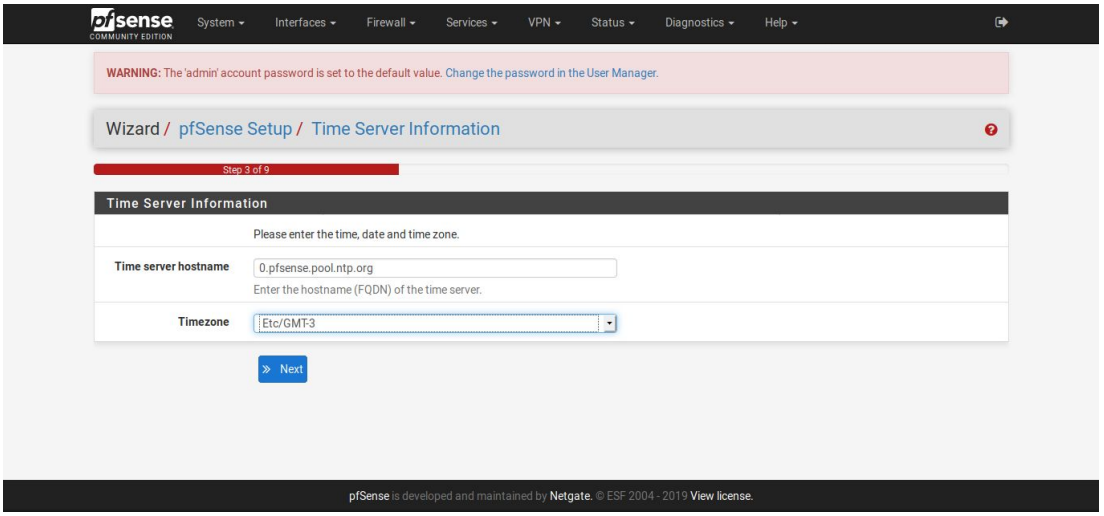


Fig.7 configurando servidor de hora.

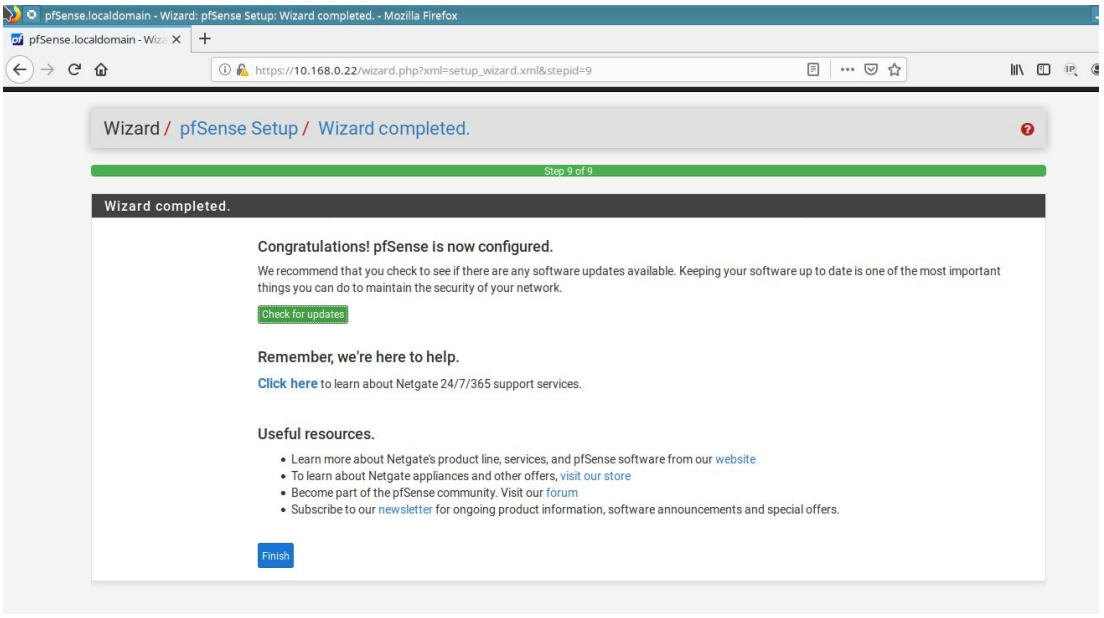


Fig.8 Instalación finalizada.

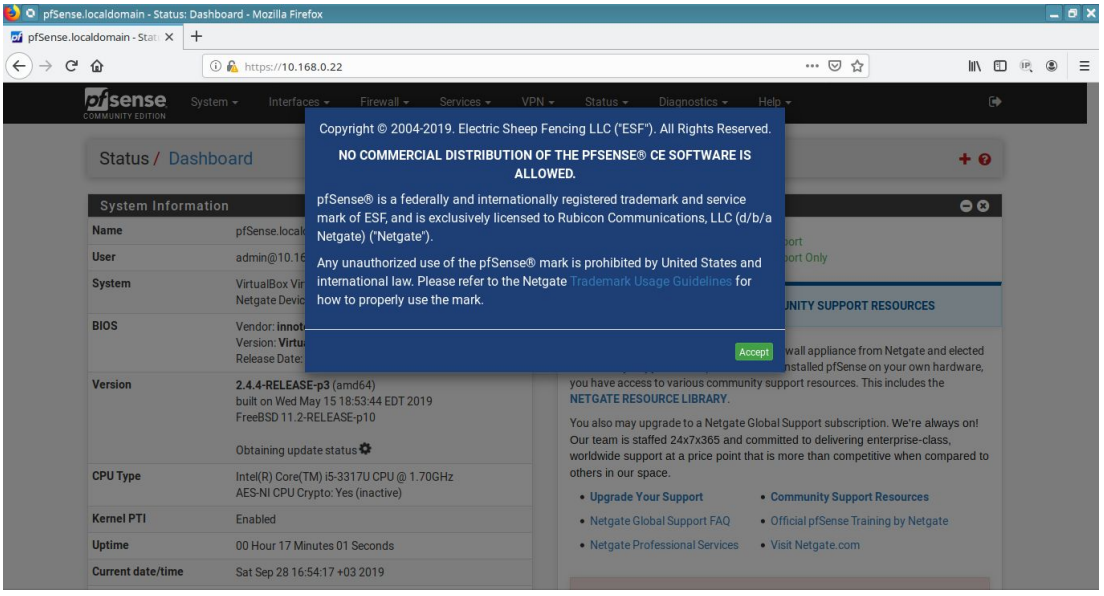


Fig.9 Primer ingreso desde el administrador web.

Hasta acá la instalación básica, bastante simple, siguiendo el proceso automático y solo completando pocos campos, por ejemplo el de ubicación para establecer fecha y hora del sistema.

Como la máquina virtual solo admite hasta 4 interfaces de red y en este ejemplo vamos a configurar algo más de 4, aprovechando para mostrar la forma de crear interfaces virtuales en el PFSense.

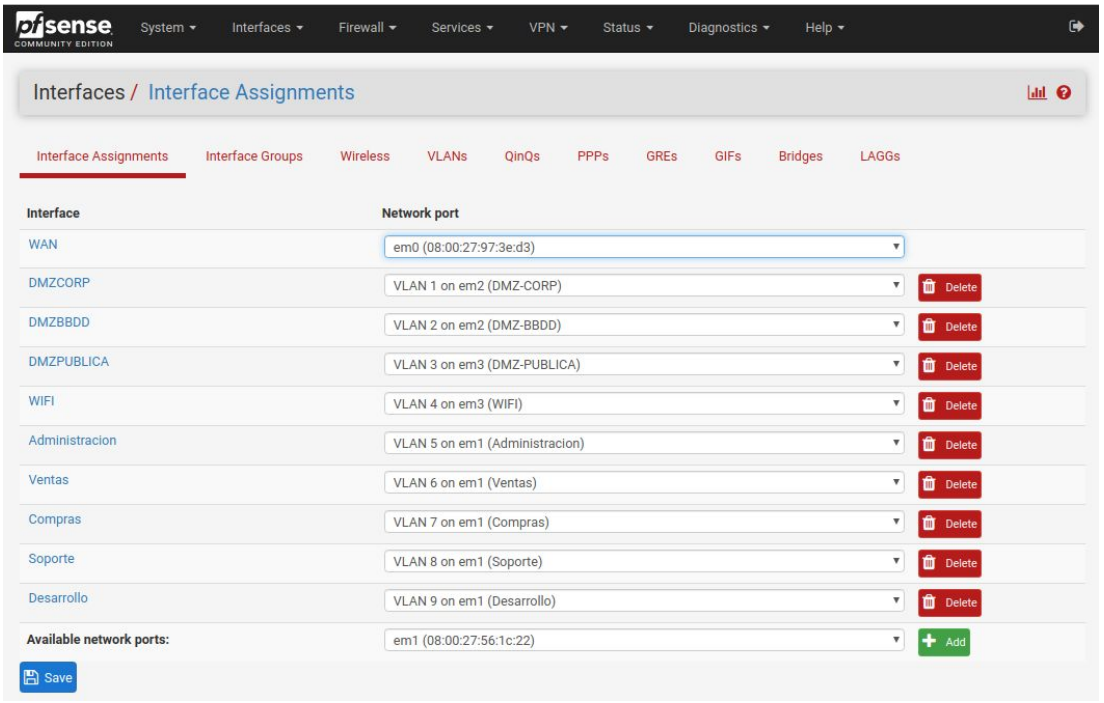


Fig.10 Creación de VLANs y asignación a las interfaces.

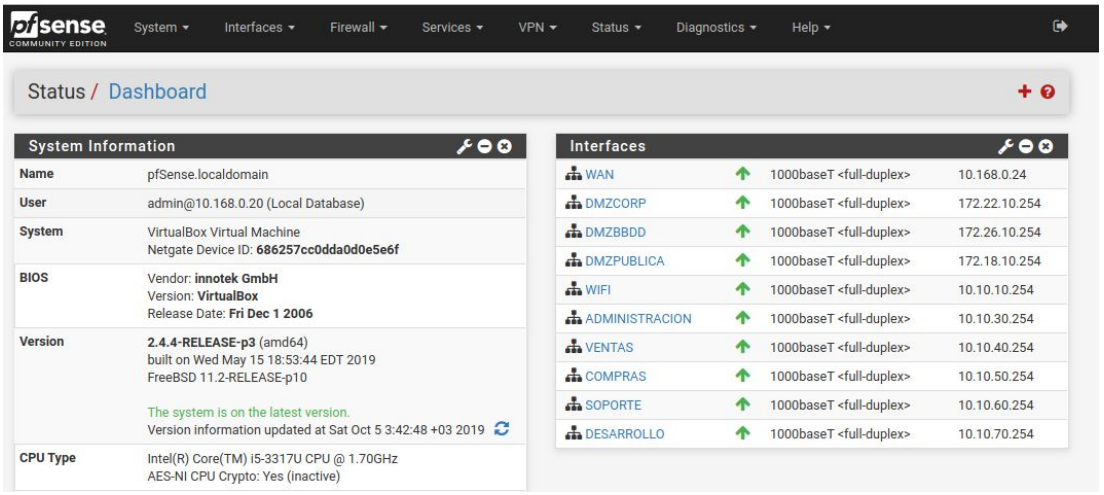


Fig.11 Tablero principal - DMZs creadas con sus VLANs.

Para crear las interfaces virtuales en PFSense primero debemos crear las VLAN, con un nombre y número de vlan, y seleccionar una de las interfaces “físicas” con las que cuenta el equipo. Pongo entre comillas el término físicas porque el software lo entiende de esta manera, aunque sabemos que en realidad también son virtuales como todo el hardware de este firewall que fue creado en VirtualBox. Una vez creada la Vlan, en la pestaña de Interface Assignment utilizamos el botón de agregar, y aparecerá dentro de las opciones la recientemente creada para seleccionar y agregar la interfaz virtual.

2.2 Servidor de nombres de dominio - DNS

Dentro de los servicios esenciales de cualquier red se encuentran los DNS, este servicio está incorporado en el FPSense y es de fácil configuración.
Servidor de nombres de dominio, es el sistema encargado de hacer la traducción de los nombres de los objetos buscados a su correspondiente dirección de IP. Por ejemplo cuando un usuario escribe una url en su navegador http://www.google.com el navegador consulta al DNS para saber a qué dirección IP debe dirigirse, y este le devolverá por ejemplo 172.217.30.132 para el caso de google argentina.
En la configuración se indican los servidores de nombres públicos, para que el sistema pueda resolver los nombres en internet, y permite también generar un registro interno de los nombres y las direcciones IP de los servidores, usuarios, impresoras, etc. que corresponden a nuestro dominio.

Ref: [5]

2.3 Proxy

El servicio de Proxy es el encargado de proveer la navegación a los usuarios, reduciendo el uso de ancho de banda y permitiendo el filtrado y control sobre las categorías de sitios permitidos. Para esto el PFSense incorpora el paquete de Squid, un reconocido software de proxy que se encarga de intermediar entre los requerimientos del usuario y los sitios de internet, adicionalmente podemos agregar el paquete de SquidGuard para filtrar los destinos por categorías permitidas/prohibidas mediante listas que se actualizan diariamente de forma gratuita y automática. Cabe señalar que estos softwares forman parte muchas veces de soluciones comerciales de proxy que se venden en el mercado. Un plus es la posibilidad de incorporar el antivirus en línea con la navegación, habilitando ClamAV para inspeccionar en busca de virus directamente en el proxy.
La configuración de Squid como software de proxy por si sola se encuentra en un archivo de texto plano llamado squid.conf donde se declaran todos los

parámetros, que son muchos y muy variados, ya que se trata de un software muy flexible y de gran madurez programática. Este programa se encuentra ampliamente documentado dentro del mismo archivo de configuración, todos los parámetros tienen comentarios sobre su funcionalidad y formas de uso, pero carece de una interfaz de configuración propia, cosa que resuelve muy bien el paquete de PFSense donde incluye en la sección de servicios el acceso a la configuración de Squid Proxy, previamente se debió incluir a Squid y a SquidGuard como paquetes adicionales.

Ref: [6] [7]

2.4 Red privada virtual - VPN

Por estos tiempos es muy común el trabajo remoto, o home office, así como las sucursales o puntos de venta. Para este caso es de gran utilidad el uso de Redes Privadas Virtuales, o VPN. PFSense incorpora OpenVPN e IPSec como solución. En el caso de sucursales que requieren de una conexión permanente resulta muy práctico el uso del protocolo IPSec para realizar una conexión site-to-site, que puede realizarse contra otro PFSense instalado en dicha sucursal o cualquier otro dispositivo de ruteo que entienda el protocolo.

Para el caso del trabajo remoto, vendedores viajantes, o road-warriors resulta muy práctico el uso de OpenVPN, que entre sus ventajas de seguridad en la comunicación agrega una forma fácil de instalación para el usuario cliente, incluyendo un certificado personal para su identificación, para el caso de usuarios con sistema operativo de Microsoft ® genera un archivo ejecutable con el certificado y la configuración completa embebida que resulta muy práctica, el usuario solo debe proveer la contraseña para realizar la conexión.

En mi experiencia, y siguiendo las buenas prácticas, resulta muy beneficioso activar el uso de OTP (One Time Password o Contraseña de única vez) que es soportado por OpenVPN y que puede utilizarse en conjunto con Google Authenticator por ejemplo, aportando un segundo factor al login. Ref:[8]

2.5 Detección/Prevención de intrusos - IDS/IPS

IDS (Intrusion Detection System) o sistema de detección de intrusiones es un software que analiza todo el tráfico de red, entendiendo una gran diversidad de protocolos, puede encontrar en los paquetes de datos porciones de código llamadas firmas, que tiene registrada en su base de datos como maliciosas, o determinar patrones anómalos de comportamiento en base a estadísticas. El IDS permite dar visibilidad de lo que pasa en la red, tiene sus interfaces configuradas en modo promiscuo para capturar todas las comunicaciones.

El IPS (Intrusion Prevention System) sistema de prevención de intrusiones se encarga precisamente de eso, prevenir las intrusiones tomando acciones inmediatas ante la detección de una anomalías, funciona de la misma forma que el IDS, pero además de alertar también reacciona. El más utilizado para estas tareas es Suricata que puede configurarse como IDS o como IPS indistintamente. También es un software open source y puede agregarse como funcionalidad en el mismo Firewall PFSense. De la misma manera podemos agregar el paquete de Snort con las mismas funcionalidades de detección y prevención de intrusiones.

Ref: [9]

2.6 Virtualización

Los datacenters modernos grandes o pequeños hoy en día se encuentran completamente virtualizados, esto es crear hardware virtual en base a software sobre hardware físico, que puede reunirse en cluster y sumar recursos para optimizarlos en una plataforma llamada Hipervisor. Existen varios sistemas Hipervisores open source, entre ellos, Open Stack, Virtual Box, Proxmox, Xen, etc.

La virtualización permite crear servidores o máquinas virtuales e instalar en ellas sistemas operativos y softwares tal como si fueran máquinas físicas, con ventajas administrativas muy grandes, posibilidad de copiado,

redundancia, migración, actualización, crecimiento, etc. Se comparten los recursos de memoria, cpu, discos, redes, de forma de lograr una diferencia cuantitativa de servidores virtuales respecto de los servidores físicos.

EL líder del mercado en virtualización de VMWare ®, pero el costo de su licencia es privativo para la mayoría de las pequeñas y medianas empresas.

Una vez elegido un sistema de virtualización solo resta crear el Datacenter virtual, dándole un nombre, y a partir de allí comenzar a crear las máquinas virtuales que se colocarán en las distintas subredes conforme a nuestro propio diseño.

Ref: [10] [11] [12] [13]

2.7 Suite de Oficina

La suite de oficina es un elemento muy utilizado y la mayoría de las distribuciones de Linux vienen con el paquete de Libreoffice instalado, que incluye un sistema para escribir documentos, una planilla de cálculos, una herramienta de presentaciones, un editor matemático, editores de texto, etc.

Esta suite es compatible con la mayoría de lo producido con MS Office de Microsoft ®, y puede exportar los documentos en múltiples formatos, tanto de MS como PDF o formatos abiertos en XML.

También existen una alternativas a las suites de oficina “en la nube” que son cada vez más utilizados, como Google Docs ® , u Office 365 ®. El primero gratuito, el segundo es pago.

Estos sistemas tienen la gran ventaja de permitir editar los documentos o planillas de cálculo desde cualquier conexión a internet, y sin tener que llevar encima dichos documentos, sino que solo se acceden desde su propia cuenta de usuario.

Otra gran ventaja es la posibilidad de realizar trabajo de edición colaborativo y en simultáneo.

Son todas ventajas a pesar que las funcionalidades y herramientas son algo más limitadas que las del software que se utiliza de forma local, sirven para la mayoría de los trabajos. Sin embargo un tema no menor en estos

sistemas es la privacidad, ya que los documentos residen “en la nube” y están fuera de nuestro control, y cuando se tratan de documentos que puedan darnos una ventaja competitiva o cualquier tipo de datos sensibles de la empresa cuya exposición nos crearía graves inconvenientes, entonces estas grandes ventajas comienzan a ser seriamente cuestionadas.

Para el caso encontré muy conveniente OnlyOffice, un software open source que tiene las mismas funcionalidades y ventajas antes mencionadas y que además podemos instalar en nuestra propia “nube”. Permite la edición en simultáneo o trabajo colaborativo, Chat entre los participantes, agrega un manejador de proyectos muy interesante, un CRM, un Calendario y un cliente de Correo electrónico.

Tiene varias formas de instalación e incluso una muy fácil utilizando la nueva tecnología de docker o contenedores.

Fig. 12 Pantalla principal de OnlyOffice.

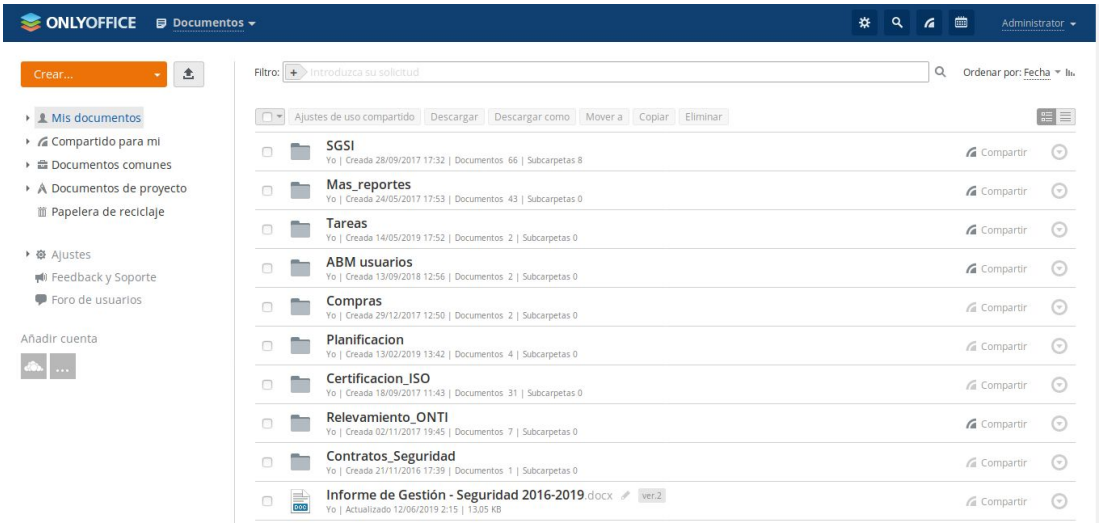


Fig.13 Listado de carpetas en OnlyOffice.

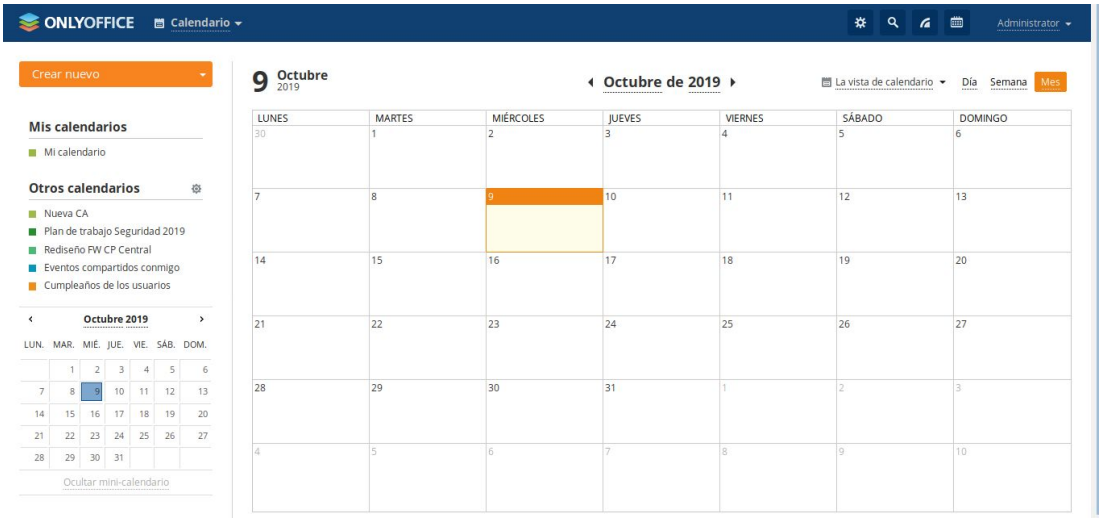


Fig.14 Calendario de OnlyOffice.

Ref: [14] [15]

2.8 Servidor de archivos o Fileserver

Ante la necesidad de compartir archivos dentro de la organización puede utilizarse para este fin un viejo y conocido software llamado Samba que permite compartir archivos organizados en carpetas que pueden ser anidadas, compartir carpetas enteras, otorgar distintos niveles de permisos, ejecución, lectura, escritura, copiado, borrado, etc. Con la suite de oficina Onlyoffice (que también permite compartir y organizar los documentos y permisos de acceso a los mismos) se reduce considerablemente la

necesidad de utilizar un fileserver, al menos en lo que respecta al almacenamiento y administración de documentos, planillas de cálculo, presentaciones de diapositivas, etc.

Samba utiliza el mismo protocolo de compartición de archivos que Windows® (smb), y facilita la interoperabilidad entre win y linux, permitiendo la validación de usuarios tanto desde un controlador de dominio de MS como desde un LDAP por ejemplo.

Ref: [16]

2.9 Servidor Web

En cuanto a servidores web las elecciones pueden ser varias, el más utilizado es Apache, seguido por Nginx y Tomcat, dependiendo del lenguaje utilizado para desarrollar el sitio web, ya sea una web pública o una intranet.

En cualquier caso la instalación de estos softwares es muy sencilla en linux y solo requiere de un par de comandos. Por ejemplo estos para Apache:

```
root@server:~# apt-get install apache2 apache2-doc
```

y luego para lanzar el servidor ejecutar:

```
root@server:~# service apache2 start
```

Arranca el servidor web HTTP mostrando su típica página de bienvenida a continuación.

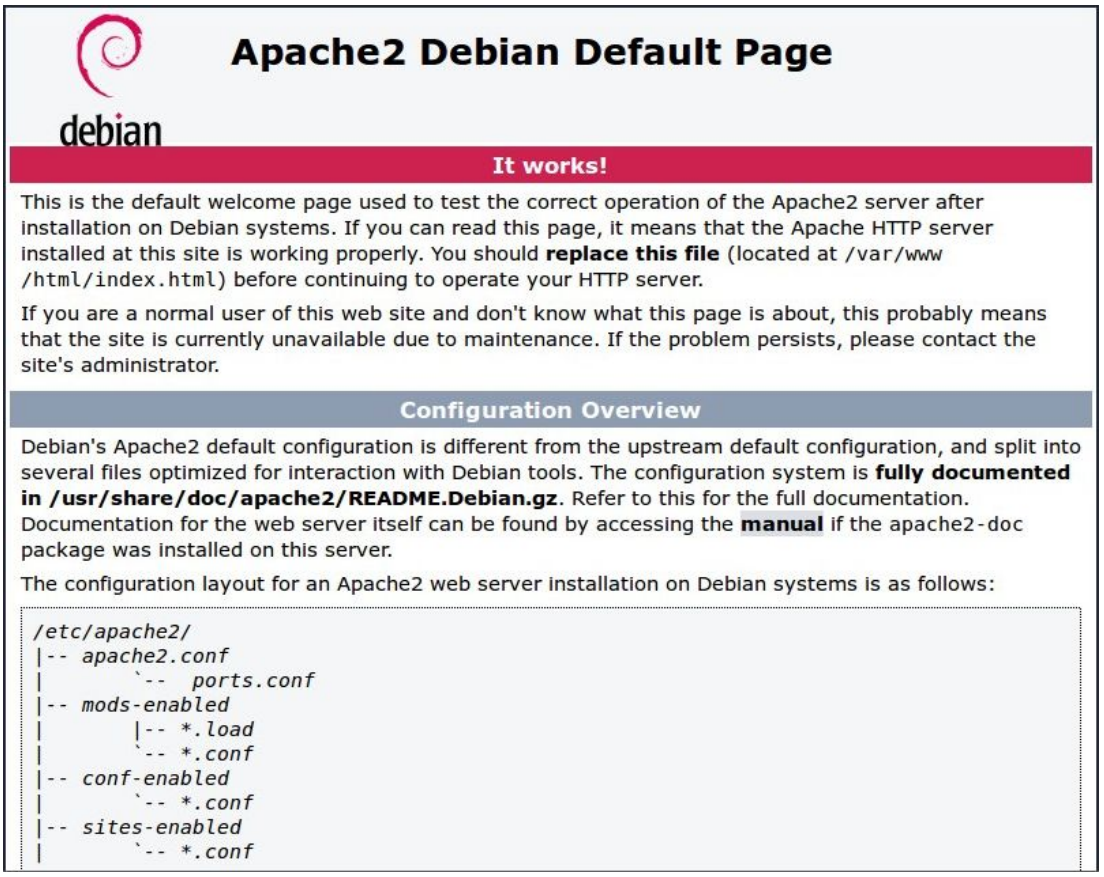


Fig. 15 Página por defecto de servidor web Apache Ref:[17]

2.10 Base de Datos BBDD

Habitualmente las páginas web o servicios varios dentro de las empresas requieren de una base de datos para el almacenamiento de registros. Existen muchos motores de base de datos open source, siendo los más conocidos y utilizados PostgreSQL, MySQL y su derivado MariaDB.

Para instalar Postgres en un servidor Debian o derivado, basta con ejecutar el siguiente comando:

```
root@server:~# apt-get install postgresql-all
```

Un gran complemento para administrar esta base de datos en Postgres es el PGAdmin, cuya instalación es también trivial en un servidor Debian o derivado:

```
root@server:~# apt-get install pgadmin3
```

En el caso del PGAdmin, se trata de una GUI o interfaz gráfica para la administración de la Base de Datos.

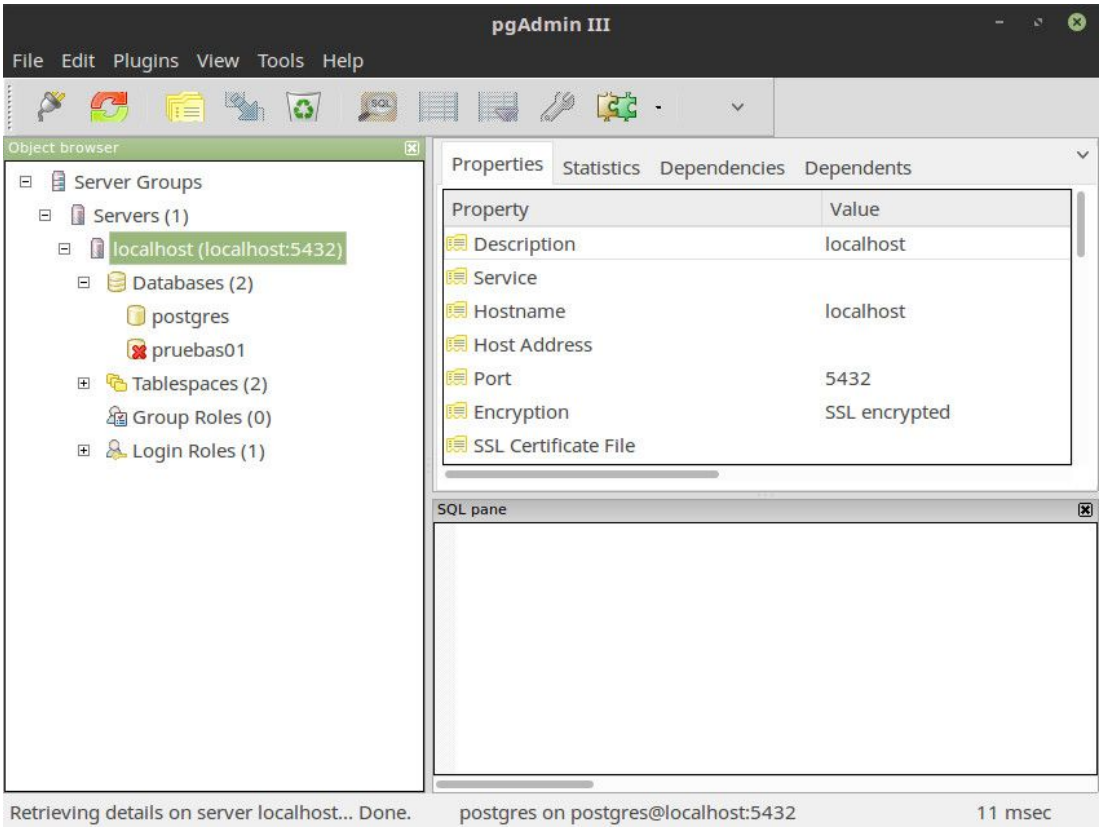


Fig.16 pgAdmin III conectado a una BBDD Postgres SQL. Ref: [18]

2.11 Servidor de Correo

Existen varios servidores de correo en Linux, el más popular y utilizado es Postfix, no obstante por su facilidad de manejo e instalación encuentro muy recomendable la versión Community de Zimbra. Este servidor de correo incluye un frontend web tanto para la administración del server como para el uso diario, donde se puede organizar el correo en diferentes carpetas, crear filtros, utilizar firmas, utilizar certificados para firma digital y cifrado. También integra un calendario y un To-Do list o listado de pendientes. Entre otras ventajas, la programación del frontend es “responsible”, lo que significa que puede detectar si se está accediendo desde un celular o tablet y mostrar la versión móvil en ese caso, además de contar con una aplicación en los repositorios de Android o Apple, y versiones de cliente para escritorio en diferentes sistemas operativos para quien prefiera esta opción en lugar de utilizar un navegador web.

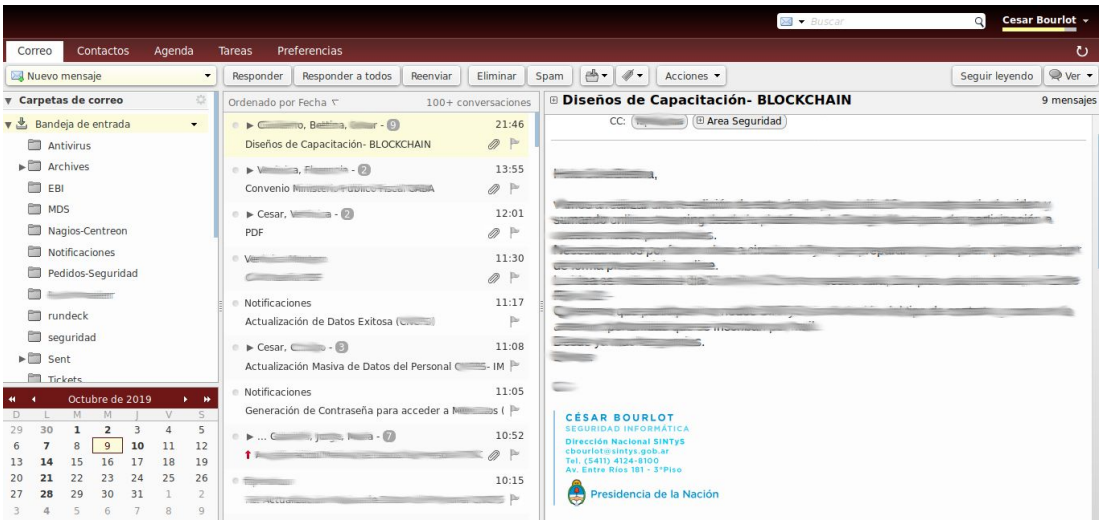


Fig.17 Pantalla de correo Zimbra web Ref: [19]

2.12 Monitoreo de logs

En Seguridad Informática es fundamental el monitoreo de logs de los distintos sistemas, y para esta tarea contamos con una herramienta muy potente donde se integran tres softwares a saber: Elasticsearch, Logstash/Beats y Kibana, que funcionan en perfecto ajuste.

Este conjunto de programas es conocido como ELK Stack. El stack es una pila, donde en la base se encuentran Logstash y Beats, que se encargan de recibir los logs provenientes de los distintos servidores o servicios.

Encima de esta base se encuentra Elasticsearch, que es un motor de búsqueda analítica, basado en Json, y por arriba de todos está el Kibana que es la interfaz de usuario y visualización.

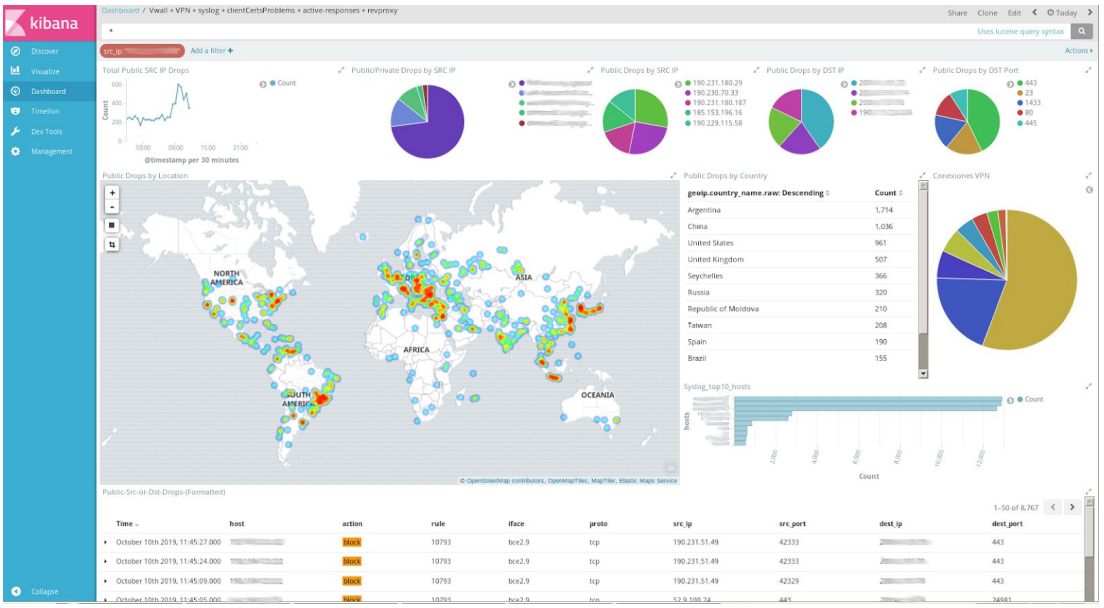


Fig.18 Tablero de Kibana representando logs de bloqueos del firewall

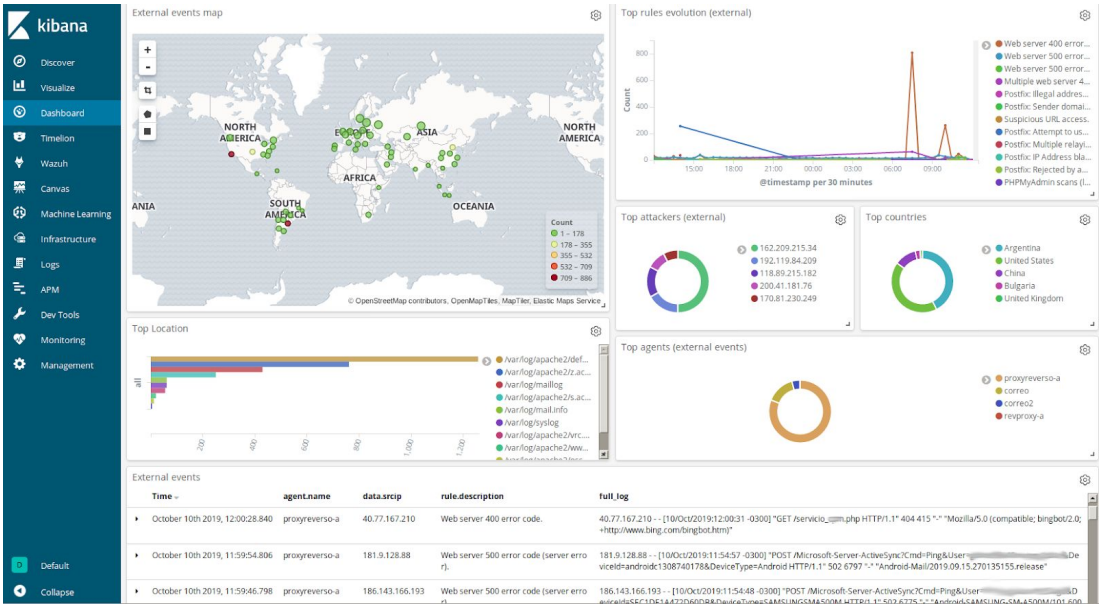


Fig.19 Tablero de Kibana representando logs de Apache y OSSEC. Ref: [20]

2.13 Sistema de respaldo - Backups

El más conocido y utilizado para esta tarea es Bacula. Este software tiene todas las funcionalidades de backup necesarias incluso para grandes centros de cómputo. Permite programar las tareas de respaldo según una agenda, haciendo backups incrementales o totales, en diferentes medios,

cinta o disco, realizando el indexado en catálogos y recuperación de los datos ante una contingencia o restore de rutina.

También incluye una app para administración desde dispositivos móviles.

Es un sistema cliente-servidor, o sea requiere de agentes instalados en los servidores o PCs que se desean respaldar, y un servidor de backup propiamente que controla y administra las librerías de cintas o medios de respaldo, con sus respectivos catálogos y base de datos. Este sistema no es de fácil configuración para usuarios sin el conocimiento necesario, pero es uno de los más ricos en funciones deseadas en un manager de backups.

Ref: [21]

Imágenes del sitio oficial. Tablero principal.

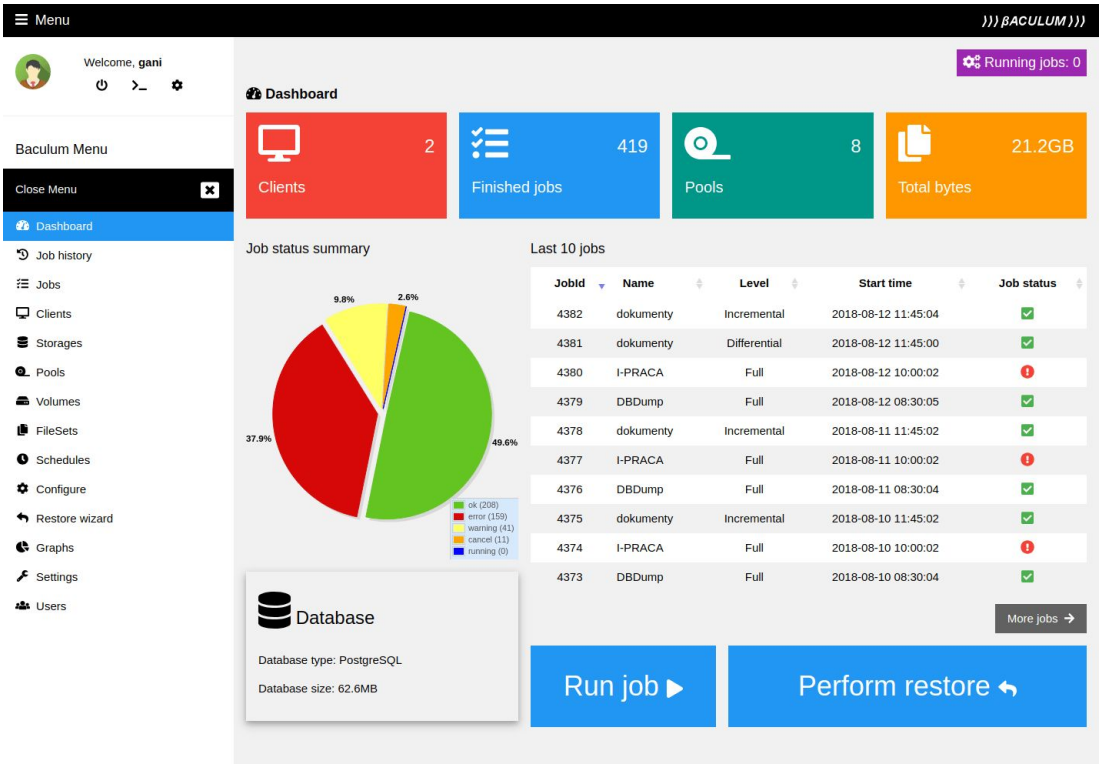


Fig. 20 Tablero principal de Bacula.

Aplicación para dispositivos móviles.

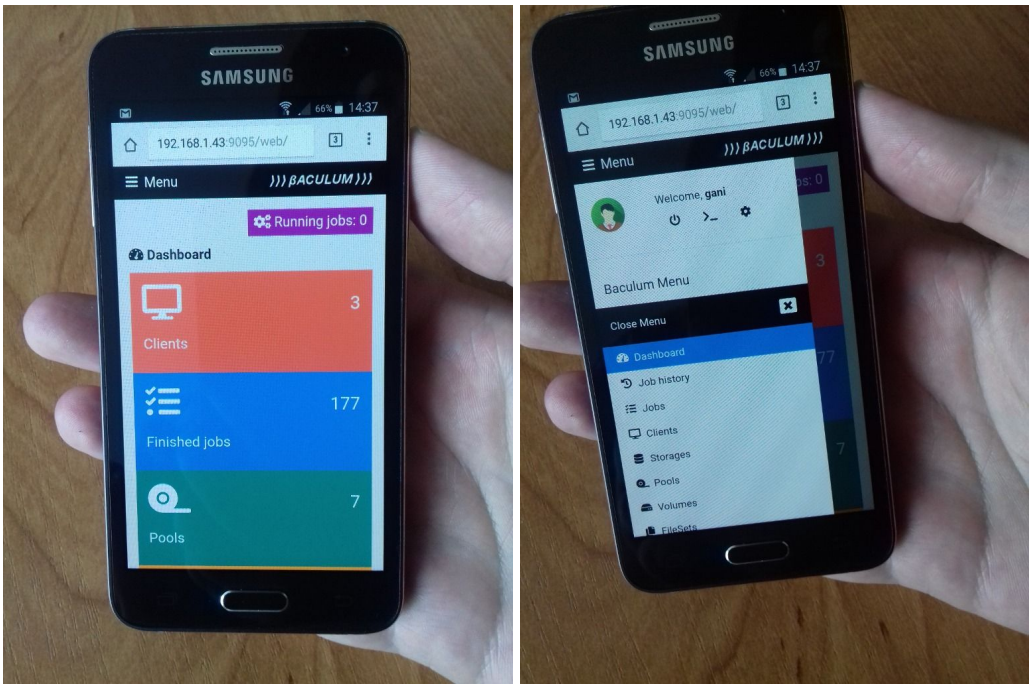


Fig. 21 Aplicación móvil de Bacula.

2.14 Manejador de Eventos de Seguridad (SIEM)

Como corolario de este trabajo, y para completar el espectro de protecciones y monitoreos que podemos hacer sobre la infraestructura se puede instalar un SIEM.

Que es un SIEM?

(Security Information Event Manager) como su nombre en inglés lo indica, es un manejador de eventos de seguridad de la información.

Y para que lo necesitamos?

En nuestro entorno actual, en el manejo de todo centro de cómputos y en cualquier empresa o establecimiento de mediano tamaño, nos encontramos

con una multiplicidad importante de dispositivos interconectados de todo tipo y variedad.

A saber:

- Routers
- Switches
- Servidores
- Access Points (routers WiFi)
- Storages
- Robots de cintas
- Cámaras de vigilancia
- Teléfonos IP
- UPS
- Sistemas de control de acceso físico
- Terminales de trabajo PC
- Notebooks
- Tablets
- SmartPhones, etc.

La lista puede ser interminable, igual que la cantidad de tráfico de red que estos dispositivos crean, con sus logs y registros.

Además los sistemas de monitoreo de seguridad que por su parte están haciendo escaneos, reportes y análisis todo el tiempo.

El volumen de información y de logs que hay que mirar es realmente muy grande, y se hace casi imposible de manejar y observar de forma eficiente por cualquier persona o equipo de personas, que estuvieran dedicadas a esta tarea.

Ahí es donde el SIEM viene a ayudarnos en nuestra tarea, haciendo que podamos concentrar los esfuerzos en los eventos que disparan alertas según las reglas del SIEM.

Para esta tarea encuentro una muy buena opción de la comunidad Open Source que se llama OSSIM y es de AlienVault.

Ossim es uno de los SIEM más utilizados de la actualidad, por tener origen Open Source y ser de carácter gratuito.

Este tipo de productos suele ser de un costo muy elevado y usualmente fuera del alcance de las PyMe.

AlienVault tiene una versión comercial del producto que extiende las funcionalidades a la recolección de Logs (reemplazando al Syslog) y con soporte profesional y otras ventajas que luego analizaremos.

El software puede descargarse en formato ISO, listo para instalar tipo "Appliance" sobre un servidor físico o virtual.

Viene embebido en un Sistema Operativo tipo FreeBSD.

La url de descarga:

https://www.alienvault.com/products/ossim/download

Actualmente la ISO de 64bits tiene un tamaño de 653MB.

La instalación es muy sencilla y guiada.

Es importante para un producto de este tipo que integra entre otras cosas un IDS (Suricata o Snort) tener "visibilidad" completa de la red para poder aprovecharlo al máximo y no perder eventos.

Esta visibilidad es posible conectando una interfaz de red a cada Lan, SubRed o DMZ de la institución o realizando un "port mirror" de todas las VLans en los puertos que le conectemos al OSSIM.

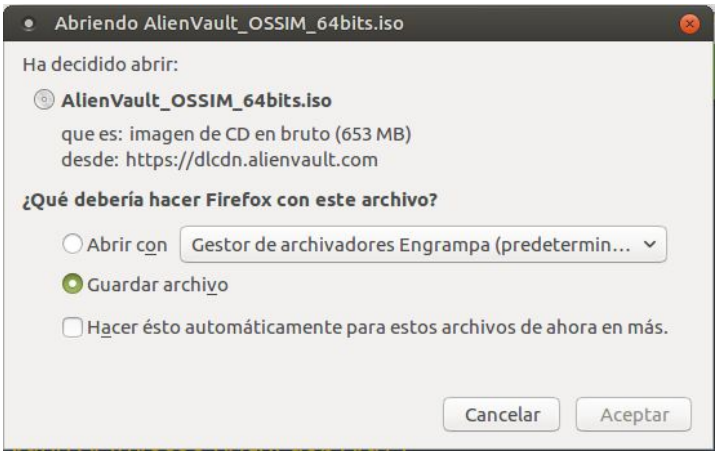


Fig.22 Descargando imágen de CD.

Principales características:

Entre las herramientas más notorias encontramos las siguientes:

- Asset discovery
- Vulnerability assessment
- Intrusion detection
- Behavioral monitoring
- SIEM

Asset discovery: (Descubrimiento de activos)

Descubrimiento de equipos, cualquier cosa que esté conectada a la red y tenga una IP.
Permite de forma automatizada o manual lanzar descubrimientos, así como su inventariado en forma pasiva.
Nos permite hacer agrupados por áreas o subredes por ejemplo.
Las IP descubiertas pueden ser reconocidas via su reverso DNS si lo habilitamos.

Vulnerability assessment: (evaluación de vulnerabilidades)

OSSIM trae embebido un server OpenVas (más conocido como Nessus, versión OpenSource).
Esta conocida herramienta nos permite realizar escaneos de vulnerabilidades a todos los elementos inventariados, de forma programada, o manual, con todos los settings a los que nos tiene acostumbrados. Genera unos reportes de calidad muy profesional exportables en varios formatos, html, pdf, doc, csv, etc.

Intrusion detection: (detección de intrusiones)

Al igual que PFSense, incorpora también en la función de IDS a Suricata o Snort según nuestra preferencia. Ambos basan la detección en firmas y contienen reglas para detección de emerging threats (nuevos trucos) que combinan varias técnicas para detectar shellcodes o malware.

Behavioral monitoring: (monitor de comportamiento)

Analiza el comportamiento de la red detectando anomalías y cambios en las trazas habituales, cambios en los servicios de los dispositivos, nuevos puertos, cambios de sistema operativo, cambios en la fecha y hora, cambios en los usuarios asociados a los equipos, etc.

SIEM

Integración y correlación de todos los eventos en tableros de fácil comprensión y formato gráfico linkeados o enlazados con los datos correspondientes, lo que los hace muy atractivos y usables. Visualización clara con opción de agrupamiento por categorías, dispositivos, tipos, servicios, fechas, etc.

También muestra un conveniente gráfico con los Top 5 o Top 10 de orígenes más agresivos o los destinos más atacados.

Algunos de los tableros o “dashboards” más usados:

Tablero ejecutivo.

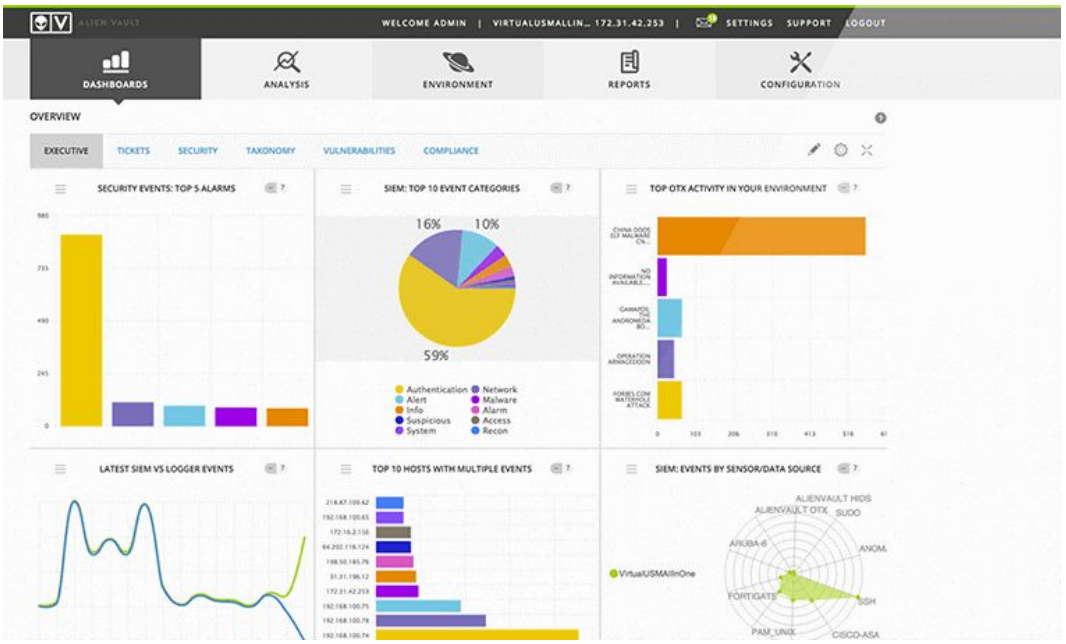


Fig. 23 Tablero ejecutivo

Tablero de monitoreo de servicios.

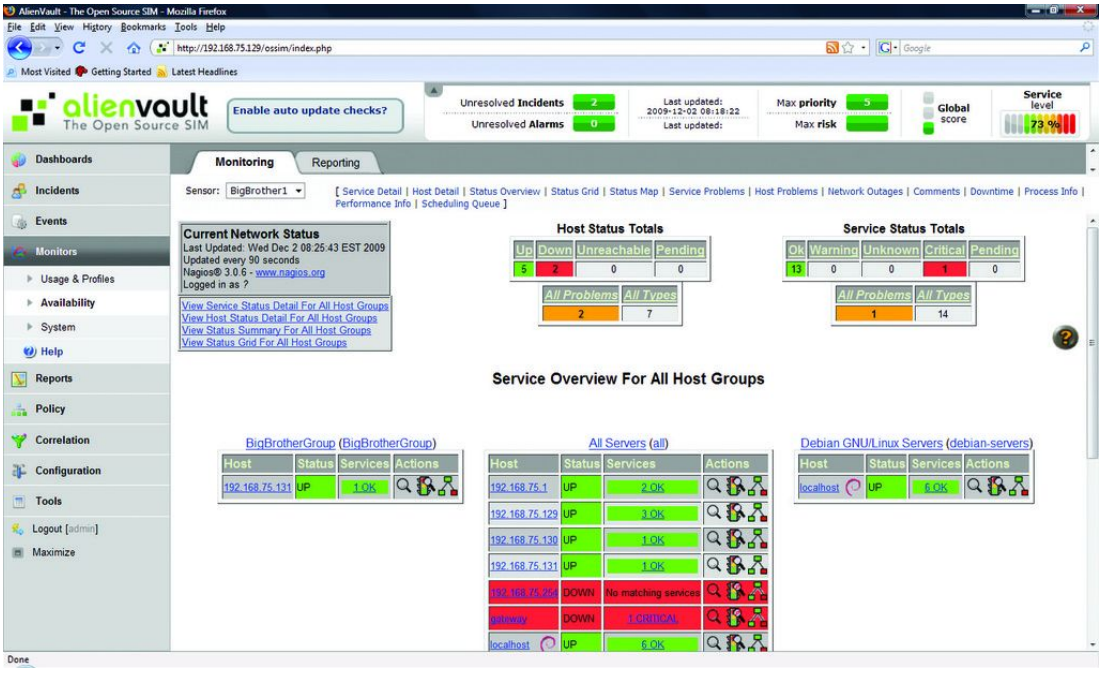


Fig. 24 Monitoreo de servicios con Nagios incluido.

Sistema de Ticketing para verificación de eventos.

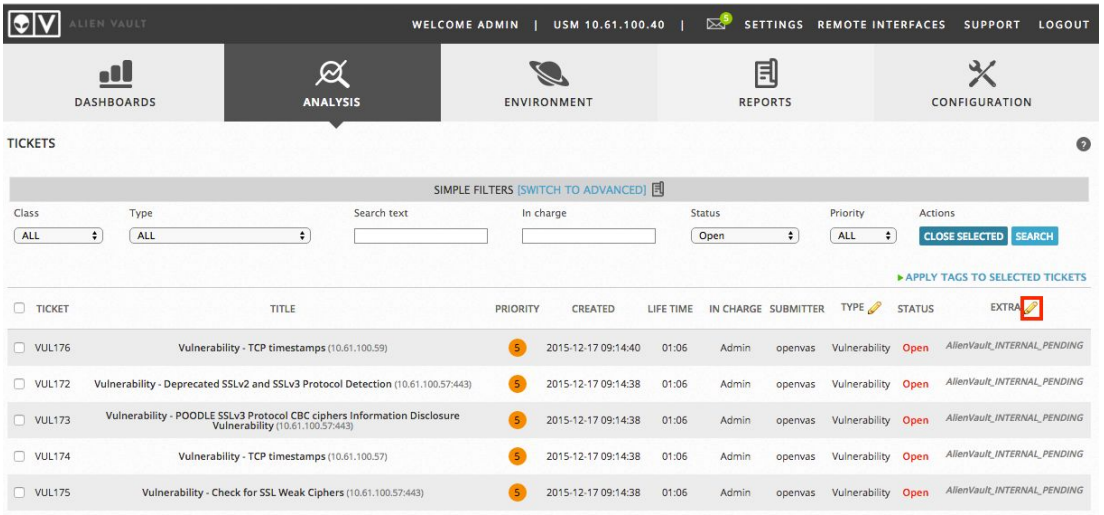


Fig. 25 sistema de tickets incluido en el OSSIM.

SIEM eventos agrupados:

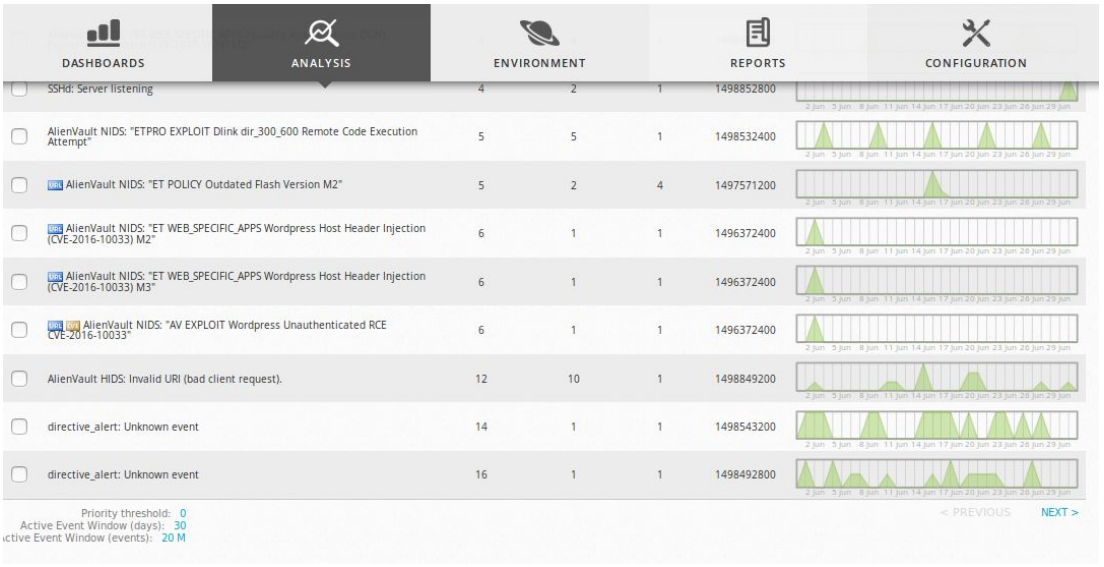


Fig. 26 Tablero de eventos agrupados.

OSSEC HIDS server y agentes:

OSSEC es un sistema de detección de intrusiones basado en host, puede utilizarse en modo solo, o en modo agente y servidor como sería el caso de uso en conjunto con el SIEM. En este caso el SIEM incluye el OSSEC server que se utiliza para configurar y concentrar los logs y eventos de los agentes remotos instalados en otros sistemas. Básicamente estos agentes inspeccionan los logs del sistema que están monitoreando en busca de alertas como ser intentos fallidos de login, errores de servicios,

modificaciones de archivos críticos, etc. Al detectar alguna de estas anomalías el agente se comunica con el servidor que es quien le indica que acción tomar. Usualmente además de disparar una alerta al administrador sobre el evento de seguridad ocurrido también puede por ejemplo bloquear temporalmente la dirección IP del sistema ofensor, o incluirlo en una blacklist. Esta es una protección activa, súmamente útil para parar ataques por ejemplo en los servidores web cuando están siendo escaneado en busca de determinados scripts o páginas administrativas, el agente lo detecta y rápidamente crea una regla en el firewall local que bloquea el acceso del atacante.

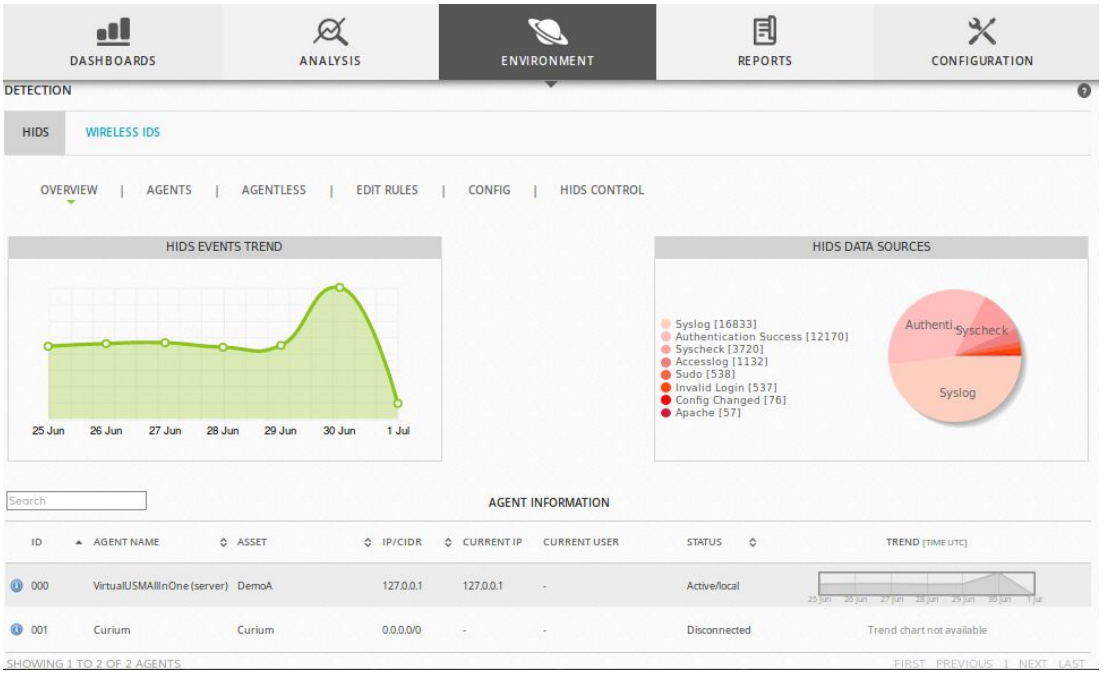


Fig. 27 Tablero de agentes OSSEC y admin del mismo.

Análisis de Vulnerabilidades y Reporte:

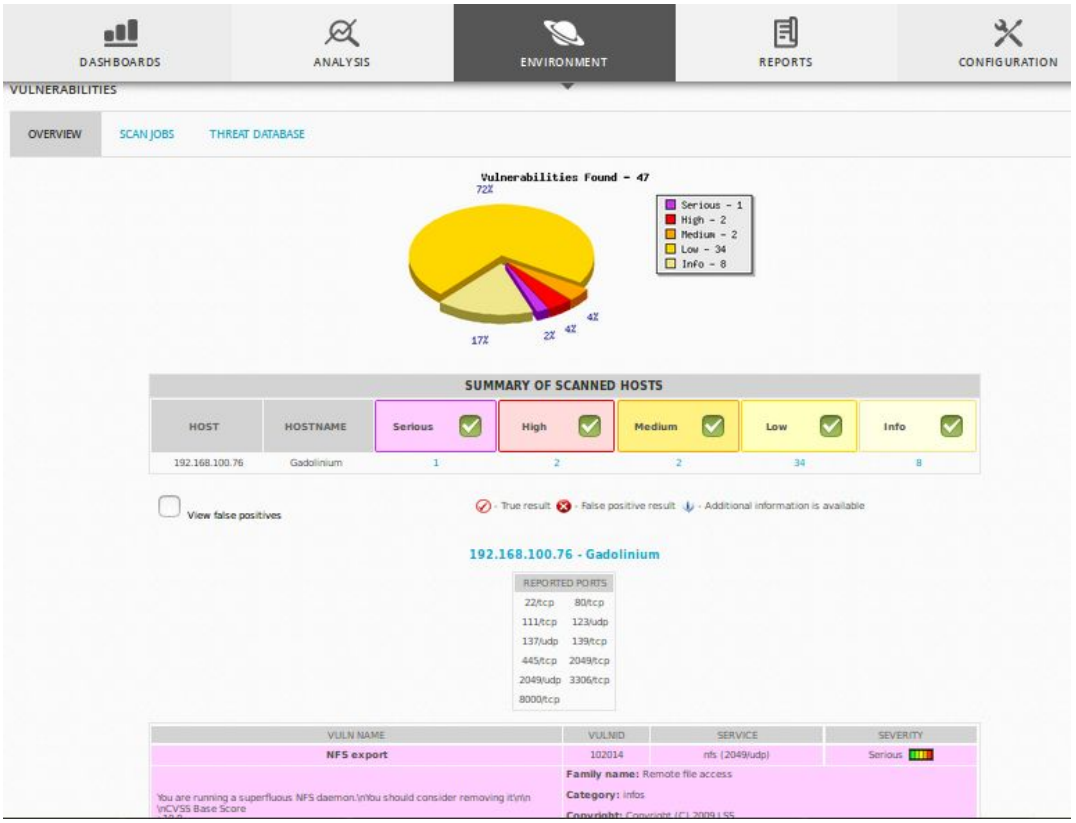


Fig. 28 Tablero de reporte de vulnerabilidades.

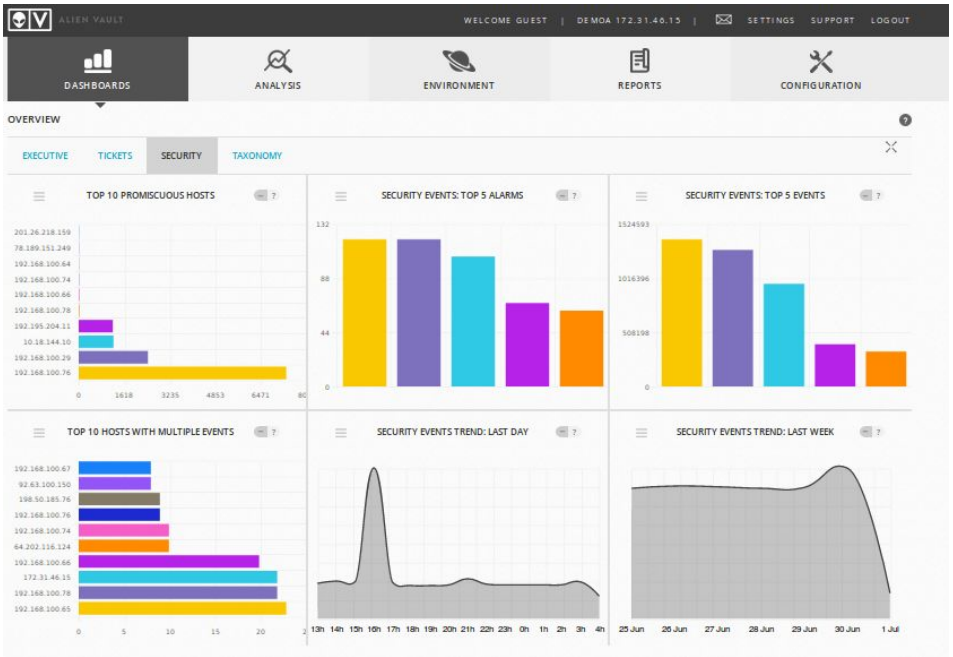


Fig. 29 Tablero de eventos de seguridad.

OTX (Open Threat Exchange) Intercambio Abierto de Amenazas.

Es la primera comunidad de inteligencia de amenazas verdaderamente abierta del mundo que permite la defensa colaborativa con datos de amenaza impulsados por la comunidad, y que suma verdadero valor a la herramienta ya que al ser alimentada por usuarios expertos de todo el mundo nos permite mantenernos en la avanzada de la detección de amenazas.

Cuenta con una API de conexión que asocia de forma rápida y limpia nuestra instalación con la base de conocimiento comunitario.

Pantallas del OTX

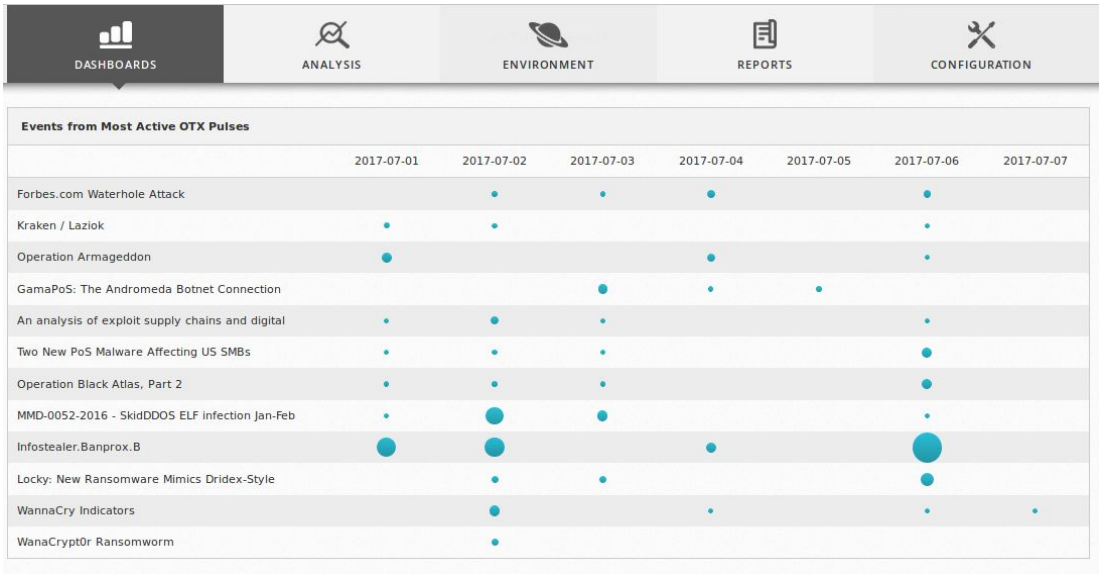


Fig. 30 Pantallas de OTX parte 1

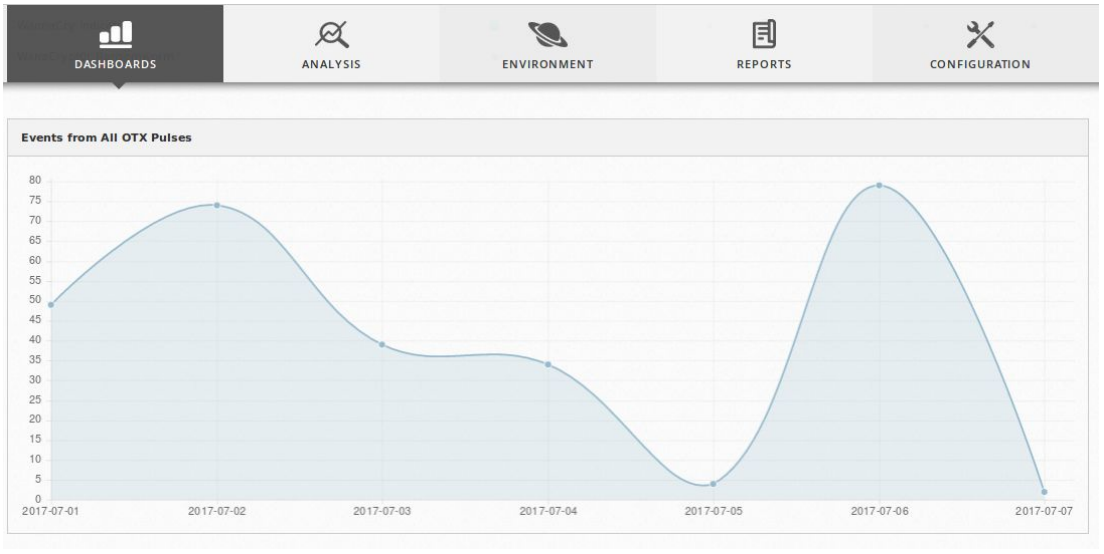


Fig. 31 Pantallas de OTX parte 2

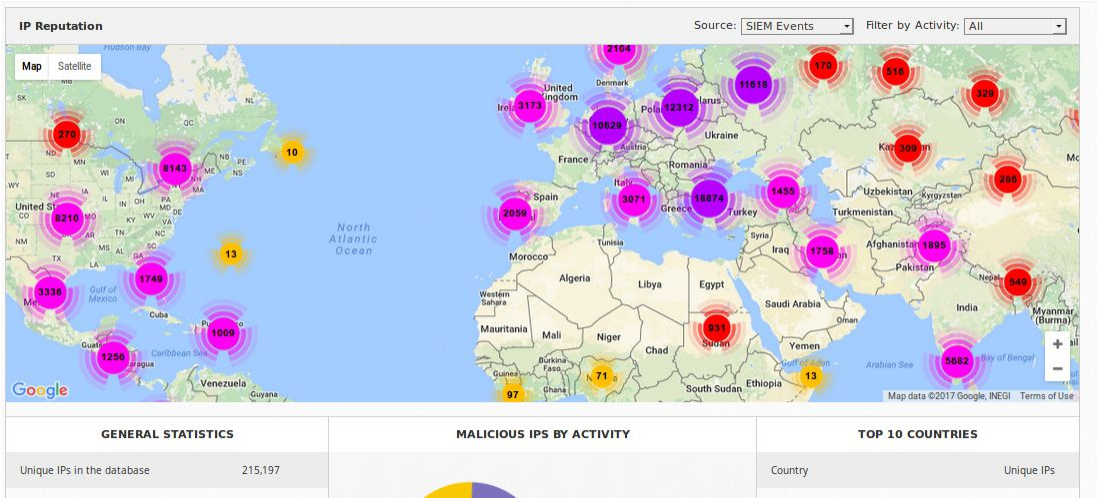


Fig. 32 Pantallas de OTX parte 3

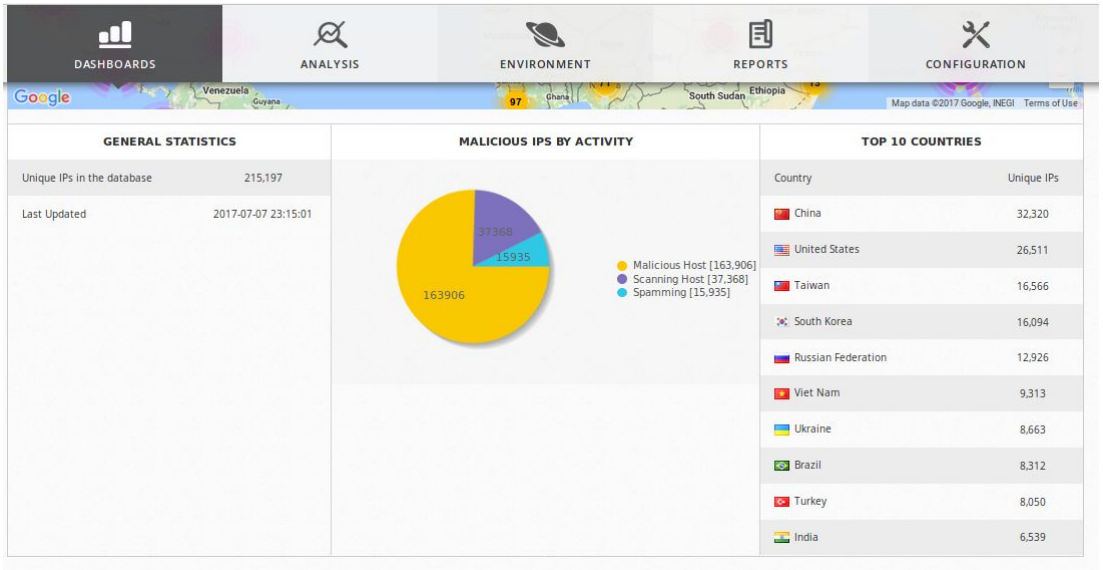


Fig. 33 Pantallas de OTX parte 4

Una herramienta super profesional, con una comunidad enorme detrás desarrollando reglas de detección de nuevas amenazas, con la capacidad de correlacionar eventos de múltiples fuentes, integrado con herramientas de sniffing de red, análisis de vulnerabilidades, loggin, monitoreo, generación de reportes, envío de alertas por email, ayuda de compliance de múltiples normas internacionales, etc.

De verdad un infaltable en toda organización que desee mejorar sus niveles de seguridad con una inversión muy baja o nula.

Ref: [22]

Capítulo 3 - Cumplimiento de normas

3.1 Gestión de Riesgos

Siguiendo las buenas prácticas y las recomendaciones de la ISO 27001 sobre el sistema de gestión de seguridad informática debemos analizar nuestra infraestructura realizando una clasificación de activos informáticos y hacer una clasificación de riesgos en base a la probabilidad de ocurrencia de un ataque sobre un activo y el impacto que ese ataque podría tener afectando la integridad, disponibilidad o confidencialidad de los datos.

Para este caso tomando como ejemplo los sistemas mencionados en el presente trabajo se realizó una matriz de riesgos que nos permite visualizar cuales son los más expuestos y donde hay que poner más atención en la seguridad. La probabilidad la estimamos en base a la cantidad de vulnerabilidades reportadas en cada software y la exposición tanto externa como interna del activo, cantidad de usuarios habilitados a acceder al mismo y factores de protección instalados. Típicamente quedaría como sigue:

Activo	Probabilidad	Impacto	Conf.	Disp.	Int.	**Riesgo**
Fileserver	3	3	1	1	1	**12**
OnlyOffice	3	3	1	1	1	**12**
BBDD	3	3	1	1	1	**12**
Webserver	3	3	1	1	1	**12**
Correo	3	3	1	1	1	**12**
LDAP	2	2	1	1	0	**6**
Proxmox	1	3	1	1	1	**6**
Radius	1	3	1	1	0	**5**
Bacula	1	2	1	1	1	**5**
SIEM	1	3	1	0	0	**4**
IDS/IPS	1	3	1	0	0	**4**
Firewall	1	3	0	1	0	**4**
Openvpn	1	3	0	1	0	**4**
Kibana	2	1	0	0	1	**3**
Proxy	1	1	1	0	0	**2**

No hay una única forma de realizar la calificación de riesgo, ya que tiene un alto grado de subjetividad y condicionantes. Para este ejemplo se realizó

una calificación simple, donde se multiplica la probabilidad de ocurrencia por el impacto de la misma, y se suman las categorías afectadas. La calificación en caso de integridad, confidencialidad y disponibilidad es binaria, 0 o 1 para afecta o no afecta. Para probabilidad e impacto una escala de 1 a 3 conforme a bajo, medio o alto respectivamente. De esta forma el máximo alcanzable de riesgo queda en 12 y el mínimo en 1.

	Bajo	Medio	Alto
Probabilidad	1	2	3
Impacto	1	2	3
Riesgo	1 a 4	5 a 8	9 a 12

Del análisis de riesgo anterior surge que los sistemas de mayor riesgo son el Fileserver, la suite de oficina y repositorio de documentos Onlyoffice, la base de datos, el servidor web y el servidor de correo. Los dos primeros expuestos de forma interna, y los restantes en la DMZ pública, expuestos a internet de forma directa o indirecta como el caso de la base de datos.

Para mitigar estos riesgos necesariamente deberemos comenzar por realizar una buena configuración o “hardening” de los mismos, poniendo especial atención a las recomendaciones de seguridad.

- Hardening del sistema operativo y el software de servicio.
- Reglas de Firewall específicas y restrictivas por origen, destinos y puertos necesarios.
- instalación de agentes OSSEC que reporten al servidor del SIEM.
- utilizar cifrado en las comunicaciones siempre que esté disponible, prefiriendo siempre las de mayor robustez.
- Configurar los sistemas para reportar vía Syslog al stack ELK (Kibana) para su monitoreo y visualización.

3.2 Políticas y Procedimientos de Seguridad

Para que el software de seguridad y monitoreo que instalamos funcione de manera adecuada es necesario establecer políticas de seguridad alineadas con las mejores prácticas, en este caso con las ISO27001.
De esta forma buscamos bajar el nivel de riesgo aplicando medidas de mitigación o eliminación de los que podemos controlar y aceptación de aquellos sobre los que no tenemos medios de contención.
A continuación algunas políticas y procedimientos sugeridos de forma genérica y abarcativa para cubrir aspectos comunes de PyMEs y organizaciones.

3.3 Política de Seguridad

La información es un activo esencial para la organización, ya que es crítica a la hora de la toma de decisiones, tanto en el orden operativo como gerencial, para el propio Organismo como para las otras partes interesadas.

El Director o Gerente General establece los siguientes lineamientos de Seguridad de la Información para la institución:

Confidencialidad: la información debe ser accedida solamente por personas, entidades o procesos autorizados y los derechos de propiedad sobre la información deben estar adecuadamente establecidos.

Integridad: la información debe mantenerse precisa y completa, sin modificaciones no autorizadas.

Disponibilidad: la información debe mantenerse accesible y utilizable por las personas, entidades o procesos debidamente autorizados, en el momento en que sea requerido.

Gestión de Riesgos: los activos de información de importancia deben identificarse y clasificarse; las vulnerabilidades y las amenazas sobre los

activos deben identificarse y analizarse; los riesgos deben evaluarse y tratarse con controles de Seguridad de la Información.

Cumplimiento con los requisitos de las partes interesadas: la empresa debe desempeñar sus actividades orientadas al cumplimiento de los requisitos de las partes interesadas, en cuanto a la normativa legal, la reglamentación emitida por organismos regulatorios, la normativa interna y los procedimientos establecidos por la propia Dirección o Gerencia.

Mejora Continua: la probabilidad de cumplir con los requisitos y expectativas de las partes interesadas en la Seguridad de la Información debe aumentar en el tiempo.

Participación del personal: el personal es la esencia de la empresa, y su total implicación mediante las actividades de concientización, educación y entrenamiento posibilita que sus capacidades sean utilizadas para beneficio de los objetivos de seguridad.

La presente Política del SGSI (Sistema de Gestión de Seguridad Informática) se enmarca dentro de los requisitos establecidos por la norma ISO 27001.

3.4 Política de Control de Accesos

Objetivo

Establecer los controles necesarios a nivel de seguridad física y lógica, para garantizar la aplicación del principio del mínimo privilegio (necesidad de saber).

Alcance

El control de acceso físico a oficinas, basado en el mínimo privilegio, soporta las premisas básicas de seguridad física. Las oficinas podrán ser de diferente criticidad: centro de procesamiento de datos (CPD), sala de

reuniones, oficina de administración, etc. Los controles de acceso físico deberán tener una complejidad acorde, ya sea mediante tarjetas magnéticas o cerradura tradicional con llaves en poder de las personas del área.

En cuanto a los controles de acceso lógico a recursos, deberán aplicarse las correspondientes Listas de Control de Acceso (ACL) o reglas en el firewall de manera de respetar el principio antes mencionado.

Implementación

Deberán implementarse controles de acceso a todos los recintos u oficinas. Se deberán implementar controles de acceso en distintas capas y abstracciones de cómputo y comunicaciones.

Para ello, se segmentan las distintas redes lógicas en distintos dominios, de acuerdo al grado de criticidad de los activos a los que dan servicio, de tal manera de poder aplicar controles a todo tráfico que se curse de una red a otra diferente, incluido el acceso a Internet.

Se promoverá el uso de tecnologías de autenticación multifactor para servidores críticos.

Se instalará en los equipos de los usuarios, sólo el software estandarizado y necesario para las funciones operativas de los mismos. Sólo se permitirá el uso de servicios necesarios y autorizados, según cada caso. Se controlará además el uso inapropiado de medios digitales de extracción de información, para garantizar la confidencialidad de los datos internos de la empresa.

Se deberá llevar control del contenido consultado a Internet por cada equipo de escritorio, incluyendo descargas, asociado a un usuario determinado. Se auditará por muestreo el consumo de contenido apropiado, según los logs del sistema de proxy.

Se promoverá el uso responsable de administración de equipos, soportando la separación de funciones con el objetivo de evitar fraudes internos.

Para accesos remotos de servicios de red por parte de usuarios, será obligatorio el uso de mecanismos de múltiple autenticación.

Se otorgarán credenciales de ingreso a servicios remotos, exigiendo métodos de autenticación multifactor a dichos usuarios, previos controles de identidad real de cada solicitante, antes de autorizar su acceso.

Deberá llevarse un inventario de credenciales otorgadas, activas, modificadas e inactivas, para cada servicio.

Responsabilidades

Seguridad Informática y los responsables de cada área de infraestructura tendrán a cargo el otorgamiento del acceso a los servicios y recursos de red, dichos accesos deberán ser solicitados por el responsable del área para el personal a su cargo y bajo la supervisión de Seguridad Informática, quien asegurará la correctitud de los perfiles solicitados.

Difusión

La presente política es de carácter restringido y deberá ser comunicada formalmente a todo el personal.

Aprobación

La dirección o gerencia aprueba la presente política de control de acceso, manifestando su incondicional apoyo a los esfuerzos organizados por el área de seguridad para el mantenimiento de los niveles de riesgo sobre el tratamiento de los activos informáticos dentro de valores residuales aceptables.

3.5 Política de dispositivos móviles

Objetivo:

El presente documento establece la política para conexión de dispositivos móviles en la red de la empresa.

Política:

En vista de la necesidad de proveer conexión de los dispositivos móviles personales dentro del área de trabajo de la empresa, se pone a disposición de los usuarios una red WiFi.

Utilización:

Se provee acceso a internet sin conexión interna con los servicios de la empresa.

Seguridad de la red:

Se deberán configurar los Puntos de Acceso o Access Point (AP) con un SSID que identifique al área para una mejor visualización, y ajustar la seguridad con WPA2 + PSK ya que es la más alta al momento de redactar este documento.

Como medida adicional se activará el acceso solo mediante lista blanca de filtrado por dirección física (MAC) . La red donde se encuentran los AP pertenece a una red virtual (vlan) exclusiva para tal efecto sin contacto ni permisos sobre las redes de la empresa, solo salida a Internet.

Usuario interno:

El usuario deberá solicitar el acceso y proveer la dirección MAC de su dispositivo, y podrá conectarse mediante una contraseña que le proveerá el administrador.

Capítulo 4. - Seguridad de la plataforma

La seguridad informática está apoyada en tres grandes pilares que son la tecnología, los procesos y las personas. En cuanto a la tecnología aquí mencionada, sus configuraciones por defecto usualmente no contemplan la seguridad, por lo tanto hay que prestar especial atención al instalar cualquier tipo de programa, en particular si se trata de un servidor que estará expuesto a internet.

La fortaleza de seguridad de esta propuesta se compone de integrar un buen diseño de red, utilizar software libre de oficina y aplicaciones de probada eficacia configurados de forma segura, tecnologías de monitoreo y control específicos de seguridad, y propuestas de políticas y procedimientos alineados con las buenas prácticas que vimos en el capítulo anterior.

Luego verificando lo siguiente:

Firewall: crear las reglas de firewall de modo restrictivo, o sea todas las comunicaciones denegadas por defecto y solo permitidas las conexiones necesarias para el funcionamiento.

Monitoreo: configurar los syslogs de cada servidor para loguear remotamente en nuestra plataforma ELK (Elasticsearch-Logstash-Kibana), instalar los agentes OSSEC que se comunican con el SIEM.

Protección activa: habilitar las protecciones del sistema IDS/IPS.

Navegación: habilitar el proxy con filtrado de contenido y antivirus.

Backups: instalar los agentes y programar la agenda de backups.

Hardening: realizar las configuraciones sugeridas de seguridad para cada sistema. Se adjuntan a modo de anexo los hardening de Apache, PostgreSQL, servidor de archivos Samba, suite de oficina OnlyOffice, servidores Debian y correo Zimbra que son los que según nuestro análisis de riesgo deben ser más protegidos por su exposición.

Es claro que esto no es todo lo que se puede hacer ni significa que sea la única forma, pero se eleva de forma importante la seguridad de toda la infraestructura tecnológica que da soporte a la empresa.

Conclusiones finales

La decisión de atender las cuestiones de seguridad para cualquier empresa es cada vez más necesaria a la vista de la cantidad creciente de ataques informáticos y pérdidas generadas por estos ataques como podemos observar por ejemplo en los anexos adjuntos "*Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina*", y los costos y porcentajes de inversión con estadísticas a nivel global que si bien no son extrapolables a nuestra realidad, sirven para tener una idea de cual es la situación en nuestra región, podemos ver algunos datos en los anexos "*El impacto financiero de la seguridad de IT en las empresas europeas"* y " *Encuesta Mundial sobre el estado de la Seguridad de la Información 2018*" elaborado por la consultora internacional PWC para el mercado español.

En todos los casos y con toda esa información cuánto invertir y cómo es la parte realmente difícil de determinar.

Por esto mi propuesta de ir por las soluciones de software libre atiende a esta cuestión fundamental de lograr un entorno seguro de trabajo que no dependa de un gran presupuesto.

Estas soluciones requieren de personal con ciertas habilidades y conocimiento que si bien no son lo más común entre los técnicos informáticos, tampoco son ciencia oculta. Cualquier técnico autodidacta puede adquirir las habilidades necesarias para instalar y administrar estas herramientas, sin embargo la capacitación en seguridad informática y seguir los lineamientos de las normas internacionales creadas por especialistas en el tema es fundamental para realmente atender y elevar el nivel de seguridad de la información de la empresa.

Todos los sistemas aquí presentados aunque sea de forma breve y descriptiva fueron probados por mi, instalados y administrados en entornos muy exigentes con gran carga de tareas y multiplicidad de usuarios y requerimientos, en entornos productivos, de desarrollo y de testing.

En lo personal hace más de 15 años que no utilizo software cerrado, salvo contadas excepciones, tanto en lo laboral como en lo hogareño, he aprendido que siempre existe una opción de software libre para lo que sea que necesite hacer, con la satisfacción de aprender algo nuevo en el camino, y teniendo siempre presente los principios de seguridad.

Se puede tener altos estándares de seguridad invirtiendo en los recursos humanos y su capacitación.

Anexo 1 - El impacto financiero de la seguridad de IT en las empresas europeas

IMPORTANCIA DE LOS COSTES

Al ponderar sus presupuestos, la mayoría de las empresas son conscientes de que los costes reales de un incidente de seguridad o un robo de datos pueden ser enormes si se tienen en cuenta el impacto en la reputación y las consecuencias financieras. El estudio muestra que el 47% de las empresas europeas (frente al 52% mundial) presupone que su seguridad TI se verá comprometida en algún momento. Es más, en los últimos 12 meses, el 32% de las empresas (frente al 38% mundial)

afirma haber sufrido pérdidas de productividad por ataques con virus y software malicioso; mientras que el 30% ha tenido problemas por el uso inapropiado que los empleados hacen de los recursos TI (36% a nivel mundial). Tipos de eventos de seguridad ocurridos en los últimos 12 meses (media del total de empresas por tipo de ataque) Frente al verdadero coste financiero de estos tipos de incidentes, solo cabe destacar la importancia de estar preparado y contar con presupuestos que sean eficaces. Nuestro estudio reveló que más del 84% de las empresas europeas (en comparación con el 82% a nivel mundial) han sufrido entre uno y cinco incidentes de exposición, filtración o pérdida de datos en los últimos 12 meses

Como resultado de esa clase de incidentes, el 10% de las empresas europeas perdió acceso a información crítica durante una semana (en comparación con una de cada diez empresas en todo el mundo) y el 15% sufrió interrupciones que les impidieron realizar transacciones comerciales durante más de siete días. Descubrir que se ha producido un robo de datos tampoco es fácil y una de cada diez empresas (10%) podría tardar hasta un año. Esta falta de visibilidad y preparación que la mayoría ve como una consecuencia inevitable del panorama tecnológico que vivimos puede tener repercusiones financieras inimaginables. Si se considera este tema en contexto, el impacto financiero de un solo vector de ataque y robo de datos se calcula aproximadamente en 77.372 euros para las pymes a nivel mundial y en 770.252 euros para las grandes empresas. En este cálculo, la reasignación del tiempo del personal de TI representa el mayor coste adicional, tanto para las pymes como para las grandes empresas. La investigación realizada sirvió para determinar hasta qué punto están ajustados los presupuestos y por qué hay poco margen para el error en la asignación de recursos a la seguridad. Para ello, se realizó una

comparación de la media anual del gasto en seguridad TI en las pymes y en las grandes empresas con las pérdidas previstas de un solo ataque. Si tenemos en cuenta el gasto habitual de 193.000 euros que las pymes invierten en seguridad y lo comparamos con el coste de un ataque (77.372 euros), las medidas de seguridad de las pymes solo necesitan evitar dos ataques y medio para ahorrarse elevadas cantidades, por no mencionar los daños a su reputación.

Ref:
https://go.kaspersky.com/rs/802-IJN-240/images/KasperskyLabReport_Financial_Europe_SP.PDF

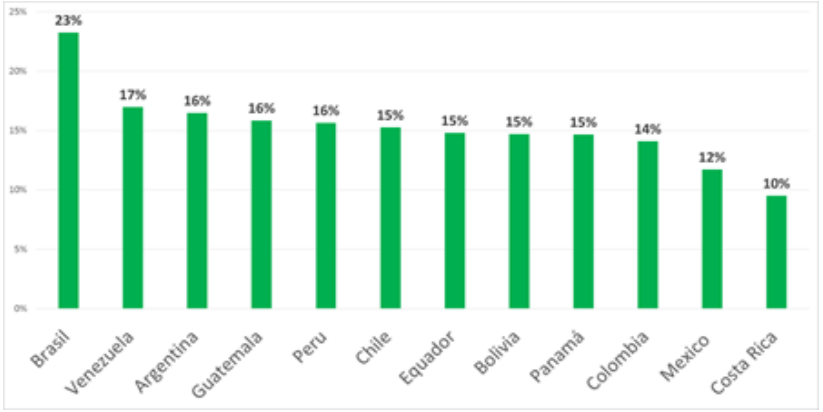
Anexo 2 - Kaspersky Lab registra un alza de 60% en ataques cibernéticos en América Latina

Kaspersky Lab registró más de 746 mil ataques de malware diarios durante los últimos 12 meses en América Latina, lo que significa **un promedio de 9 ataques de malware por segundo**. Además, los ataques de phishing – correos engañosos para el robo de la información personal de los usuarios– han sido constantes en la región, principalmente en Brasil. Los resultados, presentados durante la Octava Cumbre de Analistas de Seguridad para América Latina que se está realizando en la Ciudad de Panamá, demuestran que toda la región ha experimentado una considerable cantidad de ciberamenazas, con la gran mayoría orientada al robo de dinero.

Según **Dmitry Bestuzhev, Director del Equipo de Investigación y Análisis para América Latina en Kaspersky Lab,** hubo un incremento del 60% en ataques cibernéticos en la región, donde Venezuela registra el mayor número de los ataques en proporción a su población con un total de 70.4%, seguido por Bolivia (66.3%) y Brasil (64.4%). Al igual que en 2017, Brasil continúa encabezando a los países latinoamericanos en términos de alojamiento de sitios maliciosos ya que 50% de los hosts ubicados en América Latina que se utilizaron en ataques a usuarios de todo el mundo está ubicado en este país.

Según los datos de la empresa, la mayoría de estos ataques ocurre en línea – mientras se está navegando, descargando archivos o cuando reciben adjuntos de correos electrónicos engañosos– y afectan más a los usuarios domésticos que a empresas. Sin embargo, la investigación también reveló que las empresas son más propensas a ataques vía email (60%) y vectores offline (43%); es decir, través de USBs contaminadas, la piratería de software u otros medios que no requieren el uso obligatorio del Internet.

“El año pasado Brasil también estuvo dentro de los 20 países más atacados a nivel mundial. Esto se debe, en gran parte, a que los cibercriminales utilizan el correo electrónico, mensajes de SMS, llamadas telefónicas, anuncios en redes sociales, entre otros, con nombres de empresas conocidas, lo que hace que los usuarios no desconfíen de esos mensajes, aumentando la probabilidad de que estos sean compartidos con su red de amigos”, alertó. “Para tener una idea, solamente este año, bloqueamos 40 millones de ataques en América Latina, siendo Brasil el país más afectado”.



Ranking de países latinoamericanos afectados por phishing durante los primeros 7 meses de 2018

Ref:
https://latam.kaspersky.com/blog/kaspersky-lab-registra-un-alza-de-60-en-ataques-ciberneticos-en-america-latina/13266/

Anexo 3 - Encuesta Mundial sobre el Estado de la Seguridad de la Información 2018

Pérdida de datos sensibles, daños en activos físicos, deterioro en la calidad de los productos y suspensión de operaciones, las principales consecuencias de los ciberataques para las empresas españolas.

- El 49% de directivos reconocen que sus empresas carecen de una estrategia integral de seguridad
- Las empresas de todo el mundo sufren 3,4 incidentes de seguridad al año, con pérdidas de 4,8 M$
- En España, las compañías, forzadas a parar unas 17 horas al año por ataques informáticos

El auge de los ciberataques

El informe constata el auge de los ataques informáticos masivos y cómo el proceso generalizado de digitalización que han experimentado las empresas en todo el mundo hace que haya aumentado sensiblemente su exposición. **En España, por ejemplo, el 67,7% de los directivos encuestados consideran "probable" o "muy probable" que sus empresas vayan a ser objeto del algún tipo de ciberataque** en los próximos meses.

En la actualidad, las empresas de todo el mundo sufren, de media, **3,4 incidentes de seguridad al año, y unas pérdidas de 4,8 millones de dólares.** Según la encuesta, las empresas españolas se ven obligadas a parar sus operaciones 17 horas de media al año como consecuencia de los ataques informáticos.

El estudio concluye que, en España, aproximadamente el **47% de los ciberataques que tienen su origen dentro de la compañía son realizados por empleados o ex empleados**. Y una proporción algo menor -del 40,7%-, por proveedores. En cuanto a aquellos de origen externo, el 28,2% son realizados por competidores, el 25,4% por organizaciones criminales y un 17,5% por activistas y *ciberactivistas.*

¿Cuál es el grado de preparación de las empresas en materia de ciberseguridad?

Muchas compañías siguen sin estar preparadas todavía para afrontar los riesgos derivados de los ciberataques. El 49% de los directivos españoles entrevistados –el 44% en el mundo- reconocen que sus empresas carecen de una estrategia integral de seguridad, el 53% que no cuentan con programas de formación para los empleados y el 55% que no disponen de procedimientos previamente establecidos para responder a los incidentes de seguridad. De hecho, cuando se produce un ciberataque la mayoría de compañías reconocen que no son capaces de llegar a identificar su autoría –el 41%, en España y el 39%, en el mundo-.

Ref: https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html

Anexo 4 - Configuración segura de servidor Apache

Configuración por defecto
Salvo que se le diga lo contrario, Apache mostrará cualquier archivo que pueda acceder, por lo que es necesario negar todo por defecto e ir agregando según haga falta directorios. Negar todo por defecto con la siguiente directiva:

<Directory />
Order Deny,Allow
Deny from all
</Directory>

Permitir, por ejemplo un sitio:

<Directory /var/www/htdocs>
Order Allow,Deny
Allow from all
</Directory>

Options
Es necesario restringir la posibilidad de links simbólicos maliciosos o mal configurados que apunten fuera de DocRoot, usando la directiva Options de la siguiente manera:

Options -FollowSymLinks

AllowOverride
Apache permite por defecto que se agreguen directivas de configuración dentro del DocRoot, lo cual no es deseable. Para restringirlo, utilizar:

AllowOverride None

Scripts
Ya que no es necesario, se recomienda quitar el alias /cgi-bin/ quitando estas líneas:

ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
<Directory "/usr/lib/cgi-bin">
AllowOverride None
Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
Order allow,deny
Allow from all
</Directory>

Icons
En Debian, viene creado el Alias icons, configurado con indexing por defecto. El archivo es: */etc/apache2/mods-available/alias.conf*

```
<IfModule alias_module>
#
# Aliases: Add here as many aliases as you need (with no limit). The format is
# Alias fakename realname
#
# Note that if you include a trailing / on fakename then the server will
# require it to be present in the URL. So "/icons" isn't aliased in this
# example, only "/icons/". If the fakename is slash-terminated, then the
# realname must also be slash terminated, and if the fakename omits the
# trailing slash, the realname must also omit it.
#
# We include the /icons/ alias for FancyIndexed directory listings. If
# you do not use FancyIndexing, you may comment this out.
#
Alias /icons/ "/usr/share/apache2/icons/"
<Directory "/usr/share/apache2/icons">
        Options Indexes MultiViews
        AllowOverride None
        Order allow,deny
        Allow from all
</Directory>
```

</IfModule>
Se recomienda comentar la línea: Alias /icons/ "/usr/share/apache2/icons/"

Signature

A los efectos de minimizar la información brindada a un atacante, se sugiere brindar la menor
información posible sobre la tecnología utilizada.
Para ello, se recomienda quitar la versión del Apache de los encabezados HTTP, configurando en el archivo /etc/apache2/conf.d/security:
ServerTokens Prod
ServerSignature Off

Trace

Se recomienda deshabilitar el método TRACE utilizado para debug. Para ellos, configurar en el archivo
/etc/apache2/conf.d/security:
TraceEnable Off

Nivel de log

Se recomienda el siguiente nivel de verbosidad:
LogLevel info

SSL: protocolos y ciphers

SSLCipherSuite EECDH+AESGCM:EDH+AESGCM
 # Requires Apache 2.4.36 & OpenSSL 1.1.1
SSLProtocol -all +TLSv1.3 +TLSv1.2
SSLOpenSSLConfCmd Curves X25519:secp521r1:secp384r1:prime256v1
 # Older versions
 # SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder On
Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains; preload"
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff
 # Requires Apache >= 2.4 mitiga Crime attack
SSLCompression off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"
 # Requires Apache >= 2.4.11
SSLSessionTickets Off

Ref:
https://wiki.debian.org/Apache/Hardening
https://cipherli.st/

Anexo 5 - Configuración segura de servidor Linux.

Setear una Password de BIOS
Antes de instalar el Sistema Operativo en el servidor, configurar una contraseña de BIOS
Esquema de Partición del sistema
Los siguientes directorios tienen que tener el siguiente esquema de particiones separadas
/home
/tmp
Cualquier partición que pueda variar, p.e.
/var (especialmente /var/log)
también debe estar en una partición separada.
/*var/log* (algunos servicios utilizan mucho espacio para logs)
Cualquier partición donde haya que instalar un software fuera de la distribución debe estar en una partición separada. De acuerdo con la jerarquía estándar de archivos:
/*opt o /usr/local*
El file system recomendado y por default en Debian es *ext4*
No conectarse a Internet hasta estar listo
El sistema no debería ser conectado inmediatamente a internet durante la instalación hasta cumplir varios pasos previos de configuración. Es una práctica habitual durante la instalación que no resulta ser una buena práctica de seguridad, ya que le instalador que estamos utilizando podría tener algún servicio no parcheado con alguna vulnerabilidad de seguridad o si algún servicio no esta propiamente configurado estaría abierto a un ataque.
Si se pueden utilizar mirrors locales, CD o pendrives.
Setear Password de Root
Configurar una buena contraseña de Root es el más básico de los requerimientos para tener una sistema seguro. Tipicamente 8 caracteres o más, debería incluir mayúsculas, minúsculas, números y caracteres especiales.
Usuarios: establecer un usuario de menores privilegios
Corriendo el mínimo de servicios requeridos
Ejecutar el siguiente comando para identificar puertos escuchando de servicios innecesarios
user@host:~$ netstat -putav
Para deshabilitar los demonios innecesarios modificar los archivos que se encuentran en /etc/rc#.d (donde # es el número del runlevel [0-6]).
Cada archivo que comienza con S es que se ejecuta al inicio del sistema, de ser innecesario renombrar el archivo para que no contenga la letra S como primer carácter, agregando la letra K al nombre original
Revisar la lista de servicios en /etc/init.d. En caso de haber un servicio que no debería estar ejecutándose utilizar /usr/sbin/update-inetd --disable (service), este comando comentará la línea correspondiente al servicio en /etc/initd.conf
Instalar la menor cantidad de software posible.
El paquete de debian contiene un montón de software adicional, inclusive herramientas de programación y compilación que ayudan a comprometer el equipo y que no deben instalarse de no ser necesarias.
Shared Memory
Para asegurar esta porción de memoria que es un vector de ataque muy utilizado debemos editar el archivo */etc/fstab* y agregar al final del archivo lo siguiente:
tmpfs /run/shm tmpfs defaults,noexec,nosuid 0 0
Este cambio se hará efectivo luego de reiniciar el sistema.

Restringir acceso a SU
A menos que se configure de otra forma, los usuarios Linux pueden usar el comando SU para cambiar a un usuario diferente, y cuando se hace eso se obtienen los permisos y privilegios de ese usuario, por este motivo es necesario configurar el sistema de la siguiente forma:
Primero crear un nuevo grupo de administradores en el servidor
sudo groupadd admin

luego agregar usuarios a este grupo, por ejemplo el usuario cesar
sudo usermod -a -G admin cesar
y luego permitir el acceso al comando SU al grupo admin
sudo dpkg-statoverride --update --add root admin 4750 /bin/su
De esta forma el usuario cesar que es administrador puede cambiar a cualquier otro del sistema, pero otro usuario no tiene acceso al comando SU.

Instalar agente de OSSEC

Instalar siguiendo las instrucciones del servidor OSSIM para protección de archivos de sistema, monitoreo de logs y bloqueo automático de intentos fallidos de login o escaneo de puertos.
Los sistemas Linux son ampliamente configurables y hay muchos más parámetros que se pueden ajustar, esto es solo una configuración básica.

Ref:
https://wiki.debian.org/Hardening
https://www.lifewire.com/harden-ubuntu-server-security-4178243

Anexo 6 - Configuración segura de Samba

Esta es una configuración básica para un servidor de archivos utilizando Samba

Editar el archivo de configuración:
/etc/samba/smb.conf

En la sección de Networking - use "hosts allow" and "hosts deny"
 # hosts allow = 127.0.0.1 192.168.1.0/24
hosts allow = 127.0.0.1 192.168.1.1 192.168.1.2
hosts deny = 0.0.0.0/0

Esta última línea significa todos los demás denegados, solo se permiten los incluidos en hosts allow.

Cuando se configura un Samba se pueden restringir los usuarios que tendrán acceso a determinados objetos compartidos, archivos o carpetas.

Compartidos (shares)
Cuando se define un compartido, considerar las siguientes opciones:
browseable = no - No se muestran los compartidos cuando se recorre la red.
users = user1 user2 - Listado de usuarios permitidos a utilizar estos compartidos

```
[private]
    comment = Private Share
    path = /path/to/share/point
    browseable = no
    read only = no
    valid users = user1 user2 user3
```

De esta forma solo los usuarios user1, user2 y user3 tienen permiso de acceso al compartido "private".

Luego configurar los permisos en el firewall para que solo los usuarios del servidor de archivos tengan acceso a los puertos

UDP 137 y 138

TCP 139 y 445

Ref:
https://help.ubuntu.com/community/Samba/SecuringSamba

Anexo 7 - Configuración segura de PostgreSQL

Editar el archivo de configuración pg_hba.conf ajustando las opciones a nuestras necesidades, limitando el acceso solo desde las IP necesarias y denegando el resto.

```
# Allow any user on the local system to connect to any database under
# any database user name using Unix-domain sockets (the default for local
# connections).
# TYPE  DATABASE    USER        CIDR-ADDRESS          METHOD
local   all         all                               trust
# The same using local loopback TCP/IP connections.
# TYPE  DATABASE    USER        CIDR-ADDRESS          METHOD
host    all         all         127.0.0.1/32          trust
# Allow a user from host 192.168.12.10 to connect to database
# "postgres" if the user's password is correctly supplied.
# TYPE  DATABASE    USER        CIDR-ADDRESS          METHOD
host    postgres    all         192.168.12.10/32      md5
host    all         all         0.0.0.0/0             krb5
# If these are the only three lines for local connections, they will
# allow local users to connect only to their own databases (databases
# with the same name as their database user name) except for administrators
# and members of role "support", who can connect to all databases.  The file
# $PGDATA/admins contains a list of names of administrators.  Passwords
# are required in all cases.
#
# TYPE  DATABASE    USER        CIDR-ADDRESS          METHOD
local   sameuser    all                               md5
local   all         @admins                           md5
local   all         +support                          md5
```

Roles de usuarios

En PostgreSQL usuarios y roles son lo mismo, cuando se crea un nuevo usuario puede asignarse diferentes opciones con esta sintaxis:

CREATE ROLE name [[WITH] option [...]]

Un ejemplo de creación de un rol puede ser:

CREATE ROLE miriam WITH LOGIN PASSWORD 'jw8s0F4' VALID UNTIL '2021-01-01';

Privilegios de acceso

Luego de la creación de un rol hay que dar los privilegios de acceso a cada base específica. Una buena práctica es crear al menos dos usuarios distintos para cada base de datos, el primero con control completo, el segundo con solo lectura por ejemplo para ser usado en una aplicación web, entonces en caso de ser comprometido ese usuario no tendría privilegios para modificar la estructura, borrar datos, insertar o crear nada.

La sintaxis del comando es la siguiente:

GRANT { { SELECT | INSERT | UPDATE | DELETE | REFERENCES | TRIGGER } [,...] | ALL [PRIVILEGES] } ON [TABLE] tablename [, ...] TO { [GROUP] rolename | PUBLIC } [, ...] [WITH GRANT OPTION

Remover el esquema Public

Por defecto el esquema Public es usado para guardar información sobre las base de datos, tablas y procedimientos. Este esquema es accesible por todos los usuarios, por lo tanto todos pueden ver las estructuras de las tablas o procedures.
Desde la consola de SQL ejecutar:
REVOKE CREATE ON SCHEMA public FROM PUBLIC;
CREATE SCHEMA myschema AUTHORIZATION [nombre_usuario];
SET ubicacion TO myschema,public;
De esta forma la estructura de la base de datos se guardará en un esquema privado y el acceso se permitirá solamente al usuario correcto.
Por defecto PostgreSQL deniega el acceso al sistema de archivos del sistema operativo y a rutinas de sistema a todos los usuarios, así que solo el super usuario puede hacerlo.

Ref:
https://www.owasp.org/index.php/OWASP_Backend_Security_Project_PostgreSQL_Hardening#pg_hba.conf_-_Client_Authentication

Anexo 8 - Configuración segura de Zimbra

Securizar smtpd_sender_restrictions

De esta forma evitamos a usuarios locales impersonar a otro usuario.
Sacar la lista de los dominios que maneja nuestro Zimbra
su - zimbra
zmprov gad

Editar este fichero > */opt/zimbra/conf/zmconfigd/smtpd_sender_restrictions.cf* y añadir al final
%%contains VAR:zimbraServiceEnabled antivirus^ check_sender_access hash:/opt/zimbra/postfix/conf/access_table%%
Crearemos el fichero */opt/zimbra/postfix/conf/access_table* con la lista de dominios que hemos extraído primero, y adicionalmente pondremos un mensaje "**amistoso**" para nuestros amigos hackers, podemos ser más o menos sarcásticos, o legales incluso:
localdomain.com REJECT No eres yo!
otrodominio.com REJECT No eres yo!
Ahora tenemos que crear el Hash para el fichero */opt/zimbra/postfix/conf/access_table*
postmap /opt/zimbra/postfix/conf/access_table
Y reiniciar zmmtactl
zmmtactl restart

Forzar verificación entre nombre de usuario y remitente
Abrir y agregar en el fichero opt/zimbra/conf/zmconfigd/smtpd_sender_restrictions.cf
permit_mynetworks, reject_sender_login_mismatch

Rechazar falsos correos
Loguearse al sistema como usuario zimbra y ejecutar los siguientes comandos:

zmprov mcf zimbraMtaSmtpdRejectUnlistedRecipient yes
zmprov mcf zimbraMtaSmtpdRejectUnlistedSender yes
zmmtactl restart
zmconfigdctl restart

Ref:
https://www.jorgedelacruz.es/2014/04/03/zimbra-seguridad-i-parte/
https://www.jorgedelacruz.es/2014/09/08/zimbra-seguridad-ii-parte-enforcing-a-match-between-from-address-and-sasl-username-en-zimbra-8-5/
https://www.jorgedelacruz.es/2015/07/21/zimbra-seguridad-iii-parte/

Anexo 9 - Configuración segura de OnlyOffice

Cambiar el protocolo de conexión web utilizando SSL.

Panel de Control le ofrece la posibilidad de cambiar su portal al protocolo HTTPS protegido de manera rápida y sencilla.
Hay dos maneras de activar el protocolo HTTPS para su portal a través de la interfaz del Panel de Control:

> Si Usted no tiene ningún certificado SSL, puede generar un certificado firmado nuevo con un solo clic. El Panel de Control usa el servicio letsencrypt.org para generar un certificado firmado por entidad certificadora (CA).
>
> Si Usted ya tiene una clave privada generada en su servidor y un certificado de clave pública creado sobre su base (autofirmado o emitido por una Entidad Certificadora), puede simplemente cargarlos en el Panel de Control.

Para generar un certificado nuevo:

> En la página HTTPS haga clic en el botón GENERAR Y APLICAR. Aparecerá el cuadro de mensaje emergente informando de que el certificado y la clave privada han sido generados con éxito.
>
> Después de eso su Panel de Control y el portal se reiniciará y dejarán de estar disponibles durante este proceso. Esto puede tardar hasta 5 minutos. Una vez finalizado el proceso de instalación del certificado, su portal estará disponible sobre HTTPS.

Para usar un certificado existente .crt y la clave privada .key:

> En la página HTTPS haga clic en el botón Plus (Más) junto al campo Certificado CRT y seleccione su certificado .crt para cargarlo.
>
> Haga clic en el botón Plus (Más) junto al campo Clave HTTPS y seleccione su clave privada .key para cargarla.
>
> Una vez subidos los archivos .crt y .key, haga clic en el botón APLICAR en la parte inferior de la página.
>
> Después de eso su Panel de Control y el portal se reiniciará y dejarán de estar disponibles durante este proceso. Esto puede tardar hasta 5 minutos. Una vez finalizado el proceso de instalación del certificado, su portal estará disponible sobre HTTPS. El nombre de dominio para el que se emitió su certificado se muestra ahora en la sección Generado para dominio en la página HTTPS del Panel de Control.

Ref:
https://helpcenter.onlyoffice.com/es/server/controlpanel/enterprise/switch-to-https.aspx
https://letsencrypt.org/

Glosario de términos

AP: Access Point o Punto de Acceso inalámbrico.
DNS: Acrónimo de Domain Name Server o Servidor de nombres de dominio, es el sistema encargado de la traducción de los nombres de objetos de red a direcciones IP y viceversa.
Hardening: se refiere al endurecimiento de las configuraciones de los sistemas operativos o programas, para esto se dan de baja servicios innecesarios, se aplican políticas restrictivas de acceso y se cambian los datos por defecto entre otras cosas.
LDAP: El Protocolo ligero de acceso a directorios (en inglés, Lightweight Directory Access Protocol, LDAP) es un conjunto de protocolos abiertos usados para acceder información guardada centralmente a través de la red. Se utiliza en reemplazo del Active Directory de Microsoft(r) y al igual que este permite o deniega el acceso a los distintos sistemas, carpetas compartidas y demás recursos de red.
MAC: dirección física de la tarjeta de red de un dispositivo o computador. Se trata de un identificador que corresponde al fabricante y serie de la interfaz de red y es único para cada dispositivo.
Phishing: técnica utilizada por delincuentes informáticos con el objetivo de “pescar” víctimas engañandolos con hipervínculos falsos, utilizando el spam como medio de propagación para llegar de forma masiva a los usuarios.
PSK: (Pre Shared Key o Clave Compartida Previamente) es la clave que se debe conocer para poder conectarse a la red inalámbrica.
PyMEs: Pequeñas y Medianas Empresas
Radius: (acrónimo en inglés de Remote Authentication Dial-In User Service) es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP.
Shellcodes: Una shellcode es un conjunto de órdenes programadas generalmente en lenguaje ensamblador que se inyectan en la pila para conseguir que la máquina en la que reside se ejecute la operación que se haya programado.
Sniffing: se refiere al monitoreo y captura de paquetes de red para su análisis.
Spam: correo no deseado, usualmente con contenido publicitario o con fines de engaño del usuario.
SSID: (Service Set Identifier) es el nombre de la Red Inalámbrica con el cual se identifica.
Troyano: es una variedad de virus diseñado para actuar desde dentro del sistema infectado, al igual que en la leyenda de Troya, donde los soldados escondidos dentro del caballo de madera abrieron las puertas de la ciudad al ejército que esperaba afuera, el virus troyano abre puertos en el sistema para permitir conexiones y hace una llamada hacia afuera para contactar a un sistema de control que le envía órdenes para que éste ejecute desde dentro.

Virus: Programa malicioso creado para causar algún tipo de daño o alteración en el sistema infectado, generalmente intentan propagarse y reproducirse en otros sistemas vecinos.
Vlan: es un acrónimo que deriva de una expresión inglesa: virtual LAN. Esa expresión, por su parte, alude a una sigla ya que LAN significa Local Area Network. Esto quiere decir que, en una misma red física, pueden establecerse diferentes vlan o redes virtuales.
WPA2: (Wi-Fi Protected Access 2 - Acceso Protegido Wi-Fi 2) es un sistema para proteger las redes inalámbricas

Referencias:

[1] Software libre - El sistema operativo GNU - www.gnu.org Consultada 2 de febrero de 2019.

[2] Enterprise Open Source: A Practical Introduction By The Linux Foundation www.linuxfoundation.org Consultada 2 de febrero de 2019.

[3] Who is Linus Torvalds - Biografía. linustorvaldslinux.weebly.com Consultada 2 de febrero de 2019.

[4] Filtrado perimetral - Firewall - PFSense www.pfsense.org Consultado 2 de febrero de 2019.

[5] DNS configuración en PFSense https://docs.netgate.com/pfsense/en/latest/dns/unbound-dns-resolver.html Consultado 9 de febrero de 2019.

[6] Proxy - Configuración de Squid Proxy en PFSense. https://docs.netgate.com/pfsense/en/latest/cache-proxy/setup-squid-as-a-transparent-proxy.html Consultado 9 de febrero de 2019.

[7] Configurando un servidor de acceso remoto OpenVPN. https://docs.netgate.com/pfsense/en/latest/vpn/openvpn/openvpn-remote-access-server.html

[8] Configurando el paquete SquidGuard https://docs.netgate.com/pfsense/en/latest/cache-proxy/squidguard-package.html Consultado 9 de febrero de 2019.

[9] IDS/IPS PFSense. https://docs.netgate.com/pfsense/en/latest/ids-ips/index.html Consultado 4 de mayo de 2019.

[10] Virtualización - OpenStack https://www.openstack.org Consultado 4 de mayo de 2019.

[11] Virtualización - VirtualBox https://www.virtualbox.org Consultado 4 de mayo de 2019.

[12] Virtualización - Proxmox https://www.proxmox.com/en/ Consultado 4 de mayo de 2019.

[13] Virtualización - Xen https://xenproject.org Consultado 4 de mayo de 2019.

[14] Suite de oficina - OnlyOffice. https://www.onlyoffice.com/es/ Consultado 18 de mayo de 2019.

[15] Instalar OnlyOffice como un contenedor docker. www.techrepublic.com/article/how-to-run-onlyoffice-server-as-a-docker-container/ Consultado 18 de mayo de 2019.

[16] Samba Server Simple - Debian
https://wiki.debian.org/SambaServerSimple consultada 15 de agosto de 2019.
[17] Servidor Debian - Apache2.
https://servidordebian.org/es/stretch/internet/http/apache2 consultada 15 de agosto de 2019.
[18] PostgreSQL - BBDD.
https://www.postgresql.org/download/linux/debian/ consultada 3 de octubre de 2019.
[19] Correo electrónico . Zimbra.
https://zimbra.org/download/zimbra-collaboration/8.8 consultada el 18 de mayo de 2019.
[20] ELK - Elasticsearch - Logstash - Kibana
https://www.elastic.co/es/products/kibana consultada el 15 de agosto de 2019.
[21] Sistema de Backup - Bacula.
http://www.bacula.org
[22] SIEM - OSSIM Alien Vault incluyendo OSSEC, Nagios; Openvas, OTX.
www.alienvault.com consultada el 15 de agosto de 2019.
www.ossec.net consultada el 15 de agosto de 2019.
https://www.nagios.org consultada el 15 de agosto de 2019.
http://www.openvas.org consultada el 15 de agosto de 2019.
https://otx.alienvault.com consultada el 15 de agosto de 2019.

Bibliografía general:

https://servidordebian.org/
http://www.cisco.com
https://www.normas-iso.com/iso-27001/