DEFENSA EN PROFUNDIDAD BASADA EN SERVIDORES.

Luís Eduardo Rico Ávila
luiserico@gmail.com
Universidad Piloto de Colombia

Resumen: Hoy en día la infraestructura de red de las organizaciones cada día es más vulnerable a ataques, por lo cual debemos buscar herramientas que nos brinden asegurar la información mediante software y hardware. En el mercado encontramos diferentes marcas con funcionalidades que nos pueden proporcionar controles pero no una seguridad profunda, por eso es importante conocer la infraestructura que administramos para lograr integrar y asegurar de una manera eficaz los elementos de nuestra con las recomendaciones y buenas practicas que nos brindan los proveedores para mantener una sola firma y una infraestructura asegurada.

Abstract: Today the network infrastructure of organizations is increasingly vulnerable to attack, so we should look for tools that give us secure the information through software and hardware. In the market we find different brands with functionality that we can provide a thorough checks but not safety, it is important to know the infrastructure we manage to achieve integration and ensure effectively the elements of our network with the recommendations and best practices that give us the suppliers and manufacturers to maintain a single firm and a secure infrastructure.

Índice de Términos - Hardening, PDUs, SSH, UPS, WSUS.

I. INTRODUCCIÓN

La seguridad informática se define como un conjunto de medidas técnicas y legales que permiten a las organizaciones asegurar la confidencialidad, integridad y disponibilidad de sus sistemas de información. Se conocen métodos y normas que nos indican los procedimientos para lograr fortalecer nuestros sistemas previniendo que la información sea vulnerada por los atacantes. Una forma de asegurar nuestra infraestructura es la defensa en profundidad la cual nos da a conocer un modelo por capas para prevenir y fortalecer nuestra estructura de red evitando a que sea vulnerado tanto interna como externamente por atacantes con mecanismos de defensa para hacerlos desistir del ataque. Un mecanismo conocido es el llamado Hardening que no nos permite asegurar nuestros servidores con recomendaciones e instrucciones básicas para endurecer nuestros servidores.

II. DEFENSA EN PROFUNDIDAD

La Defensa en profundidad es una estrategia práctica para el aseguramiento de la información y busca mitigar y administrar el riesgo de los elementos que hacen parte de la infraestructura de una red. Las estrategia de la defensa en profundidad requiere la implementación de múltiples obstáculos en una estructura definida para lograr filtrar y detener amenazas a las que están expuesto nuestros recursos físicos y los servicios que son prestados a los usuarios, cada estrategia cuenta con diferentes controles de seguridad disminuyendo el impacto de una intrusión en la red y mejorar la probabilidad de detección.

Los controles de seguridad se deben establecer de acuerdo a la infraestructura de red que las organizaciones estén administrando, debemos conocer los factores y condiciones que conforman la seguridad para planear e implementar una estrategia adecuada de seguridad para el aseguramiento respectivo. Cada uno de las estrategias genera unas tareas y recursos para implementar una estrategia y mantener una infraestructura segura generando costos que a veces no son muy bien vistas por parte de las organizaciones, pero es importante transmitirles el concepto de seguridad para nuestra infraestructura y los daños irreversibles que se pueden obtener sino la aseguramos.

La utilización de múltiples estrategias en defensa en profundidad nos permite estar protegidos de acuerdo a los controles que estén definidos en cada una de ellas, la motivación de tener múltiples capas es que si una capa falla o no puede contra restar una amenaza las otras capas puedan prevenir la amenaza y cumplir con la protección del sistema.

La Fig.1 nos presenta el modelo y el orden de las capas para realizar el aseguramiento de nuestra infraestructura, iniciando de arriba hacia abajo.

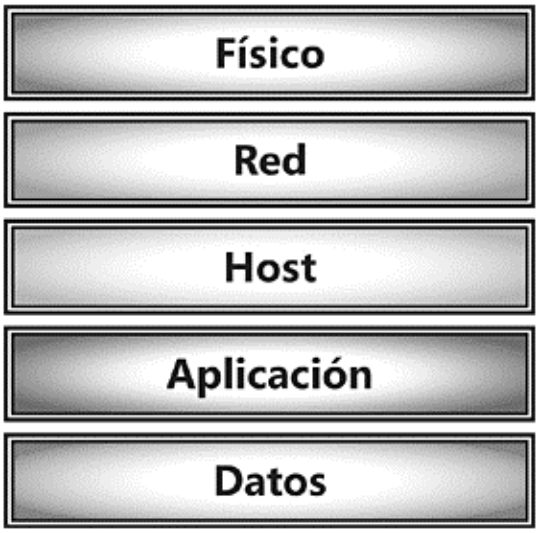

Fig.1. Modelo de defensa en profundidad.
https://www.microsoft.com/spain/technet/recursos /artículos/srsgch06.mspx

III. HARDENING EN SERVIDORES

Hardening significa endurecimiento, y está definido por un conjunto de actividades que son realizadas por los administradores de sistemas operativos para fortalecer la seguridad de los servidores. El objetivo de realizar hardening en los servidores consiste en retardar la acción de un atacante disminuyendo incidentes de seguridad y evitando que el atacante lo concrete en su totalidad.

El aseguramiento del servidor implica hacer configuraciones en el sistema operativo o simplemente atender las recomendaciones de los expertos y fabricantes que nos guían con buenas prácticas para fortalecer nuestros servidores.

De esta forma asegurar el servidor depende del sistema operativo, Windows o Unix. Este procedimiento por la general debe ser documentado para que los administradores lo conozcan y establecer el grado o número de pasos que se realizó para asegurar el servidor. Es importante hacer la verificación correspondiente para no enjaular nuestro servidor con los procedimientos o pasos para asegurar nuestro servidor y salir perjudicados. Los servidores son un elemento importante en las organizaciones ya que con ellos podemos entregar plataformas de alta disponibilidad y servicios a usuarios internos y externos de las organizaciones, estos servidores hoy en día los podemos encontrar físicos y virtuales de acuerdo a la infraestructura que disponga la organización. Un servidor dentro de la estructura de la organización puede brindar un sin número de servicios, como por ejemplo: servidores de archivos, bases de datos, aplicaciones, de autenticación, virtualización, ftp, correo electrónico, actualizaciones y de gestión. El Servidor o host es uno de los elementos que hace parte de la estrategia en la red de la defensa en profundidad.

Un servidor está expuesto a amenazas comunes desde el momento de su conexión física, instalación del sistema operativo y de su conexión a la red, estas Amenazas comunes podemos definirlas como las que se encuentra por defecto, usuarios, puertos, servicios, conexiones de red.

Cuando se realiza una instalación de un sistema operativo, se debe tener los controles básicos como la habilitación de usuarios con los privilegios o roles correctos para tener acceso al servidor, deshabilitar los servicios y puertos que no se utilizan, en muchas ocasiones cuando se realiza la instalación de una aplicación o una base de datos podemos encontrar usuarios y contraseñas definidas por los fabricantes del software y no son cambiadas por los administradores.

Estas amenazas generan vulnerabilidades que son aprovechadas por usuarios no confiables dentro y fuera de las organizaciones generando accesos no autorizados, denegación de servicios y consultas de información confidencial. Es importante tener el conocimiento y la responsabilidad para entender que estas amenazas comunes pueden dejar expuesto nuestros servicios y llegar a comprometer los servicios de la organización.

De acuerdo a nuestra infraestructura independiente del tamaño sea grande o pequeña, tener un espacio donde alojaremos nuestros servidores. Las condiciones de este espacio deben estar diseñadas para que nos brinde alta disponibilidad en caso de una falla. Este espacio donde estarán alojados los servidores, deben tener la disponibilidad de aires acondicionados de acuerdo a la proporción de máquinas y la carga térmica que estos generen, la parte eléctrica debe disponer de una planta, UPS (Sistema de Alimentación Ininterrumpida), PDUs (Unidades de Distribución de Energía) estos elementos son importantes y básicos para disponer de conexiones seguras, redundancia y disponibilidad de los equipos.

Uno de los pasos iniciales para el aseguramiento de los servidores y obviamente para toda una infraestructura de red, es tener claramente identificados todos los activos que la conforman, la descripción mínima de cada componente tanto de software y de hardware.

Teniendo esta base de información nos facilitara rápidamente la identificación de nuestros recursos para definir los planes y acciones a realizar cuando se presenten fallas y amenazas.

Con la información de los sistemas operativos, se empezara a identificar la versión del sistema operativo por ejemplo: Windows 2003 server, Windows 2008 Server o Windows 2012 o para los sistemas operativos Linux, Ubuntu, Centos o Red Hat. Inicialmente cuando se instala cada uno de estos sistemas operativos con

imágenes o propiamente con el cd, ejecutamos una instalación por defecto instalando los servicios iniciales para que inicie el sistema o a veces servicios que no son necesarios, esta nos demuestra que los fabricantes no son conscientes de las necesidades de seguridad de cada organización.
Para corregir estas instalaciones por defecto, los administradores deberán configurar los servidores y realizar reconfiguraciones del caso a medidas que van cambiando los requisitos. Esto se debe hacer bajo un marco de requisitos y políticas de seguridad establecidas por la organización, teniendo guías y listas de chequeo podremos tener la certeza de una administración coherente y eficaz.
Para asegurar un sistema operativo se debe tener en cuenta los siguientes pasos:

A. Actualizar el sistema operativo.

Una vez instalado el sistema operativo se deberán aplicar los parches correspondientes para corregir las vulnerabilidades conocidas, este procedimiento debe realizarse antes de que los servidores sean colocados en producción, no es recomendable realizar estas actualizaciones cuando ya estén prestando sus servicios en producción debido a que se puedan presentar problemas de funcionamiento en el servidor. Las actualizaciones también pueden corregir problemas de compatibilidad, funcionamiento y programación permitiendo un mejor desempeño.
Todos los sistemas operativos son vulnerables la única manera de estar protegidos es realizando las actualizaciones, todo sistema que no tenga las actualizaciones es un riesgo para nuestra red.

B. Eliminar o deshabilitar los servicios innecesarios.

Los servidores pueden entregar varios servicios pero en condiciones normales cada servidor que tengamos dentro de nuestra organización debería estar dedicado a un solo servicio, esto evitaría fallas y confusiones en el momento en que se presenten dificultades con los servicios del servidor. Instalar la configuración mínima del sistema operativo, implica habilitar, añadir y quitar componentes de los servicios, aplicaciones y protocolos de red que se han necesarias para ofrecer un servicio óptimo, la eliminación o desactivación de los servicios innecesarios mejoran la seguridad del servidor. Los administradores tienen la obligación de definir los servicios que se habilitan en el servidor controlando el riesgo ya que en varios casos hay que instalar servidores de archivos, administración remota o web que pueden aumentar el riesgo para el servidor.

C. Configuraciones de autenticación de usuario del sistema operativo.

La configuración de los usuarios autorizados que pueden acceder al servidor a realizar tareas de administración o usuarios que desarrollen una tarea específica, se les debe limitar a pequeños grupos con roles y permisos establecidos para controlar el acceso y comprobar que el usuarios este autorizado para dicho acceso.
Se deben deshabilitar las cuentas que por defecto instala el sistema operativo (cuenta de invitado) estas cuentas por los general vienen sin clave de autenticación y son conocidas por los atacantes.
Crear grupos con permisos y roles para un manejo más efectivo cuando se tienen gran cantidad de usuarios facilitando la administración. No se deben tener cuentas compartidas y solo se deben crear las cuentas necesarias, cada usuario es único en la red y debemos identificar que hace nuestro usuario con la cuenta y los permisos entregados. Debemos temporizar la sesión que el usuario abre en tiempos cortos para evitar intrusiones por parte de otros usuarios poniendo en riesgo disponibilidad e integridad de nuestro servidor.
También es importante tener presente las contraseñas, es un elemento de autenticación el cual nos va a permitir el acceso a nuestro servidor, la complejidad que podamos otorgarle nos da la satisfacción de que no va hacer descifrada rápidamente. La creación de una contraseña debe tener una complejidad en el tamaño, la combinación de los caracteres letras mayúsculas minúsculas, números y caracteres especiales. Utilice siempre contraseñas seguras, utilice diferentes contraseñas para todas las cuentas de usuario, tenga presente la seguridad donde guarda las contraseñas.
Se deben disponer políticas para evitar la reutilización y la renovación periódica de las contraseñas.

D. Seguimiento a la seguridad.

Luego de haber realizado los controles anteriormente mencionados, debemos mantener la seguridad, pero de qué manera podemos controlar y hacerle seguimiento.
Aquí también encontramos varias controles que debemos tener en cuenta para dar esa continuidad luego de tener asegurado nuestro servidor.
Uno de los controles más conocidos en la gran mayoría de los sistemas operativos o diría que en todos es revisar los registros de log del sistema operativo para identificar las alertas y fallas que se estén creando. Este registro es generado en un formato de archivo texto que debe ser analizado cuidadosamente identificando las líneas que nos muestren alertas de advertencia o líneas críticas para tomar las medidas preventivas o correctivas según sea el caso. Los archivos de registro log deben estar sincronizados con n el servicio NTP

para que el reloj interno del sistema sea de tiempos precisos y verídicos a la hora de hacer el análisis.
Otro control es el servicio de backup que garantiza la recuperación de un sistema, los backup son copias de respaldo de información que se generan automáticamente o manualmente. Esta copia luego de ser etiquetada y almacenada correctamente, nos brindara la recuperación en caso de una falla o pérdida de información. Los backup tienen 3 formas para realizar las copias completa, incremental y diferencial. Todos los procesos de copias que se generen deben estar contemplados en la política de seguridad con un procedimiento de retención y recuperación.
Un control que también se puede tener en cuenta, sé que posiblemente por temas de costos no es viable, pero tener servidores en ambientes de prueba o desarrollo con las mismas características de hardware y software del servidor que está en producción, es una opción de control en caso que se presente una falla. Ya que mientras se recupera el sistema podemos utilizar cualquiera de estos 2 ambientes y seguir brindando nuestros servicios. Estos ambientes pueden ser muy interesantes ya que en ellos como sus nombres los indican podemos realizar todas las pruebas y desarrollos antes de llevarlos a los servidores de producción.
Por último podríamos hablar del manejo de incidentes, que debe estar en marcado por las políticas y procedimientos de la organización. Debemos tener un plan de respuesta de incidentes un documento donde se indique el procedimiento, el equipo de respuesta con el conocimiento necesarios para realizar el seguimiento y trazabilidad del incidente, tener una base del conocimiento y documentar lo que se encontró y como se realizó la recuperación. Se debe entregar un informe donde se refiera todo lo contemplado.

IV. SISTEMAS WINDOWS

Los sistemas Windows ofrecen un buen desempeño para nuestros servicios y aplicaciones instaladas, a continuación vamos a indicar algunos pasos y actividades que nos ayudan asegurar nuestro servidor.

A. Preparación e instalación.

La preparación del servidor e instalación del sistema operativo debe realizarse en un lugar adecuado y aislado "área de preparación de equipos" área donde se den unas condiciones de conexión de una red independiente a la red de la organización para evitar tráfico hostil hacia el servidor inicial. Se deben revisar los requisitos físicos del servidor Procesador, memoria, disco duro, para realizar la instalación del sistema operativo, Por recomendaciones el servidor sea físico o virtual debe tener un arreglo de disco RAID para disponer de alta disponibilidad.
Las particiones del disco duro se realizan de acuerdo al tamaño de disco, en lo posible generar dos particiones, una para el Sistema operativo y la segunda para el almacenamiento de información y configuraciones, para efectos de soporte con el fabricante es conveniente que la instalación del sistema operativo sea en idioma inglés.

B. Revisión y actualizaciones.

La actualización de seguridad del sistema operativo deben realizarse inmediatamente se termina la instalación del sistema operativo, este opción la conocemos como Windows update, por lo general está habilitada para que automáticamente inicie una conexión hacia los servidores de Microsoft y realiza las descargas de las actualizaciones correspondientes al sistema operativo que se haya instalado. Terminada las actualizaciones de seguridad se debe deshabilitar las actualizaciones automáticas por razones de disponibilidad de los servicios del servidor, ya que frecuentemente las actualizaciones de seguridad pueden generar problemas en nuestros servidores de producción, es por eso que se recomienda mantener los ambientes de pruebas y desarrollo para hacer las pruebas correspondientes con estas actualizaciones antes de que se han instaladas en ambientes de producción.
Una buena práctica y por seguridad es disponer de nuestro propio servidor de actualizaciones llamado WSUS (**Windows Server Update Services)** el cual nos proporciona las actualizaciones locales sin necesidad de que el servidor se conecte a internet y así mantener mayor seguridad.
Otra herramienta para verificar las actualizaciones de nuestros servidores es suministrada por Microsoft de manera gratuita se llama **Microsoft Baseline Security Analyzer** que determina el estado de seguridad de las actualizaciones, tanto las que hacen falta como las actuales. Las actualizaciones que hace nuestro servidor se clasifican de tres formas, actualizaciones importantes que ayudan a mantener la confiabilidad y la seguridad del servidor, las actualizaciones recomendadas que ayudan a mantener el software actualizado y un rendimiento óptimo del servidor y por último la actualizaciones opcionales que incluyen actualizaciones de software de componentes o controladores de dispositivos que se han conectado a nuestro servidor.

C. Directivas de cuentas de usuario.

La definición de un usuario con su respectiva

contraseña es fundamental para iniciar el proceso de seguridad de nuestro servidor, de esta forma inicia a ser parte de la auditoria interna del server.
Las directivas locales se aplican a los servidores y están definidas como:
Directiva de Auditoria: registra los sucesos de seguridad, intentos de inicio de sesión correctos y fallidos, Asignación de derechos de usuario: Determina los privilegios que tiene el usuario en el server. Opciones de Seguridad: Habilita o deshabilita la configuración de seguridad.
Directiva de contraseñas: para cuentas de usuarios del dominio o locales, definición de contraseña, obligatoriedad y ciclo de vida. Directiva de Bloqueo de Cuentas: para cuentas de usuarios del dominio o locales, determinando el bloqueo de una cuenta.
De esta manera nos permitirá restringir el acceso a nuestro servidor de cualquier usuario que no cumpla con las políticas definidas. No sobra recordar que debemos generar claves que cumplan con las políticas de seguridad de la organización y cumpliendo con lo mínimos requerimientos que son vigencia máxima de la contraseña, longitud mínima de la contraseña por lo menos de 8 caracteres y la complejidad que nos ayudara para que el acceso de un atacante no sea fácil.
Por último tener claro el bloqueo de cuentas, por ejemplo cuando un usuario tiene varios intentos fallidos también se deben definir estas políticas.

D. Controles de acceso de red.

Desactivar los servicios innecesarios en nuestro servidor es un control importante ya que mejora los recursos de la máquina y tenemos una seguridad apropiada.
Tener en cuenta los servicios que debemos desactivar no es tarea facial. Para saber cuáles servicios está ejecutando nuestro servidor, abrimos una ventana del sistema ejecutar y escribimos services.msc el cual nos desplegara una ventana con el nombre de los servicios, seleccionando cada uno nos indicara el estado en que se encuentra el servicio actualmente, iniciar, detener, reiniciar. Cuando realizamos la instalación del sistema operativo algunos servicios vienen configurados y listos para que el sistema los ejecute. Podemos revisar servicios como IIS, Terminal Services, DNS, Active Directory, estos servicios tienen vulnerabilidades conocidas por tal motivo deben ser configurados correctamente para evitar ataques.
De la mano con los servicios también viene el acceso a los puertos que no se estén utilizando, para identificar rápidamente que puertos tiene nuestro servidor abierto podemos utilizar la herramienta nmap (Explorador de red y auditor de seguridad)
Para Windows se puede descargarse libremente de internet y realizar la comprobación de los puertos que tiene el servidor abierto.
Para reforzar la seguridad de puertos, Windows trae un firewall muy robusto el cual nos permite crear reglas de exclusión e inclusión para nuestras aplicaciones y puertos con protocolo UDP y TCP.

E. Auditoria del servidor.

Por último para garantizar que nuestro servidor este con los controles adecuados es habilitar las auditorias del sistema, herramienta del sistema que nos entregara alertas de cambios en las políticas de seguridad, intentos de rompimientos de claves, accesos no autorizados, modificaciones a privilegios de usuario. Esta información es relevante para identificar que pasa en nuestro servidor y actuar rápidamente ante cualquier cambio. Esta opción la podemos encontrar en la siguiente ruta
Configuración del equipo\Directivas\ Configuración de Windows\Configuración de seguridad\ Directivas locales\Directiva de auditoría.

V. SISTEMAS UNIX

Unix es un sistema operativo portable, multitarea y multiusuario, este sistema puede ser manejado gráficamente o por línea de comandos mediante una consola llamada ssh (Secure Shell) esta consola nos proporciona seguridad para la conexión remota hacia nuestro servidor y solo se podrá ejecutar comandos de Unix.

A. Instalación y configuración.

Iniciaremos con las particiones lógicas del sistema operativo permitiendo una separación y protección de los datos. El esquema de particiones lógicas para los sistemas operativos Unix y por recomendación de los fabricantes del sistema operativo debe ser de la siguiente manera /directorio raíz, nivel superior del sistema de archivos, /boot Linux kernel, archivos del gestor de arranque, /etc archivos de configuración, /home directorio principal de usuarios, /usr directorio compartido para usuarios, /opt directorio donde se instala el software y complementos de paquetes, /var directorio de datos variables tales como archivos temporales, archivos de registro, /tmp directorio de trabajo temporal. Las particiones deben tener un tamaño apropiado de acuerdo a los datos y servicios que vaya a prestar el servidor.
Estas particiones por recomendación deben ser creadas con un gestor de volúmenes lógicos LVM para que luego puedan extender los tamaños de los volúmenes si

son requeridos.

B. Actualizaciones

Para realizar las actualizaciones de paquetes de software de los sistemas operativos Unix se realiza con el comando yum, en los sistemas operativos Linux Red Hat para realizar las actualizaciones debe tener una suscripción con el proveedor de lo contrario no va a obtener las actualizaciones. Con el siguiente comando podemos comprobar las actualizaciones.

yum check-update
yum update

C. Cuentas de usuario.

Para los sistemas Unix el usuario administrador se conoce como "root" este usuario contiene los permisos de un administrador de sistema operativo. Algo muy particular con los sistemas Unix es cuando creamos nuevos usuarios y para poder ejecutar o realizar algún cambio en el sistema con este nuevo usuario hay que anteponer el comando (su) o sudo para obtener los privilegios de administrador, este nos permite tener un registro de auditoria sobre cada línea o instrucción ejecutada.

Utilice useradd / usermod para crear y mantener cuentas de usuario. Asegure el servidor con los siguientes comandos:

Revise con el siguiente comando el estado de configuración de una cuenta: # chage -l luis

Con este comando modifica los parámetros de la cuenta.

chage luis

Aquí podrá modificar los valores de cada uno de los ítems y asegurar la cuenta de usuario.

Minimum Password Age [0]:
Maximum Password Age [99999]:
Last Password Change (YYYY-MM-DD)
Password Expiration Warning [7]:
Password Inactive [-1]:
Account Expiration Date (YYYY-MM-DD)

Para las contraseñas tenemos la opción de forzar el cambio de contraseñas, para que los usuarios no reutilicen para este se fijan tiempo de 90 a 360 días.

Con el comando podemos realizar los ajustes para forzar el cambio de una contraseña: La M nos da el tiempo de vida de la contraseña, m el primer cambio que debe realizarse, W la longitud mínimo de la contraseña.

chage -M 60 -m 7 -W 7 USER

Verifique el inicio de sesión del usuario con el comando.

last

Quien se encuentra conectado a sus servidor con el comando # w o who.

D. Controles de acceso de red.

TCP Wrapper ("Envoltorio de TCP") es un sistema de red ACL que trabaja en terminales y que se usa para filtrar el acceso de red a servicios. Unix trae dos directorios que permiten o deniegan el acceso a servicios del servidor. Los podemos encontrar en esta ruta # /etc/hosts.allow verifica y si encuentra una regla que coincide permite la conexión y # /etc/hosts.deny verifica y si encuentra una regla que coincide deniega la conexión.

Otra forma de controlar es el firewall en Unix conocido como iptables, es bastante robusto ya que en el podemos aceptar y denegar conexiones de red, con los siguientes comandos podemos revisar el firewall de nuestra máquina.

Verificar el estado del firewall

iptables –nL –line-numbers

Ingresar una regla que permita la conexión a un puerto.

iptables -I INPUT 4 -m state --state NEW -m tcp -p tcp --dport 5555 -j ACCEPT

iptables -I INPUT 8 -s 172.28.13.23 -m state --state NEW -p tcp --dport 1521 -j ACCEPT

Terminada las configuraciones para que se guarden nuestras nuevas reglas ejecutamos:

Service iptables save
Service iptables restart

E. Servicios.

Determinar los servicios que se están ejecutando en nuestro sistema operativo Unix es bastante fácil, con los siguientes comandos vamos a identificar los servicios que se están ejecutando actualmente.

chkconfig --list | grep :on

Si queremos deshabilitar un servicio ejecutamos el siguiente comando:

chkconfig srvname off

Unix inicia algunos servicios por defecto, por lo cual debemos tener en cuenta y tener cuidado con algunos servicios que vamos a mencionar.

Servicios de impresión, consola, servicios web (httpd, mysqld y postgresqld), servicio nfs, samba, shh, vnc, telnet, ftp. Se pueden identificar con el siguiente comando los servicios registrados.

ls –l /etc/init

Lista los servicios en ejecución.

initctl list

Si estos servicios no son necesarios en nuestro servidor por seguridad debemos deshabilitarlo.

Con el siguiente comando se pueden listar los puertos abiertos y asociar los programas.

netstat -ltup

netstat -ltup | grep http

F. Servicio secure shell

El servicio ssh (Secure Shell) es un protocolo de comunicación segura, utiliza una arquitectura cliente/ servidor permitiendo a los usuarios hacer conexión remota hacia un host.

Si vamos a habilitar este servicio debemos realizar una configuración adecuada.

Para realizar la configuración de este servicio buscamos la ruta /etc/ssh/sshd_config, debemos hacer algunos cambios a este archivo:

Port
Puerto ssh (Por defecto 22) se debe cambiar
Protocol
Versión shh (1 or 2)
PermitRootLogin
Permite el inicio de sesión no
PermitEmptyPasswords
Permite la contraseña vacía no
AllowUsers user1 user2
Lista de usuarios permitidos.
DennyUser user1 user2
Listado de usuarios no autorizados.
LoginGraceTime
Tiempo de espera de inicio de sesión.
MaxAuthTries
Intentos máximos para iniciar sesión.

G. Auditoria del servidor.

Para determinar las advertencias y fallas de nuestro sistema es necesario identificar donde se guardan el log del sistema. El demonio rsyslogd es responsable de recolectar los mensajes de servicio que provienen de aplicaciones y el núcleo para luego distribuirlos en archivos de registros (usualmente almacenados en el directorio /var/log/). Obedece a su archivo de configuración: /etc/rsyslog.conf.

Para iniciar este servicio digitamos el comando:

chkconfig rsyslog on

Para que los log este sincronizados y nos informe la hora exacta de los eventos es importante la configuración del protocolo (Network Time Protocol) el cual sincronizara el reloj del sistema.

Esta sincronización se debe realizar hacia un servidor en internet o con un servidor de la red que tenga el servicio NTP. En la siguiente ruta se configura el servicio /etc/ntp.conf/.

VI. CONCLUSIONES

Realizando la consulta e investigación para el aseguramiento de la información bajo la seguridad en profundidad se encuentran estrategias para fortalecer nuestra infraestructura, cada capa con un objetivo diferente pero que se deben complementar cada una con las otras iniciando desde la parte física infraestructura corriente eléctrica, aires acondicionados y finalizando con los datos. Lograr el aseguramiento total implica conocer en profundidad la infraestructura y aplicar las políticas de acuerdo a los servicios y aplicaciones que se estén ejecutando en los servidores cada sistema operativo trabaja con instalaciones y servicios diferentes para realizar los controles y el endurecimiento sin afectar a los usuarios. Asegurar los servidores no implica comprar dispositivos robustos ni software fuera de lo común el aseguramiento lleva un estudio y conocimiento previo para lograr buenas políticas y herramientas que nos permita actuar ante una falla de seguridad. Asegurar plataformas Windows y Unix es un tema bastante amplio por lo cual se debe identificar en cada sistema operativo las herramientas disponibles que vamos a utilizar, tener el conocimiento básico de los sistemas operativos para seguir los procedimientos y recomendaciones y en la ejecución de los comandos básicos para lograr el objetivo.

REFERENCIAS

[1]Windows 2003 Server Hardening Checklist http://security.utexas.edu/admin/win2003.html

[2]Windows 2008R2 Server Hardening Checklist https://wikis.utexas.edu/display/ISO/Windows+2008 R2+Server+Hardening+Checklist.

[3]Windows Server 2012 R2 Hardening Checklist https://wikis.utexas.edu/display/ISO/Windows+Serv er+2012+R2+Hardening+Checklist

[4] CIS_Microsoft_Windows_Server_2008_R2_Bench mark_v2.1.0 https://benchmarks.cisecurity.org/tools2/windows/CI S_Microsoft_Windows_Server_2008_R2_Benchmar k_v2.1.0.pdf

[5] Guide to the Secure Configuration of Red Hat Enterprise Linux5. Revision 4.1: Operating Systems Division UNIX Team of the Systems and Network Analysis Center. https://www.nsa.gov/ia/_files/os/redhat/rhel5-guide-i731.pdf

[6]Red Hat Enterprise Linux Security Guide: https://access.redhat.com/documentation/enUS/Red_ Hat_Enterprise_Linux/7/pdf/Security_Guide/Red_H at_Enterprise_Linux-7- Security_Guide-en-S.pdf.

[7]Linux server hardening Security Tips 20 http://www.cyberciti.biz/tips/linux-security.html

[8]Figura Modelo de defensa en profundidad. https://www.microsoft.com/spain/technet/recursos /artículos/srsgch06.mspx.