ROBUSTECIMIENTO DE SISTEMAS

HARDENING o BASTIONADO

- Hardening (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas.

- Otros nombres: bastionado, securizado, hardening

Bastionado

- **Un conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de su equipo**

- Para desarrollar un proceso de **hardening** efectivo es necesario analizar los sistemas que forman parte de una organización, para detectar fortalezas y, sobre todo, aquellas debilidades que podrían suponer una puerta abierta a los ciberdelincuentes.

Como se realiza?

- Eliminar todo aquel software que la empresa ya no use o que esté obsoleto.
- Eliminar aquellos servicios que ya no son necesarios para la empresa y que pueden suponer un riesgo para la seguridad.
- Eliminar datos de acceso, permisos y privilegios que tuvieran todos aquellos usuarios que ya no formen parte de la organización.
- Actualizar el firmware de los equipos a su última versión para que incluyan las nuevas opciones de ciberseguridad.

Como se realiza?

- Cerrar todos aquellos puertos que ya no se usen.
- Instalar sistemas operativos y software de forma segura, y mantenerlos actualizados a su última versión.
- Implementar las herramientas antivirus o antimalware necesarias para evitar, prevenir o actuar rápidamente ante ataques eternos.
- Desarrollar una política de contraseñas segura, mediante el uso de passwords seguros.

- Un proceso de hardening adecuado permite mitigar ataques tipo *Zero Day* ya que el bastionado de sistemas va más allá de seguir las configuraciones por defecto de un fabricante. Se evita el robo de datos, suplantación de identidades, ataques tipo Ransomware ..etc.

Herramientas que se usan son:

- Nessus vulnerability security scanner
- Microsoft Baseline Security Analyzer
- Herramientas Microsoft sysinternals.
- Herramientas de auditoría técnica de seguridad

Referencias y directrices

-INTECO (Instituto Nacional de Tecnologías de la Comunicación), que proporciona guías para asegurar servidores, etc. Se pueden buscar las guías en: ***http://www.inteco.es***.
-CCN (Centro Criptológico Nacional), que bajo registro proporciona guías para securizar sistemas operativos Windows Server, Red Hat Linux, Suse, Debian, etc.
-NIST (National Institute of Standards and Technology), que proporciona una extensa biblioteca sobre seguridad de la información.
-CIS (Center for Internet Security), que proporciona una extensa colección de guías de comparación o benchmarking, de robustecimiento de distintos sistemas (Windows, Linux, etc.).

- Guías STIG
- Guías de seguridad CCN.
- Guías de bastionado Microsoft.
- Controles CIS.

Principios:

- **Mínima exposición**: consiste en reducir al mínimo el número de componentes y servicios del sistema que se encuentren expuestos al exterior, ocultando o eliminando aquellos que no sean esenciales para el funcionamiento del sistema o no se utilicen. De esta manera, se reduce la superficie de ataque del sistema, es decir, la cantidad de componentes y servicios que pueden ser atacados por un atacante.
- **Defensa en profundidad**: implementación de medidas de seguridad en varias capas o niveles del sistema. La idea es que, en caso de que un atacante consiga superar una capa de seguridad, se encuentre con otras capas adicionales que protegen el sistema.
- **Mínimo privilegio**: esta práctica se basa en el concepto de que cada usuario o proceso tenga el mínimo de privilegios, solamente los necesarios para realizar su trabajo. Esto significa que cada usuario o proceso debe tener acceso solo a los recursos y funciones que necesita para su trabajo, y no a más.
- **Confianza cero**: también conocido como zero trust, es un enfoque que se basa en la idea de que, por defecto, se debe de desconfiar de todos los usuarios o dispositivos, lo cual exige verificar la identidad y la actividad de todos los usuarios y dispositivos.

Tipos de protección:

PROTECCIÓN MEDIA

- Fortificación de la estructura informática de la empresa.
- Fortificación de redes inalámbricas.
- Análisis de tráfico de la organización con IPS para la detección de virus e intrusiones.

PROTECCIÓN AVANZADA

- Integración de honeypots como herramienta señuelo.
- Creación de redes virtuales para minimizar el riesgo y las amenazas.
- Fortificación de redes a través firewall de nueva generación.
- Protección y replicación de datos.

MEDIDAS

Medidas Sistemas: Seguridad de la información

- Autenticidad, Confidencialidad, Integridad de la Información.
- Aplicación de la criptografía a la seguridad de la información.
- Técnicas para el cifrado de información confidencial.
- Certificados Digitales, Gestión de PKI (Public Key Infraestructure).
- Aplicación de la Firma digital.
- Facturación electrónica.

Medidas: Autenticación y Gestión de identidades

- Políticas y procedimientos de seguridad para los procesos de autenticación.
- Autenticación de dos factores, utilización de tarjetas criptográficas (smart-card logon).
- Sistemas de Single Sign On (SSO).
- Autenticación remota de usuarios, utilización de servidores de autenticación RADIUS.
- Acceso remoto a la red interna mediante conexiones VPN.

Medidas: Seguridad perimetral

- Diseño y definición de modelos para el establecimiento del perímetro de seguridad.
- Configuración de políticas y reglas de filtrado de cortafuegos.
- Configuración segura de servidores y servicios sobre la DMZ.
- Comunicaciones seguras a servicios internos a través de conexiones IPSEC.
- Establecimiento de túneles “cifrados” para conexión entre delegaciones. (Túneles IPSEC).
- Establecimiento de túneles VPN mediante el protocolo SSLAcceso seguro mediante SSL a servidores Web y servidores de Correo.

Medidas: Seguridad en redes inalámbricas

- Configuración de dispositivos inalámbricos : Punto de acceso. Tarjetas inalámbricas.
- Autenticación WPA2 basada en Radius: Elementos necesarios. Servidor RADIUS. Directorio Activo. Certificados. Configuración de la autenticación PEAP.

Medidas: Seguridad en portátiles y sistemas móviles

- Seguridad física/lógica para el control de acceso: Seguridad de inicio en sistemas Windows y Linux. Seguridad de contraseñas. Sistemas de autenticación biométricos.
- Cifrado de la información confidencial: Cifrado simétrico mediante contraseña única. Cifrado asimétrico mediante llave publica/privada (GPG). Herramientas para repositorio de contraseñas.
- Control de dispositivos removibles, memorias, discos USB,…: Riesgos en el uso de dispositivos de almacenamiento externos. Control de acceso y utilización de dispositivos externos (DEVICELOOK)
- Medidas de seguridad en smartphones y tablets: Seguridad dispositivo. Seguridad aplicaciones instaladas.

FIREWALLS

- Son sistemas de alta seguridad que filtran el tráfico de red entrante y saliente por medio de una serie de reglas, que permitirán su paso o lo rechazarán.

- Son soluciones imprescindibles tanto para el funcionamiento cotidiano en la **oficina** como para asegurar los accesos entre delegaciones o de personal en teletrabajo.

UTM (UNIFIED THREAD MANAGEMENT)

- Este sistema ofrece como su nombre indica una gestión unificada de las amenazas con más funcionalidades:
  - registro de eventos, monitorización, filtrado de tráfico, control de aplicaciones, seguridad del correo electrónico, DLP (Data Leak Prevention) o antivirus.

NGFW (NEXT GENERATION FIREWALLS)

- Es un cortafuegos de nueva generación indicado para organizaciones con un gran número de conexiones, tipo data centers, o empresas que proporcionan soluciones basadas en la nube.

SEGMENTACION DE REDES

- Para aumentar la seguridad de la **red de la empresa**, la dividimos en distintas subredes más pequeñas.

- La compartimentamos con cortafuegos o firewalls, estableciendo protocolos para controlar el acceso en función de niveles de usuarios.

ANTIVIRUS Y FILTROS ANTISPAM

- Protegemos los equipos de trabajo, fijos y móviles, de nuestros empleados mediante técnicas y tecnologías que ofrecen una seguridad superior a los sistemas antimalware tradicionales.

ZONAS DMZ

- Son áreas ‘desmilitarizadas’, en la que hay una red aislada dentro de la red interna de la organización.

- En ella están los recursos de la **empresa**, como el servidor web o de correo, permitiendo las conexiones tanto procedentes de internet como de la red local.

- La empresa queda protegida en caso de ciberataque y se garantiza su funcionamiento.

Ejemplo Bastionado LINUX

- https://www.incibe-cert.es/blog/bastionado-sistemas-el-caso-linux

Algunas acciones

- **Control de cuentas de usuario**: podemos configurar el control de cuentas de usuario de Windows de diferentes formas. Es interesante la opción de permitir exclusivamente ejecutables con firmas válidas para ser lanzados con privilegios elevados.
- **Asociaciones de archivo**: podemos retirar asociaciones de programas predeterminados para archivos que puedan ser perjudiciales o no utilicemos a menudo.
- **Ajustes de seguridad de Windows**: aquí tenemos una buena lista de tweaks a nuestro alcance, por ejemplo deshabilitar el motor de scripting de Windows (Script host), habilitar DEP (Data Execution Prevention) o mostrar archivos y extensiones ocultas.
- **Ajustes de software vulnerable**: podemos aplicar más o menos restricciones a aquellos programas o protocolos con mayor índice de ataque, como puede ser Flash, secuencias JavaScript, macros, etc.
- **Servicios de Windows**: podemos desactivar servicios de Windows innecesarios, como puede ser el spooler (impresión), Bluetooth
- **Firewall de Windows:**

Acciones básicas (I)

- **Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina**. upgrade de firmware, el establecimiento de contraseñas complejas para el arranque del equipo y la configuración de la BIOS, la deshabilitación de inicio de sistema para cualquier unidad que no sea el disco duro principal, y en casos de servidores, la deshabilitación de dispositivos ópticos, usb o similares.
- **Instalación segura del sistema operativo**. considerar al menos dos particiones primarias (1 para el sistema operativo en sí y otra para carpetas y archivos de importancia), el uso de un sistema de archivos que tenga prestaciones de seguridad.
- **Activación y/o configuración adecuada de servicios de actualizaciones automáticas**, parches de seguridad .

Acciones (II)

- **Instalación, configuración y mantención de programas de seguridad** tales como Antivirus, Antispyware, y un filtro Antispam según las necesidades del sistema.
- **Configuración de la política local del sistema**, **Política de contraseñas robusta**, con claves caducables, almacenamiento histórico de contraseñas (para no usar contraseñas cíclicas), bloqueos de cuentas por intentos erróneos y requisitos de complejidad de contraseñas.
- **Renombramiento y posterior deshabilitación de cuentas estándar del sistema**, como administrador e invitado.
- **Asignación correcta de derechos de usuario**, de tal manera de reducir las posibilidades de elevación de privilegios, y tratando siempre de limitar al mínimo los privilegios y/o derechos de los usuarios activos.

Acciones (III)

- **Restricciones de software**, basado en lo posible en el uso de listas blancas de software permitido más que en listas negras del mismo.
- **Activación de auditorías de sistema**, registro de algunos intentos de ataque.
- **Configuración de servicios de sistema**. deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema.
- **Configuración de los protocolos de Red**. recomendable usar sistemas de traducción de direcciones (NAT) para direccionar los equipos internos de una organización. Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los mismos al mínimo.
- **Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema**. denegar explícitamente cualquier permiso de archivo a las cuentas de acceso anónimos o que no tengan contraseña.
- Proteger frente a escritura las subcarpetas dentro de C:\WIndows

Acciones (IV)

- **Configuración de opciones de seguridad de los distintos programas**, como clientes de correo electrónico, navegadores de internet y en general de cualquier tipo de programa que tenga interacción con la red.
- **Configuración de acceso remoto**. deshabilitar el acceso remoto.
- **Configuración adecuada de cuentas de usuario**, tratando de trabajar la mayor parte del tiempo con cuentas de acceso limitado y deshabilitando las cuentas de administrador.
- **Cifrado de archivos o unidades según las necesidades del sistema**.
- **Configuración de las directivas de gestión de contraseñas y privilegios en el directorio de usuarios**

- Eliminar Powershell en todo lo posible
- Desactivar fuentes no confiables de Windows 10
- Activar la detección de PUA de Windows (PUA = Aplicación potencialmente no deseada
- Activar o desactivar asistencia remota en Windows, Consola remota o Registro Remoto

Algunas GUIAS

- IMPLEMENTACIÓN DE SEGURIDAD SOBRE MICROSOFT WINDOWS 10 (CLIENTE MIEMBRO DE DOMINIO)
- https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2362-ccn-stic-599a-seguridad-en-windows-10-enterprise-cliente-miembro-de-dominio-anexoa-ens/file?format=html
- BASTIONADO WINDOWS SERVER
- https://abdulet.net/guia-de-bastionado-de-microsoft-windows-server/

Por ejemplo para Contraseñas existes estas recomendacionesç:

Directrices en guías CIS

Para Windows Server 2016, se establecen los siguientes elementos a configurar, desde las políticas de grupo del directorio activo para los requisitos de las contraseñas:

-(1.1.1.5.2.2) Longitud mínima de la contraseña de 8 caracteres, salvo en entornos de alta seguridad, donde se recomiendan 14 caracteres.

-(1.1.1.5.2.3) Tiempo de caducidad máxima de la contraseña de 60 días.

-(1.1.1.5.2.5) Tiempo de caducidad mínima de la contraseña de 1 día.

-(1.1.1.5.2.6) Complejidad de la contraseña requerida.

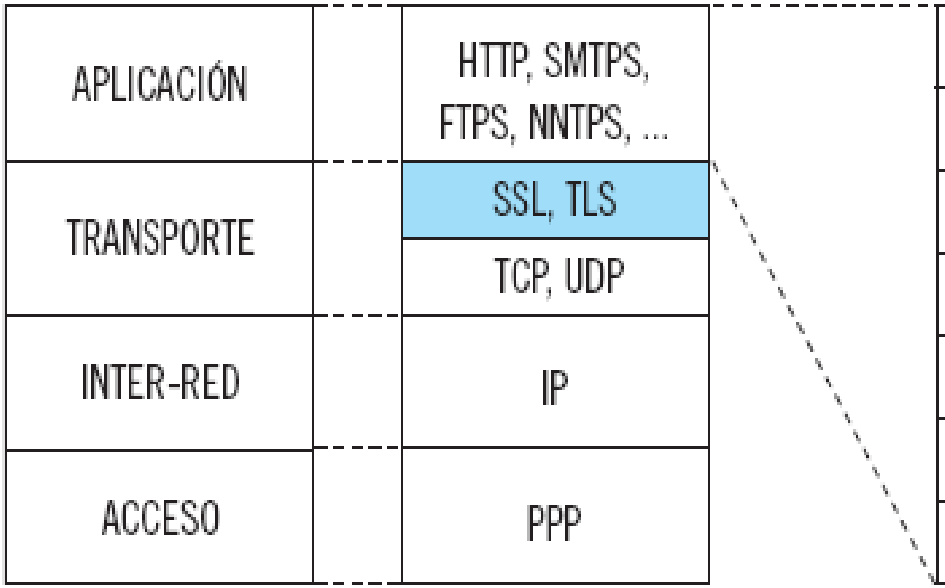
-(1.1.1.5.2.4) Histórico de contraseñas a recordar, para no repetir ninguna de las últimas 24 contraseñas empleadas.

-(1.1.1.5.2.1) Deshabilitar almacenamiento de contraseñas con cifrado reversible.

Protocolos seguros

Los protocolos de transporte seguro SSL y TLS permiten la implementación segura de los servicios de la capa de aplicación (HTTPS, SMTPS, NNTPS, etc.)

Modelo TCP/IP (RFC 1122)



Protocolo	Comentario	Puerto
https	HTTP sobre SSL	TCP 443
smtps	SMTP sobre SSL	TCP 465
ftps	FTP sobre SSL	TCP 989,990
nntps	NNTP sobre SSL	TCP 563
ldaps	LDAP sobre SSL	TCP 646
...		