



UTN.BA

UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Guia de hardenizado de equipos

Esta guía de hardening y buenas prácticas está diseñada para ayudar a fortalecer tu servidor y proteger la información que gestiona.

Desde la configuración de contraseñas sólidas hasta la implementación de medidas de seguridad mas avanzadas, se iran tratando los temas con un enfoque para un publico que si bien puede o no ser tecnico, tiene conocimientos de nivel basico a intermedio.

Tambien la mayoría de los comandos estan enfocados en la administracion de servidores basados en distribuciones de Debian (por ser los mas ampliamente extendidos en el mercado), si bien la mayoría son compatibles con otros sistemas basados en Linux pueden no estar todas las herramientas instaladas por defecto en otras distros.

Si se requieren medidas de seguridad mas avanzadas por favor contactarse con el equipo de administracion.

Consideraciones generales y buenas practicas

Con el fortalecimiento del sistema, el objetivo es eliminar tantos riesgos de seguridad como sea posible. Al minimizar la superficie de ataque, los agentes maliciosos tienen menos medios de entrada o puntos de apoyo potenciales para iniciar un ciberataque.

La superficie de ataque se define como una combinación de todos los posibles defectos y puertas traseras de la tecnología que podrían explotarse. Estas vulnerabilidades suelen incluir:

- Servicios ociosos expuestos
- Contraseñas o credenciales por defecto almacenadas en archivos accesibles
- Software y firmware sin parches
- No se han establecido correctamente los permisos de los usuarios
- Herramientas de ciberseguridad mal configuradas
- Datos sin encriptar

Servicios ociosos expuestos

Al momento de poner en produccion un servidor se tiene que tener en claro la funcion que va a cumplir, por ejemplo, un servidor que se dedica exclusivamente a gestionar bases de datos, no deberia tener el servicio de correo habilitado (cosa que suele pasar ya que en algunos SO viene por default).

Al momento de realizar la instalacion del SO se debe comprobar que servicios tiene habilitados y cuales estan expuestos, tanto hacia el resto de la red como en localhost.

El comando:

```
systemctl list-unit-files --type=service
```

Nos listara todos los servicios instalados y su estado, los que no se esten utilizando deberian ser desinstalados o como minimo deshabilitarlos.

```
systemctl disable postfix #Deshabilita el servicio
Systemctl daemon-reload #Recarga la configuración del sistema
```

Otra forma de ver que servicios tenemos expuestos es la herramienta de línea de comandos para investigar sockets de red **ss**, que permite ver información detallada sobre conexiones de red, puertos abiertos y sockets, se deja un ejemplo de su uso, los flags pueden cambiar sujeto a la necesidad de lo que se este buscando.

```
ss -tulpn
#-t: Muestra solo las conexiones TCP.
#-u: Muestra solo las conexiones UDP.
#-l: Muestra solo las conexiones que están escuchando en lugar de las que están establecidas o en estado de espera.
#-p: Muestra el proceso que está utilizando el socket.
```



LOS SERVIDORES PUESTOS EN PRODUCCION SOLO DEBEN TENER HABILITADOS LOS SERVICIOS MINIMOS Y NECESARIOS QUE VAYAMOS A CONSUMIR, SIN EXCEPCION

Manejo de credenciales

Para los accesos al servidor se desaconseja fuertemente el acceso mediante el uso directo de password. se requieren protocolos de autentificación cifrados como SSH, si bien la Private Key debería tener contraseña también, por lo que se dejan recomendaciones para su implementación.

Para el manejo de credenciales se aconseja fuertemente el uso de un gestor de credenciales de pago o gratuito es indistinto mientras que el gestor pago sea de una empresa reconocida y que las contraseñas almacenadas queden guardadas en algún archivo ENCRIPTADO, el autor de esta guía tiene como preferido [KEEPPASS](#) que es feo como el solo, pero opensource, self-hosted y cumple con los requerimientos de seguridad.

La password de administrador como la de los usuarios administradores del servidor solo debe tenerla EL MINIMO NECESARIO DE PERSONAS, debe ser una password random (cualquier gestor de contraseñas tiene la opción de generar contraseñas seguras) con un mínimo de 15 caracteres y debe contener mayúsculas minúsculas, símbolos y números.

Con respecto al tiempo de vida de las mismas 1 año es suficiente, no es necesario cambiarlas cada cortos periodos de tiempo sino cuando se tenga **CUALQUIER INDICIO** de que puede estar comprometida, ya sea porque se tenga sospechas de que se comprometió el equipo de uno de los administradores o hubo algún cambio en el equipo de administración.



NO DEJAR PASSWORD POR DEFAULT DE NINGUNA APLICACION



NO DEJAR QUE NINGUNA APLICACION ALMACENES CREDENCIALES "SIN ENCRIPTAR" NI EN ARCHIVOS DE CONFIGURACION NI EN LOGS



[GUIA PARA EL ENVIO DE PASSWORDS PLANAS Y ARCHIVOS QUE NECESITEN SER ENCRIPTADOS](#)

Actualizaciones

El objetivo principal de este apartado es hacer énfasis en la necesidad que tanto el SO como las aplicaciones que estén expuestas estén lo más actualizadas posibles cada actualización que implementamos es más que una simple mejora, es una barrera adicional contra las amenazas que evolucionan constantemente.

Teniendo en cuenta que algunas de estas actualizaciones pueden tener como consecuencia tiempo de caída del servicio y esto en un servidor debe minimizarse se entiende que no estén configuradas para realizarse automáticamente, pero se aconseja una vez por mes como mínimo realizarlas manualmente, pudiendo postergarlas solo si se requiere el reinicio del equipo al tiempo mínimo para planificar dicho reinicio.

En el caso de no tener problema con pequeños reinicios periódicos ya que el servicio implementado no tiene tal nivel de criticidad y se quiera abstraerse del tema actualizaciones, en sistemas Windows es mucho más evidente y fácilmente configurable la sección de actualizaciones automáticas, pero en sistemas Linux existen también soluciones fácilmente implementables como [UnattendedUpgrades](#) para distribuciones basadas en Debian o [DNF-AUTOMATIC](#) para distros Red Hat, los cuales también guardan un registro de los paquetes actualizados y hasta permiten su envío vía mail al administrador, se deja el link con el manual de configuración.

Permisos de los usuarios

Para todo servidor se debe evitar el uso del usuario administrador, para esto cada administrador del equipo debe tener su usuario personal solo con los accesos necesarios siguiendo el principio de mínimos privilegios, el cual escapa del alcance de esta guía pero se recomienda leer este breve [ARTICULO](#) para entender el concepto.

En SO basados en Unix el comando "su" permite cambiar de usuario, en el caso de un atacante tratará de impersonarse como un usuario con más privilegios como "root", para evitar esto se debe crear un grupo en el que solo sus integrantes puedan utilizar este comando:

```
groupadd sugroup #crea el grupo sugroup
#Modificar el archivo /etc/pam.d/su
#Agregar la linea
auth    required pam_wheel.so    use_uid group=sugroup
```

Porque no usar el comando "su"?...

Un usuario que pueda autenticarse como root permisos para ejecutar cualquier otro comando sin ningun control, para resolver este problema existe el comando "sudo" que se explicara mas adelante su configuracion, pero permite una ejecucion con permisos mas especificos de comandos y la posibilidad de realizar una auditoria sobre estos al dejar un log de cada usuario que lo ejecuto, con su fecha y el comando.

🔄Revisión #16

★Creado 23 mayo 2024 23:00:30 por Federico Alberto Bisso

✍Actualizado 26 septiembre 2024 16:01:42 por Federico Alberto Bisso