DGTIC UNAM

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

GUÍA DE SEGURIDAD DE LA INFORMACIÓN EN SISTEMAS OPERATIVOS

Código:	20230223_DGTIC-GuíaSeguridadSistemasOperativos			
Versión	1.0	**Fecha**	22 de febrero de 2023	
Vigencia	**Inicio**	22 de febrero de 2023	**Fin**	01 de marzo de 2024
Creado / redactado por:	Ing. César Varela Cruz (CVC) Ing. Andrés Martínez López (AML)			
Autorización:	M. en C. Carlos Raúl Tlahuel Pérez (CRTP) M.C. Luis Ledezma Molina (LLM) Ing. Julio César Roldán Elorza (JCRE)			
Nivel de confidencialidad:	Uso público			

Contenido

Objetivo

El presente documento tiene como propósito establecer lineamientos y recomendaciones en seguridad de la información aplicables a la instalación, administración y/o actualización de sistemas operativos que están a cargo de las entidades y dependencias universitarias de la Universidad Nacional Autónoma de México (UNAM) a fin de robustecer la seguridad de los activos universitarios.

Alcance

El alcance de los lineamientos y recomendaciones es aplicable a los activos institucionales de la UNAM. Están dirigidos al personal universitario que interviene en el proceso de instalación, administración y/o actualización de sistemas operativos en activos institucionales.

Usuarios (público objetivo)

Los presentes lineamientos y recomendaciones son aplicables por los responsables de los activos institucionales de la UNAM y las áreas vinculadas de manera directa o indirecta con los servicios, activos de información, aplicaciones e infraestructura que los soportan.

Consideraciones generales

Se recomienda al menos una revisión anual de la implementación de los presentes lineamientos y cada vez que haya cambios significativos en el sistema operativo y/o aplicativos en los activos de las entidades y dependencias universitarias.

1. Permisos en archivos de configuración

Verificar permisos de archivos ya que la incorrecta configuración de dichos permisos puede dar lugar a la infiltración de información sensible o puede crear un posible vector de ataque, el cual puede ser ocupado para acceder al sistema o para realizar la elevación de privilegios dentro del sistema.

índice	Archivos	Permisos máximos
1.1	/etc/motd	0644/-rw-r--r--
1.2	/etc/issue	0644/-rw-r--r--
1.3	/etc/issue.net	0644/-rw-r--r--
1.4	Archivos predeterminados de rsyslog	0640/-rw-r-----
1.5	Archivos dentro de /var/log/	0640/-rw-r-----
1.6	/etc/crontab	0600/-rw-------
1.7	/etc/cron.hourly	0700/drwx------
1.8	/etc/cron.daily	0700/drwx------
1.9	/etc/cron.weekly	0700/drwx------
1.10	/etc/cron.monthly	0700/drwx------
1.11	/etc/cron.d	0700/drwx------
1.12	eliminar /etc/cron.deny y asignar estos permisos a /etc/cron.allow	0600/-rw-------
1.13	eliminar /etc/at.deny y asignar estos permisos a /etc/at.allow	0600/-rw-------
1.14	/etc/ssh/sshd_config	0600/-rw-------
1.15	/etc/ssh/ssh_host_*_key	0600/-rw-------
1.16	/etc/ssh/ssh_host_*_key.pub	0644/-rx-r--r--
1.17	/etc/passwd	0644/-rw-r--r--
1.18	/etc/passwd-	0644/-rw-r--r--
1.19	/etc/shadow	0000/----------
1.20	/etc/shadow-	0000/----------
1.21	/etc/gshadow-	0000/----------
1.22	/etc/gshadow	0000/----------
1.23	/etc/group	0644/-rw-r--r--
1.24	/etc/group-	0644/-rw-r--r--
1.25	Todos los directorios de inicio de los usuarios	0750/drwxr-x---
1.26	Verificar que no existan permisos de escritura para "otros" usuarios	-xxxxxxx-x
1.27	Asegúrese de que no existan archivos o directorios sin dueño	
1.28	Asegúrese de que no existan archivos o directorios desagrupados	
1.29	Verificar la integridad de todos los archivos que tengan habilitado el SUID	4xxx/-xxsxxxxxx

1.30	Verificar la integridad de todos los archivos que tengan habilitado el SGID	2xxx/-xxxxxsxxx

2. Actualizaciones de software

Configurar actualizaciones de software, ya que mantener el software actualizado, obteniéndolo de fuentes fiables, permite mantener los últimos parches de seguridad para mantener su sistema protegido de las nuevas vulnerabilidades descubiertas.

2.1 Asegúrese de que las claves GPG estén configuradas
2.2 Asegúrese de que los repositorios del administrador de paquetes estén configurados
2.3 Asegúrese de que gpgcheck esté activado globalmente

3. Verificación de Servicios

Verificar servicios habilitados y desinstalar servicios innecesarios, ya que el poseer servicios o tecnologías en el sistema pueden representar un posible vector de ataque por lo que se considera una buena práctica el enfocarse en mantener actualizadas y configurar correctamente los servicios necesarios y desinstalar los innecesarios.

3.1 Servicios inetd

3.1.1 Asegúrese de que xinetd no esté instalado
3.1.2 Asegúrese de que los componentes del servidor X11 no estén instalados
3.1.3 Asegúrese de que Avahi Server no esté instalado
3.1.4 Asegúrese de que CUPS no esté instalado
3.1.5 Asegúrese de que el servidor DHCP no esté instalado
3.1.6 Asegúrese de que el servidor LDAP no esté instalado
3.1.7 Asegúrese de que el servidor DNS no esté instalado
3.1.8 Asegúrese de que el servidor FTP no esté instalado
3.1.9 Asegúrese de que el servidor HTTP no esté instalado
3.1.10 Asegúrese de que el servidor IMAP y POP3 no esté instalado
3.1.11 Asegúrese de que Samba no esté instalado
3.1.12 Asegúrese de que el servidor proxy HTTP no esté instalado
3.1.13 Asegúrese de que net-snmp no esté instalado
3.1.14 Asegúrese de que el servidor NIS no esté instalado
3.1.15 Asegúrese de que el servidor telnet no esté instalado

3.2 Clientes de servicio

3.2.1 Asegúrese de que NIS Client no esté instalado
3.2.2 Asegúrese de que el cliente rsh no esté instalado
3.2.3 Asegúrese de que Talk Client no esté instalado
3.2.4 Asegúrese de que el cliente Telnet no esté instalado
3.2.5 Asegúrese de que el cliente LDAP no esté instalado

4. Configuración de la Red

Realizar una correcta configuración de la red para asegurar la confidencialidad, integridad y disponibilidad de los datos que viajan a través de esta.

4.1 Deshabilitar protocolos y dispositivos de red no utilizados

4.1.1 Asegúrese de que las interfaces inalámbricas estén deshabilitadas

4.2 Parámetros de red (solo host)

4.2.1 Asegúrese de que el reenvío de IP esté deshabilitado

4.2.2 Asegúrese de que el envío de redireccionamiento de paquetes esté deshabilitado

4.3 Parámetros de red (host y enrutador)

4.3.1 Asegúrese de que los paquetes enrutados de origen no se acepten

4.3.2 Asegúrese de que no se acepten redireccionamientos ICMP

4.3.3 Asegúrese de que no se acepten redirecciones ICMP seguras

4.3.4 Asegúrese de que se registren los paquetes sospechosos

4.3.5 Asegúrese de que se ignoren las solicitudes ICMP de difusión

4.3.6 Asegúrese de que se ignoren las respuestas ICMP falsas

4.3.7 Asegúrese de que el Filtrado de ruta inversa esté habilitado

4.3.8 Asegúrese de que las cookies TCP SYN estén habilitadas

4.3.9 Asegúrese de que no se acepten anuncios de enrutador IPv6

5. Configuración de Firewall

Realizar una correcta configuración del firewall con el propósito mantener a los intrusos fuera del alcance de los datos contenidos en el sistema.

5.1 Configurar firewalld

5.1.1 Asegúrese de que firewalld esté instalado

5.1.2 Asegúrese de que iptables-services no esté instalado con firewalld

5.1.3 Asegúrese de que nftables no esté instalado o esté enmascarado con firewalld

5.1.4 Asegúrese de que el servicio firewalld esté habilitado y en ejecución

5.1.5 Asegúrese de que la zona predeterminada de firewalld esté configurada

5.1.6 Asegúrese de que las interfaces de red estén asignadas a la zona adecuada

5.1.7 Asegúrese de que firewalld elimine servicios y puertos innecesarios

5.2 Configurar nftables

5.2.1 Asegúrese de que nftables esté instalado

5.2.2 Asegúrese de que firewalld no esté instalado o enmascarado con nftables

5.2.3 Asegúrese de que los servicios de iptables no estén instalados con nftables

5.2.4 Asegúrese de que las iptables estén limpias con nftables

5.2.5 Asegúrese de que exista una tabla nftables

5.2.6 Asegúrese de que existan cadenas base de nftables

5.2.7 Asegúrese de que el tráfico de loopback de nftables esté configurado

5.2.8 Asegúrese de que las conexiones salientes y establecidas de nftables estén configuradas

6. Políticas de Contraseña

Establecer políticas de contraseña para los usuarios con el fin de evitar que los usuarios creen contraseñas consideradas inseguras o débiles y a su vez, asignar tiempo de caducidad a las contraseñas para evitar los ataques de diccionario o fuerza bruta.

6.2.1.5 Asegúrese de que la última fecha de cambio de contraseña de todos los usuarios sea anterior

7. Permisos de Escritura y Montaje

Deshabilitar la ejecución, el montado de carpetas o dispositivos y la creación de archivos con SUID en las carpetas con permisos de escritura como lo son aquellas de archivos temporales.

7.1 Asegúrese de que /tmp esté configurado
7.2 Asegúrese de que la opción noexec esté configurada en la partición /tmp
7.3 Asegúrese de que la opción nodev esté configurada en la partición /tmp
7.4 Asegúrese de que la opción nosuid esté configurada en la partición /tmp
7.5 Asegúrese de que /dev/shm esté configurado
7.6 Asegúrese de que la opción noexec esté configurada en la partición /dev/shm
7.7 Asegúrese de que la opción nodev esté configurada en la partición /dev/shm
7.8 Asegúrese de que la opción nosuid esté configurada en la partición /dev/shm
7.9 Asegúrese de que la partición /var/tmp incluya la opción noexec
7.10 Asegúrese de que la partición /var/tmp incluya la opción nodev
7.11 Asegúrese de que la partición /var/tmp incluya la opción nosuid
7.12 Asegúrese de que la partición /home incluya la opción nodev
7.13 Asegúrese de que las particiones de medios extraíbles incluyan la opción noexec
7.14 Asegúrese de que la opción nodev esté configurada en particiones de medios extraíbles
7.15 Asegúrese de que la opción nosuid esté configurada en particiones de medios extraíbles

8. Configuración de Bitácoras

Configurar el manejo y procesamiento de bitácoras con el fin de mantener un registro de las actividades ocurridas en el sistema, especialmente con el fin de identificar comportamiento sospechoso o para facilitar un análisis forense en caso de que ocurra un incidente.

8.1 Configurar rsyslog
8.1.1 Asegúrese de que rsyslog esté instalado
8.1.2 Asegúrese de que el servicio rsyslog esté habilitado y en ejecución
8.1.3 Asegúrese de que el registro esté configurado
8.1.4 Asegúrese de que rsyslog esté configurado para enviar registros a un host de registro remoto
8.1.5 Asegúrese de que los mensajes rsyslog remotos solo se acepten en hosts de registro designados.

8.2 Configurar journald
8.2.1 Asegúrese de que journald esté configurado para enviar registros a rsyslog
8.2.2 Asegúrese de que journald esté configurado para comprimir archivos de registro grandes
8.2.3 Asegúrese de que journald esté configurado para escribir archivos de registro en el disco persistente

8.3 Asegúrese de que logrotate esté configurado

9. Configuración Servicio SSH

Configurar correctamente el servicio SSH con el fin de que solo los usuarios autorizados puedan realizar conexiones remotas de manera segura.

9.1 Asegúrese de que el acceso SSH sea limitado
9.2 Asegúrese de que SSH LogLevel sea apropiado
9.3 Asegúrese de que SSH MaxAuthTries esté establecido en 4 o menos
9.4 Asegúrese de que SSH IgnoreRhosts esté habilitado
9.5 Asegúrese de que SSH HostbasedAuthentication esté deshabilitado
9.6 Asegúrese de que el inicio de sesión raíz SSH esté deshabilitado
9.7 Asegúrese de que SSH PermitEmptyPasswords esté deshabilitado
9.8 Asegúrese de que SSH PermitUserEnvironment esté deshabilitado
9.9 Asegúrese de que solo se utilicen Cifrados fuertes
9.10 Asegúrese de que solo se utilicen algoritmos MAC fuertes
9.11 Asegúrese de que solo se utilicen algoritmos sólidos de intercambio de claves
9.12 Asegúrese de que el Intervalo de tiempo de espera inactivo de SSH esté configurado
9.13 Asegúrese de que SSH LoginGraceTime esté configurado en un minuto o menos
9.14 Asegúrese de que el banner de advertencia de SSH esté configurado
9.15 Asegúrese de que SSH PAM esté habilitado
9.16 Asegúrese de que SSH MaxStartups esté configurado
9.17 Asegúrese de que SSH MaxSessions esté limitado

10. Configuración Sudo

Configurar correctamente sudo, debido a que es un programa utilizado en muchas de las distribuciones de Linux, sin embargo, la configuración incorrecta de este binario puede utilizarse con propósitos maliciosos como puede ser la escalada de privilegios.

10.1 Asegúrese de que sudo esté instalado
10.2 Asegúrese de que los comandos sudo usen pty
10.3 Asegúrese de que exista el archivo de registro sudo

Documentos de referencia

Center for Internet Security (CIS). (22 de Septiembre de 2022). *cisecurity.* Obtenido de https://learn.cisecurity.org/l/799323/2021-09-02/7tprk