**Red**

|  |  |
| --- | --- |
| Chequear servicios innecesarios | Servicios no necesarios no deben estar ejecutando |
| Asegurar el dueño de los servicios | El dueño de los servicios debe ser root. Verificar que solamente root pueda escribir en ellos |
| Asegurar servidor de impresion | /etc/cups/cupsd.conf  Permissions = 600  Owner = lp  Group = sys |
| Archivo rhosts | Asegurarse que no existen .rhosts en el sistema |
| No se deben definir equipos de confianza | No debe existir el archivo /etc/hosts.equiv |
| Interfaces ppp no deben existir | Pueden bypasear el firewall |
| Parametros de red correctamente configurados | *Revisar en /etc/sysctl.conf*  *o net.ipv4.tcp\_max\_syn\_backlog = 1024 (or higher)*  *o net.ipv4.tcp\_syncookies = 1*  *o net.ipv4.conf.all.rp\_filter = 1*  *o net.ipv4.conf.all.accept\_source\_route = 0*  *o net.ipv4.conf.all.accept\_redirects = 0*  *o net.ipv4.conf.all.secure\_redirects = 0*  *o net.ipv4.conf.default.rp\_filter = 1*  *o net.ipv4.conf.default.accept\_source\_route = 0*  *o net.ipv4.conf.default.accept\_redirects = 0*  *o net.ipv4.conf.default.secure\_redirects = 0*  *o net.ipv4.icmp\_echo\_ignore\_broadcasts = 1*  *o net.ipv4.ip\_forward = 0*  *o net.ipv4.conf.all.send\_redirects = 0*  *o net.ipv4.conf.default.send\_redirects = 0*  *o net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1* |
| Deshabilitar IPv6 | Verificar que IPv6 no este activo |
|  |  |

**Usuarios**

|  |  |
| --- | --- |
| No deben existir cuentas con ID 0, solo root. | Verificar /etc/passwd |
| Restringir logins de root solamente a consola | Verificar /etc/securetty (console) y /etc/ssh/sshd\_config (PermitRootLogin no) |
| Cuentas del sistema no deben poder realizar login interactivo | Cuentas con UID < 500 verificar “shell=/sbin/nologin”  /etc/shadow agregar “!” al campo “password” |
| Las cuentas no deben tener UID duplicados | Verificar el archivo /etc/passwd que no contengan UID duplicados |
| .- No se deben asignar contraseñas a los ID de grupo.  .- Los nombres e ID de los grupos deben ser únicos Implementación  .- Los grupos deben contener usuarios existentes válidos | Confirmar que el archivo /etc/group esta formateado correctamente mediante el archivo /usr/sbin/grpck. El archivo debe contener 4 campos de datos.  Asegurarse que los nombres de grupo y GID sean únicos en el sistema  Asegurarse que los grupos solo contentan usuarios existentes válidos |
| Bloquear cuentas luego de 3 intentos de login no exitosos | Verificar PAM |
| Todas las cuentas de usuario deben tener un shell y un home único | Todos los usuarios deben teber un shell válido (/etc/passwd)  Verificar los permisos de los directorios home no deben ser mayores a 755 (rwxr-xr-x) |
| El archivo .forward no debe existir | Asegurarse que el archivo .forward no existe en los directorios de los usuarios |
| Encriptación de las contraseñas | /etc/passwd , verificar que cada entrada tenga una “x” para indicar que están activas las shadow passwords |
| Cuentas con passwords vacíos | Verificar /etc/shadow que no exsitan passwords vacíos |
| Comando xhost | No debe existir el comando “xhost +” en los archivos de inicialización de los usuarios |
| Archivos “.exrc” | Asegurarse los archivos “.exrc” no contengan secuencias “!” |
| Grupo “disk” | Verificar que ningún usuario pertenezca al grupo “disk” |

**Procesos**

|  |  |
| --- | --- |
| Path | Verificar que el directorio actual esta removido del PATH |
| Tiempo de inactividad | Verificar en /etc/profile que exista una sentencia “tmout” |
| Mostrar ultimo login exitoso | Verificar existencia del archivo “/var/log/lastlog” |
| Sistema gráfico | Si no es necesario, verificar que no esté ejecutando el modo grádico (runlevel 5) |
| Montajes nfs | “/etc/fstab” verificar que exista la opción “nosuid” |
| Montajes removibles | “/etc/fstab” verificar las opciones “nosuid” y “nodev” para dispositivos removibles |
| Homes | “/etc/fstab” verificar las opciones “nosuid” y “nodev” para los homes |
| Deshabilitar dispositivos de almacenamiento USB | Verificar en “/etc/modprobe.conf” o lo que esta debajo exista “blacklist usb-storage” |
| Servidor NFS | Si el sistema ofrece servicio nfs, verificar lo siguiente:  “no\_root\_squash” no este presente  “no\_acl” no este presente  “anonuid” sin UID 0. Verificar que el UID sea válido  Verificar que el “/” filesystem no sea exportado  Verificar que existan límites de exportación |
| Logs de autentificación | *El archivo “/var/*log/secure” debe existir  Dueño: root  Grupo: root  Permisos: 600 |
| Deshabilitar recepción de logs (syslog) si no es necesario | Verificar que no esté en escucha el servicio syslog |
| Deshabilitar montaje de filesystems de usuario | “/etc/security/console.perms” Comentar entradas referidas a floppy y unidades de CD |
| Proteger GRUB con contraseña | “/etc/grub/grub.conf” Verificar que contenga una sección “password” |
| Auditar inicio y detención de servicios | Asegurarse los icios y detenciones de servicios queden registrados |
| Auditar comando “su” para obtener root | Verificar que “autpriv.\* /*var/*log/secure” este activo |
| Verificación directorio “lost+found” | Debe estar vacío |
| Formato del archivo “/etc/passwd” | Debe estar correctamente formateado. Debe contener 7 campos de datos (columnas) |
| Entradas “legacy” no deben existir (+) | Confirmar que el signo “+” no existe en  “/etc/passwd”  “/etc/shadow”  “/etc/group”  “/etc/gshadow” |
| Login shell, PATH completo | Asegurarse el shell de login en “/etc/passwd” sea especificado con PATH absoluto |
| Archivo de profile debe existir | Verificar que el archivo “/etc/skel/.bash\_profile”  existe |
|  |  |

**File System**

|  |  |
| --- | --- |
| Duegños de archivos y directorios | Verificar que no existan archivos y directorios sin dueños |
| Permisos de logs importantes | Chmod 600:  “/var/run/utmp”  “/var/run/utmpx”  “/var/log/wtmp”  “/var/log/wtmpx” |
| Permisos SUID/SGID | Verificar que los archivos cumplan lo siguiente  Setuid no deben ser mayores a 4755 (rwsr-xr-x)  Setgid no deben ser mayores a 2755 (rwxr-sr-x) |
| Scripts Shell y SUID/SGID | Verificar que los scripts “.sh” no contengan SUID/SGID |
| Archivo “/etc/profile” | Todos los comandos ejecutados aquí no deben ser modificables por nadie excepto root |
| Permisos del directorio “/root” | El grupo dueño de “/root” debe ser root |
| Archivos de inicio de usuarios | Todos los archivos de inicio de los HOME “.bash\_profile” .login” deben ser 750 |
| Archivos de inicializacion de root deben ser seguros | Verificar que .bash\_profile para root sea  rw-r—r-- (640)  dueño: root  grupo: root |
| Permisos por defecto | Asegurarse los siguientes permisos (umask 022)  “/etc/sysconfig/init”, “/etc/rc.d/init.d/functions”,  “/etc/profile”, “/etc/bashrc”, “/etc/csh.cshrc”, “/etc/csh.login”, “/etc/skel/.bashrc”, “/etc/vsftpd/vsftpd.conf” “/root/.bash\_profile”, “/root”.bashrc”, “/root/.cshrc”, “/root/.tcshrc” |
| Archivos .netrc no permitidos | Verificar que no exsiten archivos .netrc |
| Archivo crontab de root | El usuario root debe ser el dueño de los comandos que ejecuta en su propio crontab |
| Permisos de comandos en crontabs | Los comantos ejecutados dentro de los archivos crontab no deben tener permisos de escritura para los grupos |
| Archivos de manual y documentación | Verificad los permisos en 644 para los archivos dentro de:  “/usr/share/man”  “/usr/shared/doc” |
|  |  |
|  |  |
|  |  |