Examen Semana 3

Instrucción

El propósito del Examen 02 es aplicar los conocimientos de Endurecimiento de Servidores Linux. En este sentido, se debe preparar una máquina virtual con sistema operativo ***Ubuntu Server*** 20.04 LTS https://ubuntu.com/download/server con las siguiente características. - Memoria RAM 4G - 2 CPU (cores) - Almacenamiento 16 G - Una Tarjeta de Red - Acceso a internet

En este servidor luego de actualizarlo (update) se debe instalar un servidor Nginx, con el que se realizaran varios pruebas de endurecimiento. ## Detalles de la configuración

Del mismo modo que en el anterior examen el servidor lleva por nombre server01.jhondoe.com, donde el dominio jhondoe.com es remplazado por el designado a cada alumno. El nombre del servidor también debe estar registrado en el archivo de ***/etc/hosts***, con el ip del servido (www.xxx.yyy.zzz server01.jhondoe.com)

TAREAS A EJECUTAR

1. En el archivo sysctl.con.example se encuentra una configuración avanzada de parámetros del kernel (seguridad mas optimización de tcp para servidores con carga). este debe ser copiado al directorio /etc/sysctl.d/ con el nombre de local.conf (/etc/sysctl.d/local.conf).
2. En el archivo local.conf se encuentra la definición de limites para todos (*) los usuarios del servidor, este debe ser copiado en /etc/security/limits.d/ verificar que se aplica con el comando ulimit -a
3. Instalar el sistema de auditoria AIDE y ejecutarlo por primera vez (aide -v) inicializar la base de datos (checksum de todos los archivos del sistema). Verificar que todo el proceso termine correctamente. copiar el archivo de configuración en /etc/aide/aide.conf. Por ultimo generar un archivo de cambios con la instrucción: aide -c /etc/aide/aide.conf –check >/root/cambios.txt
4. Ejecutar la auditoria de Seguridad OpenSCAP :
    - sudo apt install -y libopenscap8
    - wget https://security-metadata.canonical.com/oval/com.ubuntu.$(lsb_release -cs).usn.oval.xml.bz2
    - bunzip2 com.ubuntu.$(lsb_release -cs).usn.oval.xml.bz2
    - sudo oscap oval eval –report /root/report.html com.ubuntu.$(lsb_release -cs).usn.oval.xml
    - Verificar que se genera el reporte en /root/report.html
5. Crear tres cuantas de usuario dentro del servidor Linux con las siguientes características: (todos con password sesamo)

- Usuario: *soporte1*
  - El Usuario debe cambiar su contraseña en la siguiente login exitoso.
  - Fecha de Expiración 31 De diciembre de 2022
  - Maximá duración de la contraseña (días antes que la contraseña expire) 90 (tres meses)
- Usuario: *admin*
  - El Usuario debe cambiar su contraseña en la siguiente login exitoso.
  - Fecha de Expiración 31 De diciembre de 2024
  - Máxima duración de la contraseña (días antes que la contraseña expire) 90 (tres meses)
  - El usuario debe tener permisos de admin (ser parte del grupo sudo)
- Usuario: *siso*
  - El Usuario debe cambiar su contraseña en la siguiente login exitoso.
  - Fecha de Expiración 31 De diciembre de 2024
  - Máxima duración de la contraseña (días antes que la contraseña expire) 90 (tres meses)

6. SISO: normalmente se denomina al Senior Information security officer, necesita revisar reportes regulares que el usuario soporte1 genera. para esto se debe:

   - El usuario siso creara una carpeta en su home (/home/siso) llamada REPORTES (todo mayúsculas).
   - Este directorio debe tener acl (listas de acceso) de modo que el usuario **soporte1** pueda ingresar al directorio del usuario **siso** y pueda crear sus reportes en este directorio (/home/siso/REPORTES).
   - como prueba de esto pude ejecutar como usuario reporte1 touch /home/siso/REPORTES/Reporte1.txt

7. Habilitar AppArmor en el servidor y adicionar el profile usr.sbin.nginx. Colocar al nginx en modo enforced con APPArmor (sudo aa-enforce nginx) Crear el directorio /var/www/html/unsafe y verificar que no es posible acceder al mismo

8. Habilitar el Firewall de Linux ubuntu, ufw y habilitar los puertos tcp 80 443 y 22