Fase 1 - Corrección de un hackeo, Reconocimiento y Recolección de evidencias

1. Introducción

Este informe documenta las medidas tomadas para mitigar un ataque y evitar la escalación en un sistema Debian comprometido. Además, se presentan recomendaciones detalladas para prevenir futuros incidentes de la misma índole. A lo largo del proceso, se ejecutaron comandos específicos, se revisaron configuraciones y se implementaron mejoras de seguridad. Este informe incluye descripciones claras de los comandos usados, sus funciones y los resultados obtenidos.

---

2. Descripción de las Acciones Realizadas

Punto 1: Inspección de intentos de acceso

- Objetivo: Identificar accesos inusuales y revisar la actividad de cuentas privilegiadas como `root`.
- Comandos utilizados:
    1. `sudo cat /etc/passwd`:
        - Revisión de todos los usuarios registrados en el sistema.
        - Resultado: Se detectaron usuarios legítimos y algunos asociados a servicios innecesarios (`ftp`, `speech-dispatcher`, `vboxadd`).
    2. `sudo last` y `sudo lastlog`:
        - Verificación de últimos inicios de sesión.
        - Resultado: No se encontraron inicios de sesión recientes con cuentas privilegiadas como `root`.

Punto 2: Identificación de archivos y procesos sospechosos

- Objetivo: Detectar posibles manipulaciones en el sistema.
- Comandos utilizados:
    1. `ps aux`:
        - Listado de todos los procesos en ejecución.
        - Resultado: Procesos sospechosos como `speech-dispatcher` y `orca` fueron identificados y marcados para eliminación.

2. `sudo find / -type f -mtime -7`:
    - Búsqueda de archivos modificados recientemente.
    - Resultado: Se encontraron scripts relacionados con VirtualBox y Orca en directorios como `/opt/` y `/home/debian/.local/share/orca`.

Punto 3: Escaneo del sistema en busca de rootkits o malware

- Objetivo: Confirmar la integridad del sistema.
- Comandos utilizados:
    1. `sudo chkrootkit` y `sudo rkhunter --check`:
        - Herramientas de detección de rootkits.
        - Resultado: No se detectaron rootkits conocidos, pero se identificó un packet sniffer asociado con `dhclient` y archivos sospechosos en directorios relacionados con Ruby y LibreOffice.

Punto 4: Bloqueo de exploits y prevención de escalaciones

- Objetivo: Neutralizar accesos maliciosos y prevenir escalaciones.
- Comandos utilizados:
    1. `sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT`:
        - Permitir acceso SSH.
    2. `sudo iptables -A INPUT -p tcp --dport 80 -j DROP`:
        - Bloquear acceso al puerto HTTP (80).
    3. `sudo systemctl stop apache2 && sudo systemctl disable apache2`:
        - Detención y deshabilitación de Apache.
    4. `sudo systemctl stop cups && sudo systemctl disable cups`:
        - Deshabilitación del servicio de impresión CUPS.

Punto 5: Reversión de cambios maliciosos

- Objetivo: Eliminar usuarios y configuraciones creadas por el atacante.
- Comandos utilizados:
    1. `sudo userdel -r ftp`:
        - Eliminación del usuario FTP.
    2. `sudo rm -r /home/debian/.local/share/orca`:
        - Eliminación del directorio de configuraciones de Orca.
    3. `sudo apt remove --purge orca -y`:
        - Eliminación del lector de pantalla Orca.

Punto 6: Actualización y configuraciones de seguridad

- Objetivo: Fortalecer el sistema tras el ataque.
- Comandos utilizados:
    1. `sudo apt update && sudo apt upgrade -y`:
        - Actualización de paquetes del sistema.
    2. `sudo nano /etc/ssh/sshd_config`:
        - Modificación de configuraciones para deshabilitar `PermitRootLogin` y permitir solo al usuario `debian`.
    3. `echo "debian:debian" | sudo chpasswd`:
        - Cambio de contraseñas para los usuarios legítimos.

---

3. Resultados obtenidos

1. Eliminación de usuarios no autorizados y servicios innecesarios.
2. Bloqueo de puertos abiertos innecesarios como HTTP (80) y FTP (21).
3. Configuración de SSH para restringir accesos.
4. Confirmación de que no hay rootkits conocidos en el sistema.
5. Sistema actualizado y reforzado contra vulnerabilidades.

---

4. Recomendaciones para prevenir futuros ataques

1. Actualizaciones regulares:
    - Asegúrate de que el sistema y todos los paquetes estén actualizados con parches de seguridad.
    - Configurar actualizaciones automáticas:
      sudo apt install unattended-upgrades
    - sudo dpkg-reconfigure --priority=low unattended-upgrades
2. Auditorías periódicas:
    - Usa herramientas como `chkrootkit` y `rkhunter` de manera regular.
    - Implementa sistemas de monitoreo para detectar cambios no autorizados.
3. Fortalecer la configuración de SSH:
    - Usa claves públicas para autenticación.
    - Restringe el acceso solo a IPs confiables.
4. Firewall avanzado:
    - Considera usar herramientas como `ufw` o configuraciones más detalladas de `iptables` para proteger los puertos críticos.

5. Eliminar servicios innecesarios:
    - Revisa periódicamente los servicios habilitados y elimina los que no sean esenciales.
6. Capacitación y mejores prácticas:
    - Educa a los usuarios sobre contraseñas seguras y buenas prácticas de seguridad.
    - Implementa un plan de respuesta ante incidentes.

---

5. Conclusión

A pesar de que el sistema ahora está protegido, el entorno digital está en constante evolución, y nuevas amenazas pueden surgir en cualquier momento. Es esencial realizar auditorías periódicas, mantener los sistemas actualizados y educar a los usuarios sobre las mejores prácticas.

Las medidas tomadas, como la eliminación de usuarios y servicios innecesarios, el bloqueo de puertos no requeridos y el refuerzo de SSH, han reducido significativamente la superficie de ataque.

Con la información recopilada y las recomendaciones proporcionadas, el sistema está ahora en una posición mucho más segura para enfrentar amenazas futuras. Pero no hay que distraerse.