Analisis forense de la maquina victima:

Sistema Operativo: Debian

Credenciales de incio de session:

-Usuario: debian

-Clave: 123456

Para iniciar se realizaron dos escaneos con la herramienta Nmap para hacer enumeracion de puertos abiertos y vulnerabiliadades en la maquina victima:A screen shot of a computer

Description automatically generatedA computer screen shot of a program

Description automatically generated

Pincipales vulnerabilidades encontradas:

Mala configuracion en el Puerto 22 del servicio ssh: el Puerto ssh un puerto usado normalmente para conexion remota se encontro Abierto, dejando la maquina vulnerable a ataques de fuerza bruta.

Mala configuracion en el 21 del servicio ftp: Al igual que el servicio ssh el servicio ftp es utilizado para conexion remota. Este estaba Abierto de igual manera dejando la maquina vulnerable a ataques de fuerza bruta para obtener acceso remote mediante este servicio.

Solucion tomada para estos:

Usando la herramienta de ufw fueron ambos puertos cerrados para no permitir entradas no autorizadas mediante estos.

A screenshot of a computer

Description automatically generated

Login data no Segura:

Realizando una busqueda en los archivos de configuracion de los servicios web se encontraron credenciales faciles de vulnerary como la clave para aceder a la base de datos alojada en la maquina victima.

La solucion para esta fue cambiar la clave ajustandola a los parametros de la buenas practicas y normas para claves seguras y robustas.

A screenshot of a computer

Description automatically generated

Archivos con permisos indevidos.

Realizando estudio de permisos en los archivos mas importantes de la maquina fue revisado el archive antes mencionado llamado wp-config.php, este archive luego de examinarlo con el comando ls para listarlo y -l para observar sus permisos y se vieron permisos con los cuales un usuario cualquiera puede leer, escribir y ejecutar en este.

Solucion:

Con el comando sudo chmod 600 le otorgamos los permisos antes mencionados a el root user, como debe de estar configurado para evitar dejar vulnerable este archive de gran importancia.

A screenshot of a computer

Description automatically generated

Listado de dominios web:

Al utilizer la herramienta gobuster nos pudimos percatar que los dominios web pueden ser listados lo que permite a los atacantes explorar y acceder a archivos que deberían estar ocultos o protegidos.

A screenshot of a computer

Description automatically generated

Solucion:

Modificando el archivo apache2.conf pudimos desactivar el listado de archivos para poder erradicar esta vulnerabilidad, se hizo de la siguiente manera.

Nos situamos en el fichero /etc/apache2 y con el comando sudo logramos tener acceso a el archive de configuracion del apache server y modificarlo para que no este active el directory listing.

A screenshot of a computer

Description automatically generated

**Recomendaciones adicionales para mantener una máquina segura**

1. Implementa Actualizaciones de Seguridad Regulares

- Parchea el sistema operativo, software y todas las aplicaciones, especialmente los servicios expuestos a Internet como Apache, MySQL, y SSH.

- Configura actualizaciones automáticas para paquetes críticos de seguridad si es posible, o implementa notificaciones para que te avisen cuando haya parches disponibles.

2. Usa el Principio de Mínimos Privilegios

- Configura cuentas y permisos para que cada usuario solo tenga acceso a lo que necesita. Elimina cuentas que no se usen y evita el uso de la cuenta root para tareas diarias.

- Limita accesos a servicios críticos (como SSH y bases de datos) a IPs específicas y de confianza.

3. Implementa un Firewall Robusto

- Usa un firewall como *ufw* en Linux para definir reglas que solo permitan puertos esenciales y restrinjan el acceso a IPs confiables.

- Revisa periódicamente las reglas del firewall para asegurarte de que solo los servicios necesarios estén accesibles.

4. Monitoreo y Detección de Intrusos

- Usa un IDS o IPS (sistema de detección o prevención de intrusos) como Snort o Suricata para monitorear el tráfico de red en tiempo real y detectar actividades sospechosas.

- Configura alertas para eventos críticos en logs del sistema, como intentos fallidos de inicio de sesión SSH, cambios en archivos sensibles (como `wp-config.php`) y accesos no autorizados.

5. Aísla Aplicaciones y Servicios en Contenedores

- Utiliza contenedores (por ejemplo, Docker) o entornos virtuales para aislar aplicaciones, lo cual reduce el riesgo de que una vulnerabilidad en una aplicación comprometa todo el sistema.

- Configura roles y permisos específicos para cada contenedor, y elimina servicios no necesarios en ellos.

6. Configura Políticas de Contraseñas Fuertes

- Implementa políticas que exijan contraseñas complejas (mínimo 12 caracteres, mezcla de letras, números y caracteres especiales) y evita la reutilización de contraseñas.

- Usa un administrador de contraseñas seguro para almacenar y gestionar credenciales.

7. Implementa Autenticación de Dos Factores (2FA)

- Habilita autenticación de dos factores en accesos SSH, sistemas de administración y paneles web críticos.

- Configura 2FA usando aplicaciones de autenticación como Google Authenticator o tokens físicos para una capa adicional de seguridad.

8. Realiza Auditorías y Revisiones de Seguridad Periódicas

- Programa auditorías regulares y pruebas de penetración para detectar posibles nuevas vulnerabilidades en el sistema.

- Revisa los logs del sistema, de aplicaciones, de la base de datos y de la red para identificar patrones inusuales y actividades sospechosas.

9. Asegura los Archivos y Directorios Críticos

- Realiza copias de seguridad regulares de archivos importantes, configuraciones y bases de datos. Almacena los backups en ubicaciones seguras y desconectadas del sistema principal.

- Usa herramientas como *AIDE* o *OSSEC* para monitorear archivos críticos y recibir alertas en caso de cambios no autorizados.

10. Implementa Políticas de Registro y Auditoría Estrictas

- Configura logs detallados en servicios críticos y almacénalos en un servidor seguro, separado del sistema principal.

- Establece políticas para retener y revisar logs regularmente, en especial aquellos relacionados con accesos, errores y cambios de configuración.

11. Establece y Practica un Plan de Respuesta a Incidentes

- Crea y documenta un plan de respuesta a incidentes que incluya la recuperación de backups, desconexión del sistema comprometido y análisis forense.

- Realiza simulacros de respuesta a incidentes y capacita al equipo en protocolos de seguridad, detección y contención de amenazas.

12. Usa Redes Virtuales Privadas (VPN)

- Para el acceso remoto al sistema, utiliza una VPN confiable para reducir la exposición del sistema a ataques externos y asegurar las comunicaciones.

- Requiere autenticación robusta para el acceso VPN y asegúrate de usar cifrado fuerte en las conexiones.

13. Establece una Cultura de Seguridad Continua

- Ofrece formación continua a los administradores de sistemas y usuarios sobre buenas prácticas de seguridad, reconocimiento de amenazas (como phishing) y manejo seguro de datos.

- Realiza una revisión de las políticas de seguridad de la organización y ajusta según sea necesario, basándote en los resultados de auditorías y análisis de incidentes previos.