Reporte Ejecutivo de Ciberseguridad: Análisis de Vulnerabilidad y Explotación en el Sistema "Domain"

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Domain"
- **Fecha**: 20 de junio de 2024
- **Nombre de la Organización**: [N/A]
- **Autor(es)**: tellmefred

2. Resumen Ejecutivo

Este informe detalla la identificación y explotación de vulnerabilidades en el sistema "Domain", una máquina práctica de DockerLabs. Se explotaron fallas en el protocolo SMB mediante ataques de fuerza bruta, y se utilizó una web shell para ejecutar comandos remotos. Finalmente, se logró una escalación de privilegios que permitió obtener acceso root al sistema. Se proporcionan recomendaciones para mitigar estas vulnerabilidades y fortalecer la seguridad del sistema.

3. Introducción

- **Contexto**: El sistema "Domain" expone un servicio SMB vulnerable, comúnmente utilizado para compartir archivos en redes, lo que permitió a los atacantes realizar ataques de fuerza bruta para obtener acceso.
- **Propósito**: Evaluar la seguridad del protocolo SMB, identificar vulnerabilidades, y proponer medidas correctivas para reducir los riesgos de seguridad.
- **Alcance**: Incluye la exploración de servicios SMB, ataques de fuerza bruta para obtener credenciales, uso de una web shell para ejecutar comandos remotos, y escalación de privilegios para obtener acceso root.
- **Metodología**: Se utilizó un enfoque sistemático que incluyó escaneos de red, fuerza bruta sobre SMB, y técnicas de post-explotación para obtener acceso privilegiado al sistema.

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**: El sistema "Domain" presenta una vulnerabilidad crítica en el servicio SMB, que fue explotada para comprometer el sistema y escalar privilegios a root.
- **Sistemas y Datos Críticos**: Servicios SMB, servidores web, y archivos del sistema.

5. Evaluación de Vulnerabilidades y Explotación

- **Reconocimiento**:
    - **Escaneo de Red**: Un escaneo de Nmap reveló un servicio SMB (protocolo SMB2) y una interfaz web disponible.

    - **Fuerza Bruta en SMB**: Se utilizó la herramienta crackmapexec para realizar un ataque de fuerza bruta sobre los usuarios obtenidos, encontrando la contraseña "star" para el usuario "Bob".
- **Explotación**:
    - **Acceso al Servicio SMB**: Con las credenciales obtenidas, se accedió al servicio SMB, donde el usuario "Bob" tenía permisos de lectura y escritura en el directorio HTML.
    - **Carga de una Web Shell**: Aprovechando los permisos, se cargó una web shell en el servidor, permitiendo la ejecución de comandos remotos.
- **Escalada de Privilegios**:
    - **Uso de SUID en Nano**: Se identificaron permisos SUID en el editor de texto nano. Se utilizó este permiso para editar el archivo `/etc/shadow` y eliminar la necesidad de una contraseña para el usuario root.
    - **Acceso Root**: Con esta modificación, se obtuvo acceso root sin necesidad de una clave, logrando el control completo del sistema.

6. Recomendaciones

- **Fortalecimiento de la Seguridad de SMB**: Implementar políticas de contraseñas robustas y limitar los intentos de inicio de sesión fallidos en SMB.
- **Monitoreo de Actividades Sospechosas**: Implementar sistemas de detección de intrusiones para identificar y responder a actividades no autorizadas en tiempo real.
- **Auditoría y Restricción de Permisos SUID**: Revisar y restringir los permisos SUID en el sistema para evitar escalaciones de privilegios similares.
- **Capacitación en Ciberseguridad**: Entrenar al personal en la importancia de la seguridad en la administración de servidores y el uso seguro de servicios de red.

7. Conclusión

El análisis del sistema "Domain" demostró que, mediante la explotación de un servicio SMB mal configurado, un atacante puede comprometer seriamente la seguridad del sistema. Es crucial implementar las recomendaciones propuestas para mitigar estos riesgos y mejorar la postura de seguridad del sistema.

8. Anexos

- Detalles técnicos sobre la explotación de SMB y el uso de la web shell.
- Resultados de escaneos de red y análisis de servicios.
- Capturas de pantalla y comandos utilizados durante la explotación y la escalación de privilegios.