Informe Técnico del Programa de Verificación de Seguridad en Ubuntu

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Título del Programa:

Verificación de Seguridad en Sistemas Ubuntu

Empresa Auditada:

EXPORTQUIL S.A.

Empresa Desarrolladora:

GENETEC S.A.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Equipo de Auditoría:

• Líder de Auditoría: Ing. Oscar Avilés

• Auditor y Desarrollador del Programa: Tnlgo. Francisco Gómez

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Introducción:

Este informe técnico ha sido elaborado para documentar las funcionalidades del programa de verificación de seguridad en sistemas operativos Ubuntu, diseñado por GENETEC S.A. y utilizado para auditar las configuraciones de seguridad en los sistemas de EXPORTQUIL S.A.. El programa está orientado a la identificación de vulnerabilidades en las configuraciones de seguridad y a la propuesta de recomendaciones para su mejora, asegurando la integridad, disponibilidad y confidencialidad de los datos gestionados por el sistema.

Bajo la supervisión del Ing. Oscar Avilés, y con el desarrollo técnico del Tnlgo. Francisco Gómez, el programa busca asegurar que las políticas de seguridad de EXPORTQUIL S.A. estén alineadas con las mejores prácticas de ciberseguridad.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Objetivos del Programa:

1. Auditoría de Políticas de Seguridad: Evaluar las configuraciones actuales relacionadas con la gestión de contraseñas y accesos.

2. Identificación de Vulnerabilidades: Detectar configuraciones inseguras que podrían exponer el sistema a ataques cibernéticos.

3. Recomendaciones de Mejora: Proponer medidas para corregir los puntos débiles detectados, mejorando la seguridad del sistema.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Funcionalidades del Programa:

El programa desarrollado por GENETEC S.A. cuenta con las siguientes funcionalidades:

1. Auditoría de Políticas de Contraseña:

◦ Revisión de la longitud mínima y complejidad de las contraseñas.

◦ Evaluación de las políticas de caducidad y restricciones de reutilización.

2. Gestión de Intentos de Inicio de Sesión:

◦ Auditoría del módulo pam\_tally2 para gestionar intentos fallidos de inicio de sesión.

◦ Informe de las políticas de bloqueo tras múltiples intentos fallidos.

3. Bloqueo de Usuarios:

◦ Análisis de las configuraciones en faillock.conf para revisar los límites de intentos fallidos y períodos de bloqueo.

4. Generación de Informes:

◦ Creación de informes detallados con las configuraciones encontradas y recomendaciones para mejorar la seguridad.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Estructura del Programa:

El programa, escrito en Bash, tiene una estructura modular que permite añadir nuevas verificaciones fácilmente. Cada funcionalidad está encapsulada en una función independiente, lo que facilita la escalabilidad y el mantenimiento del código.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Fragmento de Código de Verificación:

# Verificación de Políticas de Intentos Fallidos add\_section "11. Políticas de Intentos Fallidos" if grep -q "auth required pam\_tally2.so" /etc/pam.d/common-auth; then echo "pam\_tally2 está configurado correctamente." else echo "pam\_tally2 no está configurado." fi

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Resultados y Beneficios:

El uso del programa por parte de EXPORTQUIL S.A. permite identificar de manera rápida y precisa las configuraciones de seguridad inadecuadas, brindando un análisis completo del sistema. Las recomendaciones proporcionadas facilitan la implementación de mejoras que reducen la exposición a vulnerabilidades y mejoran el control de accesos no autorizados.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Conclusiones:

La seguridad de los sistemas operativos es crucial para cualquier organización, y EXPORTQUIL S.A. no es la excepción. Este programa de verificación, desarrollado por GENETEC S.A., se presenta como una herramienta clave para auditar y optimizar las configuraciones de seguridad en Ubuntu. Gracias a los resultados obtenidos, los administradores de EXPORTQUIL S.A. podrán implementar mejoras significativas que garanticen un entorno más seguro y protegido.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Recomendaciones Futuras:

1. Ampliación de Verificaciones: Incluir auditorías adicionales para configuraciones de red, firewall y permisos de archivos.

2. Desarrollo de GUI: Crear una interfaz gráfica de usuario para facilitar la interacción con el programa.

3. Auditorías Continuas: Realizar auditorías periódicas con este programa para asegurar que las configuraciones de seguridad estén siempre actualizadas y efectivas.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Este informe presenta un resumen exhaustivo del programa de verificación de seguridad, dirigido por el Ing. Oscar Avilés y desarrollado por el Tnlgo. Francisco Gómez, brindando a EXPORTQUIL S.A. una solución completa para auditar y mejorar las políticas de seguridad en sistemas operativos Ubuntu.