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

1. Portada

Título del Reporte: Análisis de Vulnerabilidad y Explotación en el Sistema "Greenhorn"

Fecha: 16 de septiembre de 2024

Nombre de la Organización: [N/A]

Autor(es): tellmefred

2. Resumen Ejecutivo

Este informe detalla el análisis de la máquina "Greenhorn" de Hack The Box, en la que se identificaron varias vulnerabilidades que permitieron la explotación inicial del sistema y la posterior escalada de privilegios. Se utilizó un enfoque basado en el reconocimiento y explotación de servicios web vulnerables, junto con la reutilización de contraseñas. El análisis concluye con recomendaciones específicas para mejorar la seguridad del sistema.

3. Introducción

Contexto: "Greenhorn" es una máquina de Hack The Box diseñada para enseñar técnicas básicas de reconocimiento y explotación en entornos de ciberseguridad. Ofrece un entorno donde se pueden identificar y explotar vulnerabilidades en servicios web.

Propósito: Evaluar la seguridad del sistema "Greenhorn" mediante la identificación de vulnerabilidades críticas y la aplicación de técnicas de escalada de privilegios.

Alcance: El informe cubre desde el reconocimiento inicial hasta la explotación de vulnerabilidades y la escalada de privilegios que permitieron obtener acceso root.

Metodología: Se emplearon herramientas de escaneo de red, ataques de fuerza bruta, descifrado de contraseñas y la explotación de vulnerabilidades en aplicaciones web.

4. Estado Actual de la Ciberseguridad

Resumen de la Postura de Ciberseguridad: El sistema "Greenhorn" presentó múltiples vulnerabilidades en su aplicación web y en la reutilización de contraseñas, lo que facilitó la explotación y el acceso no autorizado.

Sistemas y Datos Críticos: Servicios web en el puerto 80, aplicaciones web basadas en Pluck CMS y archivos críticos de configuración.

5. Evaluación de Vulnerabilidades y Explotación

Reconocimiento:

Escaneo de Puertos: Se realizó un escaneo con nmap, que identificó los puertos 22 (SSH) y 80 (HTTP) abiertos, con una redirección al dominio greenhorn.htb.

Vulnerabilidad en Pluck CMS: Al acceder a la página web, se detectó la versión 4.7.18 de Pluck CMS, vulnerable a un ataque, pero requería la contraseña.

Explotación:

Descifrado de Contraseña: Se encontró un archivo hash en el código fuente, el cual fue descifrado utilizando un algoritmo conocido, obteniendo la contraseña "iloveyou1".

Acceso al Sistema: Con la contraseña descifrada, se accedió al sistema y se cargó una web shell comprimida en un archivo .zip a través del módulo "install a module", lo que permitió obtener una shell interactiva.

Escalada de Privilegios:

Reutilización de Contraseña: La contraseña obtenida previamente fue reutilizada para acceder al usuario junior, lo que permitió obtener la user.txt.

Obtención de Contraseña Root: Mediante el análisis de un archivo PDF recuperado, se descubrió una clave root borrosa, que fue identificada tras un procesamiento adecuado, lo que permitió escalar privilegios y obtener acceso root al sistema.

6. Recomendaciones

Mejorar la Seguridad del CMS: Actualizar el CMS a una versión más reciente que corrija las vulnerabilidades conocidas y evitar el almacenamiento de contraseñas en texto claro o fácilmente accesibles en el código fuente.

Gestión de Contraseñas: Implementar políticas de contraseñas seguras y evitar la reutilización de contraseñas entre diferentes servicios y usuarios.

Monitoreo de Actividades Sospechosas: Implementar sistemas de monitoreo para detectar actividades sospechosas, como la subida de archivos no autorizados o intentos de explotación mediante fuerza bruta.

Seguridad en la Configuración del Sistema: Asegurarse de que los archivos de configuración no contengan información sensible y aplicar buenas prácticas de seguridad en la gestión de privilegios de usuarios.

7. Conclusión

La evaluación del sistema "Greenhorn" demostró que las vulnerabilidades en el CMS y la reutilización de contraseñas son factores críticos que pueden llevar a la explotación completa de un sistema. Se recomienda aplicar las medidas correctivas propuestas para mitigar estos riesgos y mejorar la postura de seguridad del sistema.

8. Anexos

Detalles técnicos sobre la explotación de Pluck CMS y la escalada de privilegios.

Resultados de escaneos de red y análisis de servicios.

Capturas de pantalla y comandos utilizados durante la explotación y la escalada de privilegios.