Cómo Detectar La Vulnerabilidad GHOST

La **vulnerabilidad GHOST** es una vulnerabilidad de desbordamiento de búfer que puede ser fácilmente explotada de forma local y remota, lo que hace que sea bastante peligrosa. Esta vulnerabilidad lleva el nombre de la **función gethostbynameb**, la cual es usada en la explotación.

Los atacantes utilizan vulnerabilidades de desbordamiento de búfer como éste por el envío de paquetes específicos de datos a un sistema vulnerable. El ataque permite al atacante ejecutar código arbitrario y tomar el control de la máquina vulnerable de la víctima.

Esta vulnerabilidad expone a una gran cantidad de usuarios, ya que radica en la librería glibc (GNU). Afortunadamente existen métodos y aplicaciones para **detectar la vulnerabilidad GHOST**.

¿Qué Puedo Hacer Sobre La Vulnerabilidad GHOST?

Al igual que con cualquier vulnerabilidad, la mejor manera de **acabar con la vulnerabilidad GHOST** es identificar los sistemas vulnerables, priorizar el proceso de parcheo basado en la prioridad, y desplegar parches. Debe mantener un inventario actualizado de los dispositivos, sistemas operativos y aplicaciones en su red para que pueda conocer aquellos dispositivos que son vulnerables.

AlienVault Unified Security Management (USM), también te puede ser de gran ayuda. USM ofrece el descubrimiento de **sistemas vulnerados**, evaluación de vulnerabilidades, detección de amenazas y el seguimiento del comportamiento, todo desde la misma consola; además de actualizaciones semanales de análisis de riesgos desarrollados por el equipo de investigación de seguridad de **AlienVault Labs**.

USM puede escanear la red para identificar los **sistemas vulnerables con GHOST**, por lo que es fácil identificar sistemas que necesitan ser parcheados y dar prioridad para solucionados.

USM no sólo puede identificar los sistemas vulnerables, sino que también puede ayudar a detectar los intentos de explotación de la vulnerabilidad.