Informe de Seguridad Generado por Molly AI

Sesión: scan_192_168_1_38

Fecha de Generación: 2025-07-24 21:20:09

Resumen de Escaneo de Red - Sesión: scan_192_168_1_38

Tipo de Escaneo: Network Scan

Objetivo: 192.168.1.38

Fecha de Inicio: 2025-07-24T21:19:52.740762

Estado: completed

Fecha de Finalización: 2025-07-24T21:20:09.321531

Resumen: ¡Hola! El escaneo de red en 192.168.1.38 ha finalizado. En resumen, se encontró un único host activo en esa dirección IP. El análisis reveló un servicio SSH (OpenSSH 5.3p1 Debian 3ubuntu7.1) escuchando en el puerto 22. Esta versión de OpenSSH es considerablemente antigua y presenta varias vulnerabilidades conocidas.

Hallazgos:

* **Host:** 192.168.1.38

* **Servicio:** SSH (puerto 22), versión OpenSSH 5.3p1 Debian 3ubuntu7.1.

Se detectaron varias vulnerabilidades asociadas con esta versión desactualizada de OpenSSH. Aunque no puedo acceder a una base de datos en tiempo real de vulnerabilidades para verificar cada CVE contra esta versión específica, basándome en el número de versión, es altamente probable que se trate de vulnerabilidades que permiten la ejecución remota de código (RCE), ataques de denegación de servicio (DoS), y compromisos de autenticación. Los CVEs específicos asociados a versiones similares de OpenSSH podrían incluir (pero no se limitan a) CVE-2007-2768, CVE-2008-3844, CVE-2010-4478, CVE-2010-4755, y CVE-2012-0814. Si te interesa profundizar en alguno de estos CVEs, puedes preguntarme por su ID (ej: "¿Qué es CVE-2007-2768?").

Mitigaciones:

La principal acción a tomar es actualizar inmediatamente el servidor SSH a la versión más reciente. Esta actualización parcheará las vulnerabilidades conocidas y mejorará significativamente la seguridad del sistema. Además, se recomienda:

* **Autenticación basada en claves:** Reemplazar la autenticación por contraseña con autenticación basada en claves SSH para aumentar la seguridad.

* **Restricciones de firewall:** Configurar un firewall para restringir el acceso al puerto 22 solo desde direcciones IP de confianza.

* **Auditoría de logs:** Monitorear regularmente los logs del servidor SSH para detectar cualquier actividad sospechosa.

* **Contraseñas fuertes:** Si se utiliza la autenticación por contraseña (lo cual no se recomienda), asegúrate de usar contraseñas fuertes y únicas.

Recuerda que mantener el software actualizado es fundamental para la seguridad. Un escaneo de vulnerabilidades más completo con herramientas como Nessus o OpenVAS podría revelar otras vulnerabilidades en el sistema.

¿Tienes alguna otra pregunta o necesitas más información sobre alguno de estos puntos?

Hosts Descubiertos y Servicios Abiertos

Host: 192.168.1.38 (192.168.1.38)

SO: Linux 2.6.32 - 2.6.35

Servicios Abiertos:

- Puerto: 22/tcp (ssh vOpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)) Estado: open