Informe de Seguridad Generado por Molly AI

Sesión: Escaneo_IA_192_168_1_38_20250718_182516

Host Analizado: 192.168.1.10

Fecha de Generación: 2025-12-02 09:53:02

Informe Detallado del Host: 192.168.1.10 (kali-molly)

Fecha del Informe: 2025-12-02 09:53:02

Dirección IP: 192.168.1.10

Nombre de Host: kali-molly

Sistema Operativo: Linux

Servicios y Puertos Abiertos

Puerto: 22/tcp

- **Servicio:** ssh (Versión: OpenSSH 8.9)
- **Estado:** open

Puerto: 21/tcp

- **Servicio:** ftp (Versión: vsftpd 3.0.3)
- **Estado:** open

Hallazgos de Seguridad

FTP Acceso Anónimo Permitido (High)

Tipo: vulnerability

Servicio Asociado: ftp en puerto 21/tcp

Descripción: El servidor FTP en el puerto 21 permite el acceso anónimo, lo que podría exponer información sensible.

Recomendación: Deshabilitar el acceso FTP anónimo.

Detalles Adicionales:

```
{ "accessed_files": [ "README.txt", "users.txt" ] }
```

Firewall Deshabilitado (Medium)

Tipo: misconfiguration

Descripción: El firewall UFW no está activo en el sistema, dejando los puertos expuestos.

Recomendación: Activar y configurar el firewall UFW para solo permitir el tráfico necesario.

Detalles Adicionales:

```
{ "ufw_status": "inactive" }
```

Banner SSH Enumera Versión (Low)

Tipo: info_leak

Servicio Asociado: ssh en puerto 22/tcp

Descripción: El banner SSH revela la versión exacta del servidor (OpenSSH 8.9), lo que facilita la búsqueda de exploits específicos.

Recomendación: Configurar el servidor SSH para ocultar o generalizar el banner.

Detalles Adicionales:

```
{ "banner": "SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6" }
```

Fin del Informe. Generado por Molly Security AI.