## **Herramientas Propuestas**

### 🔍 **Análisis de Vulnerabilidades Web**

#### **1. OWASP ZAP (Open Source)**

* Descripción: Escáner de seguridad web activo con API REST para automatización.
* Viabilidad Backend: ★★★★★ (API robusta, fácil integración)
* Uso Ideal: Escaneo automatizado de aplicaciones web.

#### **2. Burp Suite Pro (Comercial)**

* Descripción: Suite profesional para pentesting web con escaneo avanzado.
* Viabilidad Backend: ★★★★☆ (API estable, requiere licencia)
* Uso Ideal: Auditorías profundas en entornos empresariales.

#### **3. SQLMap (Open Source)**

* Descripción: Herramienta especializada en detección y explotación de SQL Injection.
* Viabilidad Backend: ★★★☆☆ (CLI fácil de integrar, sin API nativa)
* Uso Ideal: Pruebas de seguridad en bases de datos.

#### **4. Nuclei (Open Source)**

* Descripción: Escáner rápido basado en plantillas para vulnerabilidades conocidas.
* Viabilidad Backend: ★★★★★ (salida en JSON, escalable)
* Uso Ideal: Escaneo masivo de múltiples objetivos.

### ☁️ **Auditoría y Seguridad Cloud**

#### **5. Prowler (Open Source)**

* Descripción: Escáner de seguridad para AWS basado en CIS Benchmark.
* Viabilidad Backend: ★★★★☆ (salida en JSON/CSV)
* Uso Ideal: Cumplimiento en entornos AWS.

#### **6. Scout Suite (Open Source)**

* Descripción: Auditor multi-cloud (AWS, Azure, GCP) para configuraciones inseguras.
* Viabilidad Backend: ★★★★☆ (informes estructurados)
* Uso Ideal: Evaluación de seguridad en nubes híbridas.

#### **7. Qualys Cloud Platform (Comercial)**

* Descripción: Suite empresarial para gestión de vulnerabilidades en la nube.
* Viabilidad Backend: ★★★★★ (API empresarial completa)
* Uso Ideal: Monitoreo continuo en infraestructura crítica.

### 🛡️ **Anti-Malware & Análisis de Amenazas**

#### **8. Cylum (Comercial)**

* Descripción: Plataforma avanzada de análisis de malware con IA y sandboxing.
* Viabilidad Backend: ★★★★☆ (API REST, requiere licencia)
* Uso Ideal: Detección proactiva de malware desconocido.

#### **9. CrowdStrike Falcon (Comercial)**

* Descripción: Plataforma EDR con detección en tiempo real y respuesta automatizada.
* Viabilidad Backend: ★★★★★ (API para SOC/SIEM)
* Uso Ideal: Protección de endpoints corporativos.

#### **10. ClamAV (Open Source)**

* Descripción: Motor antivirus open source para escaneo básico de malware.
* Viabilidad Backend: ★★★☆☆ (requiere configuración adicional)
* Uso Ideal: Escaneo de archivos en servidores.

#### **11. YARA (Open Source)**

* Descripción: Herramienta para crear reglas personalizadas de detección de malware.
* Viabilidad Backend: ★★★☆☆ (integración manual con otros sistemas)
* Uso Ideal: Identificación de amenazas conocidas.

### 🛠️ **Otras Herramientas Clave**

#### **12. Metasploit Framework (Open Source)**

* Descripción: Framework de pentesting para explotación de vulnerabilidades.
* Viabilidad Backend: ★★★☆☆ (API RPC, complejidad media)
* Uso Ideal: Pruebas de penetración controladas.

#### **13. Nmap (Open Source)**

* Descripción: Escáner de red para descubrimiento de hosts y servicios.
* Viabilidad Backend: ★★★★☆ (salida en XML/JSON)
* Uso Ideal: Auditoría de redes internas/externas.

#### **14. Wireshark (Open Source)**

* Descripción: Analizador de tráfico de red para inspección de paquetes.
* Viabilidad Backend: ★★☆☆☆ (requiere procesamiento manual de PCAPs)
* Uso Ideal: Diagnóstico de ataques en la red.

## 📊 **Comparativa: Open Source vs. Comercial**

| **Criterio** | **Open Source** | **Comercial** |
| --- | --- | --- |
| Costo | Bajo/Gratis | Alto |
| Personalización | Alta | Media |
| Soporte | Comunidad | Empresarial |
| Escalabilidad | Requiere trabajo | Lista para empresa |

## ✅ **Recomendación Final**

* Para startups/empresas con presupuesto limitado:
  + Usar OWASP ZAP + Nuclei + ClamAV + Prowler.
* Para entornos empresariales con alta seguridad:
  + Incluir Burp Suite Pro + Cylum + CrowdStrike Falcon + Qualys.

### 🚀 **Próximos Pasos**

1. Definir presupuesto (priorizar herramientas comerciales si es posible).
2. Desarrollar wrappers de integración para unificar resultados.
3. Implementar un sistema de colas (RabbitMQ/Kafka) para análisis masivos.