Análisis de Vulnerabilidades

Ciberseguridad Avanzada

¿Qué es?

- Definición:
  - Proceso sistemático para identificar, cuantificar y priorizar vulnerabilidades en sistemas de TI, redes y aplicaciones.
  - Busca descubrir debilidades explotables que podrían comprometer la seguridad de la información.
- Tipos de análisis:
  - Automatizado: Uso de herramientas/software para escanear sistemas de forma sistemática.
  - Manual: Inspección realizada por profesionales, especialmente útil en entornos complejos o aplicaciones personalizadas.

Objetivos

- Identificación temprana de amenazas:
  - Detectar vulnerabilidades antes que los atacantes.
- Priorización de riesgos:
  - Clasificar las vulnerabilidades según su criticidad (alta, media, baja).
- Soporte en decisiones de remediación:
  - Facilitar la asignación de recursos a las amenazas más peligrosas.

Objetivos

- Cumplimiento normativo:
  - Sustentar auditorías para estándares de seguridad.
- Mejora continua del entorno de TI:
  - Adoptar una postura proactiva en la defensa de los activos tecnológicos.

Automatizado vs Manual

Tipo	Descripción	Ventajas	Limitaciones
Automático	Utiliza herramientas para escanear redes/sistemas de manera rápida y masiva	Rápido, escalable, repetible, ideal para entornos grandes	Limitada personalización, riesgo de falsos positivos/negativos
Manual	Realizado por expertos que revisan sistemas, código o configuraciones de forma personalizada	Preciso, adaptable a entornos complejos	Lento, costoso, no escalable para ambientes grandes

Ciclo de vida

1. Identificación: Detección de debilidades mediante escáneres automáticos o revisiones manuales.
2. Evaluación: Clasificación y priorización en base a criticidad y contexto.
3. Corrección: Aplicación de soluciones: parches, configuraciones o mitigaciones.
4. Verificación: Validación posterior a la corrección para asegurar efectividad.
5. Documentación: Registro de actividades, hallazgos, acciones y métricas.
6. Mejora continua: Retroalimentación para optimizar proceso y herramientas.

Herramientas

Herramienta	Tipo	Características Clave	Ventajas	Limitaciones
Nessus	Comercial	Amplia base de datos, fácil de usar	Precisión, gran soporte y documentación	Licenciamiento, coste
OpenVAS	Open Source	Escaneo profundo, actualizaciones regulares	Gratis, personalizable, ideal para PYMES y educación	Configuración compleja, menos soporte
Qualys	SaaS	Gestión centralizada, reporting avanzado	Escalabilidad, automatización, cumplimiento normativo	Dependencia de nube/coste, curva de aprendizaje
Burp Suite	Comercial / Open	Testing web apps, interceptación, plugins	Muy útil para pruebas manuales y pentesting web	Limitado a web, puede requerir formación avanzada
Wazuh	Open Source	Monitoreo de seguridad, detección de intrusiones, SIEM	Gratis, integración con Elastic Stack, alertas en tiempo real	Curva de aprendizaje, requiere infraestructura propia
Nmap	Open Source	Escaneo de red, descubrimiento de hosts, detección de servicios	Ligero, rápido, flexible, muy usado en pentesting	Interfaz mayormente CLI, limitaciones para auditorías avanzadas

Nessus

Características	Ventajas	Limitaciones
Más de 70.000 plugins para reconocimiento y explotación de vulnerabilidades. .	Reconocimiento global, actualizaciones constantes.	Costo por licenciamiento (no es open source).
- Interfaz intuitiva, plantillas predefinidas y personalizables.	Instalación rápida, facilidad de uso.	Puede generar falsos positivos.
Integración con flujos de trabajo y sistemas de gestión.	Excelente soporte técnico y documentación.	Algunas funciones avanzadas requieren versiones premium.

OpenVAS

Características	Ventajas	Limitaciones
Plataforma open source bajo desarrollo activo.	Gratuito y altamente personalizable.	Configuración e instalación compleja.
Integración con Greenbone Vulnerability Management (GVM).	Escaneos profundos y detección masiva.	Menor soporte profesional que alternativas comerciales.
Actualización regular de la base de datos de vulnerabilidades.	Comunidad activa y soporte extendido en foros.	Puede requerir recursos elevados en grandes despliegues.

Qualys

Características	Ventajas	Limitaciones
Plataforma SaaS, escaneo en la nube.	Amplia escalabilidad.	Dependencia de conectividad a internet.
Dashboard intuitivo, reporting avanzado y cumplimiento normativo.	Ideal para ambientes distribuidos y globales.	Costos asociados a uso y escalabilidad.
Integración con DevOps y automatización de la gestión de parches.	Alta automatización, integración con otros módulos de seguridad.	Puede resultar complejo en su configuración inicial.

Burp Suite

Características	Ventajas	Limitaciones
Suite dedicada a pruebas de seguridad web (web vulnerability testing).	Alta precisión en pruebas manuales.	Limitada en tareas fuera del entorno web.
Filtros, interceptación y manipulación de tráfico HTTP/S.	Ampliamente utilizada en pentesting y desarrollo seguro de aplicaciones web.	Curva de aprendizaje para explotar funcionalidades avanzadas.
Plugin extensible, tanto en versión gratuita como de pago.	Documentación completa.	Versión gratuita es menos potente que la profesional.

Wazuh

Desarrollada para monitorización, gestión de incidentes y detección de amenazas.

Funcionalidades Clave	Ventajas	Limitaciones	Casos de Uso Típicos
Escaneo de integridad de archivos.	Solución unificada para múltiples aspectos de seguridad.	Curva de aprendizaje para despliegues avanzados.	Monitorización de infraestructura crítica.
Monitoreo de logs y correlación de alertas.	Escalabilidad en entornos de hasta miles de nodos.	El escaneo de red puro es complementario y depende de integraciones.	Cumplimiento normativo (GDPR, PCI DSS, HIPAA).
Integración con SIEM y análisis de agentes distribuidos.	Integración con herramientas externas (Elastic Stack, Kibana, Splunk).	Requiere recursos considerables en grandes despliegues.	Seguridad multinivel en empresas y entornos educativos.
Capacidad para descubrir hosts y servicios en red.	Comunidad activa y documentación extensa.		

Nmap

Herramienta open-source utilizada globalmente en auditorías y pentesting.

Funcionalidades Clave	Ventajas	Limitaciones	Casos de Uso Típicos
Escaneo de puertos TCP y UDP.	Velocidad y precisión en grandes redes.	Interfaz básica, centrada en terminal (excepto variantes como Zenmap).	Descubrimiento de hosts y mapeo de red.
Detección de servicios, versiones y sistemas operativos.	Personalización mediante scripts NSE.	No ejecuta análisis de vulnerabilidades profundas.	Inventario de activos y puertos expuestos.
Scripting avanzado para automatizar tareas.	Documentación y comunidad amplias.	Puede ser detectado por sistemas IDS.	Primer paso en auditorías de seguridad.
Identificación de dispositivos activos y topología de red.	Compatibilidad multiplataforma.		