Informe de Planificación del Proceso de Hacking Ético

Fecha: 16 de junio de 2025

Alcance y objetivos

Este documento presenta la programación estructurada de las fases del hacking ético en un entorno vulnerable. Sirve como guía de planificación, priorización y seguimiento durante la evaluación de seguridad de OWASP Juice Shop.

Metodología

El cronograma se diseñó sobre las fases reconocidas de las guías OWASP y PTES. Cada fase recibe bloques de tiempo ajustados a su complejidad y al esfuerzo estimado de las tareas. Se prioriza el reconocimiento pasivo antes de avanzar a pruebas más intrusivas y se reserva tiempo suficiente para la validación de resultados y elaboración de documentación.

Cronograma propuesto

Fase del hacking ético	Día asignado	Duración estimada	Herramientas clave	Observaciones
Reconocimiento	Lunes (mañana)	cuatro horas	Google Dorks, Shodan, DevTools	Búsqueda OSINT y escaneo básico
Enumeración	Lunes (tarde)	cuatro horas	Nmap, Dirbuster, Burp Suite	Descubrimiento de rutas, servicios y APIs
Explotación	Martes (jornada completa)	ocho horas	SQLMap, Burp Suite, Metasploit	Pruebas de inyección, XSS y subida de archivos
Post-explotación	Miércoles (mañana)	tres horas	Meterpreter, JWT.io, scripts privesc	Movimiento lateral, persistencia y recolección

Elaboración de informe	Miércoles (tarde)	cinco horas	Word, capturas de pantalla, CVSS	Documentación de hallazgos y recomendaciones

Justificación del cronograma

La fase de reconocimiento combina OSINT y escaneo activo para establecer un mapeo inicial que reduce el riesgo en etapas posteriores. La enumeración recibe el mismo tiempo que el reconocimiento porque hallar rutas ocultas y puntos de entrada requiere un análisis detallado. La explotación ocupa una jornada completa al incluir múltiples técnicas automatizadas y manuales. En post-explotación se dedica menos tiempo, pero con un enfoque intenso en persistencia y análisis de privilegios. El informe se considera parte fundamental del proceso; a pesar de disponer de herramientas de automatización, su redacción requiere media jornada para garantizar claridad y calidad.

Herramientas de apoyo

Se sugiere utilizar hojas de cálculo (Google Sheets o Excel) para mantener actualizado el cronograma y diagramas de Gantt simples (Draw.io o TeamGantt) cuando sea necesario presentar la planificación de forma gráfica. Herramientas de gestión ágil (Trello o Notion) pueden emplearse para asignar tareas y registrar el avance en tiempo real.

Conclusión

El cronograma refleja una distribución equilibrada de tiempo y recursos, alineada con las buenas prácticas de planificación en pentesting. Facilita el control de avance, la asignación de responsabilidades y la entrega puntual de resultados.