Metodologías Hacking Ético

Santiago Hernández Ramos
@santiagohramos

IMPORTANCIA DE LAS METODOLOGÍAS

- Las metodologías nos facilitan la realización de un conjunto de actividades en un orden determinado y estableciendo una prioridad adecuada para intentar garantizar el éxito y alcanzar un objetivo final

METODOLOGÍAS PRINCIPALES

- OSSTMM (Open-Source Security Testing Methodology Manual): https://www.isecom.org/OSSTMM.3.pdf
- The Penetration Testing Execution Standard: http://www.pentest-standard.org/index.php/Main_Page
- ISSAF (Information Systems Security Assessment Framework)
- OTP (OWASP Testitng Project)

METODOLOGÍA DE ESTE CURSO

- Definición del alcance del test de penetración
- Recopilación de información
- Identificación y análisis de vulnerabilidades
- Explotación de las vulnerabilidades
- Post-explotación
- Elaboración de un documento de reporte

DEFINICIÓN DEL ALCANCE DEL HACKING ÉTICO

- Antes de realizar ninguna acción, discutir con el cliente las tareas que llevará a cabo el analista durante el Hacking Ético, así como los roles y responsabilidades de ambos
- Asegurar mediante contrato firmado que las acciones que se llevan a cabo son en representación del cliente
- Análisis de las políticas de la organización que definen el uso que los usuarios hacen de los sistemas y de la infraestructura
- Procedimiento en el caso de que se localice una intrusión por un tercero