IFCT154: Red Team. Seguridad ofensiva

Objetivo general

- Adquirir las competencias básicas para el desarrollo de una defensa ofensiva en procesos de ciberseguridad.

Objetivos específicos

- Analizar los métodos de recopilación de información y sus diferencias entre enfoques activos, pasivos, manuales y automatizados.
- Aplicar herramientas y frameworks OSINT para la obtención estructurada de datos en entornos simulados de Red Teaming.
- Evaluar la superficie de ataque mediante la identificación de activos, servicios, vulnerabilidades y dependencias tecnológicas.
- Integrar consideraciones legales y éticas en las operaciones de reconocimiento, garantizando el cumplimiento normativo y el respeto a la privacidad.
- Comprender los diferentes mecanismos de explotación y sus fases, desde la identificación de vulnerabilidades hasta el desarrollo de exploits.
- Analizar las técnicas de evasión de mitigaciones en sistemas modernos y evaluar sus implicaciones en la seguridad del software.
- Aplicar metodologías de prueba, depuración y validación de exploits en entornos controlados, respetando los principios de ética y responsabilidad.
- Identificar configuraciones erróneas y debilidades en servicios, sistemas embebidos y entornos cloud para proponer estrategias de mitigación.
- Comprender los procedimientos de postexplotación para consolidar el acceso y extraer información útil.

- Identificar y emplear los distintos canales de comunicación y herramientas para mantener la conexión con sistemas comprometidos.
- Aplicar técnicas de persistencia y movimiento lateral para ampliar el alcance de una intrusión de forma controlada.
- Elaborar documentación exhaustiva de las acciones realizadas, preservando evidencias y reportando hallazgos de manera efectiva.
- Analizar los procesos de planificación y alcance en operaciones de Red Team.
- Comprender y aplicar modelos de amenazas junto con el mapeo de TTPs.
- Evaluar y diseñar infraestructuras ofensivas que integren prácticas sólidas de OPSEC.
- Interpretar métricas y elaborar informes profesionales para la mejora continua de las operaciones.

Contenidos

IFCT154: Red Team. Seguridad ofensiva	Tiempo estimado
Unidad 1: Reconocimiento y recopilación de información. 1. Métodos de recopilación de información. 1.1. Inteligencia orientada a Red Teaming. 1.2. Identificación de objetos. 1.3. Ingeniería social. 1.4. Escaneo de vulnerabilidades y puertos. 2. Fuentes públicas y OSINT. 2.1. Fuentes web y motores de búsqueda. 2.2. Redes sociales y análisis de perfiles. 2.3. Registros públicos, bases de datos y minería de documentos. 3. Reconocimiento pasivo. 3.1. WHOIS, DNS y mapeo de infraestructura. 3.2. Análisis de metadatos y extracción de información incrustada. 4. Análisis de superficie de ataque. 4.1. Inventario de activos y clasificación de riesgos. 4.2. Mapeo de aplicaciones, servicios y dependencias. 5. Herramientas y automatización para recopilación. 5.1. Frameworks y herramientas OSINT. 5.2. Scripting, pipelines y orquestación de tareas. 6. Consideraciones legales y éticas. 6.1. Permisos, alcance y cumplimiento normativo.	
Cuestionario de Autoevaluación UA 01	**30 minutos**
Actividad de Evaluación UA 01	**45 minutos**
Tiempo total de la unidad	**13 horas**
Unidad 2: Explotación y técnicas de intrusión. 1. Diferentes métodos de explotación. 1.1. Exploits. 1.2. Canales alternativos de comunicación.	

2. Tipos de exploits. 2.1. Desbordamientos y corrupción de memoria. 3. Vectores de entrega. 3.1. Ingeniería de mensajes y archivos maliciosos. 4. Explotación web. 4.1. Inyección, RCE y lógica insegura. 5. Explotación de servicios de red. 5.1. Servicios TCP/UDP, protocolos y fuzzing. 6. Explotación móvil y embebida. 6.1. Android/iOS, firmware e IoT. 7. Explotación en entornos cloud. 7.1. Abuso de API, roles y configuraciones. 8. Técnicas de escalado de privilegios. 8.1. Elevación local y abuso de SUID/servicios. 9. Bypass de mitigaciones. 9.1. ASLR, DEP, SMEP/SMAP y técnicas de evasión. 10. Desarrollo y prueba de exploits. 10.1. PoC, debugging y pruebas en entornos controlados.	
Cuestionario de Autoevaluación UA 02	**30 minutos**
Actividad de Evaluación UA 02	**45 minutos**
Tiempo total de la unidad	**13 horas**
Unidad 3: Postexplotación y mantenimiento del acceso. 1. Realización y análisis de resultados en la postexplotación. 1.1. Canales de comunicación. 1.2. Malware. 1.3. Rootkits. 1.4. Pivoting. 1.5. Backdoors. 2. Persistencia y técnicas de permanencia. 2.1. Mecanismos de inicio y tareas programadas. 2.2. Servicios y modificaciones de configuración. 3. Recolección y exfiltración de datos. 3.1. Identificación y clasificación de información sensible. 3.2. Técnicas de exfiltración (encapsulado, esteganografía). 3.3. Compresión y cifrado de datos. 4. Evasión y anti-forense.	

4.1. Limpieza de logs y huellas. 5. Movilidad lateral y descubrimiento interno. 5.1. Recolección de credenciales y ataques Pass the Hash/Pass the Ticket. 5.2. Uso de herramientas legítimas (Living off the Land). 6. Validación, documentación y reporting. 6.1. Preservación de evidencias y documentación de pruebas.	
Cuestionario de Autoevaluación UA 03	**30 minutos**
Actividad de Evaluación UA 03	**45 minutos**
Tiempo total de la unidad	**13 horas**
Unidad 4: Planificación y ejecución de operaciones Red Team. 1. Planificación y alcance de operaciones. 1.1. Definición de objetivos y escenarios. 1.2. Desarrollo de reglas de compromiso (ROE) y límites operativos. 2. Modelado de amenazas y mapeo de TTPs. 2.1. Uso de MITRE ATT&CK y frameworks de referencia. 3. Diseño de infraestructura de ataque. 3.1. Comandos y control (C2), proxies y prácticas de OPSEC para infraestructura. 4. Operaciones OPSEC y seguridad del equipo. 5. Integración con Blue Team y ejercicios Purple Team. 6. Simulación física y acceso en persona. 7. Automatización y orquestación de campañas. 7.1. Pipelines reproducibles y CI/CD para pruebas de seguridad. 8. Métricas, KPIs y evaluación del impacto. 9. Reporting ejecutivo y técnico. 10. Revisión post operativa y transferencia de conocimiento.	
Cuestionario de Autoevaluación UA 04	**30 minutos**
Actividad de Evaluación UA 04	**45 minutos**
Tiempo total de la unidad	**11 horas**
4 unidades	**50 horas**