ITIFC0007: Funciones del Red Team, Blue Team y Purple Team

Objetivo general

- Adquirir las competencias básicas para el desarrollo de una defensa ofensiva en procesos de ciberseguridad.
- Adquirir las competencias básicas para el desarrollo de una seguridad defensiva en procesos de ciberseguridad.
- Integrar las tácticas y controles defensivos del Blue Team con las amenazas y vulnerabilidades encontradas por el Red Team.

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.
- Comprender el funcionamiento general de las redes IP en entornos corporativos.
- Identificar servicios, protocolos y equipos que intervienen en la comunicación de red.
- Analizar mecanismos de segmentación, direccionamiento, enrutamiento y traducción de direcciones.
- Aplicar criterios básicos de documentación, inventariado y organización de infraestructuras de red.
- Analizar el despliegue y bastionado de sistemas para reducir la superficie de ataque desde las fases iniciales de implantación.
- Identificar activos, servicios corporativos, dependencias y riesgos asociados a infraestructuras en producción.
- Configurar medidas de protección en sistemas Windows, Linux, redes perimetrales, firewalls y zonas de seguridad.

- Aplicar mecanismos de cifrado, autenticación y securización de servicios para proteger aplicaciones y datos en tránsito.
- Identificar ataques, anomalías e indicadores de compromiso mediante el análisis de registros, tráfico de red y actividad en sistemas.
- Aplicar procedimientos de monitorización, auditoría y respuesta ante incidentes para contener, erradicar y recuperar servicios afectados.
- Diferenciar tecnologías de detección como IDS, IPS, HIDS, NIDS, SIEM y EDR, atendiendo a su ámbito de visibilidad y despliegue.
- Correlacionar eventos procedentes de distintos sistemas para interpretar patrones sospechosos y apoyar la toma de decisiones defensivas.
- Analizar la planificación estratégica de la seguridad corporativa desde una perspectiva alineada con los objetivos de negocio.
- Diseñar políticas, normativas internas y controles de acceso que protejan sistemas, identidades y datos sensibles.
- Aplicar medidas de seguridad en entornos Cloud, servicios SaaS y escenarios de continuidad del negocio.
- Evaluar la evolución de la seguridad mediante métricas, KPIs, revisión de madurez y actualización continua de planes.
- Comprender la estructura, funciones y modelos de operación de un Centro de Operaciones de Seguridad, diferenciando sus componentes humanos, tecnológicos y procedimentales.
- Aplicar criterios de clasificación, priorización y triaje para gestionar alertas de seguridad con menor ruido operativo y mayor coherencia en la respuesta.
- Analizar flujos de trabajo, logs, telemetría e hipótesis de caza para detectar comportamientos anómalos y amenazas que no hayan generado alertas evidentes.
- Evaluar la eficacia operativa del SOC mediante métricas, revisión de procesos, coordinación interdepartamental y mejora continua.
- Planificar pruebas de seguridad mediante objetivos, alcance, reglas de enfrentamiento, ventanas de trabajo y criterios de finalización.

- Definir los elementos operativos necesarios para preparar entornos, accesos, dependencias, comunicaciones y registro de evidencias.

- Analizar el enfoque Purple Team como modelo colaborativo entre capacidades ofensivas y defensivas orientado a mejorar la detección, la respuesta y la resiliencia.

- Diferenciar las funciones de Red Team, Blue Team y Purple Team, identificando sus responsabilidades, límites y sinergias dentro de un ejercicio de ciberseguridad.

- Analizar amenazas reales para diseñar medidas defensivas alineadas con los activos del negocio.

- Seleccionar fuentes de inteligencia de amenazas atendiendo a criterios de calidad, relevancia y aplicabilidad.

- Traducir TTPs en controles preventivos, detectivos y correctivos vinculados a escenarios de ataque.

- Identificar brechas de visibilidad, cobertura y respuesta mediante el estudio de casos prácticos.

- Analizar la ejecución de una emulación de adversario mediante la comparación entre acciones planificadas, telemetría generada y resultados defensivos observados.

- Diseñar guiones de emulación secuenciados que representen técnicas realistas de acceso, persistencia, escalada, evasión, descubrimiento, movimiento lateral y acciones sobre objetivos.

- Verificar la capacidad de los sistemas defensivos para registrar, correlacionar y alertar sobre comportamientos asociados a una intrusión simulada.

- Medir la eficacia de la respuesta defensiva a partir de detecciones generadas, trazas disponibles, tiempos de detección y tiempos de respuesta.

- Analizar los principios de detección como código aplicados al Purple Team, valorando la gestión de reglas, parseadores, enriquecimientos y documentación.

- Diseñar y ejecutar pruebas automatizadas sobre reglas de detección, definiendo entradas, expectativas y aserciones y generando datos sintéticos y reproducibles.

- Integrar las detecciones en pipelines de CI/CD, gestionando entornos separados y aplicando despliegues controlados con capacidad de rollback.
- Administrar el ciclo de vida del contenido de detección mediante un catálogo de estados, ownership y la gestión de excepciones, supresiones y reglas temporales.
- Comprender la estructura de un informe Purple Team, diferenciando alcance, hipótesis, resultados, narrativa ejecutiva y anexo técnico.
- Definir métricas de desempeño que permitan evaluar detección, cobertura, tiempos operativos y calidad de la respuesta.
- Interpretar evidencias, línea temporal e indicadores observados para relacionar la actividad emulada con la capacidad defensiva.
- Diseñar un plan de remediación con backlog priorizado, criterios de verificación de cierre y seguimiento de mejoras.

- **Contenidos**

ITIFC0007. Funciones del Red Team, Blue Team y Purple Team	Tiempo estimado
IFCT154. Red Team. Seguridad ofensiva	
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	**10 horas**
Examen final	**1 hora**
4 unidades	**50 horas**
IFCT155. Blue Team. Seguridad defensiva	

Unidad 1: Fundamentos de sistemas y redes IP. 1. Conocimiento de los sistemas y redes IP. 1.1. Redes y direccionamiento IP. 1.2. Servidores IP. 1.3. Creación de zonas en redes privadas. 1.4. Virtualización de servidores. 1.5. Topologías y arquitecturas de red. 1.6. Protocolos esenciales de red (ARP, ICMP y TCP/UDP) 1.7. Introducción al direccionamiento IPv6 y coexistencia con IPv4. 1.8. NAT y técnicas de traducción de direcciones. 1.9. Segmentación y aislamiento mediante VLAN. 1.10. Servicios esenciales de red: DHCP y DNS. 1.11. Enrutamiento básico y configuración de gateways. 1.12. Equipamiento de red: switches, routers y puntos de acceso. 1.13. Documentación, inventariado y mapas de red.	
Cuestionario de Autoevaluación UA 01	**30 minutos**
Actividad de Evaluación UA 01	**45 minutos**
Tiempo total de la unidad	**10 horas**
Unidad 2: Despliegue seguro y bastionado de infraestructuras. 1. Análisis del despliegue y bastionado de sistemas. 1.1. Servicios corporativos en producción. 1.2. Creación del firewall. 1.3. Protección de comunicaciones. 2. Evaluación inicial del entorno. 2.1. Identificación de activos y dependencias. 2.2. Análisis de riesgos en sistemas y servicios. 3. Bastionado de sistemas. 3.1. Endurecimiento de sistemas Windows. 3.2. Endurecimiento de sistemas Linux. 4. Protección perimetral. 4.1. Diseño de arquitecturas de red seguras. 4.2. Segmentación de red y zonas de seguridad. 4.3. Filtrado avanzado y políticas de firewall. 5. Seguridad en servicios y comunicaciones. 5.1. Securización de servicios expuestos a Internet. 5.2. Configuración segura de protocolos y cifrado.	
Cuestionario de Autoevaluación UA 02	**30 minutos**

Actividad de Evaluación UA 02	**45 minutos**
Tiempo total de la unidad	**12 horas**
Unidad 3: Detección de amenazas, análisis y respuesta ante incidentes. 1. Detección de ataques y respuestas ante incidencias. 1.1. Análisis y detección de ataques a servidores. 1.2. Monitorización de servicios críticos. 1.3. Herramientas de detección. 1.4. Auditoría informática. 1.5. Respuesta ante incidencias y procedimientos de actuación. 2. Técnicas de detección y análisis. 2.1. Identificación de indicadores de compromiso. 2.2. Análisis de comportamiento anómalo y patrones sospechosos. 2.3. Correlación de eventos mediante plataformas SIEM. 2.4. Análisis de tráfico de red para detección de amenazas. 3. Sistemas y tecnologías de detección. 3.1. IDS/IPS: funcionamiento y despliegue. 3.2. Detección basada en host (HIDS) 3.3. Detección basada en red (NIDS) 3.4. EDR y protección avanzada de endpoints.	
Cuestionario de Autoevaluación UA 03	**30 minutos**
Actividad de Evaluación UA 03	**45 minutos**
Tiempo total de la unidad	**11 horas**
Unidad 4: Gestión avanzada de la seguridad en la organización. 1. Planificación estratégica de la seguridad corporativa. 2. Diseño de políticas y normativas internas de seguridad. 3. Gestión de identidades y accesos (IAM) 4. Seguridad en entornos cloud y servicios SaaS. 5. Protección y control de datos sensibles. 6. Gestión de la continuidad del negocio. 6.1. Plan de continuidad de negocio (BCP) 6.2. Plan de recuperación ante desastres (DRP) 7. Supervisión y evolución de la seguridad. 7.1. Definición de métricas y KPIs de ciberseguridad. 7.2. Evaluación periódica del nivel de madurez de la organización. 7.3. Actualización y revisión continua de planes de	

seguridad.	
Cuestionario de Autoevaluación UA 04	**30 minutos**
Actividad de Evaluación UA 04	**45 minutos**
Tiempo total de la unidad	**8 horas**
Unidad 5: Operaciones de seguridad y gestión del SOC. 1. Estructura y funciones de un Centro de Operaciones de Seguridad (SOC) 2. Modelos de SOC: interno, híbrido y externalizado. 3. Gestión de alertas y priorización. 3.1. Clasificación de alertas por criticidad. 3.2. Métodos de triaje y reducción de ruido. 4. Flujos operativos dentro del SOC (workflow) 5. Gestión avanzada de logs y telemetría de seguridad. 6. Técnicas de Threat Hunting. 6.1. Hipótesis de caza y fuentes de información. 6.2. Procedimientos manuales y asistidos. 7. Coordinación con otros equipos (TI, red, legal, dirección) 8. Revisión periódica de la eficacia operativa del SOC.	
Cuestionario de Autoevaluación UA 05	**30 minutos**
Actividad de Evaluación UA 05	**45 minutos**
Tiempo total de la unidad	**8 horas**
Examen final	**1 hora**
5 unidades	**50 horas**
IFCT156. Purple Team	
Unidad 1: Purple Team y la ciberseguridad. 1. Planificación de pruebas. 1.1. Objetivos de la prueba y preguntas a responder. 1.2. Alcance, exclusiones y criterios de finalización. 1.3. Selección del escenario y nivel de realismo requerido. 1.4. Reglas de enfrentamiento, ventanas de trabajo y condiciones de parada. 1.5. Preparación de entorno, accesos y dependencias. 1.6. Plan de comunicaciones y coordinación operativa. 1.7. Registro de evidencias, trazabilidad y custodia.	

2. Definición y principios del Purple Team en el contexto de ciberseguridad. 3. Diferencias y sinergias entre Red Team, Blue Team y Purple Team.	
Cuestionario de Autoevaluación UA 01	**30 minutos**
Actividad de Evaluación UA 01	**45 minutos**
Tiempo total de la unidad	**9 horas**
Unidad 2: Planificar e implementar una defensa de amenazas informada. 1. Definición de medidas. 1.1. Fuentes de inteligencia de amenazas y criterios de calidad. 1.2. Modelado de amenazas orientado al negocio y activos críticos. 1.3. Traducción de TTPs en requisitos de control (preventivos, detectivos y correctivos) 1.4. Ingeniería de detecciones: reglas, correlaciones y umbrales. 1.5. Controles de hardening y reducción de superficie de ataque. 1.6. Gestión de vulnerabilidades y parcheo informados por amenazas. 2. Análisis de casos prácticos. 2.1. Selección de casos alineados a perfiles de adversario y sector. 2.2. Descomposición del ataque en fases para identificar oportunidades defensivas. 2.3. Identificación de brechas de visibilidad, cobertura y capacidad de respuesta.	
Cuestionario de Autoevaluación UA 02	**30 minutos**
Actividad de Evaluación UA 02	**45 minutos**
Tiempo total de la unidad	**10 horas**
Unidad 3: Realizar la emulación de adversario. 1. Análisis y evaluación de la ejecución. 1.1. Preparación del guion de emulación y secuenciación de acciones. 1.2. Instrumentación y verificación de la telemetría durante la ejecución. 1.3. Ejecución controlada de técnicas y validaciones previas	

por paso. 1.4. Simulación de acceso inicial y establecimiento de persistencia. 1.5. Simulación de escalada de privilegios y evasión defensiva. 1.6. Simulación de descubrimiento y movimiento lateral. 1.7. Simulación de acciones sobre objetivos: exfiltración, impacto y/o interrupción. 1.8. Medición de resultados: detecciones generadas, trazas y tiempos de respuesta.	
Cuestionario de Autoevaluación UA 03	**30 minutos**
Actividad de Evaluación UA 03	**45 minutos**
Tiempo total de la unidad	**8 horas**
Unidad 4: Detección como código y automatización de pruebas. 1. Principios de detección como código (DaC) aplicados a Purple Team. 1.1. Estructura del repositorio: reglas, parsers, enriquecimientos y documentación asociada. 1.2. Convenciones de nomenclatura, versionado y trazabilidad de cambios. 1.3. Revisión por pares y criterios de aceptación para cambios en contenido de detección. 2. Diseño de pruebas automatizadas para detecciones. 2.1. Pruebas unitarias de reglas: entradas, expectativas y aserciones. 2.2. Generación de eventos sintéticos y datasets reproducibles para pruebas. 2.3. Reproducción de logs (replay) y simulación controlada de secuencias de actividad. 3. Integración con pipelines y entornos. 3.1. CI/CD para contenido de SIEM/EDR/XDR: empaquetado, test y despliegue. 3.2. Separación de entornos (laboratorio, preproducción, producción) y promoción controlada. 3.3. Rollback y gestión de incidencias derivadas de cambios en detecciones. 4. Gobierno del ciclo de vida del contenido de detección. 4.1. Catálogo de detecciones: estados (borrador, activo, deprecated) y ownership. 4.2. Gestión de excepciones, supresiones y reglas temporales con justificación.	
Cuestionario de Autoevaluación UA 04	**30 minutos**

Actividad de Evaluación UA 04	**45 minutos**
Tiempo total de la unidad	**14 horas**

Unidad 5: Reporte, métricas y cierre del ciclo Purple Team. 1. Estructura del informe Purple Team: alcance, hipótesis y resultados. 1.1. Narrativa ejecutiva orientada a impacto y riesgo. 1.2. Anexo técnico: evidencias, línea temporal e indicadores observados. 2. Definición de métricas de desempeño del ejercicio. 2.1. Métricas de detección y cobertura frente a TTPs emuladas. 2.2. Métricas operativas: tiempos de alerta, triage, contención y recuperación. 3. Plan de remediación y seguimiento de mejoras. 3.1. Priorización del backlog y criterios de verificación de cierre.	
Cuestionario de Autoevaluación UA 05	**30 minutos**
Actividad de Evaluación UA 05	**45 minutos**
Tiempo total de la unidad	**8 horas**
Examen final	**1 hora**
5 unidades	**50 horas**
3 programas formativos /14 unidades	**150 horas**