CYBERPEACE

Red Team

EQUIPO DE ATAQUE SIMULADO

SIMULACIÓN DE ADVERSARIOS REALES PARA EVALUAR Y FORTALECER LAS DEFENSAS DE SEGURIDAD DE SU ORGANIZACIÓN

¿QUÉ ES UN RED TEAM?

Es un grupo de expertos en seguridad que simulan ataques realistas y coordinados contra una organización, adoptando la mentalidad y técnicas de adversarios reales. Su objetivo es evaluar la efectividad de las defensas existentes y identificar puntos débiles antes de que los atacantes reales los exploten.

Simulación Realista
Imitación de adversarios reales

Enfoque en Objetivos
Ataques dirigidos a metas específicas

Sigilo y Persistencia
Operaciones prolongadas y discretas

Evaluación Integral
Prueba de personas, procesos y tecnología

BENEFICIOS

- **Evaluación Realista de Defensas**

Prueba la efectividad real de los controles de seguridad frente a adversarios determinados.

- **Detección de Brechas Ocultas**

Identifica vulnerabilidades que escapan a las evaluaciones tradicionales de seguridad.

- **Mejora de Capacidades de Detección**

Ayuda a calibrar y mejorar los sistemas SIEM, EDR y otros mecanismos de detección.

- **Validación de Contramedidas**

Verifica que las medidas de seguridad implementadas funcionen como se espera.

- **Preparación para Incidentes Reales**

Entrena al equipo Blue Team en la detección y respuesta a ataques sofisticados.

FASES DE PRUEBAS

1) Planificación

Definición de alcance, objetivos, reglas de compromiso y metodología de ataque.

- Establecimiento de objetivos
- Definición de alcance y reglas
- Recolección de inteligencia inicial
- Desarrollo de plan de ataque

2) Reconocimiento

Recopilación de información sobre el objetivo mediante fuentes abiertas y técnicas activas.

- OSINT (Open Source Intelligence)
- Escaneo de redes y puertos
- Enumeración de servicios
- Identificación de vectores de ataque

3) Acceso Inicial

Obtención del primer punto de apoyo en el entorno objetivo mediante diversos vectores.

- Phishing personalizado
- Explotación de vulnerabilidades
- Ataques a servicios expuestos
- Ingeniería social

4**) Movimiento Lateral**

Expansión dentro del entorno una vez obtenido el acceso inicial.

- Escalada de privilegios
- Movimiento entre sistemas
- Dumping de credenciales
- Análisis de la red interna

5) Ejecución de Objetivos

Cumplimiento de los objetivos establecidos y exfiltración de datos si aplica.

- Acceso a datos críticos
- Exfiltración controlada
- Impacto controlado en sistemas
- Documentación de hallazgos

SERVICIOS ESPECIALIZADOS

Pentesting

Evaluación de seguridad proactiva que simula ataques reales para identificar vulnerabilidades en sistemas, redes y aplicaciones.

- Pruebas de intrusión externas e internas
- Análisis de aplicaciones web y móviles
- Pruebas de red y infraestructura
- Evaluación de controles de seguridad
- Reportes detallados con recomendaciones

Cyber Risk Assessment

Identificación y evaluación sistemática de vulnerabilidades técnicas y su impacto potencial en el negocio.

- Escaneo de vulnerabilidades automatizado
- Análisis de configuración de seguridad
- Evaluación de exposición externa
- Priorización basada en riesgo
- Plan de remediación estratégico

CYBERPEACE

Phishing Campaign

Simulación de campañas de phishing controladas para medir la concienciación de los empleados y mejorar la resiliencia.

- Campañas de phishing personalizadas
- Simulación de spear phishing
- Métricas de click-through rates
- Entrenamiento contextual inmediato
- Reportes de concienciación

Secure Code Analysis

Revisión exhaustiva del código fuente y aplicaciones en ejecución para identificar vulnerabilidades de seguridad.

- SAST (Static Application Security Testing)
- DAST (Dynamic Application Security Testing)
- Análisis de dependencias
- Revisión de código manual
- Integración en CI/CD

PCI Analysis

Evaluación de cumplimiento con el estándar PCI DSS para organizaciones que manejan datos de tarjetas de pago.

- Evaluación de requisitos PCI DSS
- Pruebas de penetración específicas
- Revisión de controles de acceso
- Análisis de segmentación de red
- Preparación para auditorías

Awareness & Secure Code

Programas de capacitación para desarrolladores y personal técnico en prácticas de codificación segura.

- Talleres de seguridad para desarrolladores
- Entrenamiento en OWASP Top 10
- Prácticas de codificación segura
- Revisión de código guiada
- Capacitaciones internas

Wifi Attack

Evaluación de seguridad de redes inalámbricas para identificar vulnerabilidades en implementaciones WiFi.

- Auditoría de redes WiFi corporativas
- Pruebas de autenticación
- Evaluación de puntos de acceso
- Análisis de configuraciones
- Pruebas de rogue access points

Physical Attack

Evaluación de controles de seguridad física y pruebas de acceso no autorizado a instalaciones.

- Pruebas de acceso físico
- Evaluación de controles de entrada
- Análisis de sistemas de vigilancia
- Pruebas de tailgating
- Evaluación de políticas de acceso

CIS 20 Benchmarks Hardening

Implementación y verificación de los controles críticos de seguridad del Center for Internet Security.

- Evaluación de controles CIS
- Hardening de sistemas operativos
- Configuración segura de servicios
- Automatización de hardening
- Verificación de cumplimiento

Attack Simulation

Simulación de ataques avanzados persistentes (APT) para evaluar capacidades de detección y respuesta.

- Simulación de adversarios APT
- Pruebas de detección EDR/SIEM
- Evaluación de tiempos de respuesta
- Simulación de ransomware
- Pruebas de recuperación

Table Top Exercises

Ejercicios de simulación en escenario para entrenar equipos de respuesta a incidentes y alta dirección.

- Escenarios de incidentes realistas
- Ejercicios para equipos de crisis
- Pruebas de planes de respuesta
- Evaluación de toma de decisiones
- Mejora de comunicaciones

CYBERPEACE

METODOLOGÍA

Inteligencia	Arsenal	Ataque	Persistencia	Exfiltración	Reporting
• Recolección de información sobre el objetivo mediante OSINT, scanning y análisis de superficie de ataque.	• Desarrollo y preparación de herramientas, exploits y payloads personalizados para el engagement.	• Ejecución coordinada de vectores de ataque seleccionados basados en el análisis de inteligencia.	• Establecimiento de acceso persistente y movimiento lateral dentro del entorno objetivo.	• Extracción controlada de datos sensibles para demostrar impacto sin causar daño real.	• Documentación detallada de hallazgos, técnicas utilizadas y recomendaciones de remediación

RED TEAM

- Simula adversarios reales
- Enfoque ofensivo
- Busca vulnerabilidades
- Operaciones sigilosas
- Prueba defensas
- Mentalidad de atacante

VS

BLUE TEAM

- Defiende la organización
- Enfoque defensivo
- Construye defensas
- Monitoreo continuo
- Respuesta a incidentes
- Mentalidad de defensor

IMPACTO DEMOSTRABLE