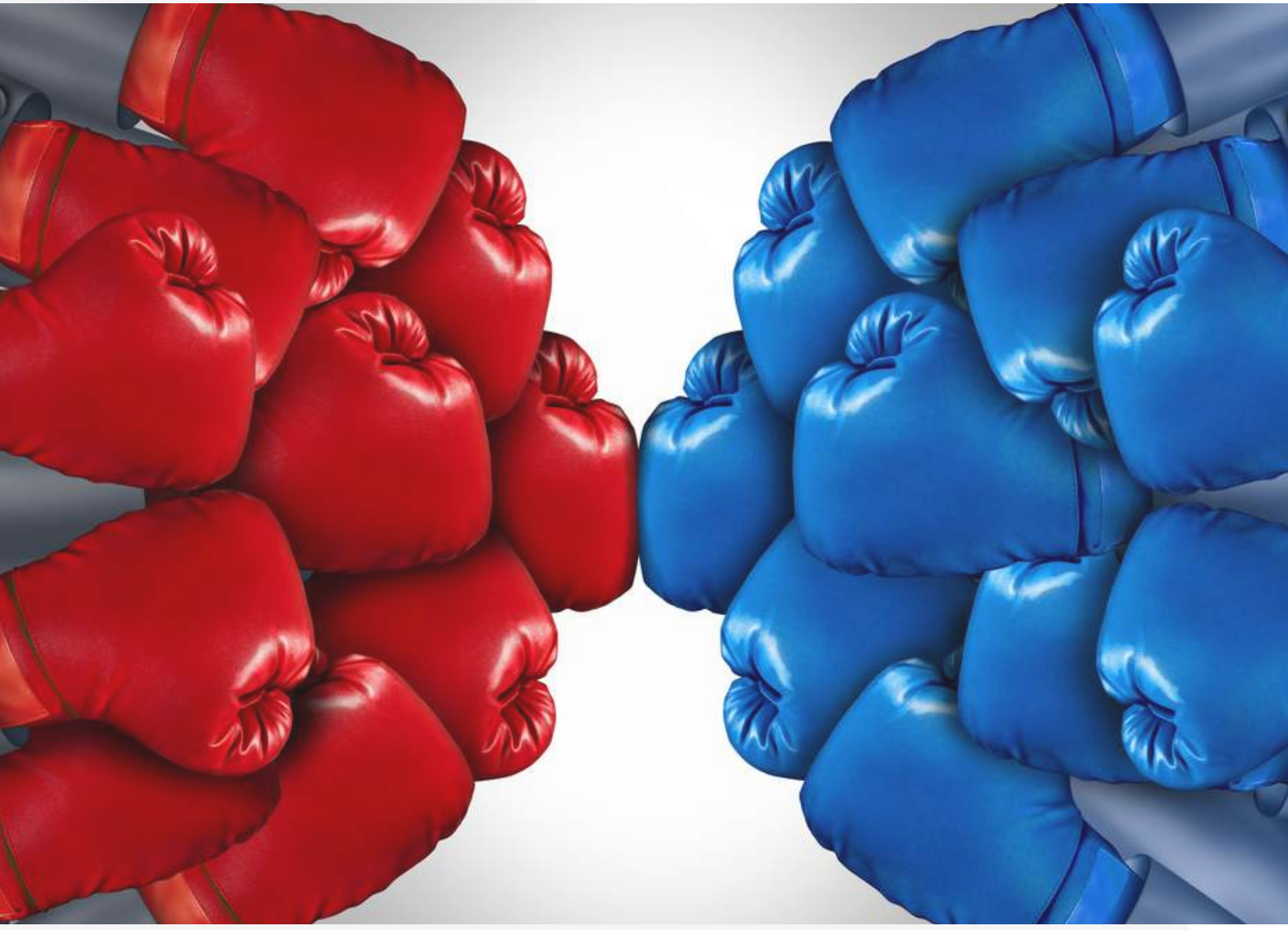
tranxfer | secure file exchange

RED TEAM, BLUE TEAM Y PURPLE TEAM.
ACCIÓN, DEFENSA Y EVALUACIÓN



RED TEAM, BLUE TEAM Y PURPLE TEAM

El sector de la ciberseguridad está en continua evolución y es necesario estar preparado para cada una de las posibles situaciones que puedan ocurrir.

En el mundo de la ciberseguridad hay diferentes equipos: el blue team, el red team y el purple team. Cada uno tiene una función diferente y se usan para evaluar y analizar posibles fallos en el sistema.

Los términos Red Team y Blue Team se usan comúnmente para describir equipos que usan sus habilidades para imitar las técnicas de ataque que los “enemigos” podrían usar, y otros equipos que usan sus habilidades para defender. De hecho, estos equipos juegan un papel importante en la defensa contra ataques cibernéticos avanzados que amenazan las comunicaciones comerciales, los datos confidenciales de los clientes o los secretos comerciales.

Cuando hablamos de seguridad informática y protección de datos estos dos equipos fundamentales realizan un trabajo complementario para detectar vulnerabilidades, prevenir ataques informáticos y emular escenarios de amenaza.

PARA ENTENDER EN DETALLE EL FUNCIONAMIENTO Y LAS FUNCIONES DE CADA EQUIPO ENTRAREMOS A DESCRIBIR CADA UNO:

Red Team

El Red team ataca el sistema para probar su seguridad y ver sus vulnerabilidades

El Red team es el que nombramos seguridad ofensiva y está formado por profesionales de la seguridad que actúan como adversarios para superar los controles de ciberseguridad. Se encarga de poner a prueba el blue team buscando vulnerabilidades.

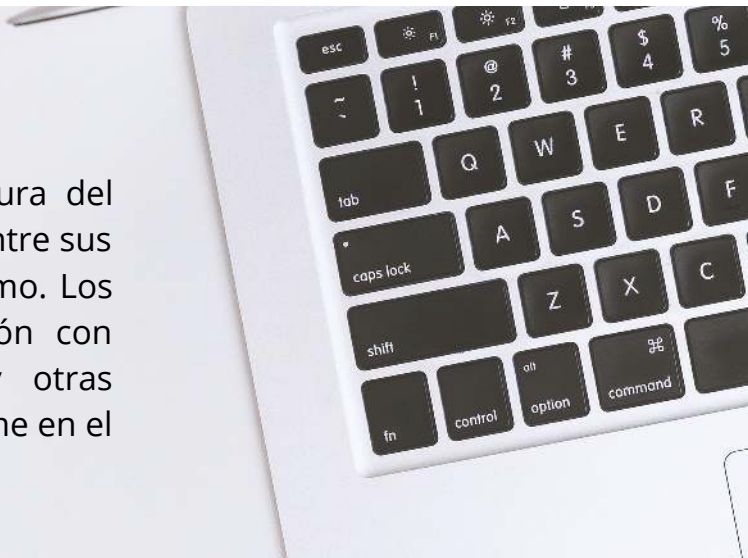
El Red team ataca el sistema de manera radical para probar la eficacia del programa de seguridad. Este ataque no es avisado para que la defensa sea con máxima objetividad y ver cómo sería un ataque real. Los ataques realizados pueden ser interno de la propia empresa o puede ser de una empresa externa. Los equipos suelen estar formados por hackers éticos que evalúan la seguridad de manera objetiva.

La eficacia del red team cae en comprobar de manera constante la posibilidad de que, alguien externo a la empresa, pueda llegar a tener acceso a los sistemas y pueda modificarlos.

Con la creación de los distintos ataques se logra ver las posibles fuga de seguridad y ver comportamientos y posibles técnicas de futuros atacantes.

Red team vs Pentesters

El Red team se suele confundir con la figura del pentesters ya que hay cierta superposición entre sus funciones y habilidades, pero no son lo mismo. Los pentesters realizan un proceso de intrusión con técnicas de pivoting, ingeniería social y otras pruebas de hacking que finaliza con un informe en el que se identifican vulnerabilidades.



¿CÓMO FUNCIONA UN RED TEAM?

Los Red Team, aunque no lo parezca, pasan más tiempo planificando un ataque que realizando ataques. De hecho, el Red team se encarga de implementar una serie de métodos para obtener acceso a una red. Se contrata el Red team para probar la efectividad del equipo azul emulando los comportamientos de un equipo negro real para que el ataque sea lo más realista y caótico posible.

Utilizan una gran variedad de métodos y herramientas para explotar y derrumbar las debilidades y vulnerabilidades de una red como phishing, identificación de vulnerabilidades, intrusión de firewall, etc. Es importante tener en cuenta que estos equipos utilizarán todos los medios necesarios, según los términos del compromiso, para ingresar en un sistema. Dependiendo de la vulnerabilidad, pueden implementar malware para infectar host o incluso eludir los controles de seguridad física clonando tarjetas de acceso.

- Por lo tanto el Red Team es un entretenimiento para el Blue Team donde se **evalúa la capacidad real que tiene una organización para proteger sus activos críticos** y sus capacidades de detección y respuesta considerando tanto el plano tecnológico, como el de procesos y humano.

FUNCIONES DEL RED TEAM

- Los Red Teams **emulan a los atacantes,** utilizando sus mismas herramientas o similares. Con los ataques quieren lograr explotar vulnerabilidades de seguridad de los sistemas y/o aplicaciones (exploits), técnicas de pivoting (saltar de una máquina a otra) y objetivos (sistemas y/o aplicaciones) de la organización.

- Realizan un **proceso de emulación de escenarios de amenazas** a los cuales se enfrenta una organización, analizando la seguridad desde el punto de vista de los atacantes, para dar al equipo de seguridad (Blue Team) la posibilidad de defenderse de forma controlada y constructiva de ataques.

Blue Team

El Blue team defiende el sistema y analiza las vulnerabilidades encontradas

El Blue Team es el que nombramos seguridad defensiva y está formado por profesionales de la seguridad que se encargan de proteger activos críticos de la organización contra cualquier amenaza. Se encarga de defender de manera proactiva ataques reales y programados por el Red Team.

El Blue Team tiene como objetivo **analizar patrones y comportamientos** que salen de lo común. También se encarga de realizar **evaluaciones de las distintas amenazas que pueden afectar a la organización**, monitorear y recomendar planes de actuación para mitigar los posibles riesgos. Para prevenir los ataques crean una base de datos con un abanico de posibles casos de uso.

En caso de ataque, el Blue team, pasa a la acción y realizan tareas de respuesta, incluyendo análisis forense de las máquinas afectadas, trazabilidad de los vectores de ataque, propuesta de solución y establecimiento de medidas de detección. Aunque el Blue team se suele usar para defenderse de ataques grandes, evalúa y analiza cualquier fallo de seguridad que pase en el sistema aunque sea diminuto.

El Blue Team se encarga de analizar patrones y comportamientos que salen de lo común para reforçar el sistema de manera continuada

Blue Team vs equipos de seguridad

El Blue team se diferencia de los equipos de seguridad convencionales porque tienen la funcionalidad de estar recogiendo datos de vigilancia de manera constante para una continua evaluación, mientras que los equipos de seguridad convencionales solo actúan al recibir un input de ataque. El Blue team suele estar formado por el personal interno de ciberseguridad de la organización.

¿CÓMO FUNCIONA UN BLUE TEAM?

El Blue Team empieza con una primera recopilación de datos, documenta exactamente lo que debe protegerse y lleva a cabo una evaluación de riesgos. Después refuerzan el acceso al sistema de muchas maneras. También se encargan de la educación del personal sobre las políticas de contraseñas más estrictas y se aseguran de que comprenden y cumplen los procedimientos de seguridad.

Normalmente se implementan herramientas de monitoreo que permiten que la información sobre el acceso a los sistemas se registre y se verifique para detectar actividad inusual. Los equipos azules realizan comprobaciones periódicas en el sistema, como auditorías de DNS, escaneo de vulnerabilidades de redes internas o externas y captura de tráfico de red de muestra para su análisis.

FUNCIONES DEL BLUE TEAM

- Los Blue Team realizan una **vigilancia constante, analizando patrones y comportamientos** que se salen de lo común tanto a nivel de sistemas y aplicaciones como de las personas, en lo relativo a la seguridad de la información.
- **Trabajan en la mejora continua de la seguridad**, rastreando incidentes de ciberseguridad, analizando los sistemas y aplicaciones para identificar fallos y/o vulnerabilidades y verificando la efectividad de las medidas de seguridad de la organización.

¿CÓMO TRABAJAN JUNTOS EL RED Y BLUE TEAM?

La comunicación entre los dos equipos es el factor más importante para la realización de ejercicios exitosos y para la **mejora constante del sistema.**

El Blue Team debe mantenerse actualizado sobre las nuevas tecnologías para mejorar la seguridad y debe compartir toda la información con el equipo rojo para poder realizar ataques prueba. Asimismo, el equipo rojo siempre debe estar al tanto de las nuevas amenazas y técnicas de penetración utilizadas por los piratas informáticos y asesorar al equipo azul sobre las técnicas de prevención.

El Red y Blue Team están en constante formación y actualización para estar preparados para cualquier circunstancia

Dependiendo del objetivo de su prueba, el Red team informará o no al Blue team de una prueba planificada. Por ejemplo, si el objetivo del ataque es simular un escenario de respuesta real a una amenaza, no querrá decirle al Blue team sobre la prueba. Únicamente alguien en la gerencia debe estar informado sobre la prueba para un análisis posterior, suele ser un líder del Blue team.

Cuando se completa la prueba, ambos equipos recopilan información e informan sobre sus resultados. **El Red team avisa al Blue team si logran penetrar las defensas y brinda consejos** sobre cómo bloquear intentos similares a un escenario real. Del mismo modo, **el Blue team informa al equipo rojo si sus procedimientos de monitoreo detectaron o no un intento de ataque**.
Finalmente, ambos equipos deben trabajar juntos para planificar, desarrollar e implementar controles de seguridad más estrictos según sea necesario.

Purple Team

El purple team existe para analizar y maximizar la efectividad del Red y Blue team.

Este team se encarga de enfrentar las técnicas de defensa del Blue team contra las técnicas de ataque del Red team. Con este enfrentamiento se logra crear más posibles casos de fallo o ataque y ver si el sistema está funcionando o está preparado de manera correcta. Si la defensa en el enfrentamiento es positiva se integran los nuevos baremos o actualizaciones pertinentes.

El Purple Team coordina y garantiza la comunicación entre en Red y Blue Team

La idea del purple team es **coordinar y garantizar que los dos equipos compartan información sobre las vulnerabilidades del sistema** para lograr una mejora constante. El purple team más que un equipo es un coordinador del blue y red team.

El Purple Team coordina el Red y Blue team para garantizar su correcto funcionamiento y evolución

FUNCIONES DEL BLUE TEAM

El principal objetivo del Purple Team es **gestionar la seguridad de la organización**, realizar pruebas para comprobar la eficacia de los mecanismos y procedimientos de seguridad y definir/desarrollar controles de seguridad adicionales para disminuir el riesgo de la organización.

¿QUÉ VENTAJAS TIENE LA EXISTENCIA DE ESTOS TEAMS?

- **Fortalecen todo tu sistema**. Con la prueba y creación de seguridad del blue team tu sistema se irá fortaleciendo y creando nuevas medidas de seguridad más efectivas.
- **Creación de plan de actuación**. Con las acciones del Purple Team podrás crear distintos planes de actuación para lograr prever posibles ataques u otros problemas informáticos encontrados por los ataques del red team.
- **Tranquilidad.** Con los ataques y defensas del Blue y Red team, aunque siempre se puede mejorar, sabrás que tu sistema está protegido.

Aunque los distintos equipos ayuden a crear una buena defensa ante posibles ataques, no hay que olvidar que los ciberatacantes están en continua formación y evolución para encontrar una mínima brecha para acceder. Es por eso que es vital estar analizando de manera continuada todos los sistemas de seguridad, más hoy en día donde los ciberataques a empresas no paran de aumentar.

“Los ciberataques en España han crecido un 125% en el último año hasta los 40.000 diarios”

CyberSecurity News - 2021

Este aumento de ciberataques es causado por la rápida implantación al mundo digital de muchas empresas que se han visto forzadas a realizar el cambio a causa de la pandemia. También se ha causado por la incorporación del teletrabajo, ya que muchas empresas no estaban preparadas para este cambio. Es por eso que la implementación de la ciberseguridad es tan importante y vital para las empresas.

Tranxfer es la plataforma B2B para la gestión integral del envío y recepción de documentación con trazabilidad y de manera segura

¡OFRECE TRANXFER!

Con TRANXFER podrás proteger a tu organización de forma fácil

- Enviar **archivos y recibir archivos sin límite de peso, y de forma segura.**
- La herramienta ofrece **trazabilidad y auditoría continua**; monitoring, acuse de recepción, lecturas y/o descargas.
- Políticas avanzadas de seguridad y una interfaz de usuario y administrador de fácil uso, en versión **web o plugin O365.**
- Disponemos de **API y Plugins** para integrar en otros sistemas
- Podemos integrarnos con el **SIEM**, **Active Directory** y ofrecemos distintas modalidades de despliegue

Fugas de información | Incumplimiento de GDPR| Entrada de malware

¿QUIERES UN FREE TRIAL? - Contáctanos para mas info

La herramienta preferida de los CISOs para luchar contra el **shadow IT** y reforzar su plan de director de seguridad para el intercambio de archivos

- Envía y recibe archivos de forma segura
- Elige tus preferencias de envío y visualización
- Previene la entrada y salida de Malware
- Controla la fuga de información
- Encriptacion end to end

GDPR COMPLIANT

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría MEDIA

Más de 1 millón de usuarios licenciados

Más de 5 millones de receptores

Contáctanos para más información: info@tranxfer.com
O a través de nuestras redes sociales:

https://www.linkedin.com/company/tranxfer

https://twitter.com/tranxfer

www.tranxfer.com