

RED & BLUE TEAM

CIBERSEGURIDAD EXPLICADA



@saulruizplaza

66

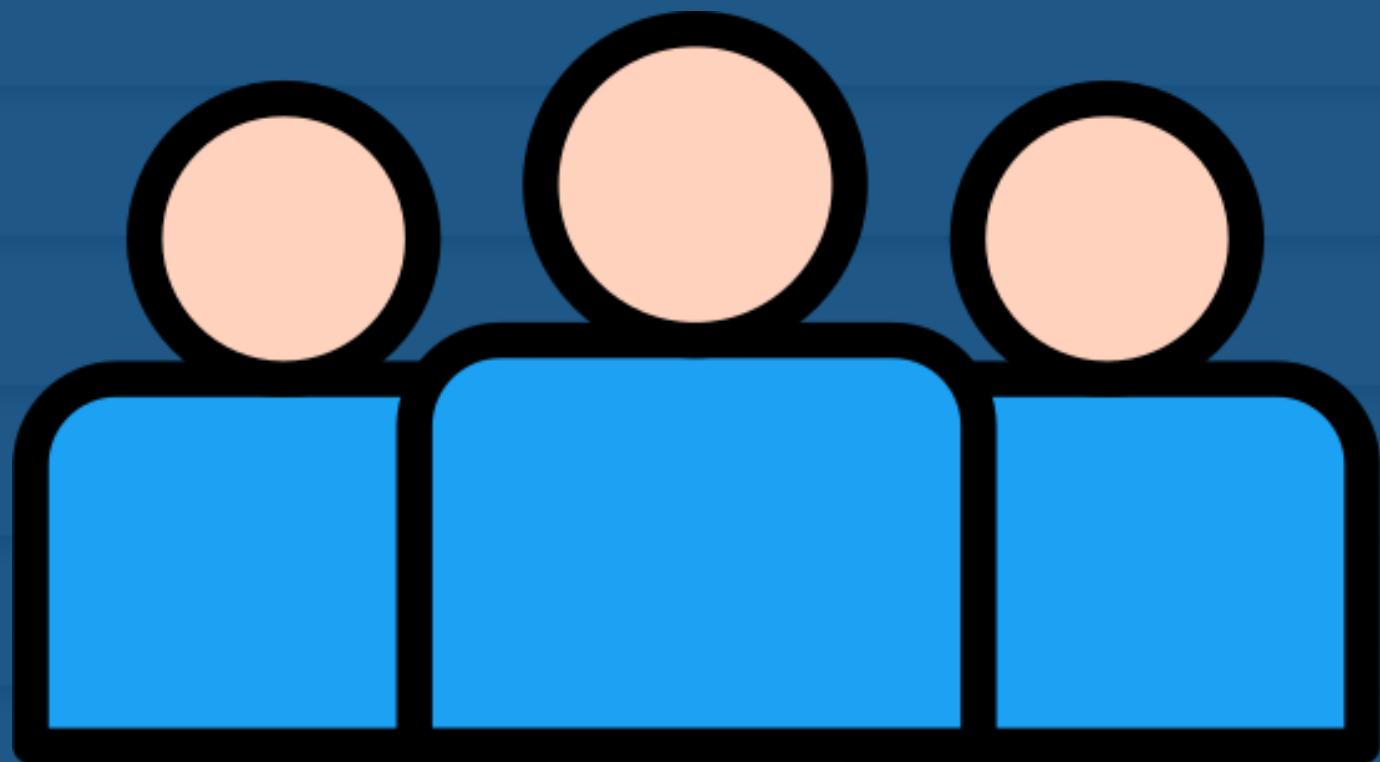
La ciberseguridad resulta esencial para proteger los datos y las infraestructuras digitales. Red Team Blue Team son dos elementos fundamentales en toda estrategia de ciberseguridad.

Los dos equipos desempeñan funciones complementarias en la seguridad, lo que posibilita a las organizaciones perfeccionar de manera constante su protección frente a potenciales amenazas ciberneticas.



@saulruizplaza

BLUE TEAM



¿Qué es Blue Team?

1



El Equipo Azul tiene la tarea de proteger las infraestructuras y sistemas de una entidad frente a ataques informáticos. Su responsabilidad primordial es **identificar, reaccionar y atenuar los incidentes de seguridad.**

Analizan, responden y gestionan los incidentes de seguridad para minimizar los daños.

Conoce Herramientas

2

SIEM (Security Information and Event Management):

Instrumentos como Splunk o Elastic Stack facilitan la recopilación y estudio de logs de seguridad con el fin de identificar incidentes en vivo.

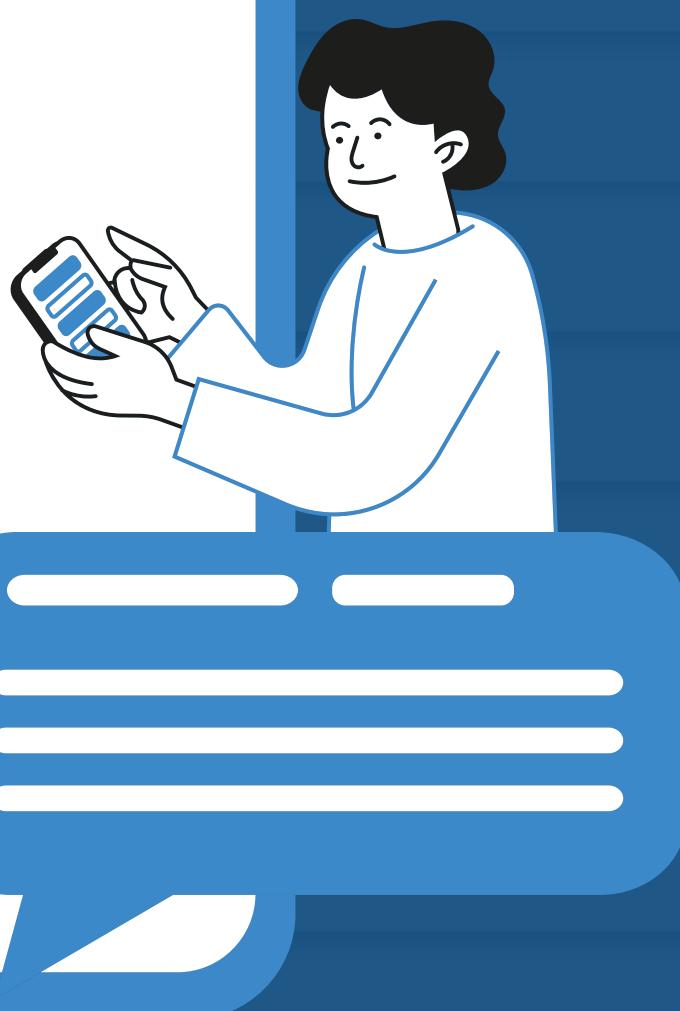
Firewalls:

Instrumentos como pfSense y Cisco ASA para regular el flujo de datos en la red y impedir accesos no permitidos.



Conoce Herramientas

2.2



Sistemas de Detección de Intrusiones (IDS):

Instrumentos como Snort o Suricata que supervisan el tráfico en la red para identificar patrones malintencionados.

IPS (Intrusion Prevention Systems o Sistemas de Prevención de Intrusiones)

Ayudan a detectar y prevenir ataques de seguridad en tiempo real. Aquí te detallo cómo funcionan y cómo son útiles

Sistemas Operativos

3

Windows Server

Utilizado para monitorizar y defender entornos corporativos

Uso

Gestión de usuarios, control de acceso, administración de redes y servicios como Active Directory, DNS, y DHCP



Security Onion

Distribución basada en Linux que incorpora herramientas para cómo análisis forense y seguimiento de seguridad.

Uso

Análisis de tráfico de red, detectar intrusiones y responder a incidentes.

Descubre Ramas

4

Analista de Seguridad

Se ocupa de supervisar, identificar y examinar sucesos de seguridad en la red para detectar potenciales amenazas.

SOC (Centro de Operaciones de Seguridad)

El SOC es el grupo responsable de administrar y armonizar las actividades de seguridad a escala organizativa.



Descubre Ramas

4.2

Respuesta ante Incidentes

Este colectivo se dedica a contener, eliminar y recuperarse de incidentes de seguridad con el menor efecto posible.

Gestión de Vulnerabilidades

Se centra en detectar, categorizar y solucionar vulnerabilidades en sistemas y aplicaciones.



Veamos Certificaciones

Principiante:

- **CompTIA Security+**: Certificación introductoria en seguridad informática, ideal para comenzar en el Blue Team.
- **GIAC Security Essentials (GSEC)**: Proporciona una base sólida en ciberseguridad para nuevos profesionales.



Veamos Certificaciones

Intermedio:

- **Certified Incident Handler (GCIH):** Se centra en la respuesta a incidentes y gestión de vulnerabilidades.
- **Certified Information Security Manager (CISM):** Aborda la gestión y liderazgo en seguridad de la información.



5.2

Veamos Certificaciones

Experto:

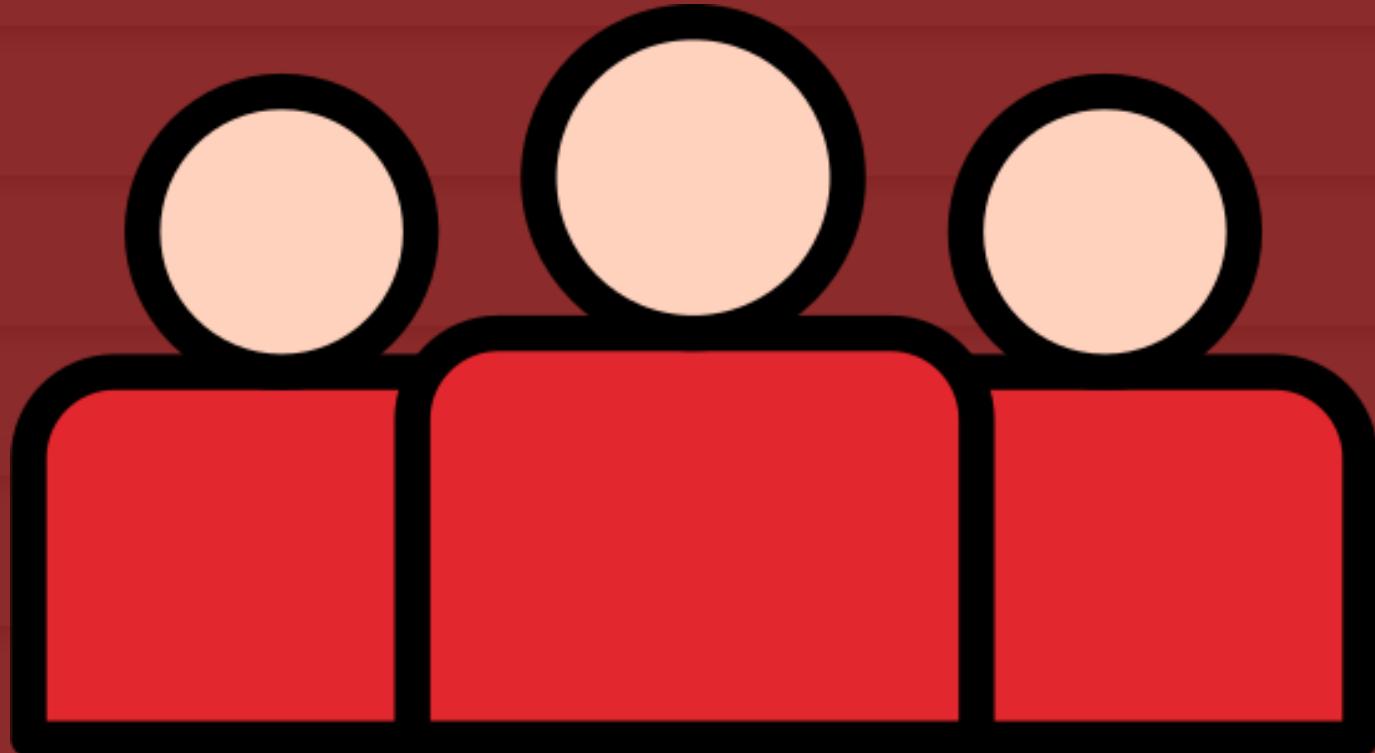
- **Certified Information Systems Security Professional (CISSP):** Certificación de alto nivel para profesionales de seguridad que lideran programas de seguridad de información.



5.3

@saulruizplaza

RED TEAM



¿Qué es Red Team?

1

El equipo rojo tiene la tarea recrear ataques reales con el objetivo de evaluar la seguridad de una entidad. Su meta es **detectar vulnerabilidades antes de que los ciberdelincuentes sean capaces de aprovecharlas.**



Detectan, simulan y aprovechan las vulnerabilidades de seguridad para valorar las defensas de la organización.

Conoce Herramientas

2

Metasploit Framework

Instrumento sofisticado para llevar a cabo pruebas de penetración que posibilita a los usuarios aprovechar las vulnerabilidades identificadas

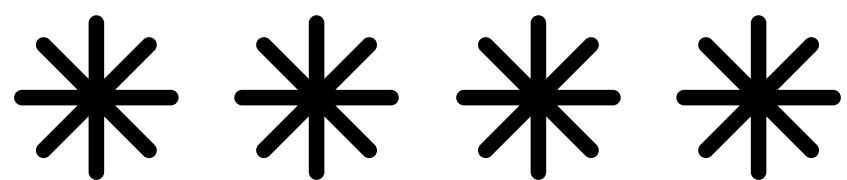


Nmap

Instrumento de escaneo de redes empleado para identificar aparatos en una red y identificar sus vulnerabilidades.

Conoce Herramientas

2.2



Burp Suite

Instrumento empleado para llevar a cabo pruebas de penetración en aplicaciones de internet, particularmente beneficioso para descubrir vulnerabilidades en el código web.

Jhon the Reaper

Un instrumento famoso para llevar a cabo ataques de cracking a contraseñas cifradas.

Sistemas Operativos

3

Kali Linux

distribución de Linux creada específicamente para ensayos de penetración, hacking ético y análisis digital forense.

Uso

Extensas variedad de herramientas preinstaladas



BackBox

Distribución de Linux basada en Ubuntu, centrada en pruebas de penetración y evaluación de la seguridad.

Uso

Auditorías de seguridad y ensayos de penetración, y incluye instrumentos para analizar vulnerabilidades y llevar a cabo ataques de prueba.

Descubre Ramas

4

Hacking Ético

Se ocupa de llevar a cabo ensayos de penetración con el fin de detectar vulnerabilidades en sistemas, aplicaciones y redes, con el permiso de la entidad objetivo.

Ingeniería Inversa

El procedimiento de desglosar y examinar programas con el fin de comprender su operación interna y detectar vulnerabilidades.



Descubre Ramas

4.2

Exploit Development

Se trata de crear y poner en marcha exploits para vulnerabilidades específicas de software o hardware, aprovechando fallos para conseguir acceso no permitido o incrementar privilegios.



Veamos Certificaciones

Principiante:

- **CompTIA Security+**: Cubre fundamentos esenciales de seguridad que son aplicables para el Red Team.
- **eJPT (eLearnSecurity Junior Penetration Tester)**: verifica destrezas en ensayos de penetración, centrándose en la detección y aprovechamiento de vulnerabilidades en sistemas.



5

Veamos Certificaciones

Intermedio:

- **Offensive Security Certified Professional (OSCP):** Certificación avanzada que requiere habilidades prácticas en hacking ético y pruebas de penetración.
- **Certified Ethical Hacker (CEH):** Introducción al hacking ético y conceptos básicos de Red Team.



5.2

Veamos Certificaciones

Experto

- **OSCE (Offensive Security Certified Expert):** Certificación sofisticada que verifica destrezas en métodos complejos de explotación de sistemas y ataques, enfocada en especialistas del Red Team.



5.3

66

Conclusión

La ciberseguridad va más allá de protegerse o atentar: implica cooperar, adquirir conocimientos y evolucionar. Es esencial tanto el Red Team como el Blue Team para construir un ecosistema digital seguro. Cada instrumento, certificación y empeño son esenciales para proteger lo que es importante.



MUCHAS GRACIAS



@saulruizplaza