¿Cuál es la diferencia entre Red Teaming y las pruebas de penetración?

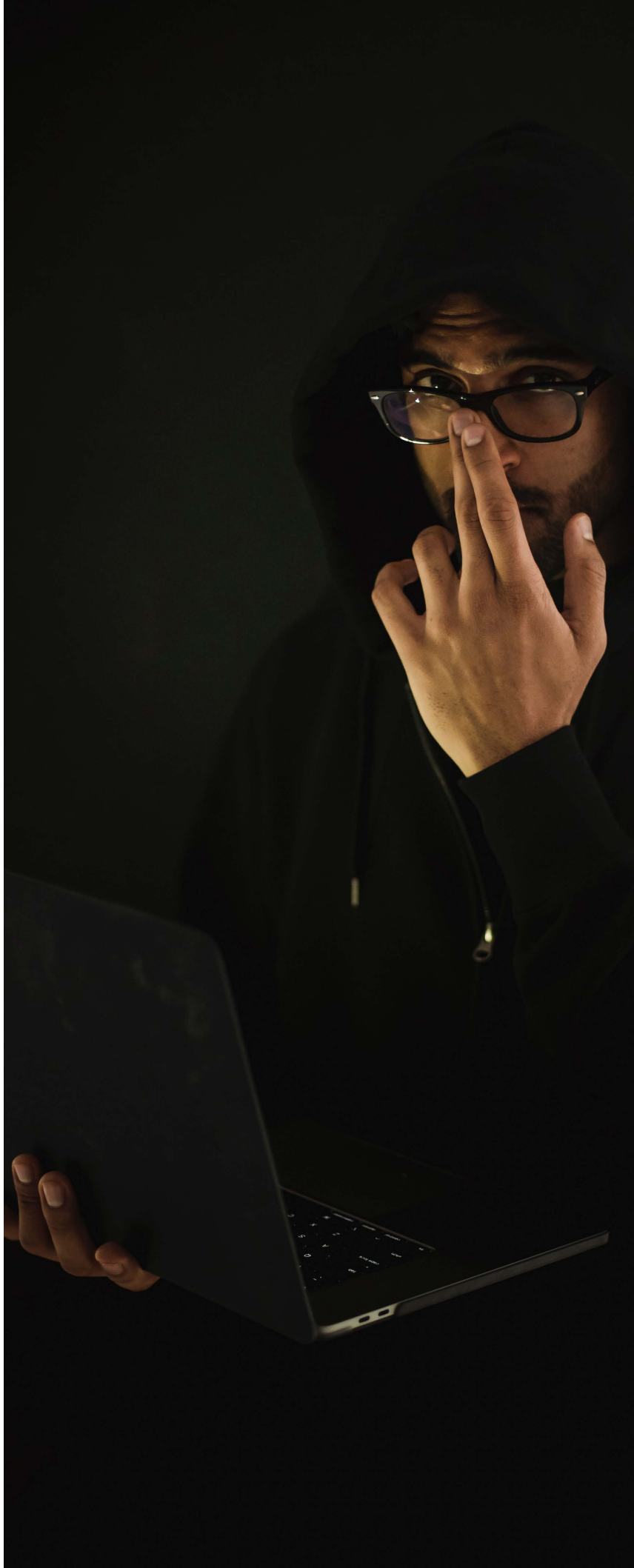
nexus aggity

A medida que las superficies de ataque continúan expandiéndose y los actores de amenazas realizan ataques cada vez más audaces e impactantes, las pruebas de Red Team preparan a las organizaciones para fortalecer las defensas de seguridad al resaltar el estado de preparación de la seguridad (o la falta de ella) y encontrar un camino a seguir para combatir las amenazas cibernéticas actuales y emergentes mientras se logra una reducción significativa del riesgo.

El Red Teaming emula una serie de adversarios avanzados y ataques del mundo real para poner a prueba defensas contra exploits electrónicos, físicos y sociales. Actuando de la forma más realista posible, los equipos rojos dan los mismos pasos que daría un adversario para lograr su objetivo, que a menudo no identifica todas las vulnerabilidades, sino que se centra en encadenar sólo las necesarias para explotar y alcanzar el objetivo general del ataque.

Las soluciones de seguridad ofensiva tienen muchas formas y tamaños, por lo que es importante que los programas de los equipos rojos se diferencien de otras soluciones de seguridad, sobre todo a la hora de comunicarse con las partes interesadas. En última instancia, esto sustenta la capacidad del equipo rojo para llevar a cabo operaciones con éxito, ya que las expectativas se ponen a la vista desde el principio.

En concreto, separar las pruebas de penetración del Red Teaming es clave para distinguir los programas de emulación de adversarios y el propósito que hay detrás de ellos.



Encontrar e informar sobre todas las vulnerabilidades bajo circunstancias controladas.	Objetivo 	Proporcionar una imagen holística y precisa de la capacidad de recuperación ante situaciones de infracción. Formar y ejercitar a los defensores. Identificar lagunas de seguridad y probar supuestos.
Cualquier/todas las vulnerabilidades y configuraciones erróneas dentro del entorno designado.	Identifica 	Vulnerabilidades relacionadas con objetivos del atacante. Puntos ciegos en preparación de seguridad y deficiencias de los controles de seguridad forenses.
Aplicación específica o aspecto de la superficie de ataque (aplicación web, aplicación móvil, SDK, etc.)	Alcance 	Amplia superficie de ataque, que incluye personas, lugares y tecnologías (red/web) y las costuras entre ellos.
¿Qué puntos vulnerables existen?	Pregunta 	¿Cómo nos desenvolveríamos frente a un escenario específico? ¿Cómo podría un adversario alcanzar un objetivo concreto?
• Por encargo • Parte del desarrollo interno de software, cumplimiento u otros procesos	Origen 	• Autodirigido, basado en el panorama de amenazas. • Vinculado a la inteligencia sobre ciberamenazas y al perfil estratégico del programa de amenazas internas (ITP). • A petición de la dirección y las líneas de negocio.

¿Cómo funciona el Red Teaming?

Red Teaming es una operación de emulación de ciberataque en la que se permite al equipo rojo aprovechar una variedad de métodos para capturar un “trofeo”. Este trofeo es identificado previamente por la organización que participa en un ejercicio de Red Teaming, y puede ser cualquier cosa que una organización considere de importancia, como información de identificación personal (PII) de clientes, acceso persistente a la red o credenciales de administrador.

Una vez determinado este trofeo por la organización objetivo, el equipo rojo trabaja desarrolla y lleva a cabo varios métodos de ataque que un adversario seguiría para capturar el trofeo. También es importante señalar que las organizaciones tienen la opción de solicitar el nivel de conocimiento que tiene el equipo rojo en el ejercicio. Puede ser uno de conocimiento cero (caja negra), o los consultores pueden tener cierto nivel de conocimiento preexistente de la arquitectura de redes y sistemas (caja gris).

> El Red Teaming es, con mucho, el método más eficaz y holístico de emular cómo un atacante podría poner en peligro una organización, y saca a la luz problemas que de otro modo no habría considerado.

Al definir los puntos en los que tiene más dificultades, la organización puede mejorar la detección y la respuesta, y disminuir el riesgo de que un atacante encuentre una vulnerabilidad conocida ya explotada en diversos ambientes.

En los últimos 30 años, los equipos rojos han pasado de ser una práctica militar esotérica a un servicio comercial generalizado. Los equipos rojos pueden ofrecer aún más valor a los clientes integrando no sólo los servicios de Red Teaming, sino también el análisis de riesgos y el modelado de amenazas en un programa global. Los tres son complementos naturales, y reunirlos puede ayudar a las organizaciones a comprender y gestionar más claramente sus riesgos de seguridad operativa en toda la superficie de ataque.

Fuente de información: cio.com.mx