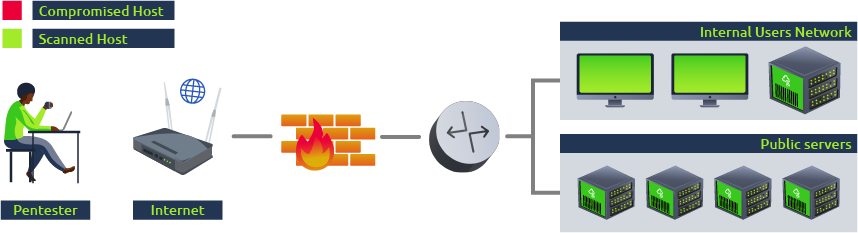
Evaluaciones de Vulnerabilidad

Esta es la forma más simple de evaluación de seguridad, y su objetivo principal es identificar tantas vulnerabilidades en tantos sistemas de la red como sea posible. Con este fin, se pueden hacer concesiones para cumplir este objetivo de manera efectiva. Por ejemplo, la máquina del atacante puede estar incluida en las soluciones de seguridad disponibles para evitar interferir con el proceso de descubrimiento de vulnerabilidades. Esto tiene sentido ya que el objetivo es mirar a cada host en la red y evaluar su postura de seguridad individualmente mientras proporciona la mayor información a la empresa sobre dónde enfocar sus esfuerzos de remediación.

Para resumir, a evaluación de vulnerabilidad se centra en escanear hosts en busca de vulnerabilidades como entidades individuales para que las deficiencias de seguridad puedan ser **identificado** y se pueden implementar medidas de seguridad efectivas para **proteger** la red de manera priorizada. La mayor parte del trabajo se puede realizar con herramientas automatizadas y realizadas por operadores sin requerir mucho conocimiento técnico.

Como ejemplo, si tuviera que ejecutar un evaluación de vulnerabilidad a través de una red, normalmente intentaría escanear tantos hosts como fuera posible, pero en realidad no intentaría explotar ninguna vulnerabilidad:



Pruebas de Penetración

Además de escanear cada host en busca de vulnerabilidades, a menudo necesitamos entender cómo afectan a nuestra red en su conjunto. Las pruebas de penetración se suman a las evaluaciones de vulnerabilidad al permitir que el pentester explore el impacto de un atacante en la red general al realizar pasos adicionales que incluyen:

* Intentar **explotar** las vulnerabilidades encontradas en cada sistema. Esto es importante ya que a veces puede existir una vulnerabilidad en un sistema, pero los controles compensatorios implementados impiden efectivamente su explotación. También nos permite probar si podemos usar las vulnerabilidades detectadas para comprometer un host determinado.
* Conducta **post-explotación** tareas en cualquier host comprometido, lo que nos permite encontrar si podemos extraer cualquier información útil de ellos o si podríamos usarlos para pivotar a otros hosts que no eran accesibles previamente desde donde nos encontramos.

Las pruebas de penetración pueden comenzar por buscar vulnerabilidades igual de regulares evaluación de vulnerabilidad pero proporcione más información sobre cómo un atacante puede encadenar vulnerabilidades para lograr objetivos específicos. Mientras que su enfoque permanece en **identificar** vulnerabilidades y establecimiento de medidas para **proteger** la red también considera la red como un ecosistema completo y cómo un atacante podría beneficiarse de las interacciones entre sus componentes.

Si tuviéramos que realizar una prueba de penetración utilizando la misma red de ejemplo que antes, además de escanear todos los hosts de la red en busca de vulnerabilidades, intentaríamos confirmar si pueden explotarse para mostrar el impacto que un atacante podría tener en la red:

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamente con confianza media

Al analizar cómo un atacante podría moverse por nuestra red, también obtenemos una visión básica sobre posibles omisiones de medidas de seguridad y nuestra capacidad para **detectar** un actor de amenaza real hasta cierto punto, limitado porque el alcance de una prueba de penetración suele ser extenso y a los probadores de penetración no les importa mucho ser ruidosos o generar muchas alertas en dispositivos de seguridad, ya que las limitaciones de tiempo en tales proyectos a menudo requieren que verifiquemos la red en poco tiempo.

Amenazas Persistentes Avanzadas y por qué el Pentesting Regular no es Suficiente

Si bien los compromisos de seguridad convencionales que hemos mencionado cubren el hallazgo de la mayoría de las vulnerabilidades técnicas, existen limitaciones en dichos procesos y en la medida en que pueden preparar efectivamente a una empresa contra un atacante real. Tales limitaciones incluyen:



Como consecuencia, algunos aspectos de las pruebas de penetración pueden diferir significativamente de un ataque real, como:

* **Las pruebas de penetración son RUIDOSAS:** Por lo general, los pentésteres no harán mucho esfuerzo para tratar de pasar desapercibidos. A diferencia de los atacantes reales, no les importa ser fáciles de detectar, ya que han sido contratados para encontrar tantas vulnerabilidades como puedan en tantos hosts como sea posible.
* **Los vectores de ataque no técnicos pueden pasarse por alto:** Ataques basados en ingeniería social o las intrusiones físicas generalmente no se incluyen en lo que se prueba.
* **Relajación de los mecanismos de seguridad:** Mientras se realiza una prueba de penetración regular, algunos mecanismos de seguridad pueden estar temporalmente desactivados o relajados para el equipo de pentesting a favor de la eficiencia. Aunque esto puede sonar contradictorio, es esencial recordar que los pentésteres tienen tiempo limitado para verificar la red. Por lo tanto, generalmente se desea no perder el tiempo buscando formas exóticas de evitar IDS/IPS, WAF, engaño de intrusión u otras medidas de seguridad, sino que se centran en la revisión de la infraestructura tecnológica crítica para las vulnerabilidades.

Por otro lado, los atacantes reales no seguirán un código ético y en su mayoría no tienen restricciones en sus acciones. Hoy en día, los actores de amenazas más destacados son conocidos como **Amenazas Persistentes Avanzadas (APTO)**, que son grupos de atacantes altamente calificados, generalmente patrocinados por naciones o grupos criminales organizados. Se dirigen principalmente a infraestructura crítica, organizaciones financieras e instituciones gubernamentales. Se llaman persistentes porque las operaciones de estos grupos pueden permanecer sin ser detectadas en redes comprometidas durante largos períodos.

Si una empresa se ve afectada por un APTO, ¿estaría preparado para responder eficazmente? ¿Podrían detectar los métodos utilizados para obtener y mantener el acceso en sus redes si el atacante ha estado allí durante varios meses? ¿Qué pasa si se obtuvo el acceso inicial porque John en la contabilidad abrió un archivo adjunto de correo electrónico sospechoso? ¿Qué pasa si se trata de un exploit de día cero? ¿Las pruebas de penetración anteriores nos preparan para esto?

Para proporcionar un enfoque más realista de la seguridad, nacieron los compromisos del equipo rojo.

Responda las preguntas a continuación

Las evaluaciones de vulnerabilidad nos prepararían para **detectar** ¿un verdadero atacante en nuestras redes? (Yay/Nay)

Principio del formulario

Respuesta Correcta

Final del formulario

Durante una prueba de penetración, ¿le preocupa ser detectado por el cliente? (Yay/Nay)

Principio del formulario

Respuesta Correcta

Final del formulario

Los grupos altamente organizados de atacantes expertos se conocen hoy en día como ...

Principio del formulario

Respuesta Correcta

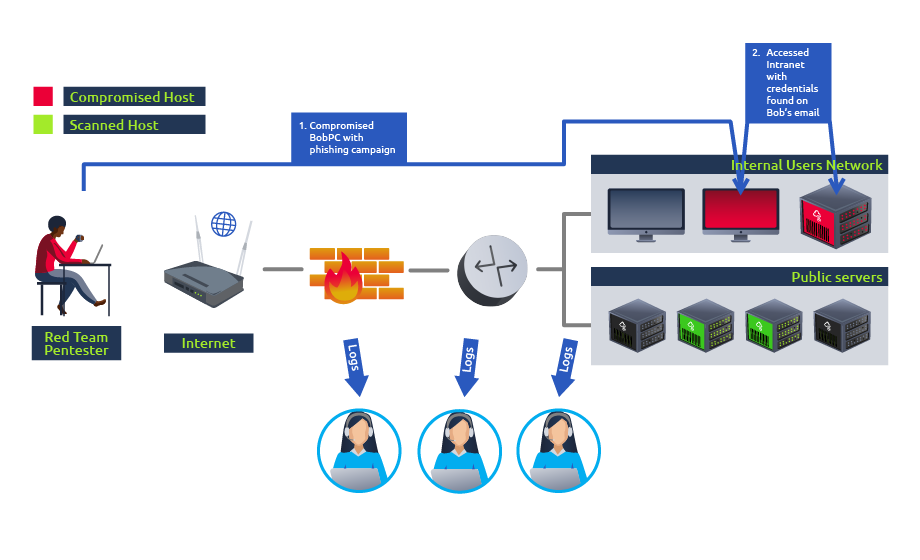
Final del formulario

Para mantenerse al día con las amenazas emergentes, los compromisos del equipo rojo fueron diseñados para cambiar el enfoque de las pruebas de penetración regulares a un proceso que nos permite ver claramente las capacidades de nuestro equipo defensivo en **detección** y **respondiendo** a un actor de amenaza real. No reemplazan las pruebas de penetración tradicionales, sino que las complementan centrándose en la detección y la respuesta en lugar de la prevención.

Equipo rojo es un término tomado del ejército. En ejercicios militares, un grupo tomaría el papel de un equipo rojo para simular técnicas de ataque para probar las capacidades de reacción de un equipo defensor, generalmente conocido como **equipo azul**, contra estrategias adversarias conocidas. Traducido al mundo de la ciberseguridad, los compromisos del equipo rojo consisten en emular a un actor de amenazas reales **Tácticas, Técnicas y Procedimientos (TTP)** para que podamos medir qué tan bien nuestro equipo azul responde a ellos y, en última instancia, mejora los controles de seguridad establecidos.

Cada compromiso del equipo rojo comenzará definiendo objetivos claros, a menudo referenciados como **joyas de la corona** o **banderas**, que van desde comprometer un host crítico dado hasta robar información confidencial del objetivo. Por lo general, el equipo azul no se le informará de tales ejercicios para evitar introducir sesgos en su análisis. El equipo rojo hará todo lo posible para lograr los objetivos sin ser detectado y evadiendo cualquier mecanismo de seguridad existente como firewalls, antivirus, etc EDR, IPS y otros. Observe cómo en un compromiso de equipo rojo, no todos los hosts en una red serán verificados en busca de vulnerabilidades. Un atacante real solo necesitaría encontrar un solo camino hacia su objetivo y no está interesado en realizar escaneos ruidosos que el equipo azul podría detectar.

Tomando la misma red que antes, en un compromiso de equipo rojo donde el objetivo es comprometer el servidor de intranet, planificaríamos una manera de alcanzar nuestro objetivo mientras interactuamos lo menos posible con otros hosts. Mientras tanto, el equipo azulse puede evaluar la capacidad de detectar y responder en consecuencia al ataque:



Es importante tener en cuenta que el objetivo final de tales ejercicios nunca debe ser que el equipo rojo "gane" el equipo azul, pero más bien simular suficientes TTP para el equipo azul aprender a reaccionar adecuadamente ante una amenaza real continua. Si es necesario, podrían modificar o agregar controles de seguridad que ayuden a mejorar sus capacidades de detección.

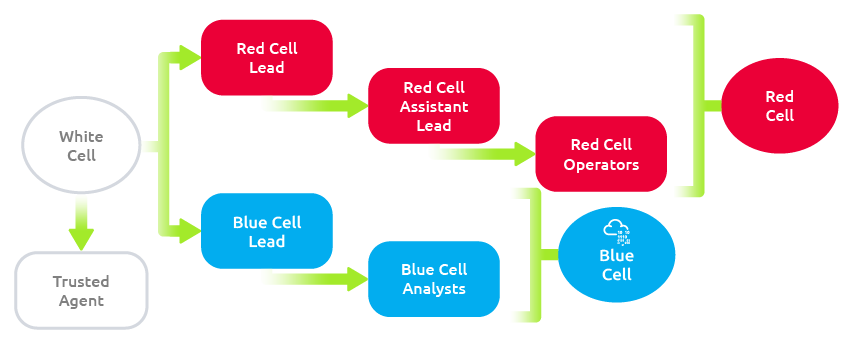
Los compromisos del equipo rojo también mejoran en las pruebas de penetración regulares al considerar varias superficies de ataque:

* **Infraestructura Técnica:** Al igual que en una prueba de penetración regular, un equipo rojo intentará descubrir vulnerabilidades técnicas, con un énfasis mucho mayor en el sigilo y la evasión.
* **Ingeniería Social:** Dirigirse a las personas a través de phishing campañas, llamadas telefónicas o redes sociales para engañarlos para que revelen información que debería ser privada.
* **Intrusión Física:** Uso de técnicas como la selección de cerraduras, la clonación RFID, la explotación de las debilidades en los dispositivos de control de acceso electrónico para acceder a áreas restringidas de las instalaciones.

Dependiendo de los recursos disponibles, el ejercicio del equipo rojo se puede ejecutar de varias maneras:

* **Compromiso Completo:** Simule el flujo de trabajo completo de un atacante, desde el compromiso inicial hasta los objetivos finales.
* **Supuesta Violación:** Comience asumiendo que el atacante ya ha ganado el control sobre algunos activos e intente alcanzar los objetivos a partir de ahí. Como ejemplo, el equipo rojo podría recibir acceso a las credenciales de algunos usuarios o incluso a una estación de trabajo en la red interna.
* **Ejercicio de mesa:**  Una simulación sobre la tabla donde se discuten escenarios entre los equipos rojo y azul para evaluar cómo responderían teóricamente a ciertas amenazas. Ideal para situaciones en las que hacer simulaciones en vivo puede ser complicado.
* Hay varios factores y personas involucradas dentro de un compromiso de equipo rojo. Todos tendrán su mentalidad y metodología para acercarse al personal de compromiso; sin embargo, cada compromiso se puede dividir en tres equipos o celdas. A continuación se muestra una breve tabla que ilustra cada uno de los equipos y una breve explicación de sus responsabilidades.

| **Equipo** | **Definición** |
| --- | --- |
| Celda Roja | Un glóbulo rojo es el componente que constituye la parte ofensiva de un equipo rojo que simula las respuestas estratégicas y tácticas de un objetivo dado. |
| Celda Azul | La celda azul es el lado opuesto del rojo. Incluye todos los componentes que defienden una red objetivo. La célula azul está compuesta típicamente por equipo azul miembros, defensores, personal interno y la gerencia de una organización. |
| Célula Blanca | Sirve como árbitro entre las actividades de glóbulos rojos y las respuestas de células azules durante un compromiso. Controla el entorno de compromiso/red. Monitorea la adherencia a la ROE. Coordina las actividades requeridas para lograr los objetivos de compromiso. Correlaciona las actividades de los glóbulos rojos con acciones defensivas. Asegura que el compromiso se lleve a cabo sin sesgos a ninguno de los lados. |

* Las definiciones provienen de [redteam.guía](https://redteam.guide/docs/definitions" \t "_blank).
* Estos equipos o celdas se pueden dividir aún más en una jerarquía de compromiso.
* 
* Como se trata de una sala roja orientada al equipo, nos centraremos en las responsabilidades de los glóbulos rojos. A continuación se muestra una tabla que describe los roles y responsabilidades de los miembros del equipo rojo.

| **Papel** | **Propósito** |
| --- | --- |
| Líder del Equipo Rojo | Planifica y organiza compromisos a un alto nivel—delegates, asistente de plomo y asignaciones de participación de operadores. |
| Líder Asistente del Equipo Rojo | Ayuda al equipo a liderar la supervisión de las operaciones de compromiso y los operadores. También puede ayudar a escribir planes de compromiso y documentación si es necesario. |
| Operador del Equipo Rojo | Ejecuta asignaciones delegadas por los líderes del equipo. Interprete y analice los planes de compromiso de los líderes del equipo. |

* Al igual que con la mayoría de las funciones del equipo rojo, cada equipo y compañía tendrán su propia estructura y roles para cada miembro del equipo. La tabla anterior solo actúa como un ejemplo de las responsabilidades típicas de cada rol.

Una función central del equipo rojo es la emulación del adversario. Si bien no es obligatorio, se usa comúnmente para evaluar lo que un adversario real haría en un entorno utilizando sus herramientas y metodologías. El equipo rojo puede usar varias cadenas de ciber-muerte para resumir y evaluar los pasos y procedimientos de un compromiso.

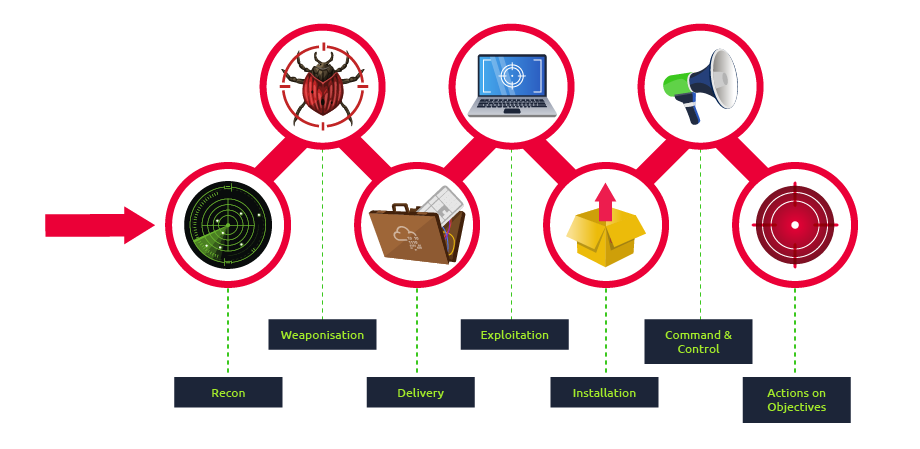
El equipo azul comúnmente utiliza cadenas de muerte cibernética para mapear comportamientos y romper un movimiento de adversarios. El equipo rojo puede adaptar esta idea para mapear los TTP adversarios (**T**actics, **T**echniques, y **P**rocedures) a los componentes de un compromiso.

Muchos organismos de regulación y estandarización han lanzado su cadena de muerte cibernética. Cada cadena de muerte sigue aproximadamente la misma estructura, y algunas profundizan más o definen objetivos de manera diferente. A continuación se muestra una pequeña lista de cadenas estándar de muerte cibernética.

* [Lockheed Martin Cyber Kill Chain](https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)
* [Cadena de Asesinato Unificada](https://unifiedkillchain.com/)
* [Cadena de Asesinatos Cibernéticos Varonis](https://www.varonis.com/blog/cyber-kill-chain/)
* [Ciclo de ataque de Active Directory](https://github.com/infosecn1nja/AD-Attack-Defense)
* [MITRA Marco ATT&CK](https://attack.mitre.org/)

En esta sala, comúnmente haremos referencia a la "Cadena de Asesinato Cibernético Lockheed Martin." Es una cadena de muerte más estandarizada que otras y se usa muy comúnmente entre los equipos rojos y azules.

La cadena de muerte de Lockheed Martin se centra en un perímetro o una brecha externa. A diferencia de otras cadenas de muerte, no proporciona una ruptura en profundidad del movimiento interno. Puedes pensar en esta cadena de muerte como un resumen de todos los comportamientos y operaciones presentes.



Los componentes de la cadena de eliminación se descomponen en la tabla a continuación.

| **Técnica** | **Propósito** | **Ejemplos** |
| --- | --- | --- |
| Reconocimiento | Obtener información sobre el objetivo | Recoger correos electrónicos, OSINT |
| Armatización | Combina el objetivo con un exploit. Comúnmente resulta en una carga útil entregable. | Explotar con puerta trasera, documento de oficina malicioso |
| Entrega | Cómo se entregará la función armada al objetivo | Correo electrónico, web, USB |
| Explotación | Explote el sistema del objetivo para ejecutar código | MS17-010, Zero-Logon, etc. |
| Instalación | Instalar malware u otras herramientas | Mimikatz, Rubeus, etc. |
| Comando y Control | Controle el activo comprometido desde un controlador central remoto | Imperio, Huelga de Cobalto, etc. |
| Acciones sobre Objetivos | Cualquier objetivo final: ransomware, exfiltración de datos, etc. | Conti, LockBit2.0, etc. |