Una guía de SANS

Equipos Rojo, Azul y Morado: Combinar las funciones de Seguridad para optimizar los resultados

Escrito por **Chris Dale**

Octubre de 2019

Patrocinado por:

Core Security

Introducción

Los términos «Equipo Rojo» y «Equipo Azul» se utilizan para hablar de dos equipos de Seguridad diferentes que trabajan enfrentados dentro de una organización. El objetivo de tener equipos adversarios es mejorar aún más la Seguridad de una organización. Sin embargo, este enfoque es imperfecto porque, por lo general, descuida errores fundamentales en la forma en que estos equipos cooperan entre sí. En lugar de colaborar estrechamente, suelen dejar pasar oportunidades que beneficiarían a ambos.

Cuando las organizaciones no son capaces de proteger todos los frentes, la ofensiva sigue logrando sus objetivos de invasión. Si el equipo ofensivo lo logra *siempre* con éxito, significa que no se ha maximizado el objetivo de su trabajo, que es ponérselo muy difícil a los atacantes reales. Lo mismo puede decirse de la defensa: si el equipo no comprende bien cómo trabajan los atacantes, tiene pocas probabilidades de crear una infraestructura resistente, que pueda obstaculizar y limitar a los atacantes hasta que puedan ser expulsados de las redes de forma segura.

La relación tradicional de adversarios no funciona; enfrentar al «Equipo Rojo» contra el «Equipo Azul» es cosa del pasado. Veremos cómo entrelazar las dos unidades para crear una relación simbiótica que permita obtener resultados mucho mejores para ambos equipos. Esto se conoce como el «equipo Morado» (consulte la figura 1).

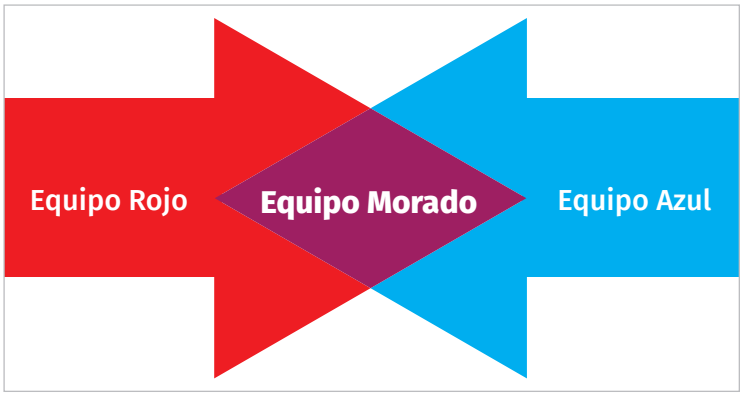

Figura 1. El Equipo Rojo y el Equipo Azul aúnan fuerzas

Además, la automatización desempeña un valioso papel en los entornos de Seguridad actuales, porque los resultados suelen ser mejores cuando los equipos Rojo y Azul logran más con menos. Por eso hay que esforzarse por lograr más mediante la automatización.

Equipo Rojo: En búsqueda del éxito

El Equipo Rojo se centra generalmente en irrumpir en la organización y demostrar el riesgo existente, con el fin de que la organización pueda mejorar su Seguridad. Si el equipo logra su objetivo, significa que el valor y la utilidad general del equipo está disminuyendo. Hay que tener en cuenta que el principal trabajo de un equipo de este tipo es hacer más difícil el trabajo de los pen testers, pero con mucha frecuencia estos se enorgullecen de irrumpir en las organizaciones por medios triviales.

Esto no significa que contar con un Equipo Rojo y hacer tests de penetración no sea una inversión necesaria. Los tests de penetración son controles y prácticas de Seguridad muy eficaces, como se señala en documento técnico de SANS «State of Application Security: Closing the Gap»;[1] sin embargo, los ataques actuales hacen necesario un nuevo enfoque para mejorar no solo el éxito del equipo atacante, sino también la defensa a largo plazo y, en resumen, la Seguridad general de la organización, que siempre ha sido el objetivo de los equipos.

Equipo Azul: Destinado al fracaso

La tarea del Equipo Azul es detectar a los adversarios e impedir que irrumpan en la infraestructura de la organización. Esta tarea es monumental: los límites de la infraestructura de IT de una organización a menudo no están definidos y cambian constantemente. Mantener actualizadas las aplicaciones resulta una labor demandante, y no hay que olvidar que siempre hay algún usuario que facilita, sin querer, la entrada de los atacantes en la organización. Otro aspecto a considerar: la organización se enfrenta a la amenaza cada vez mayor de los zero-day exploits, que un hacker puede usar para obtener acceso a la infraestructura. La IT invisible (Shadow IT), conocida también como «IT no autorizada», es una infraestructura no administrada por la organización que podría permitir a los atacantes entrar en su infraestructura.[2] El papel del Equipo Azul sería el de un portero en un partido de fútbol, con la diferencia de que el poste cambia constantemente y los atacantes utilizan todo tipo de balones para marcar goles.

Incluso con estos desafíos, la prevención da sus frutos. Cuanto más esfuerzos se dediquen a la prevención, más probabilidades hay de que los atacantes opten por rendirse e irse a objetivos más sencillos. Si se le dedica más esfuerzo a la detección de posibles riesgos, es probable que se pueda frustrar a los hackers antes de que logren sus objetivos. De esta forma, ellos pierden su tiempo y su dinero, y la organización queda protegida. En este escenario, todos ganan, aunque inicialmente existiera un riesgo.

---

[1] «State of Application Security: Closing the Gap», mayo de 2015, www.sans.org/reading-room/whitepapers/analyst/2015-state-application-security-closing-gap-35942, página 17, tabla 5.

[2] «Unsanctioned Business Unit IT Cloud Adoption Increases Risk of Data Breaches and Financial Liabilities», www.gartner.com/smarterwithgartner/dont-let-shadow-it-put-your-business-at-risk/

Equipo Morado: Unir esfuerzos genera una mayor rentabilidad de la inversión

En el panorama actual de la Seguridad, la relación de adversarios tradicional no funciona. Enfrentar al Equipo Rojo contra el Equipo Azul es cosa del pasado. Es mucho mejor combinar las dos unidades para crear un «Equipo Morado» que mejore la cooperación y permita lograr mejores resultados. A continuación daremos algunos consejos para mejorar la fusión de ambos equipos.

Qué puede aportar el Equipo Rojo al Equipo Morado

Como hemos dicho, la tarea del Equipo Rojo es complicarse más la vida. Por lo tanto, si puede entrar por medios sencillos, por ejemplo, con credenciales filtradas, vulnerabilidades y exposiciones comunes u otros medios de bajo coste, lo más probable es que el equipo pueda invertir en otros aspectos de la Seguridad en lugar de hacerlo en tests de penetración. Entonces, ¿cómo puede el Equipo Rojo seguir contribuyendo y no perder ingresos ni su razón de ser? Los siguientes enfoques muestran rápidamente las ventajas y permiten que los equipos empiecen a colaborar para poner las cosas más difíciles.

Empecemos por el alcance. Determinar el alcance de un test de penetración no es una tarea sencilla. El Equipo Azul no siempre conoce necesariamente su propio ámbito por completo, ni sabe cómo trabajan los atacantes. Como pen tester, también es difícil determinar el ámbito a testear solo con la información proporcionada por el objetivo, generalmente en reuniones sobre el tema. Esto está lejos de ser ideal, porque los procesos de reconocimiento, detección y análisis de un test de penetración suelen detectar nuevas superficies de ataque. Cambiar el alcance del test después de determinarlo suele dejar una sensación agridulce, porque podría acarrear más gastos u obligar a los pen testers a trabajar con un ámbito limitado, mientras que los adversarios reales no sufrirían esas limitaciones.

En su lugar, sugerimos un enfoque mucho más práctico, rentable y eficiente. El test de penetración se divide en dos entregas. En primer lugar se produce una fase de reconocimiento, detección y análisis del objetivo con un ámbito fácil de determinar. Esto tiene un coste mucho menor que el de un test de penetración completo y permite a los diferentes equipos generar confianza entre ellos. O, en el caso de los pen testers internos, esta interacción permite al equipo centrarse en realizar un trabajo minucioso en las fases de reconocimiento, análisis y detección, que los pen testers suelen considerar como las más valiosas. Además, resulta una experiencia más satisfactoria para los pen testers porque se tiene en cuenta el ámbito que han propuesto y no sienten que los tests se están haciendo en los objetivos equivocados. En la figura 2 se detallan las fases abstractas de un test de penetración y cómo puede dividirse en dos entregas, creando un escenario en el que todas las partes involucradas salen ganando.

Figura 2. Ciclos del test de penetración

El resultado de la fase de reconocimiento puede incluir resúmenes por colores de los activos que el Equipo Rojo considera que son más importantes y que deben incluirse en el ámbito, y puede abarcar todos los temas disponibles, lo que aumenta la superficie de ataque. Estos son:

- Servidores y aplicaciones clásicos, que son los aspectos típicos que se incluyen generalmente en un test de penetración tradicional.
- Aplicaciones y activos móviles que a menudo las organizaciones pasan por alto.
- Usuarios, preferiblemente una lista de quién está en cada unidad de Negocio; por ejemplo, gestión, operaciones de IT, desarrolladores, servicio de asistencia técnica y recepcionistas. Cada una de estas unidades tendrá su propia superficie de ataque (es decir, los altos cargos suelen ser objetivos de fraudes de ***phishing***, el departamento de IT es objeto de ataques OSINT, y el servicio de asistencia técnica y los recepcionistas podrían ser vulnerables a las solicitudes de restablecimiento de contraseñas a través de llamadas telefónicas).
- Datos filtrados, servidores mal configurados y otras vulnerabilidades detectadas sin explotación. Se trata de objetivos de ataques sencillos que se pueden solucionar antes de que el Equipo Rojo se enfrente a la infraestructura.

El equipo puede proponer un ámbito de testeo con un informe en el que se detalle la superficie identificable de ataque que el Equipo Rojo podría detectar. El Equipo Azul puede entonces introducir en el informe los activos no identificados, y ambos equipos pueden finalmente llegar a un acuerdo completo y transparente sobre un ámbito que contenga los activos más importantes. En muchos casos, el informe de reconocimiento por sí solo contendrá suficientes detalles que el Equipo Azul querrá abordar para que este proceso aporte valor.

Lo siguiente que puede hacer el Equipo Rojo es revisar cómo ampliar los reportes de los tests de penetración. Estos informes suelen incluir un resumen ejecutivo, una descripción general de los hallazgos y detalles sobre los distintos hallazgos. Cuando se generen informes para la colaboración del Equipo Morado, pueden incluir los reportes habituales ampliados, para que tengan mayor valor para el Equipo Azul.

Por ejemplo, el Equipo Rojo debería esforzarse por ofrecer múltiples sugerencias para solucionar las diferentes vulnerabilidades detectadas. Estas sugerencias pueden incluirse en el resumen ejecutivo para que los ejecutivos vean las diferentes maneras de eliminar y mitigar los riesgos. Además, gracias a los amplios conocimientos del Equipo Rojo en materia de evasión de la Seguridad, este equipo puede aportar más recomendaciones en el informe sobre cómo detectar y responder adecuadamente a las vulnerabilidades identificadas. Lo ideal sería que el informe se centrara no solo en solucionar las vulnerabilidades, sino también en aconsejar cómo puede el Equipo Azul corregir los procesos para gestionar dichas vulnerabilidades de forma más fiable y consistente en el futuro. En la figura 3 se muestra cómo se puede ampliar y desarrollar un informe tradicional para que aporte más valor al Equipo Azul.

Figura 3. Niveles de los informes del Equipo Rojo

Por último, el Equipo Rojo debe valorar las diferentes formas de presentar la información. Los editores de texto no son necesariamente el mejor formato, porque no facilitan la comunicación. Mientras el Equipo Azul se ocupa del cribado, parcheado y verificación, lo ideal es tener una forma de hacer el seguimiento de cada uno de los elementos en un sistema independiente. Además, el Equipo Rojo quiere seguir haciendo tests y evaluaciones de forma continua, y tener un portal exclusivo puede ayudarles a integrar al Equipo Azul y mantenerlos al día con notificaciones.

Qué puede aportar el Equipo Azul al Equipo Morado

La colaboración es la clave para formar un Equipo Morado eficiente. Invite a los pen testers a su plataforma de colaboración y comience la conversación:

- Mantenga un debate continuo y sencillo sobre el progreso de la interacción.
- Utilice la plataforma para dirigirse directamente a las personas sobre un tema, de modo que cada miembro del equipo pueda interactuar de forma rápida y eficaz sin tener que rebuscar correos electrónicos ni recordar llamadas telefónicas.
- Utilice Microsoft Teams, Slack y otras plataformas de comunicación para invitar a terceros a interactuar directamente con su equipo y viceversa.

Después, pida al Equipo Rojo que intente desglosar los fragmentos individuales de código, como las bibliotecas o el código de saneamiento que se usa en todas las aplicaciones de la organización. En lugar de hacer que el Equipo Rojo lleve a cabo un test a gran escala en la primera ronda de la interacción, deje que se centre en el código que crea que debe protegerse y reforzarse. Además, el Equipo Azul puede centrar sus esfuerzos en asegurarse de que su software cumpla los requisitos de las bibliotecas en todas las aplicaciones. El Equipo Rojo también puede encargarse de que los IDEs (entornos de desarrollo integrado) informen sobre la lógica de programación insegura que use datos introducidos por los usuarios o que genere datos sin las bibliotecas de saneamiento adecuadas.

La mayoría de los Equipos Azules ya realizan análisis de vulnerabilidades; los Equipos Rojos, sin embargo, suelen irrumpir con medios sencillos. Es buena idea dejar que el Equipo Rojo ejecute un análisis preliminar de las vulnerabilidades y elabore un resumen de este informe, o proporcionar al Equipo Rojo un análisis existente y pedirles su opinión antes de llevar a cabo otras actividades de test de penetración. Con frecuencia, veremos que esas interacciones tempranas proporcionan tests de penetración de mayor valor y permiten al Equipo Azul entender mejor sus debilidades antes de confirmar la realización de un test.

Del mismo modo, antes de confirmar el ámbito y alcance del testeo, se recomienda considerar la posibilidad de facilitar al Equipo Rojo unas credenciales para activos de alto riesgo que podrían tener graves consecuencias en caso de verse comprometidos. A menudo, las aplicaciones presentarán más vulnerabilidades después de la autenticación. Este ejercicio es especialmente valioso si la aplicación es de alto riesgo, ya que permitiría identificar las posibles amenazas antes de que las credenciales de un usuario se vean comprometidas. Habilitar la autenticación multifactor en la aplicación reduce el riesgo y se podría considerar la posibilidad de limitar el ámbito de los tests a la superficie de contacto y otros activos externos. En la figura 4 se ilustra la naturaleza integral de la comunicación y la colaboración en el Equipo Morado.

Figura 4. Comunicación y colaboración en el Equipo Morado

Automatización: Un enfoque necesario para todos los equipos

Si algo nos ha enseñado DevOps, es que la automatización es clave para combatir con éxito las amenazas. El Equipo Rojo puede realizar simulaciones de violaciones de perímetros de Seguridad para mejorar sus tests de penetración, ya que así se les permite centrarse en los aspectos importantes de los tests, en lugar de centrarse en las tareas más tediosas y repetitivas. Del mismo modo, el Equipo Azul puede aprovechar medidas similares para centrarse en las tácticas, las técnicas y los procedimientos de detección (TTPs) utilizados por el Equipo Eojo. JPCert tiene una visión general de los logs creados por Windows al ejecutar las herramientas que más probablemente utilizarán los intrusos en la red,[3] y Thailand Cert comparte información de las diferentes amenazas y las herramientas que usan.[4] El Equipo Azul debe anticiparse y asegurarse de que sus redes sean capaces de prevenir y detectar la ejecución de los TTPs del Equipo Rojo, y esto puede hacerse mediante automatización. El Equipo Azul también deberá considerar la posibilidad de invertir en medidas para bloquear y aislar automáticamente las presuntas amenazas en la red. En lugar de simplemente desconectar un host de la red, pueden incluir el host en una VLAN privada mientras el Equipo Azul realiza el cribado. El equipo también puede capturar y reproducir los ataques en distintos entornos para asegurarse de que toda la organización cumple las normas.

Atención con la automatización

Al implementar la automatización, proceda con cuidado. Considere cómo se registra el proceso de automatización en los dispositivos, por ejemplo, para el análisis automático de un host en riesgo. Hay que tener cuidado también de no compartir sin querer más información con los atacantes, como las credenciales, porque esto les daría más control sobre el entorno. Por ejemplo, se podría decidir que una operación de análisis de las vulnerabilidades use las credenciales de administrador de dominio para analizar un host controlado por el atacante. En este caso, las credenciales podrían ser detectadas y descifradas o podrían transmitirse los códigos hash.

Integración efectiva entre los equipos

En un ejemplo exitoso de interacción del Equipo Morado, el Equipo Azul utilizó una plataforma de colaboración para ofrecer al Equipo Rojo una sesión de pantalla compartida en uno de los sistemas potencialmente vulnerables. El Equipo Rojo concluyó que se trataba de un falso positivo en tan solo 10 minutos, en lugar de las horas que hubiera tardado normalmente. Además, el Equipo Azul detectó anomalías en la plataforma de pago de la organización, sin saber si fueron causadas por el Equipo Rojo o por otros. Con los registros y las conversaciones, los equipos pudieron descubrir juntos una vulnerabilidad relacionada con la disponibilidad de la plataforma. Se aplicaron los parches necesarios a la plataforma y se corrigió un problema que podría haber causado daños durante varios años.

Conclusiones

Para derrotar a los adversarios de forma más efectiva y mejorar la Seguridad general de nuestras organizaciones, los términos Azul y Rojo deben fusionarse bajo el concepto del Equipo Morado. Los equipos deben dejar de trabajar como simples adversarios y deben comenzar a colaborar y trabajar al unísono en el futuro. El potencial es tremendo y el listón de partida es muy bajo. La Seguridad de la Información ha llegado muy lejos, pero es esencial seguir desarrollando y buscando nuevas formas que nos permitan seguir defendiéndonos.

[3] «Tool Analysis Results Sheet», https://jpcertcc.github.io/ToolAnalysisResultSheet/

[4] «Threat Group Cards: A Threat Actor Encyclopedia», www.thaicert.or.th/downloads/files/A_Threat_Actor_Encyclopedia.pdf

Acerca del autor

Chris Dale

Chris Dale es instructor de SANS y enseña SANS SEC504: Hacker Tools, Techniques, Exploits, y Incident Handling. Como responsable de los grupos de tests de penetración y gestión de incidencias de Netsecurity, una empresa con sede en Noruega, Chris aporta una importante experiencia en materia de Seguridad y formación en desarrollo de sistemas, operaciones de TI y gestión de la Seguridad. Es un apasionado de la Seguridad y periódicamente imparte presentaciones, conferencias y talleres. Chris posee las certificaciones GCIH, GPEN, GSLC y GMOB, y participa en debates y en grupos de trabajo de las administraciones públicas para recomendar y mejorar la Seguridad en los sectores público y privado de Noruega.

Patrocinador

La SANS quiere agradecer al patrocinador de este documento:

FORTRA