Red Team Concepts

Transcribed on July 6, 2025 at 10:04 PM by Minutes AI

Speaker 1 (00:02)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a trabajar concepto de Red Team, ejercicio de Red Team, de Blue Team, que son conceptos interesantes a la hora de poder también medir la eficiencia no sólo de los controles de seguridad, las protecciones que podamos tener, como tenemos en el caso de un proyecto Kinetic, sino también nos permite medir la eficiencia de nuestros equipos de defensa, los procedimientos internos que tenemos, los sistemas de monitorización, detección y cómo trabajamos como equipo.

Para ello, en esta sesión vamos a ir definiendo los diferentes conceptos.

Vamos a comenzar hablando de lo que es el Red Team.

Un ejercicio de Red Team no va a buscar identificar el mayor número de vulnerabilidades, pero sí va a buscar en primer lugar se buscará lograr acceso a la organización, comprometer activos principales y conseguir persistencia, demostrando así cuál es el nivel de riesgo impacto que podría sufrir una organización si una amenaza, un adversario real se se llevará a cabo.

Entonces al final un ejercicio rectín lo que pretende medir es como un adversario, como una amenaza real puede impactar sobre tu organización logrando lo que una amenaza quiere lograr, que es conseguir acceso y conseguir persistencia.

Entonces en este ejercicio se va a intentar detectar o medir esa detección por parte del equipo de defensa.

El equipo de defensa tiene que tener los mecanismos adecuados para poder detectar esa esa intrusión, ese acceso a la organización y esa persistencia.

Si no somos capaces de detectar este ejercicio de Red Team, pues tendremos que mejorar no solamente en las medidas de protección que tengamos, sino también como equipo y con los procedimientos internos que tenemos implementados.

El ejercicio de Red Team es una emulación real, una anulación de una amenaza real y como veremos después tiene diferentes vectores por donde se pueden llevar a cabo las pruebas.

Podemos entender que actividades como un test de intrusión puede ser parte de un ejercicio Red Team, pero el Red team es algo mucho más global.

El red team como equipo es un equipo que simula un rol de adversario.

Generalmente las empresas contratan este servicio de red teaming, aunque también hay empresas que pueden tener su equipo de red team internamente para realizar a cabo este tipo de ejercicios.

Generalmente los ejercicios red team más puros, por definición, suelen llevar bastante tiempo, la preparación, el diseño, la planificación.

Hay una serie de fases bastante elaboradas, desde el diseño de cómo va a ser el ejercicio hasta la preparación, ese aprovisionamiento de herramientas, de técnicas, de conocimiento y esa planificación de cómo se va a llevar a cabo hasta que se lleve a cabo el ejercicio.

También estamos hablando de un transcurso de bastantes semanas o meses y el objetivo va a ser lograr la intrusión, comprometer los principales activos de organización, conseguir esa persistencia.

Como veis, lo que una amenaza real ocurriría o realizaría en una organización.

Las amenazas reales lo que buscan es lograr el acceso, conseguir información, conseguir persistencia para persistir el mayor tiempo posible, para poder sacar el máximo juego de ese ataque.

En un ejercicio rectín, un equipo de rectín va a seguir las mismas técnicas, tácticas y procedimientos que un atacante real.

Esto se llama TTPs, técnicas, tácticas y procedimientos.

Y esto hay una matriz de conocimiento de Mitre que se llama Attck, también se estudió en una sesión, en el cual nos intentan dar o reflejar en una matriz todo el conocimiento que se tiene sobre amenazas reales potentes que han existido y qué técnicas y prácticas utilizan esas amenazas.

El equipo de Red Team debe evitar ser detectado durante el desarrollo del ejercicio, eso sí es importante.

Bueno, aquí tenéis un libro donde podéis obtener más información sobre técnica de Red Team, el recting de la empresa, los equipos, etc.

Más información sobre este libro.

Llegamos a la parte de Blue Team.

El equipo de Blue Team es un equipo formado por personal interno, aunque también podemos tenerlo formado por personal externo, que hará lo que son las funciones de seguridad efectiva para los entornos, con las protecciones, controles de seguridad, salvaguardas adecuados, tener sistemas de monitorización, detección, intentar dar respuesta lo antes posible y sobre todo detectar la amenaza lo antes posible para poder aislarla y luego poder recuperarse de ella.

Tienen como obligación o su objetivo es defender los sistemas ante cualquier tipo de amenaza.

Cuando se realizan ejercicios rectil en una organización, lógicamente ellos no van a conocer las pruebas cuando se va a realizar, ni quién las va a realizar, es decir, ellos no pueden estar alerta, ellos no pueden estar conociendo que un ejercicio, recuerda que la gente estará en alerta, estará más a la defensiva, tiene que darse en un entorno lo más real, posiblemente real posible.

Es un día a día o un día cualquiera, enfrentarse a una situación que parece real, pero una emulación.

En este caso es el ejemplo.

Bueno, vamos a ver ahora de los vectores.

Hay un conjunto de acciones que permiten comprometer un primer sistema para una red y al final ese tipo de vector va a ser digital, físico u humano.

Es decir, en un ejercicio de rectín puro, siempre dependerá luego de lo que las empresas quieran contratar, pero en un ejercicio de rectín puro los vectores existen, tanto el digital, físico o lo humano.

Esto lo podemos traducir en cómo una empresa puede ser atacada.

Las empresas al final se enfrentan a diferentes amenazas, que no son solamente amenazas digitales, sino tenemos amenazas en un entorno físico, es decir, alguien podría ir a la oficina y alguien podría intentar acceder de forma no autorizada a los servidores o a los equipos o a la documentación que exista en oficina, podría ocurrir una visita a alguien que se cuele, por así decirlo.

Luego también tenemos el plano humano, el vector humano, que es muy asociado al engaño, a la ingeniería social, que sería pues aquí sería toda esta parte de intentar sacar información o intentar sacar algún tipo de credencial, información que pueda ser valioso para luego poder utilizarlo en los diferentes vectores.

Si os dais cuenta, el Red Team al final lo que hace es mezclar los diferentes vectores por los que una empresa puede ser atacado, de forma que preparando o planificando un ejercicio se pueda construir una amenaza a un adversario lo más real posible.

Aunque sepamos que es una emulación, lógicamente no se va a hacer nada de daño real a la organización, porque es la organización es la que está contratando este servicio, siempre dentro de un marco de hacking ético.

Como puntos clave también tenemos aquí cuál es el objetivo de un ejercicio de Red Team.

El objetivo es la emulación de un adversario, evaluar la capacidad de respuesta que tiene un equipo defensivo.

El alcance es un alcance completo, esto quiere decir que si lo comparamos por ejemplo con un test de intrusión, que ojo, es una herramienta que podemos utilizar dentro de un Red Team, podemos ver el pentest como una herramienta, pero el alcance de un ejercicio recién es completo, es decir, podemos utilizar vectores digitales, vectores físicos, vector humanos, siempre y cuando la empresa que contrata el ejercicio así lo permita, porque es realmente la emulación más real que se puede hacer.

Después el vector ataque puede combinarse, lo que se puede encontrar en el mundo físico o información que se puede obtener por el mundo físico humano se puede llevar al mundo digital, entonces la amenaza cobra más globalidad, una amenaza más real.

La duración, estamos hablando de planificación, estamos hablando de preparación, estamos hablando de diseño del ejercicio, estamos estamos hablando de aprovisionamiento de herramientas, estamos hablando de un montón de elementos.

Esto nos va a llevar de un orden de meses, semanas, meses, depende de nuevo lo que la empresa que contrata el servicio quiera hacer.

Y luego el conocimiento interno debe ser completamente desconocido, sobre todo por equipo de defensa y no solamente el personal de la empresa.

Las personas que contratan este servicio lógicamente tienen que tener responsabilidad de tu organización, pueden conocerlo.

Siempre va a haber un equipo que se llama White Team, por ejemplo, que ellos sí que van a poder conocer esto, lógicamente, e incluso ayudar al equipo de Red Team en algunas cosas para conocer algo más a la organización.

De forma que le estamos dando un poco de ayuda al equipo de Red Team, porque lo que nos interesa a nosotros como empresa es evaluar no solamente las protecciones de nuestros sistemas que tenemos implantados, sino también cómo somos capaces de responder y recuperarnos ante una amenaza que pueda ocurrir real.

Bien, en esta sesión, como conclusiones, hemos estudiado el concepto de Red Team, hemos definido lo que es el retin, lo que es un ejercicio de Red Team, sus objetivos, su alcance, su duración, los tipos de sectores en los cuales se trabajan y también hemos visto un poco el Blue Team como el elemento que vamos a evaluar.

Pero bueno, el Blue Team es mucho más que eso.

El blue team es un elemento fundamental en las empresas porque al final es el equipo de defensa, el equipo encargado de proteger las organizaciones y de tener sobre todo los sistemas de monitorización, detección y de respuesta lo más preparado posible para poder recuperarnos tanto de incidentes y de seguridad.

Bien, con esto finalizamos la sesión.

Nos vemos en la siguiente sesión.