Ciberejercicios Locked Shields

Sandra Bardón | Experta en ciberseguridad. Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN (NATO CCDCOE)

Tema

Locked Shields es el ejercicio de ciberdefensa *blue team-red team* más grande y complejo del mundo, organizado por el Centro de Excelencia de Ciberdefensa de la OTAN (*NATO Cooperative Cyber Defence Centre of Excellence*, CCDCOE), con base en Tallin, Estonia.

Resumen

Locked Shields es un ejercicio de ciberdefensa que se realiza anualmente desde 2010. A lo largo de los años, el escenario, los retos técnicos y estratégicos y su número de participantes han ido incrementándose exponencialmente hasta convertirse en el ejercicio de ciberdefensa en tiempo real más grande y complejo de los que se celebran en el mundo.

El público objetivo del ejercicio son los *blue teams* nacionales: especialistas en ciberdefensa que juegan el papel de equipos de respuesta rápida de una nación ficticia, Berylia, y que tendrán que defenderse de los continuos ataques de una supuesta nación adversaria, Crimsonia. La defensa activa es el principal objetivo del ejercicio, en el que los *blue teams* tienen que defenderse frente a posibles intrusiones y mantener operativas sus redes y servicios bajo una presión intensa y constante por los ataques recibidos de manera continuada. Esto incluye retos forenses y resolver y reportar incidentes, además de responder a los requisitos legales y estratégicos y atender a los medios de comunicación. En este sentido y con el fin de que el ejercicio sea lo más realista posible, Locked Shields se centra en tecnologías, redes y métodos de ataque completamente actualizados, acordes con la vanguardia y la evolución del mercado de las tecnologías.

Este ARI describe la organización, funcionamiento y utilidad de los ejercicios, especialmente del último año 2018.

Análisis

Locked Shields, como ciberejercicio principalmente técnico, ofrece una oportunidad única para experimentar, aprender y cooperar con naciones aliadas en el campo de las operaciones en ciberdefensa. De este modo, el ejercicio supone una gran oportunidad para todas las naciones que requieran adiestrarse en un entorno virtual y seguro, pero con retos reales y oponentes de todo el mundo.

El principal objetivo del ciberejercicio es poner a prueba la capacidad de los especialistas técnicos para prevenir, detectar, responder y reportar los continuos y

complejos ciberataques recibidos. Pero, además, Locked Shields también ofrece la oportunidad de entrenar a personas con puestos de responsabilidad en el sector de la ciberdefensa, en la toma de decisiones en momentos de ciberconflicto, con la ayuda de asesores legales.

Locked Shields siempre ha estado organizado por el CCDCOE, el Centro de Excelencia de Ciberdefensa, acreditado por la OTAN (Organización del Tratado del Atlántico Norte, en inglés *North Atlantic Treaty Organization* o NATO), cuyas tres líneas de trabajo son la investigación, la educación y los ejercicios. Se trata de una organización internacional militar con base en Estonia que ofrece una visión de 360 grados sobre la ciberdefensa dividida en cuatro áreas principales de especialización: tecnología, estrategia, operaciones y legal.

Además de organizar Locked Shields, el CCDCOE también organiza Crossed Swords, otro ciberejercicio cuyo público objetivo es el *red team*. Por otro lado, el centro ha desarrollado el *Tallinn Manual 2.0*, una guía muy útil para saber cómo aplica la ley internacional en sus ciberoperaciones. Otro de los grandes logros del centro es la Conferencia Internacional sobre Ciberconflicto (CyCon), en la que expertos en ciberdefensa de todo el mundo se reúnen en Tallin cada primavera. Este año se ha celebrado el décimo aniversario, "CyCon X: Maximising Effects", del 30 de mayo al 1 de junio de 2018.

El CCDCOE está formado y financiado por 21 países miembros, que hasta la fecha son Alemania, Austria, Bélgica, Eslovaquia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Italia, Letonia, Lituania, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Suecia, Turquía y Estados Unidos. Además, Australia, Japón y Noruega se unirán próximamente.

Los equipos que lo componen

Locked Shields está dividido en varios equipos para una correcta organización y división de roles: *blue team*, *green team*, *red team*, *white team* y *yellow team*.

Los *blue teams* son el público objetivo del ejercicio y están compuestos principalmente por especialistas en seguridad y tecnologías de la información. Como expertos en ciberdefensa, las tareas principales que deberán realizar en el contexto de Locked Shields son segurizar toda la infraestructura virtual de la cual son responsables, defender todos sus sistemas y redes de los ataques del *red team*, mantener los servicios asegurando la disponibilidad, confidencialidad e integridad, reportar los incidentes detectados al *white team*, resolver los retos forenses presentes también en el escenario y ejercitar la interacción entre elementos técnicos y estratégicos, así como obtener información sobre el proceso de toma de decisiones.

Además, los *blue teams* pueden decidir si formar un equipo puramente nacional o unirse a otras naciones y participar de manera conjunta. En cualquiera de los casos, la cooperación y coordinación son imprescindibles en ejercicios como Locked Shields, ya que la cantidad de personas involucradas y de información en tiempo real que se maneja es tan elevada que, si estos dos parámetros no se encuentran completamente alineados, será muy complicada una buena participación.

El *green team* es el responsable de preparar toda la infraestructura técnica de Locked Shields. Todos los sistemas y redes son simulados en el Cyber Range del CCDCOE, por lo que, aunque se trata de un escenario lo más realista posible, ofrece la seguridad de que todas las acciones del ejercicio se realizan en un entorno controlado. Esto permite un entrenamiento real, pero sin utilizar las redes y sistemas propios de las naciones participantes. Cabe destacar que, aunque todos los *blue teams* comparten la infraestructura principal, cada uno de ellos dispone de un escenario exactamente igual, pero independiente del resto de los *blue teams* participantes, de manera que se ofrecen entornos virtuales aislados para cada uno de ellos.

El *red team* es un equipo cuya misión principal consiste en reconocer, atacar, comprometer y degradar el funcionamiento de los sistemas de todos los *blue teams*. Los integrantes del *red team* son profesionales con amplios conocimientos y experiencia práctica en pruebas de penetración (*pentesting*) sobre aplicaciones web, redes, sistemas y *exploiting*. Todo el *red team* tiene que estar completamente actualizado en cuanto a técnicas y métodos, ya que cada año la complejidad de los sistemas y la destreza de los integrantes de los *blue teams* es mayor. Uno de los mayores retos para el *red team* es intentar actuar como si fuera uno solo para asegurar la equidad en las campañas de ataque contra todos los *blue teams*. En realidad, el *red team* es un gran equipo internacional dividido en varios subequipos a los que se asignan distintas competencias para poder completar todos los objetivos de adiestramiento previamente planificados.

El otro gran reto al que se enfrenta el *red team* es la continua adaptación y cambio de estrategia de las víctimas potenciales, puesto que cada *blue team* es distinto (personal asignado, nivel de instrucción y adiestramiento previo) y la planificación y ejecución defensiva de cada uno de los *blue teams* es completamente diferente. Por tanto, el *red team* debe ser capaz de cambiar de contexto rápidamente, así como evadir *firewalls* y antivirus, ofuscar código, inyectar *malware*, escalar privilegios en los sistemas y permanecer en los sistemas de las víctimas el mayor tiempo posible. La dirección del *red team* exige a los integrantes del equipo reportar el resultado de todos los ataques exitosos, por lo que deben aportar pruebas de su consecución. De ahí que resulte tan importante la exfiltración de información de todos los sistemas comprometidos. La capacidad de adaptación, imaginación, trabajo en equipo y coordinación resulta clave para que las campañas de ataque tengan efecto en el contexto de Locked Shields.

El *white team* es el responsable de controlar el ejercicio, para lo que establece un conjunto de reglas de juego, decide cómo y en qué fases el *red team* lleva a cabo las campañas de ataque, evalúa el progreso del ejercicio y asigna la puntuación con base en multitud de factores. Además, es el responsable de simular el comportamiento de usuarios normales en los sistemas virtualizados defendidos por los *blue teams*. Finalmente, asume el rol de los medios de comunicación interrogando al responsable de comunicación pública de cada *blue team* sobre los incidentes ocurridos y si se debería alertar a la población de las posibles consecuencias cibernéticas de los ataques recibidos. El *white team* dispone de la visión global de todo el ejercicio y su estado en todo momento, de tal manera que la toma de las decisiones que afectarán a todos los equipos en todos los niveles se pueda realizar con toda la información.

Por último, el *yellow team* es el responsable de proporcionar al resto de los equipos la conciencia situacional (*situational awareness*), tan importante en ejercicios de gran escala como Locked Shields, así como en la vida real.

El ejercicio se ejecuta parcialmente en remoto, es decir, los *blue teams* participan desde sus respectivas naciones conectándose a través de una VPN (Virtual Private Network) a la plataforma donde se ejecuta el escenario, mientras que los equipos *green team*, *red team*, *white team* y *yellow team* están presentes en la ejecución del Locked Shields en Tallin, Estonia.

Por otro lado, el sistema de puntuación está considerado una de las partes más importantes del ejercicio, ya que proporciona muchísima información en todos los aspectos. Además, es un sistema en el que los *blue teams* pueden comparar la eficacia de sus esfuerzos defensivos, lo cual permite una sana competitividad entre los diferentes *blue teams* participantes. Incluso el *red team* observa la puntuación para comprobar si los ataques han restado puntos a los *blue teams* atacados con éxito. Si bien una parte de la puntuación se contabiliza de manera automatizada, especialmente la relativa a la disponibilidad de los servicios al estar monitorizados de manera continua toda la infraestructura, redes, sistemas y servicios, otra parte de la puntuación se revisa manualmente basándose en lo reportado por el *red team*, además del análisis del *yellow team* y las decisiones del *white team* con base en las reglas definidas del ejercicio.

Paralelamente al ejercicio técnico, se realizan también ejercicios en los campos legal, estratégico y de análisis forense. Estos ejercicios están completamente vinculados al escenario principal y al progreso técnico de los *blue teams*. El objetivo de la parte estratégica en Locked Shields es practicar y evaluar la toma de decisiones por parte del personal directivo responsable ante una eventual situación de crisis. La toma de decisiones efectiva en el ámbito estratégico requiere la comprensión de los marcos nacionales, los procedimientos y las posibles interdependencias entre las naciones aliadas para poder adoptar la postura estratégica más adecuada y deseable para la nación afectada y sus aliados. Además, esta parte del ejercicio permite tomar conciencia de los resultados en la toma de decisiones estratégicas al poderse comprobar el impacto que se produciría en caso de crisis en materia de ciberdefensa. En cuanto a la parte legal, los expertos en la materia brindan asesoramiento legal en asuntos de ciberseguridad, incluyendo las operaciones y la gestión de riesgos legales relacionados principalmente con el derecho internacional general y la ley de responsabilidad estatal.

Locked Shields 18

La semana del 23 de abril de 2018 se celebró Locked Shields 18, en el que participaron casi 30 países divididos en 22 equipos, incluido un equipo propio de la OTAN. Este año el ejercicio ha destacado la creciente necesidad de mejorar la comunicación entre los expertos de diferentes áreas en el mundo de la ciberdefensa y los responsables de la toma de decisiones.

Esta edición ha sido la segunda en la que se ha integrado un ejercicio estratégico con un ejercicio técnico, lo que ha permitido a las distintas naciones participantes practicar toda la cadena de mando en caso de ocurrir un incidente grave, desde el plano táctico

al estratégico, con la participación además de capacidades tanto civiles como militares. Si bien el objetivo del ejercicio técnico es mantener la operatividad de los diferentes sistemas simulados bajo una intensa presión ofensiva, la ejecución de la parte estratégica sirve para comprender el posible impacto de las decisiones tomadas.

El escenario se desarrolla en una nación ficticia llamada Berylia que ha experimentado una degradación en la seguridad de sus sistemas y donde además una serie de acontecimientos hostiles coinciden con varios ciberataques coordinados contra un importante proveedor de servicios de internet y una base aérea militar. Cada *blue team* ha tenido su propia Berylia y ha sido responsable de defenderse de manera activa de los ataques sufridos por el *red team*, que simulaba las acciones ejecutadas por los agentes de la nación adversaria, Crimsonia. El *red team* atacó toda la infraestructura virtualizada de cada uno de los *blue teams* participantes, incluidas las infraestructuras críticas de Berylia.

Cabe destacar que este año el diseño del escenario asignado a cada *blue team* incluía una subestación de red eléctrica que fue objeto del ataque de los integrantes del *red team*, con lo que llegaron a interrumpir el suministro de corriente eléctrica a calles, hospitales y otros servicios críticos de Berylia. También se desarrolló, en exclusiva para el ejercicio, una red 4G que el *red team* tenía que atacar para intentar dejar temporalmente sin servicio los terminales móviles de los *blue teams*, de tal manera que en el mundo real ni siquiera podrían haber realizado llamadas de emergencia en caso de ocurrir algún incidente grave en Berylia.

En continuidad con otros años, los *blue teams* también tenían que segurizar y defender sus drones ante posibles ataques y toma de control por parte del *red team*. Y, como máxima novedad este año, Locked Shields 18 ha contado con *smart cities*, una para cada *blue team*, que simulaban la estación de purificación de aguas de Berylia, contra la que el *red team* se encargó de realizar ataques para conseguir llenar de químicos los tanques de agua y envenenar así a los ciudadanos de la nación. Gracias a todos estos sistemas de control industrial, el realismo y la complejidad del ejercicio resultaron muy próximos al mundo real, lo que ofreció una gran oportunidad a todas las naciones de adiestrarse con sistemas habituales dentro de una organización. Además, permitió adiestrarse con sistemas de infraestructuras críticas habitualmente presentes en ciudades occidentales o despliegues militares en zonas de operaciones, sistemas de vital importancia a la hora de garantizar la seguridad ya no solo de la información, sino también de las personas.

El ejercicio ha estado compuesto aproximadamente por 4.000 sistemas virtuales y se han realizado 2.500 ataques sobre ellos. Cada *blue team* tenía que mantener operativos los servicios de más de 150 sistemas complejos de tecnologías de la información (TI), además de informar sobre incidentes, tomar decisiones estratégicas y resolver desafíos relacionados con la comunicación externa, el campo legal y la atención a la prensa. El escenario de este año enfatizaba la creciente necesidad de mejorar el diálogo entre los expertos en el plano técnico y los responsables de la toma de decisiones, tanto civiles como militares.

En esta edición, el *blue team* que finalmente obtuvo más puntos fue el equipo que representaba a la OTAN, que por primera vez participaba con representantes de

diferentes agencias internas de la organización. Este equipo, de hecho, destacó por el elevado nivel demostrado en todas las categorías del ejercicio.

La dirección y ejecución del Locked Shields 18 la ha llevado a cabo el CCDCOE en cooperación con las Fuerzas Armadas de Estonia y de Finlandia, la Universidad de Defensa de Suecia, el Ejército de Gran Bretaña, el Mando Europeo de los Estados Unidos, el Instituto de Investigación de Seguridad Nacional de la República de Corea y la Universidad Técnica de Tallin. Además, diferentes empresas han colaborado tanto en el desarrollo como en la ejecución de Locked Shields 18: Siemens AG, Ericsson, Bittium, Goodmill, Threod Systems, Cyber Test Systems, Clarified Security, Iptron, Bytelife, BHC Laboratory, openvpn.net, GuardTime y otras muchas.

Hoja de ruta y conclusiones

Locked Shields es un ciberejercicio anual que ofrece una oportunidad única para que los expertos en ciberdefensa de distintos países practiquen la protección de los sistemas de TI y de las infraestructuras críticas en un escenario simulado bajo la presión intensa y constante de un gran ciberataque.

En realidad, una de las grandes presiones del ejercicio y que supone un gran hándicap para los participantes es la limitación temporal. Los equipos que llevan una correcta gestión del tiempo se encuentran en una posición de ventaja, ya que pueden establecer una estrategia adecuada y estar preparados ante posibles ataques futuros.

No obstante, al tratarse de un ejercicio en tiempo real, los cambios suceden continuamente, por lo que no debe descuidarse la capacidad de respuesta. Esto requiere, por parte de los *blue teams* participantes, de un análisis exhaustivo de la situación y la toma de decisiones adecuadas en tiempo y forma, además del establecimiento de una estrategia que seguir teniendo en cuenta todas las situaciones posibles. Es decir, deben ser capaces de controlar el ritmo y el tiempo y tener en cuenta que “el *red team* nunca para…”.

Cada año la parte correspondiente al ejercicio técnico es completamente nueva, por lo que los participantes de varias ediciones nunca se encuentran en ventaja con respecto a los equipos que se unen por primera vez a participar, de modo que ninguno de ellos conoce con antelación los sistemas que hay que defender. Además, cada año se busca que la complejidad técnica sea mayor y que el número de sistemas que defender también aumente, por lo que… ¿qué nos encontraremos en Locked Shields 19?

Personalmente, con la experiencia acumulada tras años de participación tanto en la ejecución como en la preparación de diferentes ejercicios a nivel nacional e internacional, he de decir que ninguno de ellos cubre tantos aspectos y de una manera tan compleja como Locked Shields. La preparación es dura, complicada, siempre intentando mejorar y complicar aún más el escenario con respecto a la edición anterior, pero lo mejor viene durante la ejecución.

Hay multitud de equipos que llevan meses preparándose para ese momento, nervios y ganas de empezar para ver qué sucede y cuál es su verdadero nivel… Eso es lo que se vive desde cada país, pero en Tallin, en realidad, los equipos lo vivimos de la misma manera. Son días de máximo estrés en los que intervienen multitud de especialistas. Para ofrecer una idea de la magnitud del personal implicado, este año más de 1.000 personas nos coordinamos para ejecutar el ciberejercicio con éxito.

No obstante, a la hora de la verdad, el *red team* tiene que cambiar continuamente de estrategia para adaptarse a los participantes y así volver a comprometer sistemas defendidos por los *blue teams* o continuar con la campaña de ataque. Mientras tanto, se recibe a representantes de multitud de medios de comunicación de diferentes países y personalidades a las que se muestra en tiempo real lo que está ocurriendo en el ejercicio. Locked Shields es una rueda que nunca para…

Y la sensación, una vez que todo ha terminado, es de una gran satisfacción, una sensación compartida por todos, incluidos los equipos participantes, que ven cómo el esfuerzo de varios meses se ve recompensado. Siempre se ha dicho que lo importante es participar, pero en Locked Shields es una realidad, ya que, independientemente de la posición en las puntuaciones finales, todos aprendemos algo nuevo. Algo nuevo que debemos aplicar sobre los sistemas reales; ese es el objetivo más importante del ejercicio. Ese incentivo es lo que lleva a que cada año más naciones quieran unirse y participar en Locked Shields.

Ya queda poco tiempo para comenzar a preparar la siguiente edición… ¿Qué tendremos entre manos para Locked Shields 19? Lo veremos en abril del año que viene.