TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 3 – UNIDAD 1

Universidad Tecnológica de Pereira

faceIT

Lección 3: Ejercicios de juego de guerra

Son eventos de prueba de seguridad en los que dos equipos se encargan de probar la seguridad y las directivas de un sistema. Para la táctica se usan dos equipos (rojo y azul, por ejemplo)

El equipo atacante (rojo) simula ataques reales para detectar brechas de seguridad. Si encuentran brechas, pueden demostrar el impacto de un ataque.

El equipo azul asume el rol del equipo de DevSecOps. Durante el ataque pueden demostrar la capacidad de respuesta y recuperación.

Progreso de una estrategia de juegos de guerra

Los juegos de guerra son eficaces para reforzar la seguridad porque motivan al equipo rojo a encontrar y poner a prueba problemas. Probablemente sea mucho más fácil de lo esperado al principio. Los equipos que no han intentado atacar activamente sus propios sistemas no suelen tener en cuenta el tamaño y la cantidad de brechas de seguridad a disposición de los atacantes. El equipo azul puede desmoralizarse al principio, ya que volverán a sufrir los ataques repetidas veces. Afortunadamente, el sistema y los procedimientos deben evolucionar con el tiempo de manera que el equipo azul pueda salir vencedor consecuentemente.

Preparación de los juegos de guerra

Antes de comenzar los juegos de guerra, el equipo debe ocuparse de cualquier problema que pueda encontrar a través de un pase de seguridad. Este es un gran ejercicio para realizar antes de intentar lanzar un ataque, ya que aportará una experiencia base para que todos los usuarios comparen con la situación después de detectar la primera vulnerabilidad más adelante. Empiece por identificar vulnerabilidades mediante una revisión manual del código y el uso de herramientas de análisis estático.

Organizar equipos

Los equipos rojos y azules deben organizarse por especialidad. El objetivo es crear los equipos más capaces en cada ámbito lado con el fin de ejecutar las operaciones lo más eficazmente posible.

El equipo rojo debe estar formado por algunos ingenieros orientados a la seguridad y desarrolladores que estén muy familiarizados con el código. También resulta útil integrar en el equipo a un especialista en pruebas de penetración.
El equipo azul debe estar formado por ingenieros de operaciones que conozcan muy bien los sistemas y registros disponibles. Estos tienen más posibilidades de detectar y neutralizar la actividad sospechosa.

Ejecución de los primeros juegos de guerra

Se debe esperar que el equipo rojo sea efectivo en los primeros juegos de guerra. Deben poder realizarse correctamente a través de ataques bastante simples, como encontrar secretos mal protegidos, inserción de código SQL y campañas de suplantación de identidad eficaces. Dedique mucho tiempo entre sesiones a aplicar correcciones y dejar comentarios sobre las directrices. Esto puede variar según la organización, pero no es recomendable empezar la siguiente sesión hasta que todos estén seguros de que la anterior se ha explotado todo lo posible y aconsejable.

Desarrollo de los juegos de guerra

Tras unas sesiones, el equipo rojo tendrá que confiar en técnicas más sofisticadas, como scripts de sitios (XSS), ataques de deserialización y vulnerabilidades del sistema de ingeniería. La incorporación de expertos externos en seguridad en áreas como Active Directory puede resultar útil para contrarrestar vulnerabilidades de seguridad poco conocidas. En este punto, el equipo azul no solo debe tener una plataforma protegida para defender, sino que también usará el registro completo y centralizado para los análisis forenses posteriores al ataque.

Si pasa mucho tiempo, el equipo rojo tardará mucho más en alcanzar los objetivos. Cuando lo hacen, a menudo se necesita la detección y encadenamiento de varias vulnerabilidades para tener un impacto limitado. A través del uso de herramientas de control en tiempo real, el equipo azul debe empezar a detectar posibles ataques en tiempo real.

DIRECTRICES

Los juegos de guerra no deberían ser una barra libre para todos. Es importante reconocer que el objetivo es generar un sistema más eficaz ejecutado por un equipo más eficaz.
Código de conducta

Este es un código de conducta de ejemplo que se practica en Microsoft:

1. Los equipos rojo y azul no harán ningún daño. Si la posibilidad de causar daños es significativa, debe documentarse y resolverse.
2. El equipo rojo no debe poner en peligro más de lo necesario para capturar los recursos de destino.
3. Las reglas del sentido común se aplican a los ataques físicos. Aunque se anima al equipo rojo a ser creativo con ataques no técnicos, como la ingeniería social, no deben imprimir credenciales falsas, hostigar a las personas, etc.
4. Si un ataque de ingeniería social tiene éxito, no revele el nombre de la persona que se ha visto involucrada. La lección se puede compartir sin alienar o avergonzar a un miembro del equipo con el que todos los usuarios necesitan seguir trabajando.

Reglas de juego

Estas son ejemplos de reglas del juego usadas por Microsoft:

1. No afectar a la disponibilidad de ningún sistema.
2. No acceder a datos externos del cliente.
3. No debilitar significativamente las medidas de seguridad en ningún servicio.
4. No realizar intencionadamente intervenciones destructivas contra ningún recurso.
5. Proteger credenciales, vulnerabilidades y otra información crítica obtenida.

Resultados

Los riesgos de seguridad o las experiencias aprendidas deben documentarse en un trabajo pendiente de elementos de reparación. Los equipos deben definir un acuerdo de nivel de servicio (SLA) para responder a los riesgos de seguridad rápidamente. Los riesgos graves deben subsanarse lo antes posible, mientras que los problemas menores pueden tener un plazo límite de dos sprints.

Se debe presentar un informe a toda la organización con las experiencias aprendidas y las vulnerabilidades detectadas. Es una oportunidad de aprendizaje para todos los usuarios, así que hay que aprovecharlo.

Experiencias aprendidas en Microsoft

Cada cierto tiempo, Microsoft poner en marcha juegos de guerra y ha sacado muchas conclusiones y experiencias durante todo este tiempo.

- Los juegos de guerra son una manera eficaz de cambiar la cultura de DevSecOps y tener como prioridad la seguridad.
- Los ataques de suplantación de identidad (phishing) son muy eficaces para los atacantes y no deben ser subestimados. El impacto se puede contener limitando el acceso a la fase de producción y mediante autenticación de dos factores.
- El control del sistema de ingeniería lleva a poder controlar todo. Asegúrese de controlar estrictamente el acceso al agente de compilación o versión, la cola, el grupo y la definición.
- Practique la defensa en profundidad para que los atacantes lo tengan más difícil. Cada barrera que tengan que sobrepasar los ralentiza y da otra oportunidad para atraparlos.
- Nunca cruce dominios de confianza. El equipo de producción nunca debe confiar en nada en la prueba.