Los compromisos pueden ser muy complejos y burocráticos. La clave para un compromiso exitoso son los objetivos o metas del cliente claramente definidos. Los objetivos del cliente deben discutirse entre el cliente y el equipo rojo para crear un entendimiento mutuo entre ambas partes de lo que se espera y se proporciona. Establecer objetivos es la base para el descansar de la documentación y planificación del compromiso.

Sin objetivos y expectativas claros y concretos, se está preparando para una campaña muy no estructurada y no planificada. Los objetivos establecen el tono para el descansar del compromiso.

Al evaluar los objetivos de un cliente y planificar los detalles del compromiso, a menudo deberá decidir qué tan enfocada está la evaluación.

Los compromisos se pueden clasificar entre una prueba de penetración interna/de red general o una emulación de adversario enfocada. Una emulación de adversario enfocada definirá un específico APTO o grupo para emular dentro de un compromiso. Esto generalmente se determinará en función de los grupos que se dirigen a las industrias particulares de la empresa, es decir, las instituciones financieras y [APT38](https://web.archive.org/web/20230325143301/https:/content.fireeye.com/apt/rpt-apt38). Una prueba de penetración interna o de red seguirá una estructura similar, pero a menudo estará menos enfocada y usará TTP más estándar.



Los detalles del enfoque dependerán de una base caso por caso del compromiso definido por los objetivos del cliente.

Los objetivos del cliente también afectarán las reglas generales de compromiso y alcance del compromiso.

Estos temas se ampliarán en la Tarea 6.

Los objetivos del cliente solo establecen una definición básica de los objetivos del compromiso del cliente. Los planes de compromiso específicos ampliarán los objetivos del cliente y determinarán los detalles del compromiso. Los planes de compromiso se cubrirán más adelante dentro de esta sala.

La siguiente piedra angular para un compromiso preciso y transparente es un alcance bien definido. El alcance de un compromiso variará según la organización y cómo se vean su infraestructura y postura. El alcance de un cliente generalmente definirá lo que usted *canno*t hacer o apuntar; también puede incluir lo que usted *puede* hacer o apuntar. Si bien los objetivos del cliente se pueden discutir y determinar junto con el equipo proveedor, el cliente solo debe establecer un alcance. En algunos casos, el equipo rojo puede discutir una queja del alcance si afecta un compromiso. Deben tener una comprensión clara de su red y las implicaciones de una evaluación. Los detalles del alcance y la redacción siempre se verán diferentes, a continuación se muestra un ejemplo de cómo puede verse la verborrea dentro del alcance de un cliente.

* Sin exfiltración de datos.
* Los servidores de producción están fuera de los límites.
* 10.0.3.8/18 está fuera de alcance.
* 10.0.0.8/20 está en alcance.
* El tiempo de inactividad del sistema no está permitido bajo ninguna circunstancia.
* Exfiltración de PII está prohibido.

Al analizar los objetivos o alcances de un cliente desde la perspectiva de un equipo rojo, es esencial comprender el significado y las implicaciones más profundos. Al analizar, siempre debe tener una comprensión dinámica de cómo su equipo abordaría los problemas/objetivos. Si es necesario, debe escribir sus planes de compromiso o comenzarlos solo con una lectura simple de los objetivos y el alcance del cliente.

Responda las preguntas a continuación

Lea los objetivos del cliente de ejemplo y responda las preguntas a continuación.

Principio del formulario

Completo

Final del formulario

A continuación se muestra un ejemplo de los objetivos del cliente de una organización madura con una fuerte postura de seguridad.

Ejemplo 1 - Empresas globales:

**Objetivos:**

1. Identifique las configuraciones erróneas del sistema y las debilidades de la red.
   1. Centrarse en los sistemas exteriores.
2. Determinar la efectividad de los sistemas de detección y respuesta de punto final.
3. Evaluar la postura y respuesta de seguridad general.
   1. SIEM y medidas de detección.
   2. Remediación.
   3. Segmentación de DMZ y servidores internos.
4. Se permite el uso de tarjetas blancas dependiendo del tiempo de inactividad y la duración.
5. Evaluar el impacto de la exposición y exfiltración de datos.

**Alcance:**

1. El tiempo de inactividad del sistema no está permitido bajo ninguna circunstancia.
   1. Cualquier forma de DDoS o DoS está prohibida.
   2. El uso de cualquier malware dañino está prohibido; esto incluye ransomware y otras variaciones.
2. La exfiltración de PII está prohibida. Usar datos de exfiltración arbitrarios.
3. Se permiten ataques contra sistemas dentro de 10.0.4.0/22.
4. Los ataques contra sistemas dentro del 10.0.12.0/22 están prohibidos.
5. Bean Enterprises supervisará de cerca las interacciones con la DMZ y los sistemas críticos/de producción.
   1. Cualquier interacción con "\*.bethechange.xyz" está prohibida.
   2. Se permite toda interacción con "\*.globalenterprises.thm".

Reglas de Compromiso (RoE) son un esquema legalmente vinculante de los objetivos y el alcance del cliente con más detalles de las expectativas de compromiso entre ambas partes. Este es el primer documento "oficial" en el proceso de planificación del compromiso y requiere la autorización adecuada entre el cliente y el equipo rojo. Este documento a menudo actúa como el contrato general entre las dos partes; un contrato externo u otras NDA (**N**en**D**isclosure **A**el acuerdo) también se puede utilizar.

El formato y la redacción de la RoE son críticos ya que es un contrato legalmente vinculante y establece expectativas claras.

Cada RoE la estructura será determinada por el cliente y el equipo rojo y puede variar en la longitud del contenido y las secciones generales. A continuación se muestra una breve tabla de secciones estándar que puede ver contenidas en el RoE.

|  |  |
| --- | --- |
| **Nombre de la Sección** | **Detalles de la Sección** |
| Resumen Ejecutivo | Resumen general de todos los contenidos y autorización dentro RoE documento |
| Propósito | Define por qué el RoE se utiliza el documento |
| Referencias | Cualquier referencia utilizada en todo el RoE documento (HIPAA, ISO, etc.) |
| Alcance | Declaración del acuerdo sobre restricciones y directrices |
| Definiciones | Definiciones de términos técnicos utilizados a lo largo de la RoE documento |
| Reglas de Acuerdo de Participación y Apoyo | Define las obligaciones de ambas partes y las expectativas técnicas generales de la conducta de compromiso |
| Disposiciones | Definir excepciones e información adicional de las Reglas de Compromiso |
| Requisitos, Restricciones y Autoridad | Defina las expectativas específicas del equipo rojo |
| Reglas de Tierra | Defina las limitaciones de las interacciones del equipo rojo |
| Resolución de Problemas/Puntos de Contacto | Contiene todo el personal esencial involucrado en un compromiso |
| Autorización | Declaración de autorización para el compromiso |
| Aprobación | Firmas de ambas partes que aprueban todas las subsecciones del documento anterior |
| Apéndice | Cualquier información adicional de las subsecciones anteriores |

Al analizar el documento, es importante recordar que es solo un resumen, y su propósito es ser un documento legal. Se requiere una planificación futura y más profunda para ampliar el RoE y objetivos del cliente.

Para esta tarea utilizaremos un documento abreviado adaptado de [redteam.guía](https://redteam.guide/docs/templates/roe_template/" \t "_blank)

Responda las preguntas a continuación

Descargue las reglas de compromiso de muestra de los archivos de tareas.

Una vez descargado, lea el documento de muestra y responda las preguntas a continuación.

PLANIFICACION DE CAMPAÑA  
Antes de esta tarea, nos hemos centrado principalmente en la planificación del compromiso y la documentación desde la perspectiva comercial. La planificación de campañas utiliza la información adquirida y planificada a partir de los objetivos del cliente y RoE y lo aplica a varios planes y documentos para identificar cómo y qué hará el equipo rojo.

Cada equipo rojo interno tendrá su metodología y documentación para la planificación de campañas. Mostraremos un conjunto profundo de planes que permite una comunicación precisa y una documentación detallada. El resumen de la campaña que utilizaremos consta de cuatro planes diferentes que varían en profundidad y la cobertura adaptada de los documentos de operaciones militares. Cada plan se puede encontrar en la tabla a continuación con una breve explicación.

|  |  |  |
| --- | --- | --- |
| **Tipo de Plan** | **Explicación del Plan** | **Contenido del Plan** |
| Plan de Compromiso | Una descripción general de los requisitos técnicos del equipo rojo. | CONOPS, Requisitos de Recursos y Personal, Líneas de Tiempo |
| Plan de Operaciones | Una expansión de la **Plan de Compromiso**. Va más allá en los detalles de cada detalle. | Operadores, Información Conocida, Responsabilidades, etc. |
| Plan de Misión | Los comandos exactos para ejecutar y el tiempo de ejecución del compromiso. | Comandos a ejecutar, Objetivos de Tiempo, Operador Responsable, etc. |
| Plan de Remediación | Define cómo procederá el compromiso después de que finalice la campaña. | Informe, consulta de remediación, etc. |

Otro ejemplo de un plan de campaña es el [redteam.guía](http://redteam.guide/) lista de verificación de compromiso. La lista de verificación, encontrada [aquí](https://redteam.guide/docs/checklists/red-team-checklist/), actúa como un enfoque más generalizado para la planificación de una campaña y la información necesaria.

En las próximas tareas, profundizaremos más en estos planes, documentación y detalles de cada uno a medida que profundizamos en la planificación de la campaña.

DOCUMENTACION DE COMPROMISO

La documentación de participación es una extensión de la planificación de campañas donde las ideas y pensamientos de la planificación de campañas están documentados oficialmente. En este contexto, el término "documento" puede ser engañoso ya que algunos planes no requieren la documentación adecuada y puede ser tan simple como un correo electrónico; esto se cubrirá más adelante en esta tarea.

En esta tarea, cubriremos una descripción técnica de los contenidos de cada plan de campaña antes de mirar los planes y documentos en las próximas tareas.

**Plan de Compromiso:**

|  |  |
| --- | --- |
| **Componente** | **Propósito** |
| CONOPS (**Con**cept de **Op**eration**s**) | Descripción general no técnicamente escrita de cómo el equipo rojo cumple con los objetivos del cliente y se dirige al cliente. |
| Plan de recursos | Incluye líneas de tiempo e información requerida para que el equipo rojo tenga éxito: cualquier requisito de recursos: personal, hardware, requisitos de nube. |

**Plan de Operaciones:**

|  |  |
| --- | --- |
| **Componente** | **Propósito** |
| Personal | Información sobre los requisitos de los empleados. |
| Condiciones de detención | Cómo y por qué debería detenerse el equipo rojo durante el compromiso. |
| RoE (opcional) | - |
| Requisitos técnicos | Qué conocimiento necesitará el equipo rojo para tener éxito. |

**Plan de Misión:**

|  |  |
| --- | --- |
| **Componente** | **Propósito** |
| Libros de juego de comandos (opcional) | Comandos exactos y herramientas para ejecutar, incluyendo cuándo, por qué y cómo. Comúnmente visto en equipos más grandes con muchos operadores en diferentes niveles de habilidad. |
| Tiempos de ejecución | Tiempos para comenzar etapas de compromiso. Opcionalmente puede incluir tiempos exactos para ejecutar herramientas y comandos. |
| Responsabilidades/roles | Quién hace qué, cuándo. |

**Plan de Remediación (opcional):**

|  |  |
| --- | --- |
| **Componente** | **Propósito** |
| Informe | Resumen de los detalles de compromiso e informe de los hallazgos. |
| Remediación/consulta | ¿Cómo remediará el cliente los hallazgos? Se puede incluir en el informe o discutir en una reunión entre el cliente y el equipo rojo. |