5 Guía específica de trabajo

5.1 Inicio del ejercicio

Importante: El ECD-INTEL 1 se inicia con una explicación de la infraestructura sujeto de simulación[1] por medio del uso del documento adjunto *" ECD-INTEL 1_Manual del Ejercicio-Anexo A.pptx"*. Para poder avanzar en el ECD-INTEL 1 deberá estar funcionando el 100% de los componentes de las RCI y de la RGI según lo explicado en la Sección 2.2[2].

5.2 Nivel Estratégico del Conflicto

Es el nivel en el que se establecen los objetivos de alto nivel y se asignan los recursos necesarios para lograrlos. El nivel estratégico ese el encargado de fijar además la orientación a seguir en el contexto de la geopolítica internacional. Este involucra la toma de decisiones en los máximos niveles de responsabilidad de una nación, e involucra a organismos del estado tanto civiles como militares y a recursos del sector privado.

5.2.1 Proceso de Surgimiento del Conflicto (PSC)

5.2.1.1 Gestión de Riesgos

El Modelo de Sistema Ofensivo de Referencia (MSOR) se inicia en un estado inicial de equilibrio en el que a pesar de no existir hipótesis de conflicto, se debe abordar la problemática de riesgos existentes, tanto internos como externos, en base a las diferentes amenazas y vulnerabilidades existentes.

Guías para el desarrollo de I/P:

¿Cuales son los activos de infraestructura crítica del EA?

¿Cuales son las amenazas existentes?

¿Que tan probable es que una determinada amenaza ejecute un ataque? (enemigo)

¿Que vulnerabilidades a nivel de organización, de procesos o de tecnologías existen?

¿Que vulnerabilidades a nivel humano existen?

¿Que vulnerabilidades podrían ser explotadas por el enemigo?

¿Qué recursos podrían conformar un blanco para el enemigo?

¿Qué tan importantes o valiosos son estos recursos?

¿Qué tan bien se está protegiendo a estos recursos?

¿Cuales son los recursos de infraestructura y humanos que, de ser seleccionados como blancos y destruidos, podrían forzar una situación de sumisión ante el adversario?

¿Que vulnerabilidades del enemigo pueden ser explotadas para obtener información sobre alguna de las preguntas realizadas arriba?

[1] Quizá resulte conveniente realizar una visita a una planta física afín para profundizar la situación de compromiso del personal involucrado.
[2] Para comenzar con la simulación del ataque al CDD se deberá asegurar que la Controladora (ctrolN1) se encuentre ejecutando la lógica original disponible en el directorio /AUX como 'ctrolN1_logic.py.bak'.

5.2.2 Desarrollo de Capacidades

En este nivel los actores desarrollan las capacidades del ciberespacio necesarias para llevar adelante las misiones en base a los objetivos planteados. El desarrollo contempla tanto capacidades defensivas y ofensivas, como de inteligencia.

Guías para el desarrollo de I/P:

¿Qué áreas de formación de RRHH vinculadas directa o indirectamente con OC se están formando?

¿Qué capacitaciones y entrenamientos se llevan a cabo?

¿Qué herramientas están siendo adquiridas?

¿Que trabajos y/o vínculos de I+D se están presentando a niveles local e internacional?

¿Cual es la participación en foros internacionales?

¿Que TTPs se están desarrollando?

¿Que ejercicios aislados y conjuntos, locales o internacionales, se desarrollan?

¿Cual es la evolución de las estructuras orgánicas militares relacionadas con ciberdefensa?

¿Existe asignación presupuestaria para ciberdefensa?

¿Existen convenios de desarrollo de capacidades con el sector privado?

¿Que empresas/organizaciones brindan productos/servicios de seguridad de la información y ciberdefensa? (cadena de suministros)

¿Que indica la realidad sobre el desarrollo de nuevas doctrinas?

¿El enemigo posee una estrategia para el ciberespacio?

¿Existen planes de transformación de las fuerzas en base a los requerimientos impuestos por el ciberespacio?

¿Existen estrategias para las fuerzas vinculadas con el ciberconflicto?

¿Que vulnerabilidades del enemigo pueden ser explotadas para obtener información sobre alguna de las preguntas realizadas arriba?

5.2.3 Desarrollo Legal Nacional e Internacional

Toda nación con desarrollo de capacidades militares debe establecer el marco jurídico interno en base al cuál regular el derecho al uso de la fuerza de ciberdefensa.

Guías para el desarrollo de I/P:

¿Existe un marco jurídico para regular el uso de ciberdefensa?

¿Que indican las leyes de la Defensa Nacional sobre ciberconflicto en cuanto a que esta permitido y que esta prohibido?

¿La ciberdefensa aplica a recursos de infraestructura fuera del sector militar?

¿Existen convenios de cooperación interna entre agencias públicas y/o privadas?

¿Existen convenios de cooperación internacional en el marco de la ley?

Ante un eventual ciberconflicto:

¿Se tiene certeza de las fronteras y los límites? (geográficas, lógicas, grupos, ciberpersonas, etc.)

¿Se tiene conocimiento de las autoridades aplicables en el lugar?

¿Se tiene conocimiento de las leyes aplicables en el lugar?

¿Se ha establecido el potencial impacto sobre la nación en términos de sanciones al ejecutar una OC?

¿Que vulnerabilidades del enemigo pueden ser explotadas para forzar una situación de ventaja sobre este?

5.2.4 Diplomacia

El manejo de los intereses y relaciones entre las naciones establecerá la manera en la que actuarán ante la eventual inminencia de un conflicto en el ciberespacio.

Guías para el desarrollo de I/P:

¿Existen intereses que podrían motivar el uso de OC en relación a las amenazas existentes?

¿Existen antecedentes sobre el uso de OC de alguna de la amenazas?

¿Existen antecedentes locales vinculados a negociaciones sobre las áreas de interés que podrían derivar en OC?

¿Los antecedentes se circunscriben al marco de las leyes nacionales e internacionales?

¿Existen operaciones de información de las cuales se es blanco, a nivel nacional como internacional?

¿Existen operaciones con efectos demostrados en el ciberespacio?

¿Han surgido conflictos con alguna de las corporaciones proveedoras de tecnología de carácter global en línea con la disputa diplomática?

¿Han surgido conflictos con alguna fuerza irregular de carácter nacional o transnacional en línea con la disputa diplomática?

¿Se encuentra resuelto el tema de atribución?

¿La situación de crisis alcanza a otras naciones?

¿La situación de crisis se inicia con nosotros o es derivada?

¿Que vulnerabilidades del enemigo pueden ser explotadas para forzar una situación de ventaja sobre este?

5.2.5 Declaración del Conflicto

La declaración del conflicto en el MSOR fuerza el inicio de la ejecución de las OC.

Guías para el desarrollo de I/P:

¿Existe una causa justa para la justificación del conflicto?

¿Existe una declaración formal de inicio del conflicto?

¿Las causas que sustentan la declaración se sostienen desde la perspectiva de la situación interna y geopolítica?

¿Ha existido agresión al territorio, bienes o patrimonios?

¿Se ha dado una invasión, ocupación no autorizada o algún acto intrusivo?

¿Se han incumplimiento tratados?

¿Se han realizado actos terroristas?

¿Existe una amenaza evidente sobre el bien nacional?

¿Existe una amenaza al orden interno?

¿La declaración formal de inicio del conflicto es legal bajo la luz del derecho y los tratados nacionales e internacionales?

¿Existe apoyo internacional o regional a las partes?

¿El arsenal del potencial adversario es legal?

¿Que vulnerabilidades del enemigo pueden ser explotadas para forzar una situación de ventaja sobre este?

5.2.6 Proceso de Planificación Estratégica

El Proceso de Planificación Estratégica (PPE) se desarrolla sobre el continuo ante la existencia de amenazas.

5.2.6.1 Inicio de la planifcación

Iniciado el proceso de planificación, será menester definir su alcance y establecer el conjunto de objetivos estratégicos asociados. En este sentido, es importante determinar el marco jurídico aplicable, los blancos potenciales, y los requerimientos a nivel del conjunto de la fuerzas.

Guías para el desarrollo de I/P:

¿Que razones justifican el inicio del proceso de planificación? (riesgos, conflicto irregular)

¿En que jurisdicciones se desarrolla el conflicto?

¿Cual es la autoridad en dichas jurisdicciones?

¿Cual es el marco legal aplicable al conflicto?

¿Cuales son las convenciones internacionales a las que debe darse cumplimiento?

¿Que recursos podrán ser seleccionados como blancos?

¿Que tan bien estos recursos se encuentran diferenciados del resto, desde la perspectiva de selección de blancos? (pcipio. distinción del LDCA)

¿De que maneras el adversario podrá proyectar poder sobre nuestros recursos?

¿Bajo el esquema de amenazas definido, cuales son las mejores formas de lograr sinergias a nivel conjunto por parte del adversario?

¿Existen antecedentes de operaciones conjuntas?

¿Que vulnerabilidades del enemigo pueden ser explotadas para forzar una situación de ventaja sobre este?

5.2.6.2 Análisis de misión

Con respecto al análisis de la misión, poder establecer un estado claro de la situación requiere de la determinación de los actores clave del conflicto (problemática de la atribución) y del análisis de las potenciales respuestas del adversario y el impacto que esta podría tener sobre los recursos propios.

Guías para el desarrollo de I/P:

¿Quienes son los enemigos?

¿Con que grado de certeza se ha determinado la atribución?

¿Que antecedentes de situaciones similares existen ligados al enemigo?

¿Quienes son los aliados?

¿Que antecedentes de situaciones similares existen ligados a los aliados?

¿Quienes son neutrales y de relevancia para la dinámica del conflicto?

¿Que respuestas podría materializar el adversario ante nuestros estímulos defensivos?

¿Que impacto podrían tener sobre los propios recursos las respuestas del adversario?

¿Cual es la relevancia de los blancos seleccionados?

¿Como impactaría la afectación de alguno de los blancos en el esquema PICN?

¿Que vulnerabilidades del enemigo pueden ser explotadas para forzar una situación de ventaja sobre este?

5.2.6.3 Desarrollo de cursos de acción

Identificados los enemigos, los potenciales blancos y las consecuencias posibles, se debe avanzar en el desarrollo de los cursos de acción (CDA) para los dos paradigmas de defensa posibles:

A. CDA Pasivos

Guías para el desarrollo de I/P:

¿Que blancos califican para esquemas de defensa pasiva?

¿Las capacidades desarrolladas son viables para la ejecución de las acciones?

¿Que efectos podrían derivar de este tipo de acciones?

¿Que efectos en cascada podrían generarse a partir de este tipo de acciones?

¿Que recursos son necesarios para sustentar las OC desde la perspectiva de la logística?

¿Que recursos son necesarios para sustentar las OC desde la perspectiva de abastecimiento?

¿Cuales son las formas en que el enemigo podrá obtener posiciones relevantes a nivel táctico?

¿Cuales son las mejores formas de aproximación a los blancos por parte del enemigo?

¿Es viable la aplicación de fuerza por medios tradicionales?

¿Es viable la aplicación de operaciones conjuntas?

¿Cuales son los escenario que aportan la mayor sinergia desde la perspectiva de aplicación conjunta?

¿Que vulnerabilidades del enemigo pueden ser explotadas para forzar una situación de ventaja sobre este?

B. CDA Activos o indirectos

Guías para el desarrollo de I/P:

¿Que blancos califican para esquemas de defensa activa?

¿Las capacidades desarrolladas son viables para la ejecución de las acciones?

¿Que daños colaterales podrían derivar de este tipo de acciones?

¿Que efectos en cascada podrían generarse a partir de este tipo de acciones?

¿Que recursos son necesarios para sustentar las operaciones desde la perspectiva de la logística y el abastecimiento?

¿Cuales son las formas de obtener posiciones relevantes a nivel táctico?

¿Cuales son las mejores formas de aproximación a los blancos?

¿Es viable la aplicación de fuerza por medios tradicionales?

¿Es viable la aplicación de operaciones conjuntas?

¿Cuales son los escenario que aportan la mayor sinergia desde la perspectiva de aplicación conjunta?

¿Que vulnerabilidades del enemigo pueden ser explotadas para forzar una situación de ventaja sobre este?

5.2.6.4 Plan

Sobre el conjunto de CDA desarrollados, se avanzará en su simulación y análisis para posteriormente realizar una comparación entre ellos y seleccionar el más conveniente para lograr los objetivos estratégicos planteados. El CDA seleccionado será transformado en un plan.

En la Figura se presenta una serie de acciones destinadas a complementar los CDA tradicionales sujetos al POC, en base a una serie de acciones derivadas de la inteligencia en los planos operacional y estratégico.

	Detectar	Denegar	Interrumpir	Degradar	Engañar	Destruir
Motivación	Inteligencia de fuente abierta	Relaciones institucionales, Aplicación del marco legal		Relaciones institucionales		
Objetivos	Análisis de I/P Web, Inteligencia de fuente abierta			Seguridad operativa y Ciberdefensa	Relaciones institucionales	
Ruta de aproximación	Análisis de I/P de red y servicios de infraestructura y de usuarios		Seguridad operativa	Seguridad operativa	Forzar el paso por seguridad reforzada	
Capacidades	Inteligencia de fuente abierta		Programas de amenaza interna	Seguridad operativa y Ciberdefensa	Forzar el paso por seguridad reforzada	
Acceso	Análisis de I/P de red y servicios, Inteligencia de fuente abierta	Inteligencia de fuente abierta		Seguridad operativa		
Acciones	Inteligencia de fuente abierta, Análisis de cadena de abastecimiento	Roles y Control de acceso		QoS	Tecnologías Honey*	
Evaluación	Análisis de I/P Web, Análisis de redes sociales	Relaciones institucionales			Relaciones institucionales, Tecnologías Honey*	
Contraataques	Análisis de I/P de red y servicios, Inteligencia de fuente abierta Auditoría Log	Seguridad Operativa y Ciberdefensa			Relaciones institucionales, Tecnologías Honey*	

Figura. Ejemplo de CDA de nivel estratégico.

5.2.7 Métricas y medición de las OC

La evaluación de los resultados de las OC debe ser implementada como una herramienta a todos los niveles de conflicto militar ya que permite la determinación de los efectos de las OC tanto propias y de los aliados, como del enemigo.

5.2.7.1 Evaluación de nivel táctico (ET)

Subproceso que consiste en la determinación de la efectividad de las operaciones a nivel táctico.

5.2.7.2 Evaluación de nivel operacional y estratégico (ESE)

Subproceso destinado a soportar el juicio analítico de la estrategia implementada, es decir de los fines, las formas y los medios empleados para el logro de los objetivos y así determinar el éxito de la misión y las necesidades de ajustar la estrategia y los posibles CDA futuros.

5.3 Nivel operacional del ciberconflicto

Es el nivel del conflicto en el que se planifican, conducen y mantienen las campañas u operaciones mayores con el fin de lograr los objetivos estratégicos. En este nivel, si bien las tareas pueden ser ejecutadas de manera rápida, distan mucho de estar sujetas a las velocidades de la red.

El nivel operacional se vincula mayormente a la necesidad de establecer los recursos tecnológicos y de seguridad necesarios como soporte de la misión y el logro de los objetivos. Esta responsabilidad implica, entre otras tantas cosas, la obtención de información relativa a los recursos humanos, a las *técnicas, tácticas y procedimientos (TTP)* y a las herramientas involucradas en las operaciones. Los aportes de inteligencia a operacional resultan esenciales para la identificación de los enemigos, sus motivaciones y capacidades, de tal manera de poder aportar inteligencia al proceso de toma de decisiones a mediano y largo plazo. Cuanto más se sepa sobre los objetivos y las capacidades de un adversario, mejor se estará preparado para desarrollar un defensa proactiva.

Si bien el proceso CDA hace uso de las capacidades tácticas para lograr el objetivo, se completa con las primeras fases del POC correspondientes al nivel operacional del ciberconflicto.

5.3.1 Nivel operacional del POC

A nivel operacional se consideran los siguientes eslabones del POC: *análisis de campañas, potenciación o adaptación de capacidades y doctrinas, y validación de objetivos.*

5.3.1.1 Potenciación o adaptación de capacidades y doctrinas

En este nivel los actores modifican capacidades tácticas existentes con el objetivo de llevar adelante una campaña en base a los objetivos planteados. En este proceso se deben consolidar las posiciones relevantes en base a las cuales ejecutar el nivel táctico.

Guías para el desarrollo de I/P:

¿Que técnicas, tácticas y procedimiento está siendo utilizadas?

¿Que información puede derivarse del ciclo operacional del enemigo?

¿Que información puede derivarse sobre las formas de toma de decisión?

¿Que información puede obtenerse en torno a sus procesos y tecnología de C2?

¿Que nuevas capacidades o variaciones de estas han sido desarrolladas?

¿Que nuevas doctrinas o variaciones de esta han sido desarrolladas?

¿Que información registrada avala las operaciones de inteligencia del adversario destinadas a realimentar sus procesos de potenciación o adaptación?

¿Que recursos de información que utiliza el enemigo podría ser utilizada como blanco para afectar alguno de sus procesos de combate?

¿Que vulnerabilidades del enemigo pueden ser explotadas para obtener información sobre alguna de las preguntas realizadas arriba?

5.3.1.2 Validación de objetivos

Con el conjunto de capacidades a punto, el nivel operacional debe realizar una validación de los blancos sobre los cuales se desarrollará la operación.

Guías para el desarrollo de I/P:

¿Que rutas de aproximación están siendo utilizadas por el enemigo?

¿Que estímulos son observados a nivel tecnológico sobre la infraestructura protegida? (redes, SS:II)

¿Que estímulos son observados a nivel humano sobre la infraestructura protegida? (personal, cadena de abastecimiento)

¿Que recursos de información que utiliza el enemigo podría ser utilizada como blanco para afectar alguno de sus procesos de combate?

¿Que vulnerabilidades del enemigo pueden ser explotadas para obtener información sobre alguna de las preguntas realizadas arriba?

En la Figura se presentan los elementos del CDA del nivel operacional que completan el modelo POC.

	Detectar	Denegar	Interrumpir	Degradar	Engañar	Destruir
POC.1	Análisis de IPCC			Honey*	Honey*	
POC.2	Análisis Web	Firewall ACL				
POC.3	NIDS	NIPS				

Figura. Curso de Acción de nivel operacional.

5.3.2 Análisis de campaña

La inteligencia que surge de los niveles táctico y operacional permite desarrollar un recursos analítico de inmenso valor para el plano estratégico denominado análisis de campañas y para la identificación positiva asociada a la problemática de atribución y la determinación del objetivo final del adversario, de su misión.

Guías para el desarrollo de I/P:

¿Que alianzas pueden derivarse de la información de campaña?

¿Que blancos son mayormente estimulados por el enemigo en las campañas?

¿Cuales de los blancos estimulados son de misión crítica?

¿Que información podría ser utilizada para determinar si tal acción fue ejecutada por alguien?

¿Es posible determinar cual es la misión del enemigo en base a la información recolectada y a la inteligencia generada?

¿Que vulnerabilidades del enemigo pueden ser explotadas para obtener información sobre alguna de las preguntas realizadas arriba?

El AC se basa en el análisis de información de los diferentes CDA vinculados a las OC en base a procesos de correlación. En la siguiente figura puede verse un ejemplo aplicado a dos CDA diferentes derivados el análisis de los niveles táctico y operacional.

I/P Clave de Campaña (I/PCC): Son aquellos I/P que resultan más confiables, y sobre los cuales se sustenta la priorización y el desarrollo de los cursos de acción. La siguiente figura presenta un ejemplo de I/PCC. Estos resultan menos volátiles y por consiguiente conforman la base de análisis para predecir la dinámica de futuras operaciones.

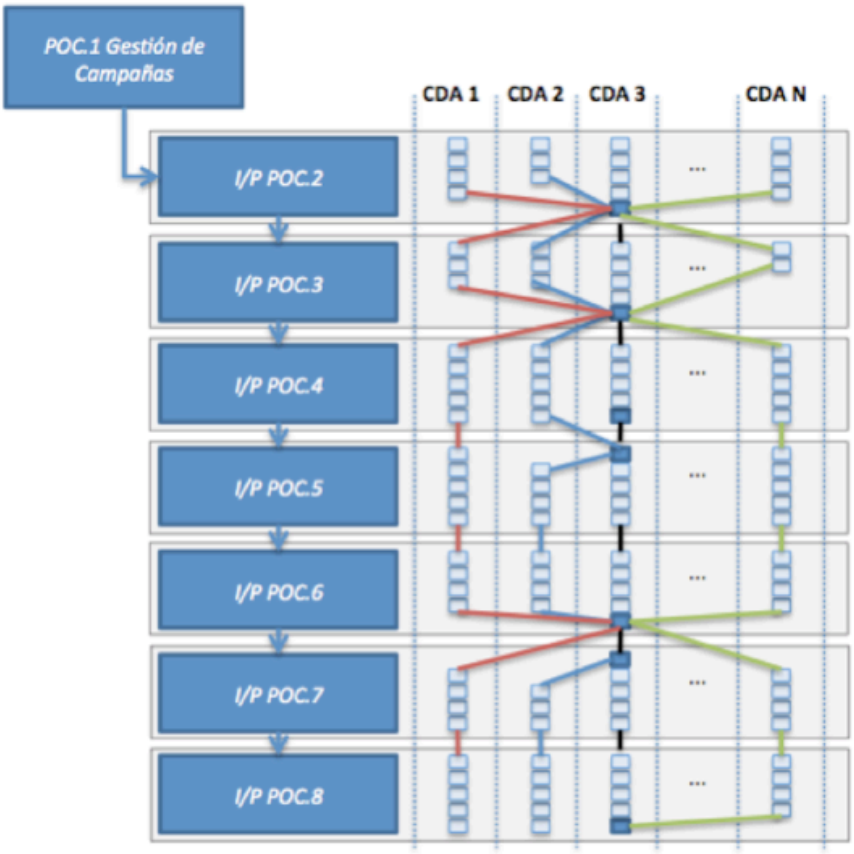

Figura. Análisis de Campáña e Indicadores Clave.

5.4 Nivel táctico del ciberconflicto

El táctico es el nivel del ciberconflicto en el que se planifican y ejecutan las operaciones destinadas a conducir al logro de los objetivos militares. El táctico es el nivel del ciberconflicto que se vincula con la segunda parte del modelo de cadena ofensiva definido en el *Proceso de Operaciones en el Ciberespacio (POC)*.

5.4.1 Nivel táctico del POC

A nivel táctico se consideran los siguientes eslabones del POC: *entrega, explotación, instalación, comando y control, y acciones sobre los objetivos.*

5.4.1.1 Entrega

En la fase de entrega se realiza la transmisión del arma al ambiente objetivo.

Medio de Entrega	Tecnológico	Humano
Directo	Se transmite el arsenal directamente al ambiente objetivo: - Transmisión mediante mecanismos establecidos a tal fin (FTP, HTTP/HTTPS, SMB, SSH, etc.) - Transmisión mediante la explotación de vulnerabilidades	Se transmite el arsenal directamente al ambiente objetivo comprometiendo procesos operativos vinculados a las personas de la organización objetivo: - Transmisión mediante Unidades de almacenamiento, correo electrónico, repositorios de software, etc.
Indirecto	Se transmite el arsenal a un ambiente determinado el cual posee algún tipo de vinculación funcional con el ambiente objetivo: - Transmisión mediante mecanismos establecidos a tal fin (FTP, HTTP/HTTPS, SMB, SSH, etc.) - Transmisión mediante la explotación de vulnerabilidades	Se transmite el arsenal al ambiente objetivo comprometiendo procedimientos operativos vinculados a personas de la cadena de abastecimiento con algún tipo de vinculación funcional con el ambiente objetivo. - Considera todos los mecanismos posibles vistos en el resto de los casos

Una observación importante a la hora de diseñar el conjunto de I/P destinados a soportar los mecanismos de detección es que en última instancia, la entrega siempre se realizará sobre recursos tecnológicos.

La acción de transferencia del arsenal tiene un efecto final que puede ser categorizado en base a los siguientes criterios:

- Copia de recursos a un nuevo sistema
- Reemplazo de recursos existentes en un sistema
- Modificación de recursos existentes en un sistema
- Generación de enlaces o vínculos (ln, XSS)

Guías para el desarrollo de I/P:

¿Qué eventos pueden ser detectados a nivel tecnológico que violen las políticas de seguridad vinculadas a control de acceso y acciones de transferencia? (violaciones de acceso, tipos de datos, mecanismos, etc.)

¿Qué eventos pueden ser detectados a nivel humano que violen las políticas de seguridad vinculadas a control de acceso y acciones de transferencia?

¿Que cambios o anomalías pueden ser derivadas del conocimiento del régimen permanente en base al conjunto de acciones de transferencia definidas?

¿Que vulnerabilidades del enemigo pueden ser explotadas para obtener información sobre alguna de las preguntas realizadas arriba?

5.4.1.2 Explotación

Una vez transmitida y entregada el arma, la fase de explotación dispara o inicia el código malicioso de manera automática o manual.

Guías para el desarrollo de I/P:

¿Qué vulnerabilidades existen que puedan ser explotadas por una amenaza interna o externa a nivel técnico? (redes, SS:OO, servicios, aplicaciones)

¿Qué vulnerabilidades existen que puedan ser explotadas por una amenaza interna o externa a nivel humano? (procesos, procedimientos)

¿Qué vectores de ataque se registran por medio de interfaces sociales? (estímulos internos y externos, violación a las políticas de seguridad)

¿Qué alertas de ataque se registran en los sistemas IDPS, tanto de dispositivos como de red?

¿Que anomalías funcionales pueden ser derivadas del conocimiento del régimen permanente?

¿Que vulnerabilidades del enemigo pueden ser explotadas para obtener información sobre alguna de las preguntas realizadas arriba?

5.4.1.3 Instalación

En la fase de instalación se establece la presencia (de troyanos o puertas traseras) de tal manera de lograr acceso con características de persistencia en el ambiente objetivo.

Guías para el desarrollo de I/P:

¿Qué registros de actividad evidencian desvíos con respecto a la información vinculada con gestión de activos? (SS:OO, servicios y aplicaciones)

¿Qué alertas de ataque se registran en los sistemas IDPS de dispositivos?

¿Que anomalías funcionales pueden ser derivadas del conocimiento del régimen permanente de los diferentes dispositivos?

¿Que vulnerabilidades del enemigo pueden ser explotadas para obtener información sobre alguna de las preguntas realizadas arriba?

5.4.1.4 Comando y Control

Consumada la fase de ejecución, el dispositivo comprometido envía una señal a un controlador por medio de Internet con el fin de establecer un canal de C2.

Guías para el desarrollo de I/P:

¿Qué registros de actividad evidencian señales de tráfico de datos fuera de los autorizados por las políticas de seguridad? (servicios lícitos, nuevos procesos y servicios)

¿Qué alertas IDPS evidencian señales de tráfico de datos fuera de los autorizados por las políticas de seguridad? (servicios lícitos, nuevos procesos y servicios) (resolución acceso C2 por IP y dominios, fluxing)

¿Que anomalías funcionales pueden ser derivadas del conocimiento del régimen permanente de los diferentes dispositivos y su software? (servicios lícitos, nuevos procesos y servicios)

¿Existe tráfico de red ofuscado o cifrado fuera de las definiciones de la política de seguridad? (servicios lícitos, nuevos procesos y servicios)

¿Contra que servidores externos se genera el tráfico?

¿A quién pertenecen los servidores externos involucrados?

¿Que tipo de arquitectura sustenta a la red de C2? (estrella, jerárquica, p2p)

¿Que vulnerabilidades del enemigo pueden ser explotadas para obtener información sobre alguna de las preguntas realizadas arriba?

5.4.1.5 Acciones sobre los objetivos

Con acceso total a los blancos seleccionados y en base a las órdenes recibidas por medio de la red C2, el enemigo procede a la ejecución de las acciones, es decir al ataque propiamente dicho

Guías para el desarrollo de I/P:

¿Qué vulnerabilidades existen que puedan ser explotadas por una amenaza interna o externa a nivel técnico? (SS:OO, servicios y aplicaciones)

¿Qué vulnerabilidades existen que puedan ser explotadas por una amenaza interna o externa a nivel humano?

¿Que dispositivos están comprometidos?

¿Qué ataque se registran por medio de interfaces sociales?

¿Qué registros de actividad evidencian señales de tráfico de datos fuera de los autorizados por las políticas de seguridad?

¿Qué alertas IDPS de red y de dispositivo evidencian señales de tráfico de datos fuera de los autorizados por las políticas de seguridad?

¿Qué registros de actividad evidencian ataques?

¿Qué alertas IDPS de red y de dispositivo evidencian ataques?

¿Que anomalías funcionales pueden ser derivadas del conocimiento del régimen permanente?

¿Cuales son los efectos directos de los ataques?

¿Cuales son los efectos potenciales directos de los ataques?

¿Cuales pueden ser los efectos indirectos en forma de daño colateral y efectos en cascada?

¿Cuales son los efectos sobre la IC propia?

¿Cuales son los efectos sobre la IC de sistema nacional?

¿Que I/P podrían evidenciar robo de información?

¿Que vulnerabilidades del enemigo pueden ser explotadas para obtener información sobre alguna de las preguntas realizadas arriba?

5.4.2 Cursos de acción y el análisis de cadena ofensiva

La inteligencia obtenida del análisis de los diferentes I/P a nivel táctico tiene un efecto directo y prácticamente instantáneo sobre los flujos de realimentación del proceso de planificación. El nivel táctico es, ni más ni menos, el nivel del conflicto en el que se manifiesta la realidad y por lo tanto requiere de respuestas adecuadas. Estas respuestas toman la forma de cursos de acción (CDA) y podrán o no estar predefinidos por la planificación. Los CDA representan el proceso organizacional, humano y tecnológico por medio del cual se plasman las acciones de defensa en el AO/TO. La tabla 1 muestra un posible CDA basado en un conjunto predefinido de acciones de ciberdefensa.

	Detectar	Denegar	Interrumpir	Degradar	Engañar	Destruir
POC.4	Sensor	Filtro Proxy	Antivirus	Colas		
POC.5	HIDS	Parches	DEP			
POC.6	HIDS	Chroot	Antivirus			
POC.7	NIDS	Firewall ACL	NIPS	Tarpit	Redirección DNS	
POC.8	Auditoría Log			QoS	Honeypot	

Figura. Curso de Acción de nivel táctico.