

Vamos a priorizar la seguridad de la información sobre la de la red

- Inteligencia llevar la información a certeza
- Ciber medio digital y electrónico
- Archivo Digital solo vive en la computadora
- Electrónico existe físicamente y se pasó a electrónico, al cual podemos ver en computadora o físico
- Físico es el original e lo electrónico

Evaluación

- 10% Expo en equipo. Una a fines de septiembre y otra a fines de noviembre
- 10% Tareas (4 tareas)
- 20, 20, 25 exámenes parciales + final
- Proyecto 15. El proyecto final es un CTF casero hecho por el profe.

Ciberspacio

El ciberespacio no tiene un espacio físico y real definido. Los servidores están en USA, Brazil, etc. Las personas están en distintas partes del mundo y las acciones que se realizan en el espacio cibernético (p. ej. en una llamada de Zoom) ocurren en múltiples lados a la vez (servidores que procesaron la información, persona que lo hizo, víctima, etc).

Ciclo de inteligencia

De acuerdo a la OTAN, pero pueden ser ciclos distintos, específicos para el objetivo de quien lo diseña. Por ejemplo si el ciclo está enfocado a lo corporativo o a lo militar.

CNI: Centro Nacional de Inteligencia. Ex. CISA. La inteligencia para seguridad nacional se refiere hacia el interior y exterior.

En una historia hay 3 verdades, la tuya, la mía, y la verdad

Proyecto: Solo tenemos 1 semana para prepararlo, pero solo hay que preocuparnos hasta Noviembre

1. Planificación: Saber qué necesitamos, qué conocimiento se necesita para el objetivo que se quiere alcanzar.
 - Hacemos el plan de obtención, cómo vamos a obtener la información
2. Obtención de información: Todo lo que necesitamos de información.
 - Qué tipo de información necesitamos?
 - Apegarse al marco legal
 - Técnicas:
 - ▶ HUMINT, Human Intelligence: Persona a persona, con pláticas para obtener información
 - Ingeniería Social: No es ilegal
 - En un experimento de ingeniería social en la SEDENA el 70% dio sus credenciales de inicio de sesión.
 - No tiene por qué ser directamente con los directamente involucrados, pero por medio de personas que conviven en su ambiente (ej. un boleador de zapatos).

- El tipo de preguntas que se hacen afecta en el resultado de la información que se obtienen. O si se hace con trampa para forzar una respuesta específica (ej. Y qué otro detalle tenía la chamarra roja? Cuando era verde).
- Ej hablar con los testigos/personas que rodean un hecho
- ▶ SIGINT, Inteligencia de Seniales: Radio y televisión.
 - Con las noticias hay que tener cuidado con la manipulación de noticias, y a la línea de quien lo dice (ej. es de izquierda).
 - Ej. Frecuencias de radio aficionado: Ponemos nuestra antena y ponemos nuestra propia estación de radio en el alcance que tenga.
 - Ej. Walkie-talkies y eso
 - Un fantasma en el sistema.
- ▶ OSINT, Open Source Intelligence: Información de fuentes abiertas.
 - Cualquier cosa a la que se puede acceder como civil.
 - No tiene por qué ser gratuito, con que cualquier persona pueda acceder (ej. cualquiera puede pagar por un portal que obtiene información).
 - Deep Web no es lo mismo a Dark Web. Son publicas y son abiertas, mas se necesita saber cómo entrar.
 - Fake news: Tenemos que tener cuidado de no obtener información basura.

3. Procesamiento:

- Convertir los datos en información
- Tenemos que tener certeza para cada cosa que se descarta, elimina.
- Procesamos qué tipo de información tenemos, qué contiene, etc.
- Separamos lo que nos sirve de lo que no nos sirve, lo que vale la pena analizar de lo que no.
- No “eliminamos” del todo la información, sino que lo clasificamos.

4. Análisis:

- Revisión de la información.
- Que se conforme con el objetivo, nos sirve para el conocimiento que seleccionamos
- Que sea verdad (no fake new)
- Que sea vigente (ej. no nos sirve de nada una foto que pasó hace 20 años)

5. Difusión:

- Se entrega un producto de inteligencia para tomar decision
- Para el ptoyecto: Tiene que ser clara, consisa y certera
- El CNI la gran mayoría de veces le entrega los reportes de inteligencia al Presidente y al Secretario de Gobernación, de forma que puedan tener *control* y *gobierno*. Los casos donde el objetivo no se cumple, el CNI puede no reportarlo al presidente, determinado por el director de la organización. Un analista no tiene el panorama completo
- Los militares tienen la sección 2da, de inteligencia
- Responder a las preguntas de qué, quién, cómo, en dónde, cuál fue la situación: Resumen de lo que pasó.
- El resumen de la difusión tiene que ser rápido, corto.

6. Retroalimentación (Opt):

- La retroalimentación se hace en cada punto del ciclo y al final
- Saber que todo lo que se hizo fue en el sentido correcto. Que el objetivo de la inteligencia se cumpla.
- **Llevar la información al grado de certeza**

Seguridad informática: Datos de un medio cibernético. Seguridad de la información: Datos de cualquier medio y formato, físico, virtual.

Dentro de HUMINT y OSINT hay una técnica llamada *dumpster diving*, en la basura se puede encontrar mucha información. La privacidad es muy importante, no escondemos cosas porque es malo, sino por seguridad, etc.

El hecho de buscar información y analizarlo hará que sigamos el ciclo, sea ciber o no. Sea para seguridad o no.

Contra-inteligencia

La protección de nuestra información para que no sea tan sencillo/posible obtenerla por actores externos. Evitar que puedan terminar el ciclo de inteligencia.

El tener muchos rumores, cuentos, desinformación, cuentan como contra-inteligencia. La estrategia para lograrlo puede iniciar desde los empleados (ej. un empleado de CocaCola me dijo que la receta está en París).

El ciclo de información y el de un ataque se ven similares. Consejo personal: Pedir ayuda si algo va mal, la presión para defender la información es mucha.

La mejor defensa no es un buen ataque. No podemos atacar con un globo a una persona, puede que tenga una pistola. Si alguien nos demostró que nos atacó, probablemente lo hizo porque tiene asegurado el acceso y control, si intentamos devolverse, nos atacará aún peor.

APT

Advanced-Persistent-Threat.

Cuando nos enfrentamos a una amenaza, depende de quién lo haga. No es lo mismo tener una amenaza de un niño a una persona del gobierno. Con actores más grande, entran más factores como OT (Operational Technology).

Mientras más queramos avanzar, más especialistas en cada área necesitaremos. No solo hay programadores y personas de sistemas.

Enlaces

MITRE: <https://attack.mitre.org/> Organización sin fines de lucro, que ayuda en la parte de análisis, revisión y clasificación de vulnerabilidades (físicas, ciberseguridad, etc). Ej. para verificar si un aeropuerto es seguro.

CERT, CSIRT, PSIRT

CERT de la fuerza área.

- CERT: Derechos reservados
- CERT: Equipos de seguridad y funcionalidad que actúan a veces xD.
- PSIRT: Product Security Response Team: Que los productos no tengan fallas de seguridad, se dan a conocer cada medio año

APTs

Características

- Avanzado:
- Es una amenaza:
- Persistente: Tiene que tener un objetivo

Malware engloba todo lo malo.

Otra vez caso hipotetico de Prism

Espiamos a todo el mundo?

- No, esos datos son peligrosos
- Si, pero me protejo

Acción (o lo haces por dinero) o coacción (o yo te hago algo)

Obtención de la información

- Contexto o justificación: Qué necesitamos conocer. Qué voy a buscar
- Objetivo general: Para qué lo quiero.Cuál es el objetivo de poder buscar esa información. De esa información/conocimiento cuáles son los puntos importantes.
- Objetivo específico:
 - Responsable: Quiénes están involucrados?
 - Función: Tienes que saber lo que tienes que saber, cuáles son mis funciones y a quien le puedo dar la información que tenemos. ¿Con quiénes tengo contacto? De otra forma podemos tener fugas de información o en algún momento perdamos la información.
 - Lugar: Podemos hacer prácticamente todo conectados a la red, en internet
 - Cobertura: Rango de información que podemos tener.
 - Equipo: Qué vamos a utilizar.

Nosotros deberíamos de apegarnos a las leyes, buscando los recursos que podamos usar. La cantidad de recursos que tenemos los limitan las leyes y eso. Qué herramientas tenemos, cómo las podemos aprovechar.

Como ejemplo, el 90% de presos no hicieron algo premeditado. Capacidad de Síntesis. Estamos limitados por lo legal, pero podemos compensar con conocimiento y herramientas.

Respuesta de un informe de inteligencia: Es importante subrayar que la información que se recopile deberá responder a las preguntas, ¿Qué, quién, cuándo, dónde, cómo, con qué, con quién, por qué y para qué?

https://www.theregister.com/2024/08/02/israeli_hacktivists/ Hactivista detenido y contestamos todas las preguntas.

- Asi como se dice de rapido las respuestas a la preguntas, asi de conciso debe ser el reportar los eventos.
- Qué? Planean atacar el internet, sus sistemas y proveedores,
- Quién? Hscktivisstas de Israel, WeRedDevils
- Por qué?
- Cuando? 14 Ago
- por el ataque directo de Hamas a Israel
- Dónde? La red eléctrica
- Con qué? COn ataques a la malla eletrica
- Para qué?