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.

Ciberespacio

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 multiples lados a la vez (servidores que procesaron la información, persona que lo hizo, victima, etc).

Ciclo de inteligencia

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

CNI: Centro Nacional de Inteligencia. Ex. CISN. 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 nuesrta 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 anios)
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 imporatnte, 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 Paris).

> 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 devolverselo, 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 ninio 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 (fisicas, ciberseguridad, etc). Ej. para verificar si un areopuerto es seguro.

CERT, CSIRT, PSIRT

> CERT de la fuerza área.

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

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/ Hacktivista 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?
- Cúando? 14 Ago
- por el ataque directo de Hamas a Israel
- Dónde? La red eléctrica
- Con qué? COn ataques a la malla eletrica
- Para qué?

Actores y Amenazas

Hacktivismo

Para promover una ideología?

Su presupuesto puede venir de donaciones o haciendo trabajos. Que hagan cosas ilegales no deja de hacer que sea hacktivismo

Tienen un objetivo social, escogen paginas de visualización. Vulnerabilidades no tan obvias. Siempre se presenta una idea particular marcada

- DDoS
- Defacement

Principales actores:

- Civiles
- Anonymous: Muchas personas que arman desmadre en 4Chan
- Lulz Sec: Este si es un grupo de personas especificas
- Wikileaks: Es una plataforma para poder difundir cosas, mezclado con fake news.
  - Edward Snowden: Cuando publican grabaciones de ataques a hospitales civiles.

Casos

- Primavera Arabe
- Activismo anti Vladimir Putin: Se divulgan fotos de asesinatos de la oposición

2chan no se que de anime, pero como es en ingles le ponen 4chan. La cosa de 4chan es que permite publicar sin loggearse. Todos son Anonymous y basicamente se ponen de acuerdo entre usuarios para hacer cosas

Terrorismo

Buscan la dominación en base al terror. Se usan varios medios para el terrorismo. Inflingir terror. Quieren organizar un cambio.

Tecnica de terrorismo vs fenomeno de terrorismo:

Tipos:

- Anarquista: Solo quieren ver el mundo arder
- Religioso:
- Politicos: Demuestran su superioridad
  - Ultra izquierda
  - Ultra derecha

Usan foros, y sitios propios no regulados donde es sencillo hacer su desmadre.

Actores principales

- Organizaciones gubernamentales
- Alianzas de seguridad internacional
- Organizaciones terroristas

Ataques

- Estructurado: Usan software especializado
- No estructurado: Software poco comun

Partidos politicos

- Hamas: Palestina. Son muy radicales, reclaman que quieren volver a tener el territorio de 1948

- Hezbola: No se donde

Fake news
Cambiar la verdad o no contarla completa

OSINT
Antes del internet hay información con microfono

Investigación tiene dos tipos:
- Pasiva: Usar otros medios, no directamente
- Activa: Lanzar un escaneo, directamente

Cuando se hace un ataque:
- Reconocimiento es activo y pasivo

Ejemplo: Una persona esta haciendo fraude, no se puede saber que se le está investigando. Se uso una tecnica medio xD, que parece ilegal, peero pues todo sea por los loles. El otro puso candados. Se los voló, asi que probablemente se dejo rastro, y se va a enterar que lo investigaron

OSINT
Depende de quién eres, a quién quieres investigar y por qué habrá diferencias. Es distinto qué sea un civil, una persona de gob, etc. Lo que varía es:
- Recursos económicos
- Poder de investigación, etc.

Cyberacoso
Cualquier técnica de intimidación en plataformas digitales.

Actores:
- Victima: Un individuo
- Acosador: Motivado por intimidación, venganza o placer
- Espectador(es) o testigo(s): Son muchos, anónicmos, ven y interactuan de forma anónima

Características:
- Atacar, humillar
- Varia el tipo de medio como imagenes o mensajes
- Relacionado al acoso, pero como es digital queda registro

Dependiendo del número de victimas, medios de acoso, etc. Se tienen:
- Cyberbullying
- Flamming: en foros, humillar a una persona
- Doxxing: Info privada
- Outing: Hacer publica información privada

Inteligencia
Se usa a nivel corporativo, mercadotecnia, etc. “Cuando hacemos que la información sea certeza”. Lo importante es poder tomar una decisión. Se pasa el reporte. Tipos:
- Inteligencia militar, gubernamental, estrategica

Rae: Capacidad de entender o comprender

Ciclo de la información
- Difusión:
- Planificación

- Obtención de la información
- Procesamiento
- Análisis y producción

Datos

- Datos: Alg

OSINT ?

Es como un rompecabezas buscar cosas.

- Google es una parte clave
- Flight radar: Para trackear aviones. Cada avión en el mapa envía su información a torres en tierra o a otros a viones, que hacen el relay de información a una torre. Es un estimado cercano a la realidad.
  - Ubicación
  - Información del viaje
  - Modelo e información del avión
  - Velocidad y altura
  - Numero de registro:
    - NXXXXX: Registrado por USA, para pasar por él. Matricula nectar.
  - Busqueda por avión, por origen-destino, aereopuerto, etc
  - Los aviones privados no suelen activar el *transponder*, no hay información sobre el viaje, el avión, etc. Si te deja ver la ubicación
  - También se puede ver histórico

  > Mayo Zambada: Se subió un avión que era internacional, pero cambia el rumbo a USA, donde lo agarran.

- Vessel Finder: Para rastrear barcos
  - Podemos ver:
    - Draught: La altura entre la parte más baja y la linea de flote. Con esto podemos darnos cuenta de la dimensión
    - El IMO es más usado que el MMSI
    - Velocidad en nudos
    - Ubicación
  - Podemos filtrar por:
    - Tipo de barco (ej. militar)
    - IMO

> Submarinos comerciales casi no hay. Casi todos son experimentales o militares.

- Train tracker / Open railway map. Para trenes es mejor buscar la ruta en google directamente

Buscar personas

Páginas para buscar cositas:

- Face Search:
  - search4..
  - facecheck: freemium
  - searchfaces: busquedas por tiktok
- Addons para firefox:

    - Search by image
- yandex

Pasos:
- Buscar la imagen con face search engines
- Comparar con face compare
- profit

Páginas con retos
- Manuel Travezaño: Manuel Bot
- Sofía Santos

OSINT Framework: Está desactualizado