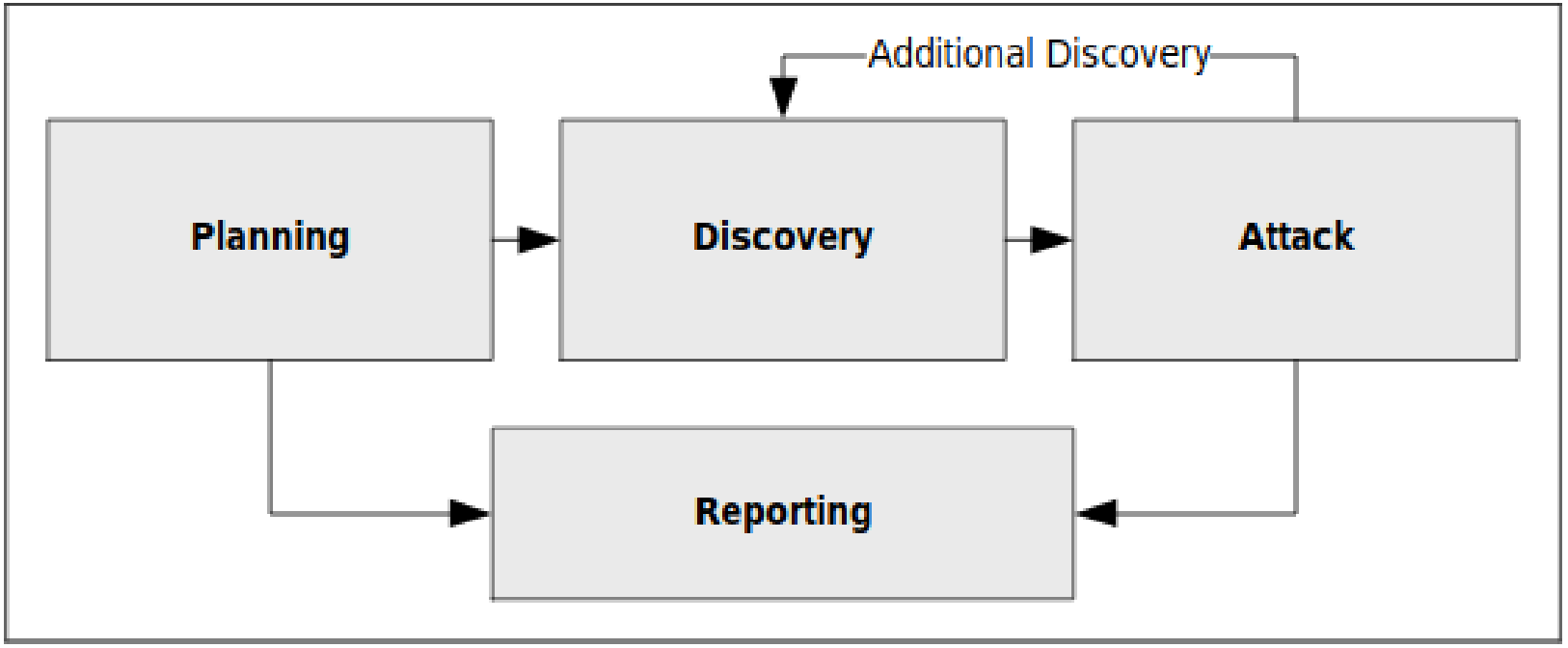
Intelligence Gathering y OSINT

Contenidos

1. Introducción.
2. Recolección pasiva vs activa.
3. Conoce a tu objetivo.
4. Conceptos y definiciones.
5. Intelligence gathering.
    1. Disciplinas de Intelligence Gathering.
    2. Ciclo de vida de inteligencia.
    3. Problemática en el footprinting

Introducción

- **Las fases de la metodología NIST**:

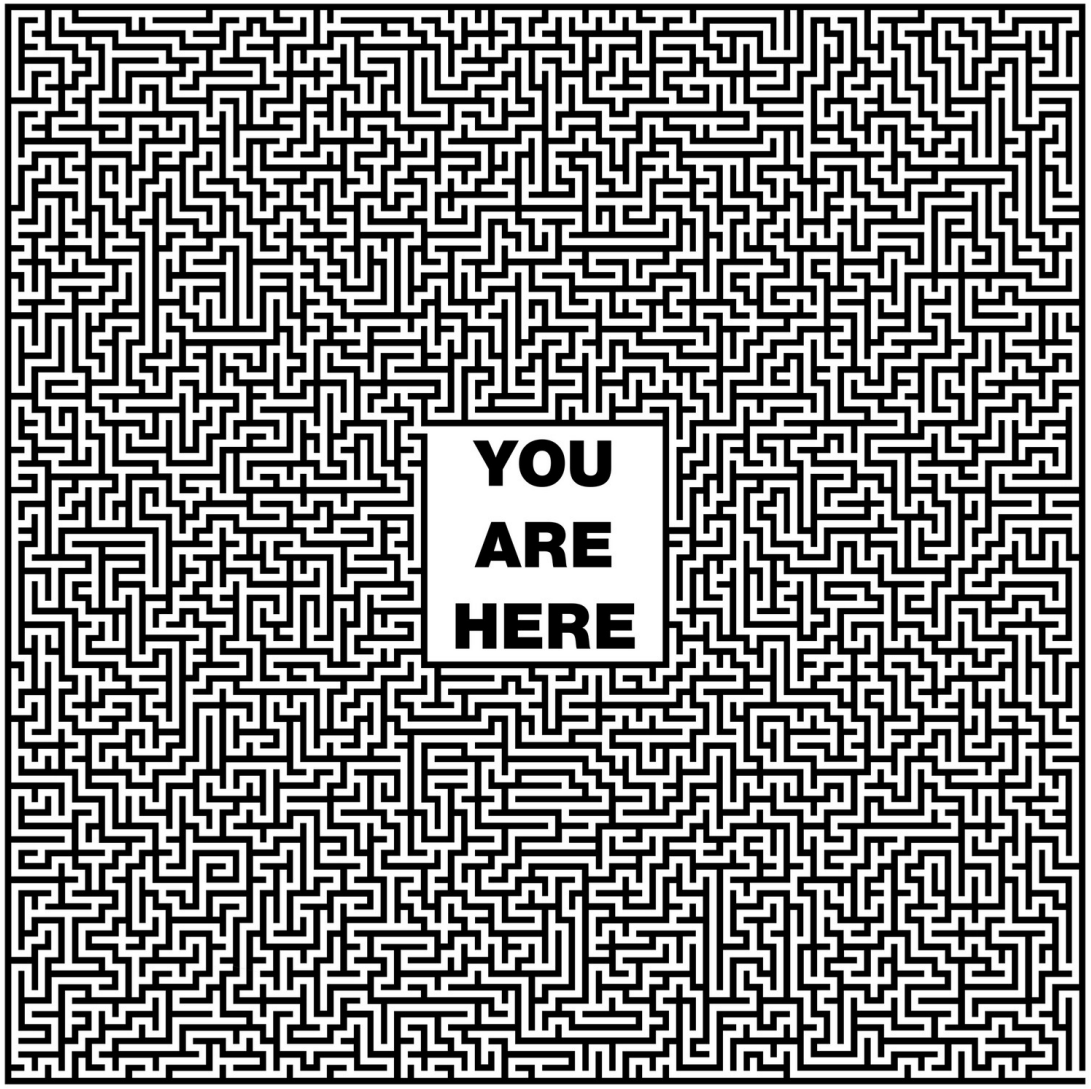


https://csrc.nist.gov/publications/detail/sp/800-115/final

Introducción

- **Las fases de la metodología NIST**:
  1) Planificación:
     1) Decidimos cómo se va a desarrollar el test.
  2) Descubrimiento:
     1) Recopilamos información, escaneamos la red, identificamos servicios y sistemas operativos.
     2) Análisis de vulnerabilidades.
  3) Ataque.
     1) Si logramos comprometer el objetivo y descubrimos nuevos objetivos, volvemos al paso 2.
  4) Informe (de todo el proceso).

Por dónde vamos



Recolección pasiva vs activa

- **Recolección pasiva** (indirecta):
  - Se obtiene información del objetivo sin dejar huella.
  - Involucra fuentes OSINT.
  - Ventaja: difícil de detectar.
  - Desventaja: la información relevante no suele ser accesible.
- **Recolección activa** (directa):
  - Se obtiene información del objetivo interactuando con sus sistemas por lo que se dejará huella.
  - Ventaja: información detallada, y posiblemente más fiable.
  - Desventaja: riesgo de ser detectados (Firewall, IDS/IPS, etc.).

Conoce a tu objetivo

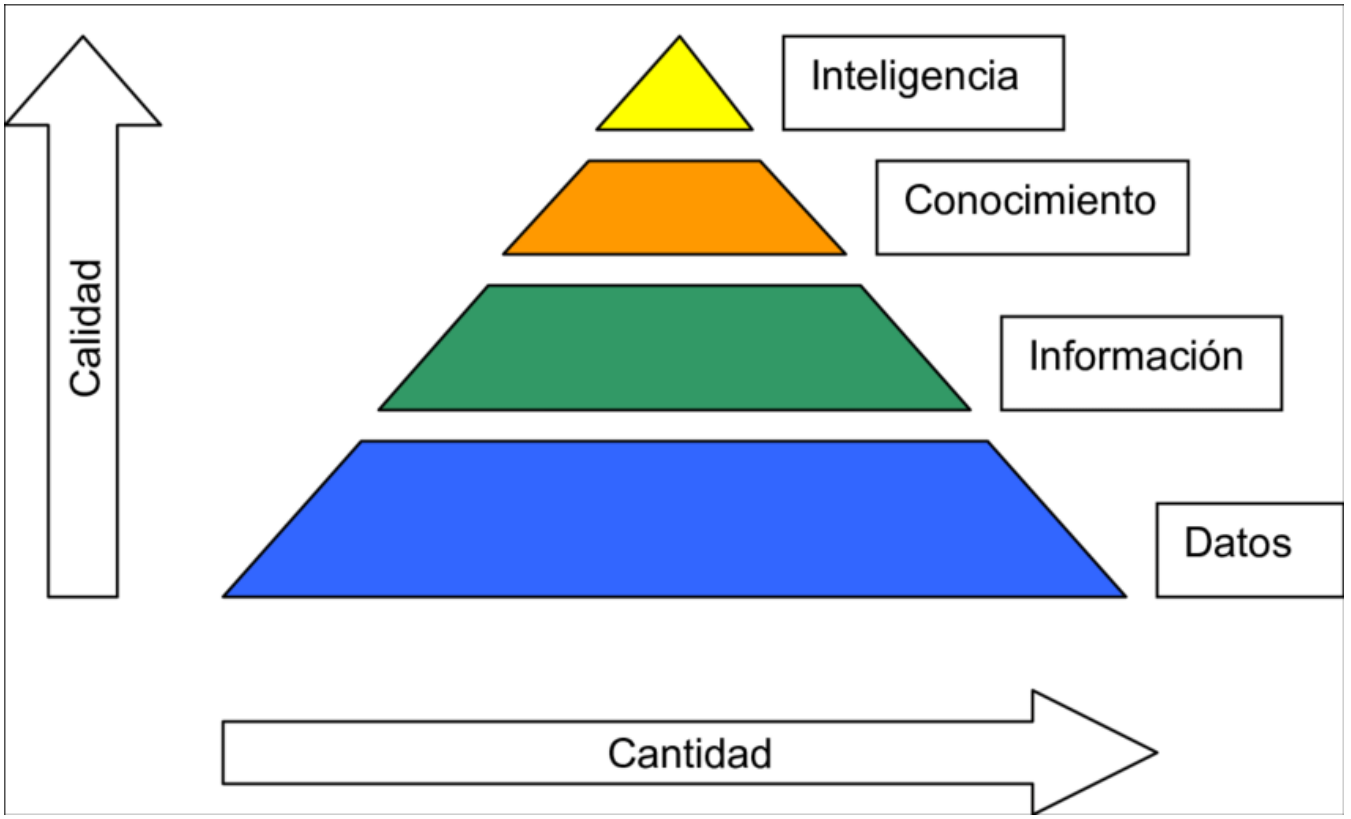
- Los **altos cargos**
  - Pocos conocimientos técnicos.
  - ¿Concienciados en invertir en seguridad?
- La **gerencia**
  - ¿Conscientes de los riesgos?
  - ¿Capacidad para dedicar suficientes recursos a seguridad?
- Los **técnicos**
  - ¿Conocimientos de seguridad?
  - ¿Tiempo y recursos que dedicar a seguridad?

Conoce a tu objetivo

- ¿Cómo es en tu empresa?

Conceptos y definiciones

- **Información o inteligencia.**



Conceptos y definiciones

- **¿Qué es la inteligencia?**
  - Producto → Ciclo de inteligencia.
  - Objetivo → Toma de decisiones.
  - Información ≠ Inteligencia.
- **¿Qué es ciberinteligencia?**
  - Inteligencia + **ciberespacio**.
  - Ámbito tradicional + tecnológico.

Conceptos y definiciones

- **¿Qué es fuente abierta?**
  - No solo es Internet o que tenga soporte tecnológico.
  - **Fuentes de carácter público**: registros, bases de datos de organismos públicos, prensa.
  - Cualquier contenido con independencia del soporte, medio de transmisión o modo de acceso.
  - Que la información no sea secreta, no significa que no tenga valor.

Intelligence Gathering

- También denominado ***footprinting***.
  - Consiste en la recolección de información de todo tipo sobre el objetivo.
  - En esta fase se realiza un reconocimiento pasivo.
  - Se utilizan fuentes de todo tipo para obtener la información: Investigación en fuentes abiertas (OSINT: ***Open Source INTelligence***).
  - La información debe ser procesada para generar inteligencia y permitir diseñar el vector de ataque.

Intelligence Gathering

- **¿Qué información nos interesa?**
  Información legal y comercial
  - Detalles de la compañía y sus empleados (direcciones de email, etc.)
  - Relaciones con otras compañías.
  - Detalles de los proyectos que desarrollan.
  - Documentos legales, marcas registradas, patentes…
  - Noticias y publicaciones sobre la compañía.

Intelligence Gathering

- **¿Qué información nos interesa?**

  Información técnica:

  - Descarga del código de la web para su análisis.
  - Análisis de metadatos de documentos para obtener información de versiones de software, autoría, …
  - Dominios registrados, direcciones IP de los diferentes servicios.
  - Documentación interna que fue publicada por error y es accesible.
  - Información de puertos abiertos, máquinas y servicios que se han ido localizando.
  - Infraestructura de la intranet y protocolos empleados.

Intelligence Gathering

- **Disciplinas**:
  - **OSINT**: Open Source Intelligence.
  - **HUMINT**: Human Intelligence.
  - **SOCMINT**: Social Media Intelligence.
  - **CYBINT**: Cyber Intelligence.
  - **GEOINT**: Geospacial Intelligence.
  - **SIGINT**: Signal Intelligence.
  - ...

Ciclo de vida de Inteligencia

1. Planificación

El primer eslabón de la cadena es definir los objetivos que queremos conseguir. En esta primera fase planificamos la estrategia y las acciones a seguir para la recogida de información, así como el tipo de información que queremos recabar.

2. Recolección

En esta fase pasamos a recolectar la información definida como objetivo en la fase de planificación, siempre procedente de fuentes fiables, públicas o privadas.

3. Análisis

Es la fase donde transformamos la información recabada en bruto y la procesamos para convertirla en información útil e inteligente que sirva a los propósitos estratégicos, tácticos y operativos de nuestra ciberinteligencia.

4. Identificación

Una vez procesados los datos, los evaluamos para extraer un producto de ciberinteligencia, es decir, reconocemos los riesgos que amenazan nuestra organización y determinamos su impacto y alcance.

5. Acción

Fruto de las fases anteriores, elaboramos un informe detallado y entendible donde determinamos el plan de acción frente a posibles incidentes de seguridad. Es la fase de toma de decisiones.

6. Evaluación

En esta última fase valoramos todas las fases del ciclo completo para su reevaluación y mejora continua.

Etapas del Plan Estratégico de Ciberinteligencia – Ingenia

Ciclo de vida de inteligencia

- **Fases del ciclo de inteligencia** (INCIBE).

Ciclo de vida de inteligencia

- **Fases del ciclo de inteligencia** (INCIBE).
  1) **Requisitos**. Se establecen las condiciones para conseguir el objetivo o resolver el problema que ha originado la investigación.
  2) **Identificar fuentes de información relevante**. A partir de la fase anterior, se determinan las fuentes de interés que serán recopiladas (imposibilidad de abordar toda la información disponible).
  3) **Adquisición**. Obtención de la información de las fuentes enumeradas.
  4) **Procesamiento**. Dar formato a la información recopilada para su posterior análisis.
  5) **Análisis**. Se genera inteligencia relacionando la información de distinto origen, mediante la búsqueda de patrones, etc.
  6) **Presentación de Inteligencia**. Se presentan las conclusiones de manera eficaz, útil y comprensible.

Problemática en el footprinting

- **Problemáticas en la recolección de información**:
  - **Demasiada información**. El exceso de información disponible conlleva a que la investigación pueda ser como buscar una aguja en un pajar.
  - **Fiabilidad de las fuentes**. Hoy en día es un asunto complejo relacionado con la desinformación y las ***fakenews*** (Ej: deepfake).

Source Reliability		Information Creditability	
A	Completely reliable	1	Confirmed by other sources
B	Usually reliable	2	Probable
C	Fairly reliable	3	Possible
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Reliability cannot be judged	6	Truth cannot be judged

https://rusi-ns.ca/a-system-to-judge-information-reliability/

FIN