**Clase lunes 16/4/2018:**

Presentaciones sobre NMAP, Wireshark y Snort.

- NMAP: La he hecho yo.

- Wireshark: Es software libre que permite analizar el tráfico de red. Soporta hasta más de 1100 protocolos. Está programado en C y C++.

Capta el tráfico de la red y permite ver y filtrar tanto por origen/destino como por protocolo.

En una empresa puede utilizarse para monitorización de conexiones.

Permite guardar trazas de la red en un archivo.

- Snort (sistema de detección de intrusos): Está desarrollado por cisco. Es un sistema basado en reglas (propias o públicas). En cuanto a su funcionamiento, siempre está capturando paquetes, cogen la parte que quieren actualizar de cada paquete, se introduce en un sistema de detección de reglas, y luego, si se cumple alguna regla, se redirecciona a un sitio u otro en función de la regla establecida.

Tiene la ventaja de que monitorea muchos hosts en una red y genera muy poco tráfico. Aún así, tiene la desventaja de que no puede examinar el trafico cifrado.

Diapositivas:

El usuario y persona humana es la mayor responsable de lo que pase con su seguridad en internet. Lo más importante para una empresa es que un equipo se encarga de hacer lo de siempre, pero teniendo en cuenta la seguridad.

Modelo conceptual de seguridad:

Seguridad del personal, de la información, del material, de las instalaciones, y de las operaciones.

STIC: Seguridad de las Tecnologías de la Información y las Comunicaciones.

Confidencialidad, integridad y disponibilidad.

- Confidencialidad: Solo las personas que tu quieres puedan acceder a la información que tú eliges. Si suplantamos la identidad o rompemos la seguridad podemos cargarnos la confidencialidad.

- Integridad: Los datos tienen que ser los que se esperan de ellos, sin que sean modificados o destruidos en su almacenamiento.

- Disponibilidad: El ataque más famoso es la denegación de servicio, por lo que la disponibilidad se centra en que los datos de una empresa estén disponibles en todo momento.