Clase 25

# SEGURIDAD INFORMATICA

Terminologías Esenciales

Amenaza: potencial violación de seguridad

Vulnerabilidad: debilidad/error en el sistema

Objeto de Evaluacion: (White hat) sistema informatico que se somete a evaluación de seguridad

Ataque: asalto en la seguridad del sistema

Exploit: vulnerabilidad conocida o no



Seguridad: estado de bienestar de la información

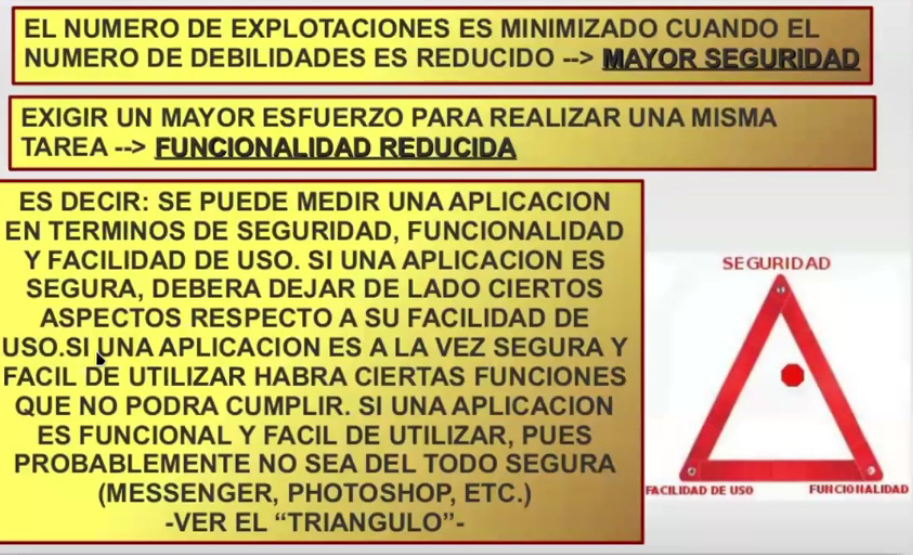
Seguridad defino eso por:

Confidencialidad: ocultar info a voluntad

Autenticidad: poder demostrar el origen y destino de la informacion

Integridad: confianza de datos

Disponibilidad: Habilidad de utilizar la info



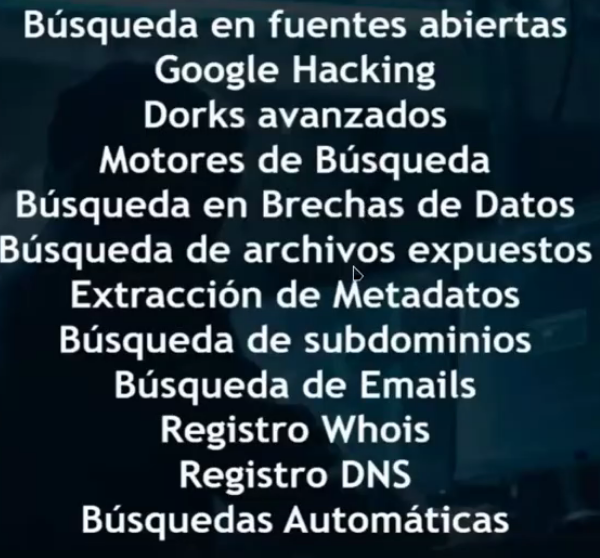
# Ehtical Hacking

Basicamente, es una simulación de un ataque a un sistema. INFORMADO a la empresa con anterioridad y a su vez, se brindan pasos para mitigar lo máximo posible la posible brecha de seguridad, si la hubiere.

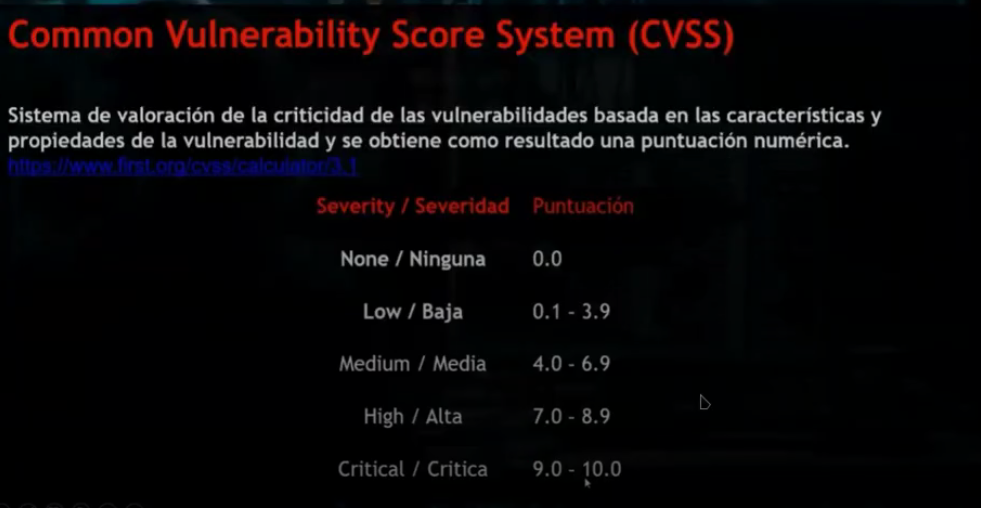
# Metodologia de Ataque



1. Adquisicion de Informacion del Objetivo. De manera legal, basciamente, información publica (fuentes abiertas). Ejemplo: \_intelligenceX, hunter, Googledorks



1. Escaneo de red sobre el objetivo. Buscar puertos, SO, servicios.
2. Obtencion detallada del objetivo sobre los PUNTOS DE ENTRADA (logins generalmente)
3. Identifica y categoriza las vulnerabilidades. (Nessus)



1. Ejecucion del ataque a la vulnerabilidad. Se ejecuta a manera consciente para no romper nada (?
2. Reporte técnico y empresarial sobre lo encontrado y como poder buscar soluciones al respecto.