Actividad 2.1. Ejercicio: clasificación de atacantes.

Realiza un mapa conceptual de los tipos de atacantes de un sistema informático atendiendo a su actividad.

Actividad 2.2. Cuestión: fases de un ataque informático.

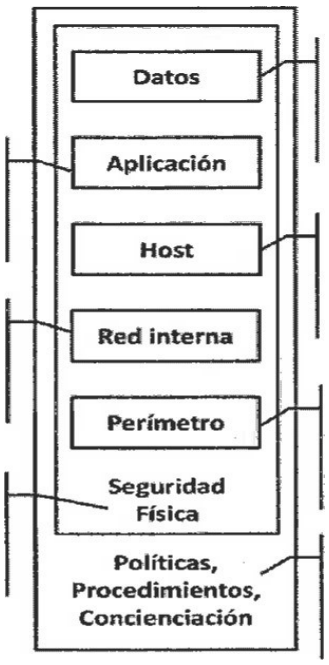
¿Cuáles son las fases de un ataque informático? Describe alguna característica específica de cada una de las fases.

Actividad 2.3. Cuestión: herramientas para el ataque.

¿Qué es una puerta trasera? Y, ¿un exploit? ¿En qué se diferencia un rootkit de un virus?

Actividad 2.4

Realiza un esquema con Smart Art que refleje la organización en niveles de la tabla 2.4 en formato gráfico Así dividiremos el problema global de la seguridad en otros más pequeños y este esquema nos ayudará a mejorar la calidad de la implantación del plan de seguridad.



Práctica 2.5

Realiza un scanner a la máquina metasplotable 2

1.- Busca qué son cada uno de los puertos abiertos.

2.- Scanea metasplotable 2 con nmap para ver la información de la hora, fecha, tiempos de ping y latencia.

3.- Scanea desde Kali tu máquina real, metasplotable y otra máquina virtual de windows 10al mismo tiempo. y redirige la salida a un fichero llamado nombreapellidos.txt

4.- Escanea todos los puertos abiertos de toda la clase y todas las máquinas instaladas en puente.

5.- ¿Qué es el scaneo multiobjetivo con Octetos? Scanea ahora sólo los equipos que hayas encontrado encendidos en el aula usando el scaneo multiobjetivo.

6.- Ahora crea un fichero con las direcciones IP de tu máquina real, la de metasplotable y la mv de windows 10. y scanea dichas máquinas usando ese fichero.

7.- ¿Has encontrado algún rango de direcciones IP que el DHCP no utilice en el aula?¿Cuál?¿Cuál sería el rango que deberías scanear para ver qué equipos hay encendidos en el aula si tuvieras que usar un rango?

8.- ¿Y si quieres scanear todos los equipos de la red excepto el tuyo, cuál es el comando nmap?

9.- Ahora averigua cuántos de los equipos scaneados en el aula tienen windows y cuántos Linux.

10.- Ahora obtén más información sobre los puertos abiertos en la mv de metasplotable, incluyendo las versiones de los servicios.

11.- Comprueba si metasplotable tiene firewall.

12.- ¿Cómo podrías averiguar sin largas esperas cuántos equipos hay encendidos en el aula?

13.- ¿Cómo podrías escanear de forma rápida los puertos usados con más frecuencia en metasplotable?

14.- ¿Qué opción de nmap nos permite obtener los puertos ordenados de forma incremental? Ejecútalo en windows 10.

15.- ¿Cuál es la opción de nmap para obtener una lista de las interfaces del equipo desde el que estamos lanzando el rastreo?

16.- Escanea ahora la máquina de metasplotable2 en el puerto 21