Actividad 2. Vectores de ataque

**Objetivos**

Con esta actividad vas a conseguir documentar un ciberdelito, analizándolo al máximo en su funcionamiento, bien a través de código, vídeos, artículos científicos, prensa, etc.

**Descripción** **de la actividad**

Podemos definir un vector de ataque como el camino que usa un ciberdelincuente para acceder al activo objetivo del ataque.

A lo largo de esta asignatura conocerás la existencia de múltiples ciberdelitos: *phising, smishing*, inserción de *malware*, *keyloggers, botnets, pharming, carding, skimming,* fraude del CEO, *rogues* y un largo etcétera, pero en todos estos casos, ¿cómo es el vector de ataque? o al menos ¿cómo creemos que haya podido ser?, es esta la tarea que se os asigna en esta actividad.

Un pequeño ejemplo concreto: si quisieras entender un *ransomware* y dar respuesta a cómo infecta una máquina, primeramente, verías un vector de ataque en forma de ingeniería social, convenciendo al usuario que haga *click* en algún sitio determinado, a partir empieza a recorrer directorios del disco, haciendo el cifrado correspondiente, para a continuación recibir un mensaje de rescate de la clave de descifrado. Esto es un proceso cíclico y bien se puede encontrar como es en Internet, aunque cuando lo veas en clase, lo acabarás de entender.

Evalúa la calidad de la información que dan estas herramientas, y si crees que, en manos no deseadas, pudieran ser el inicio de un delito contra la persona. ¿Crees que es fácil realizar un delito informático con la información recopilada?, en caso afirmativo, ¿Cómo crees que se podrían evitar?

**Rúbrica**

|  |  |  |  |
| --- | --- | --- | --- |
| Delitos informáticos en fuentes abiertas | Descripción | Puntuación máxima  (puntos) | Peso  % |
| Criterio 1 | Información recopilada | 4 | 40 |
| Criterio 2 | Explicación detallada del ataque | 4 | 40 |
| Criterio 3 | Recomendaciones para evitar el ataque | 2 | 20 |
|  |  | **10** | **100 %** |

**Extensión de la actividad**

Sin delimitación de extensión. Puede ser viable entregar código fuente, vídeos demostrativos o tantos recursos como se estime oportuno.