Actividad

Curso**: Elaboración de material de apoyo para Tecnología y FPB de los CEPA**

Ataques, conceptos y técnicas

Ciberseguridad – Sesión 3

Índice

Introducción

En esta actividad veremos las distintas vulnerabilidades que usan los ciberdelincuentes para atacarnos, como es el software malicioso o *malware*.

Un buen punto de partida para estudiar esto es el capítulo 2 del curso "Introducción a la ciberseguridad" de la CISCO Academy. Este capítulo abarca las maneras en que los profesionales de la ciberseguridad analizan qué ocurrió después de un ciberataque.

- Explica las vulnerabilidades de software y hardware de seguridad y las distintas categorías de las vulnerabilidades de seguridad.
- Analiza los diferentes tipos de software malicioso (conocido como malware) y los síntomas de malware.
- Cubre las diferentes maneras en que los atacantes pueden infiltrarse en un sistema, así como los ataques de denegación de servicio.

- La mayoría de los ciberataques modernos se consideran ataques combinados. Los ataques combinados usan varias técnicas para infiltrarse en un sistema y atacarlo. Cuando un ataque no puede evitarse, es el trabajo del profesional de ciberseguridad reducir el impacto de dicho ataque.

Objetivos

1. Conocer qué es el software malicioso o malware.
2. Conocer los tipos de malware.

Desarrollo de la actividad

Actividad 1

Aquí tienes un vídeo resumen de cómo funcionó el ransomware WanaCry.

https://www.youtube.com/watch?v=tDdLWN4aWh4

Una vez visto el vídeo, tienes aquí unos cuantos recursos que te pueden ayudar a conocer más sobre los malware y, en concreto, cómo funciona un ransomware y cómo podemos protegernos de ellos. Te serán utiles para responder a las preguntas que vienen después.

- El ransomware, cada vez más peligroso. Protégete
- Importante oleada de ransomware afecta a multitud de equipos
- Ransomware WanaCry: Qué es y cómo proteger su PC
- Un ciberataque deja fuera de juego la intranet de Telefónica en toda España
- Cómo un investigador anónimo ha detenido "accidentalmente" y con 10 euros el ransomware WannaCrypt

Una vez que has visto cómo funciona este ransomware, responde a las siguientes preguntas con ayuda de los recursos que hemos dejado al final de la actividad:

1. ¿Cómo funcionó WanaCry? ¿A quién afectó?

2. ¿Quién ayudó a bloquear el efecto y cómo lo consiguió?

3. El WanaCry se pudo solventar, pero pueden surgir ransomware similiares. ¿Qué puedo hacer para protegerme? Escribe 5 medidas de protección o precaución que puedo tener.

4. ¿De qué forma puede infectarse mi equipo con un ransomware?

5. ¿Qué pasa si mi equipo se infecta con ransomware y no quiero pagar el rescate?

6. Al pagar el rescate, ¿se descifran los datos?

7. ¿Los smartphones también podrían estar en riesgo?