[FORT] TEMA 8: Arquitectura de seguridad de Windows 11

Existen 3 niveles de seguridad:

- Equipos Cliente
- Equipos cliente de Dominio
- Redes Clasificadas (A nivel de fuerzas de seguridad)

Un equipo Windows no se considera un equipo seguro hasta que se ha pagado e instalado una licencia en el equipo. Si se tiene una licencia de Windows 8 o 10, se puede usar para activar Windows 11. Existen 3 tipos de licencia:

- Home: No permite active directory
- Profesional: Centrada en active directory
- Enterprise: Similar a la profesional.

Windows 11 y requisitos de instalación

Windows 11 exige tener un chip TPM 2.0 para cifrado de claves, ademas de una CPU y RAM mínimos. Estos requisitos pueden ser anulados usando rufus para crear el instalador de Windows 11, si se hace esto, las claves de cifrado no serán almacenadas en el TPM, pero el equipo seguirá siendo funcional.

Capa física

La capa física se podría decir que por un lado equivale a cosas de seguridad que se pueden configurar en la BIOS (Contraseña de la BIOS, de donde se arranca, si las teclas de selección de booteo están habilitadas...) Por otro lado, en una caja física se securiza si alguien abre una caja, estableciendo un sistema de alarma que envíe un mensaje de alerta si se ha abierto un equipo.

Seguridad basada en hardware

- TPM 2.0 (Trusted Platform Module): Chip físico que almacena parte de las claves de cifrado y descifrado del equipo. Normalmente una placa base trae 2 chips TMP para tener uno de backup en caso de que falle uno de ellos.
- Arranque Seguro (SecureBoot): Asegura que solo software firmado y certificado se puede arrancar sobre el hardware.
- Virtualización de seguridad (VBS): Utiliza un entorno se parado para ejecutar ciertos programas, generalmente se usa cuando aparece la UAC.

Seguridad del Núcleo del sistema

- Protección de Código Basada en virtualización (HVCI)