CURSOS INTERSEMESTRALES

PROTECO

Seguridad

Isolation and compartmentalization

Security domain

Colección de aplicaciones o dispositivos físicos, que se encuentran separados y operan de manera independiente de los otros dispositivos.

PROTECO

STATIONX
THE CYBER SECURITY COMPANY

Disminuye la superficie de ataque.

Utilizando dominios de seguridad permitiendo crear diferentes niveles de usabilidad, seguridad y diferentes identidades.

Ventajas:

*)Permite manejo de multiples identidades.

*)(dependiendo) puede protegernos incluso de zerodays

*)Mitiga el impacto de un ataque.

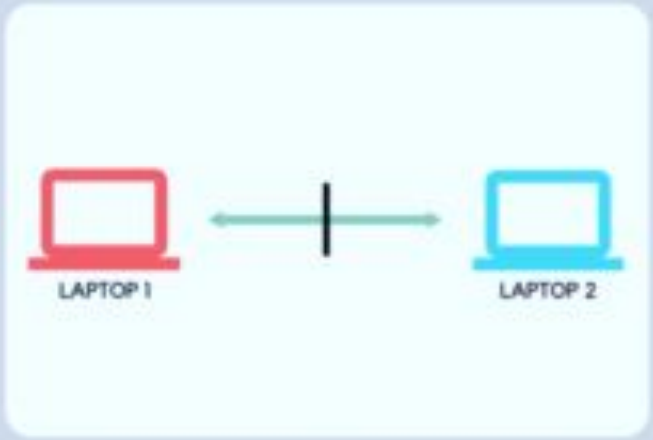
*)Los domnios pueden ser usados recursivamente. (dominios dentro de otros)

Tipos:

*) Fisica: Computadoras separadas, multiples discos duros. Equipos en ubicaciones distintas,etc.

*)Virtual: Vlans, maquinas virtuales, sandboxes, dual boot, etc.

VIRTUAL DOMAIN



PHYSICAL DOMAIN

Fisical Isolation:

*)Los identificadores únicos (mac, seriales, etc) pueden ser asociados a ti a través de las compras realizadas.

*)Es recomendable copiar o cambiar los identificadores únicos.

PROTECO

Ej:

macchanger (Se hará de forma aleatoria el cambio de mac).

dmidecode (Ver los información de hw en nuestro dispositivo)

PROTECO

Mitigaciones:

*)Comprar de forma anónima.

*)Utilizar VM's (ya que cambia los valores de HW directamente)

*)Utilizar sw especializado.

*)Comprar equipo desechable.

*)Crear lans distintas separando dispositivos confiables de los no confiables.

Virtual:

*Utilizar aplicaciones autocontenidos (ej: apps portables), application as a Service (AaaS)

*)En algunos casos deniability, protección contra examen forence.

*)Recomendable no solo usar las dadas por defecto.

PROTECO

DualBoot:

Permite tener dos dominios separados, pero no es tan flexible. Pero no hay gran isolation, ya que un Sistema puede comprometer al otro.

PROTECO

Sandbox:

"Monitoriza y restring el acceso al Sistema de archivos a un proceso".

Ventajas:

*)Evita propagación.

*)Puede ser usado recursivamente (+seguridad)

*) Hay gran cantidad de estas, con distintas funcionalidades.

*)Pueden protegerte incluso de 0days.

Desventajas:

*)No evitan la infección

*)Pueden ser escapadas.

*) Pueden dificultar la transmision de archivos legitimos.